Passwordstate

Enterprise Password Management

Password Reset Portal

Installation Instructions

Table of Contents

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 2012 R2, 2016, 2019, 2022 or Windows 10, 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.

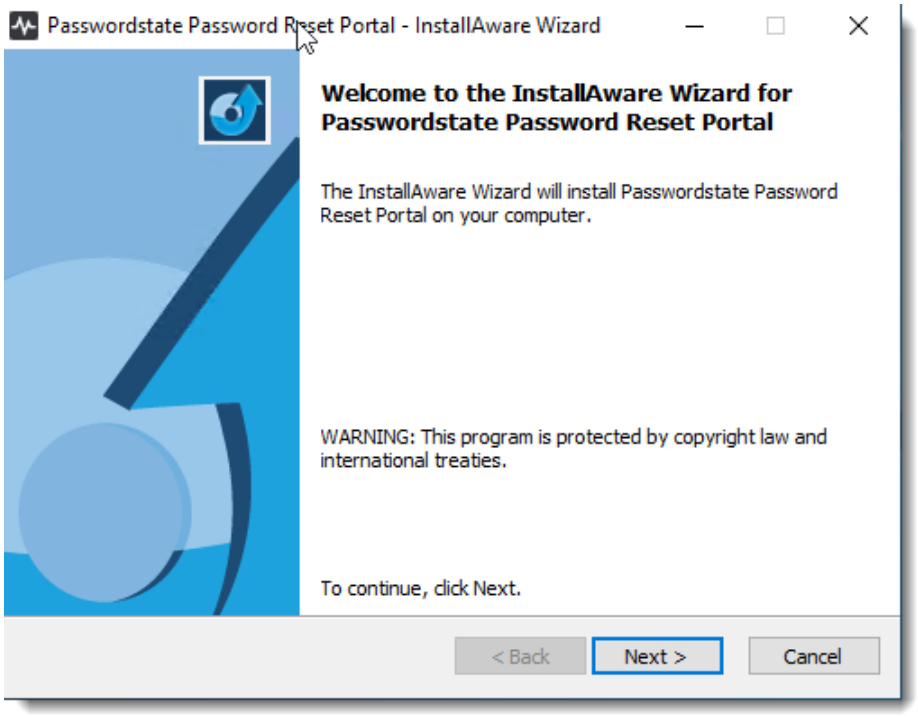
If you would prefer to use LDAPS to communicate to your domain, you must also have a **Domain Certificate Authority** installed – instructions are provided in this document as well on how to install a CA.

3 Installing Password Reset Portal

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

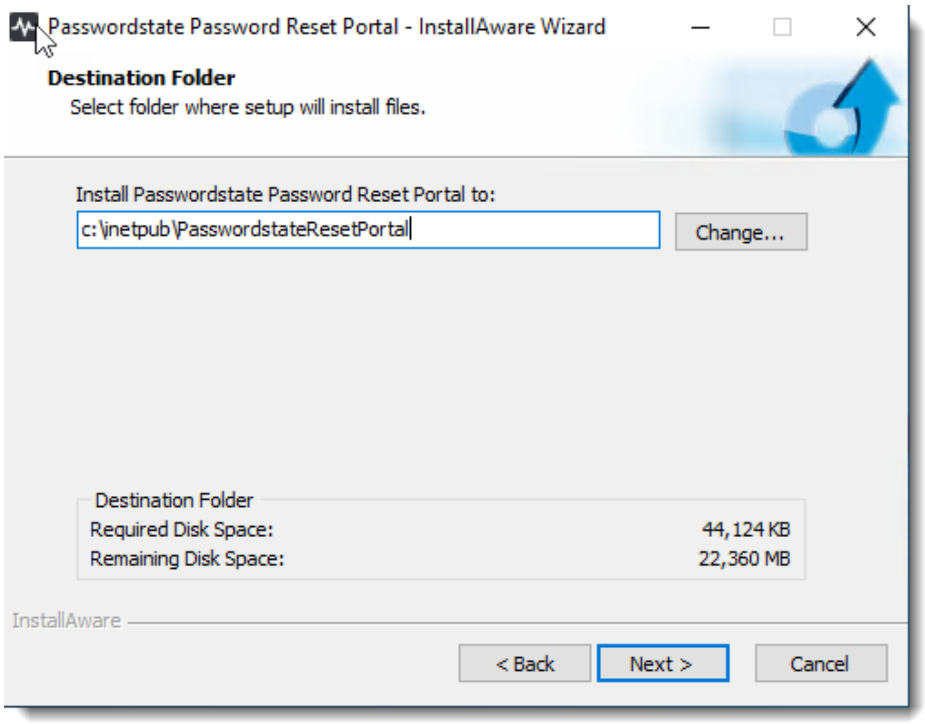
1. As an Administrator on your server, run '**PasswordResetPortal.exe**'

2. At the '**Password Reset Portal**' screen, click on the '**Next**' button



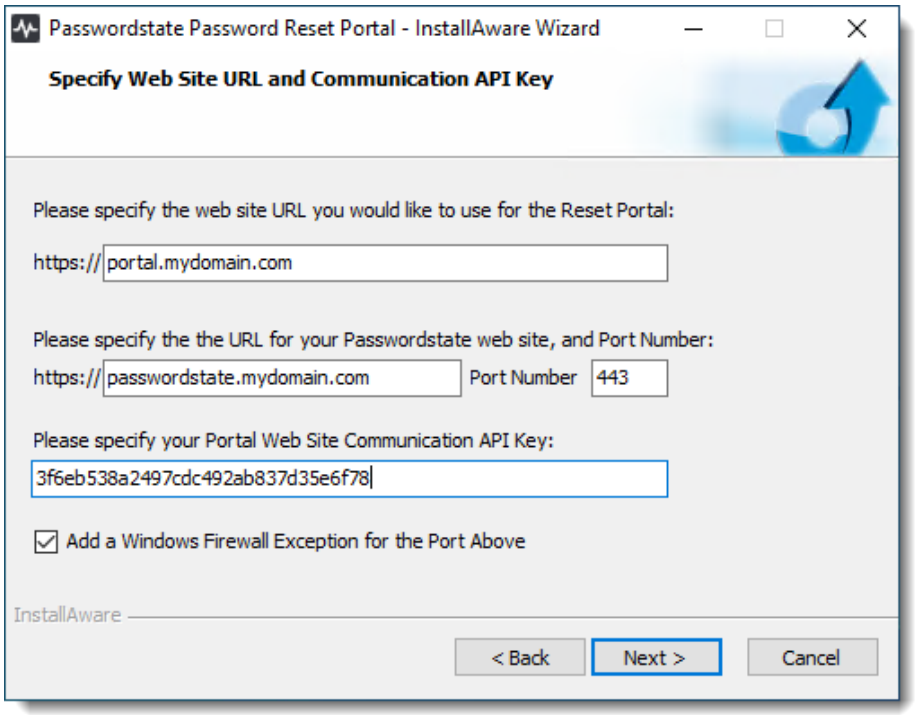
3. Accept the Licence Agreement and click '**Next**'

4. Accept the default installation path, and click '**Next**'



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:



6. To begin the installation, click '**Next**'

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

4 Encrypting the AppSettings Section within the Web.config file

To hide sensitive information in your web.config file, it is recommended you encrypt the AppSettings section. Instructions for this can be seen below:

Encrypt AppSettings Section

- Open a command prompt (as Administrator) and type or copy the line below, and hit enter:

  CD C:\Windows\Microsoft.NET\Framework64\v4.0.30319
- Now type the following and hit enter again, you should see a “Success” message:

  aspnet_regiis.exe -pef "appSettings" "c:\inetpub\PasswordstateResetPortal"

If you need to decrypt the web.config file to make it readable again for any reason, follow these instructions:

Decrypt AppSettings Section

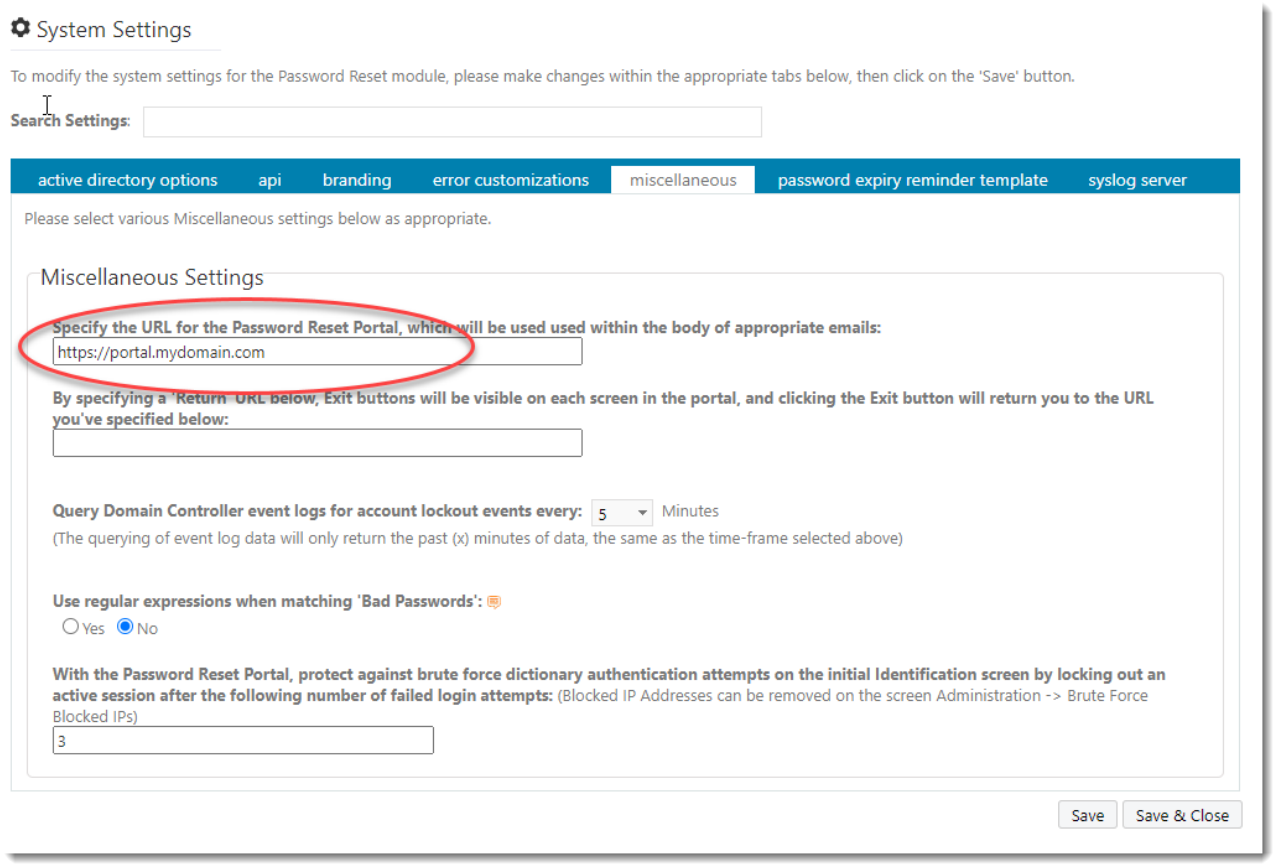
- Open a command prompt (as Administrator) and type or copy the line below, and hit enter:

  CD C:\Windows\Microsoft.NET\Framework64\v4.0.30319
- Now type the following and hit enter again, you should see a “Success” message:

  aspnet_regiis.exe -pdf "appSettings" "c:\inetpub\PasswordstateResetPortal"

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**:



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.

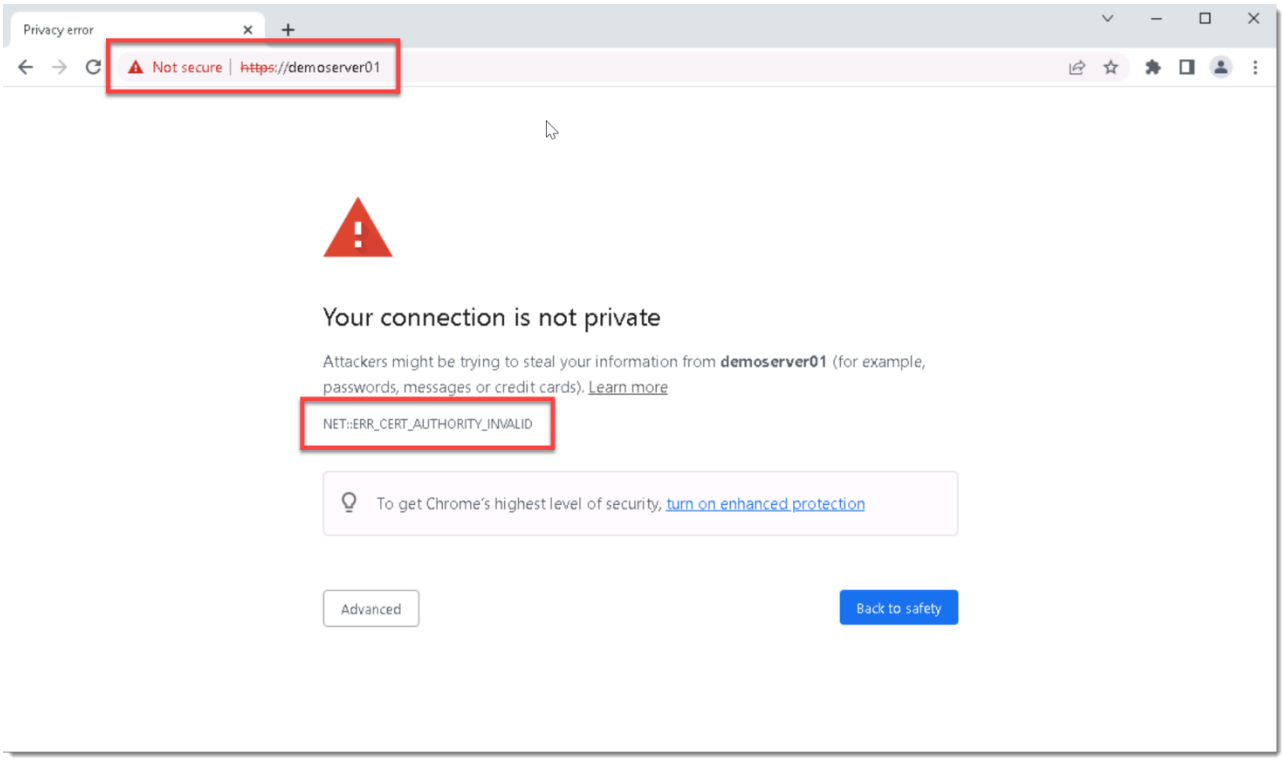
Note It is highly recommended to use a purchased an SSL certificate from an online trusted certificate authority, which will ensure a more secure and user-friendly experience for your users, on all types of devices on any type of connection (internal, internet etc)

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.

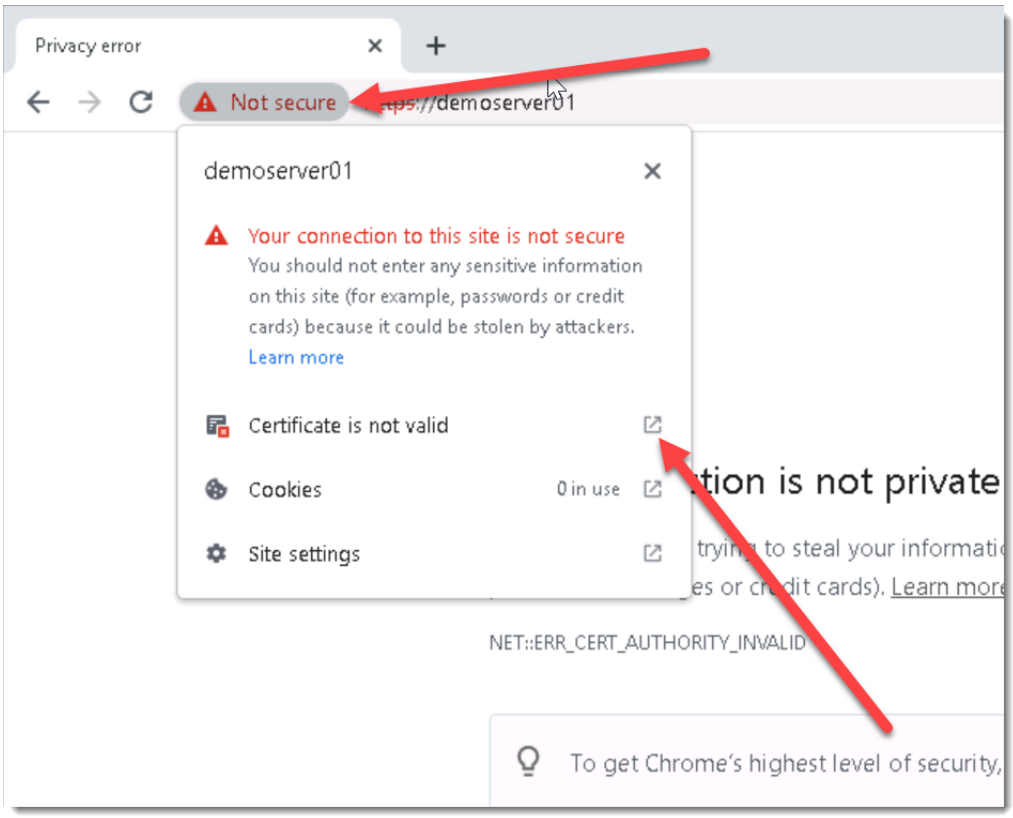
If you wish to continue using the self-signed SSL certificate, then you may want to instruct your users to "Install" the certificate on their computer, so the various Internet browsers don't complain about the certificate not being issued by a trusted authority.

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.

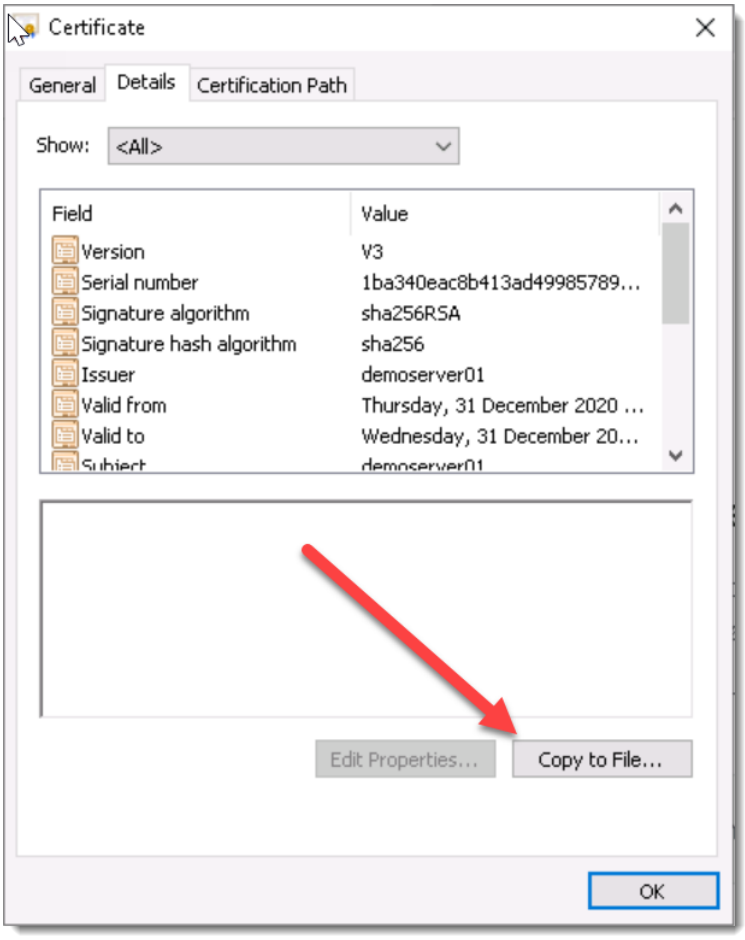
Using **Chrome**, browse to your Password Reset Portal web site and you should see a screenshot with an error saying **NET:ERR_CERT_AUTHORITY_INVALID**



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



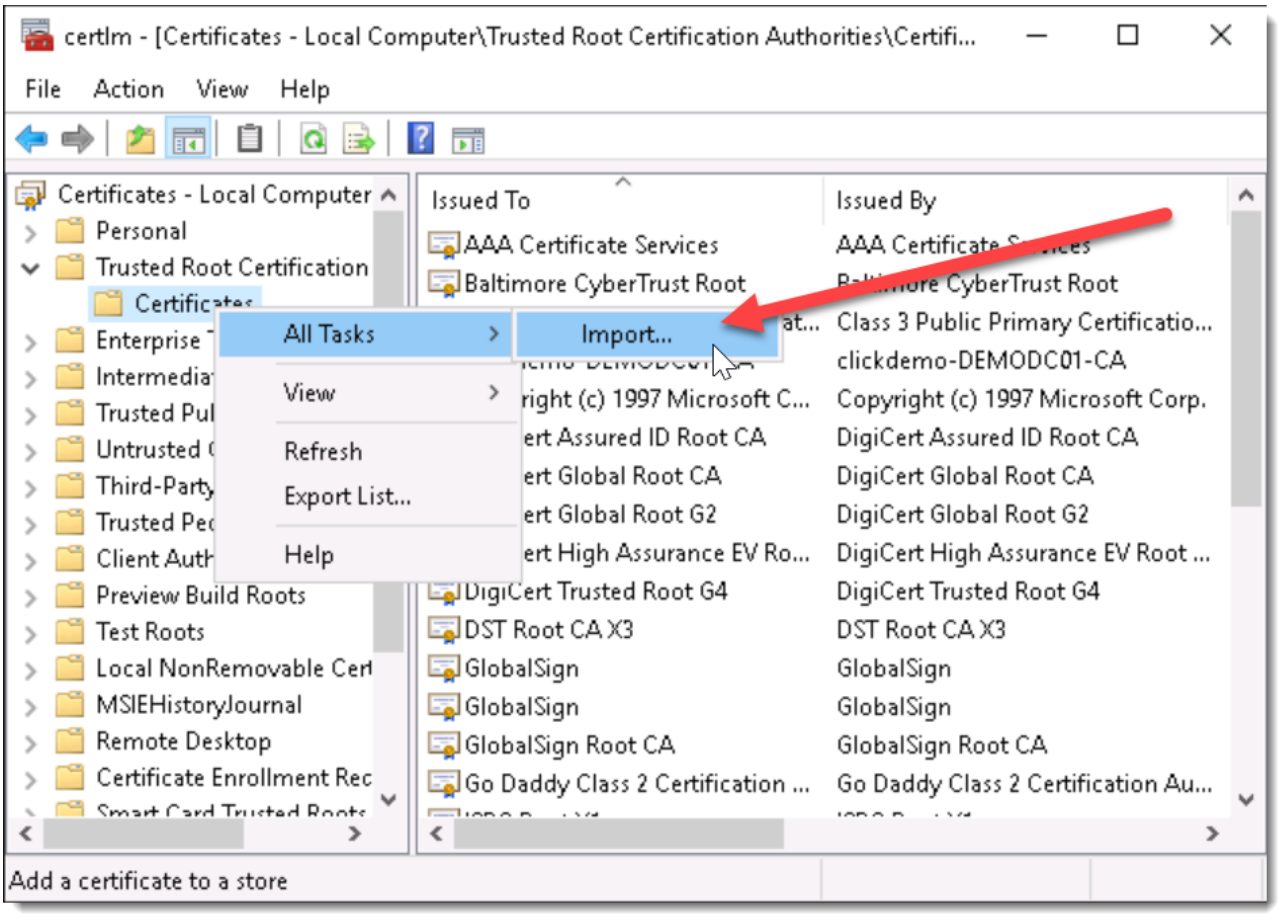
Under the **Details** tab, click **Copy to File…**



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 **certlm.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**:



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: https://www.clickstudios.com.au/community/index.php?/topic/2978-passwordstate-certificates-explained/

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://www.clickstudios.com.au/community/index.php?/topic/2934-how-to-set-up-a-internal-certificate-authority/

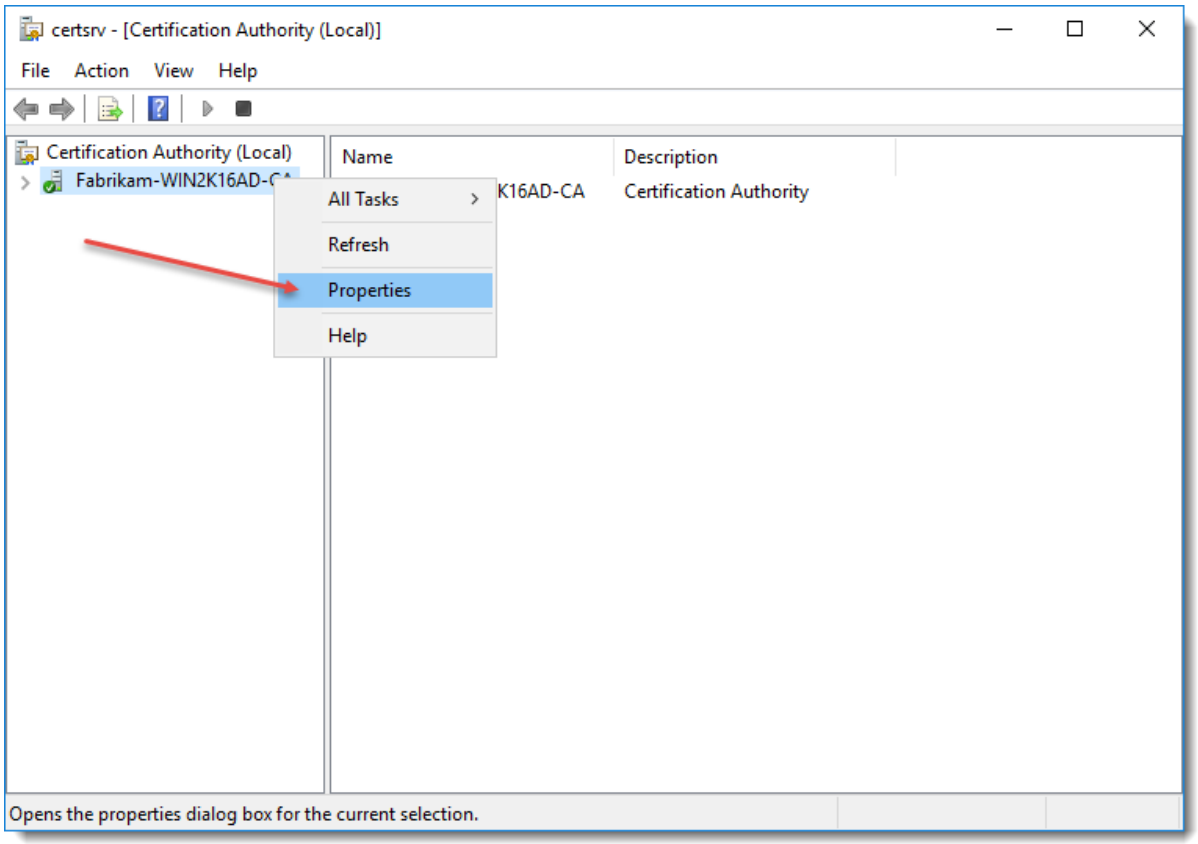
8 Additional Certificate Considerations

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*)

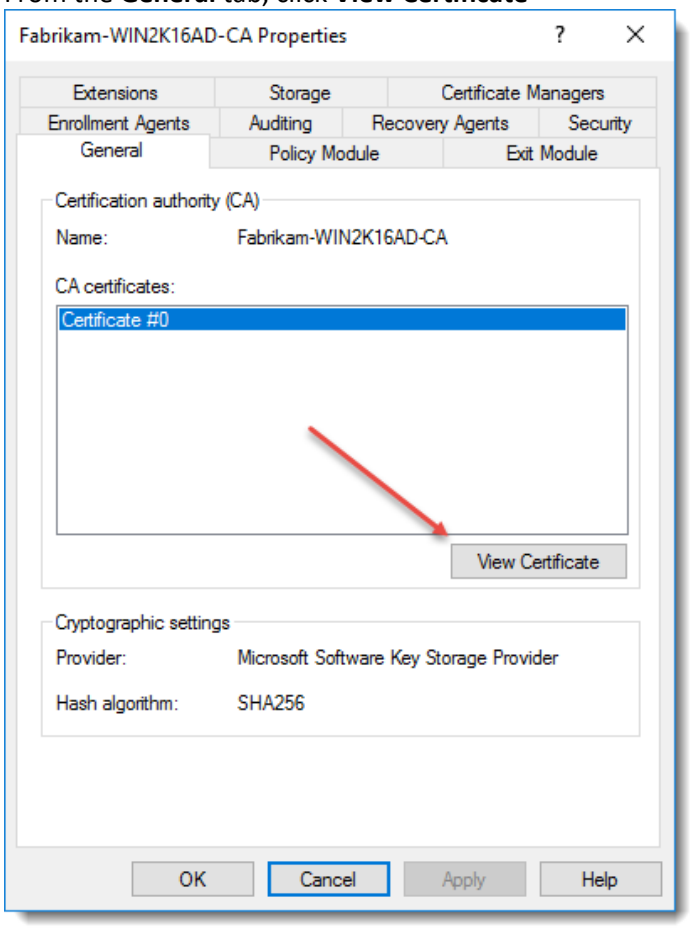
This is required so the API can securely communicate with these other domains. If this is a requirement for you, you can follow these steps:

Export the Domain CA Certificate

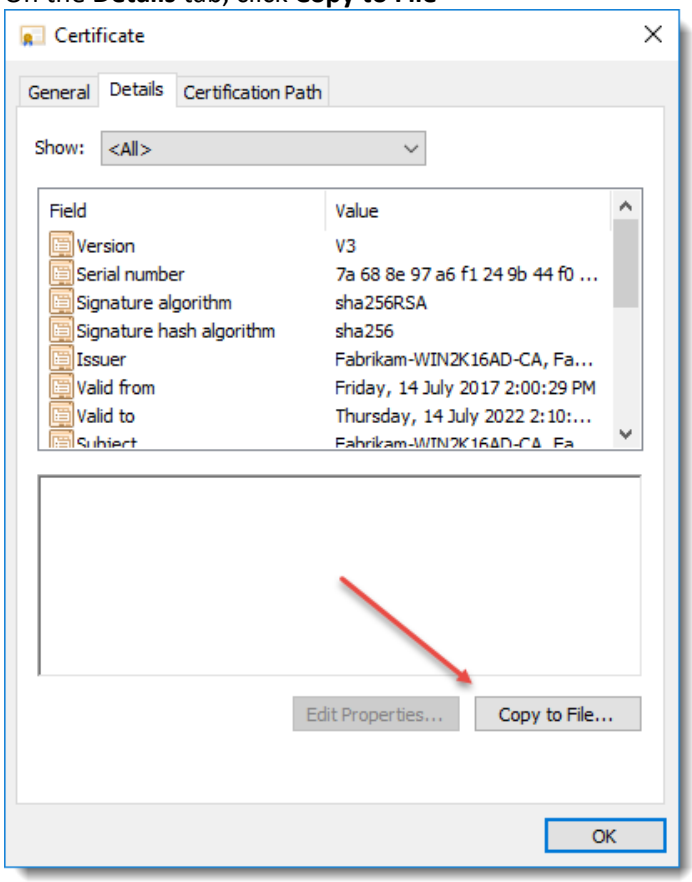
1. On your server that has the CA installed, Click **Start** > **Control Panel** -> **System and Security** -> **Administrative Tools** -> **Certificate Authority** to open the **CA Microsoft Management Console (MMC) GUI**
2. Right-click the **CA server** and select **Properties**



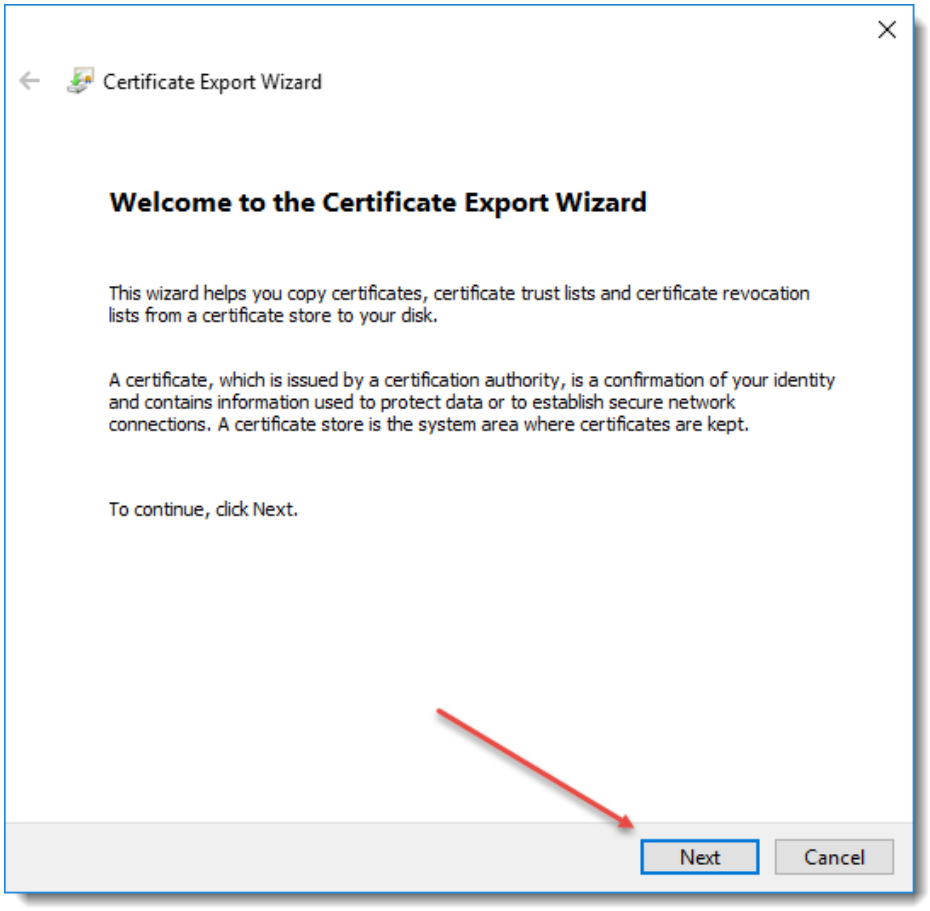
3. From the **General** tab, click **View Certificate**



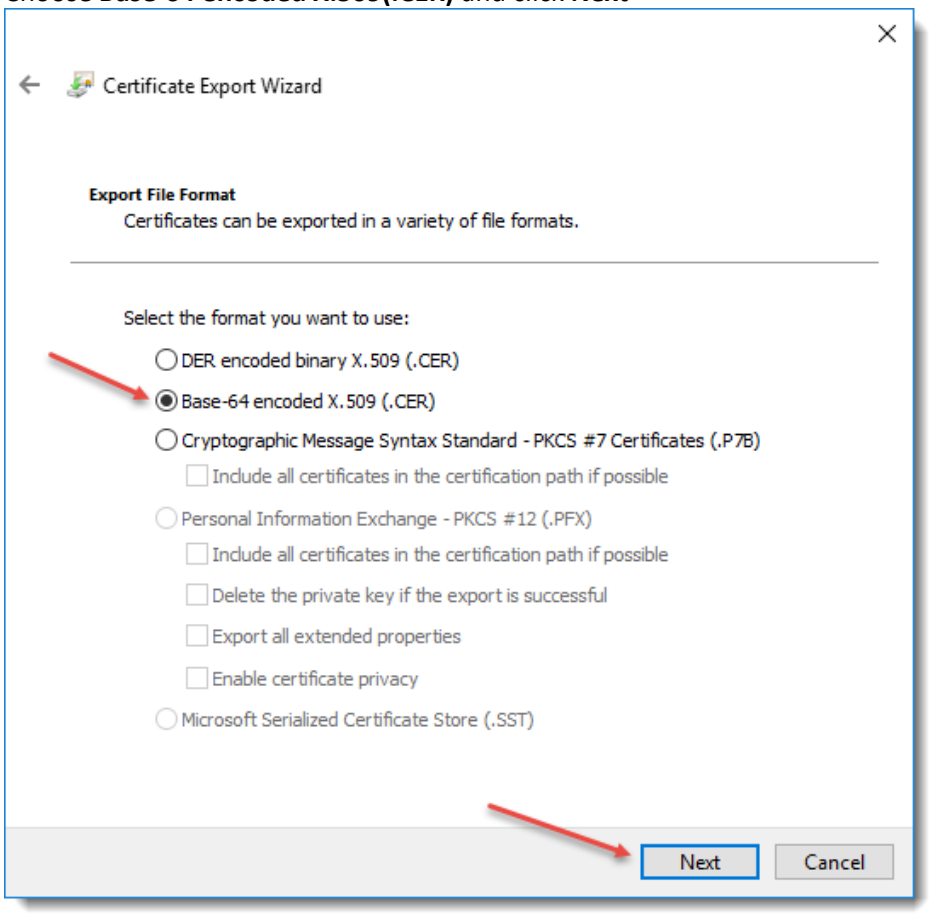
4. On the **Details** tab, click **Copy to File**



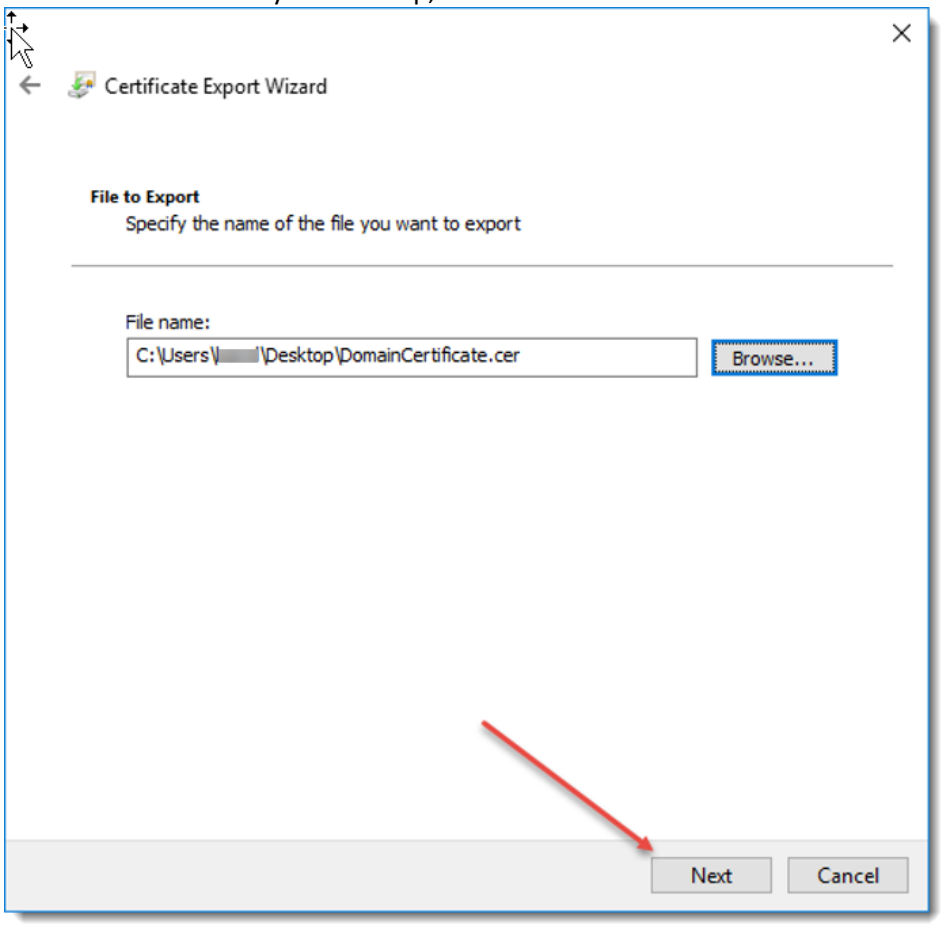
5. Click **Next**



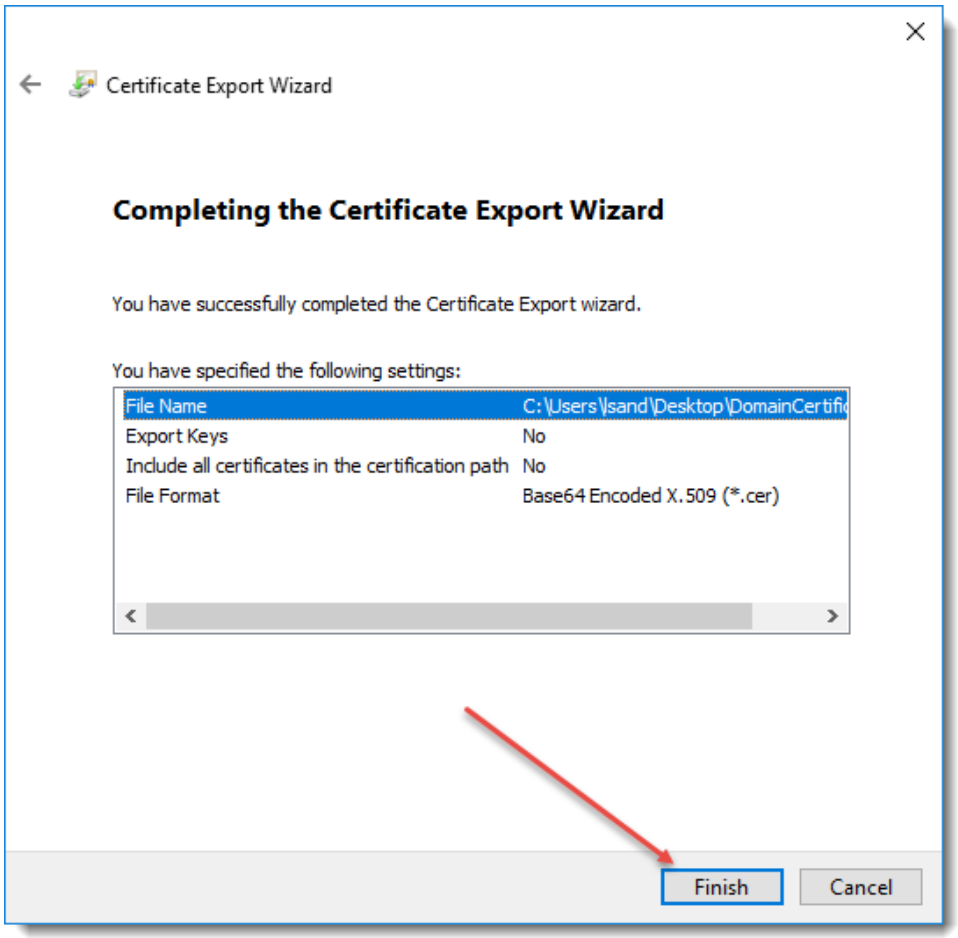
6. Choose **Base-64 encoded X.509(.CER)** and click **Next**



7. Save the certificate to your desktop, or somewhere local and click **Next**



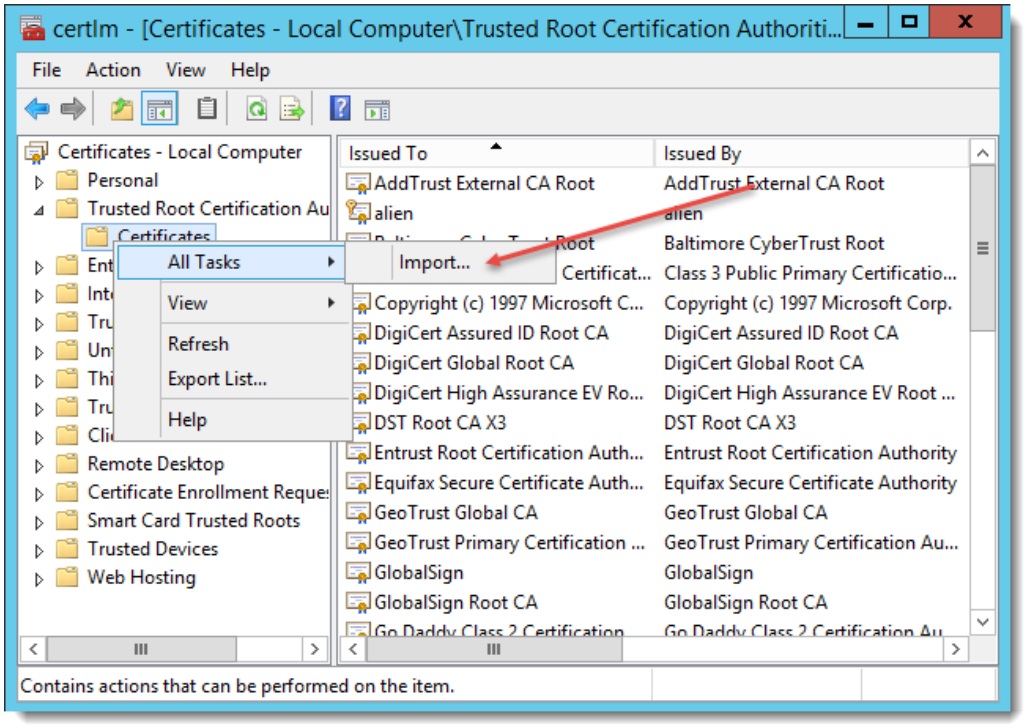
8. Click **Finish**



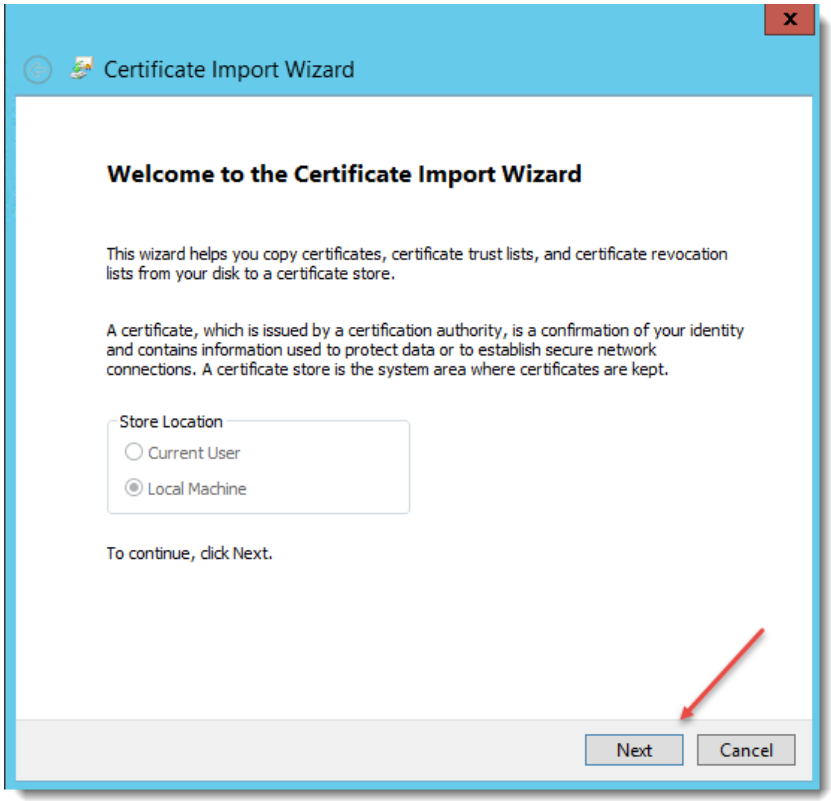
9. Transfer the certificate to your Passwordstate web server and close all windows.

Importing the Certificate into your Passwordstate web server

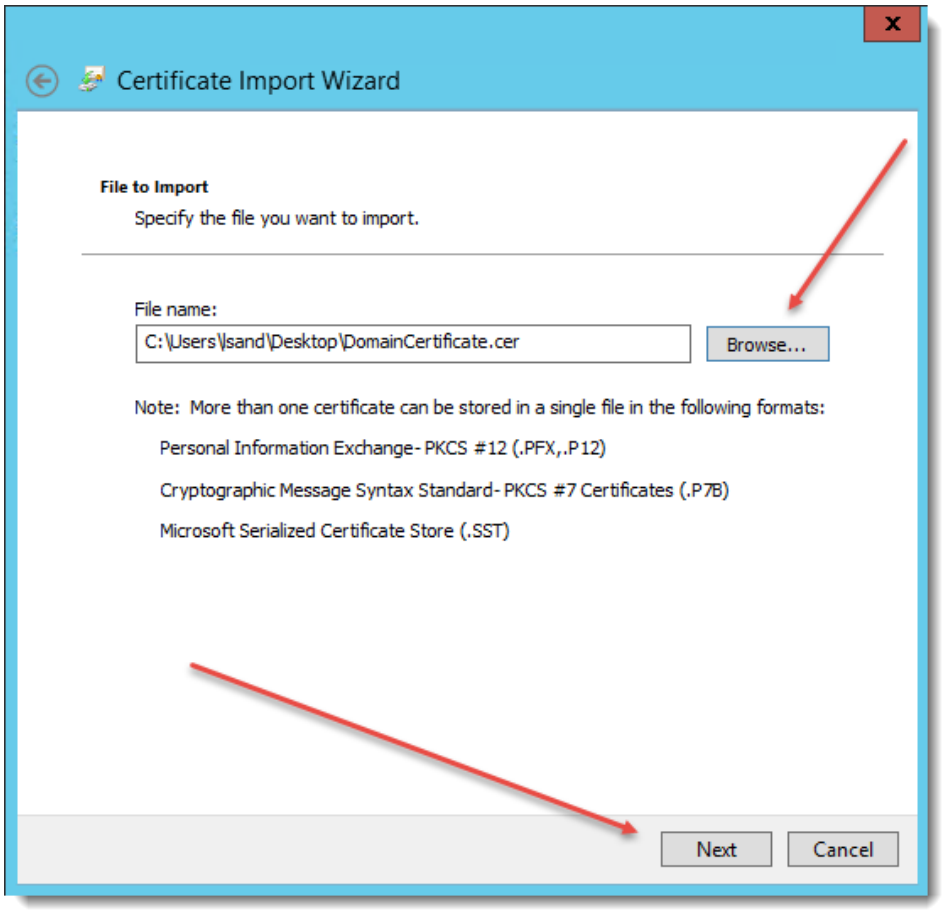
1. On your Passwordstate web server, open **Certificate Manager** by typing **certlm.msc** into your Run command bar
2. Expand **Trusted Root Certificate Authorities** -> **Certificates**
3. Right Click **Certificates** and select **All Tasks** -> **Import**



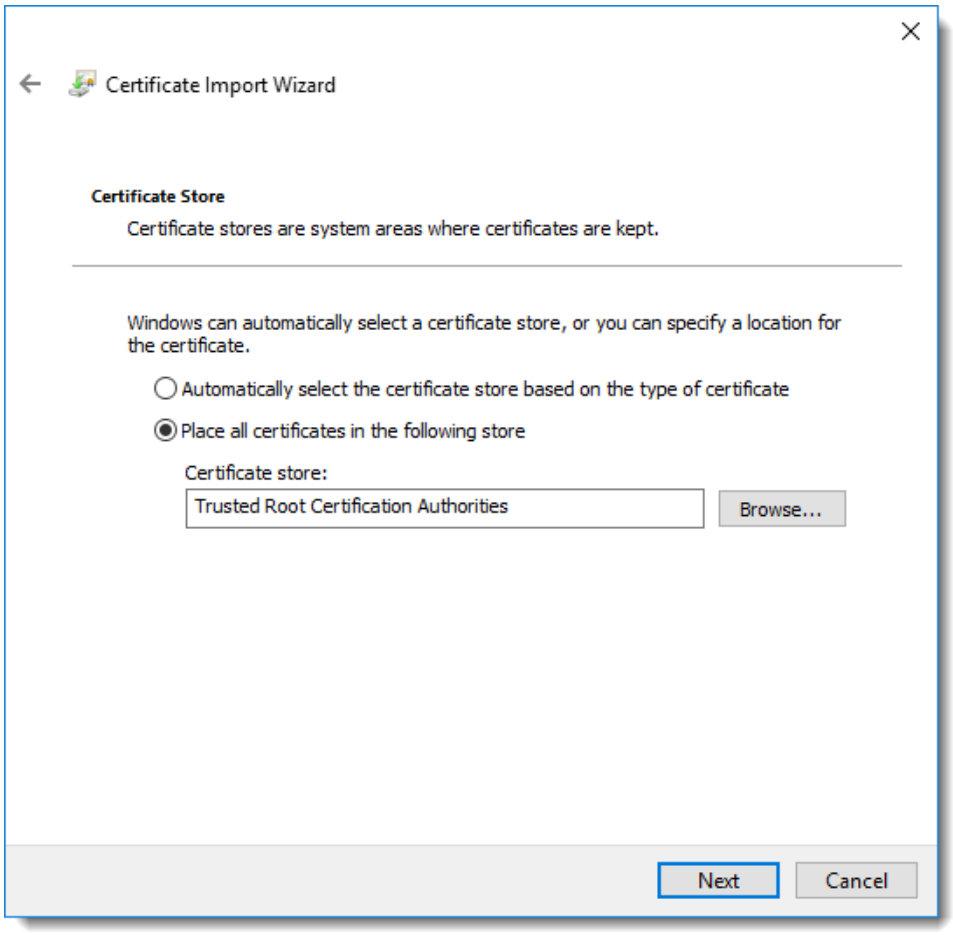
4. Click **Next**



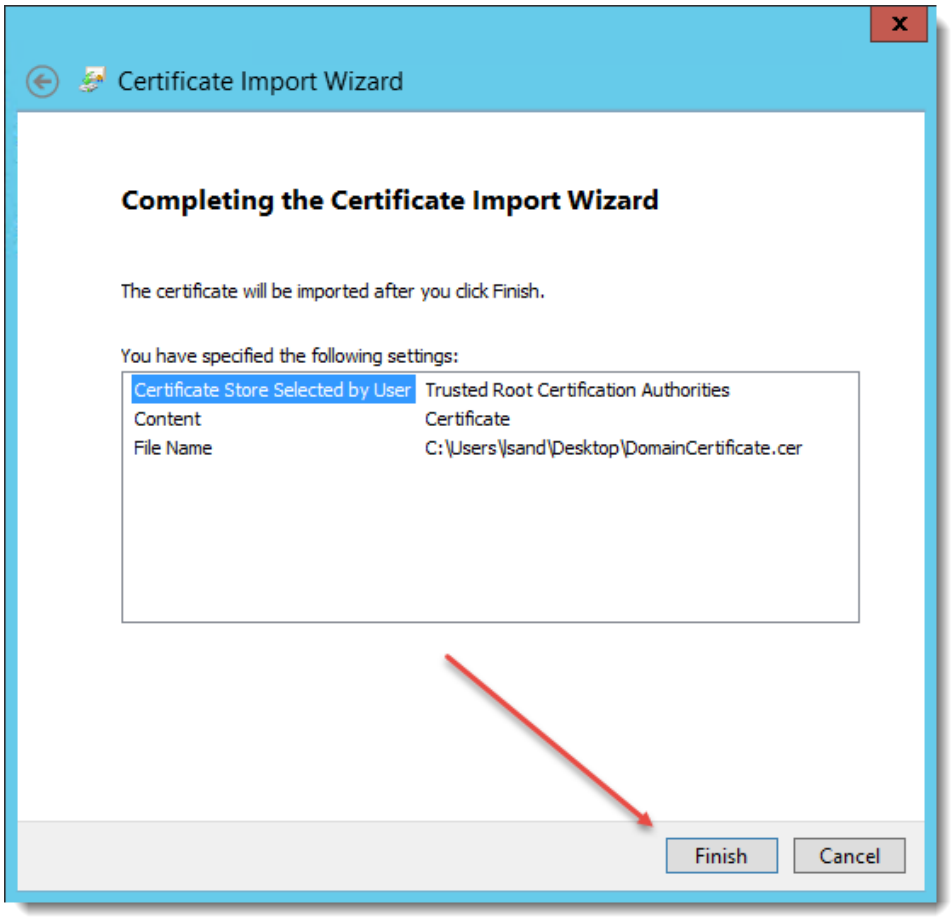
5. Browse to the certificate and click **Next**



6. Click **Next**



7. Click **Finish** and then **OK**



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 - https://www.clickstudios.com.au/passwordstate-checksums.aspx

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