PasswordState Enterprise Password Management

Password Reset Portal

Installation Instructions

This document and the information controlled therein is the property of Click Studios. It must not be reproduced in whole/part, or otherwise disclosed, without prior consent in writing from Click Studios.

Table of Contents

1	SYSTEM REQUIREMENTS - GENERAL	3
2	ARCHITECTURAL OVERVIEW	4
3	INSTALLING PASSWORD RESET PORTAL	5
4	ENCRYPTING THE APPSETTINGS SECTION IN THE WEB.CONFIG FILE	8
5	RESET PORTAL URL	9
6	SSL CERTIFICATE CONSIDERATIONS	10
7	ACTIVE DIRECTORY CERTIFICATE AUTHORITY	13
8	ADDITIONAL CERTIFICATE CONSIDERATIONS	14
9	OPEN PORT CONSIDERATIONS	21
10	WINDOWS CREDENTIAL PROVIDER INFORMATION	22
11	UPDATING THE PASSWORD RESET PORTAL URL FOR EXISTING INSTALLATIONS OF THE	
WIN	DOWS CREDENTIAL PROVIDER	23
12	RATE LIMIT CONNECTIONS TO WEB SITE	24

1 System Requirements - General

Passwordstate's Password Reset Portal (**PRP**) is an additional website that you'll install on a Windows server of your choice with the following required components:

- Microsoft Windows Server 2016, 2019, 2022, 2025 or Windows 11
- Microsoft .NET Framework 4.7.2 or above
- A separate install of **Passwordstate**, preferably configured using a trusted SSL Certificate, as the Password Reset Portal communicates with Passwordstate's API
- Your domain must be at **2012 functional level** or higher
- If using LDAPS instead of the default protocol "Kerberos" for domain communication, you will need an internal Certificate Authority, which allows for LDAP over SSL on port 636 (instructions included)

2 Architectural Overview

The **Password Reset Portal** (which we'll refer to as **PRP** for the rest of this document) 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.

If you would prefer to use LDAPS to communicate to your domain, you must also have a **Domain Certificate Authority** installed – instructions are provided in this document as well on how to install a CA.

3 Installing Password Reset Portal

The Password Reset Portal installer can be downloaded from the screen **Administration** -> **Password Reset Portal Administration** within Passwordstate.

- 1. As an Administrator on your server, run 'PasswordResetPortal.exe'
- 2. At the 'Password Reset Portal' screen, click on the 'Next' button

Passwordstate Password R	eşet Portal - InstallAware Wizard — 🗆 🗙
	Welcome to the InstallAware Wizard for Passwordstate Password Reset Portal
	The InstallAware Wizard will install Passwordstate Password Reset Portal on your computer.
	WARNING: This program is protected by copyright law and international treaties.
	To continue, dick ivext.
	< Back Next > Cancel

3. Accept the Licence Agreement and click 'Next'



D	Destination Folder Select folder where setup will install files.		-
			-
	Install Passwordstate Password Reset Portal to:		
	c: \inetpub \PasswordstateResetPortal	Change.	
	Destination Folder Required Disk Space:	44, 124	KB

5. Next you will need to specify a URL for your Password Reset Portal website, and also the URL of your existing Passwordstate website. By default, the installer will choose your server netbios name as the URL as this will already have functioning DNS, but it is possible to change this to any value you like. If any changes are made to this URL, a matching DNS CNAME record will need to be created, and a matching SSL certificate must be assigned in Internet Information Services (IIS) after the installation has completed

You must also specify the Portal Web Site Communication API Key, which you can obtain from the screen **Administration** -> **Password Reset Portal Administration** -> **System Settings** -> **API** tab in Passwordstate:

A Passwordstate Password Reset Portal - InstallAware Wizard —	□ X
Specify Web Site URL and Communication API Key	
Please specify the web site URL you would like to use for the Reset Portal:	
https://portal.mydomain.com	
Please specify the the URL for your Passwordstate web site, and Port Number	
https://passwordstate.mydomain.com Port Number 443	
Please specify your Portal Web Site Communication API Key:	
3f6eb538a2497cdc492ab837d35e6f78	
Add a Windows Firewall Exception for the Port Above	
InstallAware	
< Back Next >	Cancel

6. To begin the installation, click 'Next'

Passwordstate Password Re	eset Portal - InstallAware Wizard 🛛 — 🖂 🔀
6	Completing the InstallAware Wizard for Passwordstate Password Reset Portal
	The InstallAware Wizard is now ready to configure Passwordstate Password Reset Portal on this computer.
	- Click Next to begin configuration
	- Click Back to change settings
	- Click Cancel to exit
	< Back Next > Cancel

7. To finalize the installation, click **'Next'** and then **'Finish**'

Passwordstate Password Re	eset Portal - InstallAware Wizard — 🗌 🗙
▶ 🚺	Completing the InstallAware Wizard for Passwordstate Password Reset Portal
	The InstallAware Wizard is now ready to configure Passwordstate Password Reset Portal on this computer.
	- Click Next to begin configuration
	- Click Back to change settings
	- Click Cancel to exit
	< Back Next > Cancel

4 Encrypting the AppSettings Section in the Web.config file

It is highly recommended to encrypt the "**appSettings**" section in the web.config file, so any sensitive information such as your Communication API Key is unreadable in the file.

To encrypt this file, follow this complete guide: https://www.clickstudios.com.au/downloads/version9/Encrypt_Passwordstate_Config_Files.pdf

5 Reset Portal URL

Once you have finished installing the Password Reset Portal, log into yoru Passwordstate website and set your URL under Administration -> Password Reset Portal Administration -> System Settings:

¢	S١	/stem	Setti	no	IS
	-	,	2000		-

o modify the system settings fo	or the Pass	word Reset mo	dule, please make changes	within the appropria	te tabs below, then click on the 'Save' butto	n.
active directory options	ani	branding	error customizations	miscellaneous	password expiry reminder template	syslag server
Please select various Miscellar	neous setti	ngs below as a	ppropriate.	mocellaneous	publicità expiry reminaer template	byblog berver
Miscellaneous Settir	ngs					
Specify the URL for the https://portal.mydomain.	Password com	Reset Portal, v	which will be used used wi	thin the body of ap	propriate emails:	
By specifying a 'Return you've specified below:	UKL belov	w, Exit buttons	will be visible on each sc	reen in the portal, a	nd clicking the Exit button will return yo	u to the URL
Query Domain Controlle	er event lo	gs for account	lockout events every: 5	 Minutes 		
(The querying of event log	g data will	only return the	past (x) minutes of data, th	e same as the time-fi	ame selected above)	
Use regular expressions	when mat	tching 'Bad Pa	sswords': 👳			
With the Password Rese active session after the f Blocked IPs)	t Portal, p following	rotect against number of fail	brute force dictionary au ed login attempts: (Blocke	thentication attemp ed IP Addresses can b	ts on the initial Identification screen by I e removed on the screen Administration ->	ocking out an Brute Force
3						
						Save Save & Close

6 SSL Certificate Considerations

The installer for Password Reset Portal (PRP) installs a self-signed SSL certificate on your web server, and binds it to the Password Reset Portal web site.

Note It is highly recommended to use a purchased an SSL certificate from an online trusted certificate authority, which will ensure a more secure and user-friendly experience for your users, on all types of devices on any type of connection (internal, internet etc)

If you have your own SSL certificate you'd prefer to use, install it on your PRP server and bind it to your HTTPS binding.

If you wish to continue using the self-signed SSL certificate, then you may want to instruct your users to "Install" the certificate on their computer, so the various Internet browsers don't complain about the certificate not being issued by a trusted authority.

To install the certificate, you can follow these steps below. You will effectively be exporting the certificate and reimporting it into your **Trusted Root Certificate store** on your machine. The example below uses **Google Chrome** as the browser, but you can achieve the same thing in other browsers.

Using **Chrome**, browse to your Password Reset Portal web site and you should see a screenshot with an error saying **NET:ERR_CERT_AUTHORITY_INVALID**





Click on the **Not Secure** button, and then click on the **Show Certificate** button:

Under the Details tab, click Copy to File...

🧏 Certifi	cate			×
General	Details	Certification Path		
Show:	<all></all>		~	
Field			Value	^
Ver Ser Sig Sig Sig Sig Sig Vali	sion ial numbe nature ha uer id from id to <u>viect</u>	er gorithm Ish algorithm	V3 1ba340eac8b413ad49985789 sha256RSA sha256 demoserver01 Thursday, 31 December 2020 Wednesday, 31 December 20 demoserver01	~
		Ed	it Properties Copy to File	
			O	<

Run through the **Certificate Export Wizard**, leaving all default options. During the process, set a name for your certificate (which can be anything), and save it to disk.

Now go to **Start** -> **Run** and type in **certIm.msc** and hit enter. This opens up the **Local Computer Certificate Store** on your computer.

Expand out Trusted Root Certificate Authorities and right click Certificates, and choose All Tasks -> Import:

👼 certlm - [Certificate:	s - Local Com	nputer\Tru	isted Root Certification Autho	orities\Certifi — 🗆 🗙	(
File Action View	Help				
🗢 🔿 🖄 📰 📋	o 🗟	?			
 Certificates - Local C Personal Trusted Root Cer Certificates Enternrise 	Computer A tification	Issued T C AAA C Baltir	o Certificate Services more CyberTrust Root Import	Issued By AAA Certificate Stances Baltimore CyberTrust Root Class 3 Public Primary Certificatio	^
 Intermedia Trusted Pul Untrusted (Third-Parts 	View Refresh	>	right (c) 1997 Microsoft C ert Assured ID Root CA ert Global Root CA	clickdemo-DEMODC01-CA Copyright (c) 1997 Microsoft Corp. DigiCert Assured ID Root CA DigiCert Global Root CA	
 Trusted Pec Client Auth Preview Build Ro 	Help	Ligi DigiC	ert Global Root G2 ert High Assurance EV Ro ert Trusted Root G4	DigiCert Global Root G2 DigiCert High Assurance EV Root DigiCert Trusted Root G4	
 Test Roots Local NonRemov MSIEHistoryJourn Remote Desktop Certificate Enroll Smart Card Trust 	vable Ceri nal ment Rec	Globs Globs Globs Globs Globs	Root CA X3 alSign alSign alSign Root CA addy Class 2 Certification	DST Root CA X3 GlobalSign GlobalSign GlobalSign Root CA Go Daddy Class 2 Certification Au	~
Add a certificate to a stor	re	-			

Now run through the import process, using all default options, and browse to the certificate you saved disk in the step above. Once this completes, you will see a **Successful Import** message.

You can now restart your browser and try browsing to your Password Reset Portal URL again, and you will no longer see the browser warning about the certificate.

Note 1: For an in-depth explanation of the different types of certificates you can use on your **PRP** website, please see this forum post: <u>https://forums.clickstudios.com.au/topic/2978-passwordstate-certificates-explained/</u>

7 Active Directory Certificate Authority

By default, the Password Reset Portal will send all Active Directory tasks to your core Passwordstate webserver. Your Passwordstate web server will then attempt to communicate to your domain using the Kerberos protocol by default.

If you do not wish to use Kerberos, you can instead use LDAPS, or LDAP over SSL. When using LDAPS, you must have installed/configured a **Certificate Authority** in each of the domains where you wish to reset or unlock user's domain accounts. This is will honour any **Domain Password Policies**, or **Fine-Grained Password Policies** from these domains.

Please follow these step-by-step instructions to set up a Certificate Authority: https://forums.clickstudios.com.au/topic/2934-how-to-set-up-a-internal-certificate-authority/

8 Additional Certificate Considerations

If you intend to use additional domains that your Passwordstate Web Server is not a member of, then you will need to export the domain certificate from these domains, and import them onto your core **Passwordstate** web server. (*Not the Password Reset Portal server*)

This is required so the API can securely communicate with these other domains. If this is a requirement for you, you can follow these steps:

Export the Domain CA Certificate

- On your server that has the CA installed, Click Start > Control Panel -> System and Security -> Administrative Tools -> Certificate Authority to open the CA Microsoft Management Console (MMC) GUI
- 2. Right-click the CA server and select Properties

🙀 certsrv - [Certification Authority	(Local)]			—	×
File Action View Help					
(⇔ ⇒) 🔒 👔 🕨 🗖					
Certification Authority (Local)	Name		Description		
	All Tasks	K16AD-CA	Certification Authority		
	Refresh				
	Properties				
	Help				
Opens the properties dialog box for th	e current selection.				

Extensions	Storage		Certificate I	Manager	s
nrollment Agents	Auditing	Recover	v Agents	Sec	- uri
General	Policy Mod	lule	Exit	t Module	-
Certification authorit	ty (CA)				
Name:	Fabrikam-WIN	2K16AD-C	Ą		
CA certificates:					
Certificate #0					
Centificate #0					
Coluneate #0					
Contribute #0					
			View C	ertificate	
			View C	ertificate	•
Cryptographic settin	ngs		View C	ertificate	•
Cryptographic settin Provider:	ngs Microsoft Softv	vare Key Si	View C	čertificate	:
Cryptographic settin Provider:	igs Microsoft Softv	vare Key Si	View C corage Provi	iertificate	•

4. On the Details tab, click Copy to File



3. From the General tab, click View Certificate

5. Click Next



6. Choose Base-64 encoded X.509(.CER) and click Next

← 🛛 🐉 Certificate Export Wizard		
Export File Format Certificates can be exported in a variety of file formats.		
Select the format you want to use:		
O DER encoded binary X.509 (.CER)		
Base-64 encoded X.509 (.CER)		
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)		
Include all certificates in the certification path if possible		
Personal Information Exchange - PKCS #12 (.PFX)		
Include all certificates in the certification path if possible		
Delete the private key if the export is successful		
Export all extended properties		
Enable certificate privacy		
O Microsoft Serialized Certificate Store (.SST)		
Next Cano	el:	

~ ~	F Certificate Export Wizard
	File to Export Specify the name of the file you want to export
	File name: C:\Users\\Desktop\DomainCertificate.cer Browse
	Next Cancel
_	
Click	: Finish
÷	Sertificate Export Wizard
÷	Certificate Export Wizard
÷	Source Certificate Export Wizard Completing the Certificate Export Wizard Vou have successfully completed the Certificate Export wizard.
~	Certificate Export Wizard Completing the Certificate Export Wizard You have successfully completed the Certificate Export wizard. You have specified the following settings:
÷	Certificate Export Wizard Completing the Certificate Export Wizard You have successfully completed the Certificate Export wizard. You have specified the following settings: File Name C:\Users\\sand\Desktop\DomainCertific
÷	✓ Certificate Export Wizard Completing the Certificate Export Wizard You have successfully completed the Certificate Export wizard. You have specified the following settings: <u>File Name C: Users \sand \Desktop \DomainCertific Export Keys No Include all certificates in the certification path No File Format Base64 Encoded X.509 (*.cer) </u>
~	Image: Construct Export Wizard Completing the Certificate Export Wizard You have successfully completed the Certificate Export wizard. You have specified the following settings: Image: C:\Users\sand\Desktop\DomainCertificates in the certification path No Include all certificates in the certification path No Image: C:\Users\sand\Desktop\Certificates in the certification path No Image: C:\Users\Sand\Desktop(*,cer)
~	✓ Certificate Export Wizard Completing the Certificate Export Wizard You have successfully completed the Certificate Export wizard. You have specified the following settings: Image: Set the Set of Se

9. Transfer the certificate to your Passwordstate web server and close all windows.

Importing the Certificate into your Passwordstate web server

- 1. On your Passwordstate web server, open **Certificate Manager** by typing **certIm.msc** into your Run command bar
- 2. Expand Trusted Root Certificate Authorities -> Certificates
- 3. Right Click Certificates and select All Tasks -> Import



4. Click Next

Certificate Import Wizard				
Welcome to the Certificate Import Wizard				
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.				
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.				
Store Location Current User I Local Machine				
To continue, click Next.				
Next Cancel				

6.

5. Browse to the certificate and click Next

📀 🝠 Certificate Import Wizard
File to Import
Specify the file you want to import.
File name: C:\Users\sand\Desktop\DomainCertificate.cer Browse
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Next Cancel
ick Next

v

÷	Certificate Import Wizard	×
	Certificate Store Certificate stores are system areas where certificates are kept.	
	Windows can automatically select a certificate store, or you can specify a location for the certificate.	
	O Automatically select the certificate store based on the type of certificate	
	Place all certificates in the following store	
	Certificate store:	
	Trusted Root Certification Authorities Browse	
	Next Cano	el

7. Click Finish and then OK

	×				
🔄 🔄 Certificate Import Wizard					
Completing the Certificate Import Wizard					
The certificate will be imported after you click Finish.					
You have specified the follo	You have specified the following settings:				
Certificate Store Selected	by User Trusted Root Certification Authorities				
Content File Name	Certificate				
File Name	C: (User's (sand (Desktop (DomainCer uncate, cer				
Finish Cancel					

8. This ends the import process, and your domains should now be able to securely communicate using LDAP over SSL

9 Open Port Considerations

To ensure the Password Reset Portal functions correctly, there are various ports which need to be open on your network for both the Password Reset Portal web site itself, but also for your Passwordstate webserver so it can communicate with Active Directory Domains, and Event Logs on Domain Controllers as well. Below is a summary of these ports.

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
- 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

If you are unsure if the ports above are open, or if you believe you are having some issues because of blocked ports, you can use the following PowerShell command examples (using contoso.com as the domain)

Test-NetConnection contoso.com -Port 636

Test-NetConnection contoso.com -Port 88

Test-NetConnection contoso.com -Port 464

Test-NetConnection contoso.com -Port 135

Test-NetConnection contoso.com -Port 49153

Testing the Password Reset Portal port is open (using **dmz01.contoso.com** as the server's name which is hosting the PRP)

Test-NetConnection dmz01.contoso.com -Port 443

10 Windows Credential Provider Information

A Windows Credential Provider is also available, to be installed on your Windows Desktops to provide a link where users can reset their account's passwords from the Windows Logon screens. The Windows Credential Provider is supported to be install on Windows 10 or Windows 11.

As Microsoft no longer supports Internet Explorer, and Google Chrome and Microsoft Edge do not provide a true kiosk mode with these browsers, Click Studios' bundles their own minimal chromium-based browser with the Windows Credential Provider.

Download Instructions

The Windows Credential Provider installer can be downloaded from the Checksums page on our Click Studios' web site here - <u>https://www.clickstudios.com.au/passwordstate-checksums.aspx</u>

Installation Instructions

The Windows Credential Provider must be installed in silent mode, and run as an Administrator. This can either be done from a command prompt, or a software deployment solution, using the syntax below.

PasswordstateCredentialProvider.exe /s Text="Reset Password/Unlock Account" Url="https:// portal.mydomain.com"

"Text" is the title of the link you want to display on your login screens, and "Url" is the URL of your Password Reset Portal web site.

Upgrade Instructions

To upgrade an existing installation of the Windows Credential provider, you use the same install syntax mentioned above for "Installation Instructions".

Uninstallation Instructions

To uninstall the Windows Credential Provider, you can use the command line syntax below:

PasswordstateCredentialProvider.exe /s MODIFY=FALSE REMOVE=TRUE UNINSTALL=YES

As some files have been created, or modified, during the usage of the Windows Credential Provider, not all files would be removed with the command above. To remove these files, please follow these instructions:

- 1. Delete the folder C:\Program Files\PasswordstateCredentialBrowser
- 2. Delete the file C:\Windows\System32\Passwordstatecp_config.ini

11 Updating the Password Reset Portal URL for Existing Installations of the Windows Credential Provider

If you need modify the URL an existing installation of the Windows Credential Provider is using, you will need to edit the file C:\Windows\System32**Passwordstatecp_config.ini**, and modify the URL line as appropriate.

Alternatively, you could uninstall and reinstall the Windows Credential Provider, as per the instructions on the previous page of this document.

12 Rate Limit Connections to Web Site

If you would like to rate limit the number of connections to your Password Reset Portal web site by the IP Address of the accessing client, then this is possible with a configuration in Internet Information Services (IIS).

For further information on how to configure this, please refer to the following Microsoft documentation https://docs.microsoft.com/en-

us/iis/configuration/system.webserver/security/dynamicipsecurity/denybyrequestrate