Click Studios

Passwordstate

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 System Requirements - General

The High Availability module of Passwordstate has the same system requirements as the primary install. Please refer to the document 'Installation_Instructions.pdf' for details.

Note: When using the High Availability module of Passwordstate, your distribution and publication databases must reside on SQL Server 2008, 2012, 2014 or 2016 – SQL Express can only act as a subscriber to SQL Server replication.

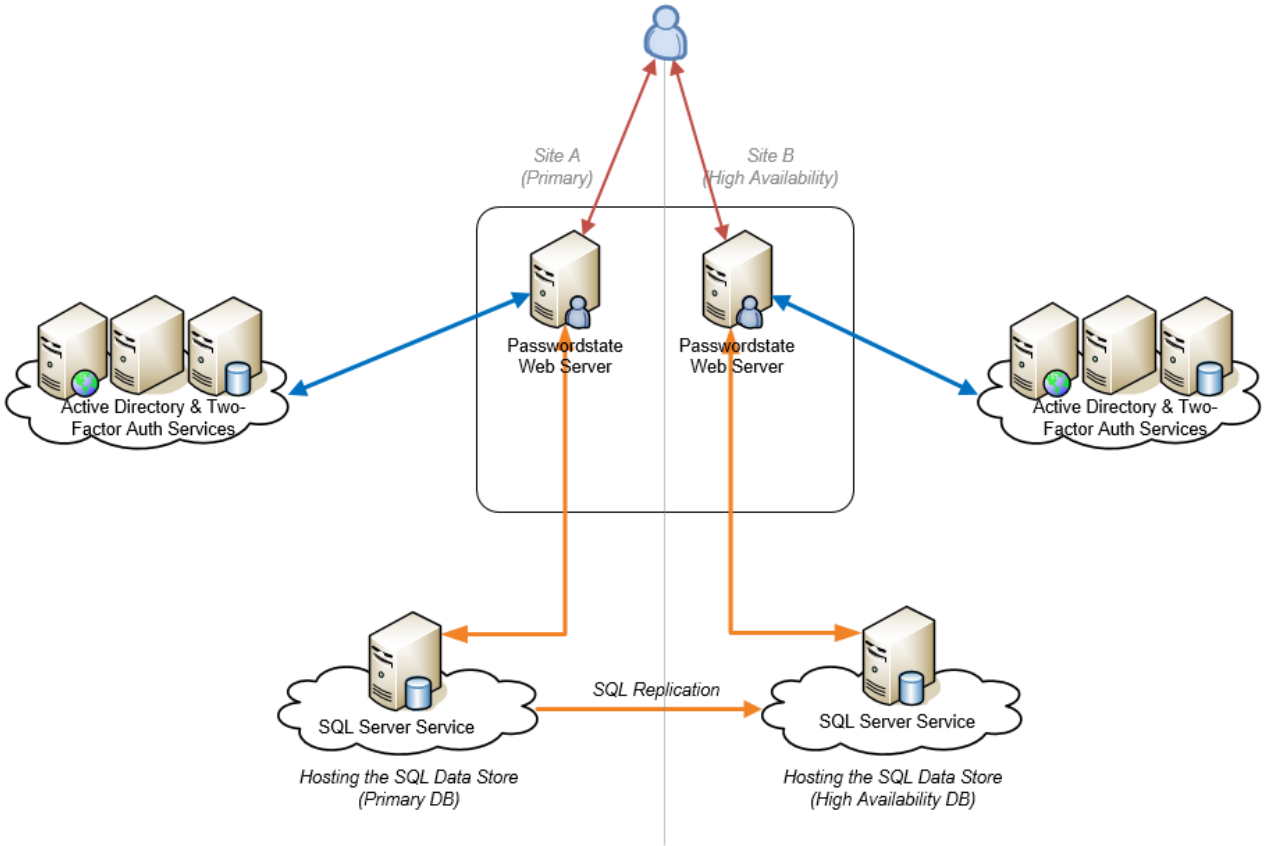
Important: SQL Server must be configured for mixed-mode authentication, so the Passwordstate web site can connect to SQL Server using an SQL Account

3 Architectural Overview

The following instructions describe an Active/Passive 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:

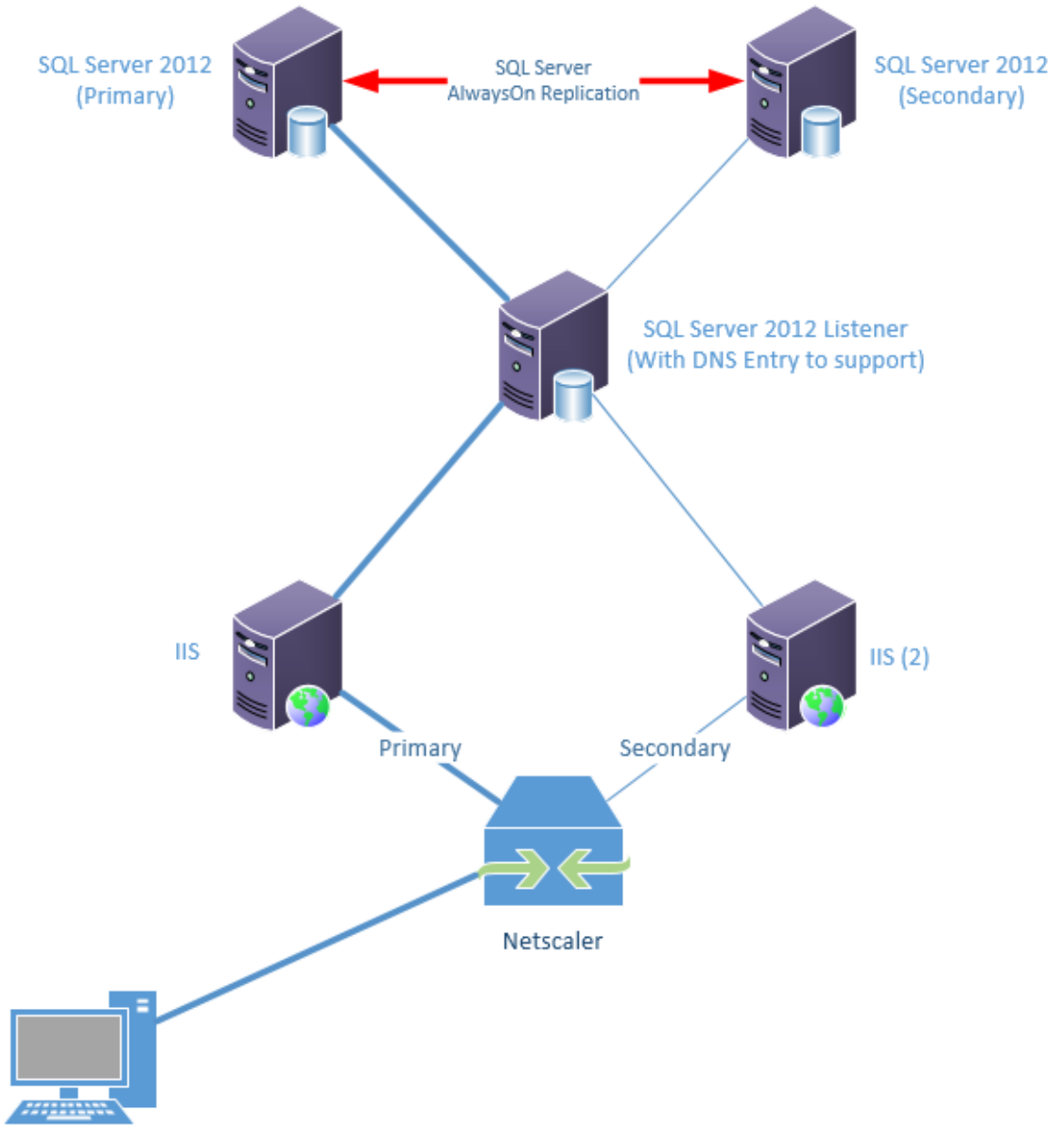
- Requires two web servers, and two database servers
- Data is replicated in real-time, using SQL Server Transactional Replication
- The publisher of the replication needs to be SQL Server Standard or above
- The subscriber of the replication needs to be SQL Server Express or above
- Generally, you only 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



We provide these instructions by default, as an Active/Active design requires additional load balancing hardware, and the use of SQL Server 2012 High Availability groups.

A summary of the Active/Active design is:

- As per the diagram below, this shows the use of a Citrix Netscaler Load Balancer, or you could use any other load balancer such as F5 BIG-IP Local Traffic Manager
- The Load Balancer monitors the availability of the Passwordstate web servers, and automatically fails over if one cannot be communicated with
- SQL Server High Availability Groups are used to monitor availability of both SQL Servers, and perform automatic failover in the event where one server becomes unavailable



If you do not have hardware load balancing available to you, then possibly SQL Server Failover Clustering may be able to help you. The following document describes how to configure this - https://support.microsoft.com/en-us/kb/970759 (Note: this has not been tested by Click Studios)

Note: The remainder of these instructions are for the Active/Passive design, using SQL Server Transactional replication. Even with this design, you can use other methods of moving data to the HA database server, such as database mirroring, log shipping, database backup and restore, etc.

4 SQL Server Considerations

For the High Availability instance of Passwordstate, there are a few things to consider relating to SQL Server.

Let Passwordstate Create its Own Database

Prior to installing Passwordstate, you must have an SQL Account with sufficient permissions to create the database and tables (generally an SQL Server role of 'sysadmin' or 'dbcreator' e.g. sa account). You must not specify a Windows Active Directory account in order to create the Passwordstate database.

Create Your Own Database, and Let Passwordstate Connect to it
You will need to have created the empty database, and an SQL Account for Passwordstate to connect to this empty database. The SQL Account requires db_owner rights to the Passwordstate database only

SQL Server Replication Permissions
For SQL Server Replication, Microsoft recommends the use of an Active Directory domain account for replicating data between source and destination databases. **This domain account must be a member of the db_owner fixed database role in the 'Distribution' and both 'passwordstate' databases. It must also have write permissions on the snapshot file share area**. You can tell if the permissions are correct by checking the folder where the snapshot data is stored to see if some replication data exists after you finish creating the Publisher. Please speak to your Database Administrator for more information relating to SQL Server Replication permissions.

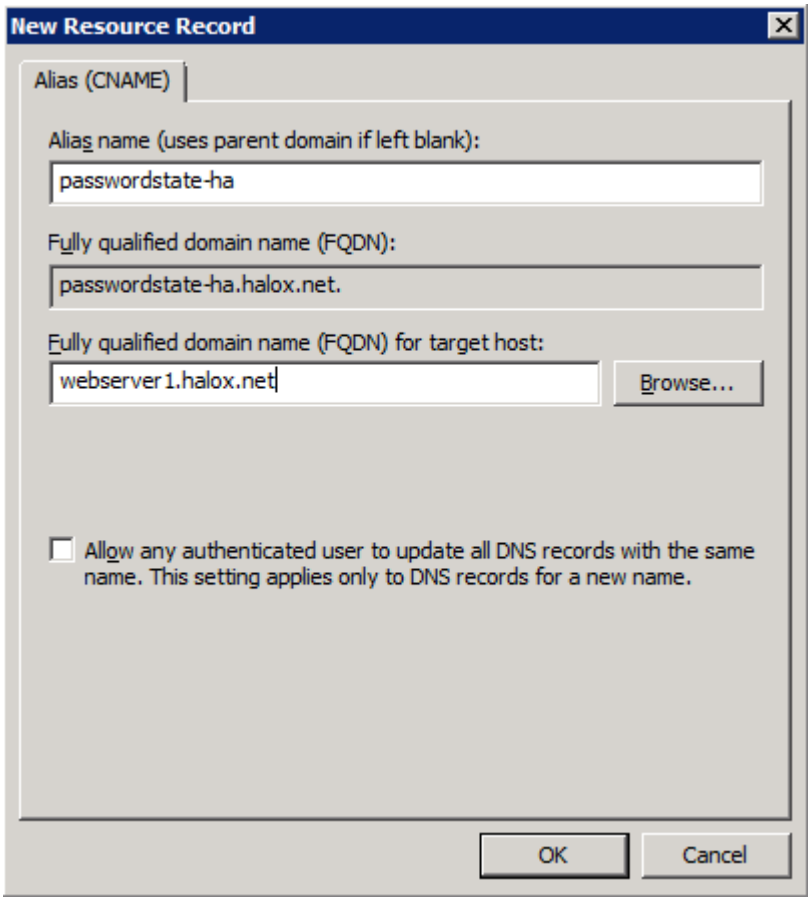
SQL Server Port Considerations
If you are running SQL Server on a non-standard port number, you will need to append the port number to the end of the Database Server Name during '5. Configuring Passwordstate for First Time Use' in the following way: ServerHostName,PortNumber i.e. sqlserver1,8484

5 Creating an Appropriate DNS Record

During the installation of the High Availability instance of Passwordstate, you have the option of using a URL which has the host name of the web server in it, or you can specify your own custom URL e.g. https://passwordstate-ha

If you want to use your own custom URL, you will need to create a CNAME DNS entry as per the following instructions (please do not use host files for name resolution, as they do not work with Windows Authentication in IIS):

1. On your server hosting DNS, start 'DNS Manager'
2. Right click on the appropriate domain, and select 'New Alias (CNAME)'
3. As per the following screenshot, specify the name of your web server host name in the 'Fully qualified domain name (FQDN) for target host' text box, then click on the 'OK' button



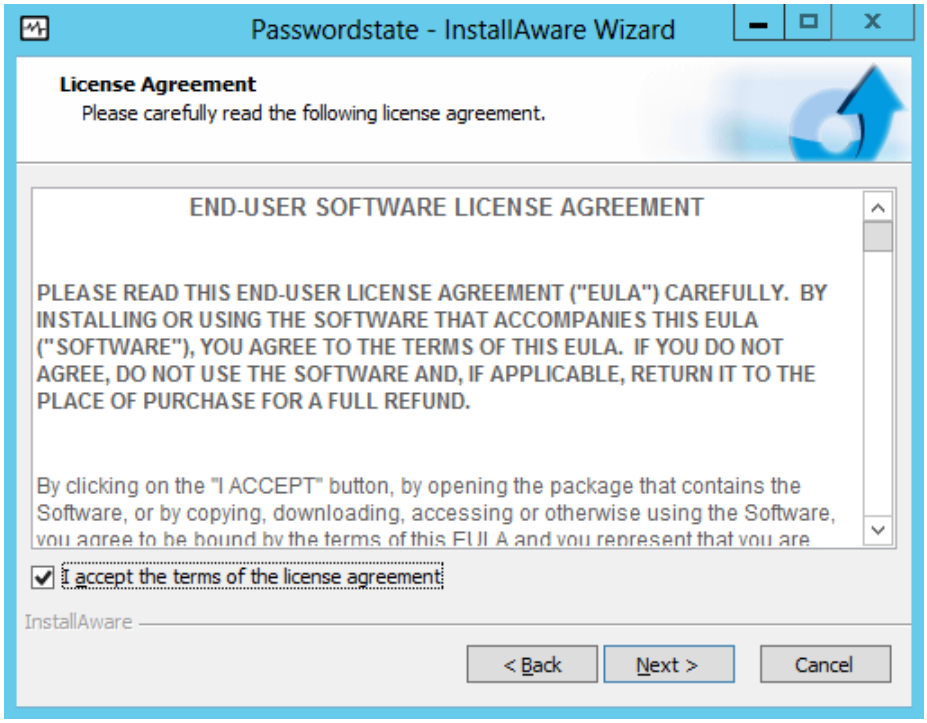
Once installed, and using the example above, you will be able to access Passwordstate by typing https://passwordstate-ha into your browser.

6 Installing Passwordstate

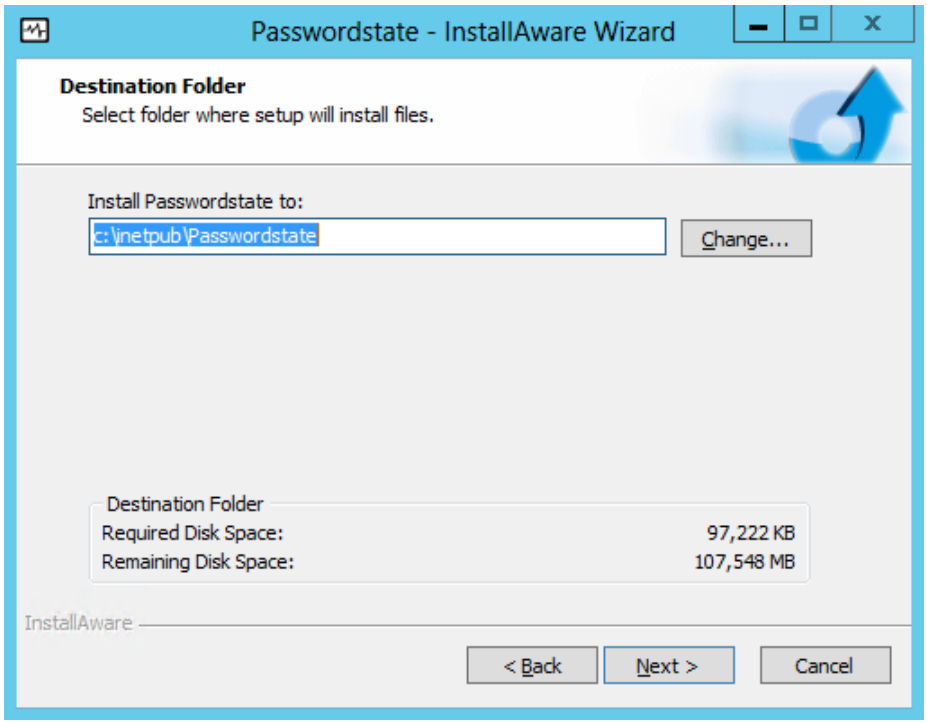
To install Passwordstate, run 'Passwordstate.exe' and follow these instructions:

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

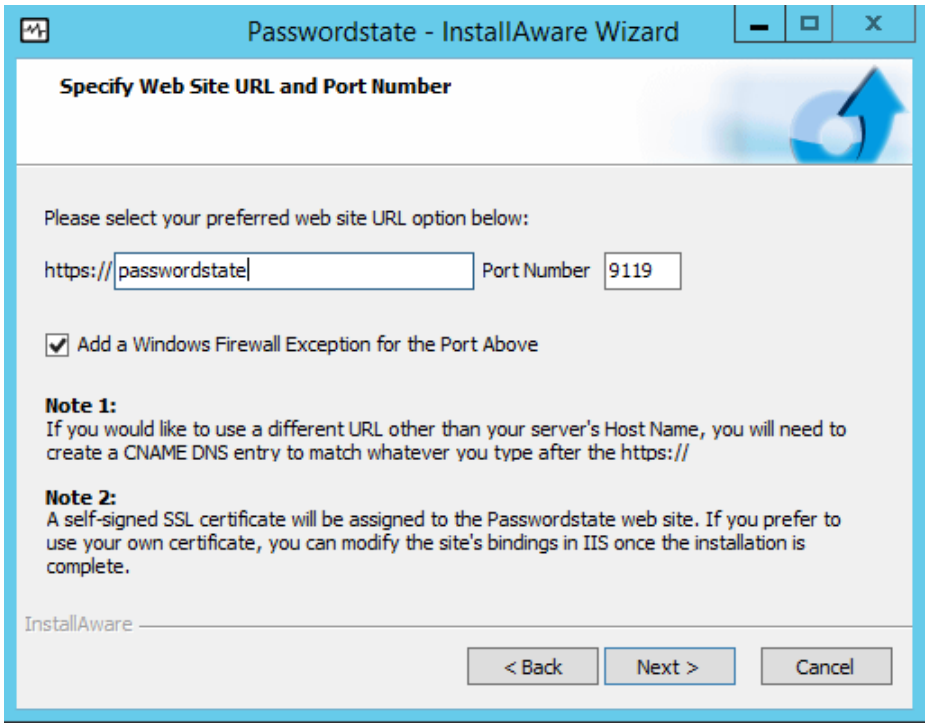
2. At the 'License Agreement' screen, tick the option 'I accept the terms in the License Agreement', then click on the 'Next' button



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



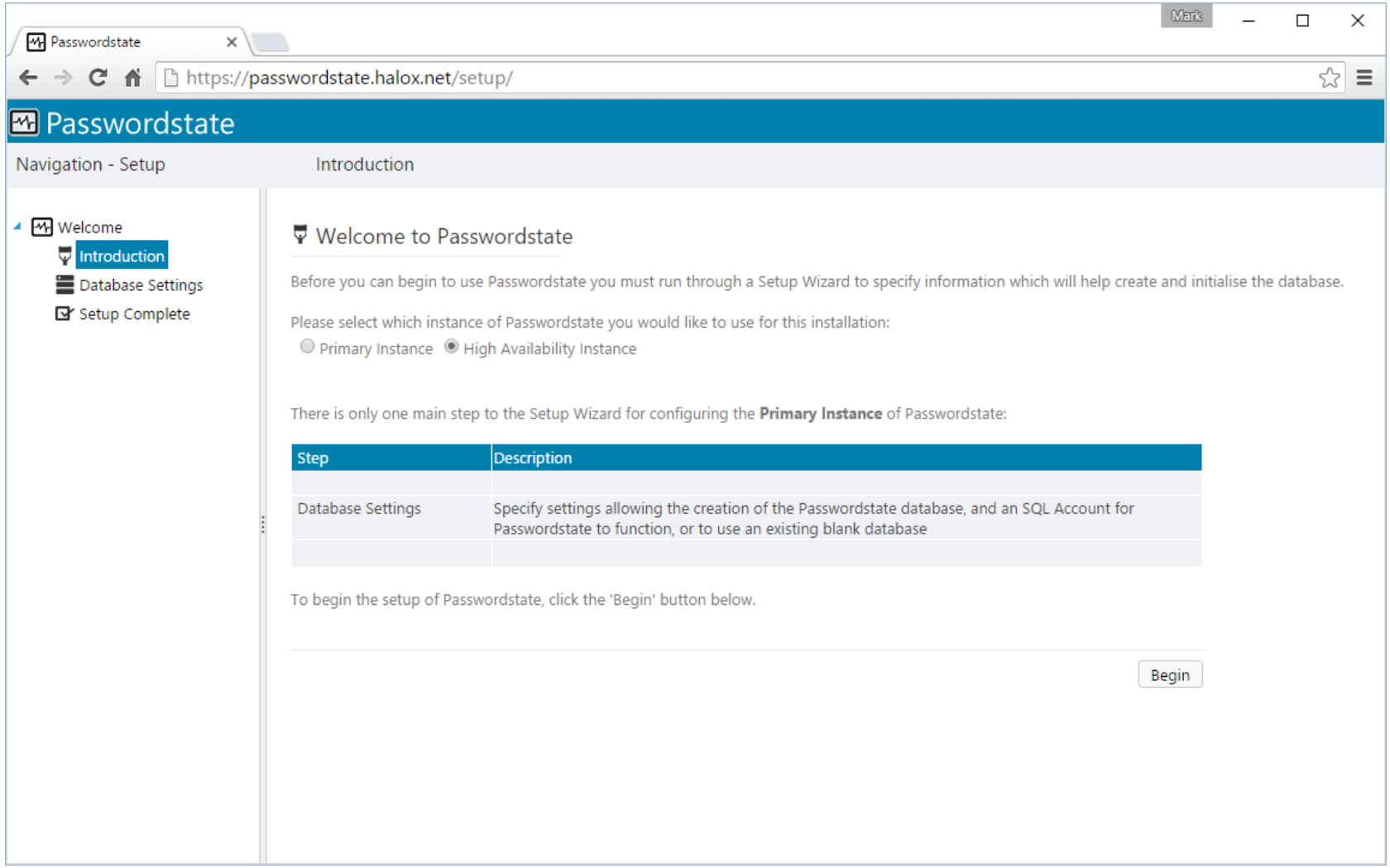
5. At the ‘Completing the InstallAware Wizard for Passwordstate’ screen, click on the ‘Next’ button

6. Once installed, click on the ‘Finish’ button

7 Configuring Passwordstate for First Time Use

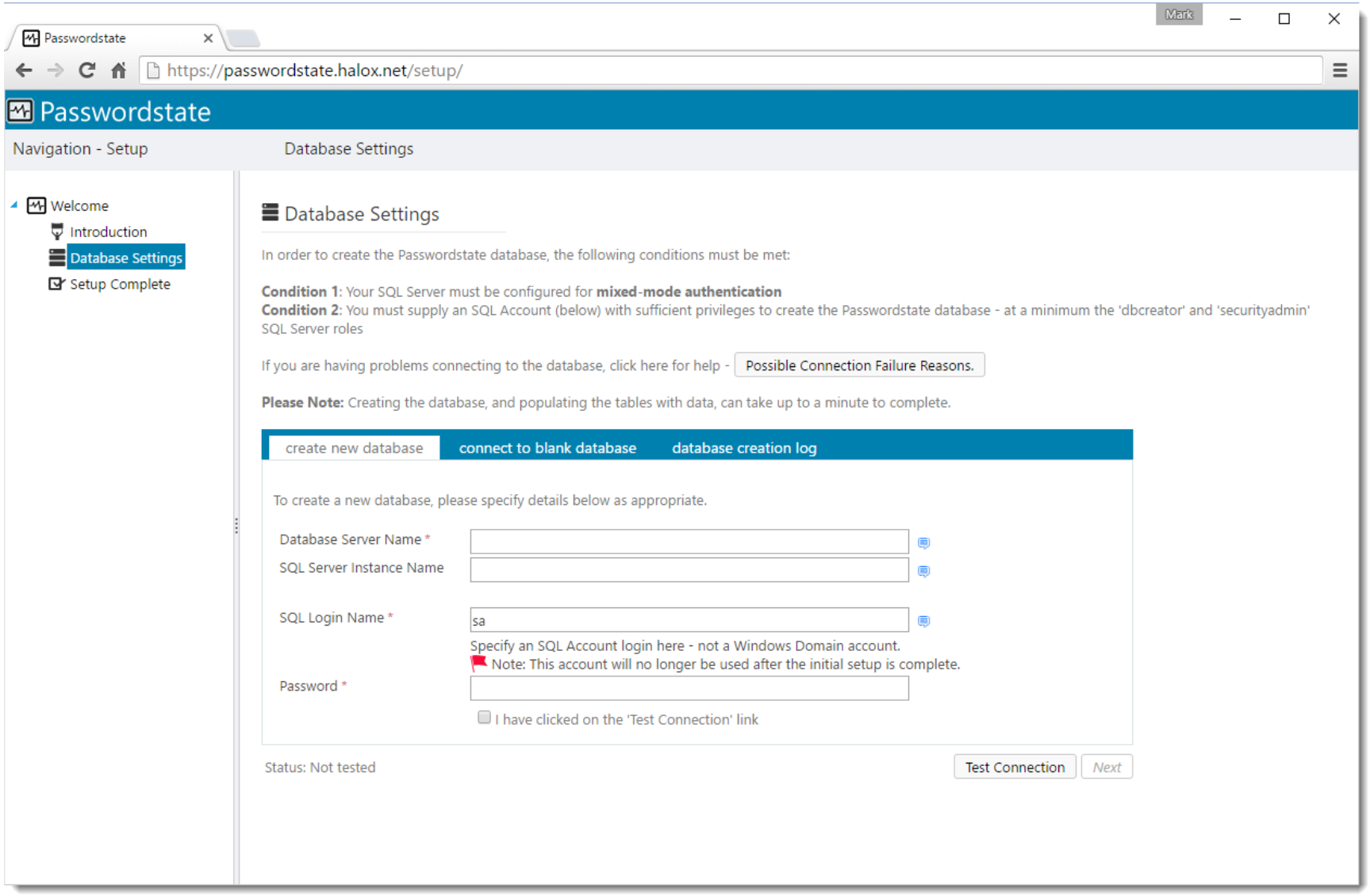
Introduction - Now that Passwordstate is installed, you can direct your browser to the DNS entry you specified in Section 3 - Creating an Appropriate DNS Record, and follow the initial Setup Wizard – this wizard will guide you through a series of questions for configuring Passwordstate for use.

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



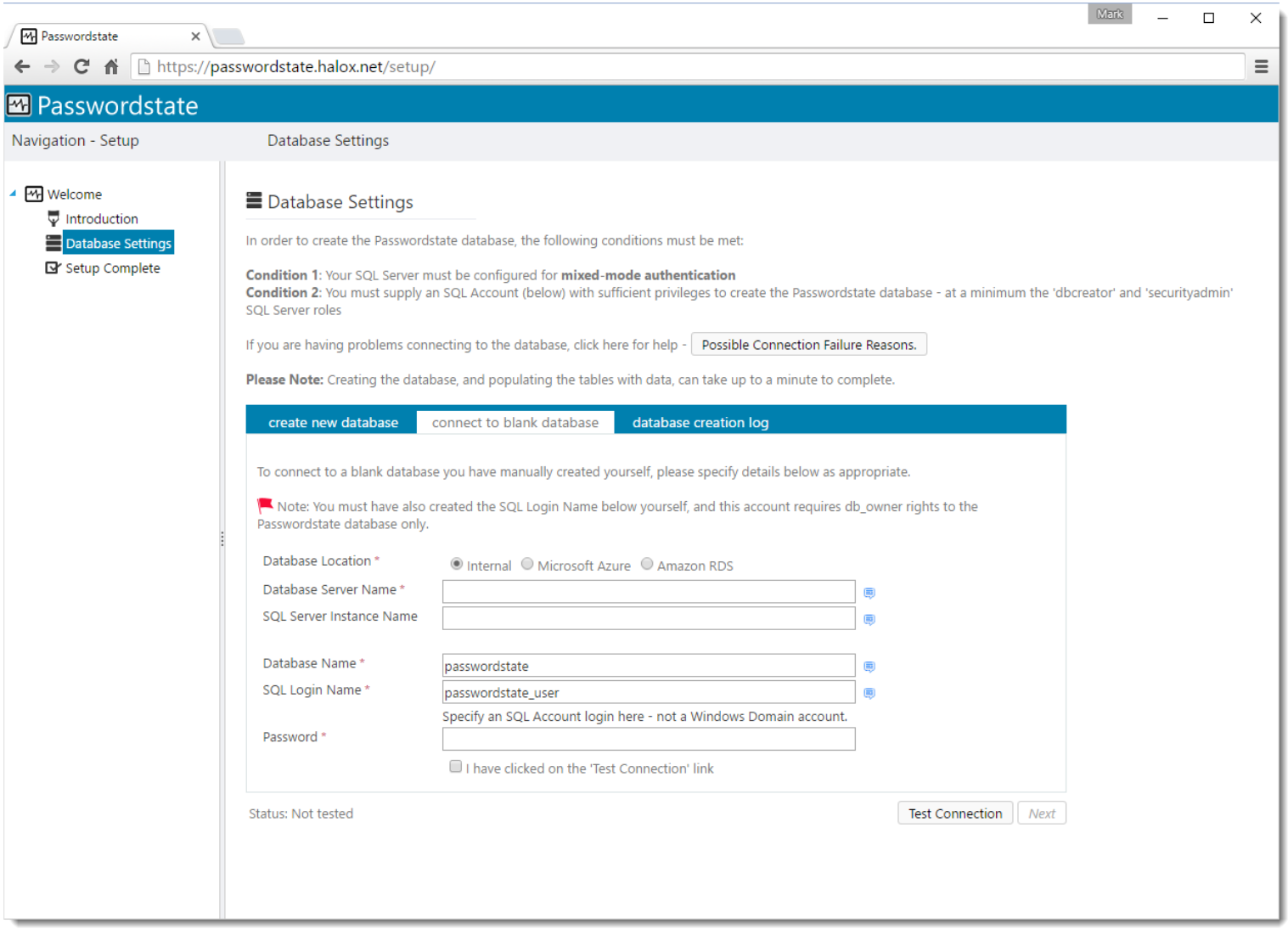
Database Settings – Create New Database – On this screen you will need to specify database settings for creating the Passwordstate database. Please use the onscreen instructions if you have any issues connecting to the database.

Please Note: After the database is created, no tables will be populated with data as SQL Server replication will fulfil this function.



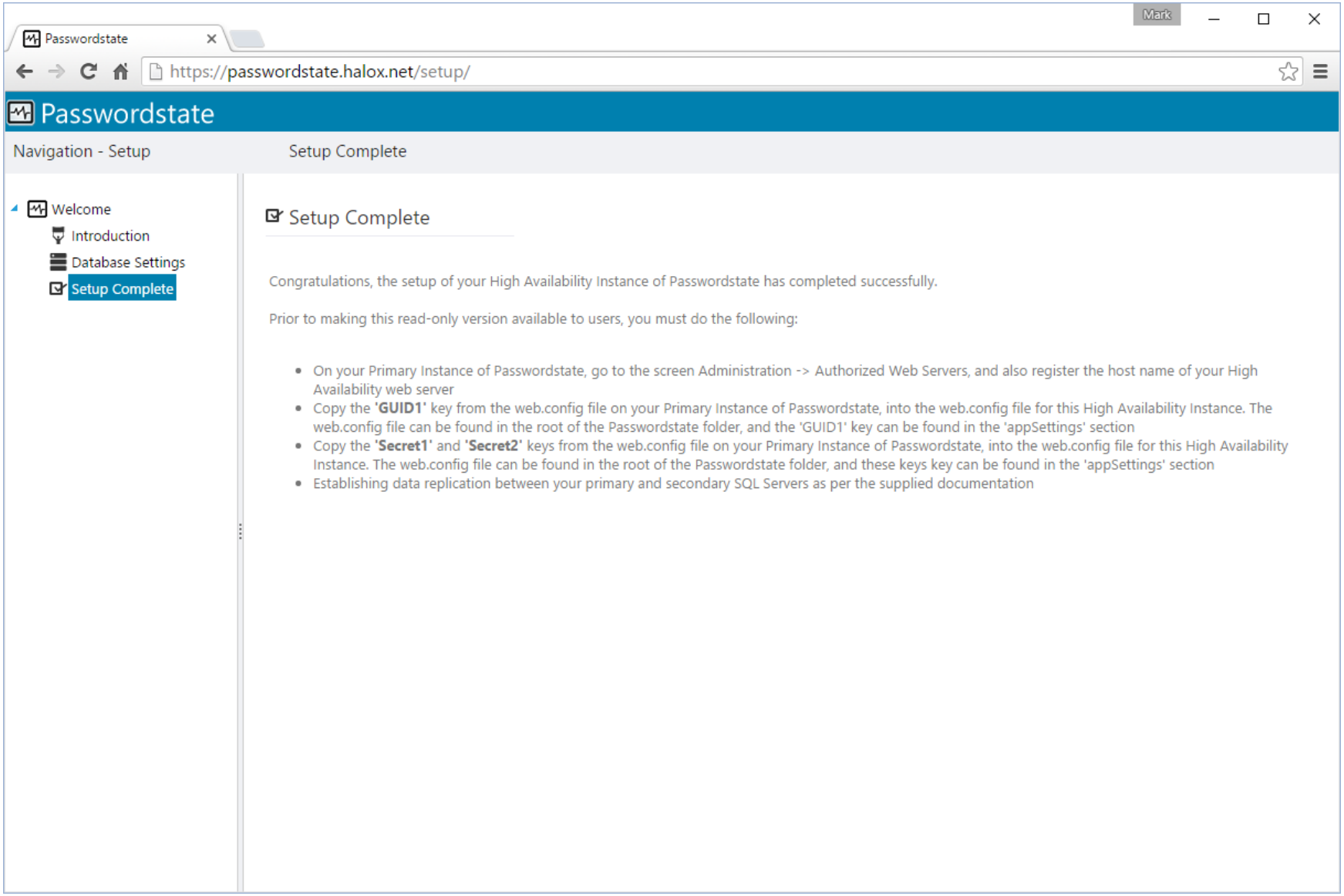
Database Settings – Connect to Blank Database – If you prefer to create the blank Passwordstate database yourself prior to tables being created and populated with data, you can do so by clicking on the 'Connect to Blank Database' tab first.

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.



Setup Complete – The installation is now complete. To configure SQL Server to replicate data, please continue reading this document.

Note: It is very important to copy the GUID1, Secret1 & Secret2 keys across from your primary instance of Passwordstate, otherwise the HA instance will not work.



8 Passwordstate Windows Service and Active/Active Configuration

Build 7253 and Above

If you are configuring Passwordstate in an Active/Active configuration, using SQL Server High Availability Groups or Clustering which allows data to be written by both Passwordstate instances, it is recommended you:

1. On the High Availability web server, open the web.config file with an editor and change:

   <add key="PassiveNode" value="true" />

   to

   <add key="PassiveNode" value="active" />

2. Then restart the Passwordstate Windows Service

By doing this, it will allow the Passwordstate Windows Service to write to disk any newly uploaded images in the database.

Below are the possible values for the PassiveNode key, and what they mean:

- <add key="PassiveNode" value="false" /> - Web Interface can have data written as normal, and Passwordstate Windows Service performs normal processing (this is used on the Primary Instance)
- <add key="PassiveNode" value="true" /> - Web Interface is in read-only mode, and Passwordstate Windows Service does not process anything (except for writing new images to disk, and moving auditing data back to the Primary Instance)
- <add key="PassiveNode" value="active" /> - Web interface can have data written as normal, and Passwordstate Windows Service does not process anything (except writing new images to disk)


Note: Do not make this change to the High Availability instance if you are using SQL Server Transactional Replication to move data between database servers.

Build 7243 and Below

When using Build 7243 or below, it is recommended you disable the Passwordstate Windows Service so that it does not try to process any data changes which may conflict with the Primary Instance of Passwordstate doing the same thing.

9 Authorized Web Server & License Keys

Prior to establishing SQL Server data replication, there are three things which need to be done:

1. On your Primary Instance of Passwordstate, go to the screen Administration -> License Information, and add your High Availability License key here
2. 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
3. Copy across the GUID1, Secret1 & Secret2 keys from the web.config file on your Primary Instance of Passwordstate, into the web.config file for this High Availability Instance. The web.config file can be found in the root of the Passwordstate folder, and these keys can be found in the 'appSettings' section. You need to copy and paste the entire keys, which is in the format of:

   <add key="GUID1" value="0aafc8ea-b14e-6719-82f3-3c1e6f0f27e9" />

   <add key="Secret1" value="2d1-1-bd05439a4d7dda2129aef6……." />

   <add key="Secret2" value="801-1-6b061297ad2c9402e7cf8f3……." />

10 Encrypting the Database Connection String in the Web.config file

Whilst it's not entirely necessary to encrypt the database connection strings within the web.config file, it is recommended so the SQL Account credentials used to access the Passwordstate database is encrypted and unreadable from anyone who can read the file system on your web server.

To encrypt the database connections string, please follow these instructions:

Encrypt Connection String

- Open a command prompt and type CD C:\Windows\Microsoft.NET\Framework64\v4.0.30319
- Type the following:
    - aspnet_regiis.exe -pef "connectionStrings" "c:\inetpub\passwordstate" (change the path if you've installed Passwordstate to a different location)

Decrypt Connection String

- Open a command prompt and type CD C:\Windows\Microsoft.NET\Framework64\v4.0.30319
- Type the following:
    - aspnet_regiis.exe -pdf "connectionStrings" "c:\inetpub\passwordstate" (change the path if you've installed Passwordstate to a different location)

Note 1: If you intend to rename your server host name, or move your Passwordstate install to a different server, you should decrypt these settings first.

Note 2: If you do not wish to use an SQL Account to connect to your database server, please refer to the section below in this document titled 'Configure Passwordstate to use a Managed Service Account (MSA) to connect to the database'.

11 Encrypting the appSettings Section within the Web.config file

It is also not entirely necessary to encrypt the appSettings section within the web.config file, but as this section of the file stores half of your split encryption keys, it is recommended for added security.

To encrypt the appSettings section, please follow these instructions:

Encrypt appSettings Section

- Open a command prompt and type CD C:\Windows\Microsoft.NET\Framework64\v4.0.30319
- Type the following:
    - aspnet_regiis.exe -pef "appSettings" "c:\inetpub\passwordstate" (change the path if you've installed Passwordstate to a different location)

Decrypt appSettings Section

- Open a command prompt and type CD C:\Windows\Microsoft.NET\Framework64\v4.0.30319
- Type the following:
    - aspnet_regiis.exe -pdf "appSettings" "c:\inetpub\passwordstate" (change the path if you've installed Passwordstate to a different location)

Note: If you intend to rename your server host name, or move your Passwordstate install to a different server, you should decrypt these settings first.

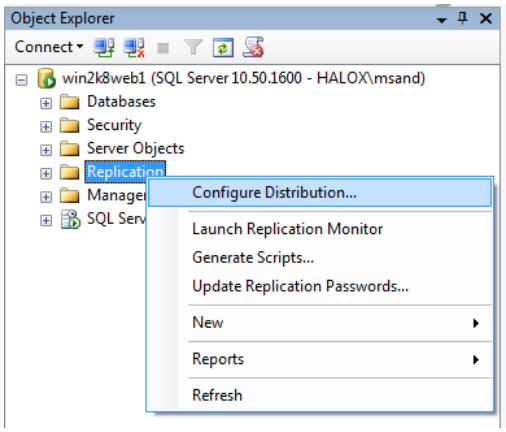
12 Configuring the Distribution Database

Prior to starting, ensure SQL Server Replication is installed on the server which will be used as the Publisher, and the server acting as the Subscriber.

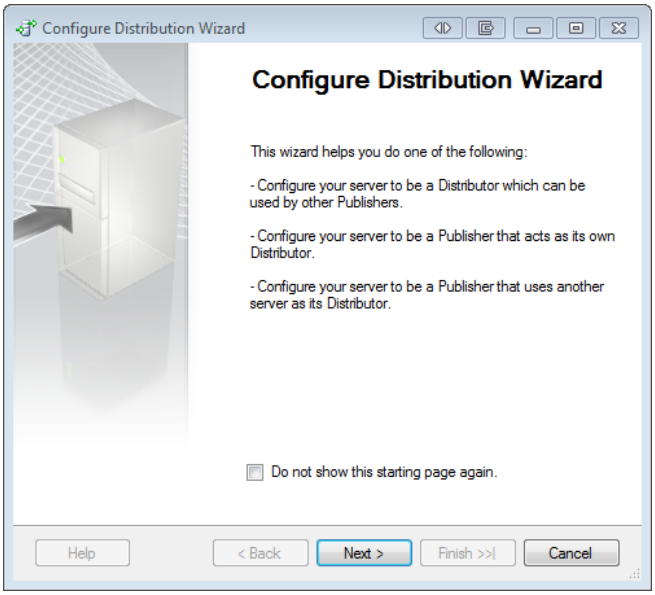
You may not need to setup the Distribution Database if you are already using SQL Server to replicate data. Please speak to your Database Administrator if you are unsure.

Please Note: The following instructions are provided using SQL Server 2008 R2 Management Studio. The screenshots and instructions may look different if you are using a different version of SQL Server

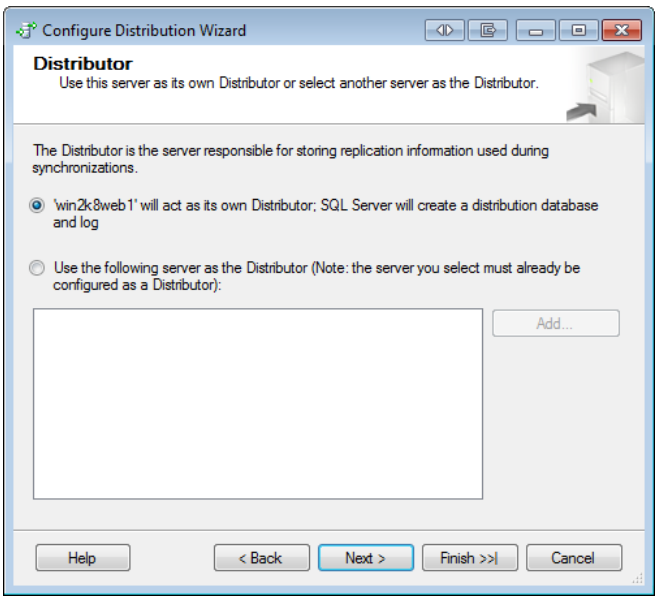
1. Right Click on the Replication node and Select Configure Distribution as shown in the screenshot below:



2. A new window appears on the screen as shown in the screenshot below:

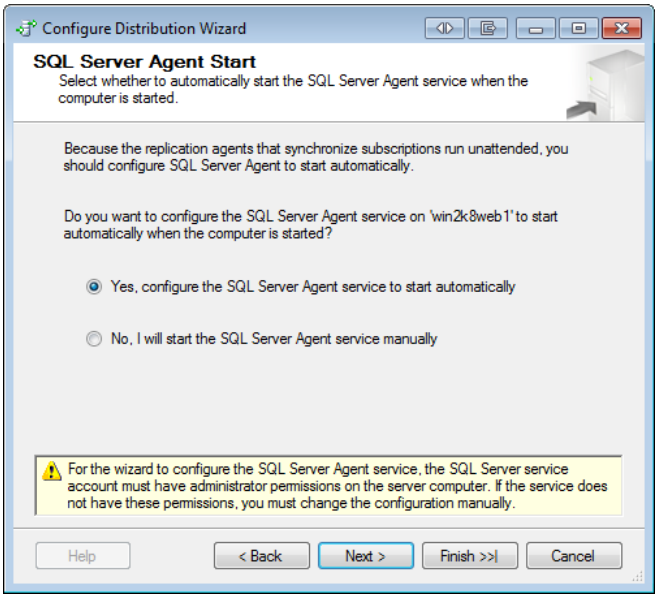


3. Click the 'Next' button and a new window appears on the screen as shown in the screenshot below:



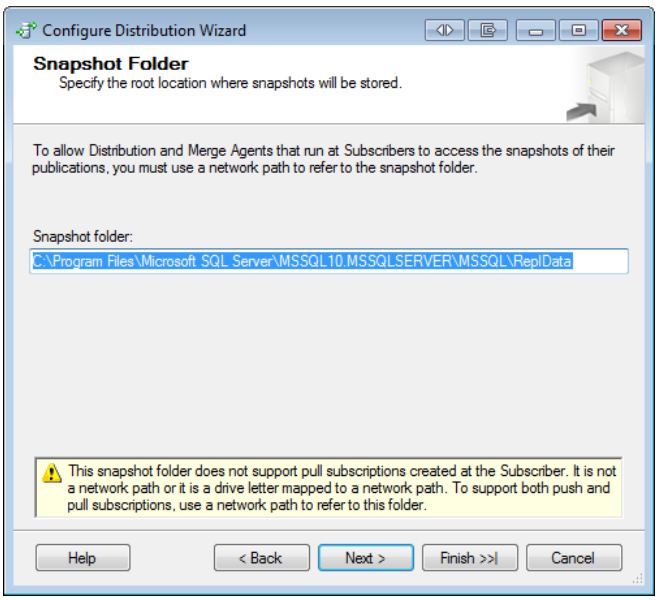
4. As you can see in the above screenshot, you will be provided two choices of where to configure the Distribution database – you can either configure it on the same server which is acting as the Publishing server, or you can configure it on a different server all together. This document describes configuring it on the same server which will be used as the Publishing server, but speak to your SQL Administrator if you are unsure of the best settings for your organisation. Then Click on the 'Next' button as shown in the screenshot above.

5. A new window appears as shown in the screenshot below:



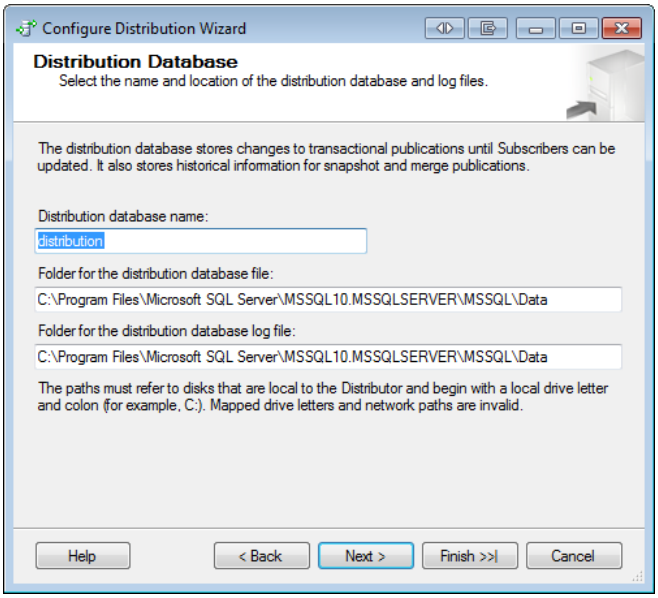
6. Select the first option, i.e. Yes, configure the SQL Server Agent service to start automatically and click on the 'Next' button as shown in the screenshot above.

7. A new window appears on the screen as shown in the screenshot below:



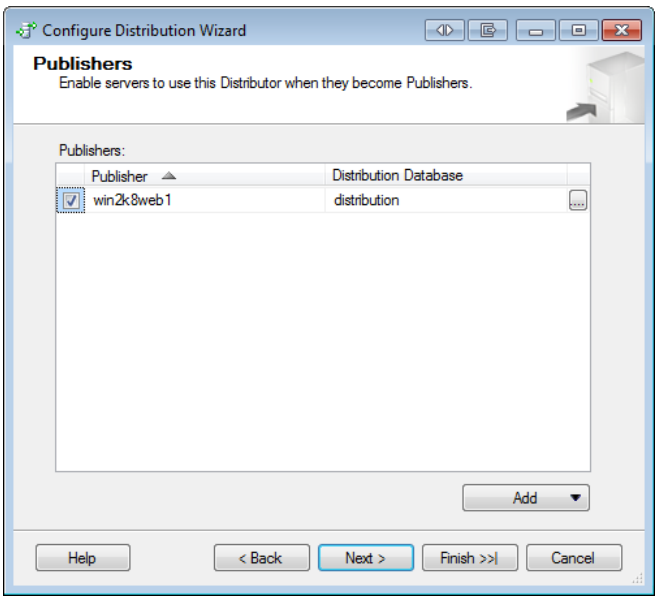
As you can see in the above screenshot, you are asked where the Snapshot folder should reside on the Server. The Snapshot Agent prepares snapshot files containing schema and data of published tables and database objects, stores the files in the snapshot folder. It is advised not to place the replication data on the C drive of the server i.e. the drive which is hosting the Operating System.
Create a folder on any other drive to hold the Snapshot folder and Click on the 'Next' button as shown in the screenshot above.

8. A new window appears as shown in the screenshot below:

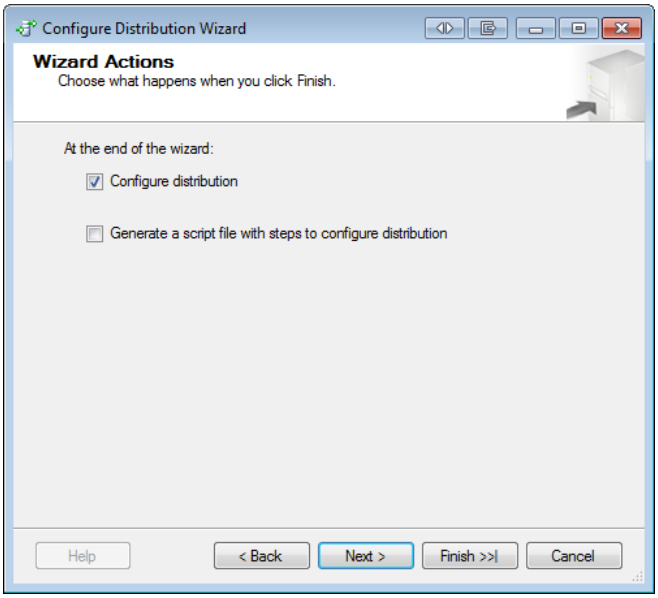


As you can see, it displays information for the name of the Distribution database, as well as its location on the file system. Click on the 'Next' button as shown in the screenshot above.

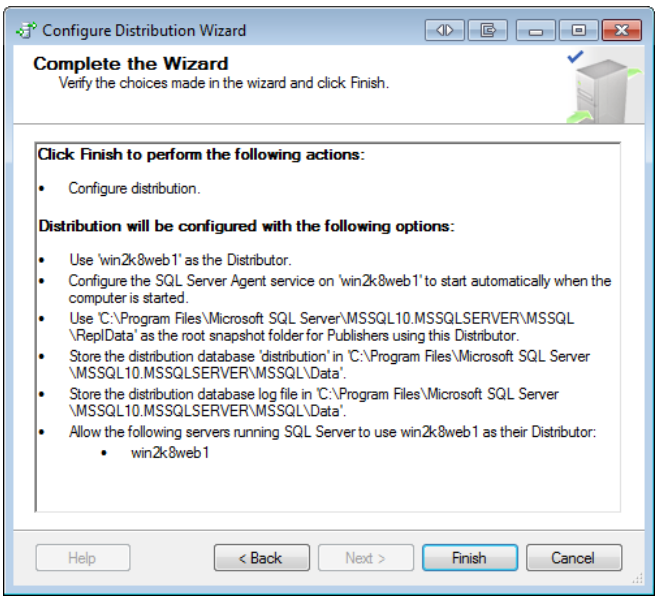
9. A new window appears as shown in the screenshot below:



10. Click on the 'Next' button.
11. Click on the 'Next' button as shown in the screenshot below:



12. Click on the Finish button as shown in the screenshot below:

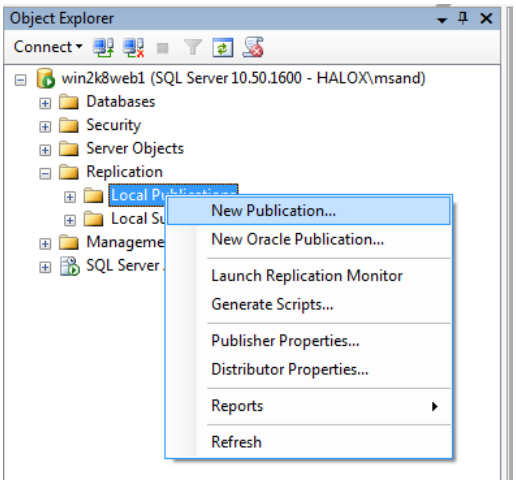


13. Now that the distribution database is created, just confirm it exists under the ‘System Databases’ node.

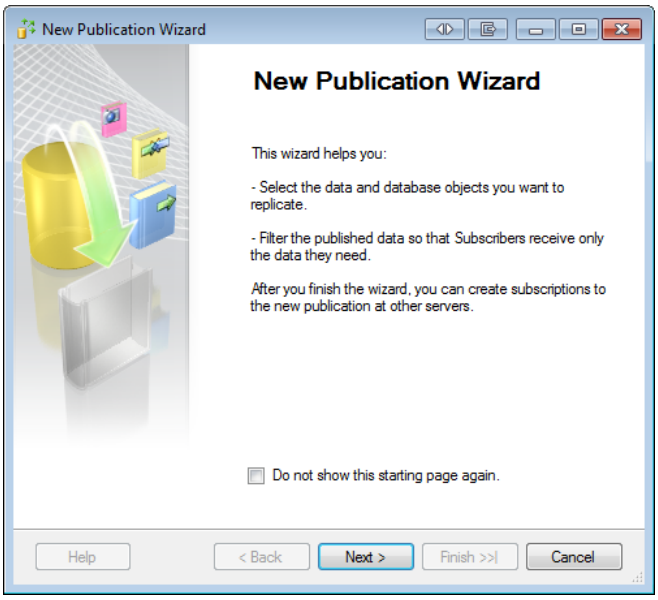
13 Creating the Publisher

The following steps need to be followed while creating the publisher.

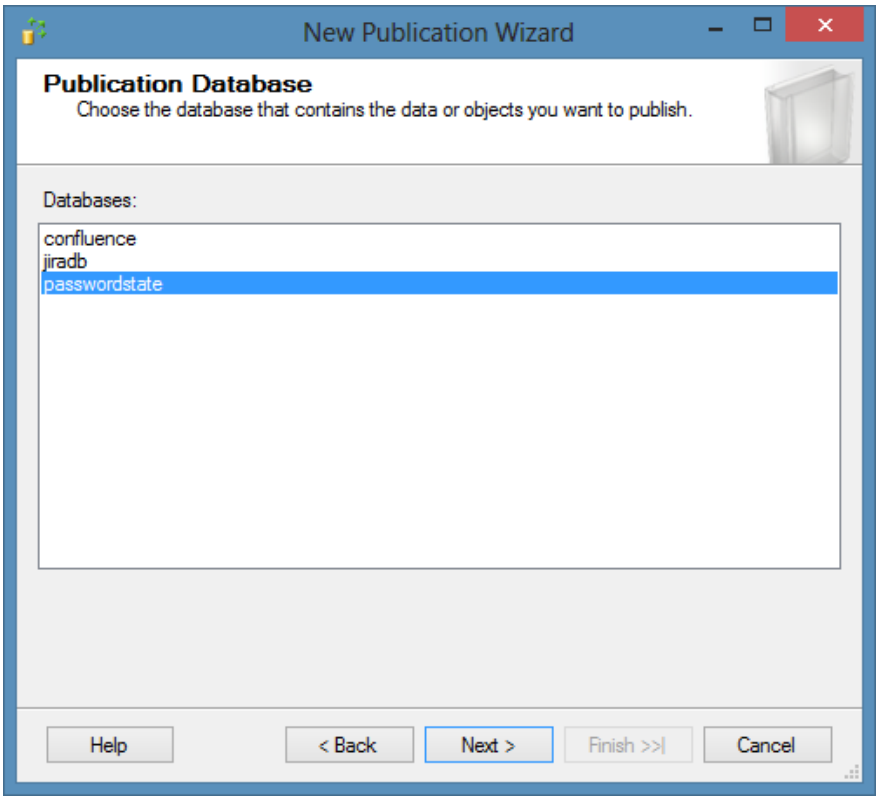
1. Right Click on Local Publications and select New Publications, please refer the screenshot below:



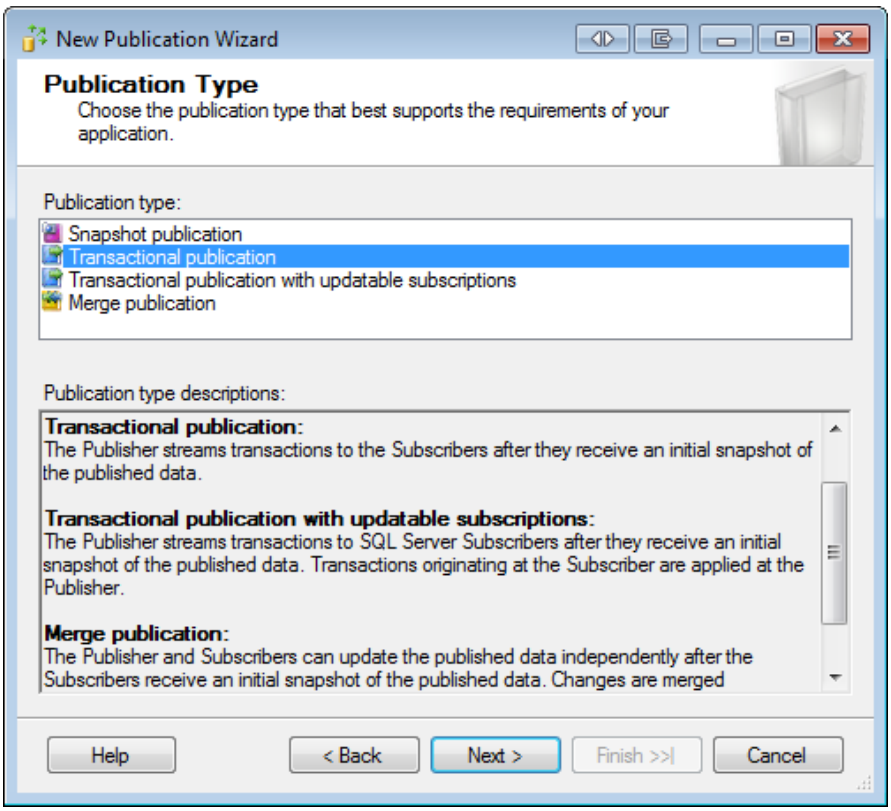
2. Click on the 'Next' button as shown in the screenshot below.



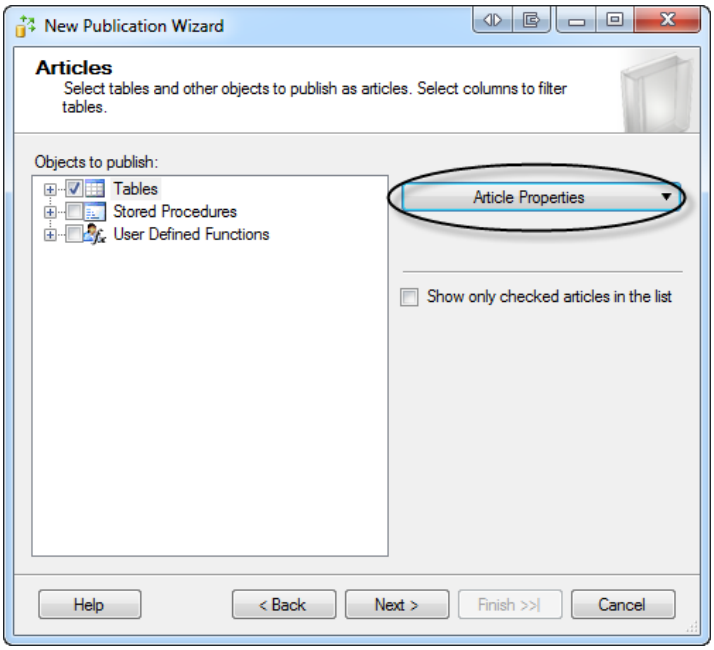
3. Select the database which is going to act as a publisher - in your case it would be **passwordstate**. Click on the 'Next' button.



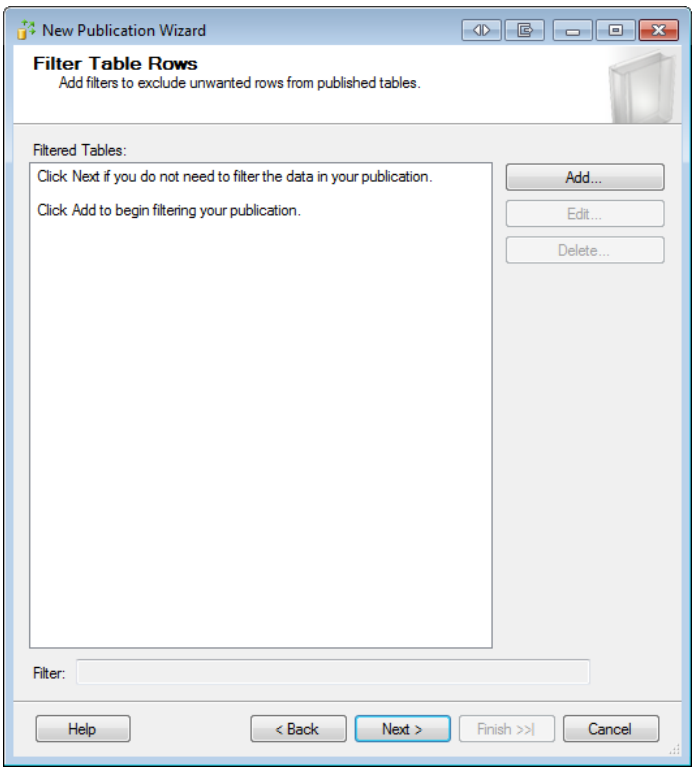
4. Select Transactional Publication from the available publication type and Click on the 'Next' button as shown in the screenshot below:



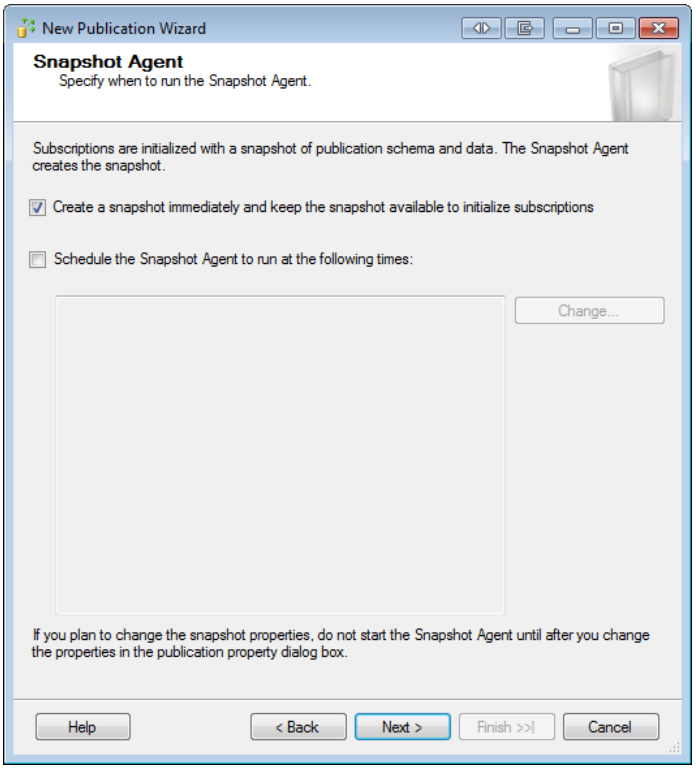
5. Select all the Tables for the Passwordstate database, select 'Set Properties of All Table Articles' from the 'Articles Properties' dropdown list and set the following options to True if not already set:
    a. Copy foreign key constraints
    b. Copy check constraints
    c. Copy clustered index
    d. Copy nonclustered indexes
    e. Copy default value specifications
    f. Copy extended properties
    g. Copy unique key constraints



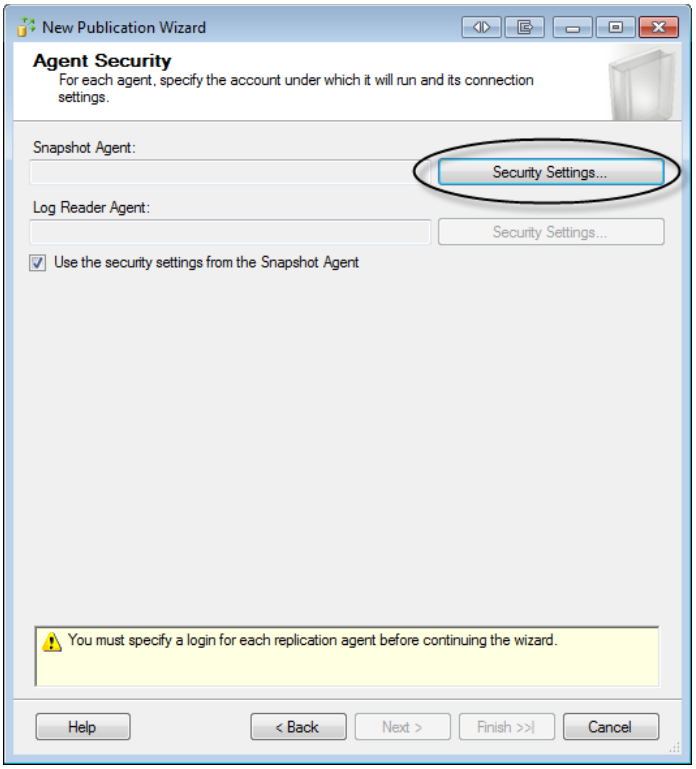
6. Since there are no filtering conditions, Click on the 'Next' button as shown in the screenshot below:



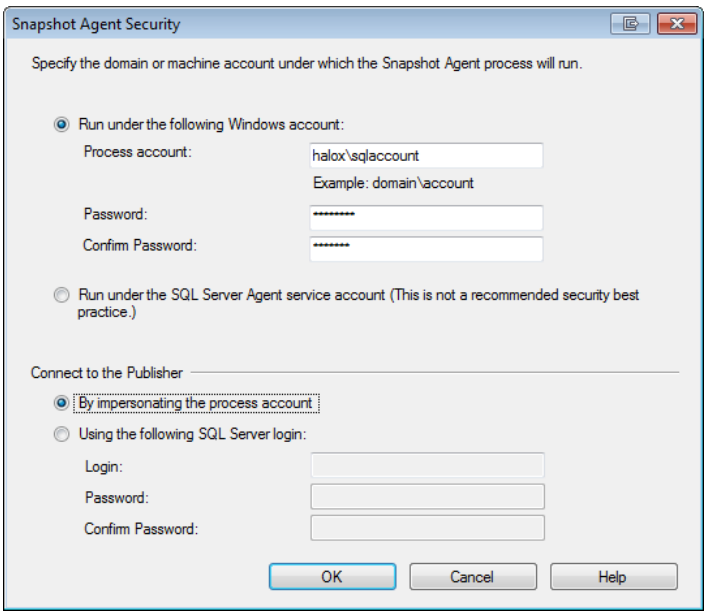
7. Check the first checkbox as shown in the screenshot below and Click on the ‘Next’ button.



8. Click on the Security Settings tab as shown in the screenshot below.

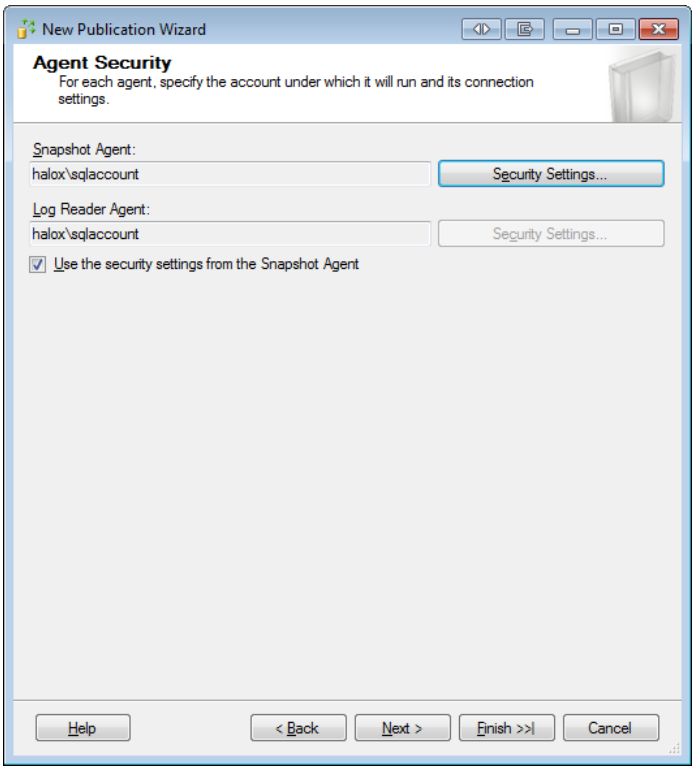


A new window appears as shown in the screenshot below.

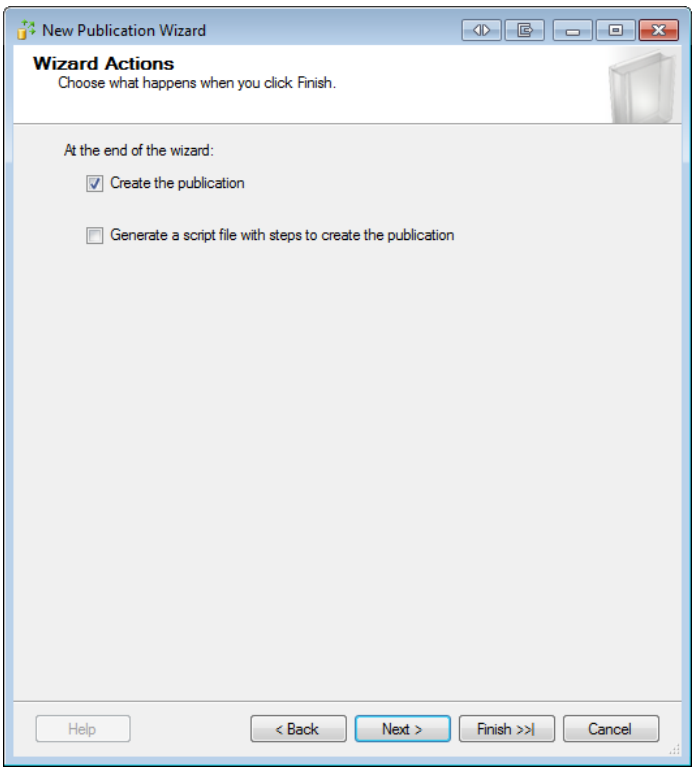


It is advised you use a Windows account for this purpose. Click on the OK button, then on the 'Next' button as per the screenshot below.

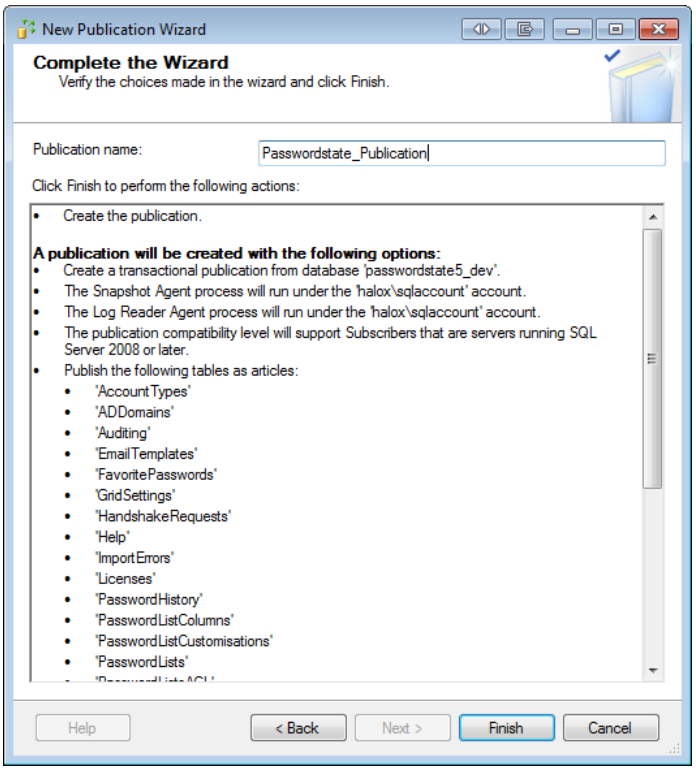
Please Note: If you specify a Windows account to use, at minimum it must be a member of the db_owner fixed database role in the 'Distribution' and both 'passwordstate' databases. It must also have write permissions on the snapshot share. You can tell if the permissions are correct by checking the folder where the snapshot data is stored to see if some replication data exists after you finish creating the Publisher.



9. Click on the 'Next' button as shown in the screenshot below.



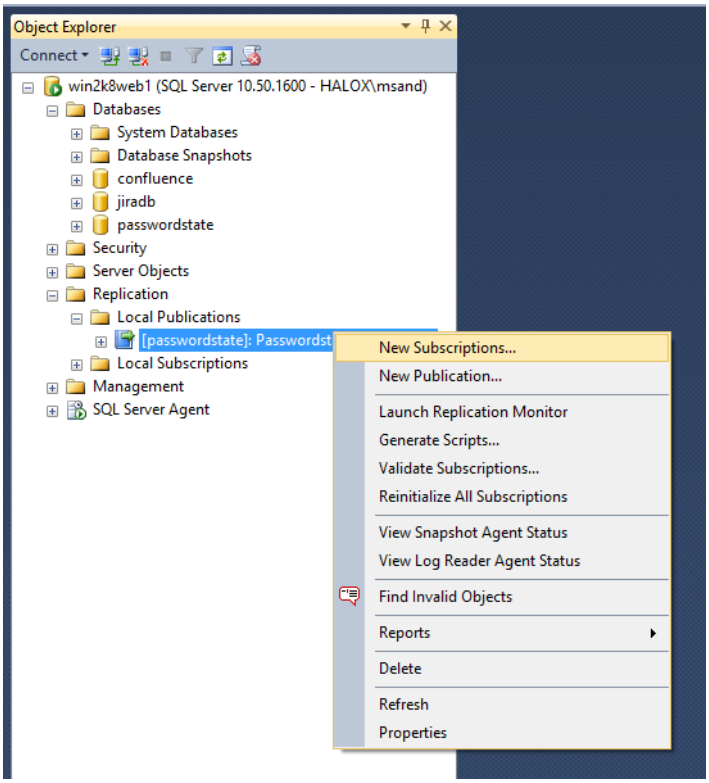
10. Give a suitable name to the publisher ad Click on the Finish button as shown in the screenshot below.



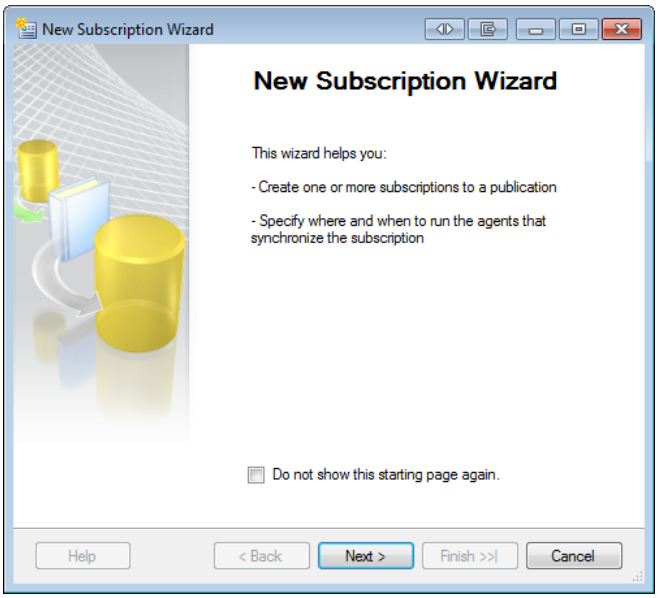
14 Creating the Subscriber

Once the publisher is created the next step is to create the subscriber for it.

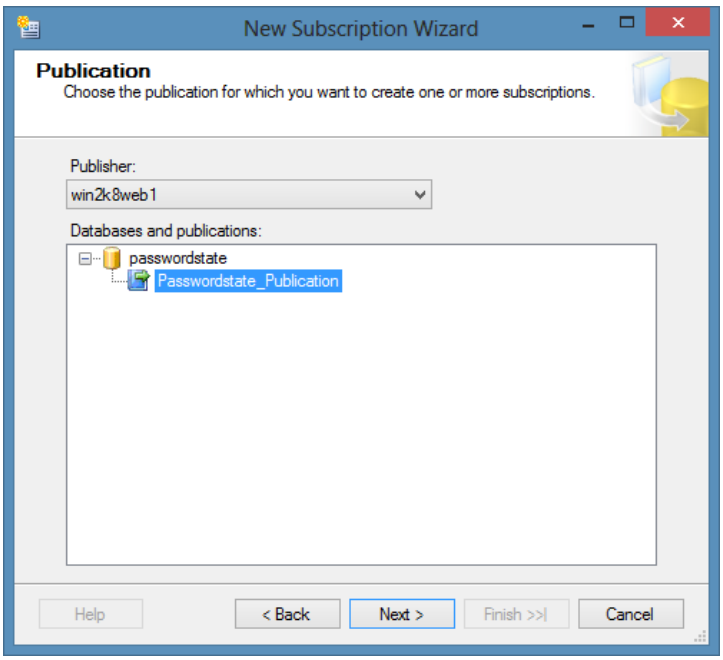
1. Right Click on the publisher created and select New Subscriptions as shown in the screenshot below.



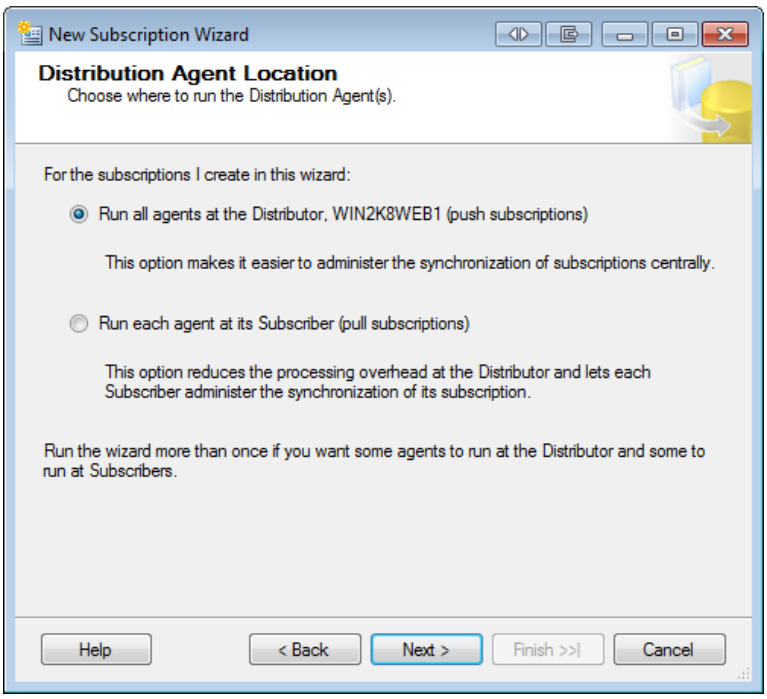
2. Click on the 'Next' button as shown in the screenshot below.



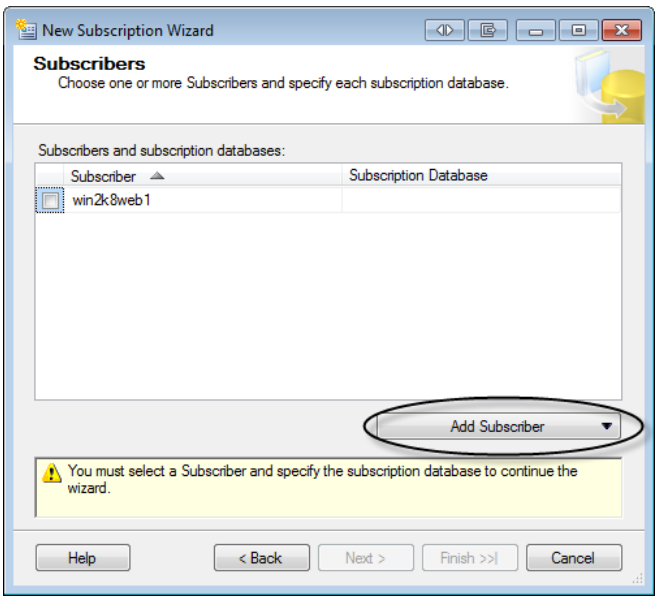
3. Click on the 'Next' button as shown in the screenshot below.



4. Click on the 'Next' button as shown in the screenshot below.

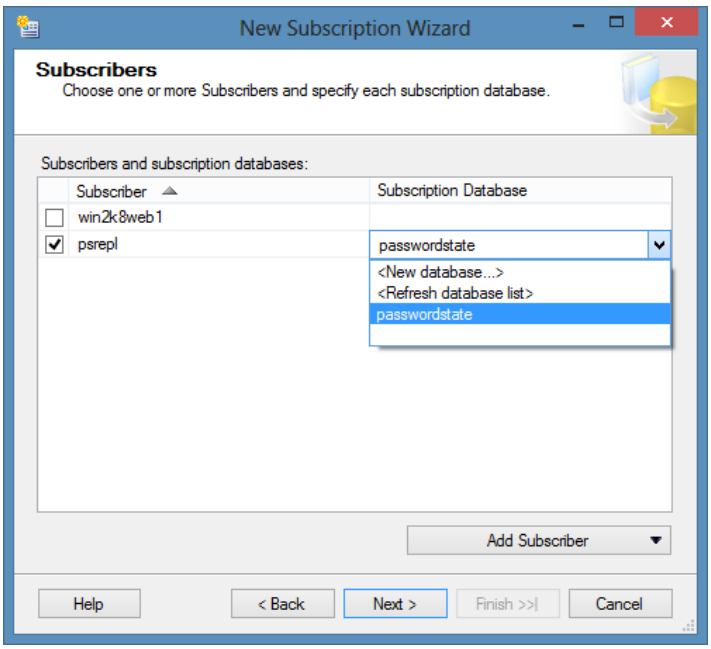


5. As shown in the screenshot below, you will need to click on the 'Add Subscriber' button to select the SQL Server you intend to use as the Subscriber.

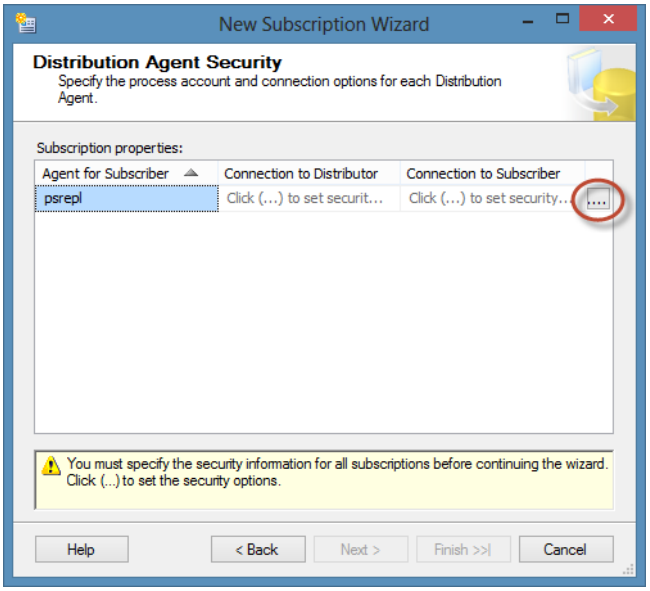


Type in the name of the Subscriber SQL Server, then click on the 'Connect' button

Select the '**passwordstate'** database from the dropdown list, and then click on the 'Next' button

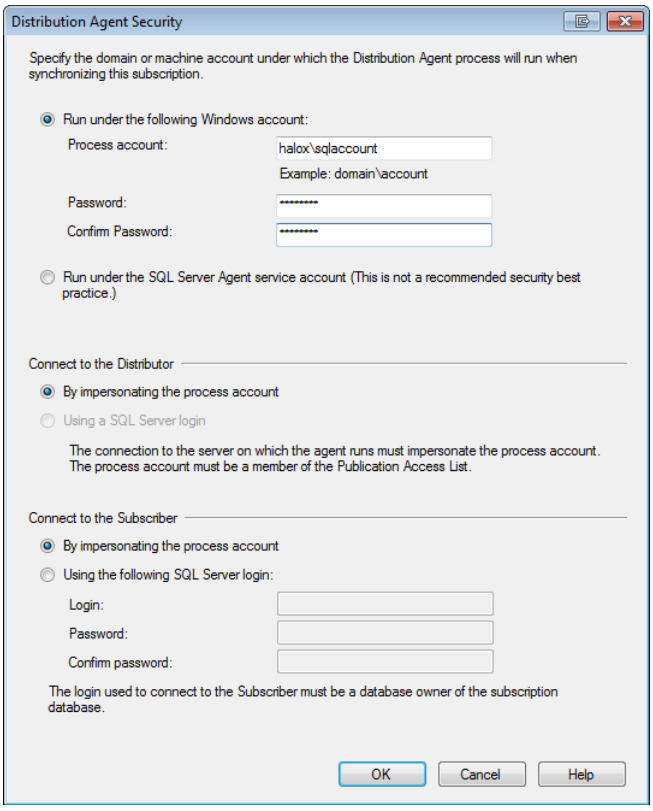


6. Click on the button as shown in the screenshot below. Here we need to specify process account as well as the connection options for the distribution agent.

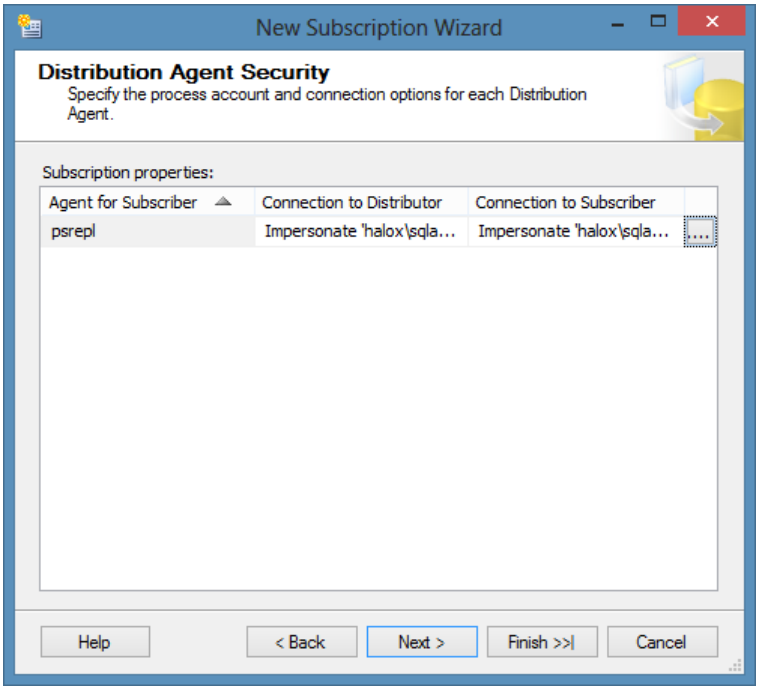


7. Specify the distribution agent to run under the security context of the same account you used for the Publisher - Please refer the screenshot below. Once done, click on the 'OK' button

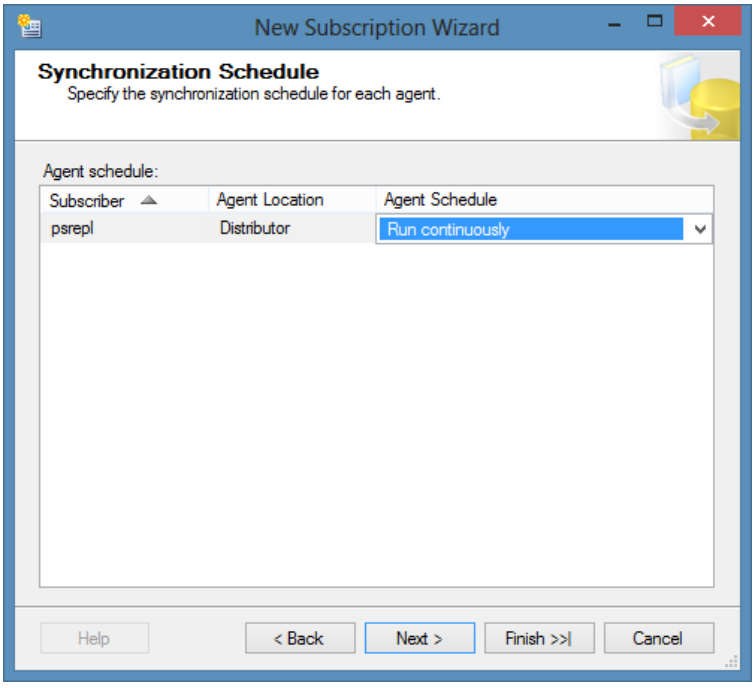
Please Note: If you specify a Windows Account to use, at minimum it must be a member of the db_owner fixed database role in the passwordstate database. It is advised you apply these permissions before click on the 'OK' button in the screenshot below.



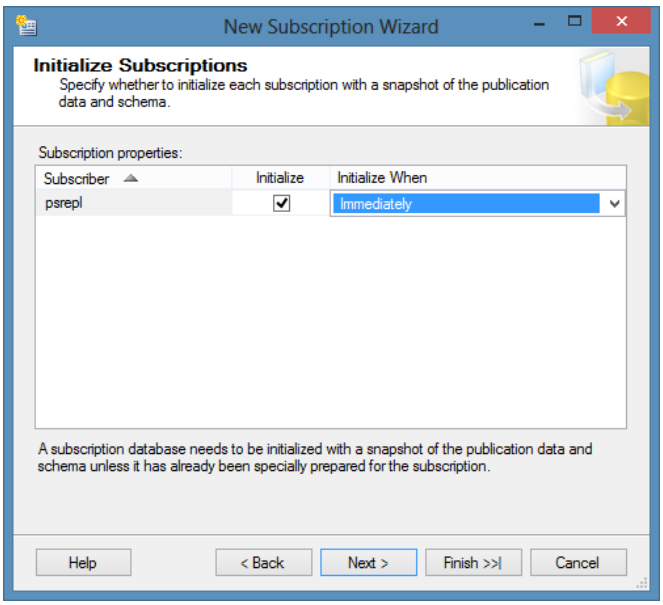
8. Click on the ‘Next’ button as shown in the screenshot below.



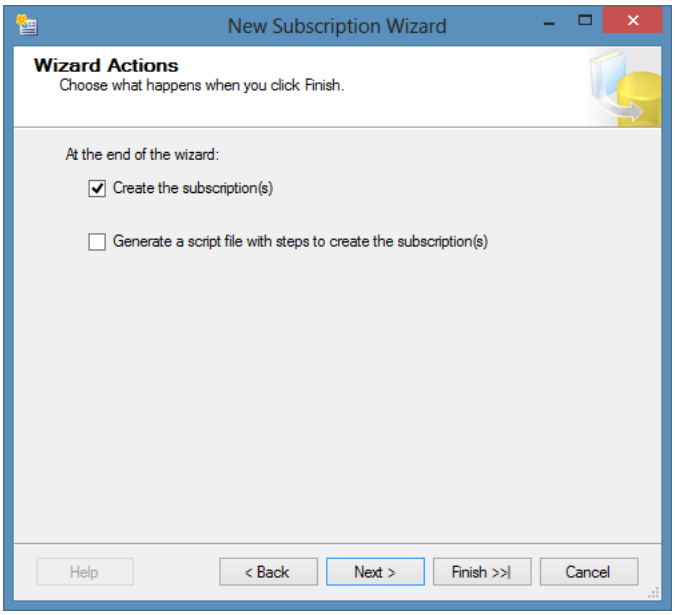
9. Ensure that the Agent is scheduled to Run Continuously and then click on the ‘Next’ button as shown in the screenshot below.



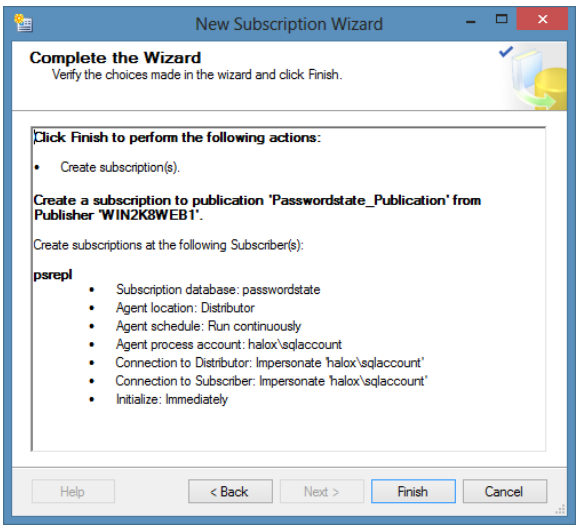
10. Ensure that the Subscriber is initialized immediately and then click on the ‘Next’ button as shown in the screenshot below.



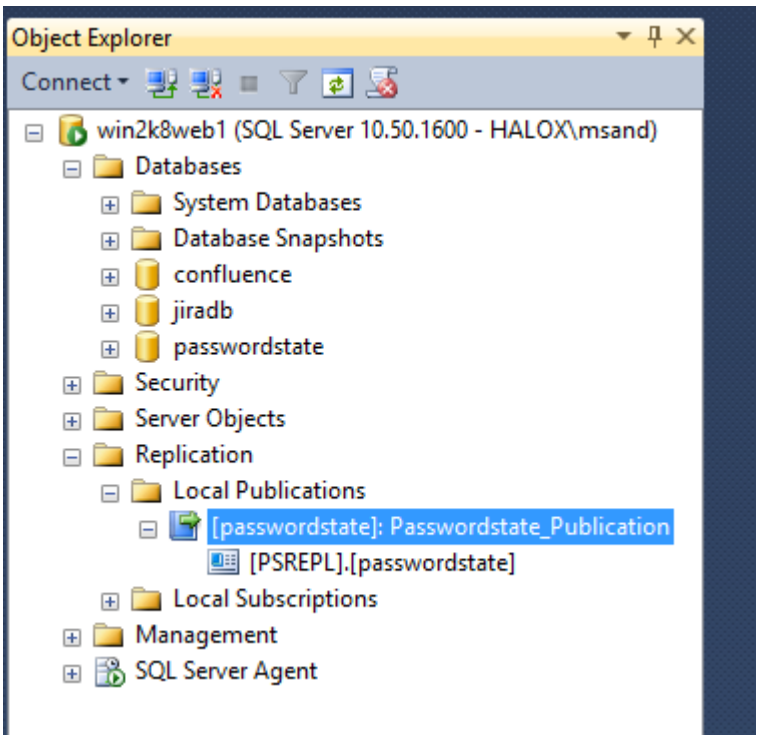
11. Click on the ‘Next’ button as shown in the screenshot below.



12. Click on the Finish button as shown in the screenshot below.



13. Expand the publisher node and you shall be able to view the subscriber as shown in the screenshot



You have now finished successfully setting up SQL Replication for your High Availability instance of Passwordstate.

You can now direct your browser the web address you created in 'Step 3 – Create an Appropriate DNS Record' above.