



Remote Session Management Manual

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	OVERVIEW	4
2	INSTALL THE CLIENT BASED LAUNCHER.....	5
3	INSTALLING THE BROWSER BASED LAUNCHER.....	6
4	INSTALL BROWSER BASED LAUNCHER FOR REMOTE SITE LOCATIONS MODULE.....	7
5	HOW TO LAUNCH A REMOTE SESSION	8
6	ADDING HOSTS INTO PASSWORDSTATE	10
6.1	MANUALLY ADDING HOSTS.....	10
6.2	ADDING HOSTS IN BULK VIA CSV FILE.....	12
6.3	ADDING HOSTS AUTOMATICALLY USING A HOSTS DISCOVERY JOB	12
6.4	ADDING HOSTS VIA API	12
6.5	ORGANISING HOSTS READY FOR CONNECTIONS	12
7	REMOTE SESSION CREDENTIALS	16
7.1	ADDING A PASSWORD RECORD	16
7.2	ADDING A REMOTE SESSION CREDENTIAL.....	17
7.3	SHARING OUT A REMOTE SESSION CREDENTIAL	18
7.4	TIME-BASED ACCESS TO REMOTE SESSION CREDENTIALS.....	19
8	PERSONAL PREFERENCES.....	20
9	ADMINISTRATION: FEATURE ACCESS	21
10	SESSION RECORDING.....	22
11	SQL SERVER CONNECTIONS	27
12	TEAMVIEWER CONNECTIONS	28
13	SSH WITH PRIVATE PUBLIC KEY	32
13.1	PASSWORD LIST REQUIREMENTS FOR USING SSH KEYS.....	32
13.2	CREATING A PASSWORD RECORD.....	33
13.3	CREATING A REMOTE SESSION CREDENTIAL	34
13.4	CONVERT PUTTY PRIVATE KEY TO OPENSSH FORMAT.....	35
14	CLIENT BASED LAUNCHER WITH MICROSOFT REMOTE DESKTOP GATEWAY	36
15	FILE TRANSFER WITH BROWSER BASED LAUNCHER.....	37
15.1	RDP FILE TRANSFER.....	37
15.2	SSH FILE TRANSFER	39
16	BROWSER BASED LAUNCHER KEYBOARD SHORTCUTS AND FAQ	41
16.1	RDP KEYBOARD SHORTCUTS.....	41
16.2	SSH SHELL HISTORY	41
17	BROWSER BASED LAUNCHER STRONG CIPHER SETTINGS & TLS.....	42
18	BROWSER BASED LAUNCHER KERBEROS CONNECTIONS	43
19	OPEN PORTS FOR REMOTE SESSION LAUNCHERS.....	44
20	PERFORMANCE METRICS FOR BROWSER BASED GATEWAY	45

20.1	CPU USAGE.....	45
20.2	MEMORY USAGE.....	45
20.3	BANDWIDTH USAGE.....	45
21	TROUBLESHOOTING REMOTE SESSION LAUNCHERS.....	46
21.1	CLIENT BASED LAUNCHER TROUBLESHOOTING STEPS	46
21.2	BROWSER BASED LAUNCHER TROUBLESHOOTING STEPS	47
22	BROWSER BASED LAUNCHER AND SELF SIGNED CERTIFICATES.....	48
23	REMOTE SESSION LAUNCHER FAQ.....	52

1 Overview

Passwordstate has two different remote session Launchers that you can use, a **Client Based Launcher** and a **Browser Based Launcher**.

The purpose of these launchers is to automatically and securely connect you to remote machines, things like Windows Servers, Desktops, Linux machines, Switches, Databases and Firewalls etc. It does this by retrieving credentials directly from the Passwordstate vault, and passes these through securely to the remote session.

You can even have your users use these launchers to remote into these hosts, without even knowing which password they are connecting in with. This is great for temporary contractors that may be doing some work for your team.

This guide will explain how you can install and configure both of the launchers, and can also help you diagnose any issues you may have when using either of them.

Below is a brief summary of each launcher:

Client Based Launcher:

- Supports connections for the following types:
 - RDP
 - SSH
 - SQL
 - VNC
 - Telnet
 - TeamViewer
- Connects using a physically installed application on your machine, like mstsc.exe or putty.exe
- Requires one installation per machine where you want to use the launcher
- No plugins or agents required on remote hosts
- No session Recording

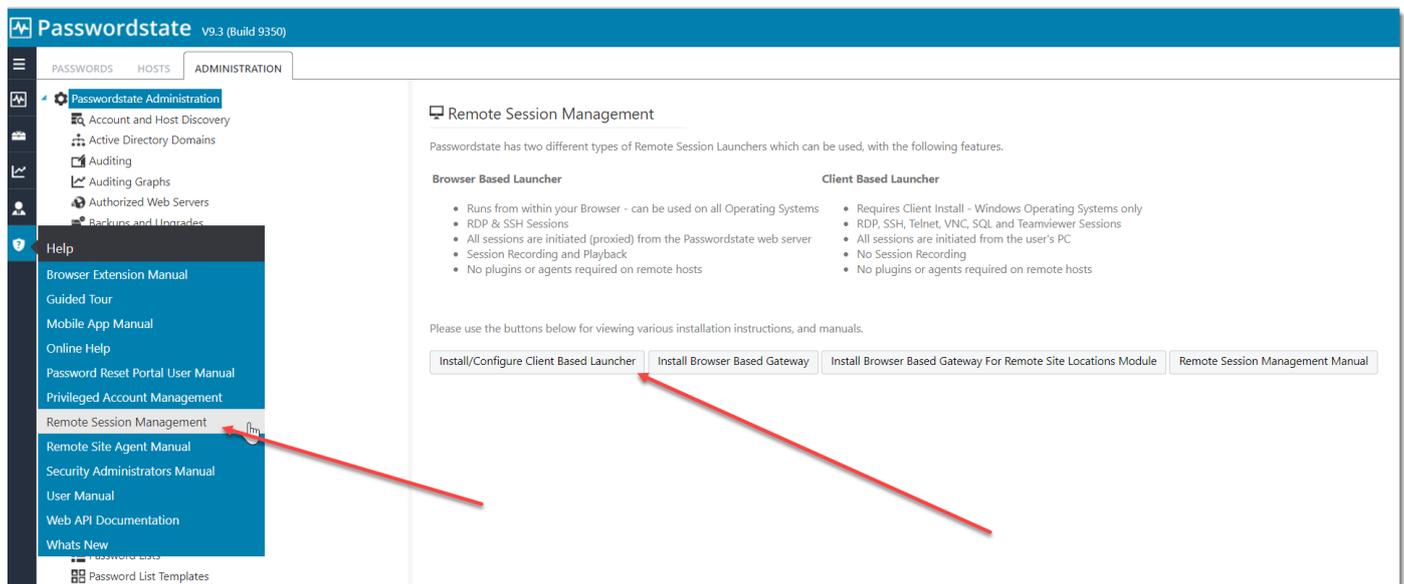
Browser Based Launcher:

- Supports connections for the following types:
 - RDP
 - SSH
- Runs directly in your browser, no installation required on each of your desktops
- All sessions are initiated (proxied) through a Gateway on your Passwordstate webserver, or you can host this Gateway on a separate server if you wish
- No plugins or agents required on remote hosts
- Allows Session Recording for playback at a later date
- Can be used in conjunction with the Remote Site Locations Module, so you can RDP or SSH into machines over the internet or disconnected networks

2 Install the Client Based Launcher

Installing and configuring the Client Based Launcher is a per machine process, and full details on how to do this can be found in Passwordstate under the Help Menu **'Remote Session Management'**

Click on the button **'Install/Configure Client Based Launcher'** and then follow the on page instructions to install the client, and then configure you browser.



Note 1: Configuring the Browser is a once off process, which allows the browser to launch the physically installed app on your machine. If you clear you Browser cache, you will need to follow this process again

Note 2: The Client Base launcher will fail to launch a session if you have popups being blocked in your browser. Please check popups are allowed in your browser if your sessions appear to “Do Nothing” when attempting to connect.

Note 3: If you would like to install the client based launcher using your software deployment tool, you can use the following switch to install it silently without the installer GUI – `passwordstatelauncher.exe /s`

3 Installing the Browser Based Launcher

Installing the Browser Based Launcher is a once off process on a single server of your choice. It can be installed on any Windows operating system of your choice, and all sessions are tunnelled through a Windows Service that you create during this installation process.

The core Passwordstate website comes preinstalled with this Browser Based Launcher, but it does still require some configuration as a once off process before you can start using it. This is the most preferred and easiest option a majority of Click Studios customers use.

Alternatively, you can install this Browser Based Launcher on a separate server to where you have Passwordstate installed.

To configure the existing install of the Browser Based Launcher on your Passwordstate webserver, or to install it separately, please see this install guide which is mostly automated for you:

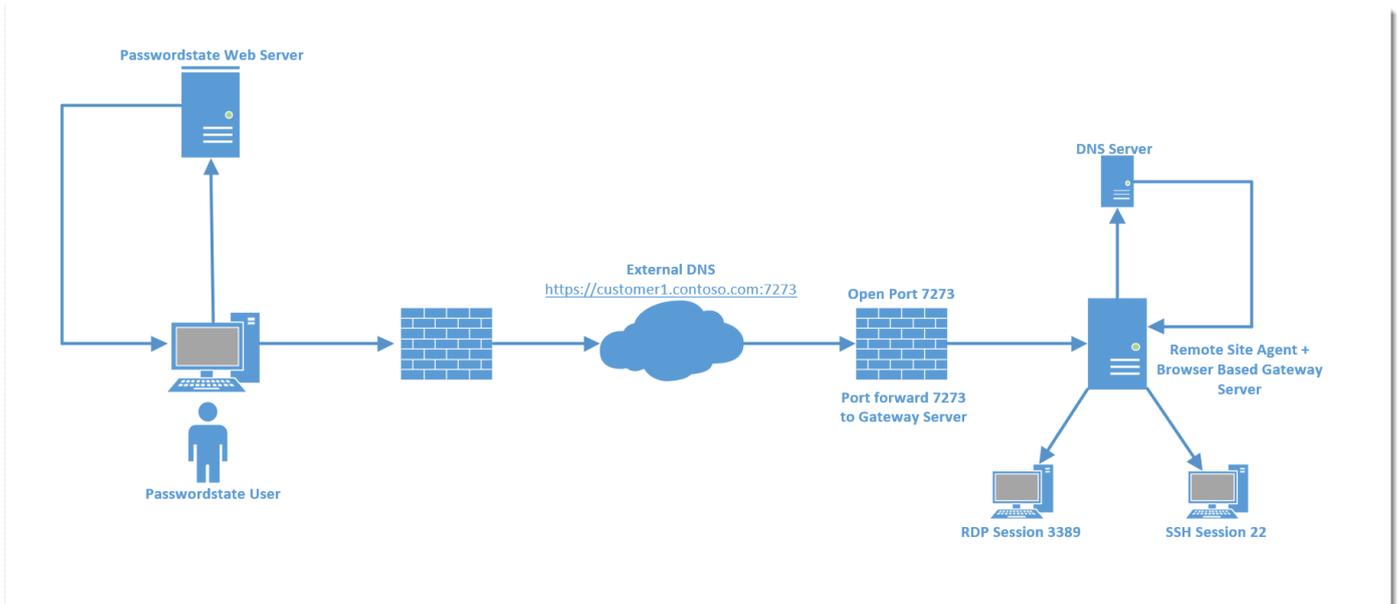
https://www.clickstudios.com.au/downloads/version9/Passwordstate_Remote_Session_Launcher_Gateway_Install_Guide.pdf

4 Install Browser Based Launcher for Remote Site Locations Module

Passwordstate has an additional module called Remote Site Locations, which allows you to deploy an agent to a remote network that you do not have direct connectivity to. This agent can discover and manage privileged accounts and passwords on that remote site, and this is all centrally managed from your internally hosted Passwordstate instance. More information on this Remote Site Locations module can be found here:

<https://www.clickstudios.com.au/remotesitelocations/default.aspx>

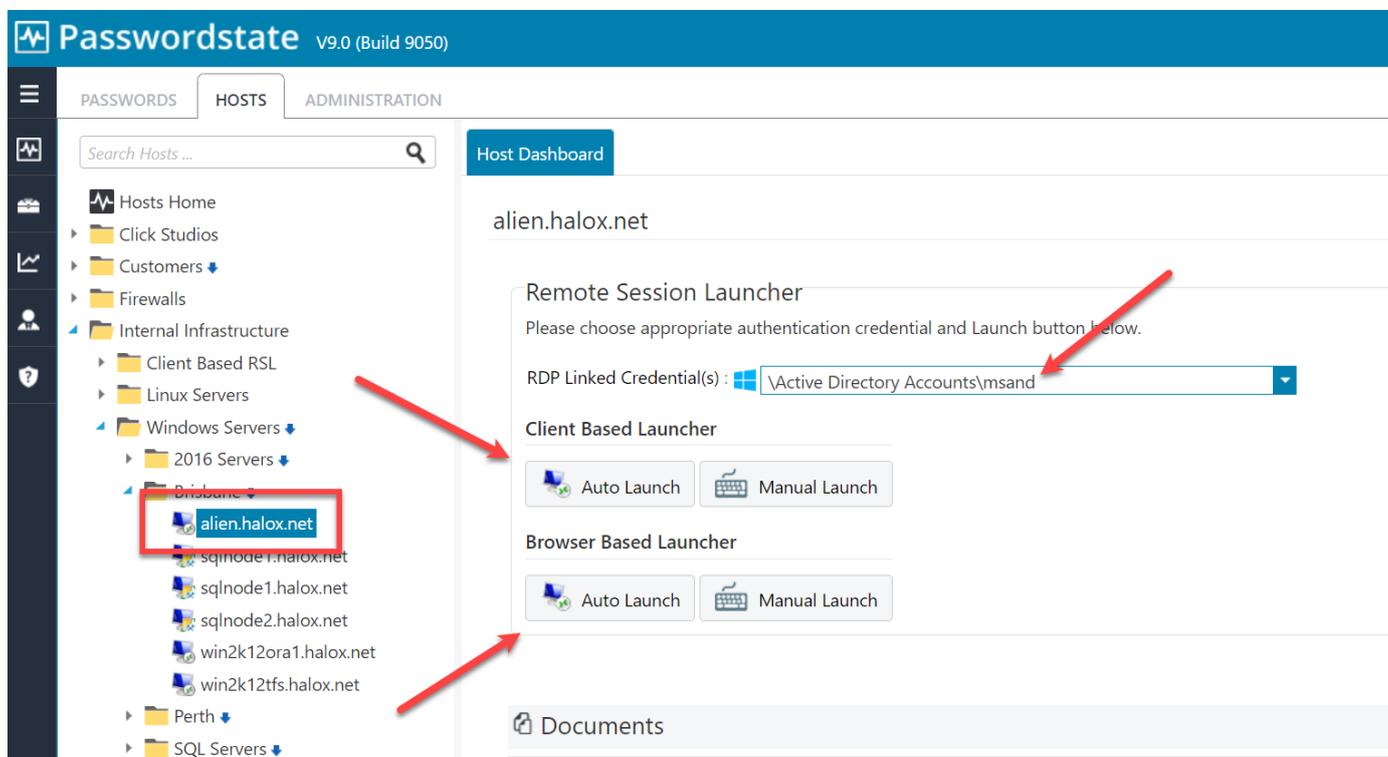
If you use this Remote Site Locations module, it's possible to install the Browser Based Remote Session Launcher on the same network. This allows you to perform RDP and SSH sessions within that remote network over the internet.



To set this up, please follow the section called “**Install Browser Based Remote Session Launcher on Remote Site**” in this manual: https://www.clickstudios.com.au/downloads/version9/Passwordstate_Agent_Manual.pdf

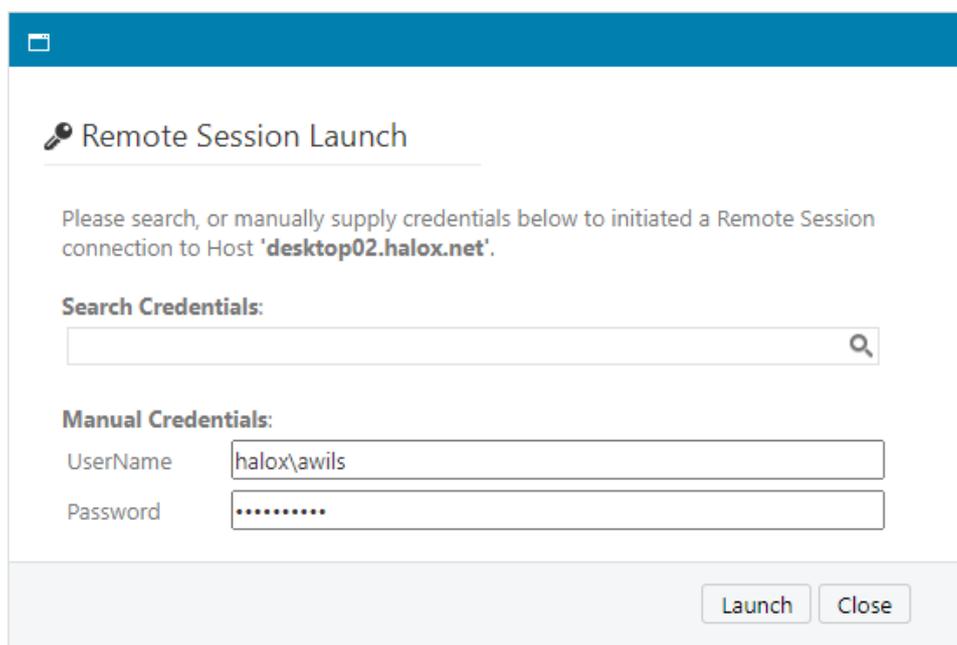
5 How to Launch a Remote Session

Once you have everything set up, launching a session using either of the Launchers is very easy. The primary way is to click on a host, and select the **Auto Launch** button. In the example below, we'll be connecting into **alien.halox.net** with an account called "msand" which is a Windows Domain account.



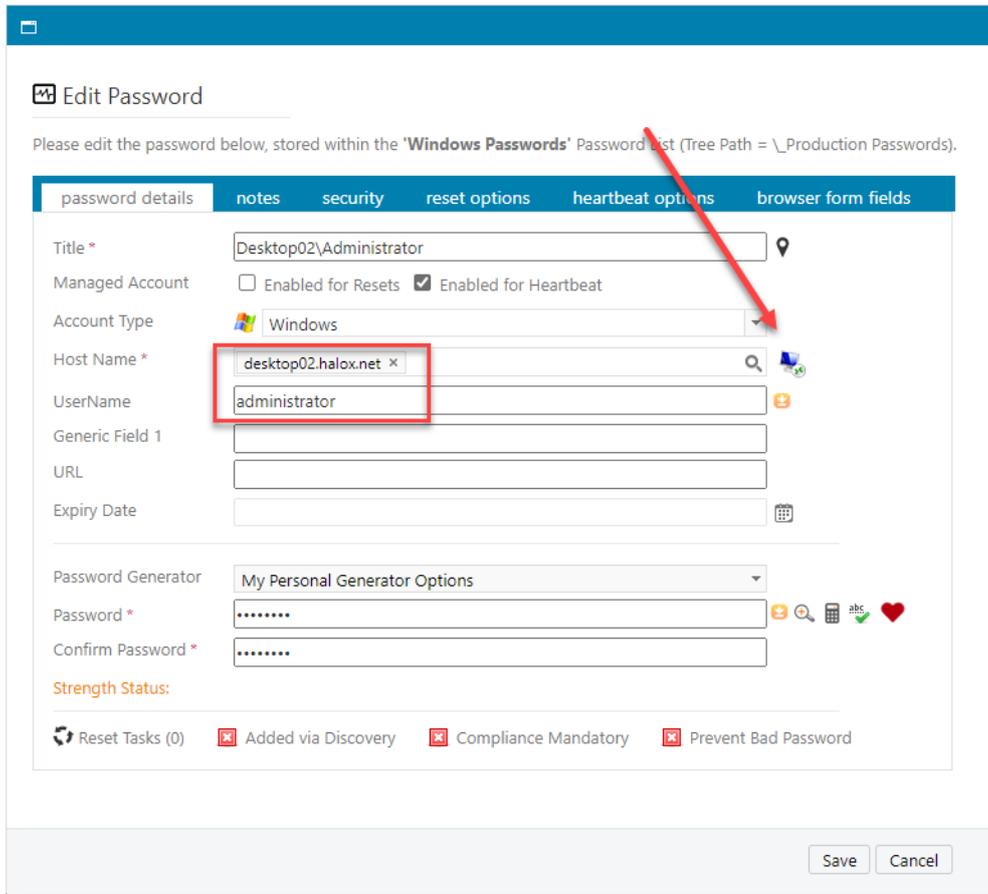
Alternatively, you can click the Manual Launch button instead, which will allow you to enter your credentials if you do not have them already saved in Passwordstate, or you do not have them linked via a Remote Session Launcher:

When entering credentials enter them in the format of **domain\username** for domain accounts, or just **username** for local accounts to the Host.



Click Studios

Another way to establish an automatic connection is directly from within a Password Record. By clicking this icon below, it will connect into the Host using a local account on the machine, in this example we'll be connecting to a host called **Desktop02.halox.net**, but using the Local **Administrator** account:



Edit Password

Please edit the password below, stored within the 'Windows Passwords' Password List (Tree Path = _Production Passwords).

password details | notes | security | reset options | heartbeat options | browser form fields

Title * Desktop02\Administrator

Managed Account Enabled for Resets Enabled for Heartbeat

Account Type Windows

Host Name * desktop02.halox.net

UserName administrator

Generic Field 1

URL

Expiry Date

Password Generator My Personal Generator Options

Password *

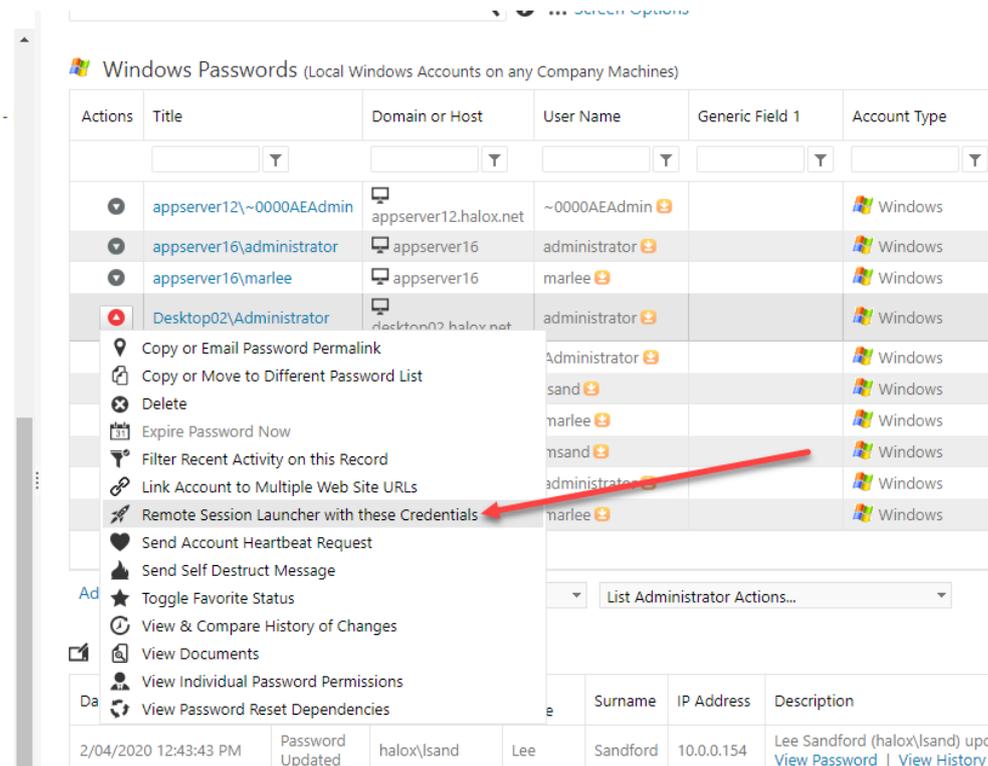
Confirm Password *

Strength Status:

Reset Tasks (0) Added via Discovery Compliance Mandatory Prevent Bad Password

Save Cancel

A second option to launch a session directly from a password record, is from the Actions Menu. Here we are launching into the same machine, with the same Administrator account:



Windows Passwords (Local Windows Accounts on any Company Machines)

Actions	Title	Domain or Host	User Name	Generic Field 1	Account Type
	appserver12\~0000AAdmin	appserver12.halox.net	~0000AAdmin		Windows
	appserver16\administrator	appserver16	administrator		Windows
	appserver16\marlee	appserver16	marlee		Windows
	Desktop02\Administrator	desktop02.halox.net	administrator		Windows
	Administrator		Administrator		Windows
	sand		sand		Windows
	marlee		marlee		Windows
	msand		msand		Windows
	administrator		administrator		Windows
	marlee		marlee		Windows

Copy or Email Password Permalink

Copy or Move to Different Password List

Delete

Expire Password Now

Filter Recent Activity on this Record

Link Account to Multiple Web Site URLs

Remote Session Launcher with these Credentials

Send Account Heartbeat Request

Send Self Destruct Message

Toggle Favorite Status

View & Compare History of Changes

View Documents

View Individual Password Permissions

View Password Reset Dependencies

List Administrator Actions...

2/04/2020 12:43:43 PM Password Updated halox\lsand Lee Sandford 10.0.0.154 Lee Sandford (halox\lsand) upd

[View Password](#) | [View History](#)

6 Adding Hosts into Passwordstate

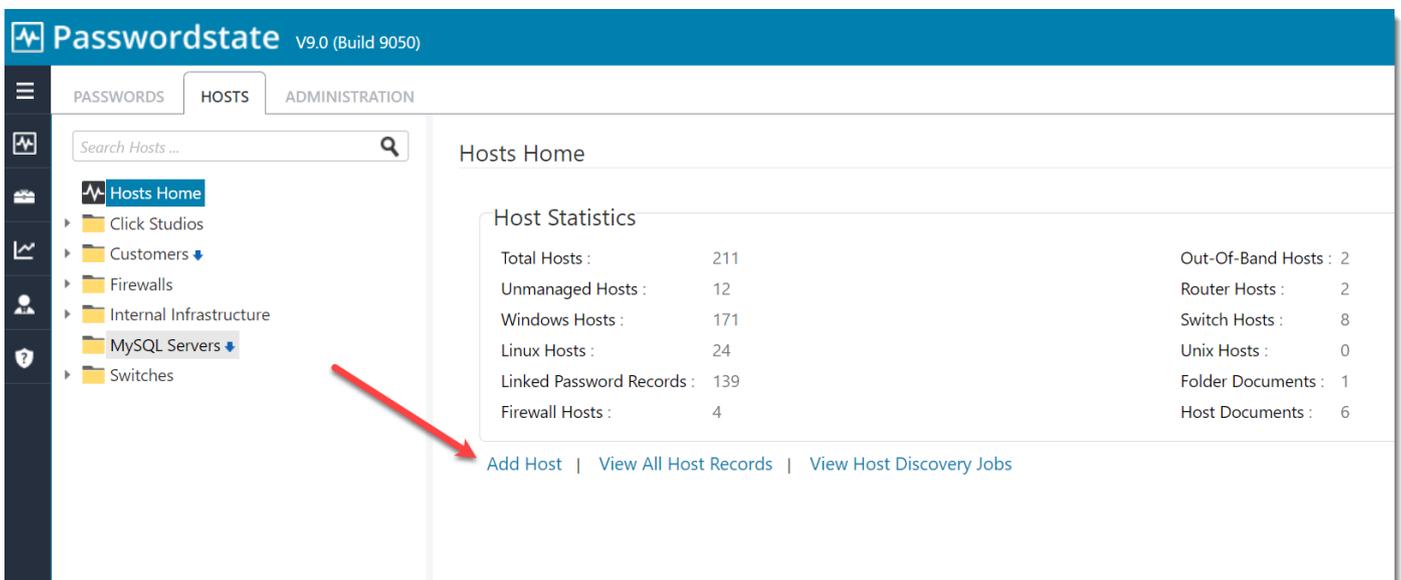
In our software a “**Host**” can be any type of Server, Desktop, Laptop, or other devices such as a Firewall or a Switch. In order to make connections to Hosts, you must first have the Host added into Passwordstate.

There are a few different methods on how to add Hosts:

1. Manually add them one by one
2. Import them from a csv file in bulk through the User Interface
3. Add them automatically on a schedule by a Host Discovery job
4. Add them via the Passwordstate API

6.1 Manually Adding Hosts

To add them manually, select the **Add Host** option under **Hosts tab** -> **Hosts Home**:



Host Statistics

Total Hosts :	211	Out-Of-Band Hosts :	2
Unmanaged Hosts :	12	Router Hosts :	2
Windows Hosts :	171	Switch Hosts :	8
Linux Hosts :	24	Unix Hosts :	0
Linked Password Records :	139	Folder Documents :	1
Firewall Hosts :	4	Host Documents :	6

[Add Host](#) | [View All Host Records](#) | [View Host Discovery Jobs](#)

When adding in a host manually, there are many different options you can set, but the most important ones that you'll need to configure to perform a remote session to it are the Host Name, the Host Type and the Connection Type:

To add a new Host, please fill in the details below.

host details notes

Please specify details for the Host as appropriate.

General Host Properties

Host Name: *
Fully Qualified Domain Name (FQDN) provides greater flexibility and performance, or NetBIOS name can be used if needed.

Title:

Tag:
Can be any descriptive Tag you want, which is also included in Host search results.

Site Location:

Host Type: *

Operating System: *

Internal IP:

External IP:

MAC Address:

Session Recording: * Yes No (record all remote sessions for this Host)

Virtual Machine: * Yes No

Virtual Machine Type: Amazon Azure Google Cloud HyperV VirtualBox VMware Xen

Database Server Type:

Database Instance:

Database Port Number:
This is for an SQL Server Instance, or Oracle Service Name if required.

Host Heartbeat: Hour Minute (time each day a Heartbeat is executed)

Remote Connection Properties

By specifying appropriate settings below, this will allow a remote connection to the host directly from within Passwordstate.

Connection Type * RDP SSH Teamviewer Telnet VNC

Port Number *

Additional Parameters

The parameters below will be passed to the Passwordstate Remote Session Launcher, in an encrypted format. If the client you're using for Remote Sessions requires additional command line parameters to function, you can specify them above.

Parameters Passed : Host Name, Port Number, UserName and Password

Save Save & Add Another Cancel

6.2 Adding Hosts in Bulk via CSV File

Importing in bulk via a csv file can be initiated from **Hosts Home** -> **View All Hosts Records** -> **Import**. This process will generate a csv file for you, which you'll need to populate with relevant data, save, and then import back into the system.

6.3 Adding Hosts Automatically using a Hosts Discovery Job

A very easy way to import your Hosts into Passwordstate automatically is via a Hosts Discovery Job. These are mainly used for Windows Servers and Desktops, but if you have Linux Servers or other operating systems added into your Active Directory domain as a computer object, it's possible to import these too via a Host Discovery Job.

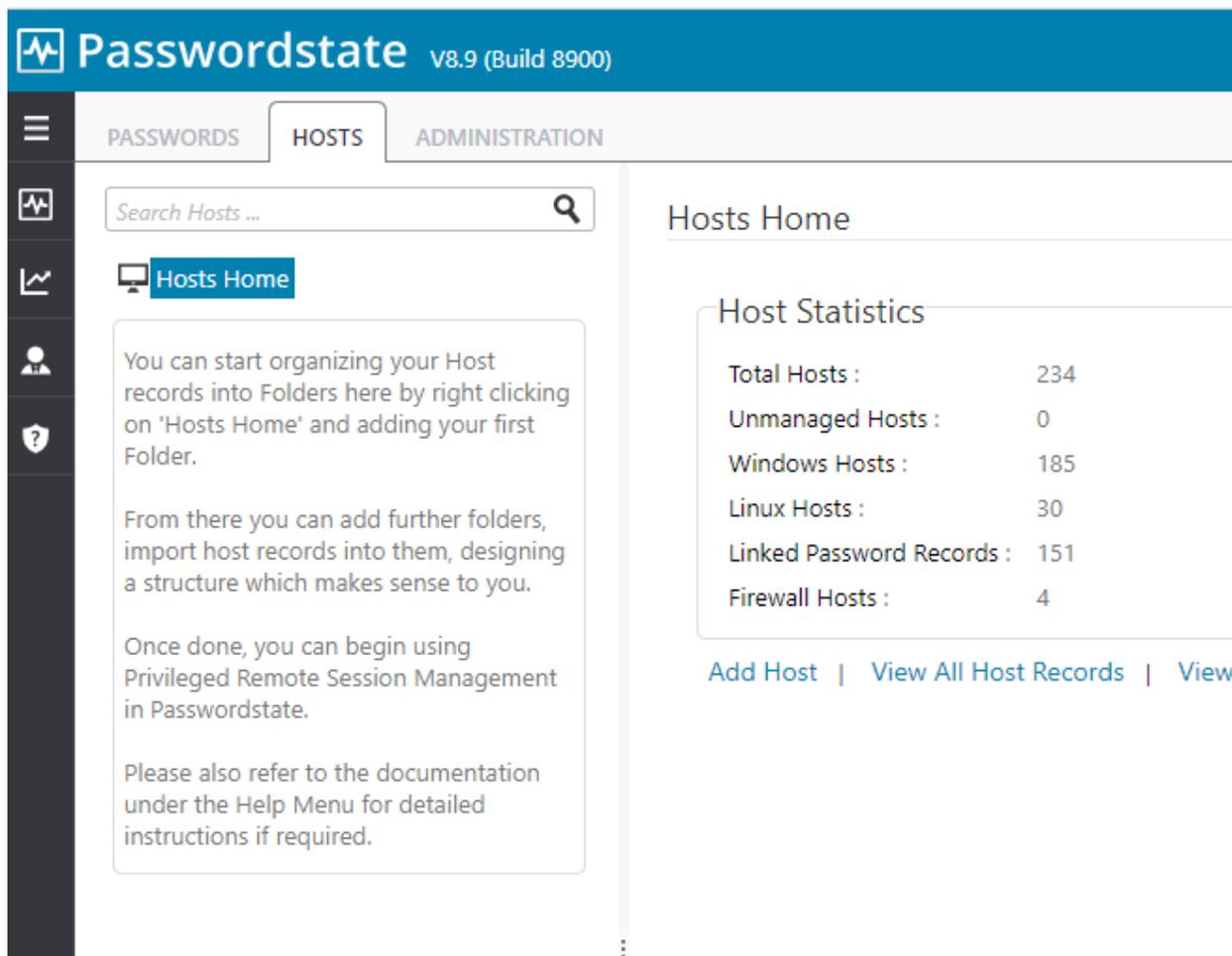
To set up a Hosts discovery job to scan Active Directory and import hosts automatically, please see this tutorial video: <https://www.youtube.com/watch?v=UifVi2rH8x0>

6.4 Adding Hosts via API

Inside Passwordstate, you'll find a manual for our APIs under **Help** -> **Web API Documentation**. In these manuals there is a section for administering Hosts in Passwordstate, which you can use to script the addition of hosts into your system

6.5 Organising Hosts ready for Connections

Now that we have added the Hosts into the system, it's time to begin organising them logically into Folders under the Hosts tab. On your Hosts Home screen, you should see an empty Navigation Tree:



You'll need to create at least one folder by right clicking **Hosts Home** and select **Add Folder**. When adding this Folder, give it a relevant name such as "Windows Servers". If needed you can automatically add Hosts into the Folder based on certain criteria. For example, you could choose Server 2019 machines and if you have tagged your Hosts you could potentially use that information as well. Using this example, all Server 2019 machines that have a matching tag will be added to this folder at the time of creation, and any new Server 2019 machine added to Passwordstate will be added to this folder as well.

Add New Host Folder

To add a new folder, allowing you to organize your Hosts in a structured way, please fill in the details below.

folder details | **guide**

Please specify appropriate details below, then click on the Save Button.

Folder Settings

Site Location *

Folder Name : *

Description :

Permission Model : Propagate permissions from this Folder down to all nested Folders.

Adding Hosts into Folder

When this Folder is created, add Host records into it which match the criteria below. Any new matching Host records added into Passwordstate will also be added to this Folder.

Host Name or Title Match :

Tag Match :

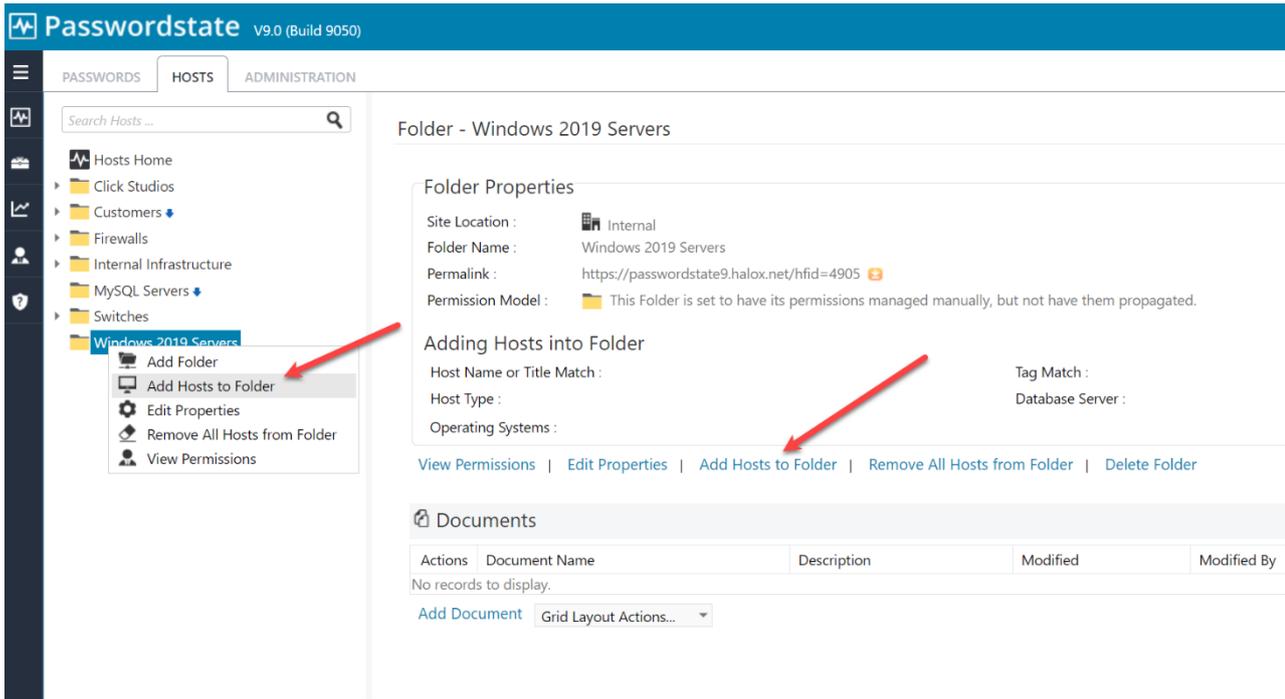
Separate search terms with a semicolon.

Host Type : Operating System : Database Server Type :

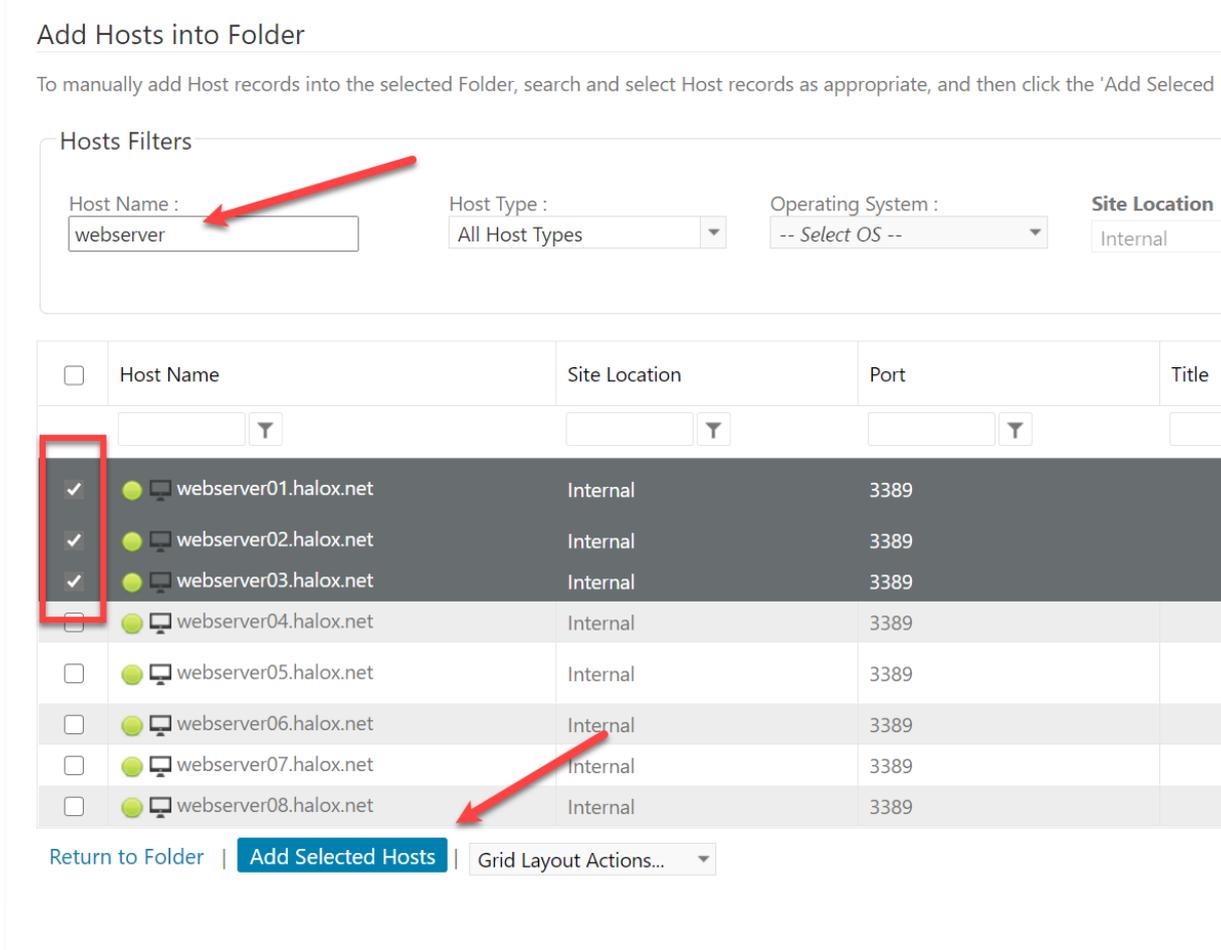
(Hosts in this Folder will only be added based on matching Site Location above)

Save Save & Add Another Cancel

For now, we'll create an empty Folder, so we can demonstrate how to manually add Hosts into this folder. To manually add Hosts to a Folder, select one of these options:



Now find the Host/s you want, and select this option to add them into the Folder:



If you'd like to share this Folder out with another colleague, or any other Passwordstate user, use the **View Permissions** button to add them in:

Folder - Windows 2019 Servers

Folder Properties

Site Location : Internal
Folder Name : Windows 2019 Servers
Permalink : https://passwordstate9.halox.net/hfid=4905
Permission Model : This Folder is set to have its permissions managed manually, b

Adding Hosts into Folder

Host Name or Title Match :
Host Type :
Operating Systems :

[View Permissions](#) | [Edit Properties](#) | [Add Hosts to Folder](#) | [Remove All Hosts from Folder](#)

Documents

Actions	Document Name	Description
No records to display.		

[Add Document](#) Grid Layout Actions...

7 Remote Session Credentials

Now that we have the Hosts entered into the system, we need to set up credentials which will be used to connect into the Hosts. Primarily we do this by way of a Remote Session Credential, and we use one Remote Session Credential to connect to multiple Hosts if desired, or we can filter them to only be used to log into specific Hosts.

In the example below, we'll set up a Remote Session Credential that uses an Active Directory Domain account. This domain account has enough permissions to RDP into any Windows Server on the network.

7.1 Adding a Password Record

First, you'll need to create a Password Record, that is in a Password List that is enabled for resets (However you can untick the **“Enabled for Resets Option”** on the record if you do not want Passwordstate to automatically reset this account's password on a schedule).

Choose the account type as Active Directory, and set the **Domain**, **Username** and **Password** for this account. If you want to confirm the password is in sync with Active directory, click the **Heartbeat** icon.

☐

Add New Password

Add new password to **'Windows Admin Accounts'** Password List (Tree Path = \).

password details	notes	security	reset options	heartbeat options
Title *	<input type="text" value="Shared Admin Account"/>			
Managed Account	<input checked="" type="checkbox"/> Enabled for Resets <input checked="" type="checkbox"/> Enabled for Heartbeat			
Account Type	👤 <input type="text" value="Active Directory"/>			
Domain *	<input type="text" value="halox"/> ✕ 🔍			
UserName	<input type="text" value="pws_windows"/> ⬇️			
Description	<input type="text"/>			
Expiry Date	<input type="text"/> 📅			
Password Generator	<input type="text" value="My Personal Generator Options"/>			
Password *	<input type="password" value="....."/> ⬇️ 🔍 📱 abc ✅ ❤️			
Confirm Password *	<input type="password" value="....."/>			
Password Strength	★★★★☆ Compliance Strength ★★★★★			
Strength Status: 1 symbol characters				
<input checked="" type="checkbox"/> Compliance Mandatory <input checked="" type="checkbox"/> Prevent Bad Password Usage				

Save
Save & Add Another
Cancel

7.2 Adding a Remote Session Credential

After creating a Password Record, go to **Hosts tab** -> **Hosts Home** and select **Add Credential**.

On this screen you should give your credential a **Description**, choose what type of **Connections** it can make, and link it to the password record we created in the step above (****Hint**** - Start typing the username in the **Link To Credential field**):

query properties | query results

Any Hosts which match the query details below will use the selected Password record for Remote Session authentication.

Remote Session Query Properties

Description: *

Include Host Name Match:

Exclude Host Name Match:

Site Location *

Host Type(s):

Operating System(s):

Connection Type RDP SSH Teamviewer Telnet VNC SQL Server

Link To Credential: *

Save Cancel

Note: On this page you can filter on which Hosts this Remote Session Credential can connect to with wildcard matches by using the **“Include Host Name Match”** or the **“Exclude Host Name Match”** fields.

To quickly see which Hosts this credential can connect into, click the **“Query Hosts”** tab under the Query Results tab:

🔑 Edit Remote Session Credential Query

Please update details for the Remote Session Credential query below as appropriate, and test the query on the 'Query Results' tab.

query properties | query results

To see the results of the query properties, please click this button

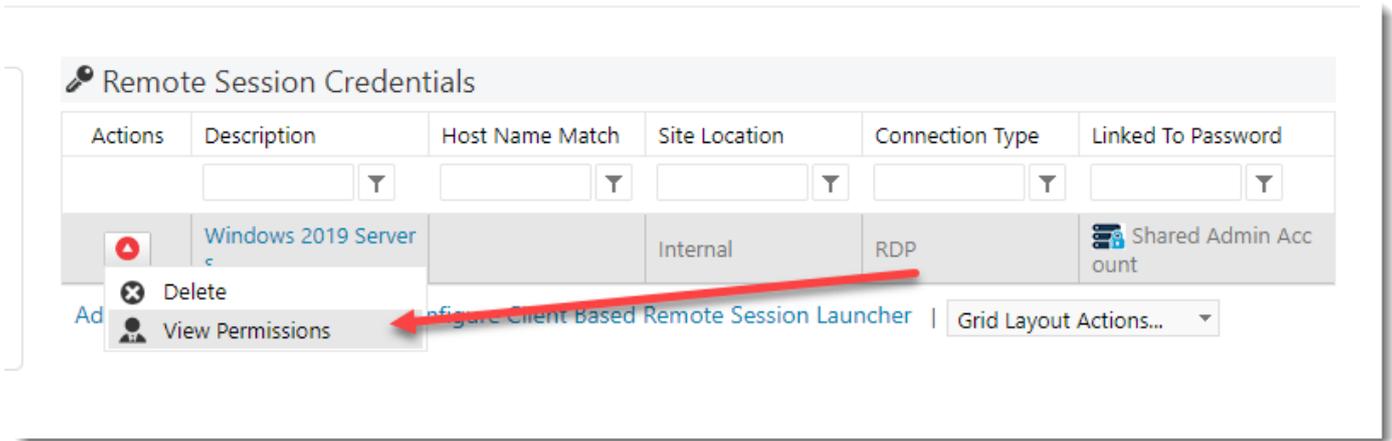
Host Name

- appserver06.halox.net
- appserver12.halox.net
- appserver13.halox.net
- appserver13appserver12.halox.net
- daserver01.halox.net
- dcserver01
- dcserver02.halox.net
- doserver01.halox.net
- exserver01.halox.net
- hyperv0.halox.net
- passwordstate01.australiaeast.cloudapp.azure.com

Save Cancel

7.3 Sharing out a Remote Session Credential

If you want to share this Remote Session Credential out, so other team members can also use it to connect into Hosts, you can do so via the **Actions** menu:



One benefit of sharing out Remote Session Credentials like this, is the user does not need to have access to the password record that it is linked to. This means those users can use this Remote Session Credential to connect to your Hosts, but they will not even know the password they are using to connect in with.

This feature is useful if you have contractors on site with a requirement to remote into different machines. As they do not know the password they are authenticating with, there is no need to reset account passwords when the contractor leaves.

If the contractor attempts to edit the Remote session Credential, the Save button will be disabled as they do not have access to the Password Record it is linked to:

Edit Remote Session Credential Query

Please update details for the Remote Session Credential query below as appropriate, and test the query on the 'Query Results' tab.

query properties | query results

Any Hosts which match the query details below will use the selected Password record for Remote Session authentication.

Remote Session Query Properties

Description: * Private Credential

Include Host Name Match:

Exclude Host Name Match: *cloudapp*

Site Location * Internal

Host Type(s): Windows

Operating System(s): -- Operating Systems Filter --

Connection Type RDP SSH Teamviewer Telnet VNC SQL Server

Save Cancel

7.4 Time-Based Access to Remote Session Credentials

When applying permissions via the Actions menu in the **Section 6.3** above, you are also able to set an expiry date so access will be automatically removed when your contactor leaves:

Remote Session Credential Permissions

Please apply permissions for who can use the Remote Session Credential **Private Credential**.

remote session credential permissions | time based access

To set an expiry date and type for the selected Remote Session Credential permission, please use the appropriate options below.

Access Expires :

Never

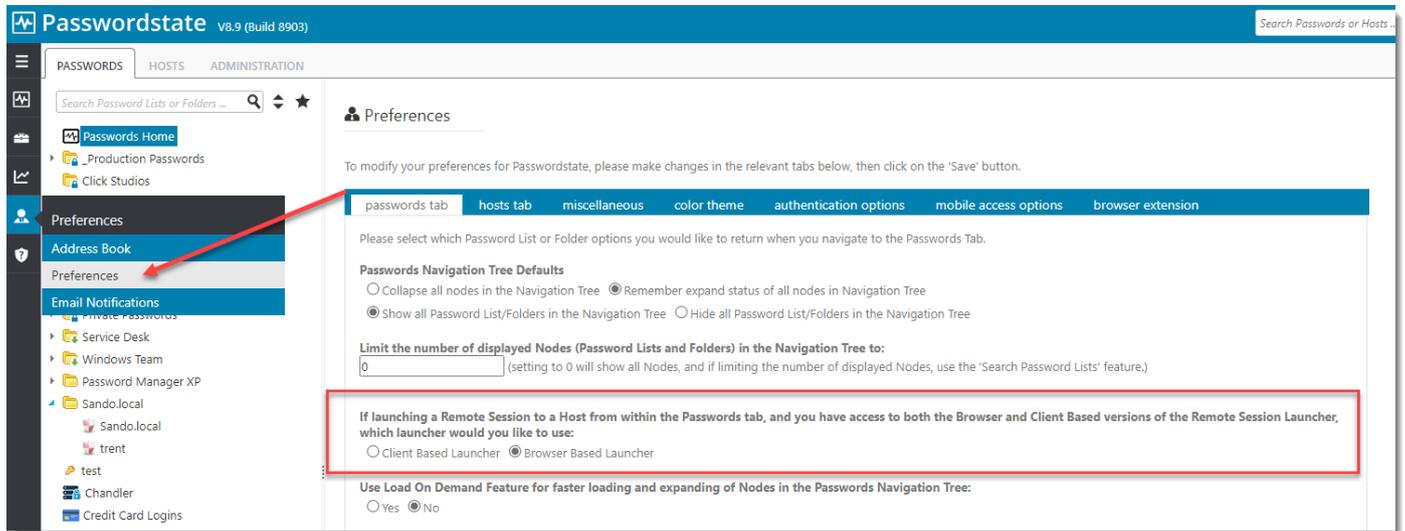
In: Days: Hours: Minutes:

At: Date: Time:

Status: Save Cancel

8 Personal Preferences

Under your personal **Preferences**, which can be accessed from the Menu pane on the left-hand side of your web page, or by clicking your name in the top right-hand corner, you can choose which Remote Session Launcher to use if launching from inside a Password Record:



The Browser Based Launcher also includes support for multiple different keyboard layouts. It's possible to change your keyboard layout under Preferences -> Miscellaneous:



9 Administration: Feature Access

As a Security Administrator of Passwordstate, you are able to control how the Remote Session Launcher behaves. There are a number of settings under **Administration -> Feature Access -> Remote Sessions**

On this page you can configure things such as who can and can't use the Remote Session Launchers, who will have their session recorded, or possibly even control who can manage Remote Session Credentials.

We'd encourage you to as a Security Administrator to browse through this page, and assess whether you will use any of these settings in your environment.

10 Session Recording

One of the features that you can use with the Browser Based Launcher is **Session Recording**. This will record the screen so an appropriate person in your company can later play it back to review what work a particular person has performed whilst in a remote session.

An example of when you might want to use this is if you have a contractor coming on site to perform some work for you, you can advise them ahead of time that their work will be recorded. This can be handy if you need to get video footage of their work for documentation purposes, or maybe even if you need to have evidence of what work was actually performed.

You can control who has their sessions recorded under **Administration -> Feature Access -> Remote Sessions** by configuring this setting below (By default no one has their sessions recorded)

Specify which users will have their sessions recorded, for later playback if required: (Browser Based Remote Session Launcher only)

Record Sessions For Selected Users

You can also choose whether or not to display a warning that the session will be recorded by enabling this option on the same page:

Do you want to display a Session Recording warning to users so they know their remote sessions are being recorded:

Yes No

If you turn on the warning for the user, they will see this message before they attempt to connect:

desktop02.halox.net

Remote Session Launcher

Please choose appropriate authentication credential and Launch button below.

RDP Linked Credential(s) :  \Remote Session Launcher Accounts\lsand

Client Based Launcher

 Auto Launch  Manual Launch

Browser Based Launcher  Your sessions will be recorded

 Auto Launch  Manual Launch



If you would prefer to record all sessions for a specific Host, rather than per user, you can set this option on the Host when editing it:

Host Dashboard

Edit Host

Please make changes below for the selected Host as appropriate, then click on the 'Save' button.

host details notes

Please specify details for the Host as appropriate.

General Host Properties

Host Name: * desktop02.halox.net
Fully Qualified Domain Name (FQDN) provides greater flexibility and performance, or NetBIOS name can be used if needed.

Title:

If the Title field has a value, this will be displayed in the Hosts Navigation Tree instead.

Tag: OU=Windows Servers,OU=Sandbox Testing,DC=halox,DC=net
Can be any descriptive Tag you want, which is also included in Host search results.

Site Location: Internal

Host Type: * Windows

Operating System: * Windows 10

Internal IP:

External IP:

MAC Address:

Session Recording: * Yes No (record all remote sessions for this Host)

Virtual Machine: * Yes No

Virtual Machine Type: Amazon Azure HyperV Google Cloud VirtualBox VMware Xen

Database Server Type: -- Select Database Server Type --

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.

Note: If you are using the High Availability module for Passwordstate, it is recommended you save recorded sessions to a Network 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.

gateway settings

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:

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:
 

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 * :

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

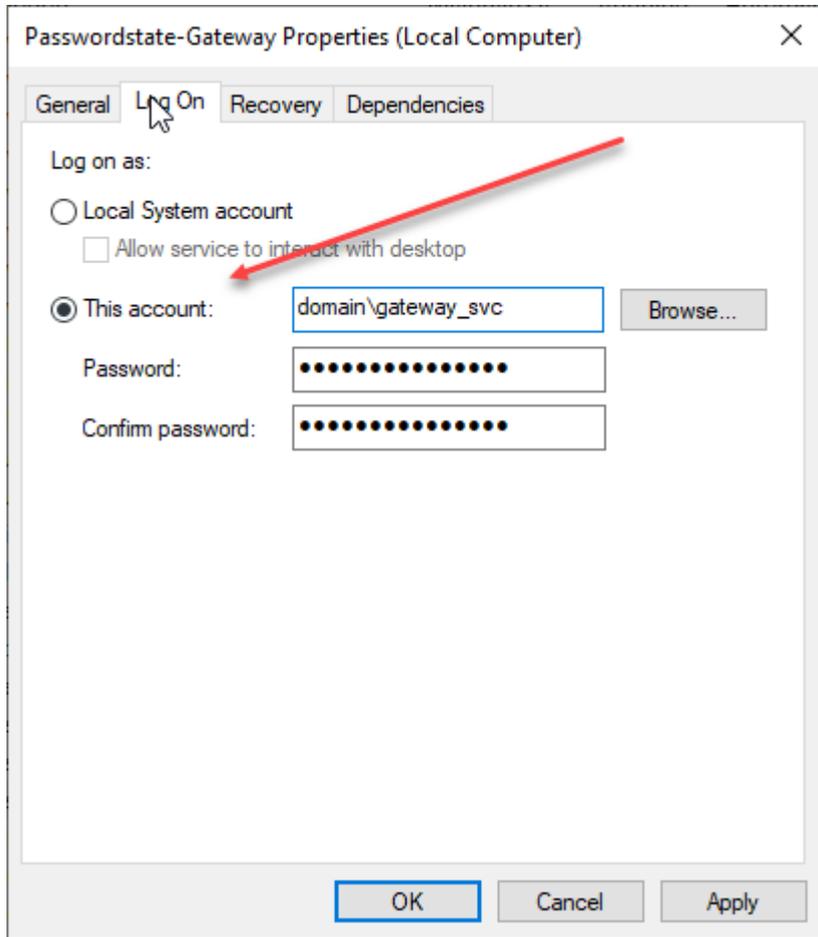
When storing session recordings using the default rec value, the NTFS permissions are already correct.

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.

Click Studios

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.



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.

To play back the recorded session, navigate to **Administration -> Remote Session management -> Recorded Sessions** and from this page you can watch the video within your browser by clicking on the Media button, or you can delete the session from the Actions Menu:

▶ Remote Session Recordings

Below are all the saved recorded Remote Sessions, which you can playback by pressing the appropriate Play button.

Actions	Date	Host Name Match	Remote Connection Type	Initiated By	Authenticating Account	File Name	In Progress	Site Location	IP Address	Duration	Playback
	28/05/2019 12:23:06 PM	hyperv0.halox.net	RDP	halox\lsand	halox\lsand	/20190528/hyperv0.halox.net_lsand.rdpv		Internal	10.0.0.85		
	30/05/2019 9:05:02 AM	webserver01.halox.net	RDP	halox\lsand	halox\lsand	/20190530/webserver01.halox.net_lsand.rdpv		Internal	10.0.0.85		
	30/05/2019 9:09:31 AM	dcserver01	RDP	halox\lsand	halox\lsand	/20190530/dcserver01_lsand.rdpv		Internal	10.0.0.85		
	30/05/2019 11:11:39 AM	hyperv0.halox.net	RDP	halox\lsand	halox\lsand	/20190530/hyperv0.halox.net_lsand.rdpv		Internal	10.0.0.85		
	Delete										
	Mark Recording as Complete	ip01.halox.net	RDP	halox\lsand	halox\lsand	/20190530/desktop01.halox.net_lsand.rdpv		Internal	10.0.0.85		
	30/05/2019 2:46:17 PM	exserver01.halox.net	RDP	halox\lsand	halox\lsand	/20190530/exserver01.halox.net_lsand.rdpv		Internal	10.0.0.85		
	3/06/2019 8:07:48 AM	alienm15.halox.net	RDP	halox\lsand	halox\lsand	/20190603/alienm15.halox.net_lsand.rdpv		Internal	10.0.0.85		
	3/06/2019 9:51:20 AM	webserver01.halox.net	RDP	halox\lsand	halox\lsand	/20190603/webserver01.halox.net_lsand.rdpv		Internal	10.0.0.85		
	14/06/2019 7:12:23 AM	hyperv0.halox.net	RDP	halox\lsand	halox\lsand	/20190614/hyperv0.halox.net_lsand.rdpv		Internal	10.0.0.153		

11 SQL Server Connections

The Client Based Remote Session Launcher is capable of establishing automatic connections with SQL database servers. It's possible to connect with a domain account, or a local SQL account.

We have a training video for this, which explains how to set this up, and launch a SQL session:

<https://www.youtube.com/watch?v=4RnzHkI-k0o>

In order to perform Remote Sessions for SQL Server, you need to have the SQL Server Management Studio installed on your PC where you are accessing Passwordstate from.

Source files for SQL Server Management Studio can be found here: <https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver15>

 Note: Microsoft have removed the ability to pass a SQL Server account password value to SQL Server Management Studio via the command line, in SQL Management Studio 2018. Authenticating with Active Directory accounts works with Management Studio 2018 and above, but if you wish to use Local SQL Accounts you will instead need to use SQL Management Studio 2017.

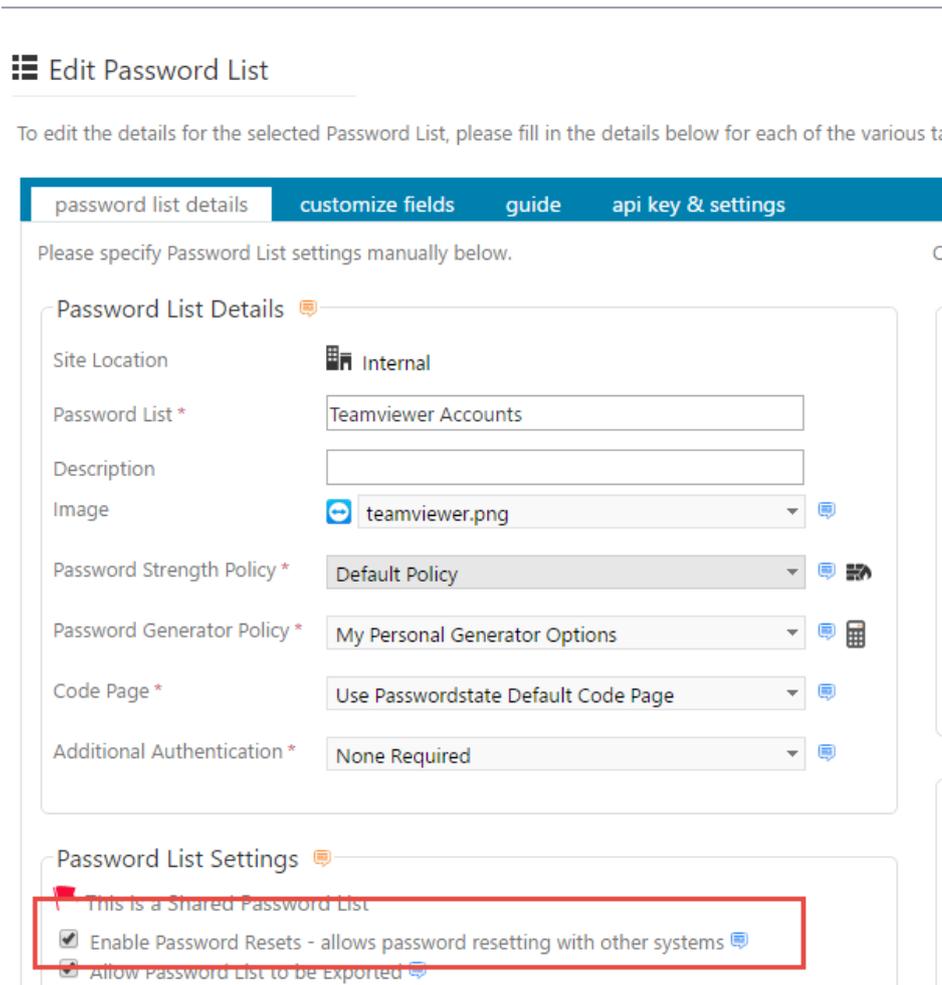
If you need to download SQL Server Management Studio 2017, see this link: <https://docs.microsoft.com/en-us/sql/ssms/release-notes-ssms?view=sql-server-2017#previous-ssms-releases>

12 TeamViewer Connections

If you use TeamViewer to do Remote Sessions over the internet, it's possible to launch these sessions automatically using our Remote Session Launcher. You must have TeamViewer installed on the computer you are accessing Passwordstate from, and source files for this software can be found here: <https://www.teamviewer.com/en/>.

You'll also need to ensure the remote machine you are connecting into has Teamviewer installed and set up for unattended access. This ensures you have a static password configured for the remote TeamViewer machine.

Next, ensure you have a Password List created for your TeamViewer Credentials, with the **“Enable Password Resets”** option enabled:



Next, we'll add in a Password Record with the following configuration:

Deselect the 'Managed Account' options, select the 'Teamviewer' Account Type, lookup the appropriate Host, and specify the TeamViewer ID as the Username field – like in the screenshot below.

The screenshot shows the 'Edit Password' interface with the following configuration:

- Title: skyfrac\123571499
- Managed Account: Enabled for Resets Enabled for Heartbeat
- Account Type: Teamviewer
- Host Name: skyfrac.halox.net
- UserName: 123571499
- Password Generator: My Personal Generator Options
- Password: [Redacted]
- Confirm Password: [Redacted]
- Strength Status: 1 symbol characters
- Reset Tasks (0)
- Added via Discovery
- Compliance Mandatory
- Prevent Bad Password

🚩 The reason we need to configure the Password List and Password record in this manner, as we need the Remote Session Credentials to be able to find a match against the Host Name and UserName field in the password record itself. This is the only way currently to guarantee this sort of accuracy with the match.

The Host you are connecting to must have the **TeamViewer** option selected:

 Edit Host

Please make changes below for the selected Host as appropriate, then click on the 'Save' button.

host details | **installed software**

Please specify details for the Host as appropriate.

General Host Properties

Host Name: *
Fully Qualified Domain Name (FQDN) provides greater flexibility and performance, or NetBIOS name can be used if needed.

Tag:
Can be any descriptive Tag you want, which is also included in Host search results.

Site Location:

Host Type: *

Operating System: *

Internal IP:

External IP:

MAC Address:

Virtual Machine: * Yes No

Virtual Machine Type: Amazon Azure HyperV VirtualBox VMware Xen

Database Server Type: SQL Server MySQL Server Oracle Server

Database Instance:
This is for an SQL Server Instance, or Oracle Service Name if required.

Database Port Number:
If using default ports, blank values will generally work here.

Host Heartbeat: Hour Minute (time each day a Heartbeat is executed)

Remote Connection Properties

By specifying appropriate settings below, this will allow a remote connection to the host directly from within Passwordstate.

Connection Type * RDP SSH Teamviewer Telnet VNC

Port Number *

Additional Parameters
The parameters below will be passed to the Passwordstate Remote Session Launcher, in an encrypted format. If the client you're using for Remote Sessions requires additional command line parameters to function, can specify them above.

Parameters Passed : Host Name, Port Number, UserName and Password

Now you'll need to set up a Remote Session Credential, from under the **Hosts** tab -> **Hosts Home** screen. When creating this Remote Session Credential, you only need to select the **"TeamViewer"** Connection Type, and are not required to link it to any Password Record

Edit Remote Session Credential Query

Please update details for the Remote Session Credential query below as appropriate, and test the query on the 'Query Results' tab.

query properties | **query results**

Any Hosts which match the query details below will use the selected Password record for Remote Session authentication.

Remote Session Query Properties

Description: *

Include Host Name Match:

Exclude Host Name Match:

Site Location *

Host Type(s):

Operating System(s):

Connection Type RDP SSH Teamviewer Telnet VNC

Best practise recommends having a different Password per Teamviewer Host, so you do not need to link to a Password record here.
- Instead, you need to store all your Teamviewer logins per Host record in a Password List. Refer to the following manual for more instructions: Help -> Remote Session Launcher.

Save Cancel

Now if you click on your Host in the to launch a session, you should notice a new Teamviewer button that you can use to launch the session:

skyfrac.halox.net

Remote Session Launcher

Please choose appropriate authentication credential and Launch button below.

Teamviewer Linked Credential(s) :

Client Based Launcher

Browser Based Launcher

13 SSH With Private Public Key

It is possible to perform SSH connections using Public/Private Key Authentication. The Client Based Launcher works with both Putty and OpenSSH keys, whereas the Browser Based Launcher only works with OpenSSH keys.

To do this, you must configure a Generic Field on a Password List and call it '**Private Key**', and then you can store your private key in this field. When you have a field configured in this manner, then the authentication for the Remote Session Launchers will use this as precedence over the standard password for the user.

If you use the same private key to authenticate against multiple Linux hosts, then you should use a Remote Session Credential for this.

If you have separate private keys for different hosts, then you can authenticate directly from a password record that has the SSH keys configured. You can also use the Manual Launch option when clicking on a Host under the Hosts tab, and search for your Password record there that has the SSH key set. If you choose this option, your Password List where you are storing your credentials to login with must be enabled for resets, and you need to have the Host configured on this password record too. More information about this below

13.1 Password List Requirements for using SSH Keys

In order to create Password Records that you can set your SSH keys with, you must first ensure your Password List has Generic Field configured. This field must be called "Private Key" and it must be Generic Field #1. You should also select this field to be encrypted and the Field Type is Free Text Field (unlimited text).

Hiding the field is also recommended, so your User Interface is not cluttered by lengthy text:

Edit Password List Properties

To edit the details for the selected Password List, please fill in the details below for each of the various tabs.

password list details
customize fields
guide
api key & settings

Below you can specify which fields are available, which ones are required fields, and select one or more Generic Fields and configure their options accordingly.

Standard Fields

Field Name	Required	Hide Column 
<input checked="" type="checkbox"/> Title	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> User Name	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Description	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Account Type	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> URL	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Password	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Password Strength	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Expiry Date	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Notes	<input type="checkbox"/>	<input type="checkbox"/>

Generic Fields (click on Field Names to rename)

Field Name	Required	Encrypt	Hide Column 	Field Type
<input checked="" type="checkbox"/> Private Key	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Free Text Field (unlimited text)
<input type="checkbox"/> Generic Field 2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Text Field
<input type="checkbox"/> Generic Field 3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Text Field

If you have multiple Private Keys for different Hosts, you will need to enable the resets option on the Password List too:

⚙️ Edit Password List Properties

To edit the details for the selected Password List, please fill in the details below for each of the various tabs.

13.2 Creating a Password Record

When creating a Password Record, you should deselect the “**Managed Account**” options. Set the Host name if the SSH Private key is only going to be used for this one machine, otherwise we will create a Remote Session Credential in the next section so the Private Key can be used with multiple Hosts.

The password that you enter on this screen is the Pass Phrase for the Private Key, not the standard user account password:

🔑 Edit Remote Session Credential Query

Please update details for the Remote Session Credential query below as appropriate, and test the query on the 'Query Results' tab.

query properties
query results

Any Hosts which match the query details below will use the selected Password record for Remote Session authentication.

Remote Session Query Properties

Description: *

Include Host Name Match:
Examples are: win2k12server1 (single host), or wildcard matches like win2k12* or ServerName*Win. Multiple hosts matches can be comma separated, and use the 'Query Results' tab to test.

Exclude Host Name Match:
Same query syntax as above, and use the 'Query Results' tab to test.

Site Location *

Host Type(s):

Operating System(s):

Connection Type RDP SSH Teamviewer Telnet VNC

Link To Credential: * 🔍

Now you can launch a session as you would normally, by clicking the Auto Launch button, and if this Remote Session Credential is selected for that session, it will use the Private Key to authenticate.

13.4 Convert Putty Private Key to OpenSSH Format

The Browser Based Launcher will not accept Putty key combinations, so you will need to create a set of OpenSSH keys or you can optionally convert your Putty keys using this process below:

- Download PuTTYgen from here - <https://www.ssh.com/ssh/putty/windows/puttygen#sec-PuTTYgen-download-and-install>
- Open PuttyGen
- Click Load
- Load your private key
- Go to **Conversions->Export OpenSSH** and export your private key, then save back into your password record

14 Client Based Launcher with Microsoft Remote Desktop Gateway

Microsoft's Remote Desktop Gateway (RDG or RD Gateway) is a **Windows Server** role that provides a secure encrypted connection to the server via RDP.

If you have a Microsoft RDP Gateway already set up, you can route your remote sessions directly from your desktop to the Microsoft RDP Gateway – which will then route traffic to the required Host. This is achieved in Passwordstate by modifying your host records and inserting the gateway parameters as per below example.

Remote Connection Properties

By specifying appropriate settings below, this will allow a remote connection to the host directly from within Passwordstate.

Connection Type * RDP SSH Teamviewer Telnet VNC

Port Number *

Additional Parameters

The parameters below will be passed to the Passwordstate Remote Session Launcher, in an encrypted format. If the client you're using for Remote Sessions requires additional command line parameters to function, you can specify them above.

Parameters Passed : Host Name, Port Number, UserName and Password

Save Cancel

If you use the default port of 443 you do not need to append it on the end of your parameter. This port is only used to connect to the Gateway, and then it will use the standard port of 3389 to connect to your remote machine.

Other command line switches such as /Admin will work if you add them in.

- 🚩 **Note 1:** This gateway will only work with Domain accounts, not local Administrator or other Local Windows accounts. Please ensure the credential you set up to remote onto your machine has the account type of **“Active Directory”**
- 🚩 **Note 2:** Routing traffic through Microsoft's RDP Gateway is only possible with Click Studios' Client Based Launcher. It is not possible using our Browser Based Launcher (gateway).

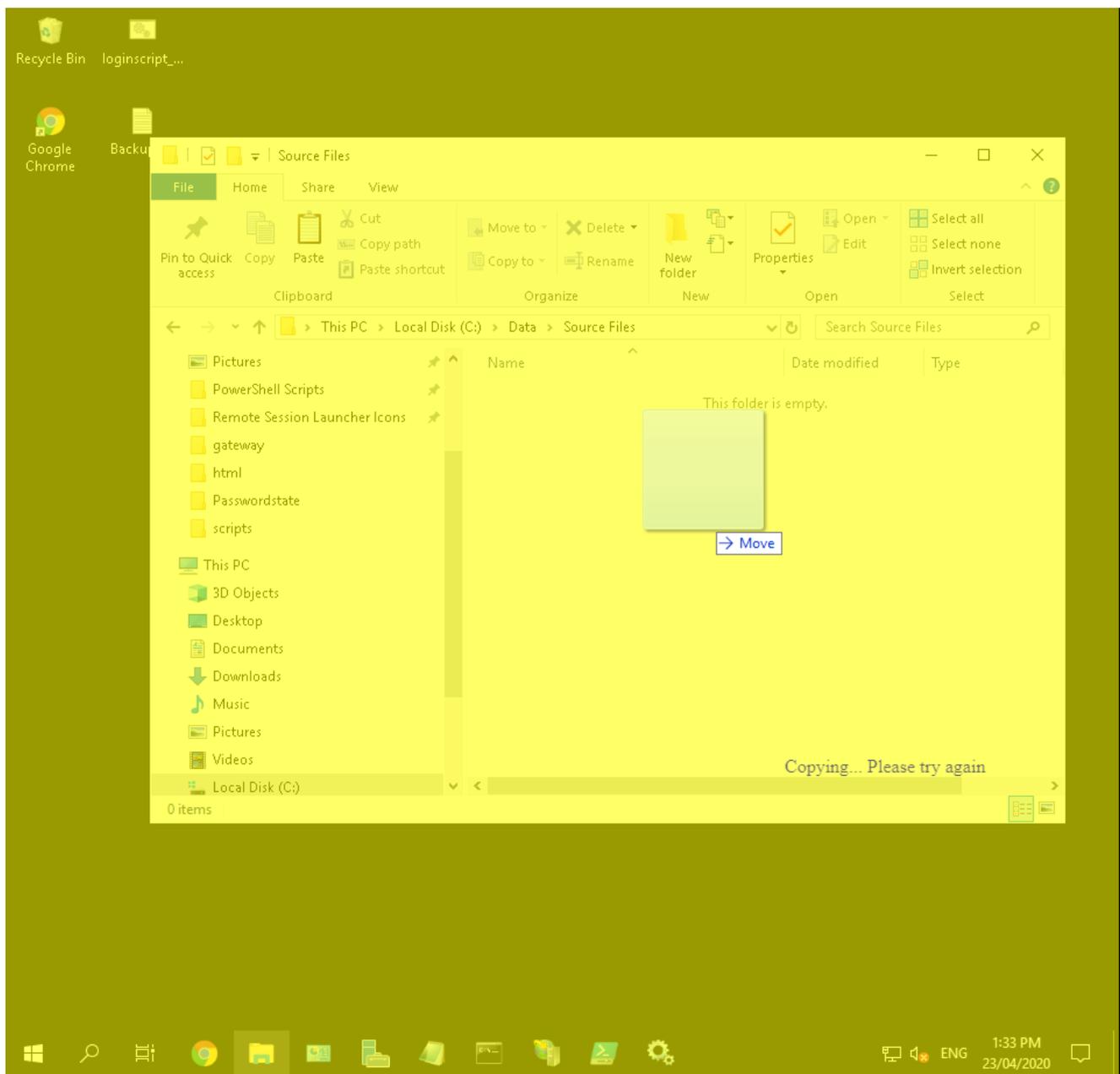
15 File Transfer with Browser Based Launcher

The Browser Based Launcher has the ability to transfer files from your local desktop to the remote machine, or vice versa. This can make data transfer easy instead of mapping drives, or browsing to a UNC path.

File transfer is different depending on if you have an SSH session established, or an RDP session. Below we will explain how we can do both.

15.1 RDP File Transfer

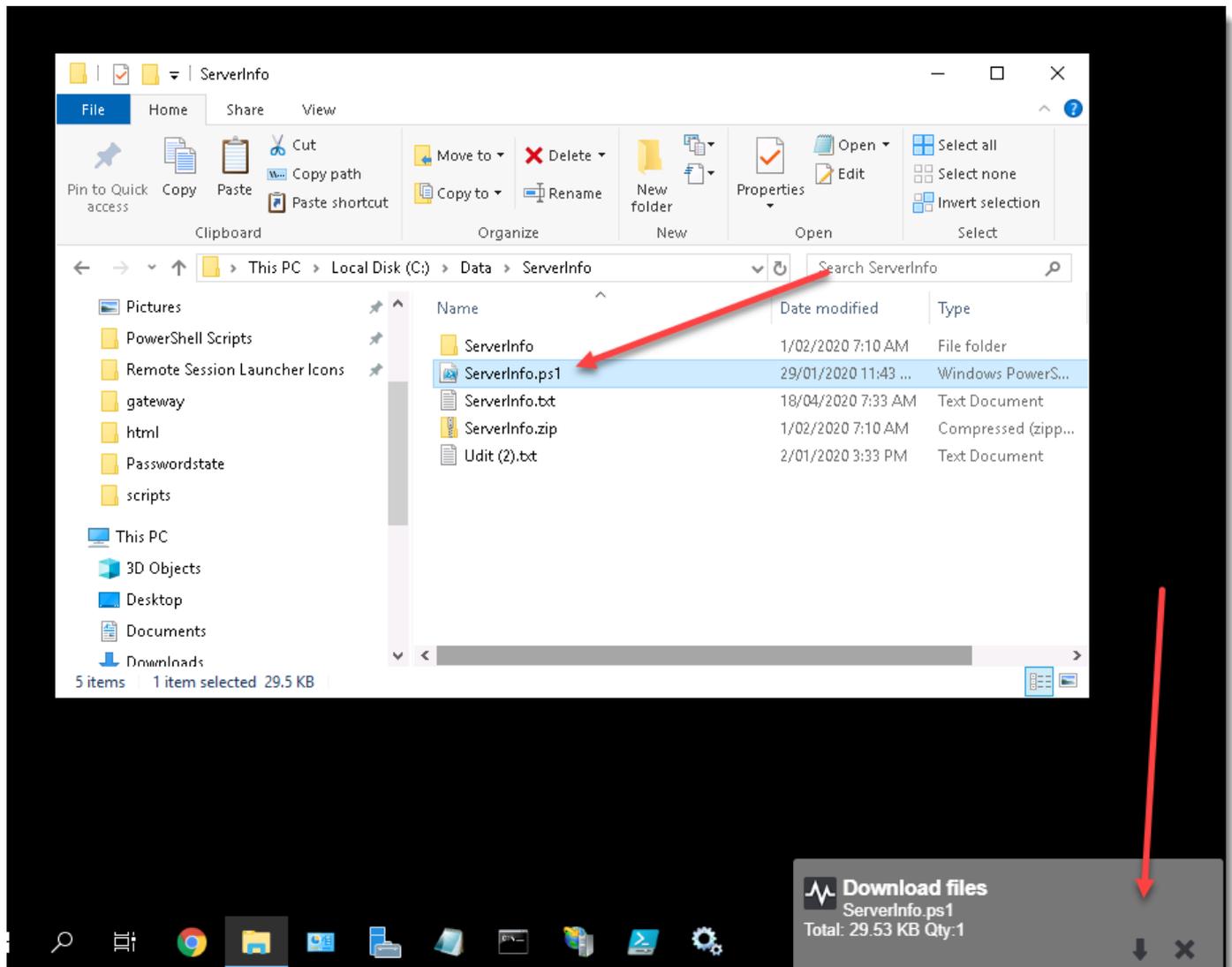
If you drag and drop a file from your local desktop, into a folder inside your RDP session, you'll see the screen turn yellow. When you release the mouse, this will copy the file into that remote folder. The remote folder, which in this below example is "C:\Data\Source Files", need to be the active window in the remote session:



Note: There is a 2GB file limit when transferring files into a remote session

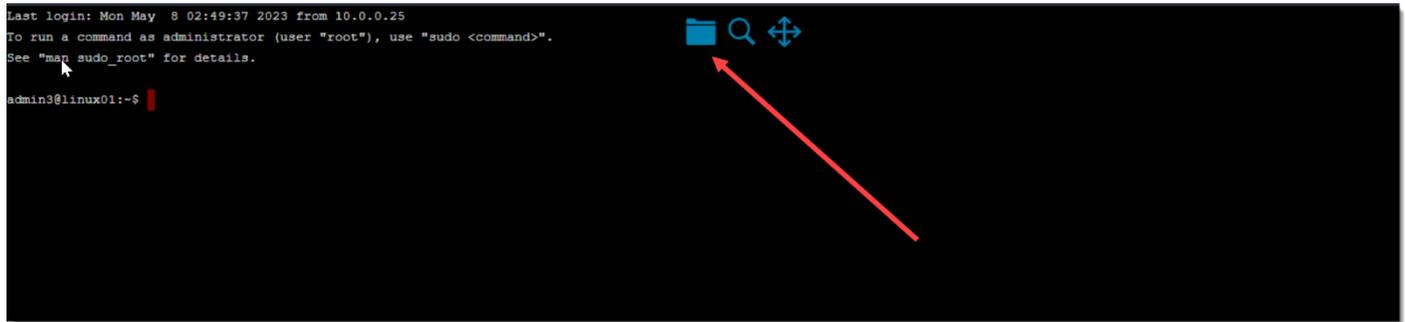
To copy a file out of an RDP session, **Right Click** the file and select **Copy**, and you'll see a pop-up window in the bottom right hand corner of your remote session. This will give you some information about the file you are copying, and you can either cancel the file copy, or click the **Download** button.

When clicking the **Download** button, this will download the file through your local browser to a directory on your local machine. This directory is determined by what you have settings you have configured in your browser, but generally this is your **Downloads** folder inside your **User Profile**.



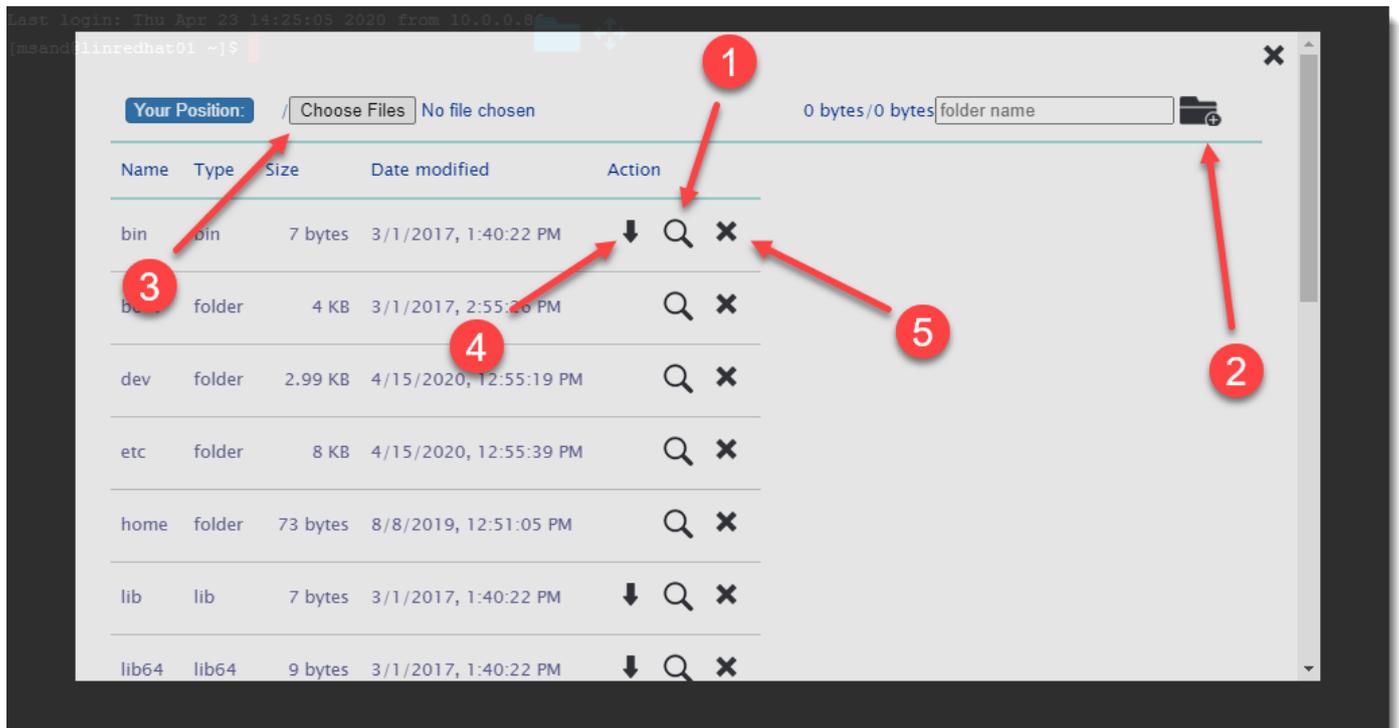
15.2 SSH File Transfer

SSH sessions have a built-in file transfer tool that you can access by left clicking anywhere in the empty space within your SSH session. You'll see this tool pop up at the top centre of your page:



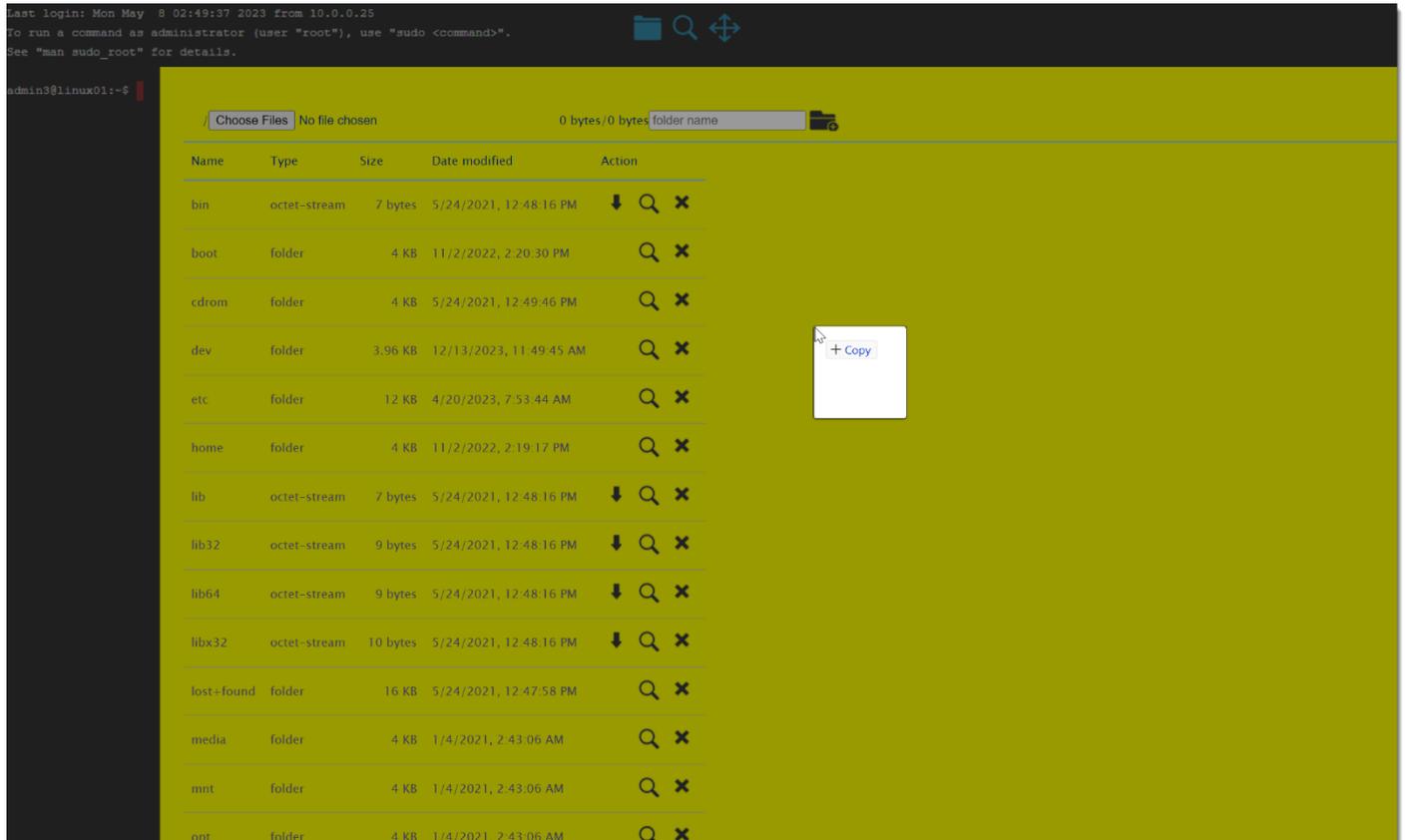
When clicking on this File Transfer tool, you'll be presented with a window similar to this screenshot below, where you can:

1. Browse into the relevant folder
2. Create a new folder
3. Upload files to the current position
4. Download file to local desktop
5. Delete file from remote file system



Click Studios

You can also drag and drop a file from your local desktop onto this File Transfer tool in your remote session, and it will turn yellow indicating it is ready to drop into the currently selected folder.



Last login: Mon May 8 02:49:37 2023 from 10.0.0.25
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

admin3@linux01:~\$

Choose Files No file chosen 0 bytes/0 bytes folder name

Name	Type	Size	Date modified	Action
bin	octet-stream	7 bytes	5/24/2021, 12:48:16 PM	↓ 🔍 ✕
boot	folder	4 KB	11/2/2022, 2:20:30 PM	🔍 ✕
cdrom	folder	4 KB	5/24/2021, 12:49:46 PM	🔍 ✕
dev	folder	3.96 KB	12/13/2023, 11:49:45 AM	🔍 ✕
etc	folder	12 KB	4/20/2023, 7:53:44 AM	🔍 ✕
home	folder	4 KB	11/2/2022, 2:19:17 PM	🔍 ✕
lib	octet-stream	7 bytes	5/24/2021, 12:48:16 PM	↓ 🔍 ✕
lib32	octet-stream	9 bytes	5/24/2021, 12:48:16 PM	↓ 🔍 ✕
lib64	octet-stream	9 bytes	5/24/2021, 12:48:16 PM	↓ 🔍 ✕
libx32	octet-stream	10 bytes	5/24/2021, 12:48:16 PM	↓ 🔍 ✕
lost+found	folder	16 KB	5/24/2021, 12:47:58 PM	🔍 ✕
media	folder	4 KB	1/4/2021, 2:43:06 AM	🔍 ✕
mnt	folder	4 KB	1/4/2021, 2:43:06 AM	🔍 ✕
opt	folder	4 KB	1/4/2021, 2:43:06 AM	🔍 ✕

+ Copy

16 Browser Based Launcher Keyboard Shortcuts and FAQ

For RDP sessions within the browser-based launcher, there are a few shortcuts you can use which are listed below. Please note Control + C and Control + V should not be used to copy and paste files, rather see section 13.1 of this document for details how to achieve this.

16.1 RDP Keyboard Shortcuts

- CTRL+ALT+END Brings up the Windows Security dialog box
- ALT+PAGE UP Switches between programs from left to right.
- ALT+PAGE DOWN Switches between programs from right to left.
- ALT+INSERT Cycles through the programs in the order they were started.
- ALT+HOME Displays the Start menu.
- CTRL + C allows you to copy text to and from a remote session (not suitable for file copy)
- CTRL + V allows you to paste text to and from a remote session (not suitable for file copy)

16.2 SSH Shell History

When in an SSH session, normally you can type **history** to get a complete history of commands for your session. With the Browser Based Launcher, if you left clicking anywhere in the empty space within your SSH session, you'll see this tool pop up at the top centre of your page a history window appears where you can scroll your entire session history, and then copy/paste as desired.

```

%Cpu(s):  0.0/0.0   0[
MiB Mem : 3932.0 total, 2566.6 free, 220.8 used, 1144.6 buff/cache
MiB Swap: 2048.0 total, 2048.0 free, 0.0 used. 3423.2 avail Mem

'include' filter delimiter is missing
  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM    TIME+  COMMAND
 3092 clickad+ 20   0  11848 3692   3176 R   0.6  0.1  0:00.01 top
   1 root       20   0 102496 11480 8500 S   0.0  0.3  0:00.57 systemd
   2 root       20   0    0     0     0 S   0.0  0.0  0:00.00 kthreadd
   3 root       0 -20    0     0     0 I   0.0  0.0  0:00.00 rcu_gp
   4 root       0 -20    0     0     0 I   0.0  0.0  0:00.00 rcu_par_gp
   6 root       0 -20    0     0     0 I   0.0  0.0  0:00.00 kworker/0:0H-kblockd
   9 root       0 -20    0     0     0 I   0.0  0.0  0:00.00 mm_percpu_wq
  10 root       20   0    0     0     0 S   0.0  0.0  0:00.07 ksoftirqd/0

```

```

command 'cdo' from deb cdo (1.9.9-rc1-1)
command 'cde' from deb cde (0.1+git9-g551e54d-1.1build1)
command 'cdw' from deb cdw (0.8.1-1build4)
command 'cd5' from deb cd5 (0.1-4)
command 'cd1' from deb cdo (1.9.9-rc1-1)
command 'cde' from deb tinycde (0.78build1)

Try: sudo apt install <deb name>

clickadmin@linux01:~/Downloads$ dir
clickadmin@linux01:~/Downloads$ ls
clickadmin@linux01:~/Downloads$ cd home
-bash: cd: home: No such file or directory
clickadmin@linux01:~/Downloads$ top
top - 14:03:16 up 2:13, 2 users, load average: 0.00, 0.00, 0.00
Tasks: 124 total, 1 running, 123 sleeping, 0 stopped, 0 zombie
%Cpu(s):  0.0/0.0   0[
MiB Mem : 3932.0 total, 2566.6 free, 220.8 used, 1144.6 buff/cache
MiB Swap: 2048.0 total, 2048.0 free, 0.0 used. 3423.2 avail Mem

'include' filter delimiter is missing
  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM    TIME+  COMMAND
 3092 clickad+ 20   0  11848 3692   3176 R   0.6  0.1  0:00.01 top
   1 root       20   0 102496 11480 8500 S   0.0  0.3  0:00.57 systemd
   2 root       20   0    0     0     0 S   0.0  0.0  0:00.00 kthreadd
   3 root       0 -20    0     0     0 I   0.0  0.0  0:00.00 rcu_gp
   4 root       0 -20    0     0     0 I   0.0  0.0  0:00.00 rcu_par_gp
   6 root       0 -20    0     0     0 I   0.0  0.0  0:00.00 kworker/0:0H-kblockd
   9 root       0 -20    0     0     0 I   0.0  0.0  0:00.00 mm_percpu_wq
  10 root       20   0    0     0     0 S   0.0  0.0  0:00.07 ksoftirqd/0
  11 root       20   0    0     0     0 I   0.0  0.0  0:00.22 rcu_sched
  12 root       rt   0    0     0     0 S   0.0  0.0  0:00.02 migration/0
  13 root      -51   0    0     0     0 S   0.0  0.0  0:00.00 idle_inject/0
  14 root       20   0    0     0     0 S   0.0  0.0  0:00.00 cpuhp/0
  15 root       20   0    0     0     0 S   0.0  0.0  0:00.00 kdevtmpfs
  16 root       0 -20    0     0     0 I   0.0  0.0  0:00.00 netns
  17 root       20   0    0     0     0 S   0.0  0.0  0:00.00 rcu_tasks_kthre
  18 root       20   0    0     0     0 S   0.0  0.0  0:00.00 kauditd
  19 root       20   0    0     0     0 S   0.0  0.0  0:00.00 khungtaskd

```

17 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,T
LS_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_RS
A_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_S
HA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_E
CDSA_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
```

```
1 accessNotInList = true
2
3 #cipherSuites. You may want to only use some strong cipher suites for SSL.
4 #You need to install Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files
5 #http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html
6 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
```

18 Browser Based Launcher Kerberos Connections

As of Passwordstate build **9785**, you can force connections in the Browser Based Launcher to use Kerberos. To configure this, edit the gateway.conf file and add in the following line, but set the domain name of your choice:

kerberos.kdc = clickdemo.com

```
*gateway.conf - Notepad
File Edit Format View Help
#Thu Feb 09 13:59:24 ACDT 2023
copyFile=true
recwarning=false
readdir.play.enable=true
keyStorePassword=/rFuOp1Ahqp5EPt7u1FHgYjRypsSLgwhfHBvHCsbZ1jdI1tN+WlCEg9hAP1hwqz2
buildTime=2022_09_27_06
showMessage=true
ssh=true
app.id=d41c4072-5703-4e89-94fd-ff1efc7812bd
ssl=true
credSSP=true
buildNumber=1015
sslProtocols=TLSv1,TLSv1.1,TLSv1.2
license=./license
sessionRecordParam=true
port=7273
passwordEncryptd=true
telnet=false
keyStore=Passwordstate.pfx
html = html
readdir=rec
#log http header, that may contains sensitive information like password. default is true.
logHTTPHeader = false
stderrLog=true
log.level = FINEST
kerberos.kdc = clickdemo.com
```

🚩 Only one domain is supported for this feature, and only one domain can be set in the **gateway.config** file

19 Open Ports for Remote Session Launchers

In order to make connections to different systems, you will need to ensure that the correct ports are open.

- The Client Based Launcher makes connections directly from the desktop machine where you are initiating the sessions from, to the remote machine.
- The Browser Based Launcher tunnels all traffic from the Desktop, through the Gateway, onto the remote machine.

Open Ports for the Client Based Launcher can be found in **Section 13** of this document:

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

Open Ports for the Browser Based Launcher can be found in **Section 14** of the same document:

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

In **Section 1** of the above linked document, we also have a tutorial on how to test for Open Ports if needed.

20 Performance Metrics for Browser Based Gateway

The Browser Based Gateway can support multiple sessions, and below is some information and statistics to help you determine what hardware requirements you will need.

20.1 CPU Usage

Primarily the CPU on the server where the gateway is installed is the hardware which performs a majority of the work. The minimum requirement for 400 concurrent connections is Pentium Dual-Core 2.7GHz, and usually adding in one more CPU will support up to another 300 – 400 concurrent RDP sessions.

20.2 Memory Usage

The Gateway is light on memory usage, and 250mb is usually enough to support 300 concurrent sessions

20.3 Bandwidth Usage

Bandwidth usage can be very different depending on the content. As the Browser Based Gateway is based on the standard RDP protocol, information about this can be found in the Microsoft white paper:

http://download.microsoft.com/download/4/d/9/4d9ae285-3431-4335-a86e-969e7a146d1b/rdp_performance_whitepaper.docx

From our testing and customer response, one RDP session needs about 260 Kbit bandwidth for normal business applications (Office, ERP etc).

21 Troubleshooting Remote Session Launchers

Below is some information and links that may help identify why sessions will not connect.

21.1 Client Based Launcher Troubleshooting Steps

Issue:

When using the Client Based Launcher, and clicking the Auto Launch button, nothing happens

Fix:

This could be due to a few different reasons:

1. The Client Based Launcher is not installed
2. The Browser has not been configured to work with Passwordstate
3. Browser Pop up is blocking Passwordstate from launching a session

This video explains how to address all three issues mentioned above:

<https://www.youtube.com/watch?v=A12eHSaGw4c>

Issue:

With the Client Based Launcher, the browser configuration page does not have a "Remember this Choice" to always open PSLauncher files, and hence the session will not initiate

Fix:

This issue is present in Chromium based browsers and was introduced in Chromium build 77. A fix for this can be deployed via Group Policy, or manually editing the registry on the local machine.

Issue:

Client Based Launcher will not connect to remote machine

Fix:

Enabling debugging for the Client Based Launcher, and attempt to launch another session. A log file will be created for you which will help understand why the session wasn't established. If needed, send this log file to Click Studios Support for analysis.

Please contact Click Studios support to get instructions on how to enable debugging.

Issue:

Client Based Launcher will not connect to remote machine, error is "**The server's authentication policy does not allow requests using saved credentials. Please enter new credentials**"

Fix:

See this forum post for a fix for this issue: <https://forums.clickstudios.com.au/topic/15452-client-based-launcher-failed-connections-the-servers-authentication-policy-does-not-allow-requests-using-saved-credentials-please-enter-new-credentials/>

21.2 Browser Based Launcher Troubleshooting Steps

Issue:

The gateway Service will not start. This is usually caused by one of three things:

1. The certificate in the Gateway install folder is not named correctly. It should be called Passwordstate.pfx
2. The certificate in the Gateway install folder has expired
3. The encrypted Password for the certificate is set incorrectly in the gateway.conf file

Fix 1:

You could try reinstalling the gateway again, as this will effectively repair the gateway, and automate assigning a new certificate. Below are the install instructions for the Browser Based Gateway

Gateway Installed internally – Section 4 or 5 of this document:

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

Gateway installed on Remote Site: Section 4 of this document:

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

Fix 2:

If you would prefer not to reinstall the gateway, you can try manually exporting your certificate from your Passwordstate web server, by following Section 6 in this document:

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

Then to encrypt the certificate password, follow 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/>

Issue:

The Browser Based Gateway is installed and the service is running, but sessions will not connect.

Fix 1:

Ensure that your desktop machine where you are initiating sessions from, has direct access to the Gateway service/server. By default, port 7273 is the port that needs to be open unless otherwise modified.

Fix 2:

The gateway may generate some error codes, which you'll find in Passwordstate Administration under the Error Console. A list of these error codes can be found here: <https://forums.clickstudios.com.au/topic/2853-error-codes-for-the-browser-based-remote-session-launcher/>

Fix 3:

The Browser Based Gateway does have verbose logging which can be sent to Click Studio Support for analysis.

<https://forums.clickstudios.com.au/topic/2852-enabling-verbose-logging-for-the-browser-based-remote-session-launcher/>

22 Browser Based Launcher and Self Signed Certificates

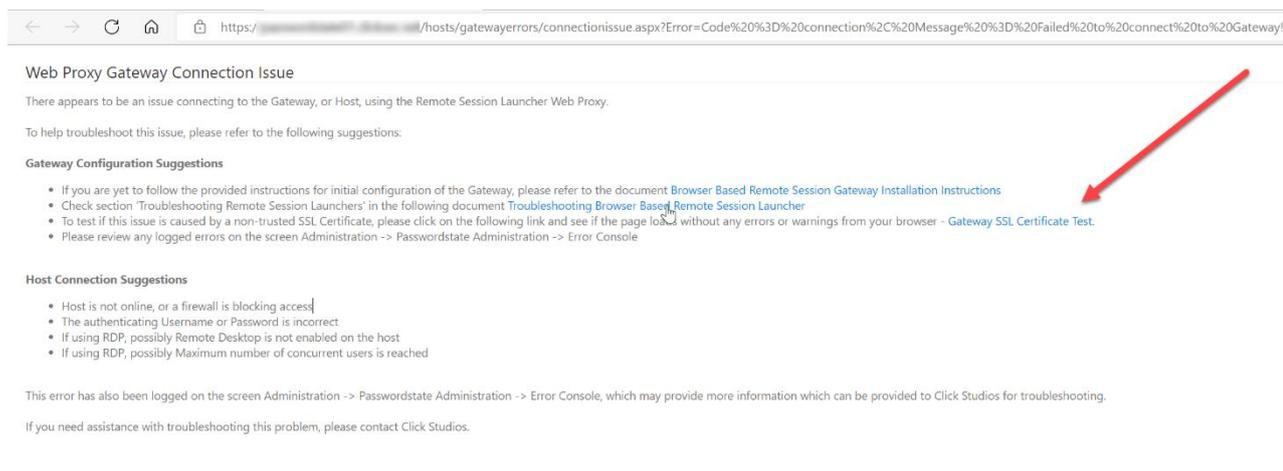
By default, Passwordstate comes installed with a Self-Signed Certificate as this is the only type of certificate Click Studios can supply during the install.

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 the Browser Based Gateway install process, your RDP and SSH remote sessions will fail until you force your browser to trust the certificate.

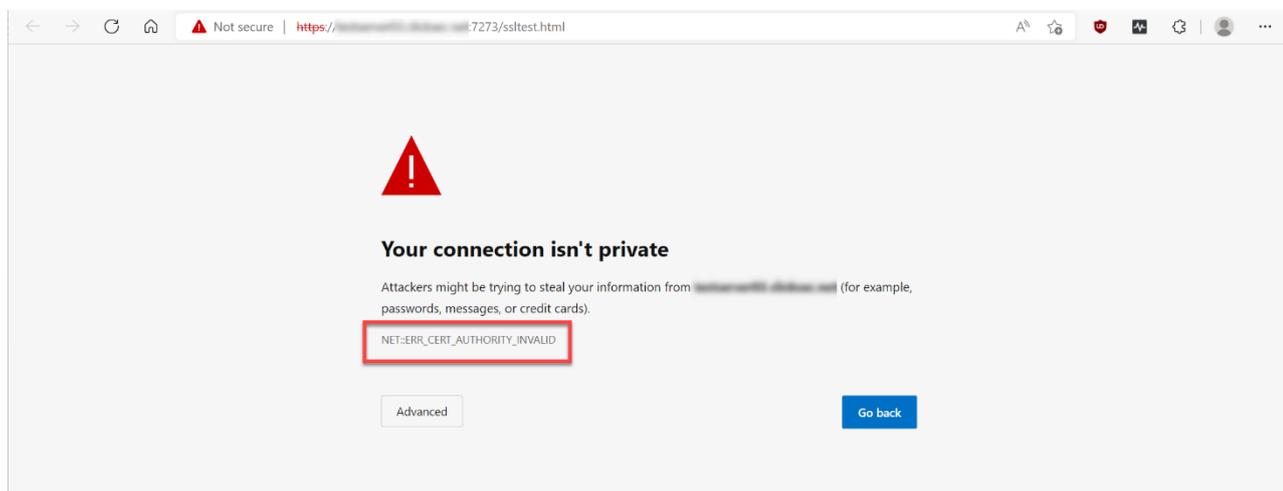
For a seamless experience with the Remote Session Launcher, you should use a trusted certificate, which can either be issued from your own internal Certificate Authority, or from an online provider. If you have no choice but to use a Self-Signed Certificate, then you will need to force your browser to 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:

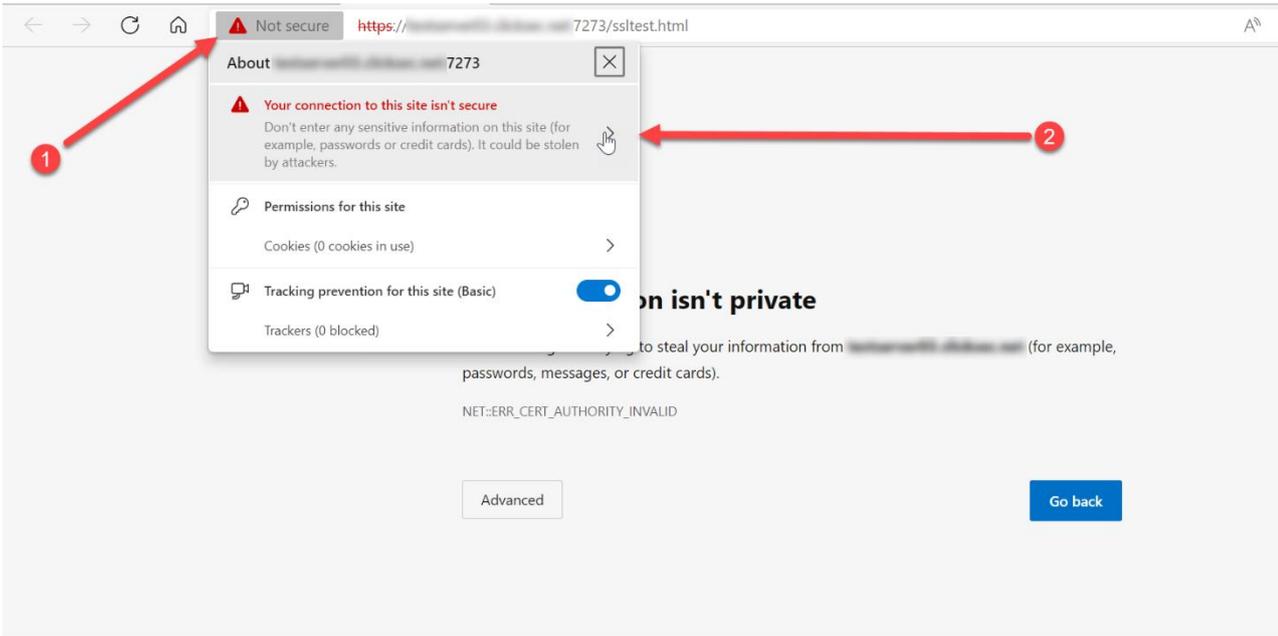


If you then get redirected to a page that looks like the screenshot below, the certificate is not trusted by your browser:

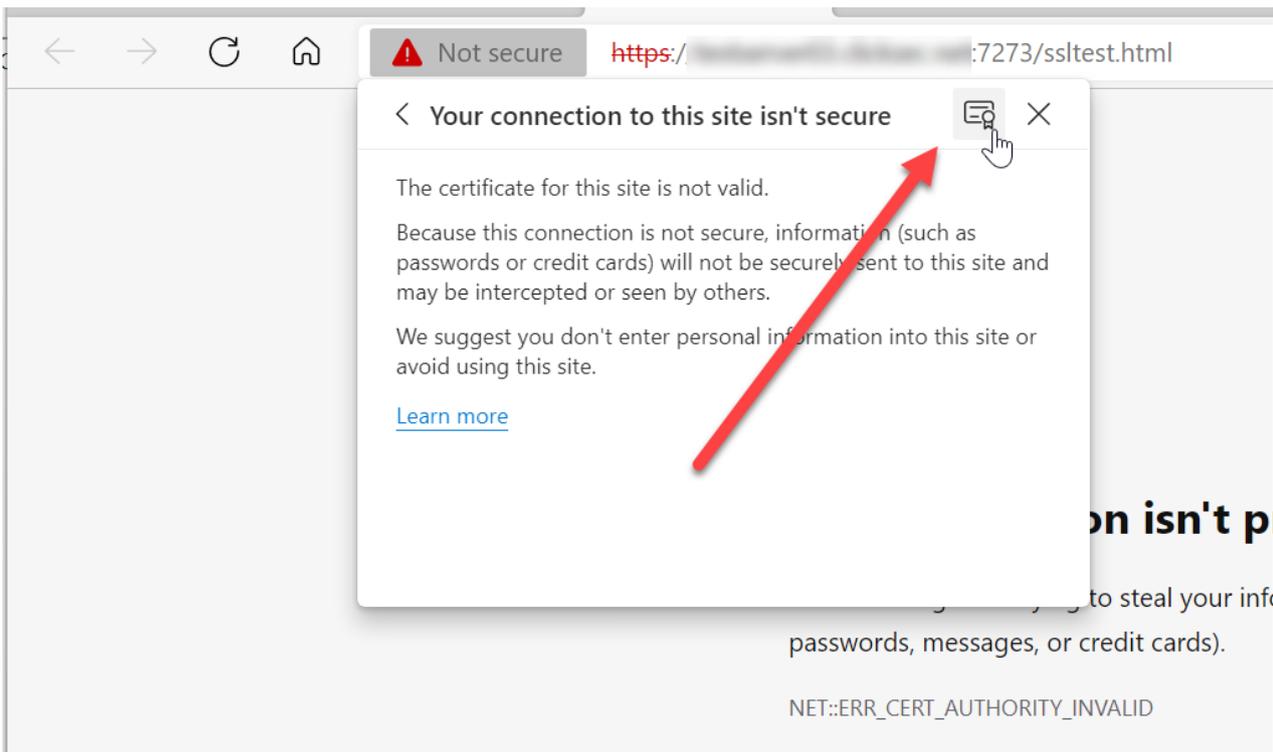


Click Studios

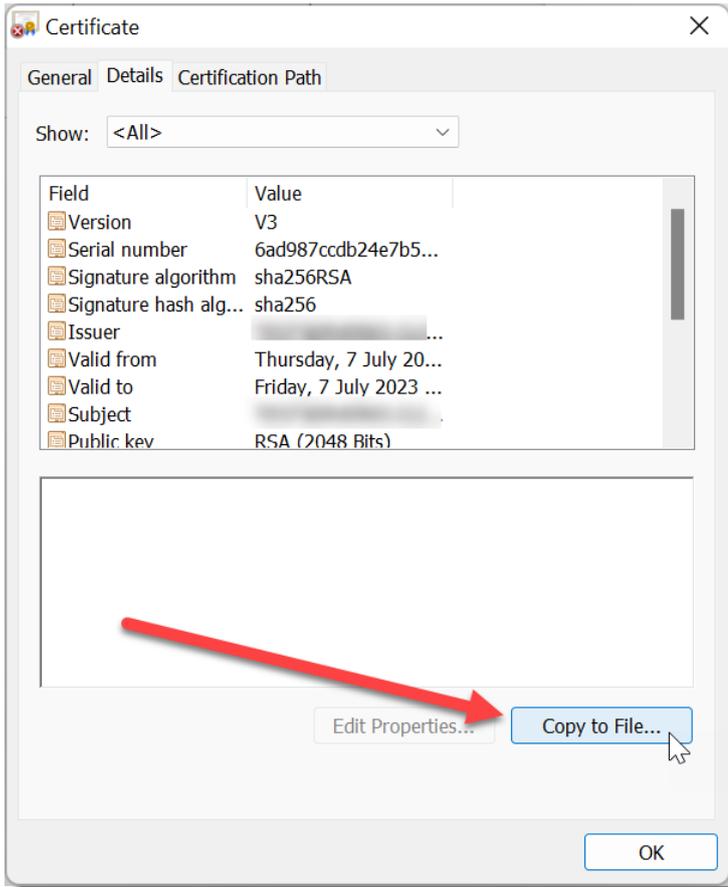
To fix this, you will need to follow this process on every machine that you intend on establishing remote sessions from. First, click the Warning button in Edge, and then click the Warning message:



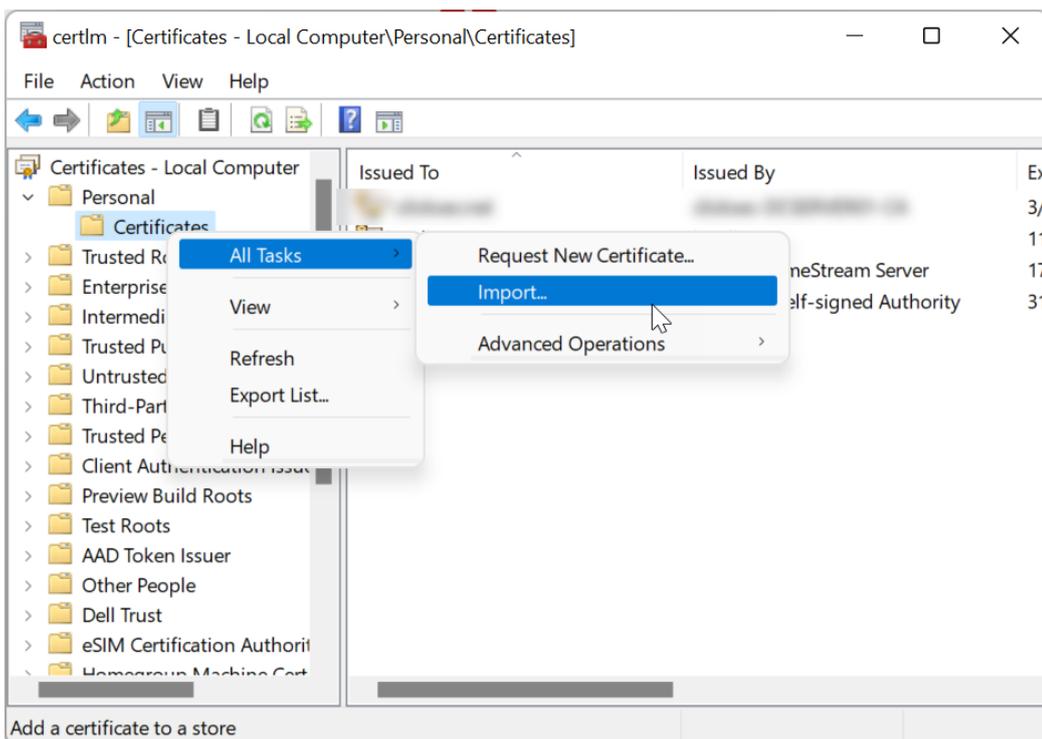
Click the **Certificate** button:



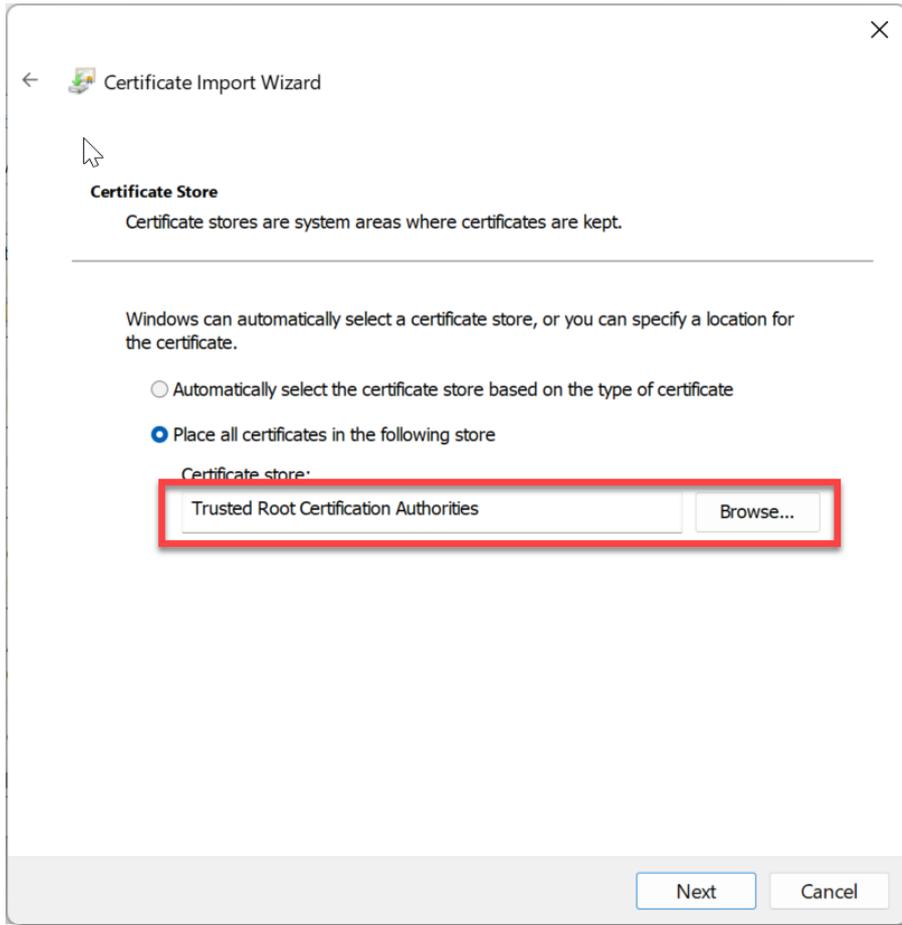
Under the **Details** tab, click **Copy to File**. Follow the prompts to save the certificate to disk, and you can choose all the default options during this process.



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:



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

23 Remote Session Launcher FAQ

If your account you are using with your Remote Session Launcher is a member of the “Protected Users” security Group, you will not be able to establish an RDP session with the Browser Based Launcher. This is because it is not possible to authenticate Protected Users on browsers.

It is possible to use a Protected User with the Client Based Remote Session Launcher. The local Windows machine must be a domain member and also must Windows 10, or Server 2012 R2 or later. You cannot log in from Windows 7, or macOS (even with MS RDP client).