



Click Studios

Passwordstate

Installation Instructions

Table of Contents

1	SYSTEM REQUIREMENTS - GENERAL	3
2	INSTALLING MICROSOFT IIS AND SQL SERVER.....	4
3	INSTALLING PASSWORDSTATE	5
4	SSL CERTIFICATE CONSIDERATIONS.....	8
5	CONFIGURING PASSWORDSTATE FOR FIRST TIME USE.....	10
6	POST INSTALL INSTRUCTIONS.....	17

1 System Requirements - General

Passwordstate has the following system requirements:

Web Server

Your web server which will host the Passwordstate web site can be any of the following Operating System versions:

- Microsoft Windows Server 2008 & IIS 7.0
- Microsoft Windows Server 2008 R2 & IIS 7.5
- Microsoft Windows Server 2012 & IIS 8.0
- Microsoft Windows Server 2012 R2 & IIS 8.5
- Microsoft Windows Server 2016 & IIS 10.0
- Windows 7 & IIS 7.5
- Windows 8 & IIS 8.0
- Windows 10 & IIS 10.0

Note: Microsoft **.Net Framework 4.5**, and **PowerShell 3.0 or above** must also be installed on your web server.

Database Server

You will need to have one of the following supported SQL Server versions installed prior to installing Passwordstate, so Passwordstate can connect to SQL Server and create a database. SQL Server can be installed either on the same web server as Passwordstate, or on any other Windows Server in your environment.

- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 Express
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008 R2 Express
- Microsoft SQL Server 2012
- Microsoft SQL Server 2012 Express
- Microsoft SQL Server 2014
- Microsoft SQL Server 2014 Express
- Microsoft SQL Server 2016
- Microsoft SQL Server 2016 Express

Important: SQL Server must be configured for mixed-mode authentication, so the Passwordstate web site can connect to SQL Server using an SQL Account. **Active Directory Accounts cannot be used to authenticate against the database.**

2 Installing Microsoft IIS and SQL Server

Before you install Passwordstate, you are required to already have Internet Information Servers (IIS) and SQL Server Express or above installed. Below are a couple of links to show how to install these if you require any help

- Install IIS (Web Server) - <https://www.clickstudios.com.au/community/index.php?/topic/1786-how-to-install-internet-information-services-iis/>
- Install SQL Server (Database Server) - https://www.clickstudios.com.au/downloads/Installing_SQLServerExpress_2016.pdf

3 Installing Passwordstate

To install Passwordstate, run 'Passwordstate.exe' and follow these instructions:

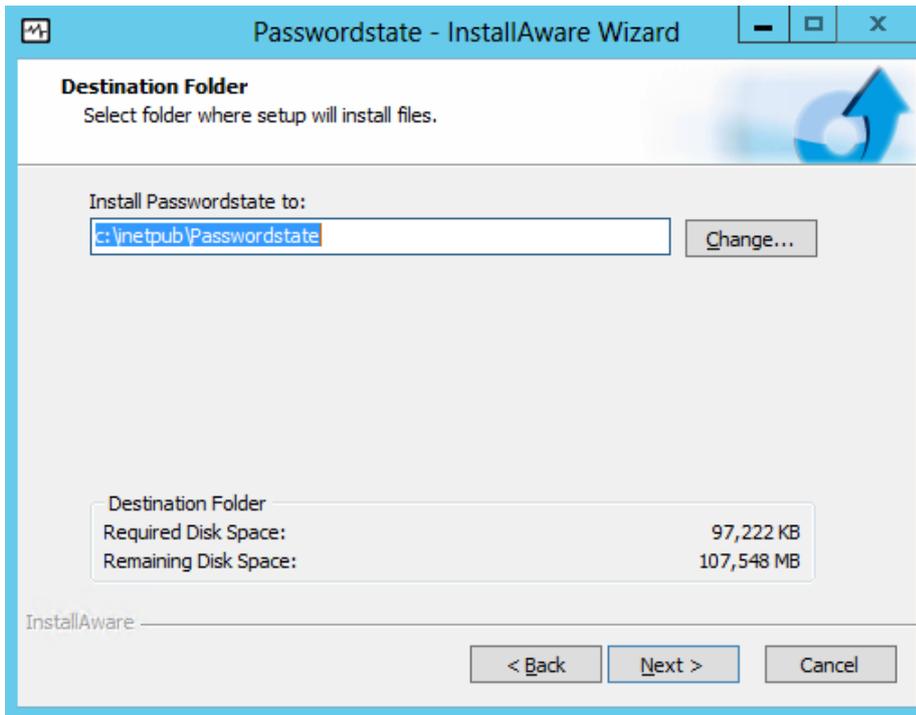
1. At the 'Passwordstate Installation Wizard' screen, click on the 'Next' button



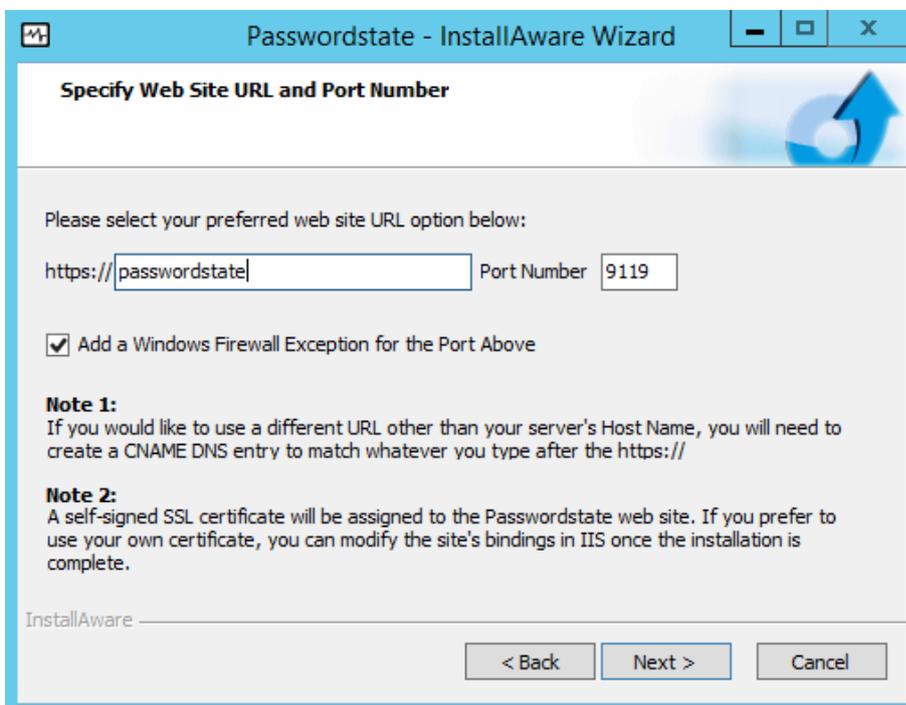
2. At the 'License Agreement' screen, tick the option 'I accept the terms in the License Agreement', then click on the 'Next' button



3. At the 'Destination Folder' screen, you can either accept the default path or change to a different location, then click on the 'Next' button



4. At the 'Specify Web Site URL and Port Number' screen, specify the URL you would like to use, then click on the 'Next' button



5. At the 'Completing the InstallAware Wizard for Passwordstate' screen, click on the 'Next' button



6. Once installed, click on the 'Finish' button
7. If you have a Firewall enabled on your web server, you may need to open up the port number you specified during the install (default is 9119), so that users are able to access the web site

4 SSL Certificate Considerations

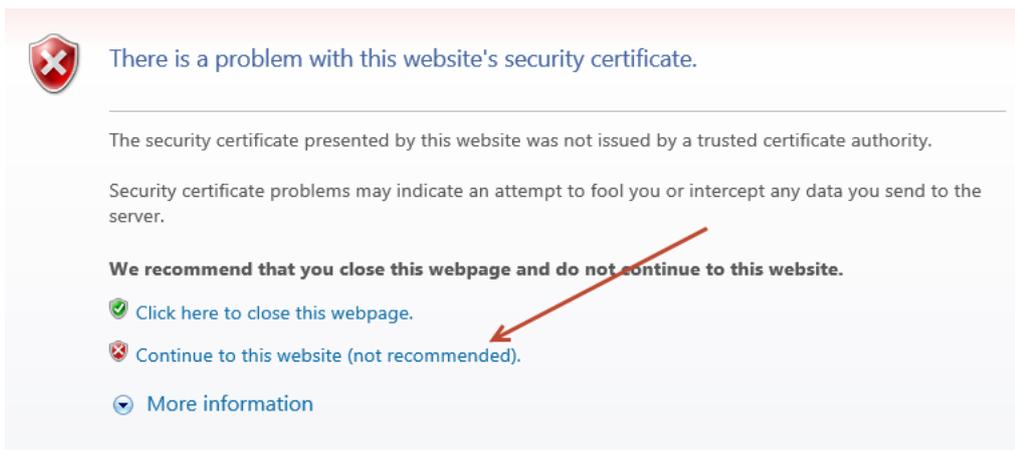
The installer for Passwordstate installs a self-signed SSL certificate on your web server, and binds it to the Passwordstate web site.

If you have your own SSL certificate installed on the web server you'd prefer to use, you can modify the bindings for the site in IIS, and select the appropriate certificate.

If you wish to continue using the self-signed SSL certificate, then you may want to instruct your users to "Install" the certificate on their computer, so the various Internet browsers don't complain about the certificate not being issued by a trusted authority.

To install the certificate, you can follow these steps:

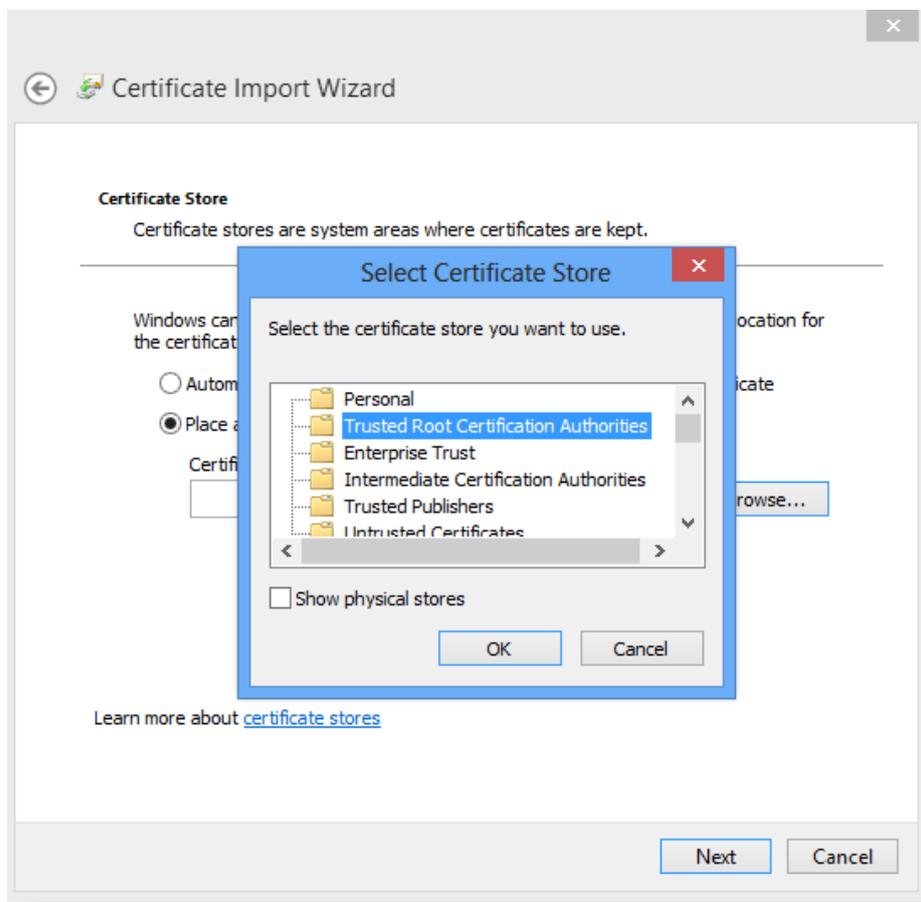
1. Using Internet Explorer, browser to the Passwordstate web site
2. When you see the following screen, click on the 'Continue to this website' link



3. Now click on the 'Certificate error' link at the top of your screen



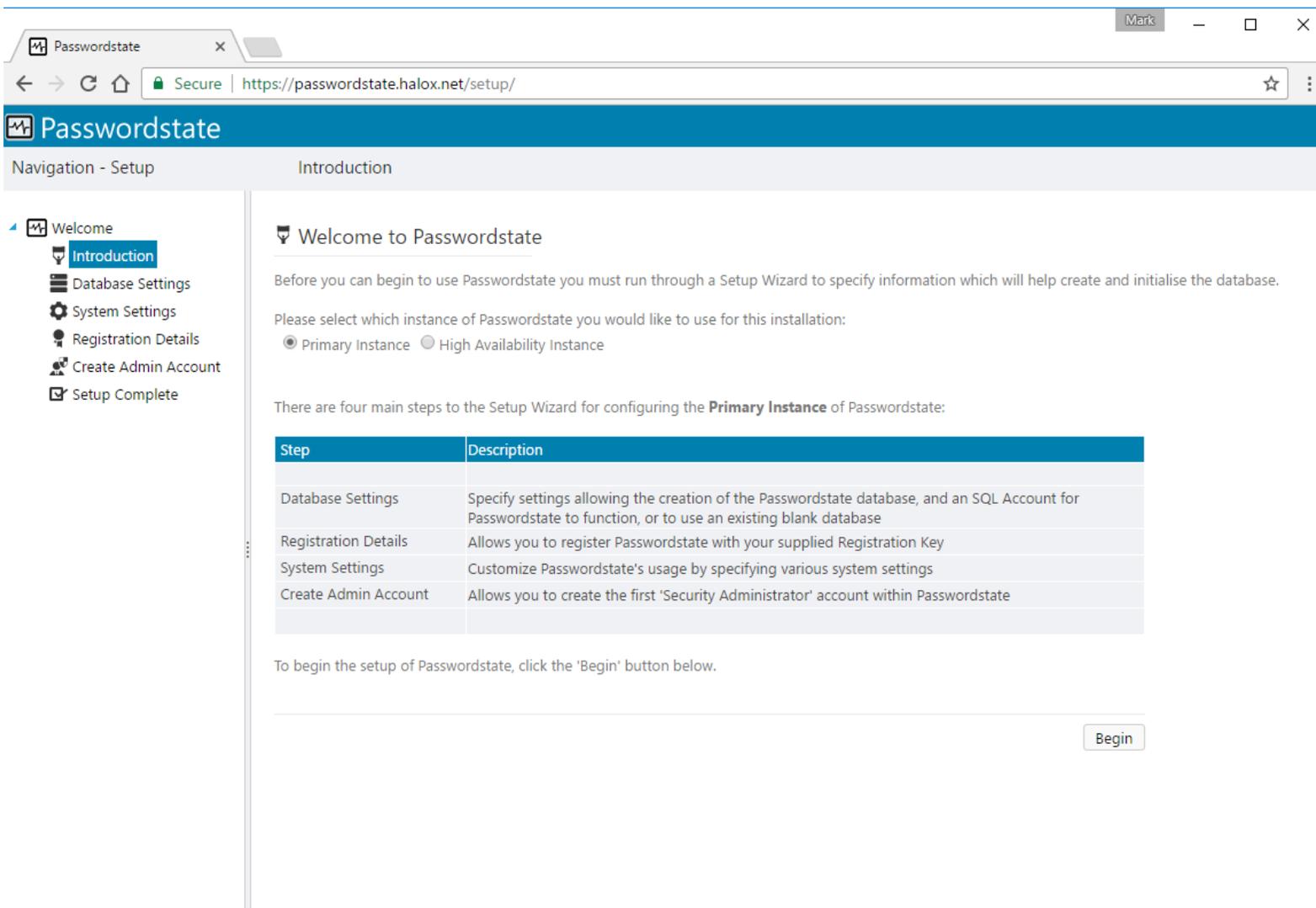
4. The click on 'View Certificates', then on the 'Install Certificate...' button
5. Select the 'Local Machine' Store Location, then click on the 'Next' button
6. Select 'Place all certificates in the following store' option, click on the 'Browse' button, and select 'Trusted Root Certification Authorities' as per the next screenshot



7. Now click on the 'OK' button, then the 'Next' and 'Finish' buttons
8. After the certificate is installed, you can close and re-open your browser to the Passwordstate web site, and it should no longer complain about an untrusted certificate

5 Configuring Passwordstate for First Time Use

Introduction - Now that Passwordstate is installed, you can direct your browser to the URL you specified during the initial install, and follow the initial Setup Wizard – this wizard will guide you through a series of questions for configuring Passwordstate for use.



The screenshot shows a web browser window with the URL `https://passwordstate.halox.net/setup/`. The page title is "Passwordstate" and the navigation menu includes "Welcome", "Introduction", "Database Settings", "System Settings", "Registration Details", "Create Admin Account", and "Setup Complete". The "Introduction" page contains the following text:

Welcome to Passwordstate

Before you can begin to use Passwordstate you must run through a Setup Wizard to specify information which will help create and initialise the database.

Please select which instance of Passwordstate you would like to use for this installation:

Primary Instance High Availability Instance

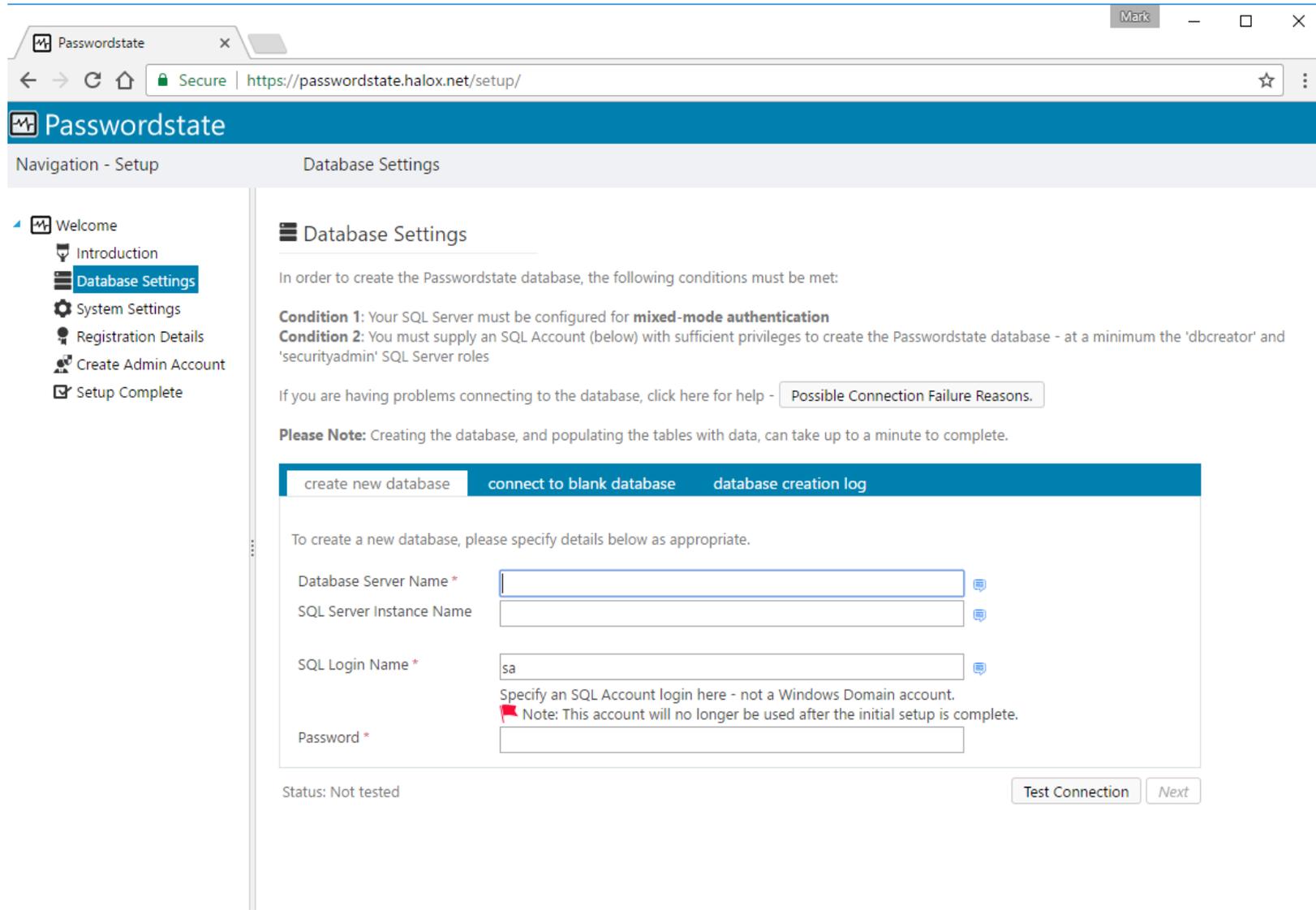
There are four main steps to the Setup Wizard for configuring the **Primary Instance** of Passwordstate:

Step	Description
Database Settings	Specify settings allowing the creation of the Passwordstate database, and an SQL Account for Passwordstate to function, or to use an existing blank database
Registration Details	Allows you to register Passwordstate with your supplied Registration Key
System Settings	Customize Passwordstate's usage by specifying various system settings
Create Admin Account	Allows you to create the first 'Security Administrator' account within Passwordstate

To begin the setup of Passwordstate, click the 'Begin' button below.

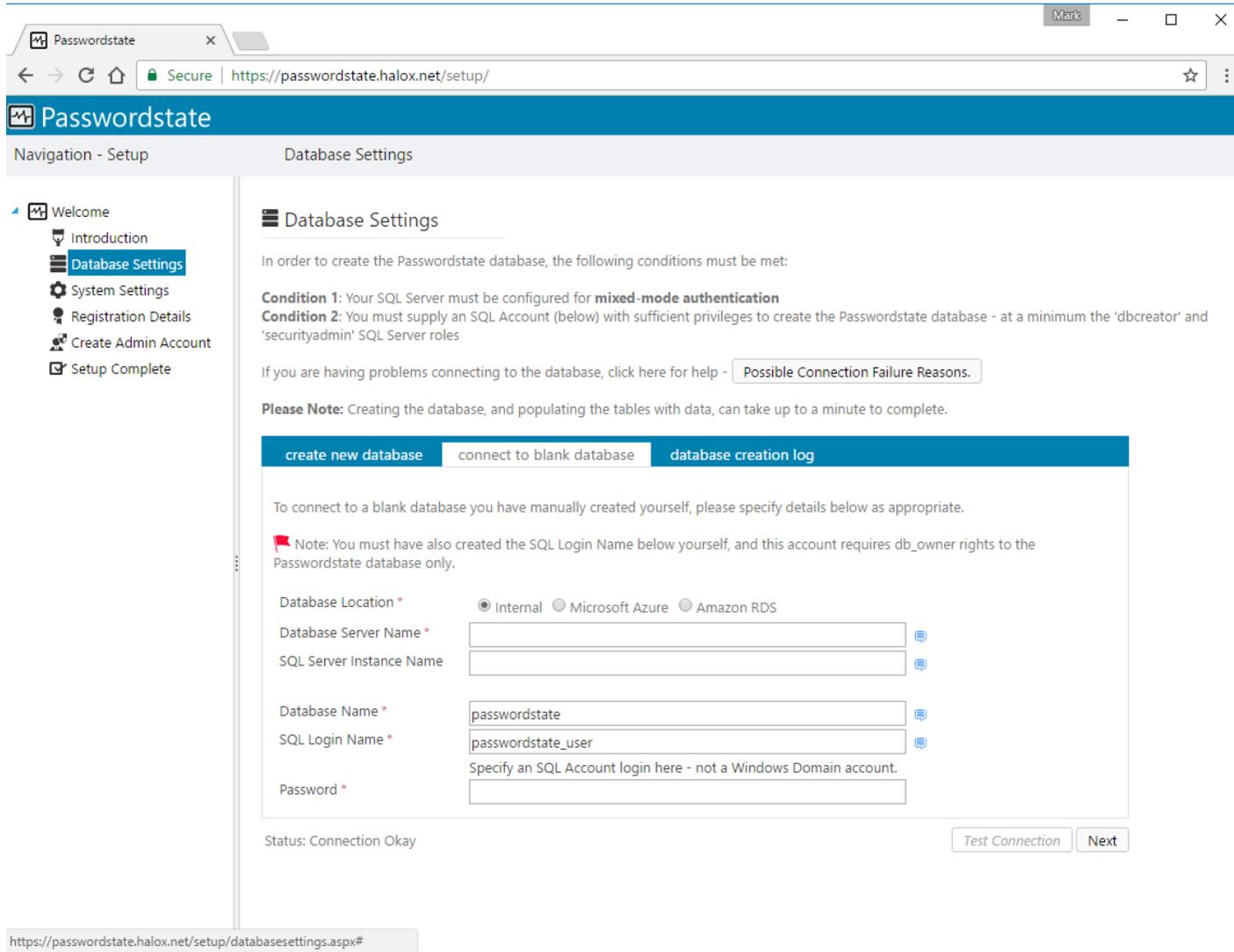
Database Settings – Create New Database - On this screen you will need to specify database settings for creating the Passwordstate database. Please use the onscreen instructions if you have any issues connecting to the database.

Please Note: Creating the database, and populating the tables with data, could take up to a minute to complete.



Database Settings – Connect to Blank Database – If you prefer to create the blank Passwordstate database yourself prior to tables being created and populated with data, you can do so by clicking on the ‘Connect to Blank Database’ tab first.

Please Note: You must first create a blank database to connect to, and an appropriate SQL Account which has db_owner rights to this database. If connecting to a Microsoft Azure or Amazon AWS database, please refer to their documentation for how to create the database and SQL Account.



The screenshot shows the Passwordstate web application interface. The browser address bar displays <https://passwordstate.halox.net/setup/>. The page title is "Passwordstate" and the navigation menu includes "Welcome", "Introduction", "Database Settings" (highlighted), "System Settings", "Registration Details", "Create Admin Account", and "Setup Complete".

The main content area is titled "Database Settings" and contains the following text:

In order to create the Passwordstate database, the following conditions must be met:

- Condition 1:** Your SQL Server must be configured for **mixed-mode authentication**
- Condition 2:** You must supply an SQL Account (below) with sufficient privileges to create the Passwordstate database - at a minimum the 'dbcreator' and 'securityadmin' SQL Server roles

If you are having problems connecting to the database, click here for help - [Possible Connection Failure Reasons.](#)

Please Note: Creating the database, and populating the tables with data, can take up to a minute to complete.

Below this text are three tabs: "create new database", "connect to blank database" (selected), and "database creation log".

The "connect to blank database" tab contains the following instructions and form:

To connect to a blank database you have manually created yourself, please specify details below as appropriate.

Note: You must have also created the SQL Login Name below yourself, and this account requires db_owner rights to the Passwordstate database only.

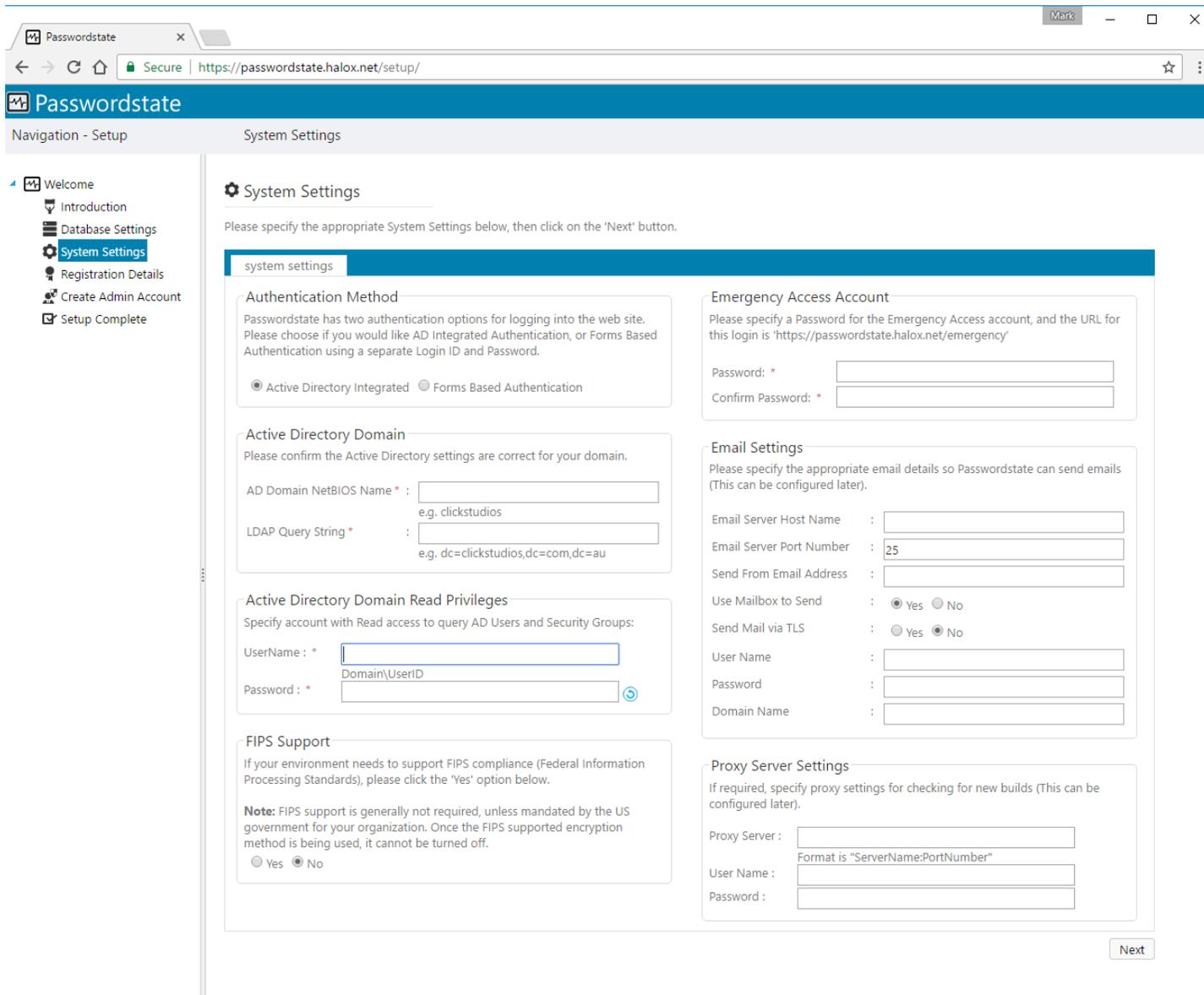
The form includes the following fields:

- Database Location * (radio buttons for Internal, Microsoft Azure, Amazon RDS)
- Database Server Name * (text input)
- SQL Server Instance Name (text input)
- Database Name * (text input, value: passwordstate)
- SQL Login Name * (text input, value: passwordstate_user)
- Password * (text input)

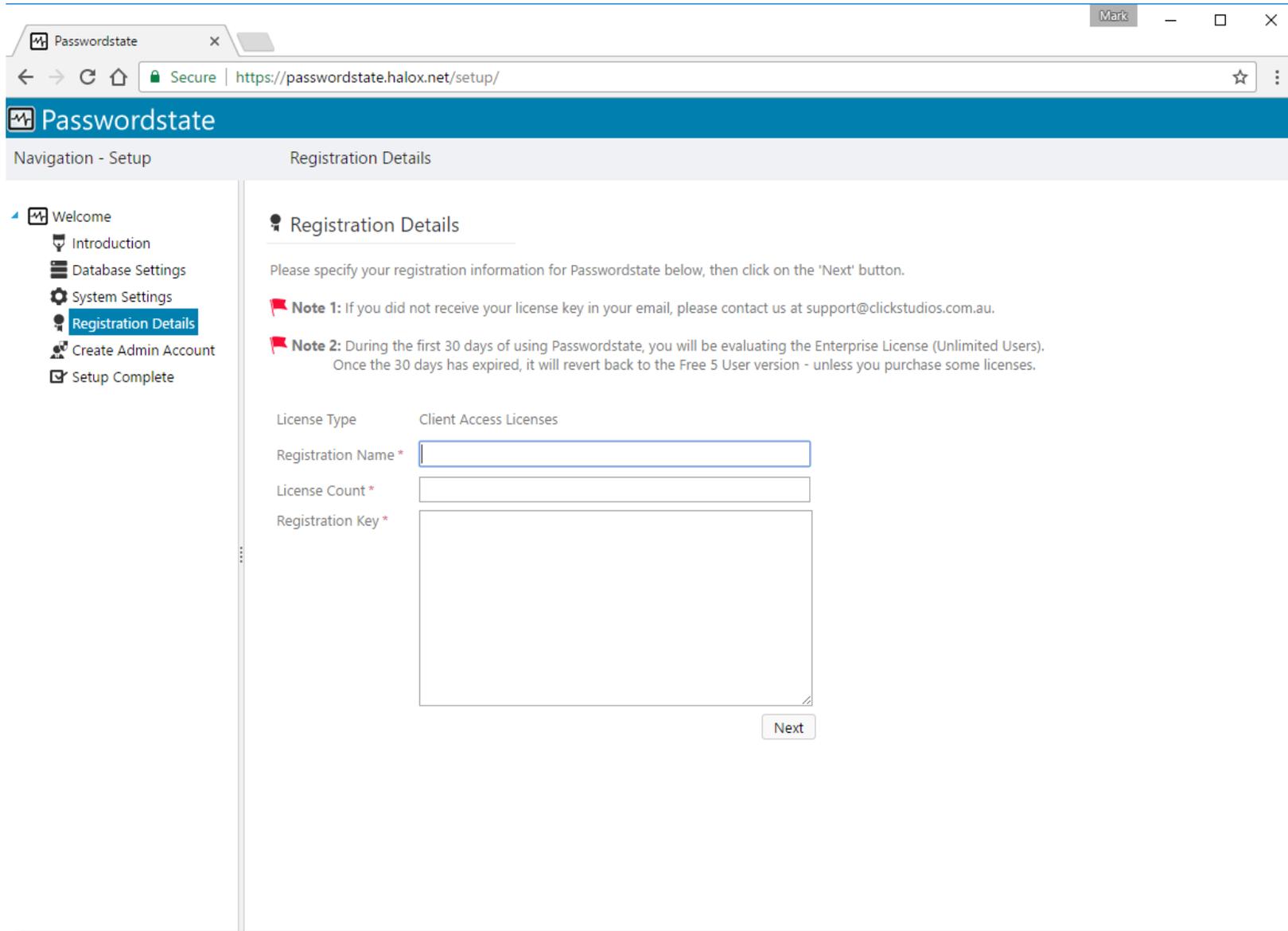
Below the form, it says "Status: Connection Okay" and has "Test Connection" and "Next" buttons.

The browser address bar at the bottom shows <https://passwordstate.halox.net/setup/databasesettings.aspx#>.

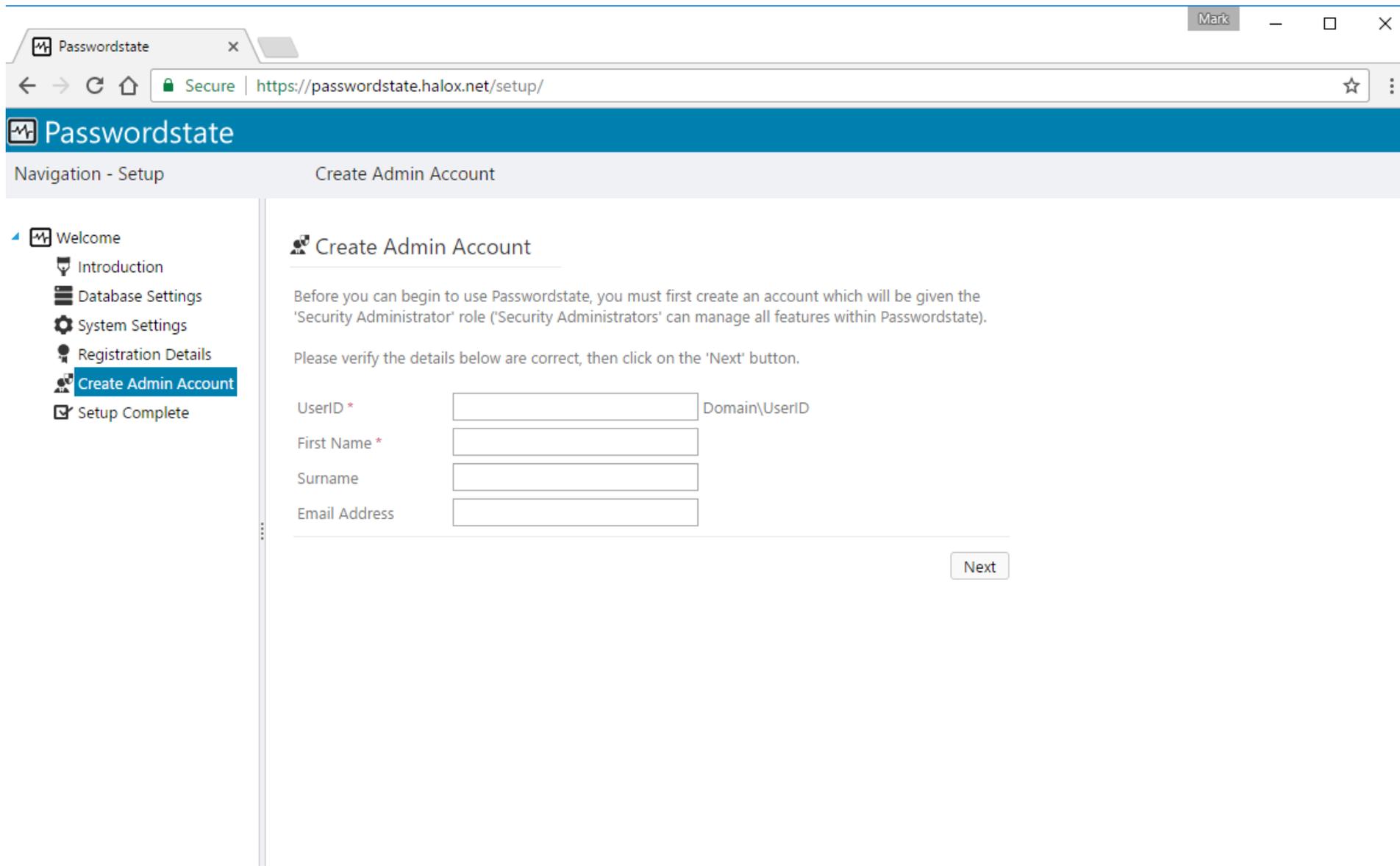
System Settings – On this screen you specify various system wide settings for Passwordstate usage. Explanation for each of these settings is detailed after this screenshot.



Registration Details – On this screen you need to specify your Registration details for Passwordstate. If you have not received your registration details, please visit www.clickstudios.com.au.

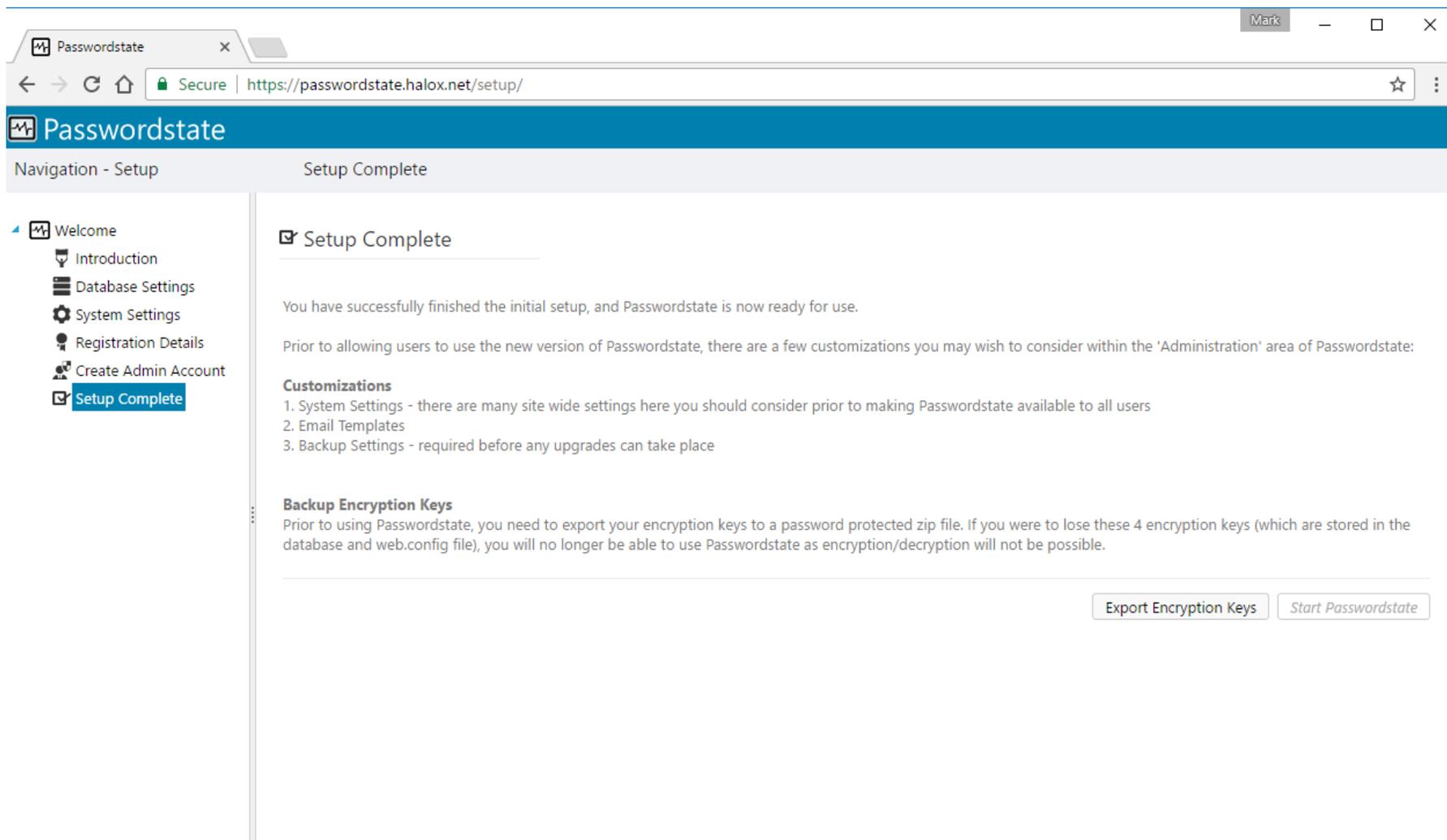


Create Admin Account – On this screen you specify details for the first user account to be created in Passwordstate. This account will be granted Security Administrator privileges, and assign all Security Administrator roles.



Setup Complete – The installation is now complete and you can begin using Passwordstate. Prior to granting access, or informing users of the new version, you may wish to review some of the system wide settings found under the 'Administration' area of Passwordstate.

Export Encryption Keys – It is very important you export your encryption keys for safe storage outside of Passwordstate. If you were to lose your web.config file in a disaster, Click Studios would not be able to help you rebuild your Passwordstate environment. The split encryptions keys are stored in the web.config file, and within the database.



6 Post Install Instructions

We also have additional information in our General Installation Guide, which answers many post install questions we have received from customers. Some of these questions include:

- Using a different URL for the site
- Encrypting settings in the web.config file
- Anti-Virus Considerations

Below is a link for our General Installation Guide if needed -

https://www.clickstudios.com.au/downloads/version7/Installation_Instructions.pdf