Passwordstate

Enterprise Password Management

High Availability Installation Instructions

Table of Contents

1 Overview

The purpose of the High Availability module is to allow you to have a second install of Passwordstate for Disaster Recovery purposes – without purchasing this license, the End User License Agreement (EULA) only allows you to have one production install.

There are two architectural designs to consider in the section 'Architectural Overview', and there are multiple methods which can be used to move data between database servers i.e. Log Shipping, Transactional Replication, SQL High Availability Groups or scheduled backup/restores.

In the event your primary Passwordstate web server or database server were unavailable, you can still access your passwords via the High Availability instance.

2 Prerequisites

The High Availability module of Passwordstate has the following prerequisites:

Note: When installing the High Availability Module, you must be installing the same build as your primary production site. If you have not kept the installer for this specific build, then you must upgrade your primary site first to the latest release. You can download the latest installer from here - https://www.clickstudios.com.au/passwordstate-checksums.aspx - Please ensure you validate the published Checksum.

To upgrade your primary site, you can use any of the recommended methods in the following document - https://www.clickstudios.com.au/downloads/version9/Upgrade_Instructions.pdf

Web Server Prerequisites

- The HA Web server has the same web server system requirements as the primary install. Please refer to the document https://www.clickstudios.com.au/downloads/version9/Installation_Instructions.pdf for details
- Prior to establishing SQL Server data replication, there are two things which need to be done:
    - On your Primary Instance of Passwordstate, go to the screen Administration -> License Information, and add your High Availability License key here
    - On your Primary Instance of Passwordstate, go to the screen Administration -> Authorized Web Servers, and also register the host name of your High Availability web server – this is the NetBIOS name of your web server

Database Server Prerequisites

Below is some information regarding the various replication and SQL Server versions:

- Always On Availability Groups requires both servers to be SQL Server Enterprise
- Basic Availability Groups requires both servers to be SQL Server Standard or above
- Transactional replication requires the primary server (Publisher) to be at least SQL Server Standard, and the subscribing server can be SQL Server Express

Note 1: You must be using the same versions of SQL Server i.e. both must be Server 2016, or 2019, etc. And generally, the same Service Pack level is required.

Note 2: If using Transactional Replication, only an Active/Passive configuration is possible.

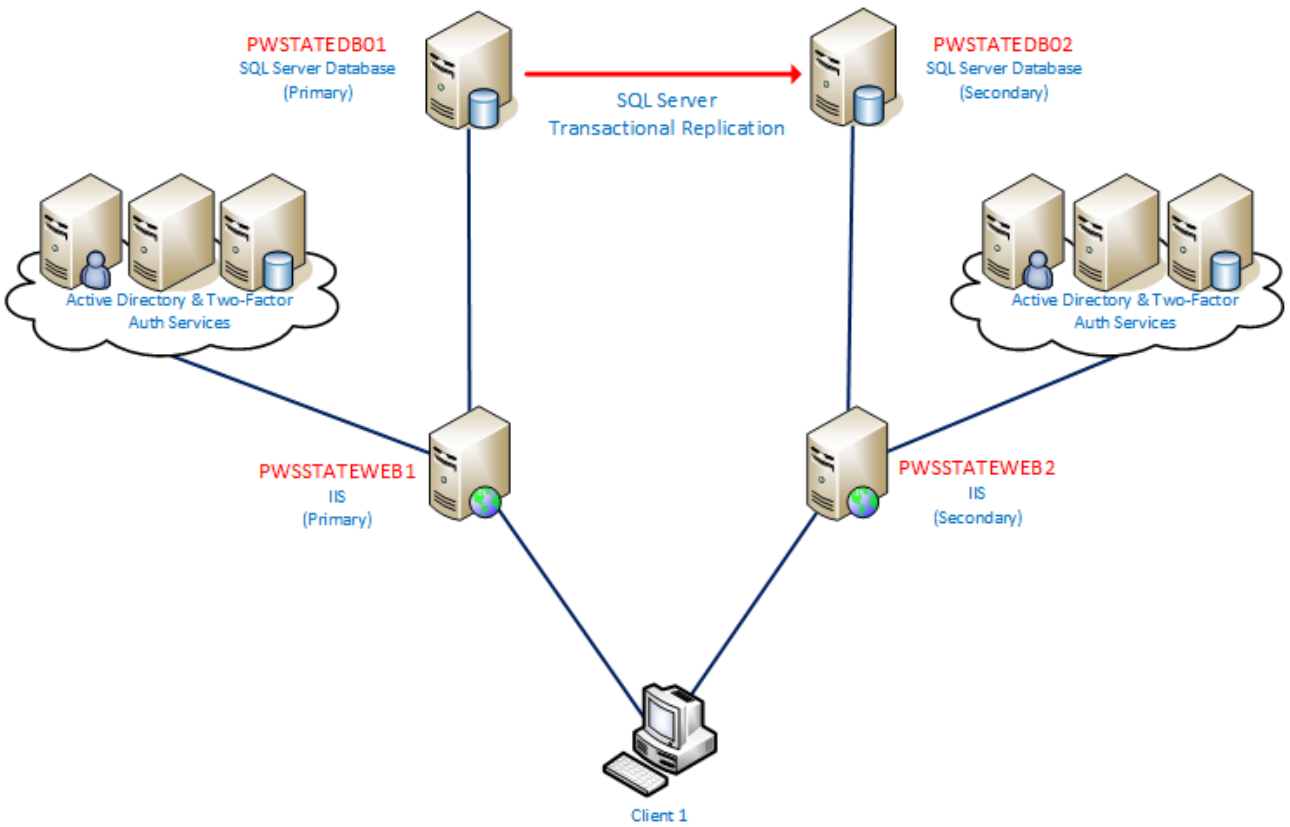
Note 3: Merge replication is not supported, due to the limitation of how many fields in a single table it can replicate

3 Architectural Overview

The following detail describes both an Active/Passive, and Active/Active architectural design for the High Availability module, where two separate web and database servers are used, and also two different URLs to access both the Primary and High Availability sites.

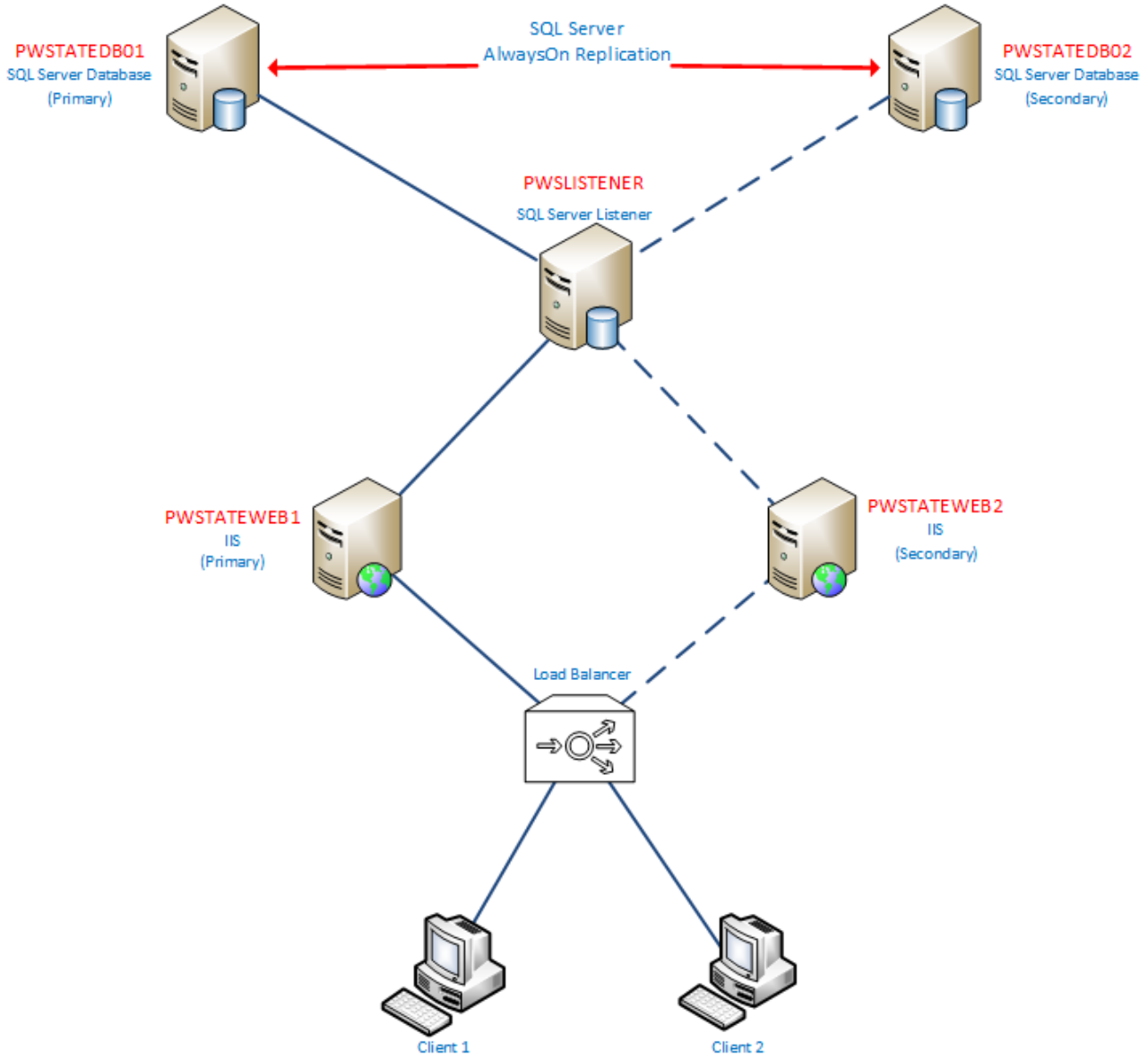
A summary of the Active/Passive design is:

- Requires two web servers, and two database servers
- Data is replicated in real-time, using SQL Server Transactional Replication
- The publisher of the replication needs to be SQL Server Standard or above
- The subscriber of the replication needs to be SQL Server Express or above
- Generally, you only ever access the primary web server, unless there is an extended outage, in which case you would need to point your browser to the URL of the HA server
- HA Server is read-only by default, but there are instructions provided to promote it to be the primary server if required
- There is no automatic failover between the two web servers, as this requires a hardware appliance-based load balancing solution to sit in front of the two web servers
- Below is an architectural diagram describing how the HA module works



A summary of the Active/Active design is:

- As per the diagram below, this shows the use of a Load Balancer for web traffic
- The Load Balancer monitors the availability of the Passwordstate web servers, and automatically fails over if one cannot be communicated with
- SQL Server Basic Availability, and Always On High Availability Groups, are used to monitor availability of both SQL Servers, and perform automatic failover in the event where one server becomes unavailable



4 Active/Passive Considerations

With High Availability, it can be configured either in an Active/Active, or Active/Passive configuration.

With an Active/Passive configuration, the passive (read-only) instance of Passwordstate is designed only to be used in a Disaster Event, where the primary instance of your Passwordstate installation is not available. It is designed to allow you access to your passwords, whilst you recover systems.

With an Active/Passive configuration, certain functionality is also not available, specifically:

- Privileged Account Management
- Remote Session Management
- Browser Extensions
- Remote Site Locations Agents
- Password Reset Portal module
- And any services provided by the Passwordstate Windows Service i.e. sending emails, syslog integration, scheduled reports, etc.

5 SQL Server Considerations

Prior to installing the High Availability instance of Passwordstate, you must have a working replicated copy of your database.

If required, below are some instructions for installing and configuring either of the three SQL High Availability methods mentioned in '2. System Requirements – General'. These documents are included in your original download of Passwordstate, or you can download them again from our documentation page here - https://www.clickstudios.com.au/documentation/default.aspx

- SQL Server Always On Availability Groups (SQL_Server_AlwaysOn_Availability_Groups.pdf)
- SQL Server Basic Availability Groups (SQL_Server_Basic_Availability_Groups.pdf)
- SQL Server Transactional Replication (SQL_Server_Transactional_Replication.pdf)

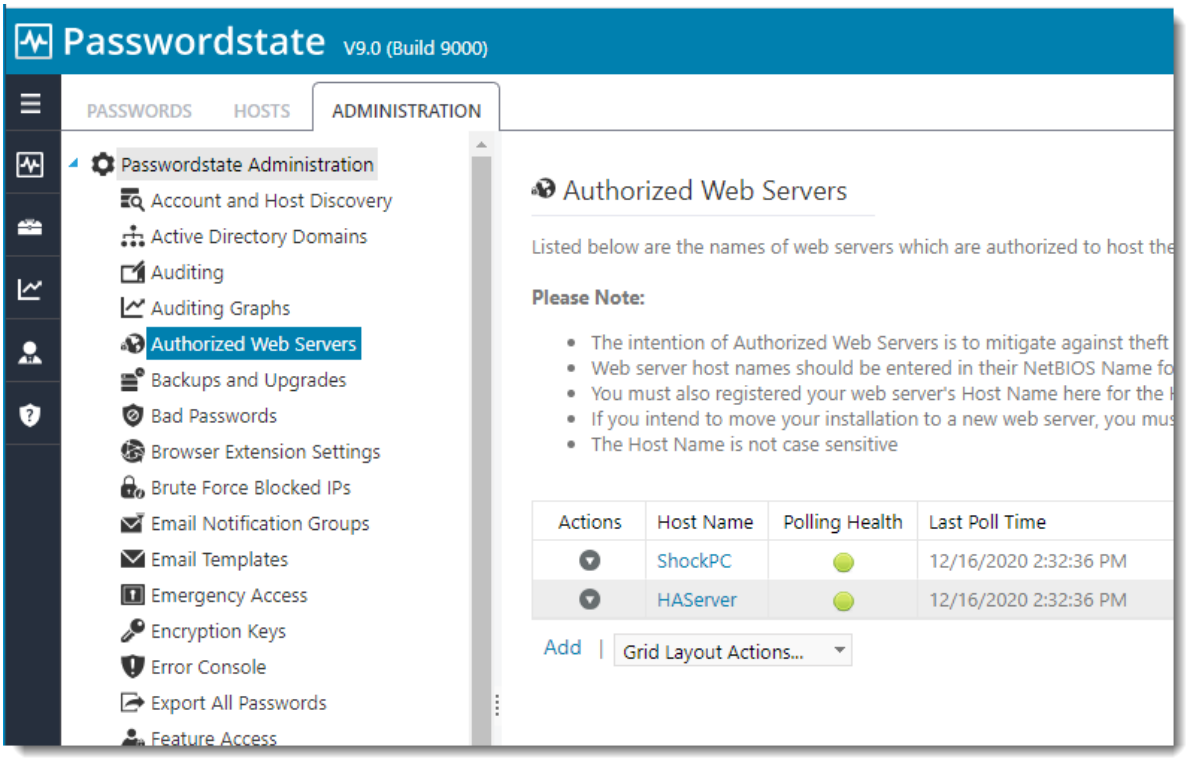

Note: The SQL installation instructions are only a guide, and if you experience any issues configuring or using SQL HA, please contact Microsoft for support.

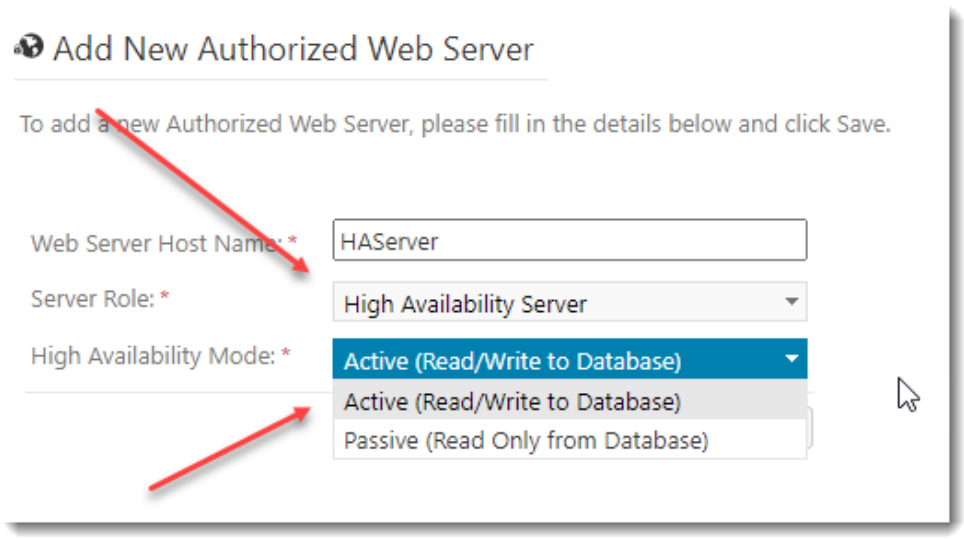
6 Authorized Web Server Considerations

Before installing the High Availability instance of Passwordstate, you first need to register your HA Server's Host name as an Authorized Web Server on your primary instance. To do this, please navigate to the screen Administration -> Authorized Web Servers, and add your server here.

Passive Node is used when using the older SQL Server Transactional Replication, and Active/Active is used for Basic or Always On replication.

Note: Do not modify the 'Primary Server' role here. You must always have one Primary Server for Passwordstate to function correctly.





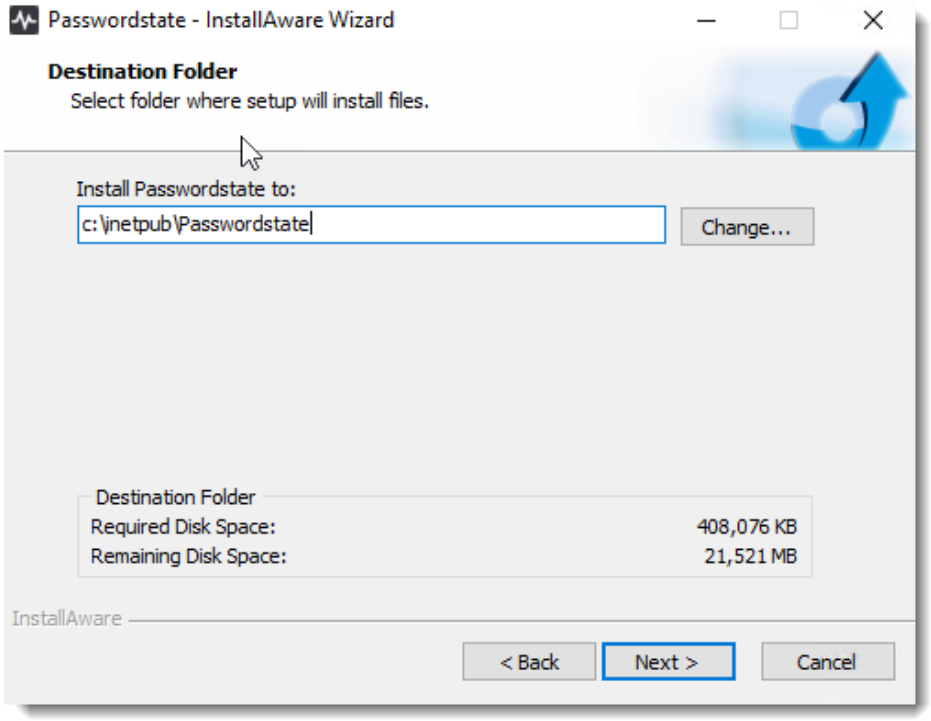
7 Installing Passwordstate

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

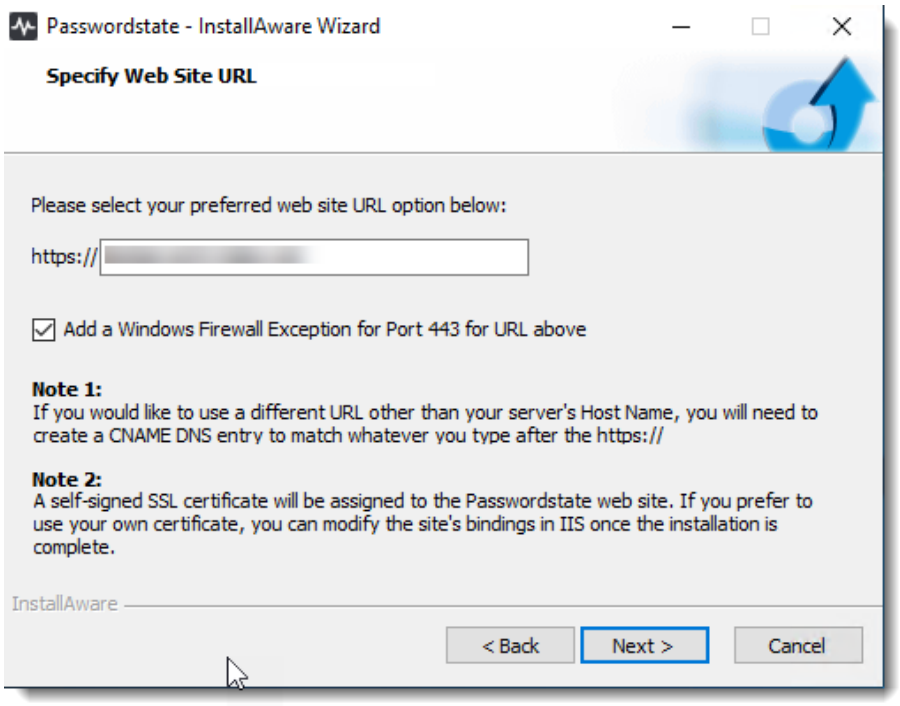
1. At the 'Passwordstate Installation Wizard' screen, click on the 'Next' button

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' screen, specify the URL you would like to use, then click on the 'Next' button (You must have a functioning DNS entry to point to this URL)



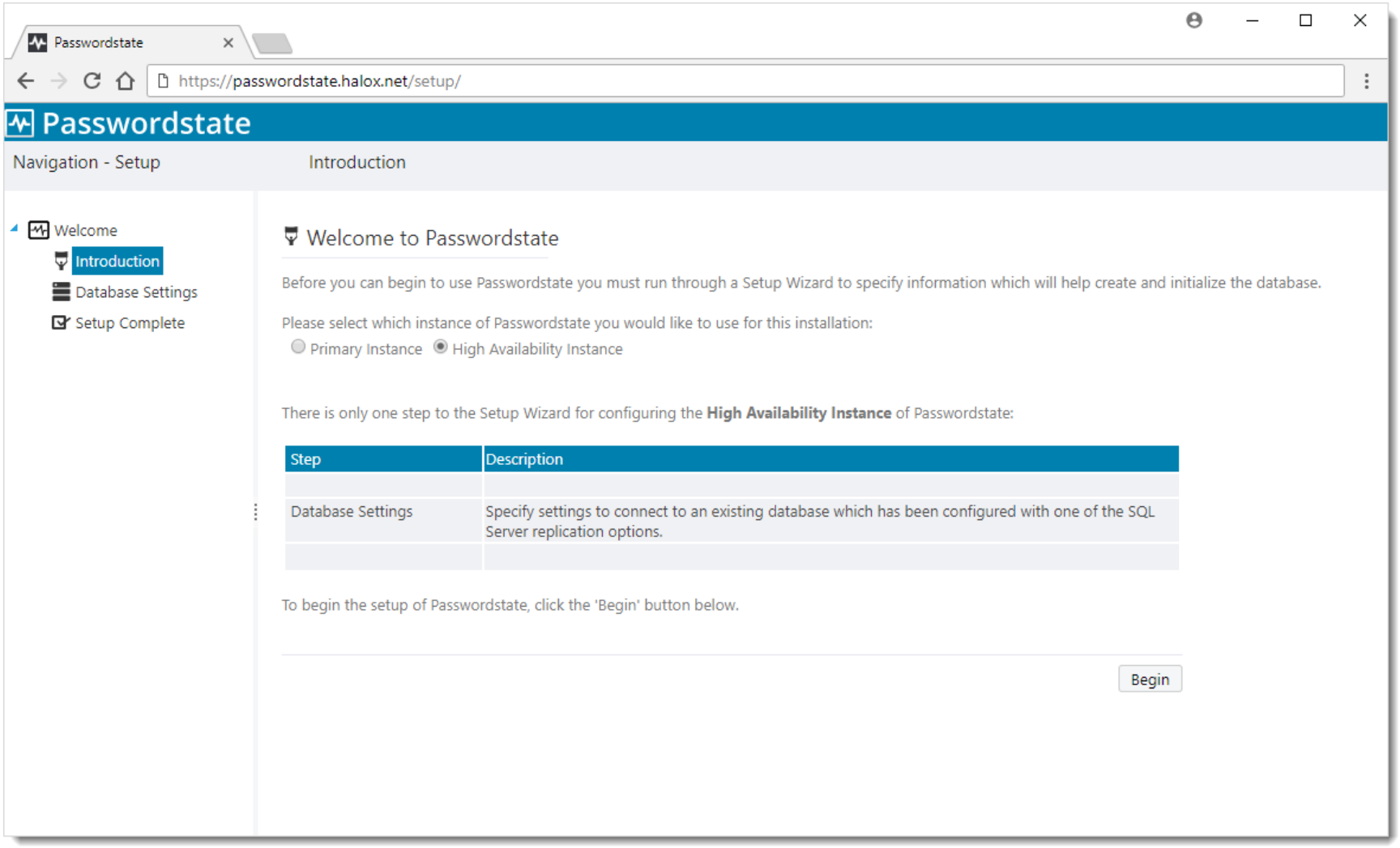
5. At the 'Completing the InstallAware Wizard for Passwordstate' screen, click on the 'Next' button

6. Once installed, click on the 'Finish' button

8 Configuring Passwordstate for First Time Use

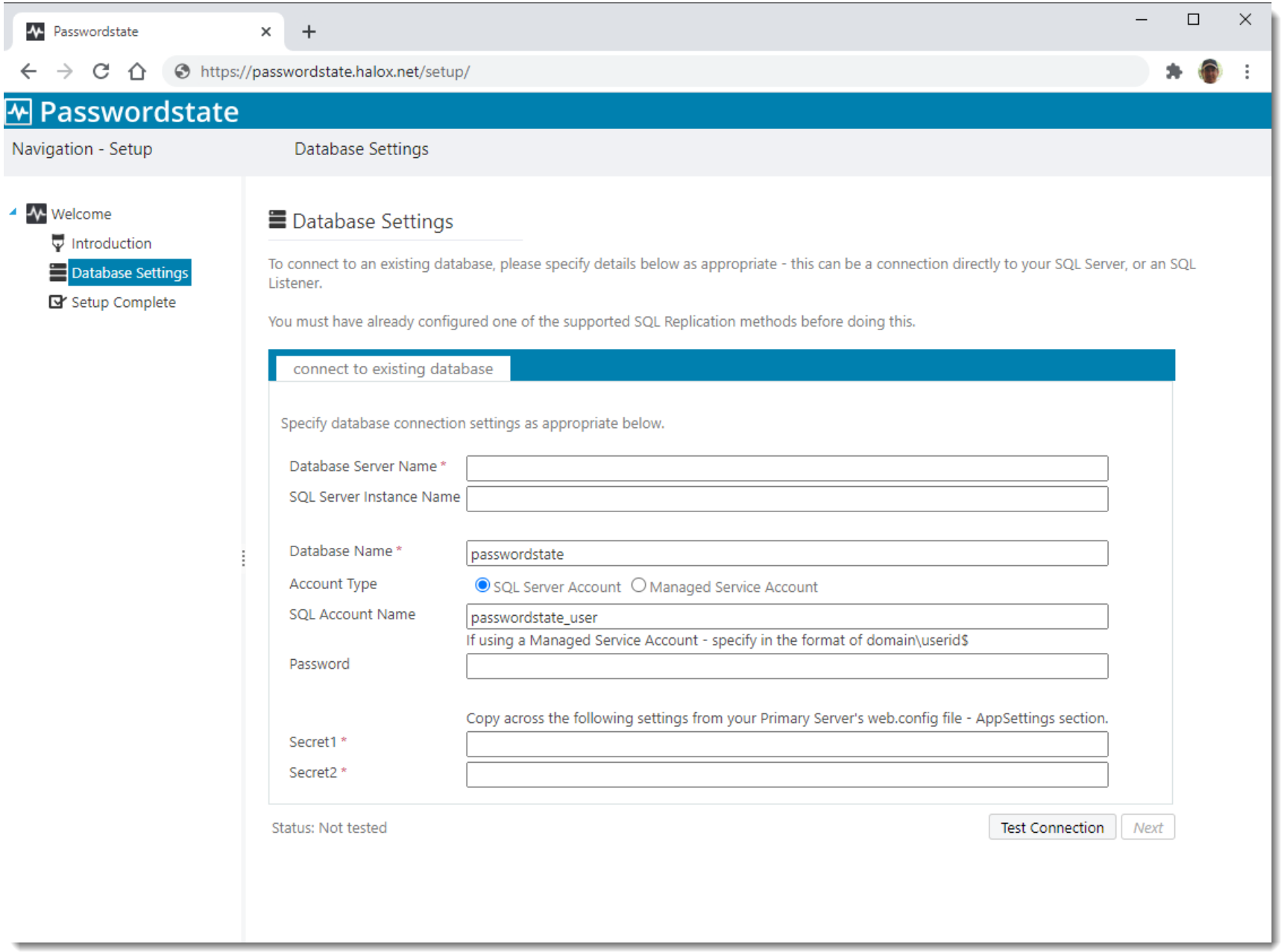
Introduction - Now that Passwordstate is installed, you can direct your browser to the URL you specified during the initial Windows Installer.

Click on the 'High availability Instance' option and you will be presented with the following screen.

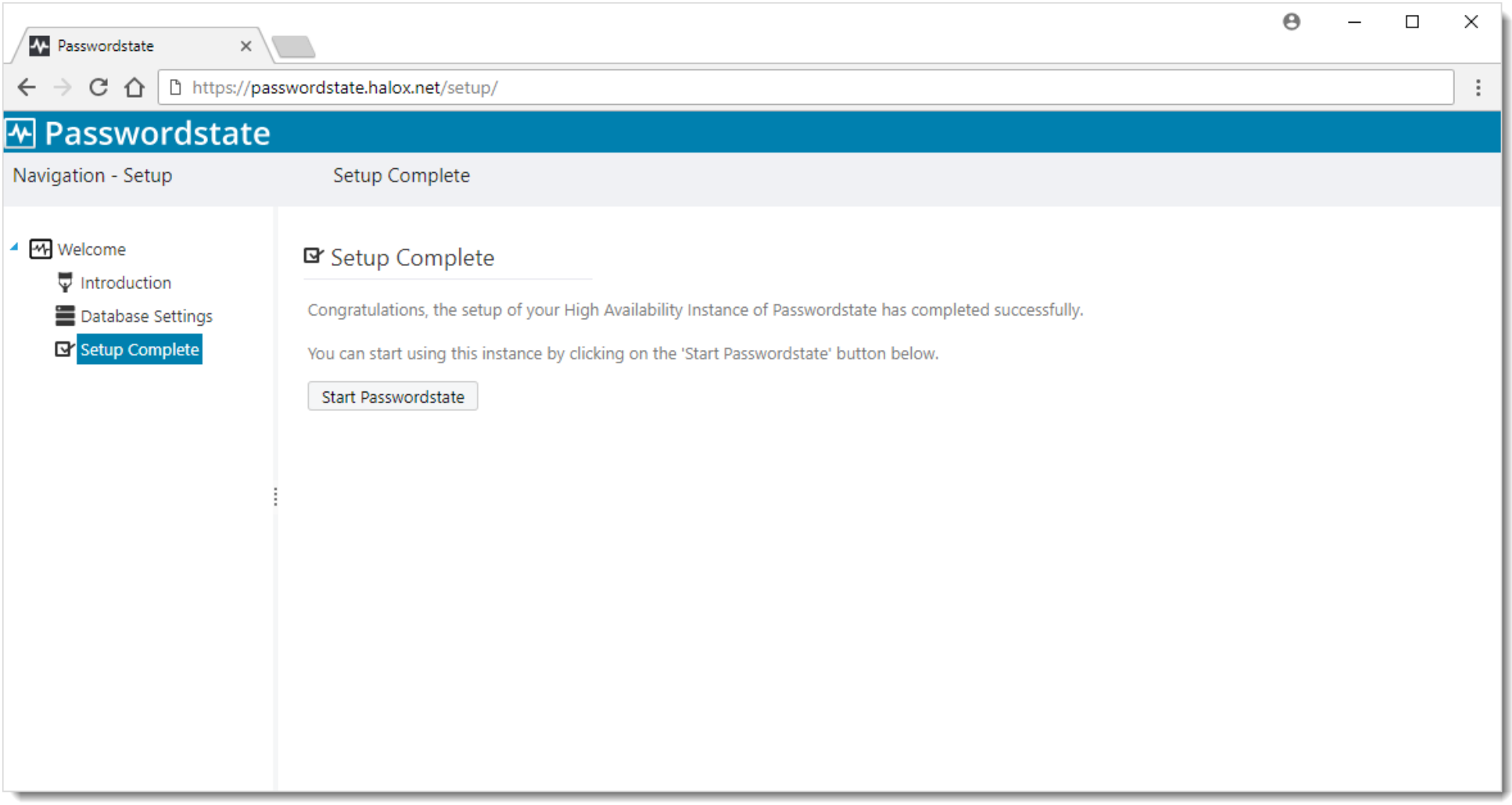


Database Settings – Connect to existing database – On this screen you will need to specify database settings to connect to your Passwordstate database. Please consider the following:

- You can either specify database connection settings to point directly to your database server, or to an SQL Listener if using Basic or Always On Availability Groups
- If you are wanting to connect using a Managed Service Account, you must first configure the Passwordstate IIS Application Pools to run under the identity of this MSA account
- You will need to copy across the Secret1 & Secret2 values from your primary site's web.config file


Passwordstate
https://passwordstate.halox.net/setup/
Passwordstate
Navigation - Setup
Database Settings
Welcome
Introduction
Database Settings
Setup Complete
Database Settings
To connect to an existing database, please specify details below as appropriate - this can be a connection directly to your SQL Server, or an SQL Listener.
You must have already configured one of the supported SQL Replication methods before doing this.
connect to existing database
Specify database connection settings as appropriate below.
Database Server Name *
SQL Server Instance Name
Database Name *
passwordstate
Account Type
SQL Server Account
Managed Service Account
SQL Account Name
passwordstate_user
If using a Managed Service Account - specify in the format of domain\userid$
Password
Copy across the following settings from your Primary Server's web.config file - AppSettings section.
Secret1 *
Secret2 *
Status: Not tested
Test Connection
Next

Setup Complete – The installation is now complete.



9 Encrypting/Decrypting the Web.config file

It is highly recommended to encrypt the **connectionStrings** and **appSettings** section in the web.config file, so any sensitive information such as your database connection string, or secret encryption keys are unreadable in the file.

To encrypt this file, follow this complete guide:
https://www.clickstudios.com.au/downloads/version9/Encrypt_Passwordstate_Config_Files.pdf

10 IIS MachineKey Requirements when Using Load balancers

By default, all Passwordstate installs set the Machine Key in IIS to “Auto-Generate” which randomises the Validation and Decryption machine key on the web server – used for ASP.NET ViewState.

If you have multiple Passwordstate web servers being Load Balanced, you will need to manually set the MachineKey on all web servers – to ensure seamless failover of session state.

Below are the steps for this:

1. On your primary web server, open **Internet Information Services (IIS) Manager**
2. Browse to the Passwordstate website, and click on **Machine Key** icon
3. Click the **Generate Keys** button on the right-hand side of the page, and then click the **Apply** button
4. Copy the "C:\inetpub\Passwordstate**web-machineKey.config**" file across to your second Passwordstate webserver, replacing the existing file