



Passwordstate Remote Site Agent Manual

© 2020 Click Studios (SA) Pty Ltd

Table of Contents

Foreword	0
Part I Introduction	3
Part II Adding Remote Site Locations	3
Part III Installation of Remote Site Agent	4
Part IV Install Browser Based Remote Session Launcher on Remote Site	7
Part V Remote Site Tables	15
Part VI Remote Agent Logging	17
Part VII Tagging Data with a Site Location	17
Part VIII Forcing An Agent Poll	17

1 Introduction



Welcome to the Passwordstate Remote Site Agent Manual.

The Passwordstate Agent is used for Remote Site Locations, where connectivity is only possible over a HTTPS or Firewalled connection.

With the Passwordstate Agent, it is possible to perform Account Discoveries, Host and Account Heartbeats, and Password Resets on remote networks.

The agent communicates securely with your Passwordstate API, over HTTPS, using unique InTransit Encryption keys for further encrypting the flow of traffic.

The following table summarizes each of the key areas for configuring and using the Passwordstate Agent.

Adding Remote Site Locations	Prior to using the Remote Site Agent, you must first add one or more Remote Site Location records
Installation	Guides you through the process of installing the Remote Site Agent
Configure Browser Based Remote Session Launcher Gateway	If you would like to also use a distributed copy of the Remote Session Launcher Gateway with your Agent, you can follow these instructions
Remote Site Tables	Provides information about synchronization of data between your Passwordstate API and the Remote Site Agents
Remote Agent Logging	Provides detail of where the Agent creates logging data
Tagging Data with a Site Location	Explain where in Passwordstate you can tag certain record for a Remote Site Location
Forcing An Agent Poll	If needed for testing/debugging purposes, you can also Force an Agent Poll within one minute, instead of waiting for the scheduled poll


2 Adding Remote Site Locations

Prior to deploying any Passwordstate Agents, you must add each Remote Site Location into the screen **Administration -> Remote Site Administration -> Remote Site Locations**.

When adding a Remote Site Location, please specify appropriate setting as appropriate below:

- The name of the Remote Site

- The In-Transit encryption key (used to further encrypt the BODY of the traffic in the HTTPS requests)
- Agent Poll Frequency - how often you would like the remote agent to poll, and check for new tasks to execute i.e. Discover Jobs, Account or Host Heartbeats, and Password Resets
- Maintenance Window - the period in which the Remote Agent will not execute any regular tasks - except for refreshing the contents of the Remote Tables. The Maintenance Window gives you a time slot in which you can perform maintenance activities on the remote server, knowing it will not effect any processing tasks.
- Functioning URL for the Browser Based Remote Session Launcher - See Section 4 in this document for more information about this
- Allowed IP Ranges - if you wish to further secure calls to the API for the selected Remote Site Location, you can specify various IP Addresses or ranges on the 'Allowed IP Ranges' tab

 **Note:** You do need to purchase the required number of Licenses to add new Remote Site Locations - See <https://www.clickstudios.com.au/buy-now.aspx> for more information

Add New Remote Site Location

To add a new Remote Site Location to Passwordstate, please fill in the details below.


remote site location
allowed ip ranges


Please specify appropriate details below for this Remote Site.


Site Location Name : *	<input type="text" value="Client1"/>		
In-Transit Encryption Key : *	<input type="text" value="5726312c2cb1cd58126dce6cb3705065b7d04af2d008a991f51a8d6fa77bd3a8"/>		<input type="button" value="Generate New Key"/>
Agent Poll Frequency :	<input type="text" value="05"/>	Minutes	
Maintenance Window : *	<input type="text" value="21"/>	Start Hour	<input type="text" value="22"/> Finish Hour
Please schedule Account & Host Discovery Jobs outside of this Maintenance Window.			
Remote Session Launcher Gateway URL :	<input type="text" value="https://client1.clickstudios.com.au:7273"/>		
	Specify in the format of https://client1.clickstudios.com.au:7273		
Purge Recorded Sessions :	<input type="text" value="0"/>		
	Older than the specified number of days - leaving as 0 will disable purging.		

3 Installation of Remote Site Agent

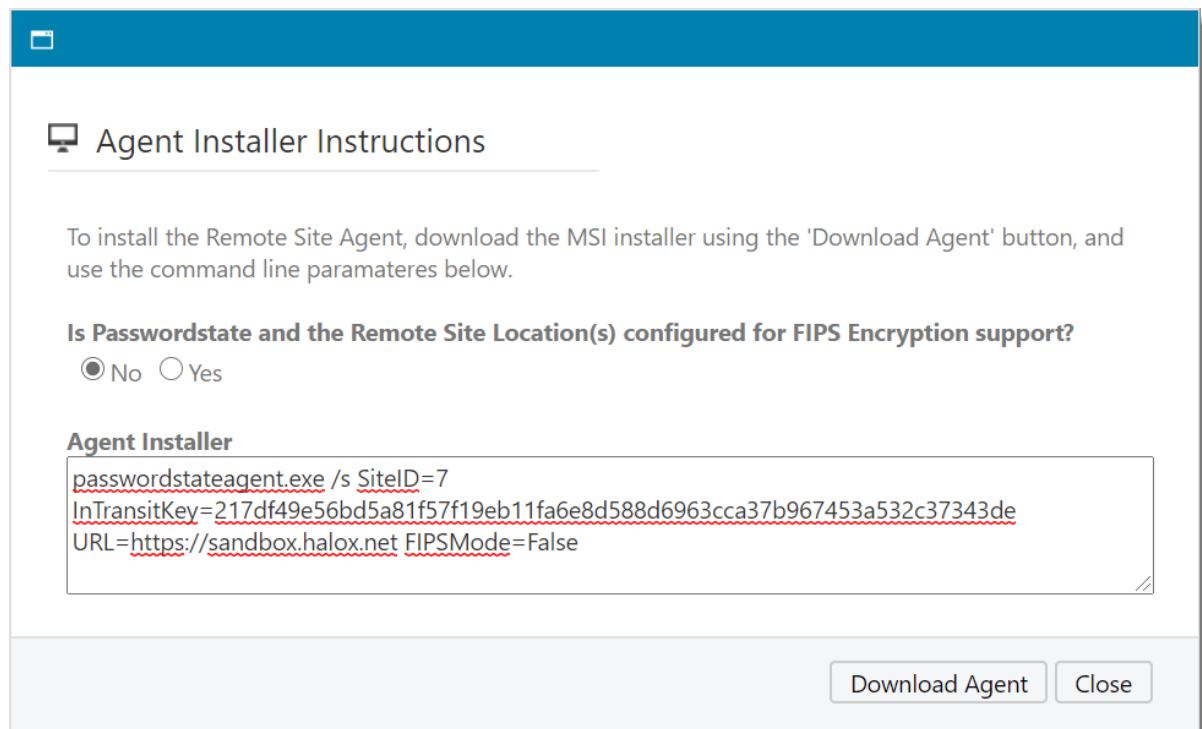
Prior to deploying any Agents, please ensure your firewall allows access through from the remote networks to your Passwordstate web server. The agents communicate back to the API in Passwordstate only. See the open Ports document for more information about this:
https://www.clickstudios.com.au/downloads/version8/Passwordstate_Open_Port_Requirements.pdf

 **Note 1:** The Server or Desktop where you install the Agent must have .NET Framework 4.5 or above installed, and PowerShell 4.0 or above.

 Note 2: For Account Discovery and Password Resets at remote site locations, please refer to the '**Password Discovery, Reset And Validation Requirements**' document on Click Studios documentation page at <https://www.clickstudios.com.au/documentation/>

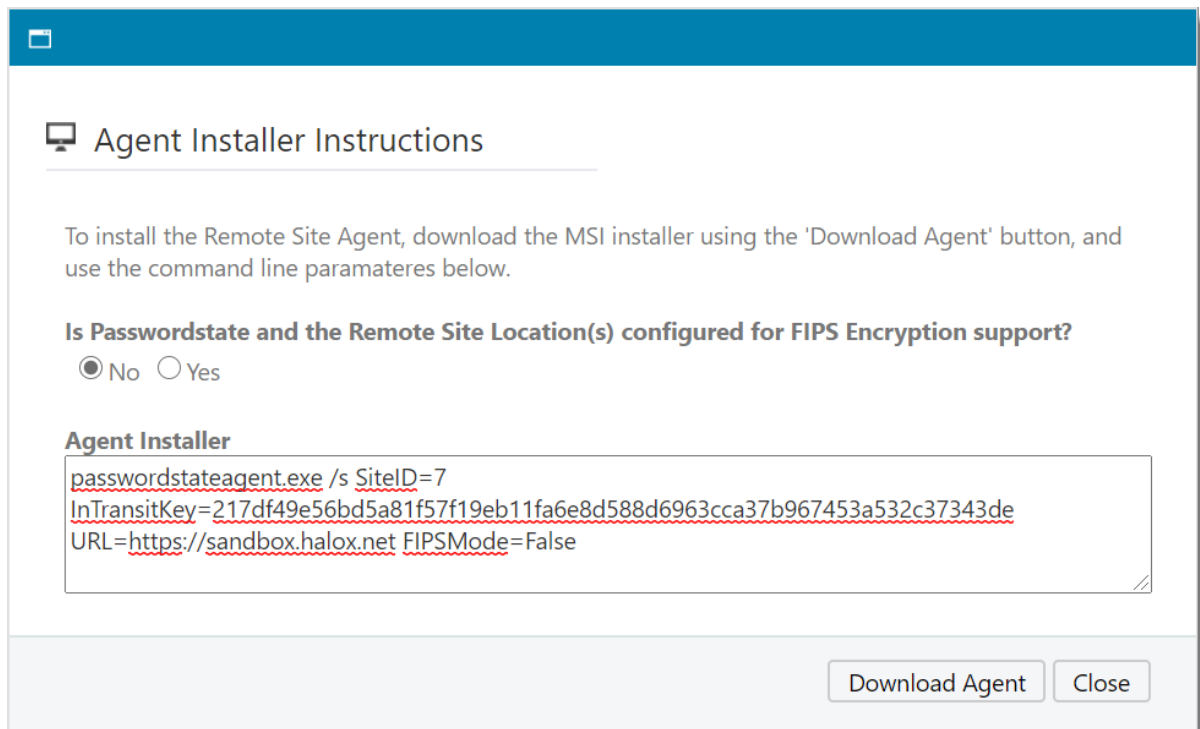
 Note 3: Once the agent is installed, it will automatically upgrade itself if required, when you upgrade your instance of Passwordstate. There is a Windows service called 'Passwordstate Agent Upgrade Service' which will automatically upgrade the agent within 10 to 15 minutes of you upgrading your Passwordstate web site. This Upgrade service reaches out to the page <https://www.clickstudios.com.au/getagentupgradeable.aspx> to download the latest **agent_upgrade.zip** file


Once you have added the required number of Remote Site Locations into the Administration area of Passwordstate, you can select the '**View Agent Installer Instructions**' Actions menu for the appropriate site, and it will give you the installer command line options for the Agent.




With the installer command line parameters you see in the below screenshot, this will install the Agent silently, as well as configure the required settings in the **C:\Program Files (x86)\Passwordstate Agent\PasswordstateAgent.exe.config** so the Agent can communicate back to your Passwordstate API. This install process takes approximately 10 seconds.

Click the **Download Agent** button, and transfer that to the remote machine where you want the agent to run, and then use the command prompt on that machine to run the command line parameters.



 Note 1: You will need to select **FIPS encryption** if your main Passwordstate website is configure for FIPS. To find out if you are using FIPS encryption, log into Passwordstate and look under the **Administration** tab - **Password Administration** page.

 Note 2: The install location for the agent is **C:\Program Files (x86)\Passwordstate Agent**

Encrypting Settings in the AppSettings Section in the PasswordstateAgent.exe.config File

If required, it is also possible to encrypt the **AppSetting** section of the **PasswordstateAgent.exe.config** File. Below are instruction for this, as well as decrypting them:

- Stop the Passwordstate Agent Service
- Rename the file PasswordstateAgent.exe.config to web.config
- Open a command prompt (as Admin) and type **CD C:\Windows\Microsoft.NET\Framework64\v4.0.30319**
- Type the following command to encrypt these settings: **aspnet_regiis.exe -pef "appSettings" "C:\Program Files (x86)\Passwordstate Agent"** , or **aspnet_regiis.exe -pdf "appSettings" "C:\Program Files (x86)\Passwordstate Agent"** to decrypt them
- Rename the web.config file back to PasswordstateAgent.exe.config

- Restart the Passwordstate Agent Service

4 Install Browser Based Remote Session Launcher on Remote Site

Passwordstate comes with a Browser Based Gateway feature, which allows you to perform RDP and SSH connections using credentials out of the Passwordstate vault to connect to the remote devices. By configuring this Browser based Remote Session Launcher Gateway with the Remote Site Locations agent, you can get secure RDP and SSH sessions to hosts at the remote network.

You do not need functioning DNS for each of the Host records from your internal Passwordstate environment, the Gateway will perform DNS lookups on the network it is installed in.

In order for this feature to work on your remote site you must have:

- It is highly recommended to use a wildcard certificate. An example of this is ***.clickstudios.com.au**. If you do not supply your own certificate, a Self Signed one will be created for you automatically, however these can be difficult to work with as browsers do not trust them by default.
- At the remote site, the externally facing firewall must allow incoming traffic on the Port you specify the Gateway to listen on. **Port 7273** is the default port. To ensure a secure connection between your company firewall, and the one at the remote end, you can restrict this open port by IP Addresses on each of your firewalls
- You must have a functioning external DNS record which can redirect traffic to the Gateway i.e. for a URL of <https://client1.clickstudios.com.au:7273>, you would need a DNS entry for client1.clickstudios.com.au to point to the remote site's firewall.
- The firewall would then need to forward traffic on Port 7273 to the host where you have installed the Remote Site Location Agent
- You must be using a trusted SSL certificate for the Remote Session Launcher Gateway. If you are using a purchased wildcard certificate, your browser will automatically trust this which makes for the most user friendly experience.

Changes Made to your Server During this Automated Install

When installing the Remote Site Locations Agent at your remote site, it also preloads some of the files required for the Remote Session Launcher. As a once off process you'll then need to run a Powershell script on the same server where you have the Remote Site Agent installed, which will finish setting up the Browser Based Launcher. This Powershell script will perform the following changes to this server:

- Create a log file in the same directory where you execute the Powershell script from
- Downloads **OpenJDK 13** from <https://cdn.azul.com/zulu/bin/> and extracts this file to **C:\Program Files (x86)\OpenJDK**. This download is approximately 200mb in size
- Adds a file path to the "**PATH**" System Environment Variable. Also adds in a new Environment Variable called **JAVA_HOME**. If these already exist, they will be removed before adding them back in
- Installs a Windows Service called **Passwordstate-Gateway**
- Removes all temporary source files that were created during this process
- Will create a Self Signed certificate with the name of your server, if you do not supply your own certificate

Installing the Browser Based Gateway on your Remote Site

1. On the server where you have the Remote Site Agent installed, download the Powershell installation script from <https://clickstudios.com.au/downloads/Install-Gateway-RemoteSite.zip>
2. Extract the zip file into a temporary location, such as **C:\Temp**
3. Open Powershell ISE "**As Administrator**" and open the **C:\Temp\Install-Gateway-RemoteSite.ps1**
4. If you are supplying your own certificate, you will need to supply it in the format of a password protected .pfx file. The exact name of this must be **Passwordstate.pfx**. Place this Passwordstate.pfx file into the same directory where you are running the Powershell script from. More information about supplying your own certificate can be found in the next section, **SSL Certificate Considerations**
5. If you are supplying your own certificate, insert the password you have created for it in line 25 of the Powershell script. Screenshot below with example of this
6. Run the script, and it should take about 1 minute to complete


```

1  <#
2  .NOTES
3  =====
4  Created:      April 2020
5  Organization: Click Studios Pty Ltd
6  Filename:     Install-Gateway-RemoteSite.ps1
7  Version:      1.0
8  =====
9  .DESCRIPTION
10     - This script will install and configure the Browser Based Gateway
11     - Powershell must be running as Administrator
12     - The script should not be executed on the same server where you have Passwordstate
13     - A log file will be created in the same folder where you execute this script
14     - If you have your own certificate you'd like to use on the gateway, place it in the
15
16
17
18     .UPDATES
19     12th May 2020 - Added uninstall of Agent Service if it existed
20                   - Added better handling of special symbols if they existed in the
21                   - Added better logic for inserting the encrypted password into the
22
23  #>
24
25  $CertPassword = 'Welcome01'
26
27  # Begin script
28  Write-Host "Begin script"
29
30  # Remove the log file if it already exists in $PSScriptRoot home
31  Write-Host "Remove the log file if it already exists in $PSScriptRoot home"
32  $logtest = Test-Path "$PSScriptRoot\Install-Gateway.txt"
33  if ($logtest -eq $true){Remove-Item $PSScriptRoot\Install-Gateway.txt -Force}
  
```

If there are any issues running the script, you should see some information in the Powershell output console, and there will be a log file created in the folder where you ran the Powershell script from. If you are unable to determine the cause of the failed install, please forward the log file onto support@clickstudios.com.au requesting assistance in diagnosing the issue.

If the installation was successful, you should see a Windows Service called **Passwordstate-Gateway** and it should be running.

SSL Certificate Considerations

Click Studios recommends using a wildcard certificate for all your clients, as this means you can use the same certificate file, and gateway.conf configuration file across all sites. An example would be to purchase a wildcard certificate like ***.clickstudios.com.au**, and then you could use URLs like <https://client1.clickstudios.com.au:7273> and <https://client2.clickstudios.com.au:7273>, etc, etc.

Note 1: You don't have to use a wildcard certificate, but it might work out more cost effective, and easier to manage, if you are deploying multiple agents.

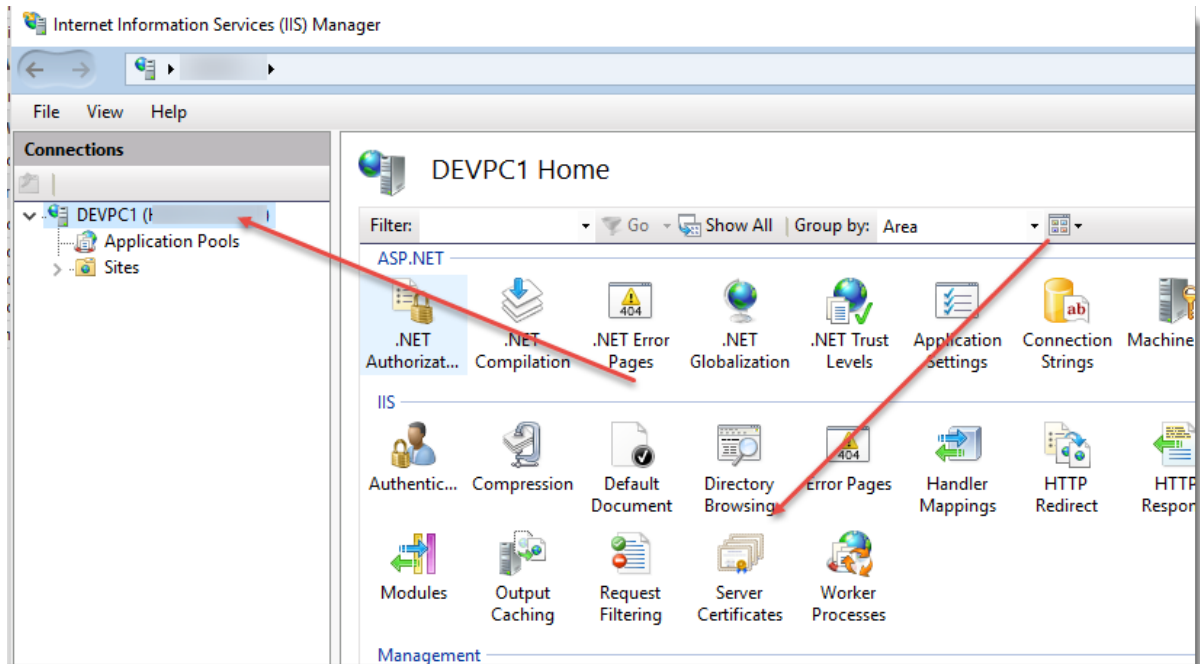
Note 2: If you instead wish to use the Self Signed Certificate that comes with the installer automatically, then you will need to trust this certificate in the browser where you trying to

establish RDP and SSH session from. Please see **section 12** of this install guide for details on how to trust certificates in your browser:

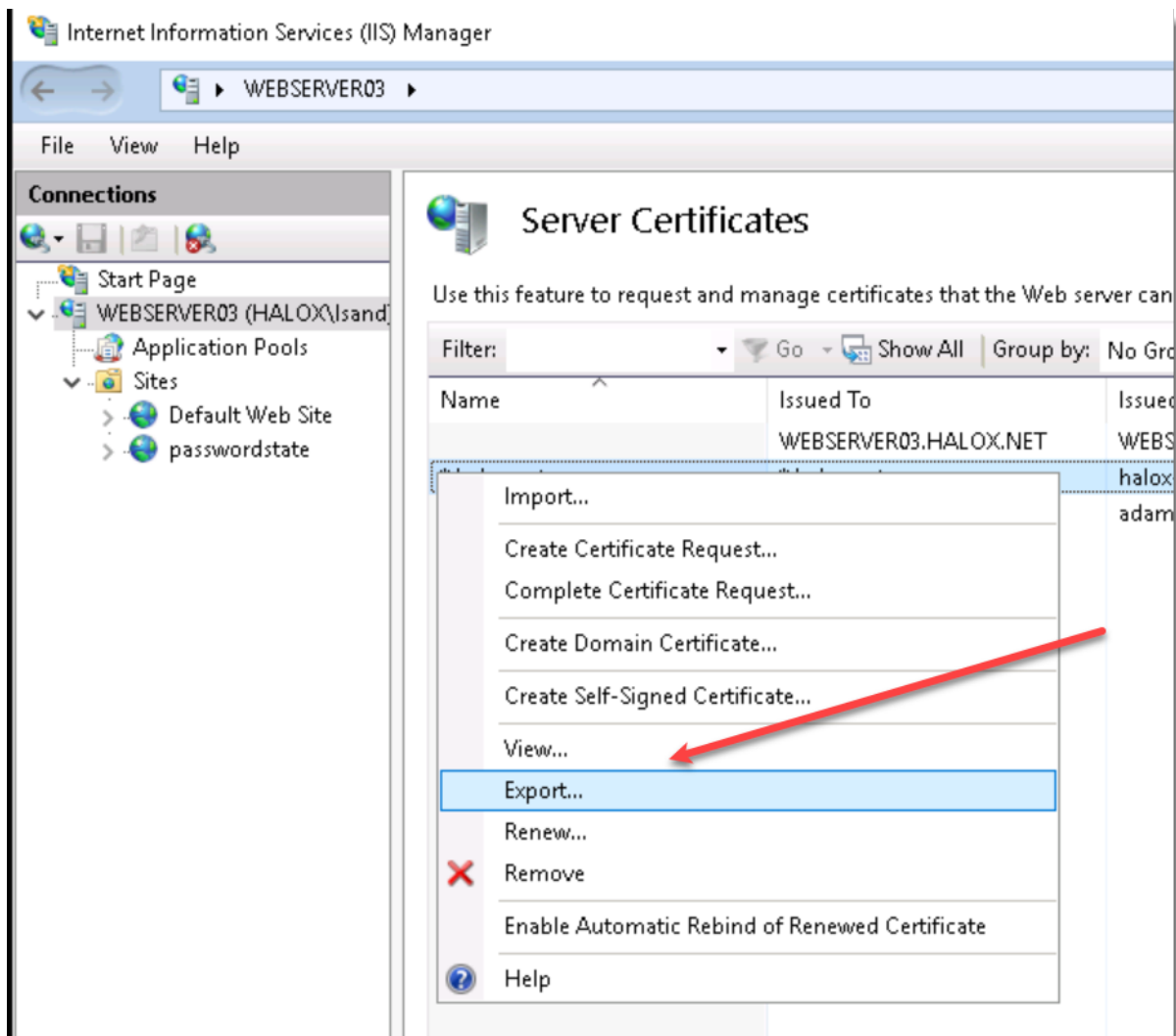
https://www.clickstudios.com.au/downloads/version8/Installation_Instructions.pdf

If you already have a wildcard certificate you can use in IIS, you can use the instructions below to export it for use.

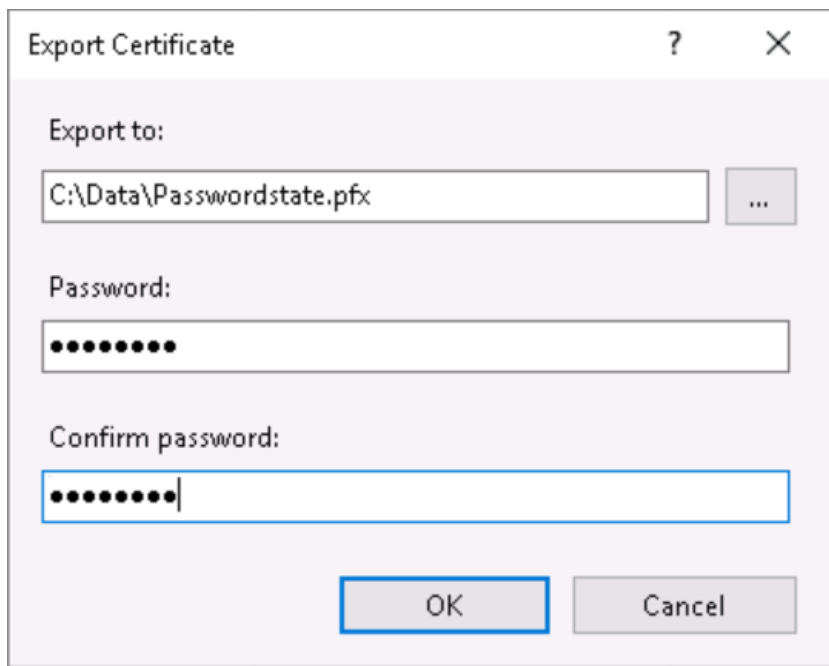
- In IIS, navigate to '**Server Certificates**'



- Right click on your certificate and select '**Export**'



- Export the certificate to a temporary folder, and name it **Passwordstate.pfx** – make sure you specify a password for the exported certificate as well, and keep this password in mind as you'll need it when you install the Gateway

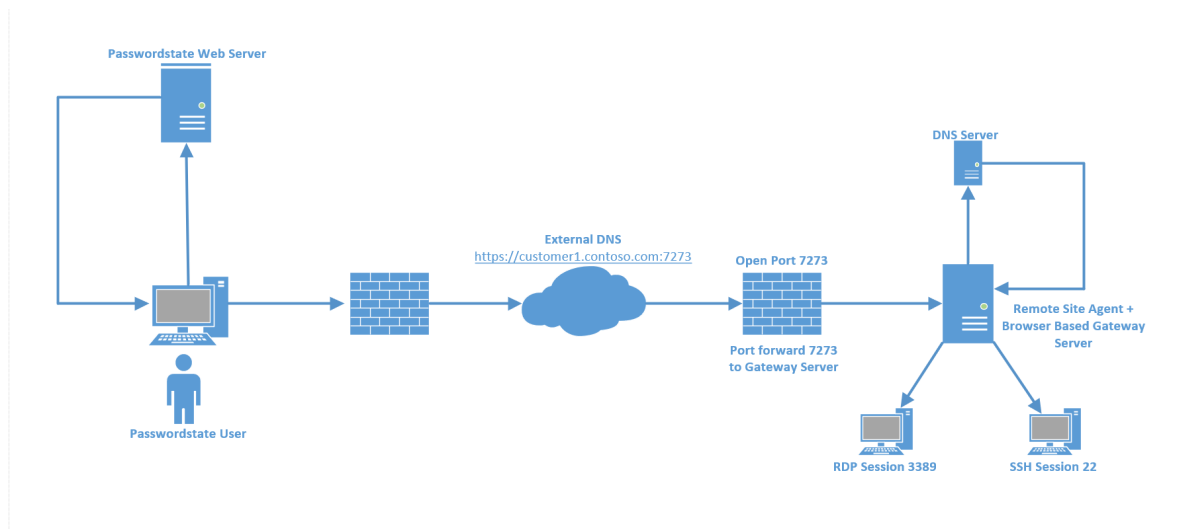


DNS and Port Considerations

In order for your RDP and SSH sessions to communicate to the remote site correctly, you will need to ensure you have a functioning DNS entry, forwarding on traffic to the Remote Site firewall. This firewall will also need an port open which forwards HTTPS traffic onto the server where you have the Remote Site Agent and the Browser Base Gateway installed.

Below is a diagram to give you a visual reference as to how a RDP or SSH Session can be established over the internet, using the Browser Based Launcher and the Remote Site Locations module. You will need to create your own external DNS entry, and this must be set on your Remote Site Location in Passwordstate Administration area. More information about where to set this can be found in the "**Specify Gateway URL in Passwordstate**" below.

Ideally if you had a wildcard certificate of ***.contoso.com** for example, this one certificate could be used on multiple sites. You could create your DNS entries as **customer1.contoso.com**, **customer2.contoso.com** etc.



Session Recording Folder in the Gateway.conf File

By default, and session recordings will be stored in the folder "C:\Program Files (x86)\Passwordstate Agent\gateway\rec".

Depending on how many session recordings you do, and their duration, then this may cause issues with disk space on the C drive, so it is recommended you move this to a different disk with more space. To do this, do the following:

- Change the 'recdir' and 'html' settings on the Gateway.conf file, like in the screenshot below
- Copy the file "C:\Program Files (x86)\Passwordstate Agent\gateway\rec\ssltest.html" into this new folder, in case you need to test the SSL Certificate back from within your Passwordstate UI - when you try and make a connection to the remote host

```


#listening port
port = 7273

#directory for session recording. Specify in the format of d:\\recordings, otherwise a folder called rec will be used from within the agent's
#Note 1: Make sure 'recdir' and 'html' paths below are the same
#Note 2: If changing the recording folder, please also copy the file /rec/ssltest.html into your new folder, so you can test the SSL Certificate
recdir = d:\\recordings

#default page to play back session recordings. Specify in the format of d:\\recordings, otherwise a folder called rec will be used from within the agent's
html = d:\\recordings
  
```

Specify Gateway URL in Passwordstate

In order for traffic to route to the correct remote site Gateway, you need to edit the Remote Site Locations record and specify the URL, as per the screenshot below.

 Remember: You need a functioning DNS record in order to route traffic to the example below of **client1.clickstudios.com.au**

Edit New Remote Site Location

Please make changes to the Remote Site Location below as appropriate, and then click on the Save button.

remote site location	allowed ip ranges
Please specify appropriate details below for this Remote Site.	
Site ID :	9
Site Location Name : *	client1
In-Transit Encryption Key : *	42c5551ecdbca10e4031445c71ccbf24114926e0e43077b97cd0321eda81bca Generate New Key
Warning: Changing this key will also require you to change the 'PasswordstateAgent.exe.config' file at the remote end.	
Agent Poll Frequency :	05 Minutes
Maintenance Window :	21 Start Hour 22 Finish Hour
Please schedule Account & Host Discovery jobs outside of this Maintenance Window.	
Remote Session Launcher Gateway URL :	https://client1.clickstudios.com.au:7273
Specify in the format of https://client1.clickstudios.com.au:7273	
Purge Recorded Sessions :	0
Older than the specified number of days - leaving as 0 will disable purging.	
Save Cancel	

Remote Sessions to Host

Now from within Passwordstate, performing remote sessions to Hosts is as simple as making connections to your own internal hosts. What's required is:

- Your Host records must be "tagged" to the correct Remote Site Location - screenshot below
- You must have access to the Web Based Remote Session Launcher in Passwordstate - please refer to the **Passwordstate Security Administrator's Manual** if you do not have access to this. Access can be granted on the page **Administration** -> **Feature Access** -> **Remote Sessions** tab
- Then you can authenticate with any of the supported methods to the Host. For more information on authenticating, please refer to the **Passwordstate User Manual** in the Help Menu, under the section **Hosts** -> **Hosts Navigation Tree** -> **Remote Session to a Host**

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: *

sandpc1.sanddomain.com

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:

CN=Computers,DC=sanddomain,DC=com

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

Site Location

SandDomain

Host Type: *

Windows

Operating System: *

Windows 10

Internal IP:

External IP:

MAC Address:

Virtual Machine: *

☐ Yes
 ☒ No

Virtual Machine Type:

☐ Amazon
 ☐ Azure
 ☐ Cloudify
 ☐ VirtualBox
 ☒ VMware
 ☐ Other

5 Remote Site Tables

With each Agent install, there are certain tables in an SQLite database which will be populated with data via your Passwordstate API.

When you first install the Agent, these tables will be populated accordingly when the Passwordstate Agent Windows Service first starts, and they will also be refreshed at the beginning of the Maintenance Window you specify for each of the Remote Site Locations.

Below are a list of tables which are refreshed regularly, but if you change the contents of these tables within your install of Passwordstate, it is recommended you manually refresh the remote site tables manually, or wait until the next Maintenance Window for them to automatically be refreshed. You can manually refresh these tables on a per site basis, or for all sites at once as per the options below - when the Agent next polls (every 5 minutes by default), then the tables will be refreshed.









Table Name	Used For	When Data For These Tables Could Change
AccountTypes	Performing Discovery Jobs	During an upgrade
DiscoveryScripts	Performing Discovery Jobs	During an upgrade
HostTypes	Performing Password Resets	During an upgrade, or if you change any within the Administration area

Table Name	Used For	When Data For These Tables Could Change
OperatingSystems	Performing Discovery Jobs	During an upgrade, or if you change any within the Administration area
Scripts	Performing Password Resets	During an upgrade, or if you change any within the Administration area
ValidationScripts	Performing Account Heartbeats	During an upgrade, or if you change any within the Administration area

Remote Site Locations

Below are all the Remote Sites where an Agent can be deployed to perform Account Discoveries, Password Resets, and Account Heartbeats.

This feature is designed for sites that are not part of your standard internal network, and are either separated by a firewall or are on a different IP range.







Actions	Site Location	Agent Health	Last Agent Poll Time
	Fabrikam		
 Clear All Progress Indicators			26/04/2017 12:45:19 PM
 Delete			18/04/2017 10:43:35 AM
 Refresh Remote Tables			
 View Agent Installer Instructions			

Re: All Remote Tables | Toggle Visibility of IDs | Grid

Remote Site Locations

Below are all the Remote Sites where an Agent can be deployed to perform Account Discoveries, Password Resets, and Account Heartbeats.

This feature is designed for sites that are not part of your standard internal network, and are either separated by a firewall or are on a different IP range.

Actions	Site Location	Agent Health	Last Agent Poll Time
	Fabrikam		
	Halox		26/04/2017 12:45:19 PM
	Sanddomain		18/04/2017 10:43:35 AM

Refresh Grid | Add Remote Site | Refresh All Remote Tables | Toggle Visibility of IDs | Grid

6 Remote Agent Logging

Once the Remote Agent is installed and functioning, it can provide logging information in a variety of ways:

- In the Agent folder, generally in the path of C:\Program Files (x86)\Passwordstate Agent, there is a Logs folder. In this folder, the following logs will be created to assist with any troubleshooting activities:
 - Discovery - Account and Host Discovery activities
 - Heartbeat - Account and Host Heartbeat activities
 - PasswordResets - Password Reset information
 - General - All other logging which do not fit into one of the categories above

Logs will be kept for a maximum of 2 weeks, then automatically deleted.

- If the Agent is able to communicate back to your Passwordstate API, any errors will also be logged to the screen Administration -> Passwordstate Administration -> Error Console
- And when the Agent reports back information around Discovery, Resets, etc, it will add Auditing data for the site as well - which can be reported against in various screens within Passwordstate

7 Tagging Data with a Site Location

Once you have added one or Remote Sites on the screen Administration -> Remote Site Administration -> Remote Site Locations, then it is possible to 'tag' different data within Passwordstate to be associated with the site. Following are a list of areas this can be done:

- Active Directory Domains
- Privileged Account Credentials
- Folders and Password Lists
- Hosts and Host Folders
- Discovery Jobs
- Remote Session Credentials (for the Remote Session Launcher feature)
- User Accounts (so clients can login and get read access to their passwords, without consuming a license)
- Scheduled Reports (based on Auditing data)

8 Forcing An Agent Poll

Each Agent that you deploy can have it's own 'Agent Poll Frequency' set - by default, it is every 5 minutes for each Site Location. Below is a screenshot of where this can be changed.

Add New Remote Site Location

To add a new Remote Site Location to Passwordstate, please fill in the details below.

remote site location
allowed ip ranges

Please specify appropriate details below for this Remote Site.

Site Location Name : *

In-Transit Encryption Key : * Generate New Key

Agent Poll Frequency : Minutes

Maintenance Window : * Start Hour Finish Hour
Please schedule Account & Host Discovery Jobs outside of this Maintenance Window.

Remote Session Launcher Gateway URL :
Specify in the format of <https://client1.clickstudios.com.au:7273>

Purge Recorded Sessions :
Older than the specified number of days - leaving as 0 will disable purging.

Save Cancel

If for testing/debugging purposes you do not wish to wait for this Poll Frequency, you can make a change to the PasswordstateAgent.exe.config file at the remote site agent end, to force a poll every minute.

What you need to do is modify the highlighted flag below to True, and then within one minute it will pick up this change and force an Agent poll – the longest you will need to wait is one minute. Remember to set it back once you have finished testing/debugging. Also, if the Agent Poll is still in progress the next time it checks in one minute, it will not perform another Poll – the previous one first needs to finish.

```

PasswordstateAgent.exe.config
1  <?xml version="1.0" encoding="utf-8"?>
2  <configuration>
3    <configSections>
4      <!-- For more information on Entity Framework configuration, visit http://go.microsoft.com/fwlink/?LinkID=237468 -->
5      <section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSection, EntityFramework, Version=6.0.0.0, Culture=neutral, PublicKeyToken=7b4132bf1d4103c9" />
6    </configSections>
7    <startup>
8      <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5" />
9    </startup>
10   <appSettings>
11     <add key="SiteID" value="4" />
12     <add key="InTransitKey" value="29d2a4e518ed8f4ccac86d6403879e260bd49b324488fa7e35dbeaeb84d2533" />
13     <add key="URL" value="https://passwordstate8.halox.net" />
14     <add key="FIPMode" value="False" />
15     <add key="ForceAgentPollEveryMinute" value="False" /> <!-- Used only for troubleshooting purposes, and do not leave on permanently. -->
16   </appSettings>

```