



# Click Studios

## Passwordstate

### Upgrade Instructions to V7 from V5.xx

# Table of Contents

1	UPGRADE OVERVIEW .....	3
2	SYSTEM REQUIREMENTS.....	4
3	PREPARING FOR THE UPGRADE.....	6
4	HIGH AVAILABILITY MODULE CONSIDERATIONS.....	7
5	UPGRADE INSTRUCTIONS .....	8
6	SSL CERTIFICATE CONSIDERATIONS.....	10
7	DECRYPTING AND ENCRYPTING THE DATABASE CONNECTION.....	12
8	ENCRYPTING THE APPSETTINGS SECTION WITHIN THE WEB.CONFIG FILE.....	13
9	TROUBLESHOOTING CONNECTIVITY ISSUES .....	14

## 1 Upgrade Overview

This document will detail instructions for upgrading to Passwordstate to version 7, from any version prior in the 5.xx range.

For upgrading from versions prior to 5.0, please visit the [Support](#) section of our web site for instructions, or contact Click Studios for support.

**Note:** Once you have upgraded to Version 7 of Passwordstate, all future upgrades will be a lot simpler due to the 'In-place Upgrades' feature available in Version 7.

## 2 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
- Windows 7 & IIS 7.5
- Windows 8 & IIS 8.0
- .Net Framework 4.5
- PowerShell 3.0 or above



### IMPORTANT

Passwordstate 7 uses Version 4.5 of the .NET Framework, so you must have this installed on your web server before you proceed any further with the upgrade.

As Version 4.5 of the .NET Framework is being used, there are additional Internet Information Services (IIS) roles required for Windows Server 2012 and Windows 8. If the following IIS roles are not installed, the Passwordstate Windows Installer will install them for you.

### Common HTTP Features

- Static Content
- Default Document
- HTTP Errors

### Application Development

- ASP.NET (or ASP.NET 4.5 on Server 2012 and Windows 8)
- .NET Extensibility (or .NET Extensibility 4.5 on Server 2012 and Windows 8)
- ISAPI Extensions
- ISAPI Filters

### Security

- Windows Authentication
- Request Filtering

### Performance

- Static Content Compression

**Database Server**

Your SQL Database which will host the Passwordstate database can be any of the following versions of SQL Server:

- 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

### 3 Preparing for the Upgrade

Please ensure the following steps are taken, prior to upgrading to Version 7 of Passwordstate

#### Step 1 – Database Changes

For the version 7 upgrade, the upgrade provides a SQL script for you to run which will rename the Passwordstate5 database to Passwordstate, and the passwordstate5\_user SQL Account to passwordstate\_user. Please ensure you take a full backup of your database prior to performing the new install.

The database script is installed with the web site when you install Passwordstate, but if your DBA's wish to have a look at the file prior to starting any upgrades, they can download the file from

[http://www.clickstudios.com.au/downloads/v7\\_database\\_naming\\_changes.zip](http://www.clickstudios.com.au/downloads/v7_database_naming_changes.zip)

#### Step 2 – Capture Web.config File Settings

There are certain settings in the web.config file (located in the root of the Passwordstate folder) which are required for the upgrade. Please open the web.config file, and take a copy of the following lines and save them to a text file somewhere:

```
<connectionStrings>
  <add name="PasswordstateConnectionString" connectionString="Data
  Source=localhost;Initial Catalog=passwordstate5;Persist Security Info=True;User
  ID=passwordstate5_user;Password=Hyhf%67g55" providerName="System.Data.SqlClient" />
</connectionStrings>
<appSettings>
  <add key="SetupStage" value="Setup Complete" />
  <add key="PassiveNode" value="False" />
  <add key="GUID1" value="0a9fb8ea-b14e-4719-82f3-3c8e6e0f28e9" />
</appSettings>
```

If the database connection string does not appear to be in the format above, it's possible that at some stage someone has encrypted the database connection string. If this is the case, please reference the section '**Decrypting and Encrypting the Database Connection String**' below to first decrypt the connection string before you proceed.

**Note:** The GUID1 string may not exist if you are using an older build of Passwordstate.

## 4 High Availability Module Considerations

If you don't use the High Availability module of Passwordstate, **you can skip to the section 5 Upgrade Instructions.**

The intention of the following instructions is to allow you to continue using the High Availability instance of Passwordstate while you upgrade the Primary Instance. You can continue to use your High Availability install until you get to Step 3 below. At this time, your Primary instance has been upgraded and your users can access this version if required.

1. Delete the SQL Server Subscriber and Publisher you established as part of the document 'High\_Availability\_Installation\_Instructions.pdf'. This needs to be done as it's not possible to make database schema changes while replication is occurring, plus we will also be renaming the database as well
2. Continue with Steps 5 onwards in this document to upgrade the **Primary Instance** of Passwordstate. Once the Primary Instance has successfully been upgrade, continue to the next step below 3 to upgrade the High Availability Instance – it's also not really an upgrade, instead we are completely uninstalling the web site at the HA end and deleting the HA database, and then following the original HA installation instructions
3. Now that the Primary Instance of Passwordstate has been upgraded, we can continue upgrading the High Availability Instance. To do this, uninstall the High Availability instance of Passwordstate from the Control Panel.
  -  Note: Please ensure the following items have been removed – if not, remove them manually:
    - a. Passwordstate5 folder
    - b. Passwordstate web site in Internet Information Services (IIS)
    - c. The Passwordstate Application Pool in IIS
4. On your secondary SQL Server (the subscriber), delete the 'passwordstate5' database and 'passwordstate5\_user' SQL Account
5. Follow the instructions in 'High\_Availability\_Installation\_Instructions.pdf' for reinstalling the High Availability instance of Passwordstate, and re-establishing SQL Server data replication. The following items in the HA installation instructions won't need to be done again, as they were configured previously when you first established replication when using version 5:
  - a. 9 – Authorised Web Server Considerations
  - b. 12 - Configuring the Distribution Database

**Build 7580 Note:** If you are upgrading from a build which is earlier than Build 7580, then it is very important to copy the Secret1 & Secret2 keys across from your primary instance of Passwordstate, otherwise the HA instance will not work. These keys are located in the web.config file, in the appSettings section.

## 5 Upgrade Instructions

To upgrade to the latest version of Passwordstate please follow these instructions:

2. Download the latest copy of Passwordstate from here – <http://www.clickstudios.com.au/downloads/passwordstate.zip>
3. Uninstall Passwordstate from Control Panel (please note your database will not be touched during the uninstall).
  - 🚩 Note: Please ensure the following items have been removed – if not, remove them manually:
    - a. Passwordstate5 folder
    - b. Passwordstate web site in Internet Information Services (IIS)
    - c. The Passwordstate Application Pool in IIS
4. Once uninstalled, reinstall Passwordstate with the latest version you just downloaded, **but do not open** your browser and run through the initial setup again
5. Using the SQL Server Management Studio tool, open and execute the script (this script will rename the database as well as the SQL Account used to connect to the database – you will also need admin rights to SQL Server to execute this script):  
c:\inetpub\passwordstate\upgrades\scripts\v6\_database\_naming\_changes.sql
6. Replace the lines in the web.config taken above in the section ‘Step 2 – Capture Web.config File Settings’, and rename the following – save the file when done:
  - a. `Initial Catalog=passwordstate5` to `Initial Catalog=Passwordstate`
  - b. `User ID=passwordstate5_user` to `User ID=passwordstate_user`
7. If you have modified the standard ‘passwordstate’ cname DNS entry for the web site, or configured the web site to use a SSL certificate, you will need to redo these steps
8. When you first browse to the Passwordstate web site you will see the following screen. As per the instructions on the screen, click on the ‘Start Upgrade’ button

### Step 2 - Upgrade the Database

To upgrade to the latest version of Passwordstate, please click on the '**Start Upgrade**' button at the bottom of the page.

Current Build: **Version 6.3 (Build 6350)**    New Build: **Version 7.0 (Build 7000)**

step 2 - upgrade the database

Progress of the upgrade will be logged below, as well as in the file /upgrades/upgradelog.txt.

**Upgrade Progress**

Status: Start Upgrade

9. Your browser will automatically redirect you after the upgrade is complete. If you experience any issues with the upgrade, please refer to the log `c:\inetpub\passwordstate\upgrades\UpgradeLog.txt`
10. **Restart the Passwordstate Windows Service** – this is required to pick up the renaming changes in the `web.config` file, and so that any custom images or logos are taken from the database and written to disk

## 6 SSL Certificate Considerations

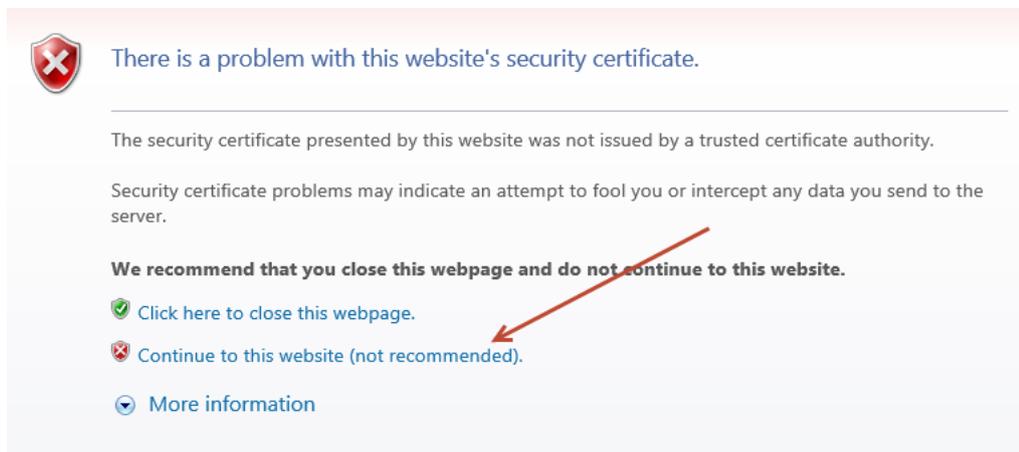
The installer for Version 7 of Passwordstate installs a self-signed SSL certificate on your web server, and binds it to the Passwordstate web site.

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:

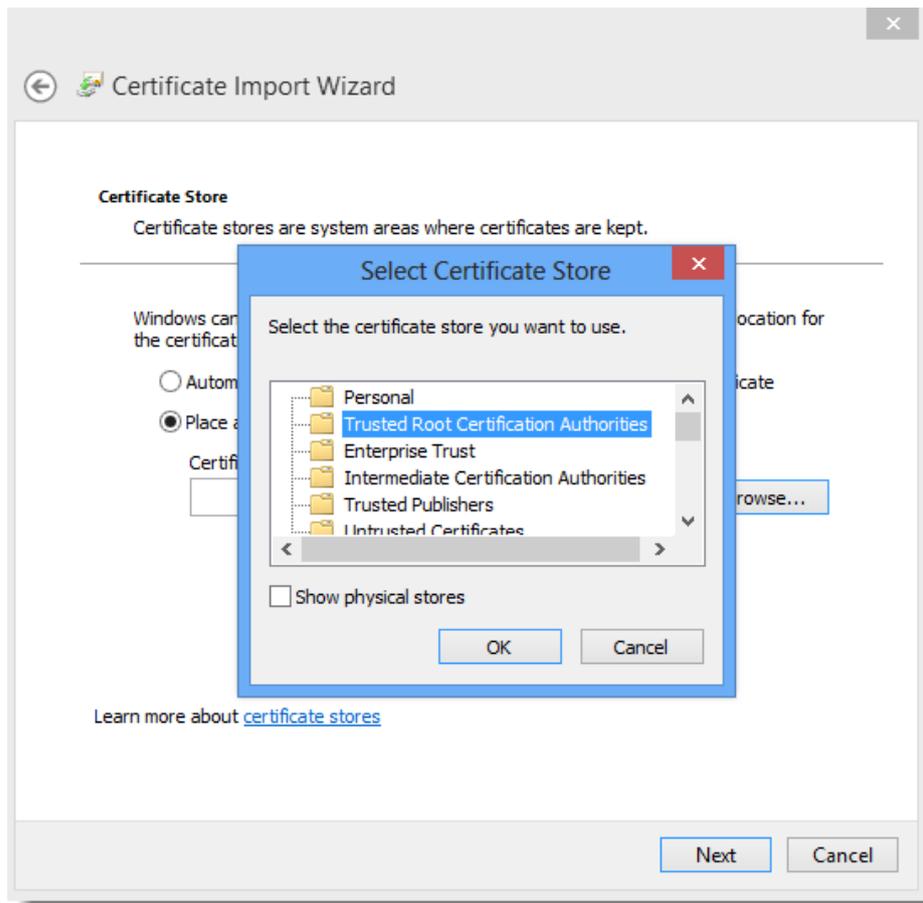
1. Using Internet Explorer, browser to the Passwordstate web site
2. When you see the following screen, click on the 'Continue to this website' link



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

## 7 Decrypting and Encrypting the Database Connection

The following instructions show you how to decrypt the database connection string in the web.config file for your Version 5 install, and then how to re-encrypt for your new Version 7 install.

It's not entirely necessary to encrypt your database connection string, as all sensitive data is encrypted in the database already, but doing so will 'mask' the credentials used to connect to the database

### Decrypt Version 5 Database Connection String

- 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\passwordstate5"` (change the path if you've installed Passwordstate to a different location)
  -

### Encrypt Version 7 Database Connection String

- 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)

## 8 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.

## 9 Troubleshooting Connectivity Issues

If when you first try and browse to the Passwordstate web site you get a blank page, or an error saying '**The page cannot be displayed because an internal server error has occurred.**', this may be caused by the order in which you installed Internet Information Services and the .Net Framework 4.5 – if you install the .NET Framework first, this error will occur.

Note: These instructions only apply to Microsoft Windows Server 2008, Server 2008 R2 and Windows 7

To resolve this, follow these instructions:

- Open an Command Prompt as an Administrator
- Type **CD C:\Windows\Microsoft.NET\Framework\v4.0.30319** or **C:\Windows\Microsoft.NET\Framework64\v4.0.30319** depending on our operating system version
- Now type **aspnet\_regiis -i**
- After ASP.NET has been re-registered, ensure the Passwordstate Application Pool in IIS is set to 'Integrated Managed Pipeline Mode', and then restart IIS (you need to open the Internet Information Services (IIS) Manager tool to do this
- Now open your browser and point it back to the Passwordstate web site

You may need to do this for both the 32bit and 64bit versions on the Framework directories above if you still experience issues.

 Note: If the above doesn't resolve the issue, and you receive at Server 500 error, then this can be caused by you copying across the entire web.config file from version 5, instead of just the lines we specify above in the section 'Capture Web.config File Settings'.