Passwordstate

Enterprise Password Management

Open Port Requirements

Table of Contents

1 Overview

This document describes the ports that are required to be open in order for Passwordstate and all of its extra modules and tools to function correctly.

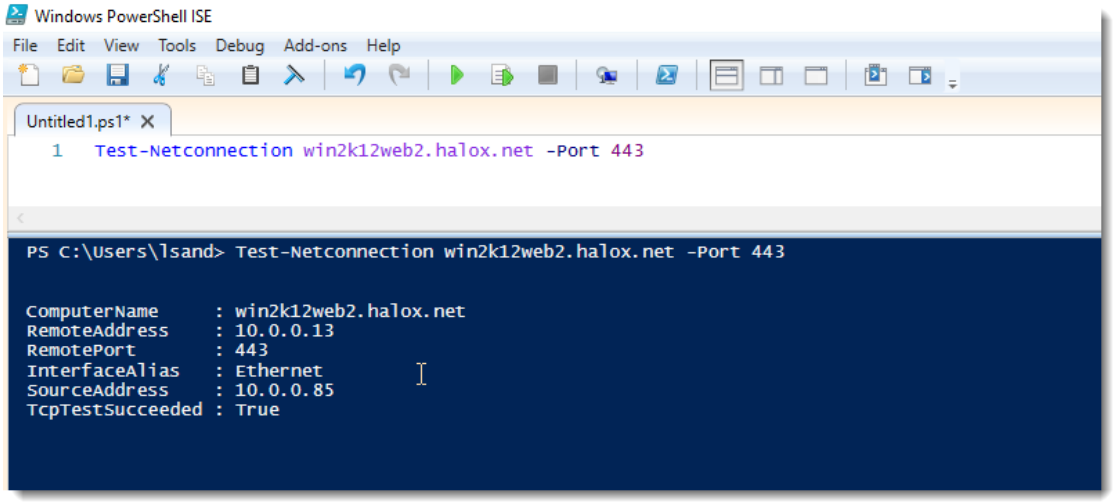
If you want to do some open port tests, you can use the following Powershell commands/syntax:

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

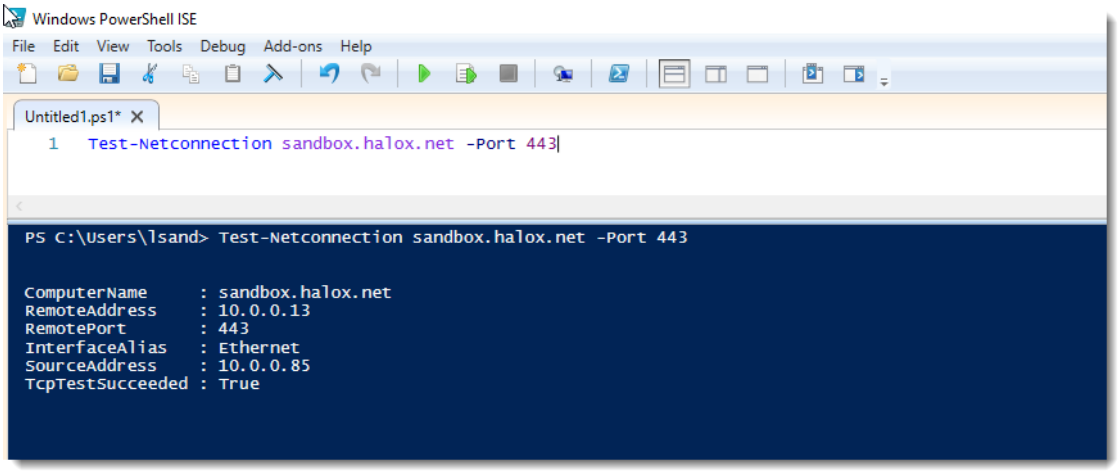
or

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

For example, in my screenshot below, I am testing that my Passwordstate server is accessible on port 443:



In my second screenshot, I am testing my Passwordstate URL is accessible on port 443:



As long as the **TcpTestSucceeded** is **True** then the port is open.

2 Main Passwordstate Website

By default, the Passwordstate website is installed with port **443**, which is the standard port used for HTTPS traffic.

You should allow any incoming HTTPS traffic on port **443** into your Passwordstate web server, unless otherwise modified.

Passwordstate also uses a Microsoft SQL database to store all of its information, and the default port for this is **1433**. If you host your database on a separate server to your Passwordstate install, then you should ensure this port is accessible from your Passwordstate web server.

3 Active Directory Integration

Passwordstate can be integrated with Active Directory to perform a number of tasks, like authenticating your users or synchronizing security groups etc. Your Passwordstate web server will need access to your domain controllers on

- UDP Port 389 (all protocols below need this port open, so a Domain Controller can be found)
- LDAP (UDP Port 389)
- LDAPS (TCP Port 636)
- Kerberos (UDP/TCP Port 88 and 464)

4 High Availability

If you are using the High Availability module and your second Passwordstate website is set to **Passive**, your second web server will need to be able to communicate to your primary webserver on the default website port. This is **443** unless you have modified this setting.

5 Passwordstate App Server

If you have installed the Passwordstate App Server, using for Mobile Apps and Self Destruct Message web site, you will need to allow access back to your Passwordstate database server, on the default SQL port of **1433** unless otherwise modified.

If you are using a SQL Listener for database connectivity, you will need to allow port 1434 UDP – unless you have modified the default port.

6 Self Destruct Website (Push /Pull version)

Passwordstate has three ways you can access you Self Destruct Messages.

Using the Embedded Version

By default, Self Destruct Messages come pre-installed with your core Passwordstate website, and you'll access your messages by appending **/selfdestruct** to your Passwordstate URL.

This method requires your users to have direct access to your Passwordstate website, using the default port you have assigned which is **443** unless otherwise modified.

Using Passwordstate AppServer

See **Section 5** of this document

Using the Push/Pull method

This method enables you to install a Self Destruct site hosted in IIS on any server of your choice. Your core Passwordstate webserver will "**Push**" messages to this separate website, where they will be stored waiting to be read. If there is any auditing information available at this time, it will "**Pull**" that information back to the core Passwordstate website.

The end user will then need access to this separate site to read the messages, which uses a default port of **443** unless otherwise modified.

At no time does the Self Destruct separate site attempt to contact your core Passwordstate website when using the **Push/Pull** method.

A System Administrator would typically set up Self Destruct messages using Push/Pull as the Self Destruct Portal does not need a port open from the DMZ back inside your internal network.

7 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 **443** unless otherwise modified.

8 Email Traffic

It's possible to configure Passwordstate with your email sever settings to allow it to automatically send notifications to your users for various reasons. 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)
Active Directory	TCP 9389, TCP 389 or TCP 636, TCP 88 and TCP 445
Cisco IOS	SSH - TCP 22
Fortigate	SSH - TCP 22
Hosts (Computer objects 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
VMWare ESXi	SSH - TCP 22 or 443 if using Powershell PowerCLI Module
Windows Dependencies	Powershell Remoting TCP 5985 (HTTP) & 5986 (HTTPS) WMI negotiation on TCP 135
Windows Local Administrator	Powershell Remoting TCP 5985 (HTTP) & 5986 (HTTPS) WMI negotiation on TCP 135

10 Password Resets

Password Reset Type	Port(s)
Active Directory	TCP 9389, TCP 389 or TCP 636, TCP 88 and TCP 445
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
IBM IMM	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
PaloAlto	SSH – TCP 22
PostgreSQL	TCP 5432
SonicWall	SSH - TCP 22
VMWare ESXi	SSH – TCP 22 or 443 if using Powershell PowerCLI Module
Windows COM+ Component	Powershell Remoting TCP 5985 (HTTP) & 5986 (HTTPS)
Windows IIS Application Pool	Powershell Remoting TCP 5985 (HTTP) & 5986 (HTTPS)
Windows Local Administrator	Powershell Remoting TCP 5985 (HTTP) & 5986 (HTTPS)
Windows Scheduled Task & Windows Service	Powershell Remoting TCP 5985 (HTTP) & 5986 (HTTPS)

11 Account Validation (Heartbeats)

Account Validation Type	Port(s)
Active Directory	TCP 9389, TCP 389 or TCP 636, TCP 88 and TCP 445
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
IBM IMM	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
PaloAlto	SSH – TCP 22
PostgreSQL	TCP 5432
SonicWall	SSH - TCP 22
VMWare ESXi	SSH – TCP 22 or 443 if using Powershell PowerCLI Module
Windows Local Administrator	135 or 445

12 Host Validation (Heartbeats)

Host heartbeats work in two stages:

First, a ping request will be sent to the remote host on the **ICMPv4** protocol. This does not require a port to be open on the remote machine, however the firewall on the remote host can have a rule to block ICMPv4 requests.

If the ping test fails, Passwordstate attempts to do a new open port test on the remote session connection protocol, which by default is 3389 for RDP and 22 for SSH.

If both tests fail, the heartbeat is considered a failure.

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 on your desktop to establish a connect to the remote host.

For this to work successfully, you will need to ensure the machine where you are accessing Passwordstate from can communicate to the remote host on the following ports:

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 the Browser Based Gateway Service. The Gateway Service is normally installed on the same server where you have Passwordstate installed, but it can be installed separately if you wish, or even on a remote site.

For Browser Based Sessions to work you will need to allow incoming traffic into your Gateway server on port **7273** – 7273 is the default port, but you can configure the gateway to use any port number you like.

This connection to port 7273 occurs from your PC browser, and not the Passwordstate web server itself.

When you open an RDP or SSH session, html files are accessed on your Passwordstate web server. Once these files are loaded into your PC browser, a call is made to your Passwordstate API, using the URL you see visible in the address bar in your browser. Once there is a successful connection to the API, then the gateway is accessed – again, from your PC browser.

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

15 Password Reset Portal

The **Password Reset Portal** (**PRP**)is an additional module available for Passwordstate, which is installed as its own stand-alone web site.

The web site can be installed on any Windows server of your choice, and typically you would host this in your DMZ, but it really depends on your requirements. You could install it on your existing Passwordstate webserver, on another shared server in your DMZ, or even on a server you have provisioned in the cloud.

The **PRP** website communicates securely back to your main **Passwordstate** website, with all traffic encrypted within the SSL tunnel. All business logic like authentication, verification, resetting passwords etc, is performed by your core Passwordstate website.

The **PRP** website is merely the front facing website your users will access to initial the resetting, or the unlocking of their Active Directory password.

From your **PRP** Server, you must have appropriate ports open back to your Passwordstate web server i.e. generally Port **443**, unless you are using a non-standard port by default for HTTPS.

By default, Kerberos will be used for communication back to your domain when password resets or account unlocks are requested, and **ports 88** and **464** need to be open on your domain for this to work.

Alternative to Kerberos, you may wish to use LDAPS for Active Directory Communication, which instead uses Port **636**.

Summary of these Ports can be found below:

Password Reset Portal Ports
Your users will need to connect to your Password Reset Portal (PRP) website, which is installed using **Port 443**. This will present them to the page to begin the process of resetting or unlocking their own Active Directory password/account.

Passwordstate Web Site Ports
The Password Reset Portal (PRP) needs to communicate back to your Passwordstate API, so generally **Port 443** is required to be open on your Passwordstate webserver. If you are using a different port for your Passwordstate web site, then this port will instead need to be open.

Domain Ports

- **Port 636** - this is required if using **LDAP over SSL** (**LDAPS**), so the Passwordstate UI and API can communicate with Active Directory to reset and unlock accounts
- **Port 88 and 464** is required if using **Kerberos**, so the Passwordstate UI and API can communicate with Active Directory to reset and unlock accounts
- **Ports 135 and Dynamic Ports** - To query Event Logs on Domain Controllers for account lockouts, Port 135 needs to be open, and also the existing Windows Firewall rule "**Remote Event Log Management (RPC)**", which uses dynamic ports

16 Remote Site Locations

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 needs to communicate back to your main Passwordstate website, so you need to ensure the server that you install this agent on can communicate through the port you have configured in section 1 of this document.

By default, this is **443** unless otherwise modified.

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 8, 9, 10 and 11 of this document.