Click Studios

Passwordstate

Mobile Client

Installation Instructions

Table of Contents

1 Overview

The Passwordstate Mobile Client web site allows mobile client access to all the Password Lists you have been given access to within your existing Passwordstate installation.

Note: These instructions only need to be followed if you want to install the Mobile Client web site on a different server other than your existing Passwordstate web server i.e. a server in your DMZ, or a separate "hardened" server. This would be required, and is also recommended, if you have concerns about exposing access to your existing Passwordstate web server via the Internet. To access the Mobile Client web site via your existing Passwordstate web server, you can do so via the URL: https://<myurl>/mobile

2 System Requirements - General

Passwordstate Mobile Client web site has the following system requirements:

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

- 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
- Windows 10 & IIS 10.0

Note: Microsoft **.Net Framework 4.5 and PowerShell 4.0 or above** must also be installed on your web server.

3 Internet Information Services (IIS) Requirements

When installing Internet Information Services, the following component/roles are required as a minimum. If these IIS roles are not installed, Passwordstate 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

- Request Filtering

Performance

- Static Content Compression

4 Installing Passwordstate Mobile Client Web Site

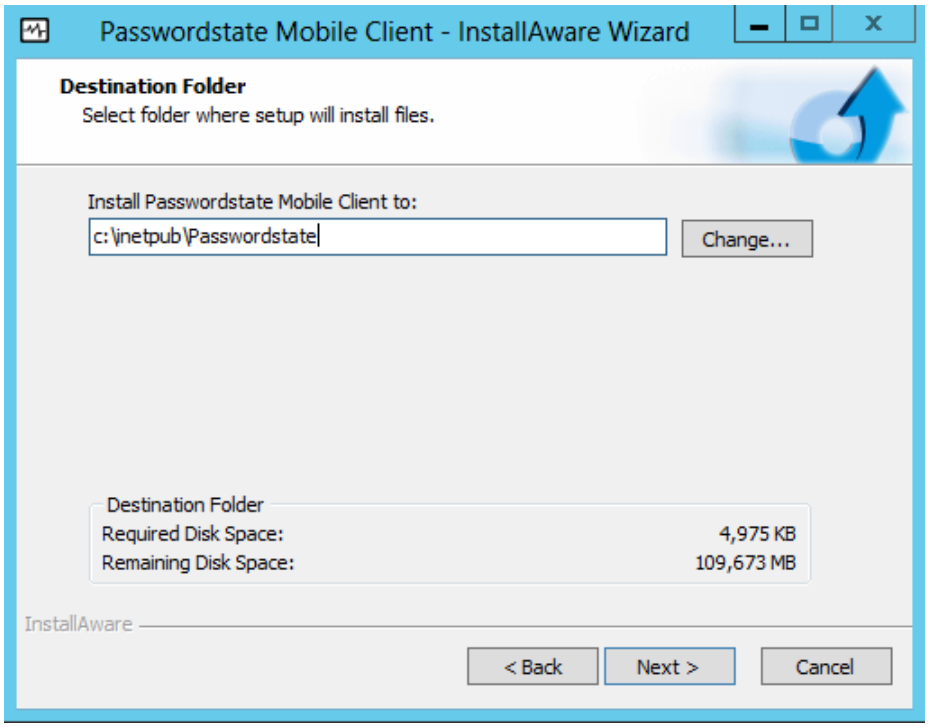
To install Passwordstate, run 'PasswordstateMobile.exe' and follow these instructions:

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

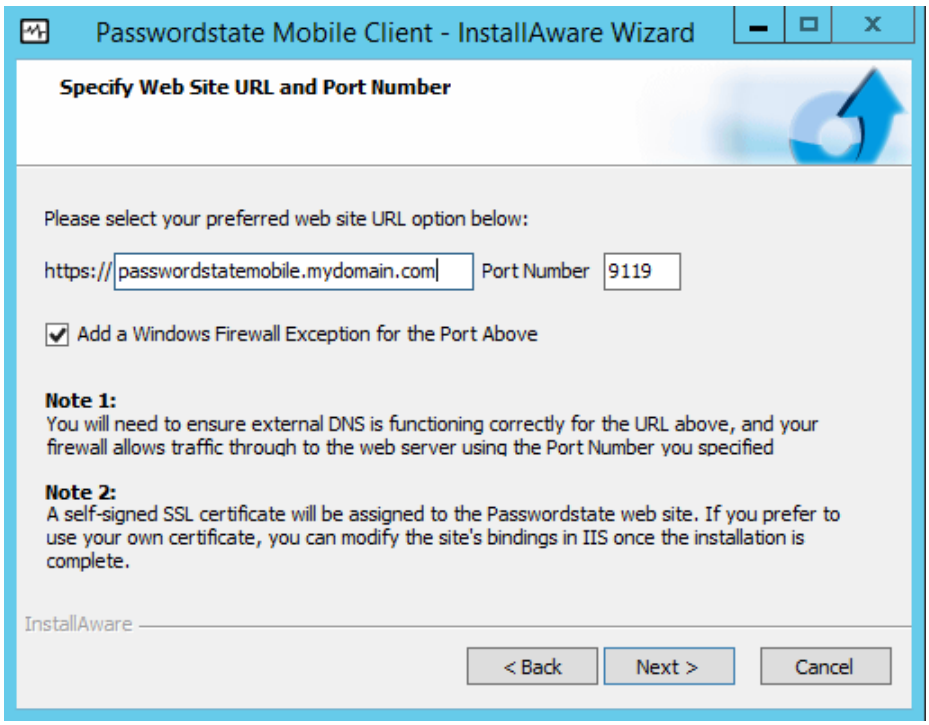
2. At the 'License Agreement' screen, tick the option 'I accept the terms in the License Agreement', then click on the 'Next' button

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. Note: The URL you use here must have external name resolution working in order to access the web site from outside of your own internal network



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

6. Once installed, click on the 'Finish' button
7. **You now need to register the host name of the web server you have installed the Mobile Client web site as an 'Authorized Web Server'** in your main Passwordstate web site. You can do this via the page Administration -> Authorized Web Servers
8. Now copy the following 4 keys from the web.config file from your main Passwordstate web site folder, to the web.config file in this Mobile Client folder:

   <add name="PasswordstateConnectionString"…… />
   <add key="GUID1" …… />
   <add key="Secret1" value="2d1-1….." />
   <add key="Secret2" value="3h6-5….." />

9. Restart the Passwordstate Windows Service
10. If you intent to use the SafeNet Two-Factor Authentication option with the Mobile Client, you will need to follow the document 'SafeNet Two-Factor Configuration.pdf' to install the pre-requisites for this.

- Note 1: During this install the site is configured with a self-signed SSL certificate. It is recommended, if possible, to purchase an SSL certificate from an appropriate reseller, or use one of your own existing certificates. If you don't do this, the user will be prompted with a screen complaining about the authenticity of the certificate, which would not be an ideal/suitable user experience.
- Note 2: Your System/Firewall administrators will need to ensure external DNS is functioning correctly for the URL you specified during the install, and the firewall allows traffic through to the web server using the Port Number you specified
- Note 3: In additional to your externally facing Firewall, if you also 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). This depends on whether or not you selected the option to allow the Passwordstate installer to open the Windows Firewall exception.

5 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 change to the folder C:\Windows\Microsoft.NET\<Framework or 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 change to the folder C:\Windows\Microsoft.NET\<Framework or 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: If you intend to rename your server host name, you should decrypt these settings first, rename the server, then encrypt again.

6 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.