Passwordstate

Enterprise Password Management

Browser Based Launcher

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

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 2016, 2019, 2022, 2025 or Windows 11
- OpenJDK 21 (will be installed automatically as part of this process if you server has internet access)
- The server must have internet access, otherwise you’ll be required to manually download Java source files

2. Architectural Overview

There are two versions of the Browser Based Gateway you can install. By default, this feature is already pre-loaded in your Passwordstate install directory.

By default, this is **c:\inetpub\passwordstate\hosts\gateway**. To finalise the setup within this location, follow section **Installing Gateway on Passwordstate Web Server** below in 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 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.

Note 1: Once our installation script has installed OpenJDK, future upgrades of Passwordstate will not also upgrade OpenJDK. Click Studios strongly encourages all customers to establish and follow a regular software patch management process, and patch OpenJDK on a regular basis.

Note 2: By default, Passwordstate comes installed with a Self-Signed Certificate as this is the only type of certificate Click Studios can supply during the install. Typically, you would change your certificate to something more secure such as one issued from your **Internal Certificate Authority**, or a purchased one from an **online provider**. If your Passwordstate website is still using a Self-Signed Certificate, and you do not supply your own during this install process, your RDP and SSH remote Sessions will fail until you force your browser to trust the certificate.

4. Installing Gateway on Passwordstate Web Server

Steps to execute the automatic installer on your Passwordstate web server

1. Download the installer from your Passwordstate instance from the folder c:\inetpub\passwordstate\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 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 this link: https://cdn.azul.com/zulu/bin/zulu21.40.17-ca-jdk21.0.6-win_x64.zip

5. Installing Gateway on A Separate Server

Steps to execute the automatic installer on a standalone server:

1. Download the installer from your Passwordstate instance from the folder c:\inetpub\passwordstate\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 **"Exporting Certificate from Passwordstate Server"** below in this document, or use any other password protected **.pfx** certificate of your choice. It does not have to be your Passwordstate certificate. Place this exported certificate in the same folder that you are extracted the zip file to, in the step 2 above
4. Open PowerShell ISE "**As Administrator**", and then open the **Install-Gateway-External.ps1** script
5. At the beginning of the script, after all the initial comments, you will see a Powershell variable called **$passwordstateurl**. Enter your Passwordstate URL into this variable. I.e. https://passwordstate.contoso.com
6. On the very next line, enter the **password** you set for certificate
7. Press **F5** to run the script, or use the **Run** 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, the URL you will use is the FQDN 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 prefer to use a custom URL, create a functioning CNAME DNS record to forward traffic to your server where you have installed the gateway, then use that URL on the **Browser Based Gateway Settings** 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 this link: https://cdn.azul.com/zulu/bin/zulu21.32.17-ca-jdk21.0.2-win_x64.zip

6. External Gateway and Local HTML folder

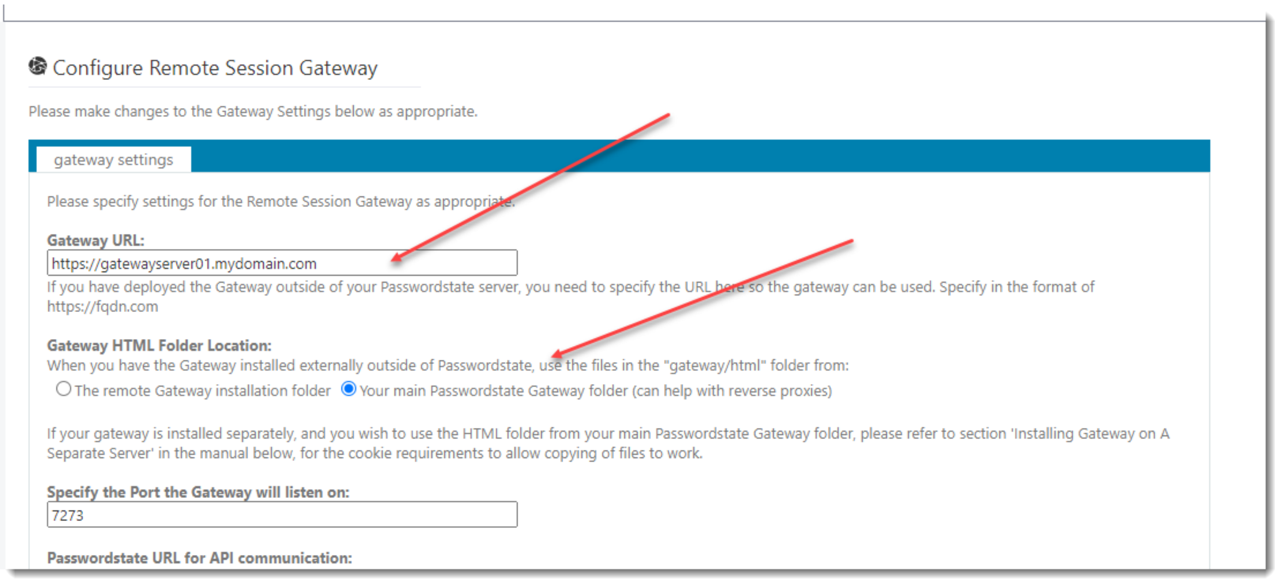
When installing the Remote Session Gateway external to your Passwordstate folder, there is a setting on the screen Administration -> Remote Session Management -> Browser Based Gateway Settings to use the local gateway html folder that comes installed with your core Passwordstate installation – see screenshot below.

This setting should not generally be required, but may help some customers who choose to access their gateway through reverse proxies.

If you choose to do this, you must edit the gateway.conf file in your external gateway installation, and add the line below – then restart the Passwordstate-Gateway Windows Service.

httpCookie=false

If you do not add this setting, then copying files out of the remote session will fail, because you are effectively using two different URLs for the Browser Based Remote Session feature.



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:
https://gatewayserver01.mydomain.com
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

Gateway HTML Folder Location:
When you have the Gateway installed externally outside of Passwordstate, use the files in the "gateway/html" folder from:
○ The remote Gateway installation folder ● Your main Passwordstate Gateway folder (can help with reverse proxies)

If your gateway is installed separately, and you wish to use the HTML folder from your main Passwordstate Gateway folder, please refer to section 'Installing Gateway on A Separate Server' in the manual below, for the cookie requirements to allow copying of files to work.

Specify the Port the Gateway will listen on:
7273

Passwordstate URL for API communication:

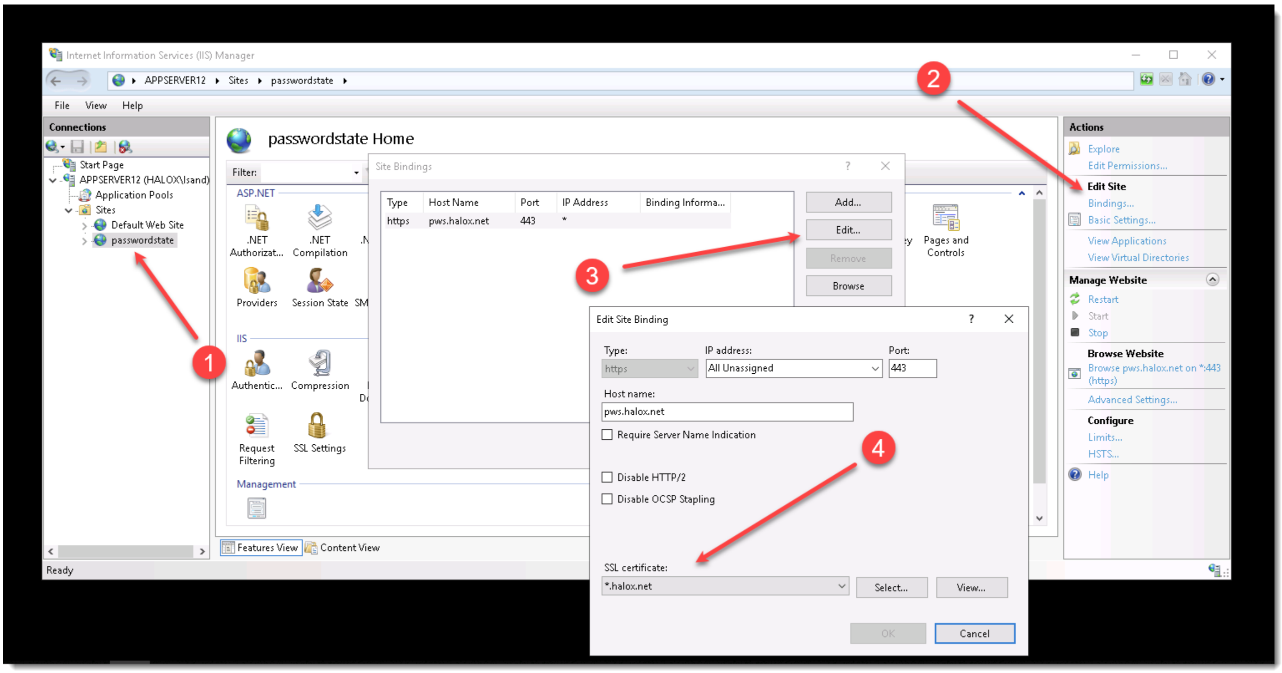
7. Exporting Certificate from Passwordstate Server

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:



Type	Host Name	Port	IP Address	Binding Informa...
https	pws.halox.net	443	*	

Type: https

IP address: All Unassigned

Port: 443

Host name: pws.halox.net

□ Require Server Name Indication

□ Disable HTTP/2

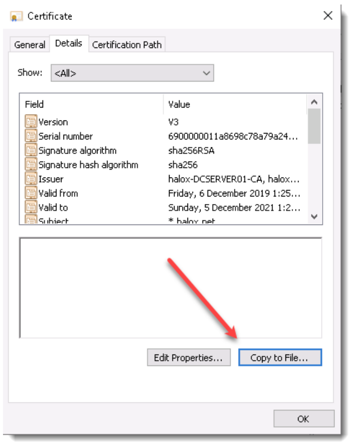
□ Disable OCSP Stapling

SSL certificate: *.halox.net

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.

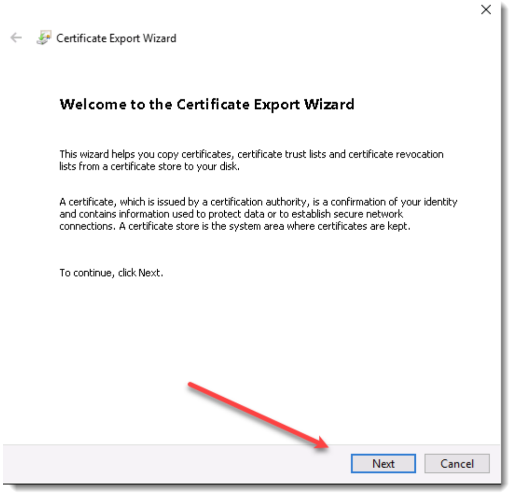
Method #2 to export certificate:

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**"



Field	Value
Version	V3
Serial number	6900000011a8698c78a79a24…
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	halox-DCSERVER01-CA, halox…
Valid from	Friday, 6 December 2019 1:25…
Valid to	Sunday, 5 December 2021 1:2…
Subject	*.halox.net

4. Click **Next**



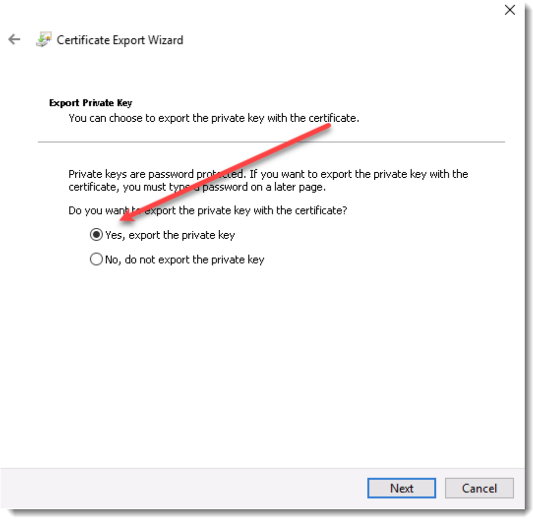
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

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



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

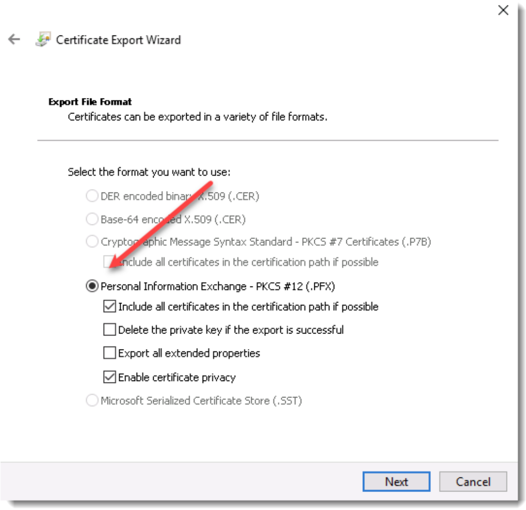
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

6. Select **Personal Information Exchange**



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

☑ Include all certificates in the certification path if possible

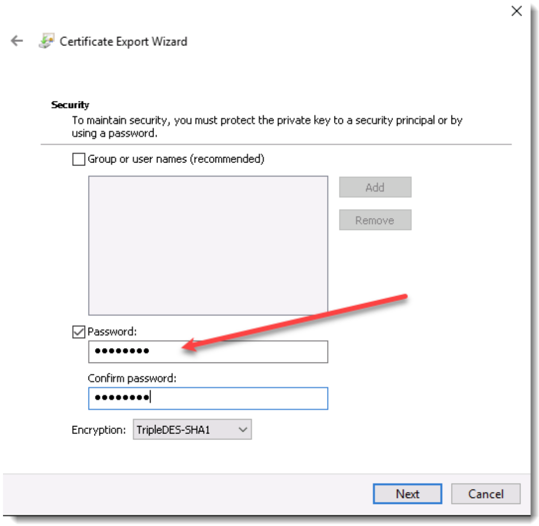
□ Delete the private key if the export is successful

□ Export all extended properties

☑ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

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



Certificate Export Wizard

Security

To maintain security, you must protect the private key to a security principal or by using a password.

□ Group or user names (recommended)

☑ Password:

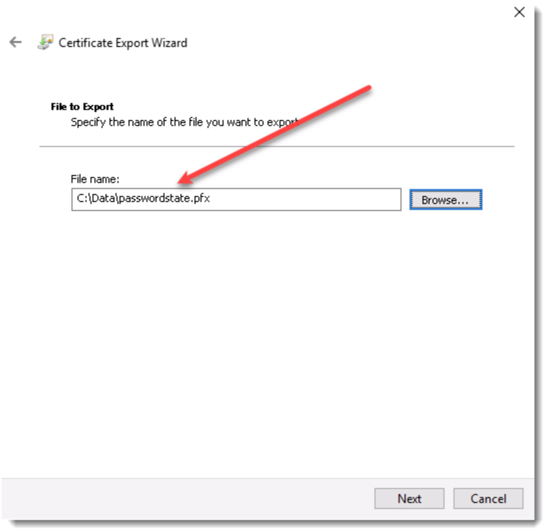
••••••••

Confirm password:

••••••••

Encryption: TripleDES-SHA1

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



File to Export

Specify the name of the file you want to export

File name:

C:\Data\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://forums.clickstudios.com.au/topic/2934-how-to-set-up-a-internal-certificate-authority/

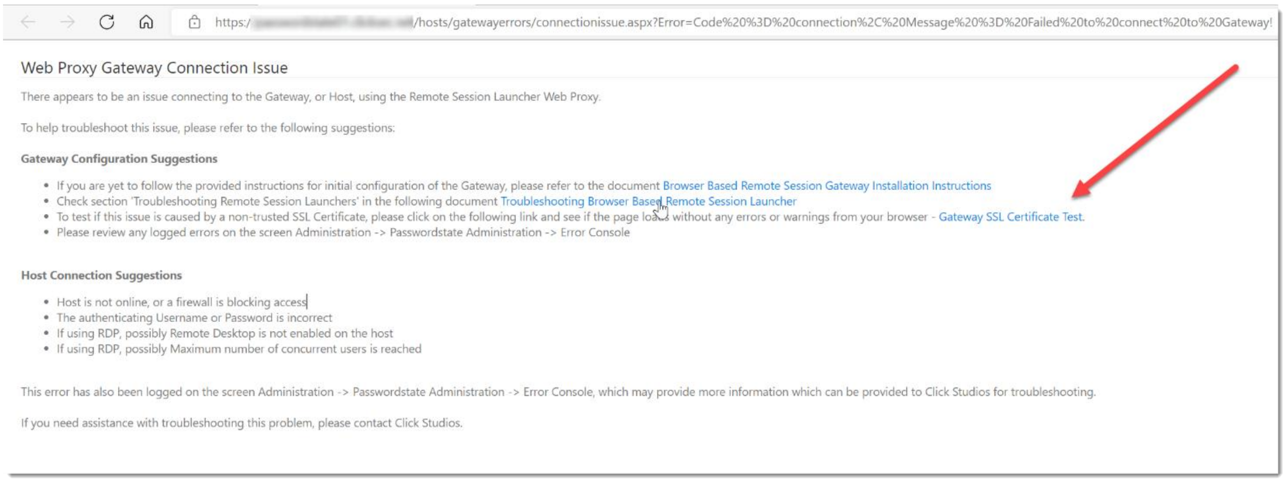
Request a certificate that is marked as "Exportable": https://forums.clickstudios.com.au/topic/1952-generate-a-new-certificate-from-active-directory-certificate-authority/

7. How to Trust a Self-Signed Certificate

For a seamless experience with the Remote Session Launcher, you should use a trusted certificate, which can either be issued from your own internal Certificate Authority, or from an online provider. If you have no choice but to use a Self-Signed Certificate, then you will need to force your browser to trust this certificate. Below are some instructions on how to do this in Microsoft Edge:

When trying to establish a Remote Session, and you receive the error below, one of the reasons this can occur is if your browser does not trust the certificate that is installed with your Browser Based Gateway.

Click on the **Gateway SSL Certificate Test** link:



https:/[redacted]/hosts/gatewayerrors/connectionissue.aspx?Error=Code%20%3D%20connection%2C%20Message%20%3D%20Failed%20to%20connect%20to%20Gateway!

Web Proxy Gateway Connection Issue

There appears to be an issue connecting to the Gateway, or Host, using the Remote Session Launcher Web Proxy.

To help troubleshoot this issue, please refer to the following suggestions:

Gateway Configuration Suggestions

- If you are yet to follow the provided instructions for initial configuration of the Gateway, please refer to the document Browser Based Remote Session Gateway Installation Instructions
- Check section 'Troubleshooting Remote Session Launchers' in the following document Troubleshooting Browser Based Remote Session Launcher
- To test if this issue is caused by a non-trusted SSL Certificate, please click on the following link and see if the page loads without any errors or warnings from your browser - Gateway SSL Certificate Test.
- Please review any logged errors on the screen Administration -> Passwordstate Administration -> Error Console

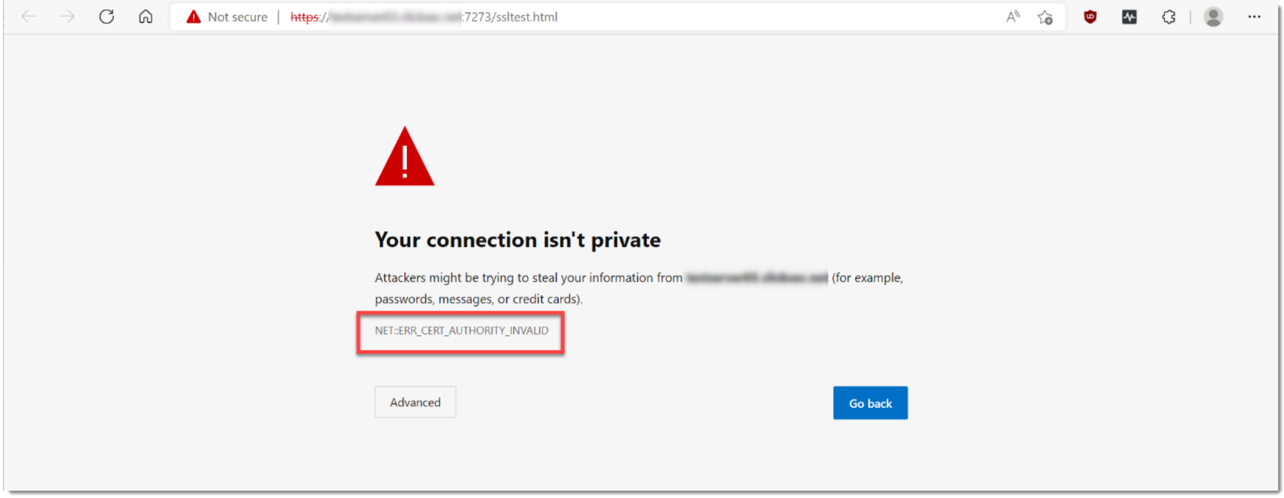
Host Connection Suggestions

- Host is not online, or a firewall is blocking access
- The authenticating Username or Password is incorrect
- If using RDP, possibly Remote Desktop is not enabled on the host
- If using RDP, possibly Maximum number of concurrent users is reached

This error has also been logged on the screen Administration -> Passwordstate Administration -> Error Console, which may provide more information which can be provided to Click Studios for troubleshooting.

If you need assistance with troubleshooting this problem, please contact Click Studios.

If you then get redirected to a page that looks like the screenshot below, the certificate is not trusted by your browser:



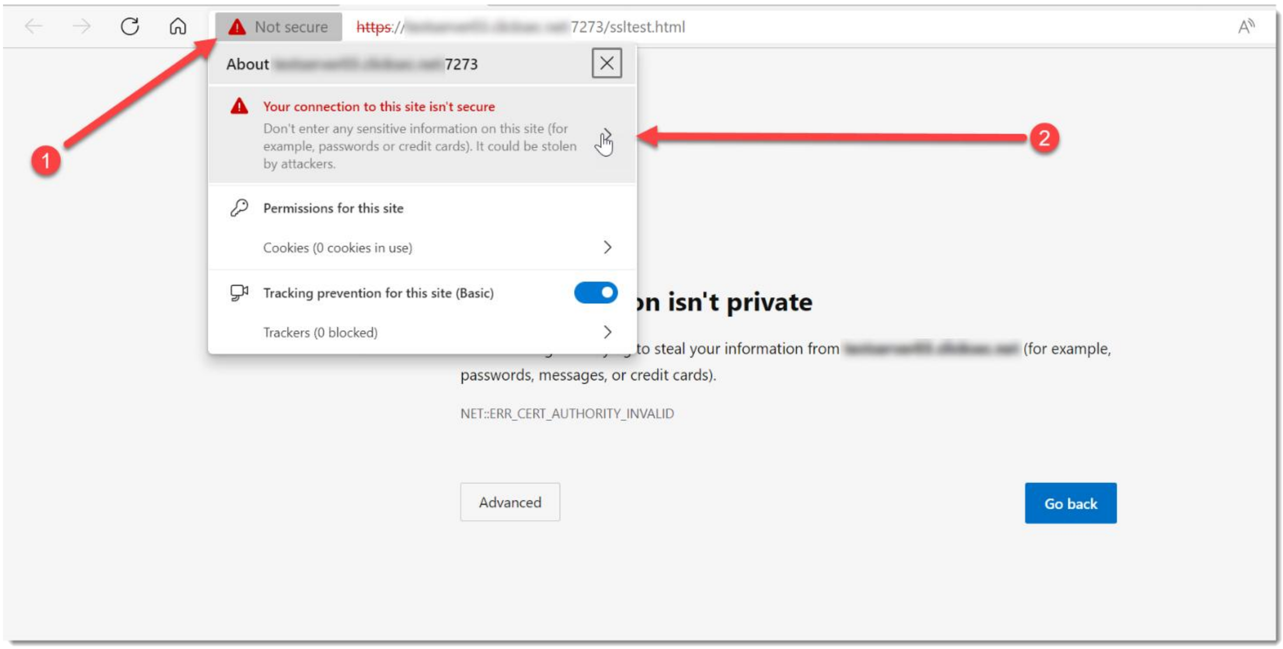
Not secure | https://[redacted]:7273/ssltest.html

Your connection isn't private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

To fix this, you will need to follow this process on every machine that you intend on establishing remote sessions from. First, click the Warning button in Edge, and then click the Warning message:



About [redacted]7273

Your connection to this site isn't secure

Don't enter any sensitive information on this site (for example, passwords or credit cards). It could be stolen by attackers.

Permissions for this site

Cookies (0 cookies in use)

Tracking prevention for this site (Basic)

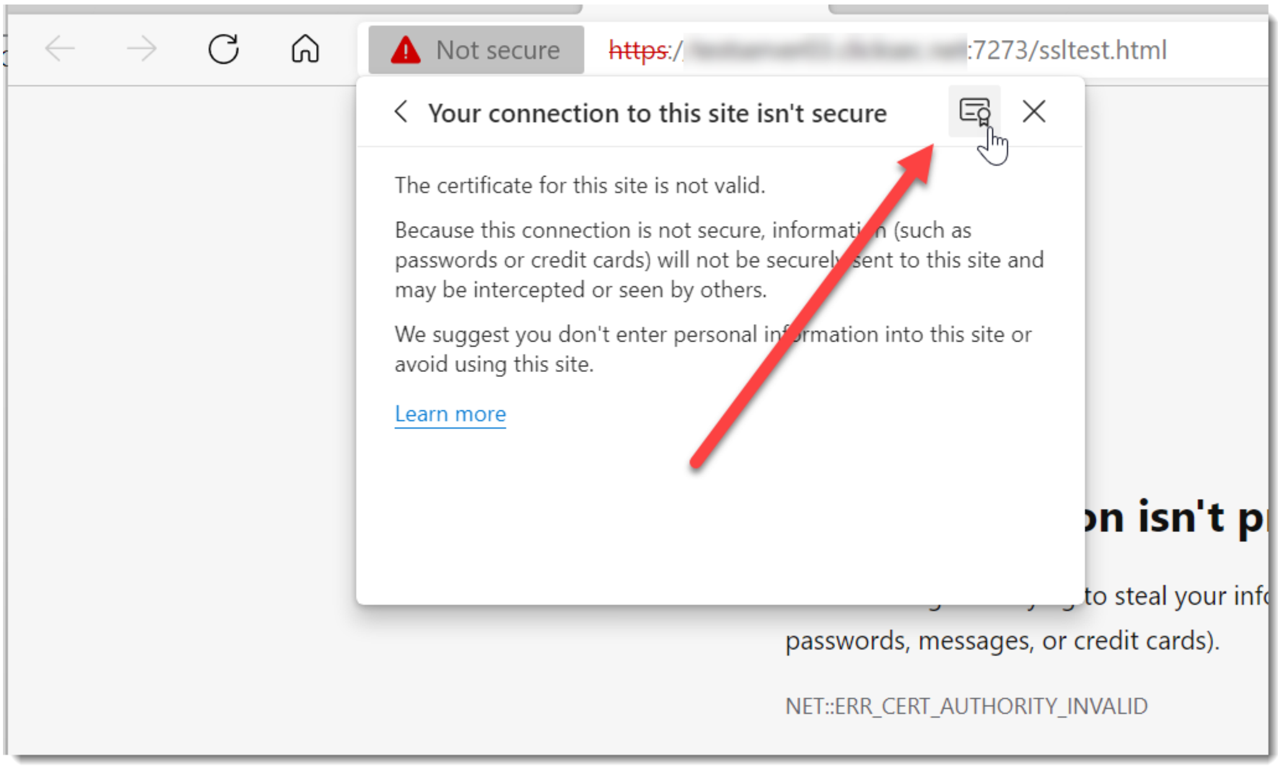
Trackers (0 blocked)

on isn't private

to steal your information from [redacted] (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

Click the **Certificate** button:



Your connection to this site isn't secure

The certificate for this site is not valid.

Because this connection is not secure, information (such as passwords or credit cards) will not be securely sent to this site and may be intercepted or seen by others.

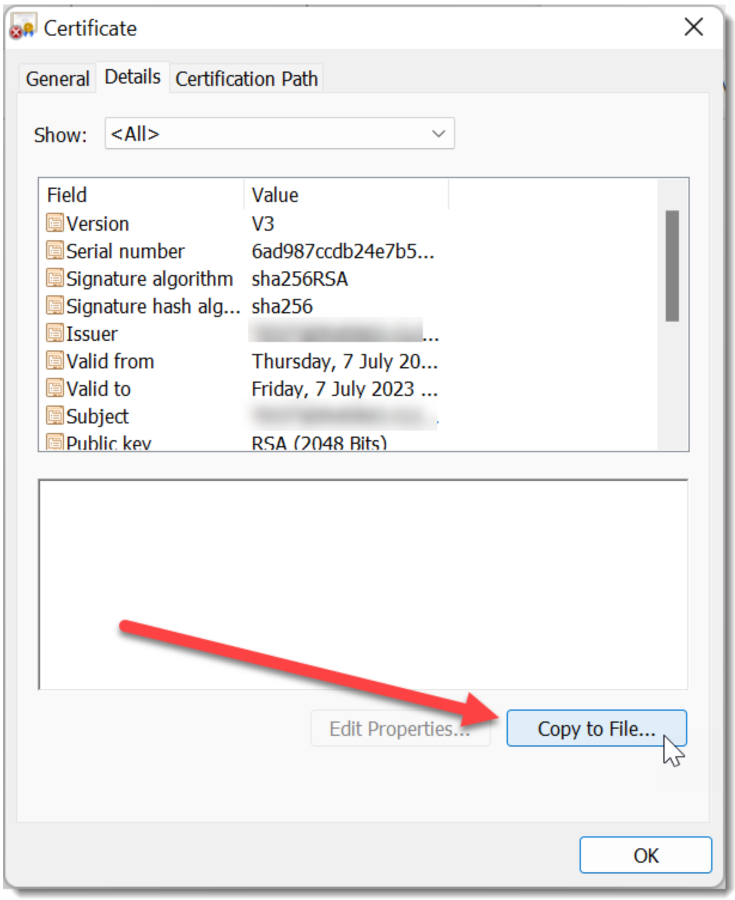
We suggest you don't enter personal information into this site or avoid using this site.

on isn't p

to steal your info passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

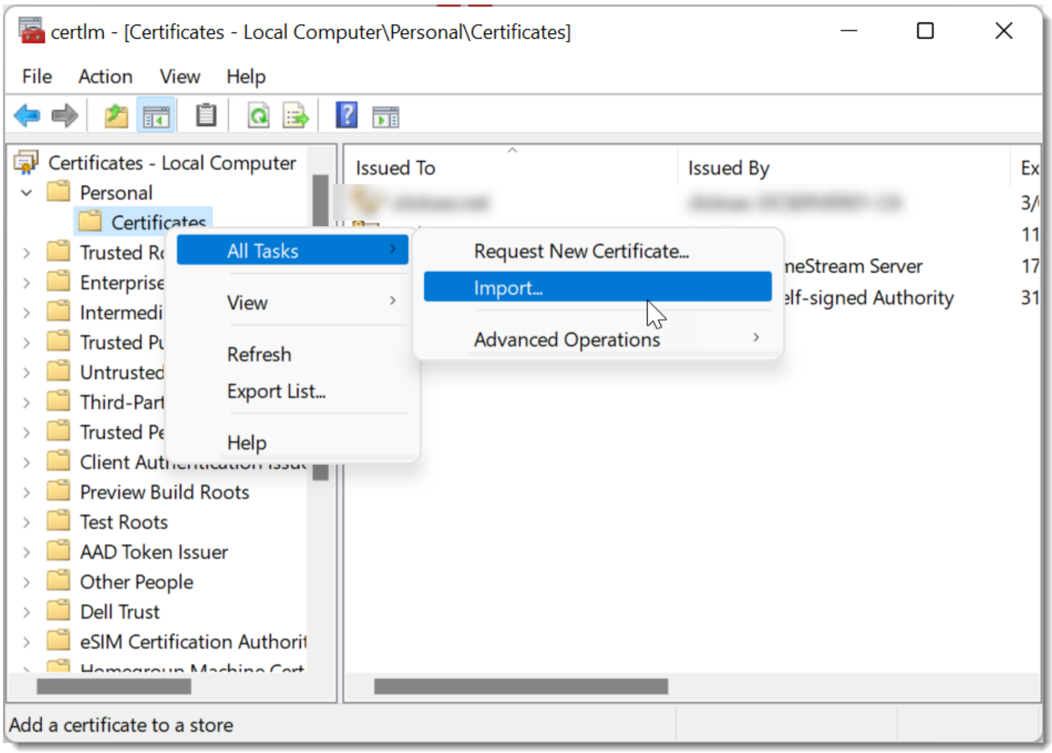
Under the **Details** tab, click **Copy to File**. Follow the prompts to save the certificate to disk, and you can choose all the default options during this process.



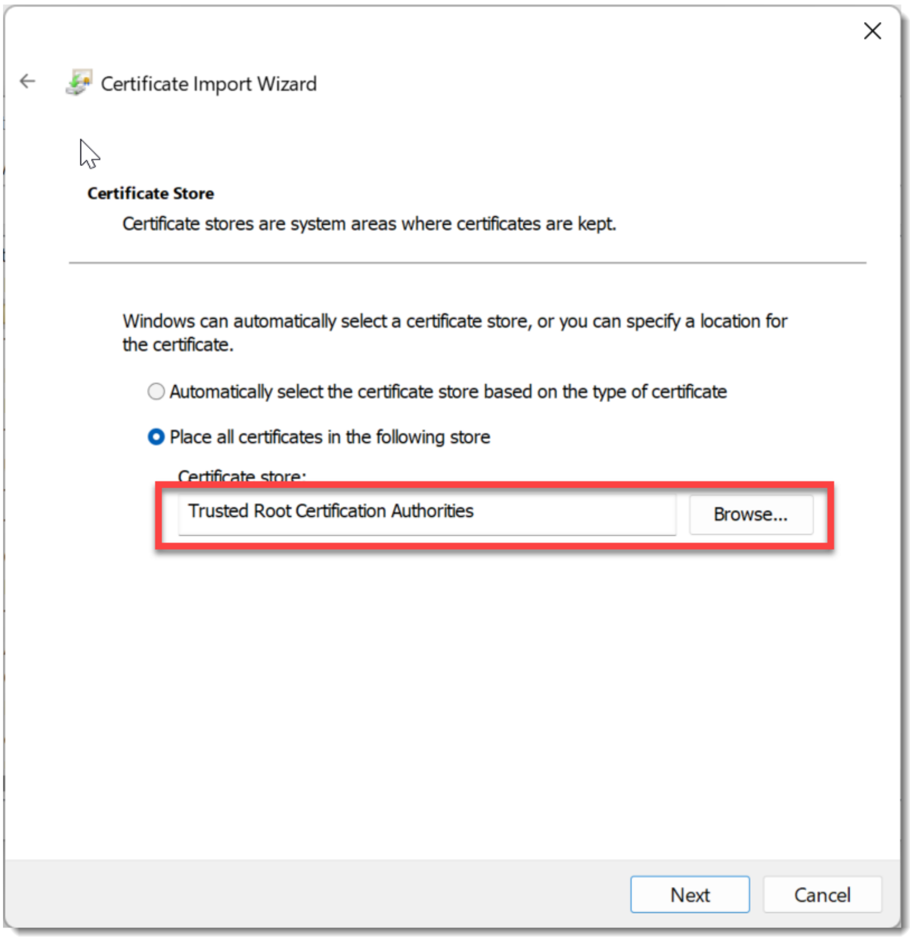
Show: <All>

Field	Value
Version	V3
Serial number	6ad987ccdb24e7b5...
Signature algorithm	sha256RSA
Signature hash alg...	sha256
Issuer	[redacted]...
Valid from	Thursday, 7 July 20...
Valid to	Friday, 7 July 2023 ...
Subject	[redacted]
Public key	RSA (2048 Bits)

Now in Windows, go to **Start** -> **Run** and type in **certlm.msc**, and this will open the **Local Certificate Store** on your machine. Expand our **Personal**, right click **Certificates** -> **All Tasks** -> **Import**:



Follow the prompts and browse to the certificate you saved to disk, and ensure you place the certificate in the **Trusted Root Certificate Authorities** store:



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

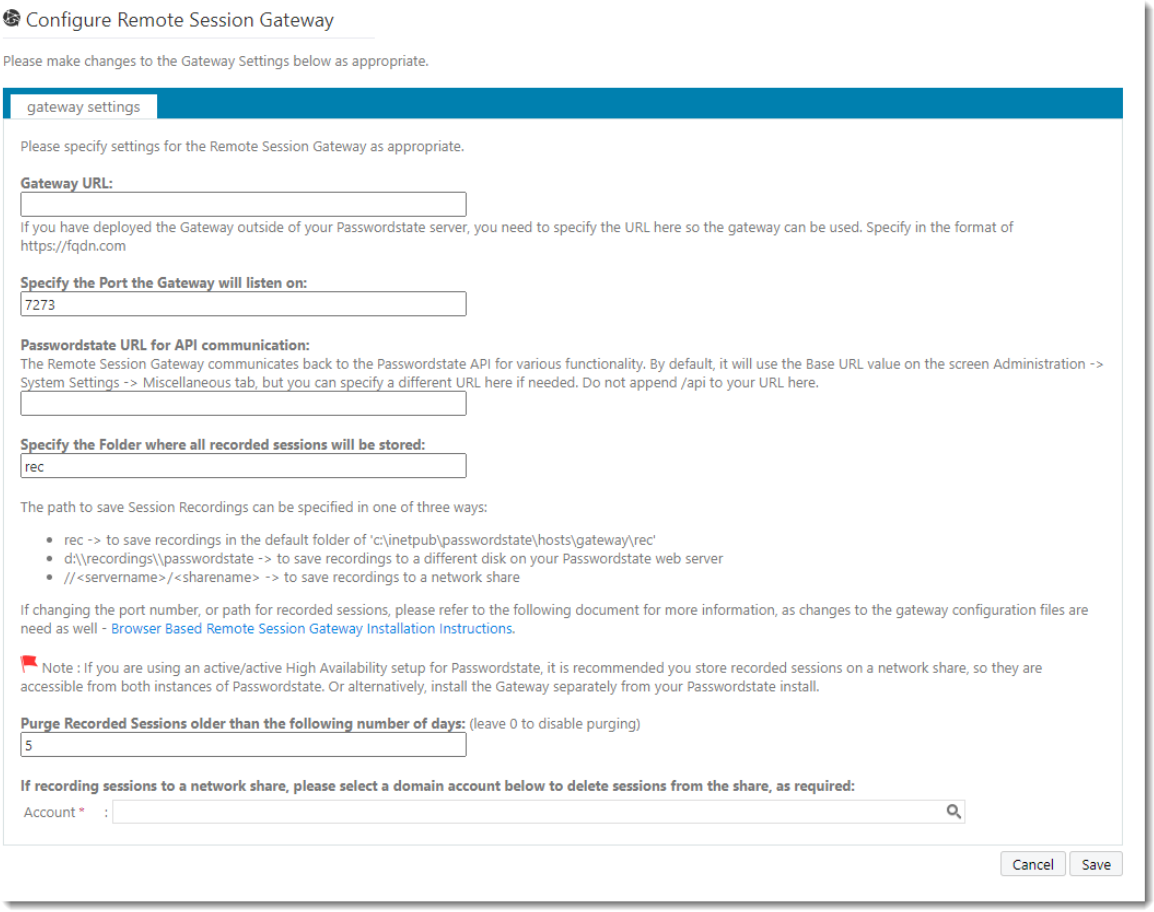
At this point, you should be able to close your browser and reopen it, and try launching a new session. It should connect successfully.

8. 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.



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: 7273

Passwordstate URL for API communication:
The Remote Session Gateway communicates back to the Passwordstate API for various functionality. By default, it will use the Base URL value on the screen Administration -> System Settings -> Miscellaneous tab, but you can specify a different URL here if needed. Do not append /api to your URL here.

Specify the Folder where all recorded sessions will be stored: rec

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) 5

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

Account * :

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.

9. 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.

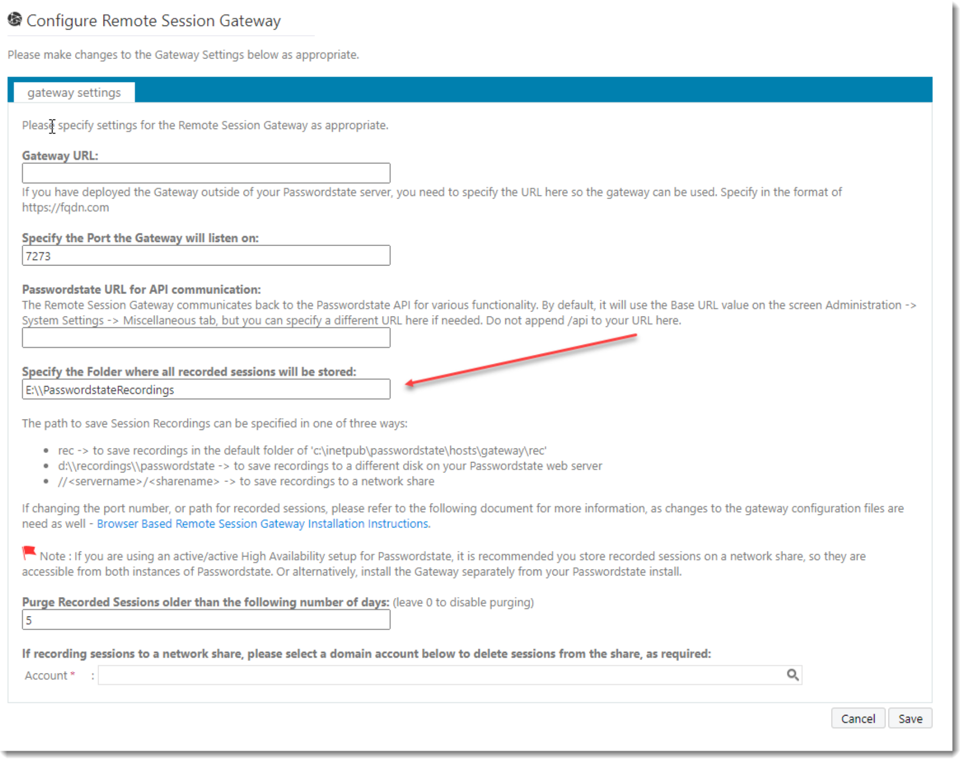
When changing the path to where you wish to save session recordings, this needs to be done in two locations:

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. **<drivename>:\\<foldername>** -> to save recordings to a different disk on your Passwordstate web server
3. **//<servername>/<sharename>** -> to save recordings to a network share

Example of changing the path in the User Interface:



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: 7273

Passwordstate URL for API communication:
The Remote Session Gateway communicates back to the Passwordstate API for various functionality. By default, it will use the Base URL value on the screen Administration -> System Settings -> Miscellaneous tab, but you can specify a different URL here if needed. Do not append /api to your URL here.

Specify the Folder where all recorded sessions will be stored: E:\\PasswordstateRecordings

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.

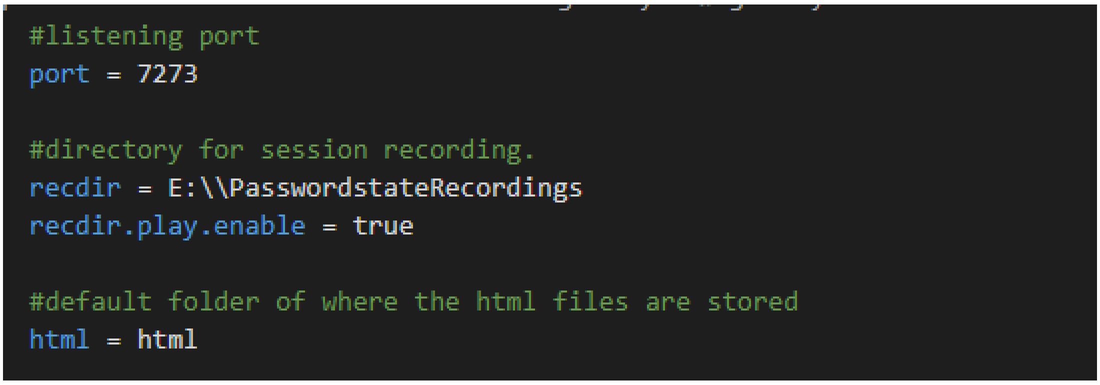
Note : If you are using an active/active High Availability setup for Passwordstate, it is recommended you store recorded sessions on a network share, so they are accessible from both instances of Passwordstate. Or alternatively, install the Gateway separately from your Passwordstate install.

Purge Recorded Sessions older than the following number of days: (leave 0 to disable purging) 5

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

Account * :

Example of the changing the path in the gateway.conf file:



```
#listening port
port = 7273

#directory for session recording.
recdir = E:\\PasswordstateRecordings
recdir.play.enable = true

#default folder of where the html files are stored
html = html
```

Note 1: the ***recdir*** setting is used to tell the gateway where to save the Session Recordings

Note 2: When changing this setting, you need to restart the Passwordstate-Gateway Windows Service to pick up the change

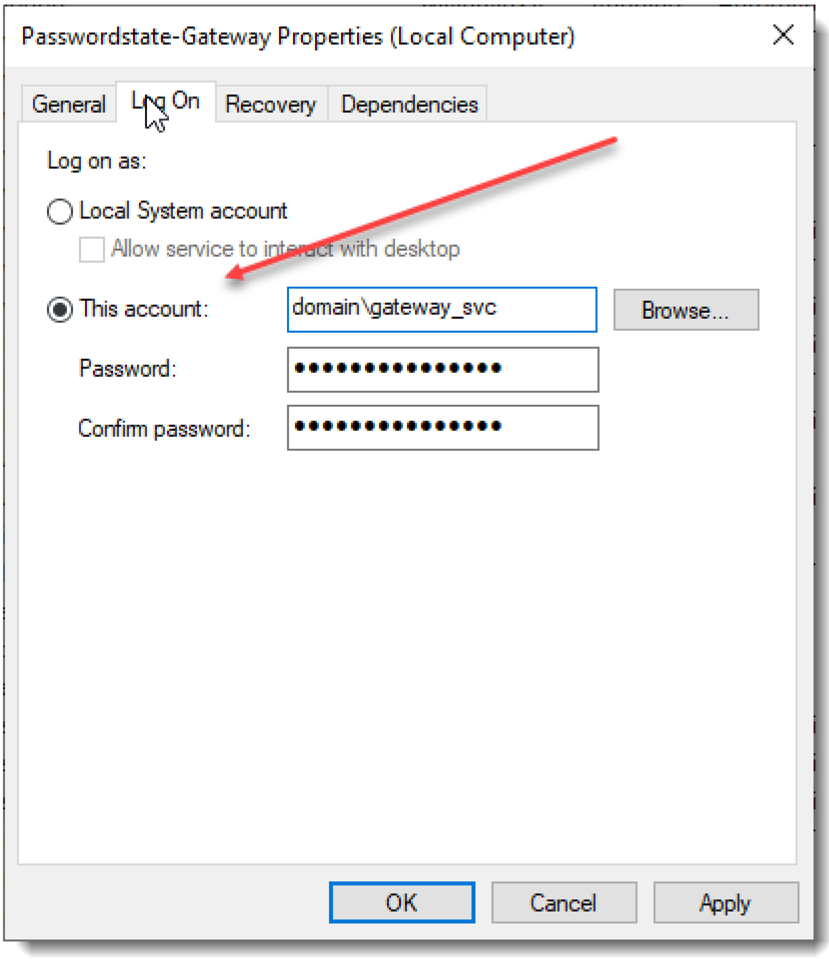
Session Recording Permissions

When storing session recordings using the default ***rec*** value, the NTFS permissions are already correct.

If, however you specify a different location such as static folder on a different disk, then you need to ensure at least Authenticated Users have modify access to the folder.

When using a Network Share, you must modify the '**Log On**' rights for the Passwordstate-Gateway Windows Service, with an account that has read/write to the share – screenshot below for this.

If you want Passwordstate to delete session recordings from the network share, please set an account on the Configure Remote Session Gateway page that also has permissions to delete from the network share.



Passwordstate-Gateway Properties (Local Computer)

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: domain\gateway_svc

Password: ●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●

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.

10. Renewing the SSL Certificate

Once your certificate expires that you are using for the Remote Session Gateway, it will need to be renewed. To do that, please follow these instructions:

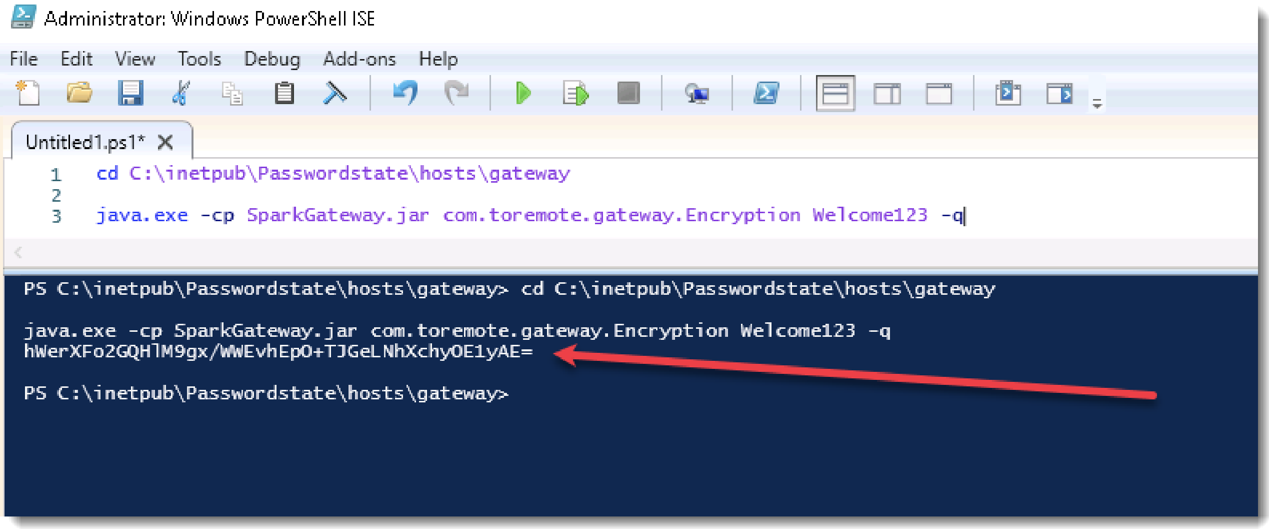
1. Export your certificate, as per the section ‘Exporting Certificate from Passwordstate Server’ above – this assumes you are going to use the same certificate as your Passwordstate web site

2. Stop the Passwordstate-Gateway Windows Service

3. Open PowerShell ISE as Administrator (Right click -> Run as Administrator) and copy in the code below. Ensure you change the password from **Welcome123** to the password you set when exporting your certificate:

```
cd C:\inetpub\Passwordstate\hosts\gateway
java.exe -cp SparkGateway.jar com.toremote.gateway.Encryption Welcome123 -q
```

This will give an output as per below screenshot:


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1*

```
cd C:\inetpub\Passwordstate\hosts\gateway

java.exe -cp SparkGateway.jar com.toremote.gateway.Encryption Welcome123 -q
```

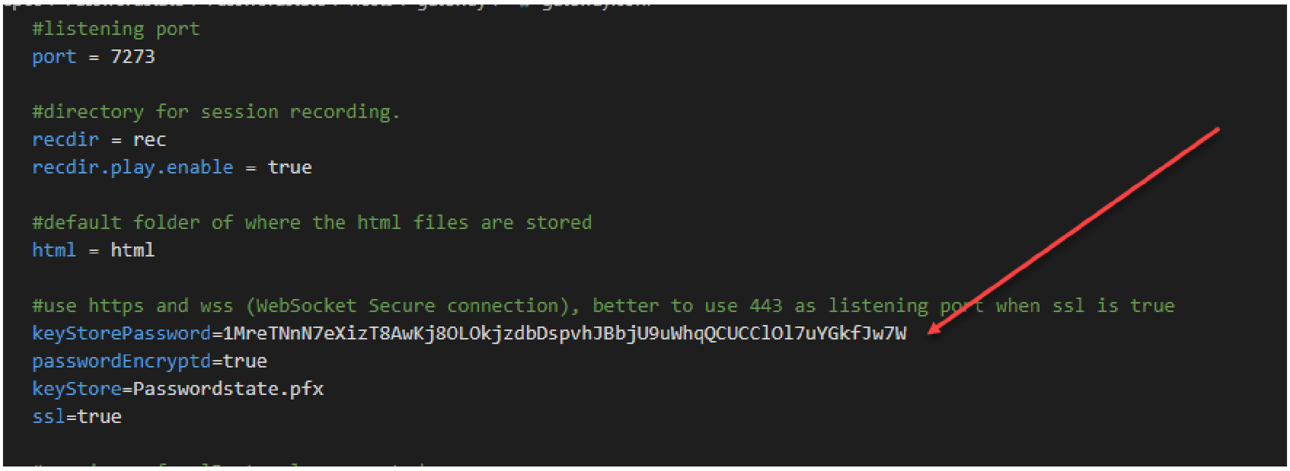
```
PS C:\inetpub\Passwordstate\hosts\gateway> cd C:\inetpub\Passwordstate\hosts\gateway

java.exe -cp SparkGateway.jar com.toremote.gateway.Encryption Welcome123 -q
hWerXFo2GQHlM9gx/WWEvhEpO+TJGeLNhXchyOE1yAE=

PS C:\inetpub\Passwordstate\hosts\gateway>
```

Note: Change the path of the gateway in the first line if appropriate

- Now open the file "C:\inetpub\Passwordstate\hosts\gateway\gateway.conf” and update the setting “keyStorePassword” with your encrypted password from the PowerShell session, as per the following screenshot



```
#listening port
port = 7273

#directory for session recording.
recdir = rec
recdir.play.enable = true

#default folder of where the html files are stored
html = html

#use https and wss (WebSocket Secure connection), better to use 443 as listening port when ssl is true
keyStorePassword=1MreTNnN7eXizT8AwKj8OLOkjzdbDspvhJBbjU9uWhqQCUCClOl7uYGkfJw7W
passwordEncryptd=true
keyStore=Passwordstate.pfx
ssl=true
```

4. Now restart the Passwordstate-Gateway Windows Service

11. Browser Based Launcher Strong Cipher Settings & TLS

By editing the gateway.conf file you can force the Browser Based Launcher to communicate on certain Ciphers, and disable old TLS settings, for extra security. Below is an example cipherSuites settings that you can add which will omit any less secure Ciphers, as well as the recommended SSL Protocols setting. You can copy and paste this code below into your gateway.conf file, ensuring the text is on a single line as per the screenshot below, and then restart your Passwordstate Gateway service for it to take effect.

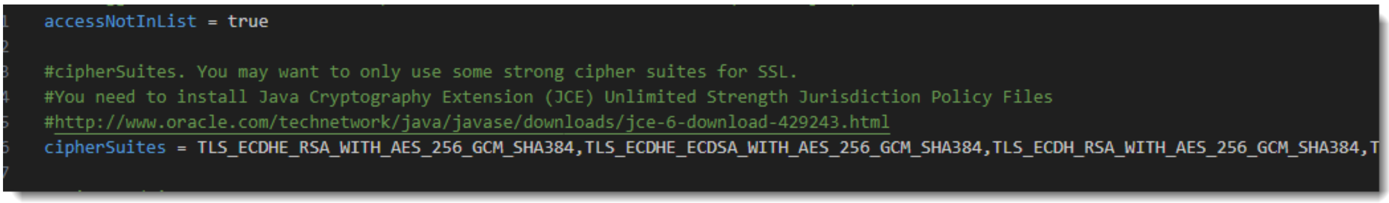
These settings below may already exist in your gateway.conf file, if you are using build 9785 or later.

Cipher Suites
Add the following block of text to your gateway.conf file.

```
cipherSuites = TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
```

SSL Protocols
Modify the sslProtocols section of the document, to only use TLS 1.2. as per the example below.

```
sslProtocols=TLSv1.2
```



```
accessNotInList = true

#cipherSuites. You may want to only use some strong cipher suites for SSL.
#You need to install Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files
#http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html
cipherSuites = TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,T
```

12. Browser Based Launcher WebSocket HTTP Server Header Settings

By editing the gateway.conf file you can add your own HHTP headers, which can be used with the WebSocket HTTP Server used for the remote session gateway – this is separate to the web site Passwordstate uses in Internet Information Services.

Examples of HTTP header attributes can be found here - https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers

An example of the format you can add to the gateway.conf file is:

```
headers=Strict-Transport-Security: max-age=31536000\r\nx-frame-options: SAMEORIGIN\r\nX-Content-Type-Options: nosniff\r\nAccess-Control-Allow-Origin: https://passwordstate.domain.com
```

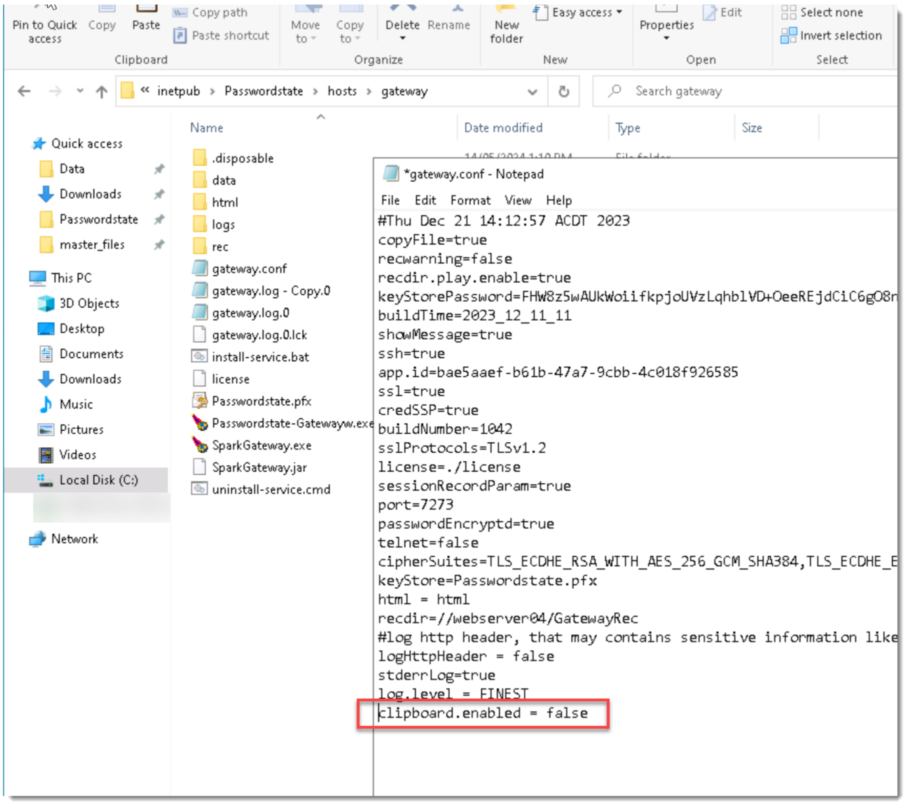
Once added to the gateway.conf file, you will need to restart the Passwordstate-Gateway Windows Service

13. Restrict Copy/Paste Files and Clipboard with RDP Sessions

With RDP Sessions, it’s possible to disable clipboard and file copying, to prevent “moving” data in and out of sessions. To do this, you need to add the following line to the gateway.conf file.

clipboard.enabled=false

Example below for this:



```
#Thu Dec 21 14:12:57 ACDT 2023
copyFile=true
recwarning=false
recdir.play.enable=true
keyStorePassword=FHW8z5wAUkWoiifkpjoUVzLqhblVD+OeeREjdCiC6gO8n
buildTime=2023_12_11_11
showMessage=true
ssh=true
app.id=bae5aaef-b61b-47a7-9cbb-4c018f926585
ssl=true
credSSP=true
buildNumber=1042
sslProtocols=TLSv1.2
license=./license
sessionRecordParam=true
port=7273
passwordEncryptd=true
telnet=false
cipherSuites=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_E
keyStore=Passwordstate.pfx
html = html
recdir=//webserver04/GatewayRec
#log http header, that may contains sensitive information like
logHttpHeader = false
stderrLog=true
log.level = FINEST
clipboard.enabled = false
```

Once this change is made, restart the **Passwordstate-Gateway** Windows Service.