



Passwordstate Mobile Client Manual

© 2016 Click Studios (SA) Pty Ltd

Table of Contents

| | |
|--|----------|
| Foreword | 0 |
| Part I Introduction | 3 |
| Part II User Preferences | 3 |
| Part III System Settings | 4 |
| Part IV Mobile Client Permissions | 6 |
| Part V Mobile Client Usage | 8 |

1 Introduction



Welcome to the Passwordstate Mobile Client Manual.

This manual will provide instructions for configuring various settings and permissions for Mobile Client support, as well as how to use the Mobile Client itself.

The Passwordstate Mobile Client supports the following mobile devices - iOS, Android, Windows 8 Phone and Blackberry.

By default, you can access the Mobile Client web site by pointing your mobile clients browser to the address <https://<MyPasswordstateURL>/mobile>. As a separate install of the Mobile Client is also provided, this URL may differ as your web/system administrators may have stand-alone installation on a different web server.

Note: As most mobile client devices will be configured to access web sites via a cellular/mobile networks, your Firewall/System Administrator(s) will need to ensure external DNS is configured for the URL you're using, and the firewall itself can pass traffic to your Passwordstate web site. As the Mobile Client web site is intended to be accessed outside of your internal network, you may wish to use the provided instructions to install the mobile client web site onto a web server in your DMZ, or on another 'hardened' server.

The following table summarizes each of the key areas for configuring and using the Mobile Client.

| | |
|---|---|
| User Preferences | Allows the users to specify various settings when using the Mobile Client, and also to specify the Mobile Pin Number for authentication |
| System Settings | Allows Security Administrator(s) of Passwordstate to specify various system wide settings for the Mobile Client |
| Mobile Client Permissions | Provides instructions for how to apply permissions for accessing passwords via the Mobile Client |
| Mobile Client Usage | Provides instructions for the Mobile Client Platform itself |

2 User Preferences

On the 'Preferences' screen on the main Passwordstate web site, you will find various settings which control how the Mobile Client will behave for you. Below is an explanation of each of these settings.

Note 1: Your Passwordstate Security Administrator(s) may disable the use of the Mobile Client, in which case all option on this tab will be disabled. The length of the Pin Number is also controlled by your Security Administrator(s).

Note 2: The first two settings below can also be configured for your account via a 'User Account Policy', in which case they will be disabled on this screen.

| | |
|--------------------------------|--|
| Default Home Page | You can either choose your default home page to browse/filter all the Password Lists you have access to, or go straight to a screen where you can search for the password record you require |
| Limit the Number of Records to | As cellular/mobile networks are typically slower than local networks, it's recommended you limit the number of records returned to help with performance. |
| Mobile Pin Number | The Pin Number you will use to authenticate with when using the Mobile Client - this is in conjunction with your UserID for Passwordstate |

Preferences

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

home page
miscellaneous
color theme
authentication options
mobile access options
api keys

Please select appropriate options below for accessing Passwordstate via a mobile device.

Set the Mobile default home page to:

Password List Search Password Search

When searching for Password Lists or Passwords, limit the number of records displayed to:
(as mobile devices typically operate on slower networks, limiting the number of records returned can help improve performance)

Mobile Pin Number:

 (Minimum length is : 4)

3 System Settings

The Mobile Access Options tab on the screen Administration -> System Settings allows you to specify multiple settings for how the Passwordstate Mobile Client behaves for your users.

Allow Mobile clients to access Passwordstate:

If you do not wish to allow Mobile Access to passwords, you can disable access altogether by selecting this option.

🚩 Note 1: If you choose to disable Mobile Access, it is recommended you set the option below to 'No', and then go to the screen Administration -> Passwords Lists -> Mobile Access Bulk Permissions, and then disable Mobile Access for all permissions

🚩 Note 2: Even if this option is enabled, your Firewall/System Administrators still need to configure external DNS and allow access through the firewall for anyone to access the Mobile Client web site

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

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

Use the following authentication method for the Mobile Client:

There are four types of Authentication Options available for the Mobile Client:

- Mobile Pin Number - a numeric pin code that the user can specify on their Preferences screen
- Active Directory Authentication - authenticate using the users Active Directory UserID and Password (🚩 Your Passwordstate web site must be using a Trusted SSL Certificate in order to use this authentication option)
- Email Temporary Pin Code - Two-Factor Authentication using the emailing of a temporary pin code, which expires after a set period of time
- AuthAnvil Authentication - Two-Factor Authentication using Scorpion Software's AuthAnvil solution
- Google Authenticator - Two-Factor Authentication using Google's Authenticator solution
- Duo Push Authentication - Two-Factor Authentication using Duo Security's Push Authentication solution
- SafeNet Authentication - Two-Factor Authentication using SafeNet's On-Premise or Cloud Based authentication services
- One-Time Password - Two-Factor Authentication using either the TOTP or HOTP algorithms for hardware or software based tokens - TOTP is Time-Based and HOTP is Counter-Based
- RADIUS Authentication - Authenticate against a RADIUS server, which can be configured for different authentication methods per user account - including multiple two-factor methods if required

The Mobile Access Pin Number for user authentication must be a minimum length of:

You can choose the length of the Mobile Access Pin Number the users must use to authenticate with. When the users specify their own Pin Number on the Preferences screen, or use the option to generate one, it must meet the minimum length requirement of this setting.

The Inactivity Timeout for Mobile Access is (mins)

If the user forgets to log out of the Mobile session, this setting will automatically log them out after the set period of inactivity, and also clear their authenticated session.

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

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

System Settings

To modify the system settings, please make changes within the appropriate tabs below, then click on the 'Save' button.

active directory options | allowed ip ranges | api keys | authentication options | branding | check for updates | email alerts & options | high availability options
hosts | miscellaneous | **mobile access options** | password list options | password options | password reset options | proxy & syslog servers | usage tracking
user acceptance policy

Please specify appropriate settings for Mobile Access to Passwordstate.

Allow Mobile clients to access Passwordstate: (Permissions needs to be set at the Password List level if this option is enabled)
 Yes No

When adding new permissions to Password Lists, enabled Mobile Access by default: (Permissions can also be changed in bulk on the page Administration -> Password Lists)
 Yes No

Use the following authentication method for the Mobile Client:
Mobile Pin Number

The Mobile Access Pin Number for user authentication must be a minimum length of:
4

The Inactivity Timeout for Mobile Access is (mins):
5

Protect against brute force dictionary authentication attempts by locking out an active session after the following number of failed login attempts:
5

Save Save & Close

4 Mobile Client Permissions

In addition to enabling Mobile Access for your users on the [System Settings](#) screen, access is also granted via applying permissions at the Password List level.

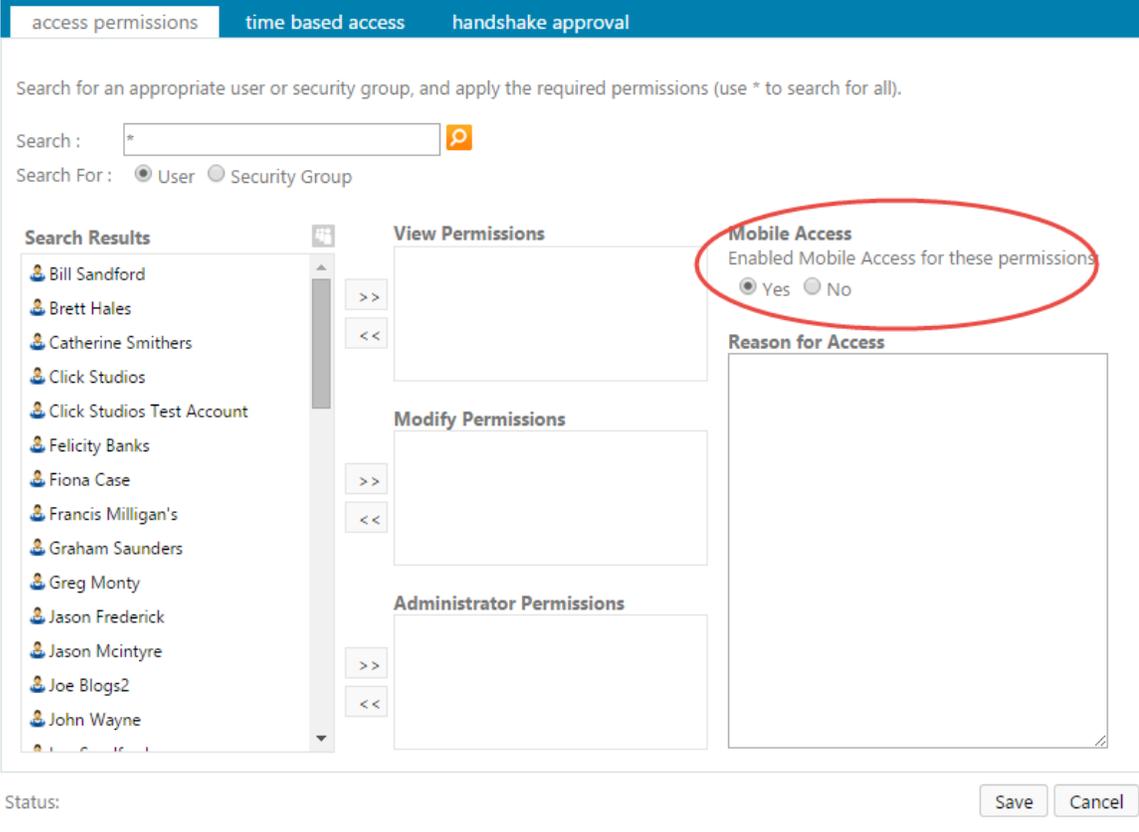
As you're able to apply permissions at the Password List level, this means you don't need to expose all passwords via the Mobile Access Client if you don't want to.

Enabling/Disabling Mobile Access when Adding New Permissions

When you add new permissions to a Password List, you can choose to enable/disable Mobile Access using the 'Mobile Access' option on the screen.

Grant New Permissions

To grant additional permissions to the '**Servers**' Password List, simply click on the three **Tab**s below to specify appropriate permissions and/or settings.



access permissions time based access handshake approval

Search for an appropriate user or security group, and apply the required permissions (use * to search for all).

Search : 

Search For : User Security Group

Search Results

- Bill Sandford
- Brett Hales
- Catherine Smithers
- Click Studios
- Click Studios Test Account
- Felicity Banks
- Fiona Case
- Francis Milligan's
- Graham Saunders
- Greg Monty
- Jason Frederick
- Jason McIntyre
- Joe Blogs2
- John Wayne

View Permissions

Mobile Access
Enabled Mobile Access for these permissions
 Yes No

Reason for Access

Modify Permissions

Administrator Permissions

Status: Save Cancel

Enabling/Disabling Mobile Access for Existing Permissions

With the permissions already applied to your Password Lists, you can choose to enable/disable Mobile Access by selecting the 'Enable/Disable Mobile Access' option under the 'Actions' dropdown menu.

Person Password List Permissions

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

Servers User Account Local Security Group Active Directory Security Group

| Actions | User or Security Group | Guest | View | Modify | Admin | Mobile Access | Expires |
|---------|------------------------|-------|------|--------|-------|---------------|---------|
| ▼ | Fiona Case | ✓ | | | | ✓ | |
| ▼ | Juniper Engineers | | | | ✓ | ✓ | |
| ▼ | Mark Sandford | | | | ✓ | ✓ | |
| ▼ | Steve Marcel | ✓ | | | | ✓ | |
| ▼ | William Wilson | | ✓ | | | | |

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

Enabling/Disabling Mobile Access Permissions in Bulk

If you would like to enable/disable Mobile Access permissions for more than one Password List at a time, then you can do so via the page Administration -> Password Lists -> Mobile Access Bulk Permissions.

Mobile Access Bulk Permissions

The page allows you to query all the permissions for one or more Password Lists, and then either enable or disable Mobile Access as required.

mobile access bulk permissions

I would like to Enable Disable Mobile Access for the Permissions I select below.

Password List(s)

Filter ...

- Banking Sites
- Canon Printers
- Customers\A\Database Accounts
- Customers\A\Generic_Unix
- Customers\A\Oracle Database Tier
- Customers\A\SCCM**
- Customers\A\Servers
- Customers\B\LAN Switches
- Customers\B\Network Monitoring
- Customers\B\SQL Server**
- Customers\True Power SA\Routers and Switches
- Customers\True Power SA\Stealth Appliances
- Gen Field Encryption**
- Gen Field Encrvation 2

Count: 35

Permissions (Select All)

- Customers\Customer's A\SCCM \ Brett Hales (Guest)
- Customers\Customer's A\SCCM \ Felicity Banks (Guest)
- Customers\Customer's A\SCCM \ Jason Frederick (Guest)
- Customers\Customer's A\SCCM \ Mark Mills (Guest)
- Customers\Customer's A\SCCM \ Mark Sandford (Admin)
- Customers\Customer's A\SCCM \ Philip Moorebank (Guest)
- Customers\Customer's A\SCCM \ Tracey Sandford (Admin)
- Customers\Customer's A\SCCM \ Trent Wilson (Guest)
- Customers\Customer's A\SCCM \ William Wilson (View)
- Customers\Customer's B\SQL Server \ Mark Sandford (Admin)
- Gen Field Encryption \ Mark Sandford (Admin)

Count: 11

Status: Save Cancel

5 Mobile Client Usage

This following information provides instructions for how to use the Mobile Client itself. The following features are currently available in the Mobile Client:

- Authentication
- Browse/Search Password Lists that you have access to
- Browse/Search Passwords within a selected Password List
- Search for an individual password record, across all the Password List you have access to - similar to searching on the 'Passwords Home' page on the normal Passwordstate web site
- View password records

Mobile Client Authentication

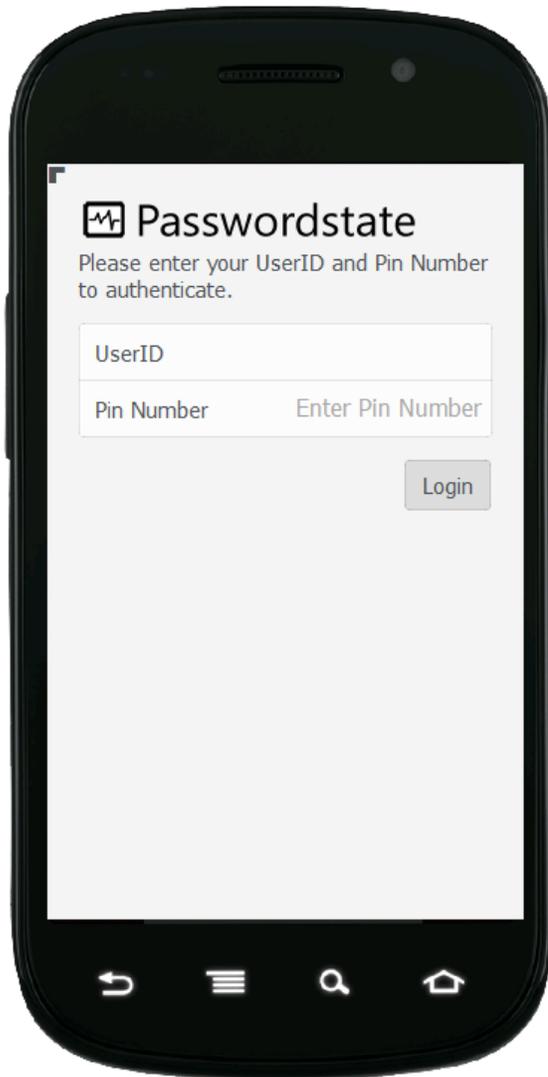
There are 4 different types of Authentication Options for the mobile client, including:

- Mobile Pin Number - a numeric pin code that the user can specify on their Preferences screen
- Active Directory Authentication - authenticate using the users Active Directory UserID and Password
- Email Temporary Pin Code - Two-Factor Authentication using the emailing of a temporary pin code, which expires after a set period of time
- AuthAnvil Authentication - Two-Factor Authentication using Scorpion Software's AuthAnvil solution
- Google Authenticator - Two-Factor Authentication using Google's Authenticator solution
- Duo Push Authentication - Two-Factor Authentication using Duo Security's Push Authentication solution
- SafeNet Authentication - Two-Factor Authentication using SafeNet's On-Premise or Cloud Based authentication services
- One-Time Password - Two-Factor Authentication using either the TOTP or HOTP algorithms for hardware or software based tokens - TOTP is Time-Based and HOTP is Counter-Based
- RADIUS Authentication - Authenticate against a RADIUS server, which can be configured for different authentication methods per user account - including multiple two-factor methods if required

Each Authentication Screen will look slightly different, dependent on the Authentication Option selected.

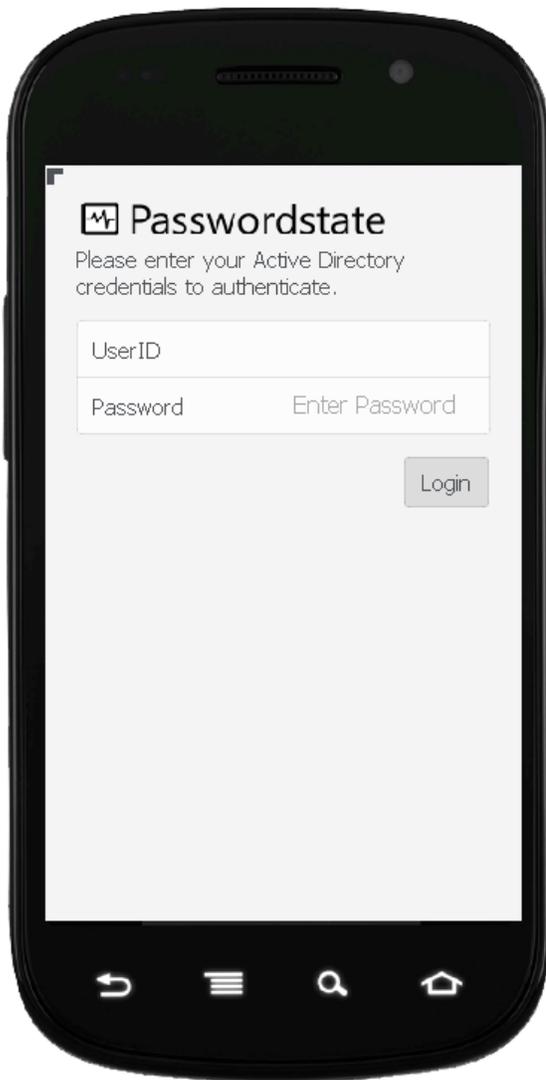
 **Note:** If using the AD Integrated version of Passwordstate, it's not necessary to specify the UserID in the format of Domain\UserID - you can simply type just the UserID. The only exception to this would be if you had multiple Active Directory domains registered in Passwordstate, and there were duplicate logon names in AD.

Mobile Pin Number Authentication Screen

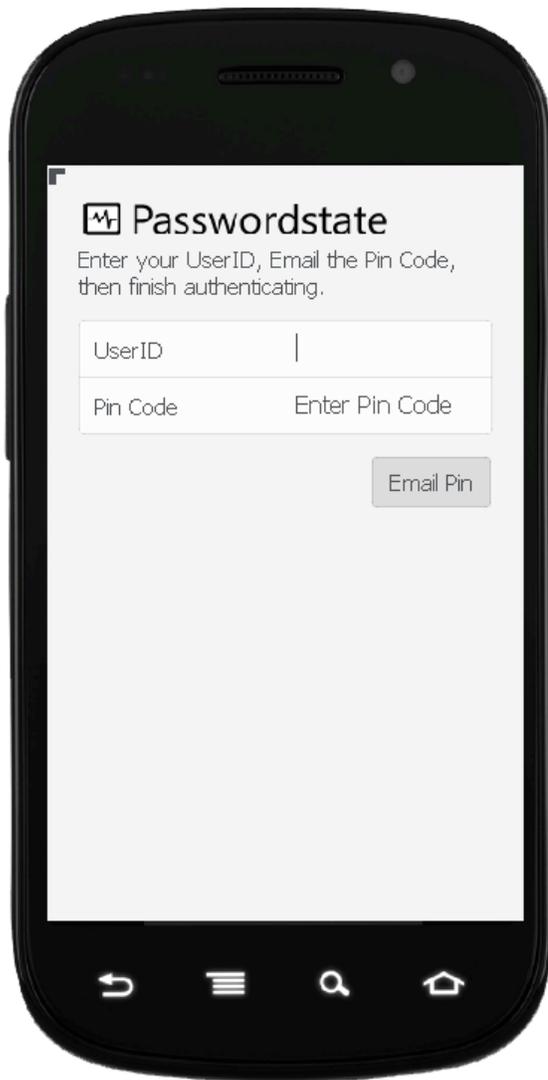


Active Directory Authentication Screen

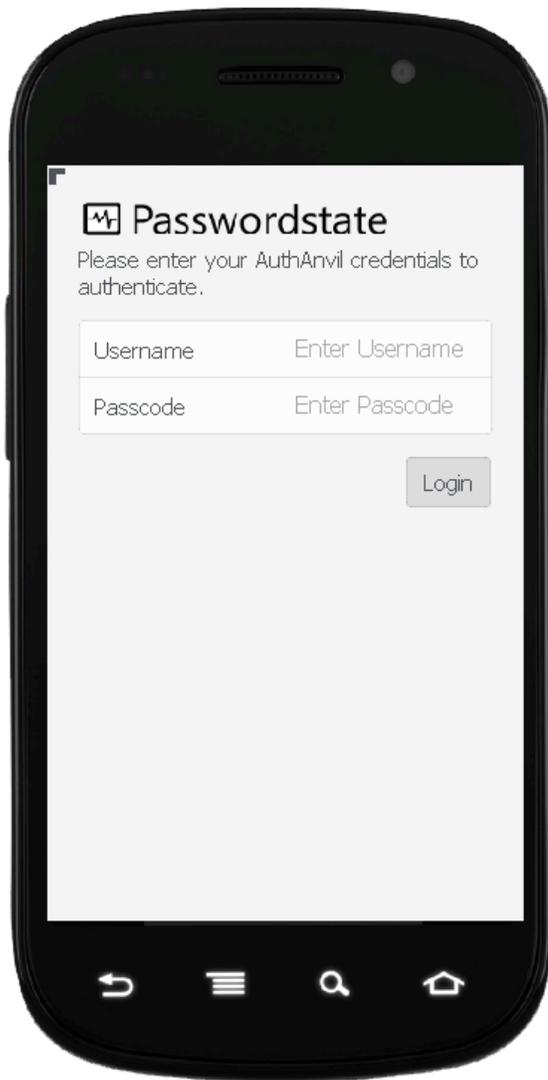
 Your Passwordstate web site must be using a Trusted SSL Certificate in order to use this authentication option



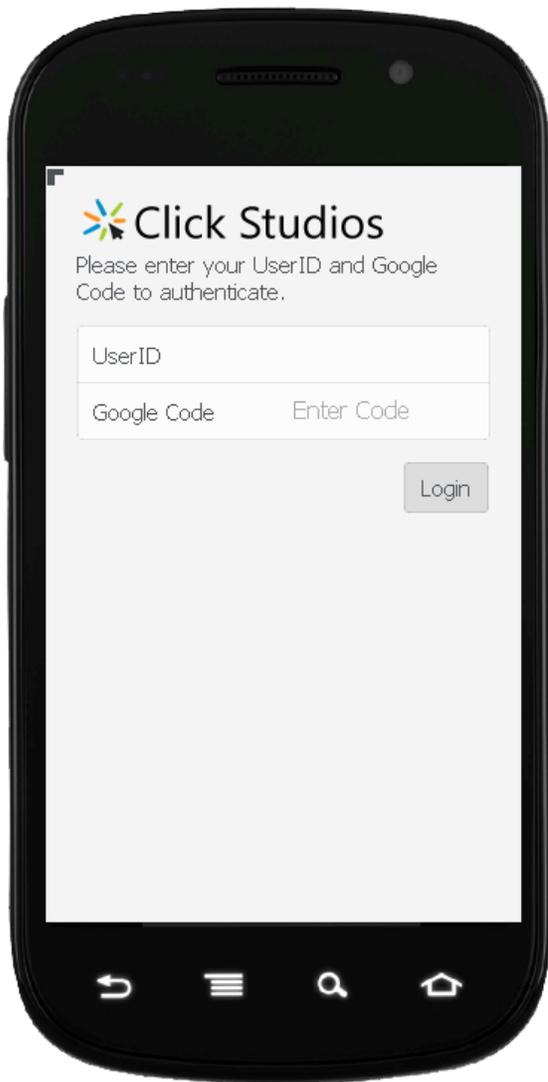
Email Temporary Pin Code Screen



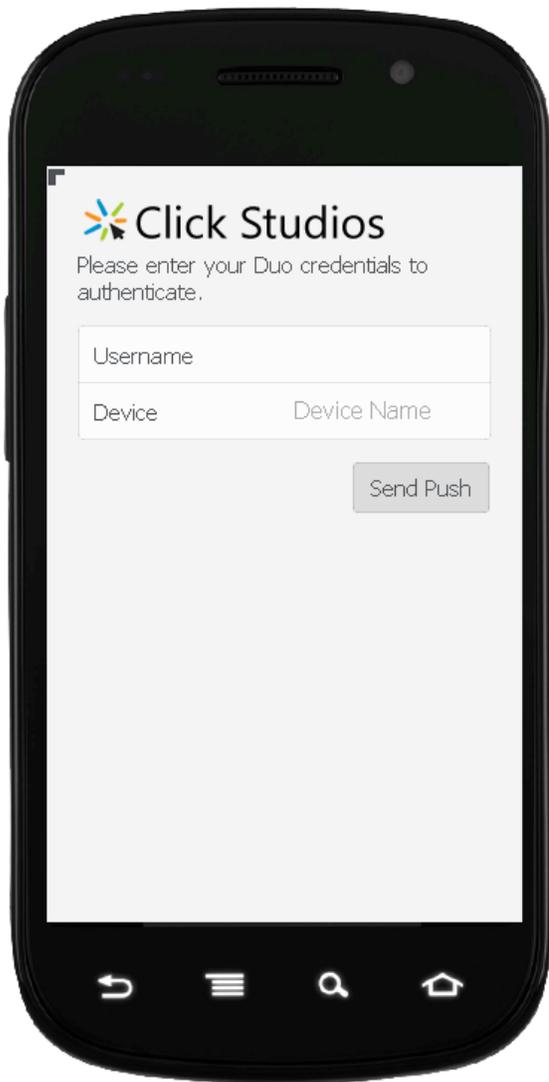
AuthAnvil Two-Factor Authentication Screen



Google Authenticator Screen



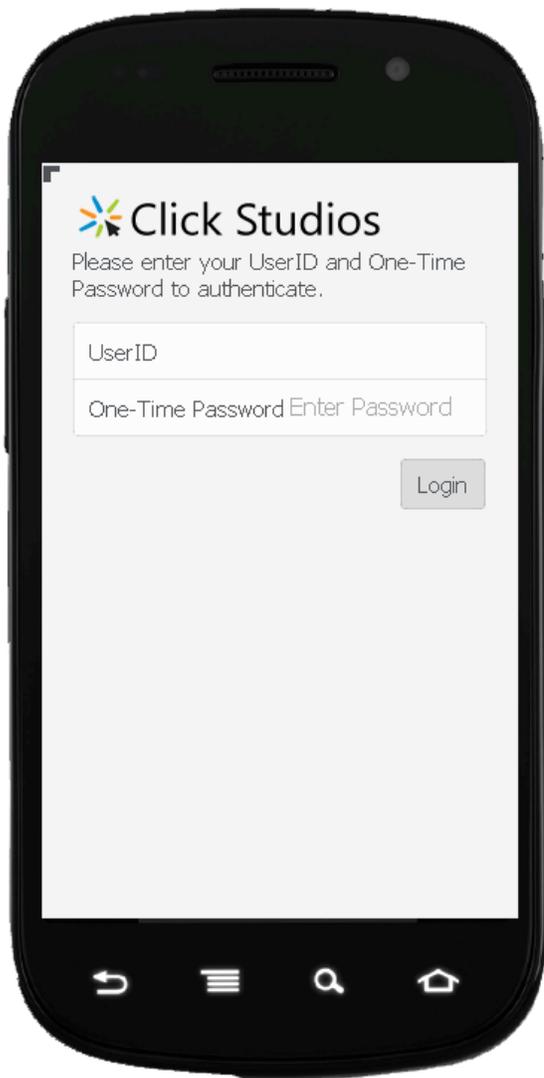
Duo Push Two-Factor Authentication Screen



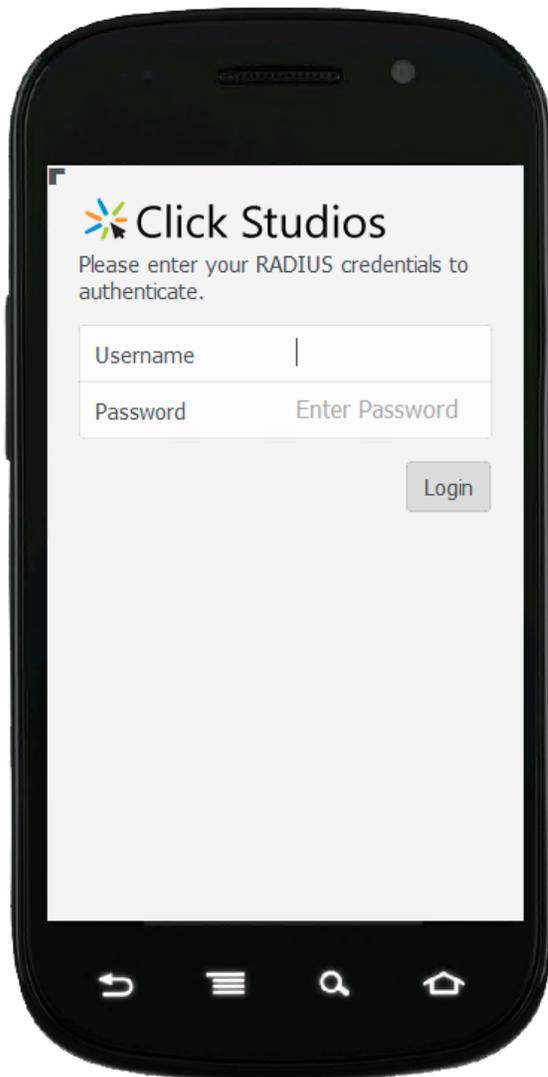
SafeNet Two-Factor Authentication Screen



One-Time Password Authentication Screen



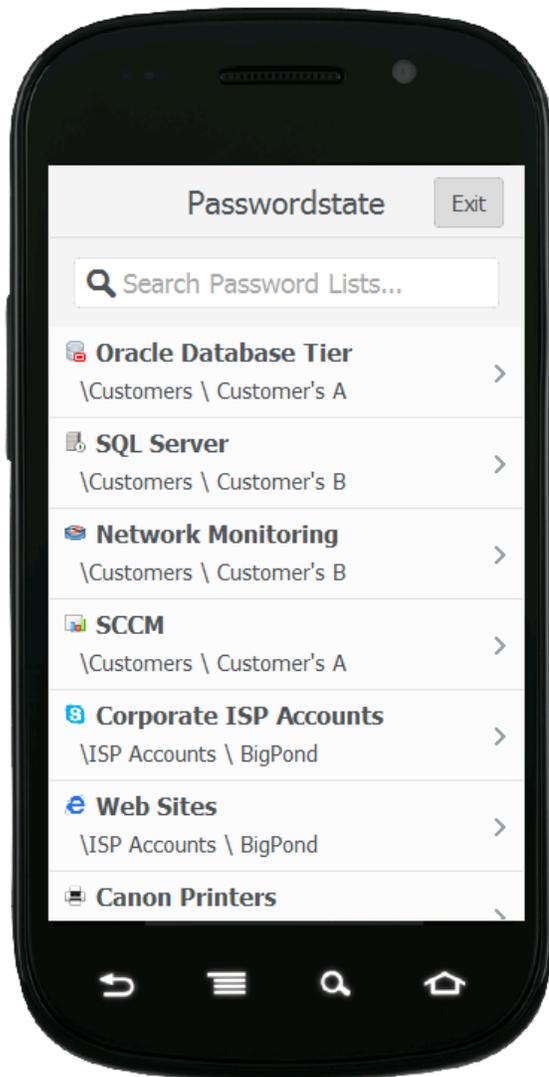
RADIUS Authentication Screen

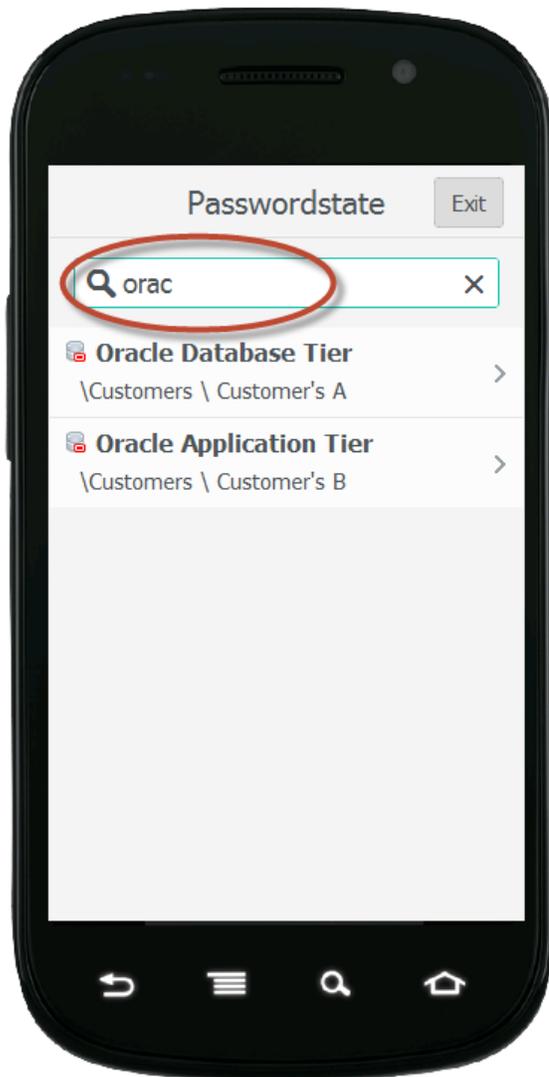


Browsing/Filtering Password Lists

After you have authenticated, the default home screen is the one below which allows you to browse all the Password Lists your account has been given access to. A couple things to note about this screen are:

1. The number of records displayed may be limited by the setting 'Limit the Number of Records to' on your [User Preferences](#) screen
2. When searching/filtering Password Lists, you can search by the Title of the Password List, and also the Tree Path of the Password List in the Navigation Tree (the Tree Path is the logical structure/path of where the Password List is positioned in the Password List Navigation Tree on the main web site)



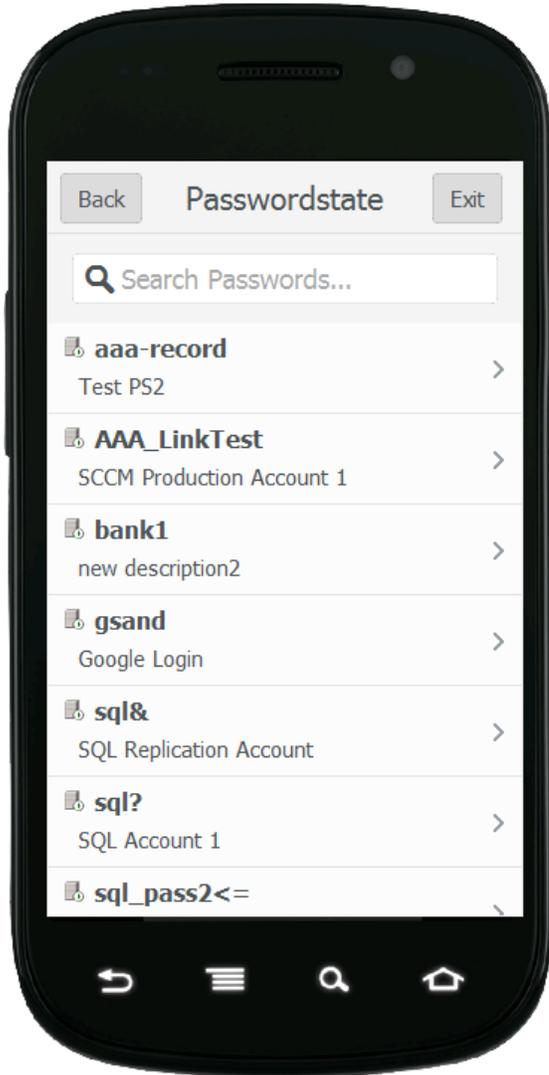


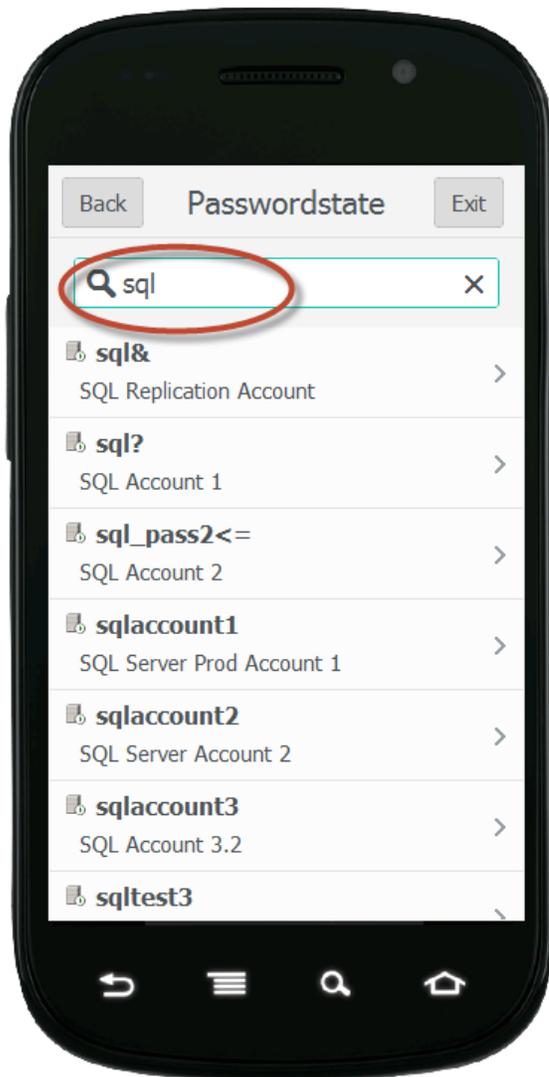
Browsing/Filtering Passwords for the selected Password List

After you have tapped on the appropriate Password List, you will be directed to the screen below which allows you to browse all the passwords in the selected Password List. A couple things to note about this screen are:

1. The number of records displayed may be limited by the setting 'Limit the Number of Records to' on your [User Preferences](#) screen
2. When searching/filtering passwords, you can search across all of the fields which can be configured for a Password record i.e. Title, Description, UserName, URL, Generic Fields, etc. The only fields you can't search are the one's which are encrypted i.e. the Password field, and any Generic Fields set as type 'Password'

 **Note:** When searching for passwords, you can perform an exact match by enclosing your search term in double quotes i.e. "root_admin"

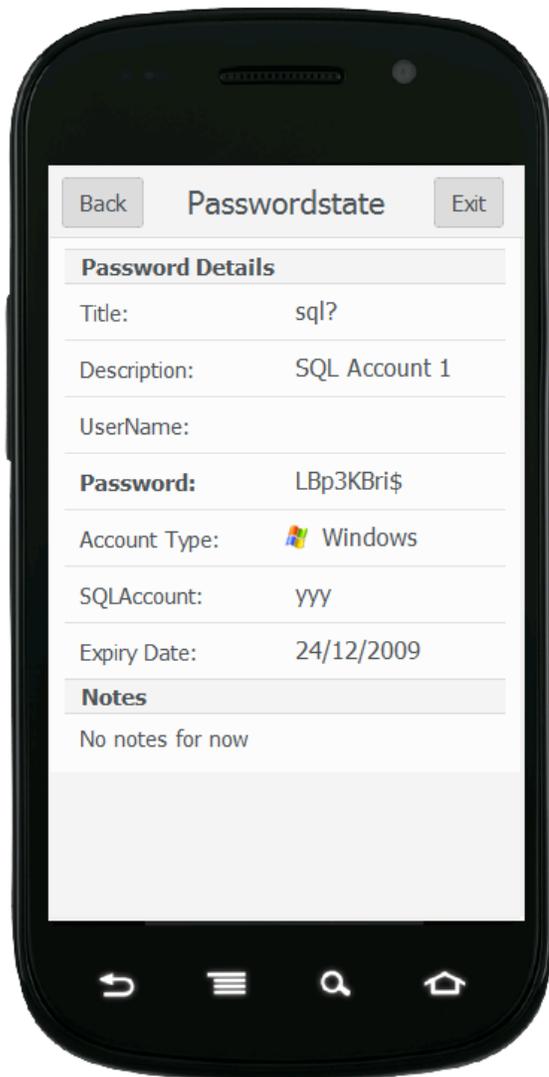




Viewing a Password Record

When you tap on one of the Password records on the screens above, you will be directed to the screen below where you can view the details of the password record. A couple of things to note about this screen are:

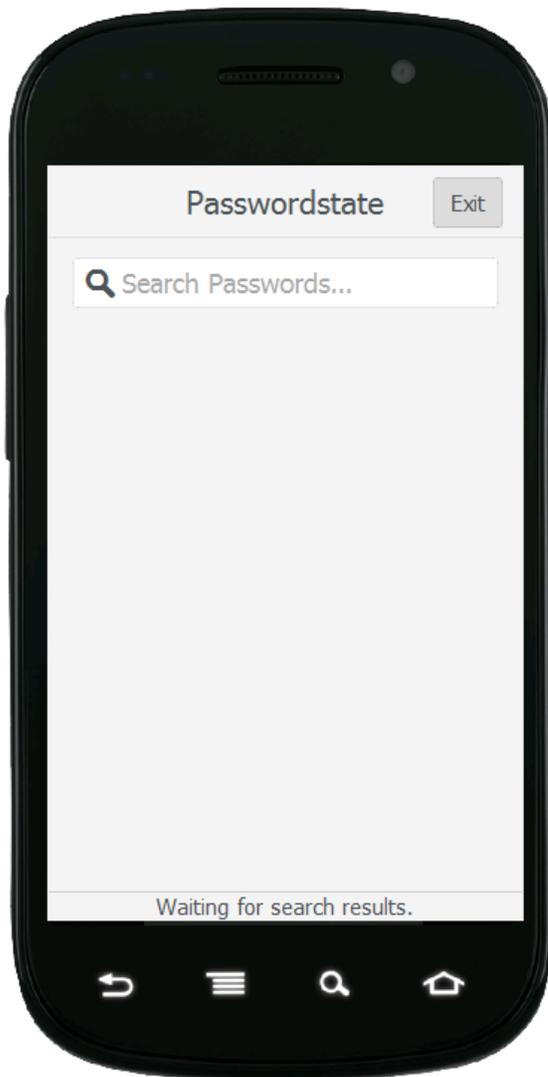
1. An auditing record will be added, as you have viewed the details of this password record. If enabled in the main web site settings, any other users who have access to this password record will receive an email notification informing them you have accessed it
2. Most mobile devices allow you to copy details to the clipboard if required, and majority of fields on this screen will allow you to copy their details
3. If there are any 'One-Time Access' permissions enabled for this password record for your account, your access will automatically be removed after you have viewed the record



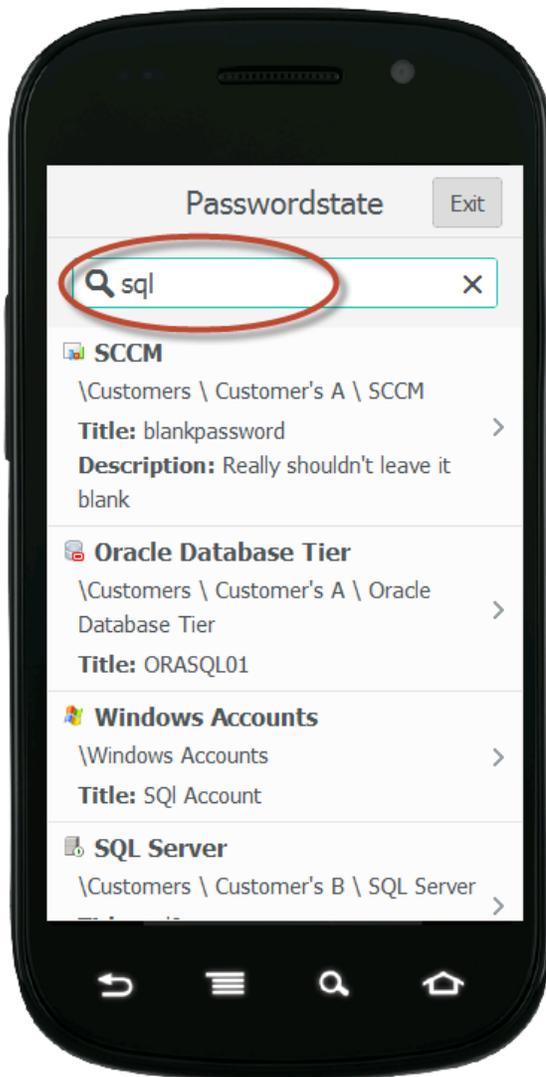
Password Search Home Page

If you have selected 'Passwords Search' as your default home page on the [User Preferences](#) screen, you will be directed to the screen below after you have authenticated. From here you can search for a password record across all of the Password Lists you have been given access to. This is a similar search feature which you will find on the 'Passwords Home' in the main web client.

Note: When searching for passwords, you can perform an exact match by enclosing your search term in double quotes i.e. "root_admin"



When searching for Password records this way, a little more detail is shown on the screen so you know which Password List the password record belongs to.



Logging Out of the Mobile Client

When you tap on the 'Exit' button on the top right-hand side of the screen, you will be directed to the screen below and your Mobile Access session will be ended. If you leave your session inactive longer than the setting specified on the [System Settings](#) page, you will also be automatically logged out and directed to this screen.

