



Passwordstate Remote Session Launcher Gateway Automated Installation Instructions

This document and the information controlled therein is the property of Click Studios. It must not be reproduced in whole/part, or otherwise disclosed, without prior consent in writing from Click Studios.

Table of Contents

1.	SYSTEM REQUIREMENTS - GENERAL	3
2.	ARCHITECTURAL OVERVIEW.....	4
3.	CHANGES MADE TO YOUR SERVER DURING THIS AUTOMATED INSTALL.....	5
4.	INSTALLING GATEWAY ON PASSWORDSTATE WEB SERVER.....	6
5.	INSTALLING GATEWAY ON A SEPARATE SERVER	7
6.	EXPORTING CERTIFICATE FROM PASSWORDSTATE SERVER.....	8
7.	CONFIGURE GATEWAY SETTINGS	12
8.	SESSION RECORDING SETTINGS & PERMISSIONS	13
9.	TROUBLESHOOTING A FAILED INSTALL	15

1. System Requirements - General

Passwordstate's Browser Based Remote Session Launcher Gateway has the following system requirements:

Windows Server Requirements

The server which will host the Gateway can be any one of the following Operating System versions, with required components:

- Microsoft Windows Server 2012 & IIS 8.0
- Microsoft Windows Server 2012 R2 & IIS 8.5
- Microsoft Windows Server 2016 & IIS 10.0
- Microsoft Windows Server 2019 & IIS 10.0
- Windows 8 & IIS 8.0
- Windows 10 & IIS 10.0
- OpenJDK 15 or higher (will be installed automatically as part of this process)
- The server must have internet access, otherwise you'll be required to manually download Java source files

2. Architectural Overview

When you install Passwordstate, the source files for the “Browser Based Gateway” are already pre-loaded in your Passwordstate install directory. By default, this is c:\inetpub\passwordstate\hosts\gateway.

There are extra steps you need to perform to finalise the setup of the gateway, which are documented in **Section 4** of this guide.

Alternatively, you can install the gateway on a completely separate server if preferred. Installing it on a separate server is required if you are using the High Availability module of Passwordstate, or maybe you just want to have the gateway installed on a separate server to your Passwordstate server.

After you have completed the setup, all SSH and RDP sessions are tunnelled through the Gateway, and there is no requirement to install any other clients on your network for this feature to function. You will be able to initiate RDP and SSH sessions through your HTML5 browser, from any device that can access your main Passwordstate website.

For a comprehensive user manual on how to use the Remote Session Launcher, look in Passwordstate under the **Help Menu -> Remote Session Management**.

3. Changes Made to your Server During this Automated Install

This guide will instruct you to download one of two PowerShell scripts, and execute it either on your Passwordstate webserver, or on a separate server of your choice. The scripts differ slightly depending on where you are intending on setting up the Gateway.

This script will perform the following tasks:

- If installing on a separate server, it will install the gateway source to **C:\Program Files (x86)\Passwordstate Remote Session Gateway**
- Creates a log file in the same directory where you execute the PowerShell script from
- Can download OpenJDK 15 from <https://cdn.azul.com/zulu/bin/> and extracts this file to **C:\Program Files (x86)**. This download is approximately 200mb in size
- Adds a value of **C:\Program Files (x86)\OpenJDK\bin** to the “**PATH**” System Environment Variable. Also adds in a new Environment Variable called **JAVA_HOME** with the value of **C:\Program Files (x86)\OpenJDK**. If these already exist, they will be removed before adding them back in
- If running this installer on your Passwordstate webserver, it will automatically export your certificate from your https binding in IIS. If installing separately, you must provide this certificate yourself
- Installs a Windows Service called **Passwordstate-Gateway**
- Removes all temporary source files that were created during this process

Please follow either **Section 4** of this document to install the gateway on your Passwordstate web server, or **Section 5** to install it on a separate server.

4. Installing Gateway on Passwordstate Web Server

Steps to execute the automatic installer on your Passwordstate web server

1. To ensure you always have the latest source files, download the installer from <https://www.clickstudios.com.au/downloads/Install-Gateway-Internal.zip> and place it in a temporary folder on your Passwordstate web server
2. Extract the zip file to the same folder, revealing a **7za.exe** and an **Install-Gateway-Internal.ps1** file
3. Open PowerShell ISE “**As Administrator**”, and then open the **Install-Gateway-Internal.ps1** script
4. Press **F5** to run the script, or use the button in PowerShell to run the script

A log file will be created and placed in the directory where you executed the PowerShell script from and can be used to troubleshoot any issues.

There will also be an output in the PowerShell console advising what step the installer is up to. Once the script has finished, the Gateway is ready to be used and this video is a quick tutorial on how to do this: https://www.youtube.com/watch?v=E_PHLAfQe7c

Note 1: If you receive an error during the install stating:

“It appears the certificate on your Passwordstate website may not be marked for export and could not be exported automatically”

You will need to export your certificate manually, or provide another certificate that you can export to a password protected .pfx file. See **Section 6** in this document on how to export certificates manually.

If you have to export your certificate manually, you’ll need to place it in the same folder where you are executing this PowerShell installer from. During the installation process, you’ll be prompted for a password which is the one you set during the exporting of the certificate.

When exporting the certificate, it must be called “**Passwordstate.pfx**”.

Note 2: If you receive an error during the install stating:

“Combination test failed. It appears your server does not have access to the internet, and the install source files were not supplied”

You will need to manually download the Java source files on another computer, and place them in the same directory where you are running the **Install-Gateway-Internal.ps1** script from.

The source files can be downloaded from https://cdn.azul.com/zulu/bin/zulu15.29.15-ca-jdk15.0.2-win_x64.zip

5. Installing Gateway on A Separate Server

Steps to execute the automatic installer on a standalone server:

1. To ensure you always have the latest source files, download the installer from <https://www.clickstudios.com.au/downloads/Install-Gateway-External.zip> and place it in a temporary folder on your server
2. Extract the zip file to the same folder, revealing a **7za.exe**, **PasswordstateGatewayInstaller.exe** and an **Install-Gateway-External.ps1** file
3. Export a copy of your certificate from your Passwordstate web server by following the instructions in **Section 6** of this document. Place this exported certificate in the same folder that you are extracted the zip file to, in the above step
4. Open PowerShell ISE "**As Administrator**", and then open the **Install-Gateway-External.ps1** script
5. On line **28**, enter your **URL** for your Passwordstate website. I.e. <https://passwordstate.contoso.com>
6. On line **29**, enter the **password** you set for certificate (see Section 6 below)
7. Press **F5** to run the script, or use the button in PowerShell to run the script
8. In Passwordstate, navigate to **Administration -> Remote Session Management -> Browser Based Gateway Settings**, and enter in your Gateway URL. By default, a URL is set up using the DNS name of the server. An example of this is if you install the gateway on a server called "**AppServer01**" that belongs to the "**Contoso.com**" domain, then the URL created for you is <https://appserver01.contoso.com>.

If you have manually created a functioning DNS record to use for your Gateway, then use that URL on this screen instead.

A log file will be created and placed in the directory where you executed the PowerShell script from and can be used to troubleshoot any issues.

There will also be an output in the PowerShell console advising what step the installer is up to. Once the script has finished, the Gateway is ready to be used and this video is a quick tutorial on how to do this: https://www.youtube.com/watch?v=E_PHLAfQe7c

Note 1: If you receive an error during the install stating:

"Combination test failed. It appears your server does not have access to the internet, and the install source files were not supplied"

You will need to manually download the Java source files on another computer, and place them in the same directory where you are running the **Install-Gateway-External.ps1** script from.

The source files can be downloaded from https://cdn.azul.com/zulu/bin/zulu15.29.15-ca-jdk15.0.2-win_x64.zip

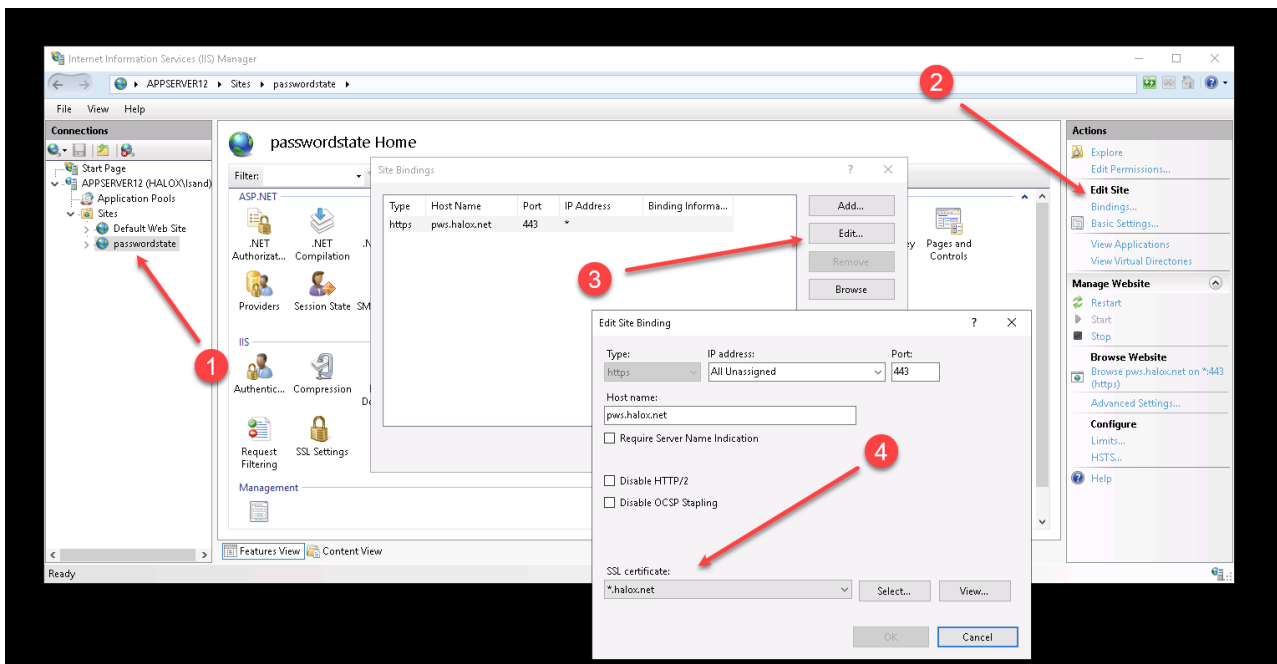
6. Exporting Certificate from Passwordstate Server

You only need to follow this process if you are installing the Gateway on a separate server to your Passwordstate web server, or if the **Install-Gateway-Internal.ps1** installer script cannot automatically export your certificate.

Method #1 to export certificate:

1. On your Passwordstate web server, open **IIS** and Select your server in the left-hand side connections pane
2. Double click **Server Certificates** button
3. Find the certificate you are using on your Passwordstate website, right click it and select **“Export”**
4. Choose a path to store the certificate, and make sure the file is saved as **“Passwordstate.pfx”**
5. Set a password for the certificate, confirm the password and then click **OK**

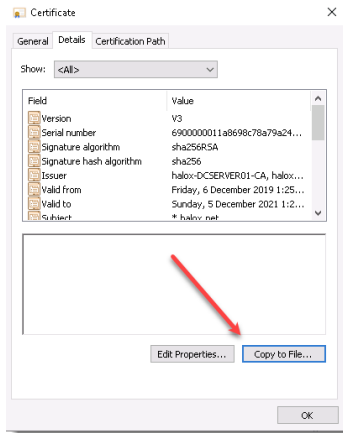
Note 1: If you have multiple certificates on the machine, but you do not know which one is being used on your Passwordstate website, open the https binding of your Passwordstate website in IIS:



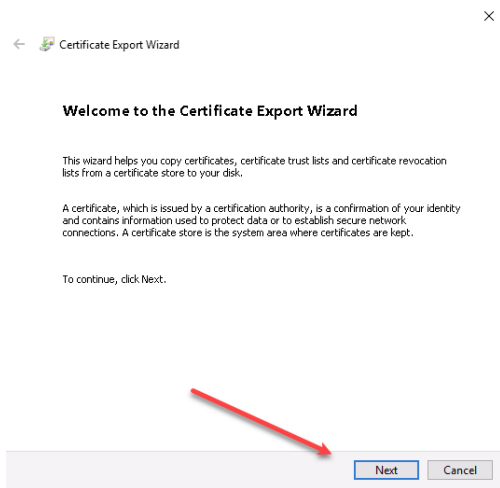
Note 2: If you do not see the **Export** option on the right click menu, this means your certificate is not marked for exporting. Try using **Method #2** below as an alternative way to export your certificate, otherwise you'll need to source a certificate that can be exported.

Method #2 to export certificate:

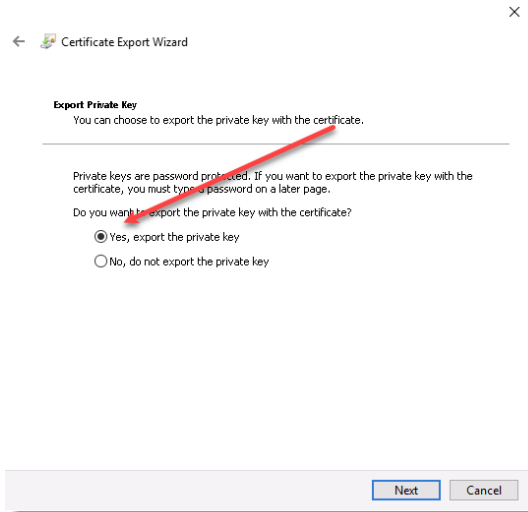
1. On your Passwordstate web server, go to **Start -> Run** and type in **certlm.msc** and hit **enter**
2. Browse to **Personal -> Certificates**, and double click your Passwordstate certificate. The certificate may also reside under **Trusted Root Certification Authorities -> Certificates**
3. Under the Detail tab, click **“Copy to File”**



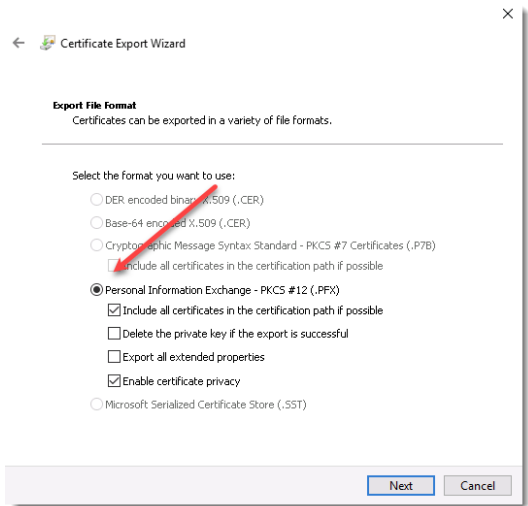
4. Click Next



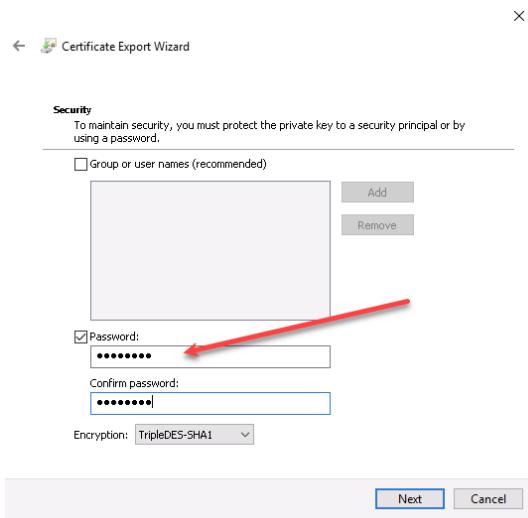
5. Click **Yes** to export the Private key:



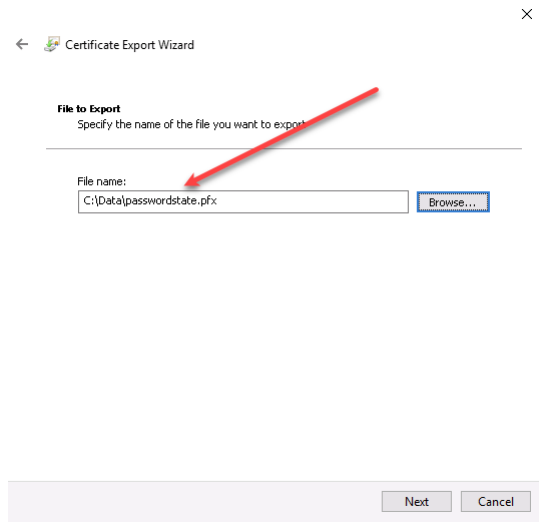
6. Select **Personal Information Exchange**



7. Set a Password and click **Next**



8. Ensure you name the certificate **Passwordstate.pfx**



9. Click **Finish**

If you cannot export your certificate, then you will need to go to your certificate source and mark the certificate as exportable. You can then try to export again using one of the methods above.

If you would like to set up an Internal Certificate Authority, and generate a new wildcard certificate from there that can be exported to a .pfx file, please see these links below:

Set up Certificate Authority: <https://www.clickstudios.com.au/community/index.php?/topic/2934-how-to-set-up-a-internal-certificate-authority/>

Request a certificate that is marked as "Exportable":
<https://www.clickstudios.com.au/community/index.php?/topic/1952-generate-a-new-certificate-from-active-directory-certificate-authority/>

7. Configure Gateway Settings

In Passwordstate you may need to configure some Gateway settings

- Gateway URL (only if you have installed the Gateway separately, otherwise leave this empty)
- Port Number the Gateway listens/operates on
- If you want to purge any recorded sessions after (x) number of days
- Where you would like to store recorded sessions - please see **Section 8** for more information on this

To make these changes, navigate to the following page in **Passwordstate** → **Administration** -> **Passwordstate Administration** -> **Remote Session Management**, and click on the '**Browser Based Gateway Settings**' button, and you will see the screen below.

gateway settings

Configure Remote Session Gateway

Please make changes to the Gateway Settings below as appropriate.

Please specify settings for the Remote Session Gateway as appropriate.

Gateway URL:

If you have deployed the Gateway outside of your Passwordstate server, you need to specify the URL here so the gateway can be used. Specify in the format of https://fqdn.com

Specify the Port the Gateway will listen on:

Specify the Folder where all recorded sessions will be stored:

The path to save Session Recordings can be specified in one of three ways:

- rec -> to save recordings in the default folder of 'c:\inetpub\passwordstate\hosts\gateway\rec'
- d:\recordings\passwordstate -> to save recordings to a different disk on your Passwordstate web server
- //<servername>/<sharename> -> to save recordings to a network share

If changing the port number, or path for recorded sessions, please refer to the following document for more information, as changes to the gateway configuration files are need as well - [Browser Based Remote Session Gateway Installation Instructions](#).

Note : If you are using an active/active High Availability setup for Passwordstate, it is recommended you store recorded sessions on a network share, so they are accessible from both instances of Passwordstate. Or alternatively, install the Gateway separately from your Passwordstate install.

Purge Recorded Sessions older than the following number of days: (leave 0 to disable purging)

If recording sessions to a network share, please select a domain account below to delete sessions from the share, as required:

Account * : \\Infrastructure\Active Directory Accounts ->

Cancel Save

Note 1: Changing the **Port Number** or **Session Recording** folder need to be done manually in the gateway.conf file, and then you need to restart the **Passwordstate-Gateway** Windows Service.

Note 2: Please make sure no firewalls are blocking access to the Port Number above - either Firewalls on the Windows Server itself, or firewalls in Microsoft Azure or Amazon AWS - if you are hosting Passwordstate in the cloud.

8. Session Recording Settings & Permissions

Session Recording Settings

Session recordings can be saved in one of three locations:

- The default path is `c:\inetpub\passwordstate\hosts\gateway\rec` (your path may be different if you've installed Passwordstate into a different folder, or deployed the Gateway separately)
- Or you can save to a different folder or disk on your Passwordstate web server
- Or you can save to a network share.

If you are using the High Availability module for Passwordstate, it is recommended you save recorded sessions to a Share, so both instances of Passwordstate have access to replay the session recordings.

When changing the path to where you wish to save session recordings, this needs to be done in two locations:

1. On the screen Administration -> Remote Session Management -> Configure Remote Session Gateway
2. In the file `C:\inetpub\Passwordstate\hosts\gateway\gateway.conf`

The different formats that can be used are:

1. `rec` -> to save recordings in the default folder of '`c:\inetpub\passwordstate\hosts\gateway\rec`'
2. `d:\recordings\passwordstate` -> to save recordings to a different disk on your Passwordstate web server
3. `//<servername>/<sharename>` -> to save recordings to a network share

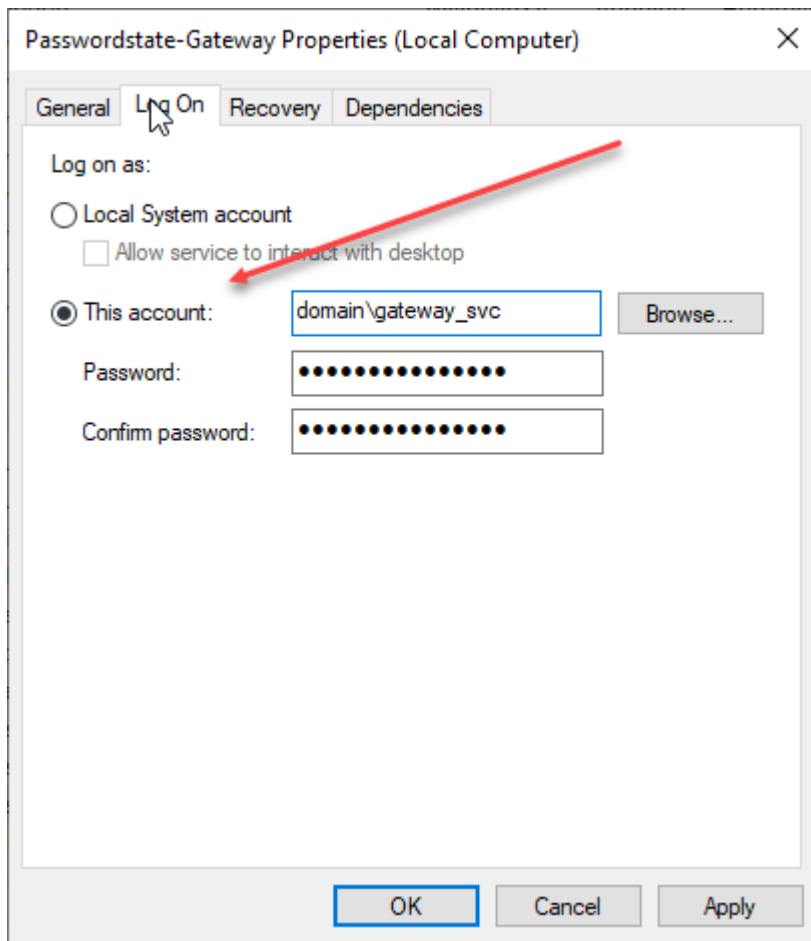
When changing these settings, you need to restart the Passwordstate-Gateway Windows Service.

Session Recording Permissions

When storing session recordings as per format 1 above, the NTFS permissions are already correct.

If, however you specify a different location e.g. a different disk than the C drive is recommended, or Network Share, then you need to ensure at least 'Authenticated Users' has Modify rights to the folder.

When using a Network Share, you must also modify the 'Log On' rights for the Passwordstate-Gateway Windows Service, so the service has correct access to write to the share – screenshot below for this.



Note: Session Recordings will not be included in the standard Passwordstate backup functionality, due to the potential size of the files. If you have left the recording folder in the default path, then you need to organize your own backups of these files if required.

9. Troubleshooting a Failed Install

If you run into any errors with this installer within the PowerShell output, this could cause other parts of the script to also fail. We've seen examples where proxy servers have blocked the download of the Java files from the internet.

It's possible to re run the PowerShell script in either Section 4 or Section 5 if something goes wrong during the initial install. Running this Powershell script again will effectively do a repair of the Gateway,

If you find that the PowerShell script is repeatedly failing, please follow the Manual Install instructions which are available here:

https://www.clickstudios.com.au/downloads/version9/Passwordstate_Remote_Session_Launcher_Gateway_Manual_Install_Guide.pdf

If the script seemed to run successfully but the service did not start, this would most likely be caused by an incorrect encrypted password being set in your **gateway.conf** file. To manually run through this process, see this forum post: <https://www.clickstudios.com.au/community/index.php?/topic/2971-how-to-encrypt-the-certificate-password-for-use-with-the-browser-based-gateway/>