Click Studios

Passwordstate

Open Port Requirements

Table of Contents

1 Overview

This document describes the ports that are required to be open in order for Passwordstate and its modules to function correctly. The documentation described below are the default ports, for which some customer may change.

If required, you can perform "open Port" tests, from your Passwordstate Web Server, using the following PowerShell command:

Test-Netconnection <*server name*> -Port <*port number*>

or

Test-Netconnection <*url*> -Port <*port number*>

If there is a successful connection, the **TcpTestSucceeded** attribute will be returned as **True**.

2 Main Passwordstate Website

By default, the Passwordstate website is installed with port **9119**, but this can be configured to use any port of your choice. Generally, port **443** is the standard port used for HTTPS traffic.

Port **9119** (or **443**) will need to be open on your Passwordstate web server, and as Passwordstate using Microsoft SQL Server has its database, Port 1433 also needs to be open.

3 Active Directory Integration

Passwordstate can integrate with Active Directory to perform a number of tasks, like authenticating your users, synchronizing security groups etc. Your Passwordstate web server will need access to your domain controllers on port **389** for LDAP traffic, and **636** for LDAPS traffic - if you are using LDAPS.

4 High Availability

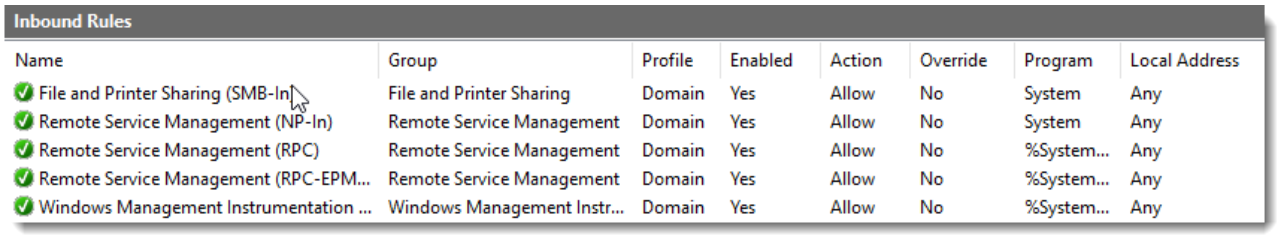
If you are using the Passwordstate High Availability module, then the same default port of 9119 needs to be open on your HA web server, and 1433 for your SQL Server.

If you are using an Active/Passive High Availability configuration, then your HA web server also needs access back to your main Passwordstate web server, as it performs various polling, and reporting back of auditing data. This is done via the API on your Primary Site.

Passwordstate also has the ability to upgrade High Availability instances from the main Passwordstate web site, and this does this using various PowerShell scripts. These scripts require the following ports to be open to your Passwordstate High Availability instance:

- Port 135 & 445 (this is so we can perform a WMI call to manage the remote Windows Services)
- Port 49154 (this is a dynamic port Microsoft can use with the WMI call above as well)

Below is a screenshot of the Windows Firewall Rules which need to be enabled.



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address
File and Printer Sharing (SMB-In)	File and Printer Sharing	Domain	Yes	Allow	No	System	Any
Remote Service Management (NP-In)	Remote Service Management	Domain	Yes	Allow	No	System	Any
Remote Service Management (RPC)	Remote Service Management	Domain	Yes	Allow	No	%System...	Any
Remote Service Management (RPC-EPM...	Remote Service Management	Domain	Yes	Allow	No	%System...	Any
Windows Management Instrumentation ...	Windows Management Instr...	Domain	Yes	Allow	No	%System...	Any

5 Mobile Client

By default, Passwordstate has the mobile client web site built into the main website. There is an option to deploy the Mobile Client web site separately to the main website, and you would normally do this if wanting to host it in your firewalled DMZ environment.

If you have installed the Mobile Client separately, you will need to allow access back to your Passwordstate database server, on the default SQL port of **1433**.

If you are using either Active Directory or SecurID authentication on your Mobile Client, then you will need to allow access back to your Passwordstate server on the default port, which is **9119,** as the Mobile Client Web Site will perform these authentication methods via the API.

6 Browser Extensions

All browser extensions will need to securely communicate with your main Passwordstate website, and these also need access on the default website port, which is **9119.**

7 Self Destruct Messages

The Self Destruct Message web site is by default installed with your main Passwordstate web site. For users to view Self Destruct Messages, they must have access to your standard Passwordstate URL, where the default port is 9119.

There is also an option to install the Self Destruct Message Web site separately to Passwordstate, for which you can select the port to use – again, default port is 9119.

Your users reading Self Destruct Messages will require access to this port, and your main Passwordstate web site will need to also communicate to this port – the main web site performs HTTP POSTS to the Self Destruct web site, but the Self Destruct Web site does not need any access back to your main Passwordstate web site.

8 Email Traffic

It's possible to configure Passwordstate to send various emails, for which the default port for mail is Port 25. If you have configured the system to send email you should ensure your Passwordstate web server can communicate to your email server and the default port for this is **25**.

If you configure your emails settings on any other port for SMTP traffic, you should ensure this port is open.

9 Account Discoveries

Discovery Type	Port(s)
Cisco IOS	SSH - TCP 22
Fortigate	SSH - TCP 22
Hosts (Computer accounts in AD)	389 or 636
HP H3C	SSH - TCP 22
Juniper Junos	SSH - TCP 22
Linux and Mac	SSH - TCP 22
MariaDB	TCP 3306
Microsoft SQL	TCP 1433
MySQL	TCP 3306
Oracle Database	TCP 1521
PostgreSQL	TCP 5432
SonicWall	SSH - TCP 22
Windows Dependencies	Powershell Remoting TCP 5985 & 5986
Windows Local Administrator	Powershell Remoting TCP 5985 & 5986

10 Password Resets

Password Reset Type	Port(s)
Active Directory	TCP 389 or TCP 636, and TCP 88
Cisco IOS	SSH - TCP 22
Dell iDRAC	SSH - TCP 22
F5 BIG-IP Advanced Shell Access	SSH - TCP 22
F5 BIG-IP TMSH Access	SSH - TCP 22
Fortigate	SSH - TCP 22
HP H3C	SSH - TCP 22
HP iLO	SSH - TCP 22
HP Procurve	SSH - TCP 22
Juniper Junos	SSH - TCP 22
Juniper ScreenOS	SSH - TCP 22
Linux and Mac	SSH - TCP 22
MariaDB	TCP 3306
Microsoft SQL	TCP 1433
MySQL	TCP 3306
Oracle Database	TCP 1521
PostgreSQL	TCP 5432
SonicWall	SSH - TCP 22
Windows COM+ Component	Powershell Remoting TCP 5985 & 5986
Windows IIS Application Pool	Powershell Remoting TCP 5985 & 5986
Windows Local Administrator	Powershell Remoting TCP 5985 & 5986
Windows Scheduled Task	Powershell Remoting TCP 5985 & 5986
Windows Service	Powershell Remoting TCP 5985 & 5986

11 Account Validation (Heartbeats)

Account Validation Type	Port(s)
Active Directory	389 or 636
Cisco IOS	SSH - TCP 22
Dell iDRAC	SSH - TCP 22
F5 BIG-IP	SSH - TCP 22
Fortigate	SSH - TCP 22
HP H3C	SSH - TCP 22
HP iLO	SSH - TCP 22
HP Procurve	SSH - TCP 22
Juniper Junos	SSH - TCP 22
Juniper ScreenOS	SSH - TCP 22
Linux and Mac	SSH - TCP 22
MariaDB	TCP 3306
Microsoft SQL	TCP 1433
MySQL	TCP 3306
Oracle Database	TCP 1521
PostgreSQL	TCP 5432
SonicWall	SSH - TCP 22
Windows Local Administrator	135 or 445

12 Host Validation (Heartbeats)

Host Validation Type	Port(s)
Cisco IOS	SSH - TCP 22
Dell iDRAC	SSH - TCP 22
F5 BIG-IP	SSH - TCP 22
Fortigate	SSH - TCP 22
HP H3C	SSH - TCP 22
HP iLO	SSH - TCP 22
HP Procurve	SSH - TCP 22
Juniper Junos	SSH - TCP 22
Juniper ScreenOS	SSH - TCP 22
Linux and Mac	SSH - TCP 22
MariaDB	TCP 3306
Microsoft SQL	TCP 1433
MySQL	TCP 3306
Oracle Database	TCP 1521
PostgreSQL	TCP 5432
SonicWall	SSH - TCP 22
Windows	135 or 445

13 Client Based Remote Session Launcher

Passwordstate has two remote session launchers, and the Client Based Remote Session launcher will use a number of different applications installed o your desktop to establish a connect to remote hosts.

For this to work successfully, your desktops where these Remote Sessions are being initiated from, will require access to the various Host's ports below.

Remote Session Type	Port(s)
RDP	3389
SSH	22
Telnet	22
VNC	5900
Microsoft SQL	1433
TeamViewer	5938, 80 or 443

14 Browser Based Remote Session Launcher

The Browser Based remote session launcher establishes all connections directly from your Passwordstate web server, rather than your desktop – a Gateway is installed on your web server, where all traffic is tunnelled through the gateway.

For this to work you will need to allow incoming traffic into your Passwordstate web server on port **7273**, unless otherwise modified.

You will also need to ensure your web server can communicate to any remote host on either port **22** for SSH, or **3389** for RDP connections.

The Gateway can also be installed separately from your main Passwordstate web site, but the same port requirements above apply for this as well.

15 Password Reset Portal Module

The Password Reset Portal is a separate website which allows users to reset the password for, or unlock, their Active Directory account – it is a Self-Service Password Reset Portal for end users.

The default port for this web site is again 9119, but can be changed to 443 if needed – your users will require access back to the portal site on this port.

The Password Reset Portal will also need to connect back to your main Passwordstate website, so you need to ensure that the portal can communicate through the port you have configured in section 1 of this document, which by default is **9119** unless otherwise modified.

For the Password Reset Portal to successfully contact and perform tasks on your domain controllers, you will also need to ensure the following ports are open between your Passwordstate webserver and your domain controllers:

LDAPS - Port **636**

Event Logs – Ports **135** and **49153**

16 Remote Site Locations Module

The Remote Site Locations module allows you to install an agent on a remote network, whether that be an internal firewalled network, or a site across the internet.

This agent itself does all the network communication itself, by pushing and pulling data to and from your Passwordstate API. On your main firewall, only one port needs to be open for this, and that is the default port of 9119 – again, a lot of customers change this port to be 443.

The objective of this agent is to perform Account Discoveries, Password Resets and Account Validations on the remote network, and the port requirements for this to work are the same as sections 9, 10 and 11 of this document.

On your firewall, you can configure IP based restrictions to firewalls at the remote network end, where you have deployed the agent, but the agent itself only needs one port open to communicate back to your Passwordstate API.