Click Studios

Password Reset Portal

Installation Instructions

Table of Contents

1 System Requirements - General

Passwordstate's Password Reset Portal has the following system requirements:

Password Reset Portal Server

The server which will host the Password Reset Portal web site can be any of the following Operating System versions, with required components:

- Microsoft Windows Server 2012 & IIS 8.0
- Microsoft Windows Server 2012 R2 & IIS 8.5
- Microsoft Windows Server 2016 & IIS 10.0
- Microsoft Windows Server 2019 & IIS 10.0
- Windows 8 & IIS 8.0
- Windows 10 & IIS 10.0
- Microsoft **.NET Framework 4.5 or above, and PowerShell 4.0 or above** must also be installed on your Reset Portal server.
- 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**, and support LDAP over SSL on port 636

2 Architectural Overview

The Password Reset Portal is an additional module available for Passwordstate, which is installed as its own stand-alone web site. The web site can be installed in your DMZ if required, and made accessible to users from their Mobile Phones when outside of your internal network.

The Password Reset Portal 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 the API in your main Passwordstate site install.

From your Password Reset Portal 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.

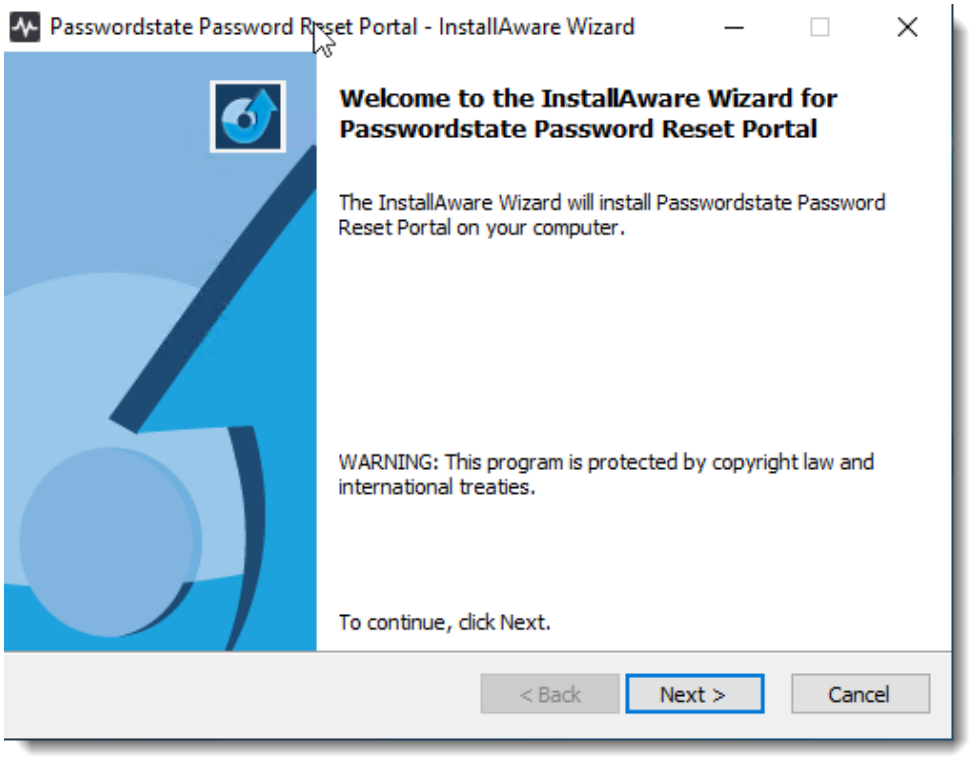
You must also have a Domain Certificate Authority installed, so that Passwordstate can communicate via LDAP over SSL – instructions are provided in this document as well on how to install a CA.

3 Installing Password Reset Portal

The Password Reset Portal installer is included with the Passwordstate download, and can also be accessed from the screen Administration -> Password Reset Portal Administration within Passwordstate.

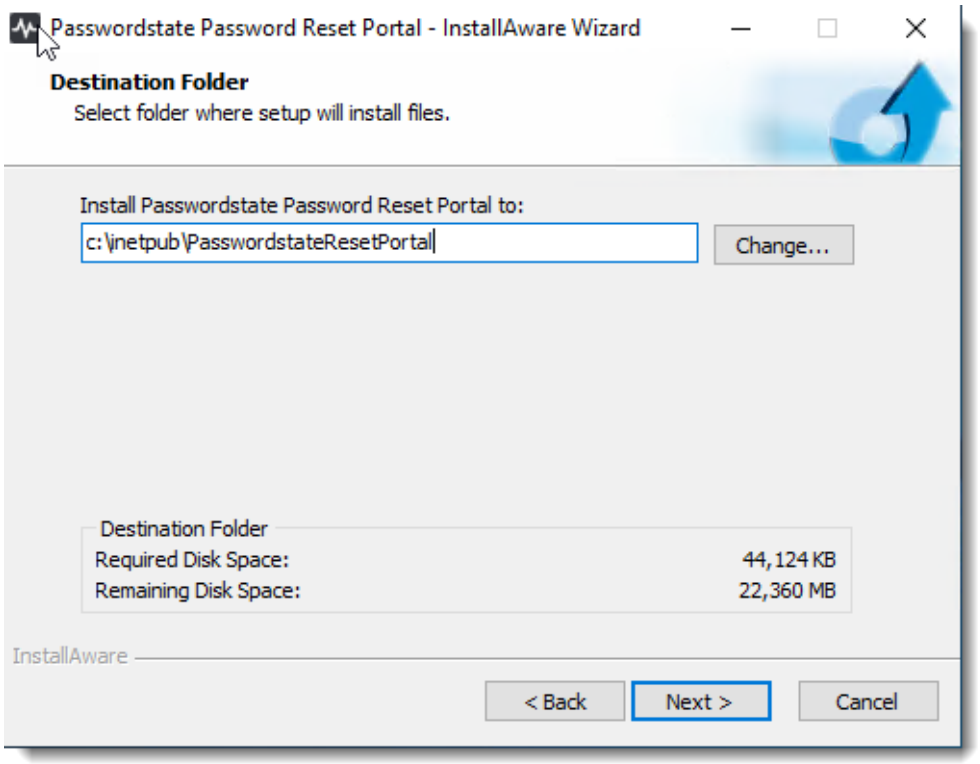
1. As an Administrator on your server, run '**PasswordResetPortal.exe**'

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



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

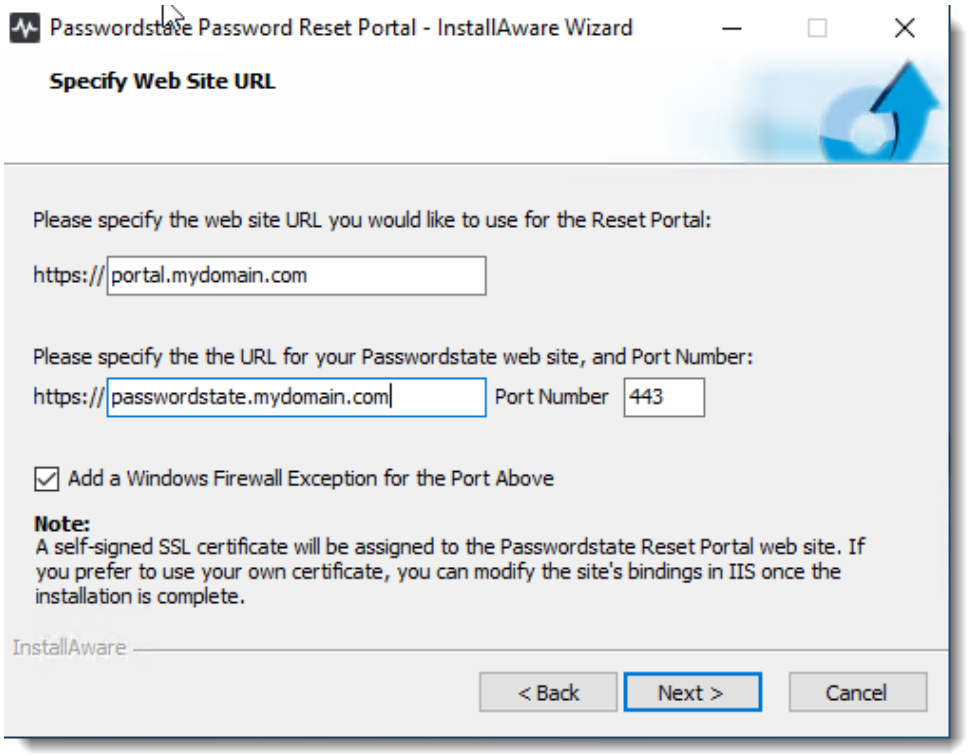
4. Accept the default installation path, and click '**Next**'



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 name as the

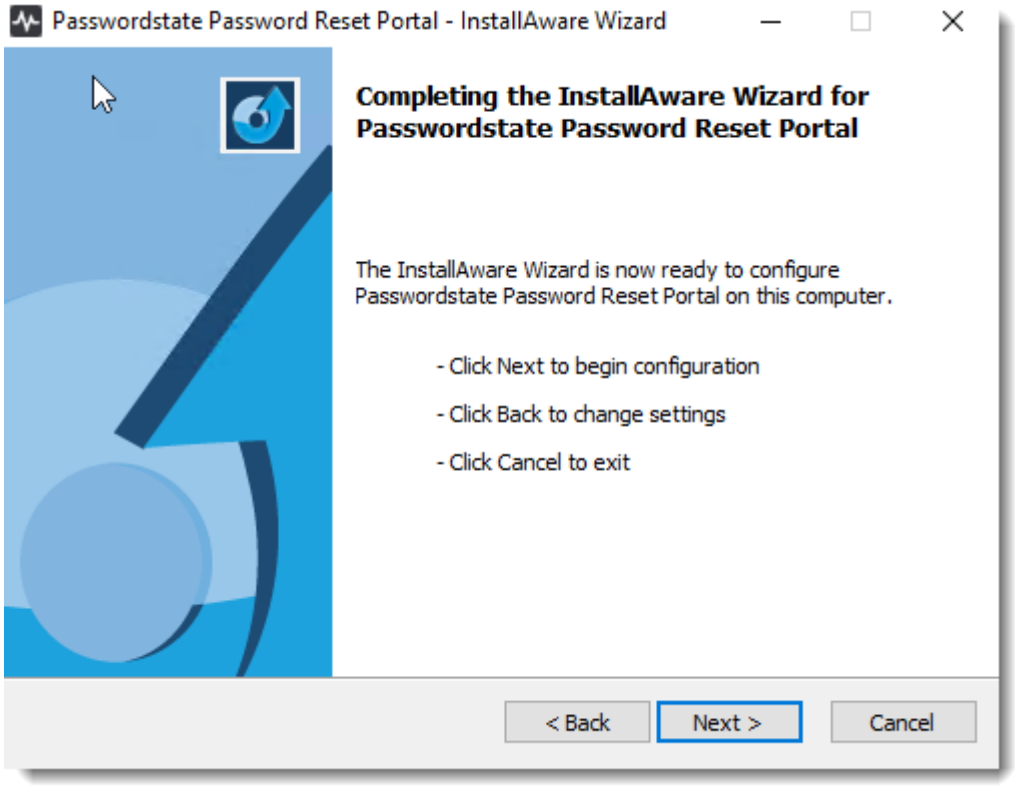
URL, but it is possible to change this to any value you like. If any changes are made to this URL, a matching DNS record will need to be created, and a matching SSL certificate must be assigned.

It is also possible to change the port number, but choosing ports other than '443', will require your users to append the port number to the end of your URL.



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

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

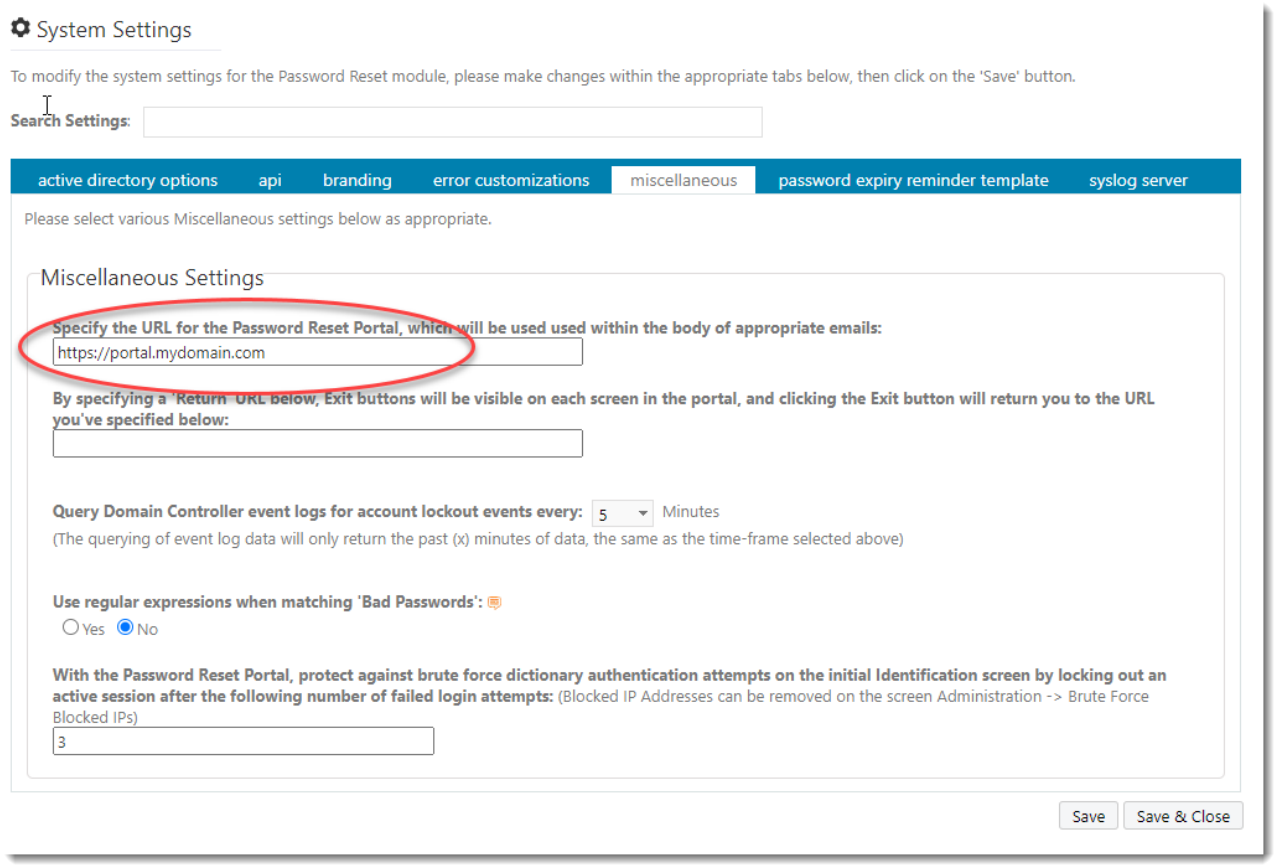


4 Reset Portal URLs

Once you have finished installing the Password Reset Portal, your users can access it via the URL you specified in the previous installer screens.

Prior to resetting or unlocking their account, they must first enroll to use this feature. From within the Administration area of Passwordstate, you must specify the URL of your Reset Portal web site, as per the screenshot below. Then when you start sending enrollments emails from within Passwordstate, the correct URL will be specified for them.

You can access your enrollment URL by appending /enroll to the end of your portal URL.



5 SSL Certificate Considerations

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

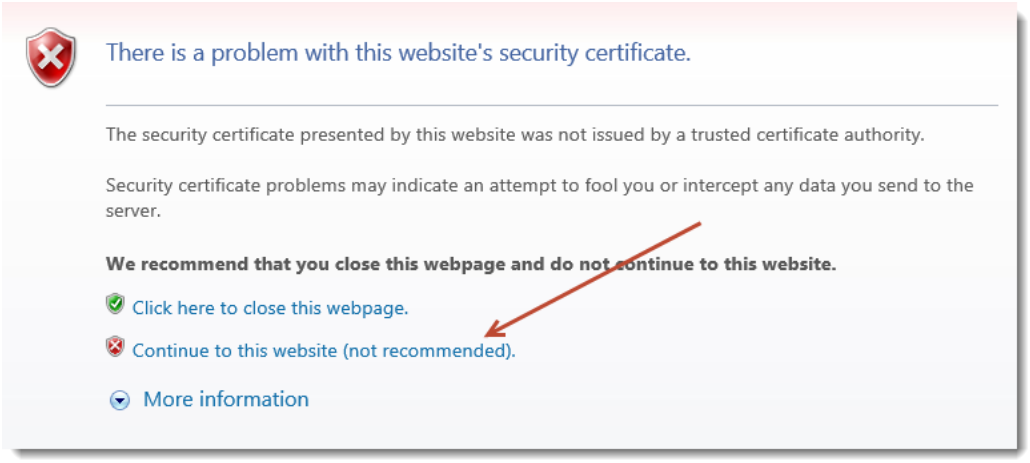
Note It is highly recommended to use a purchased an SSL certificate from an online trusted certificate authority, which will ensure a more secure and user-friendly experience for your users, on all types of devices.

If you have your own SSL certificate installed on the web server you'd prefer to use, you can modify the bindings for the site in IIS, and select the appropriate certificate.

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 display errors about the certificate not being issued by a trusted authority. This is difficult to do on mobile phones though, which is why we recommend using trusted SSL certificates.

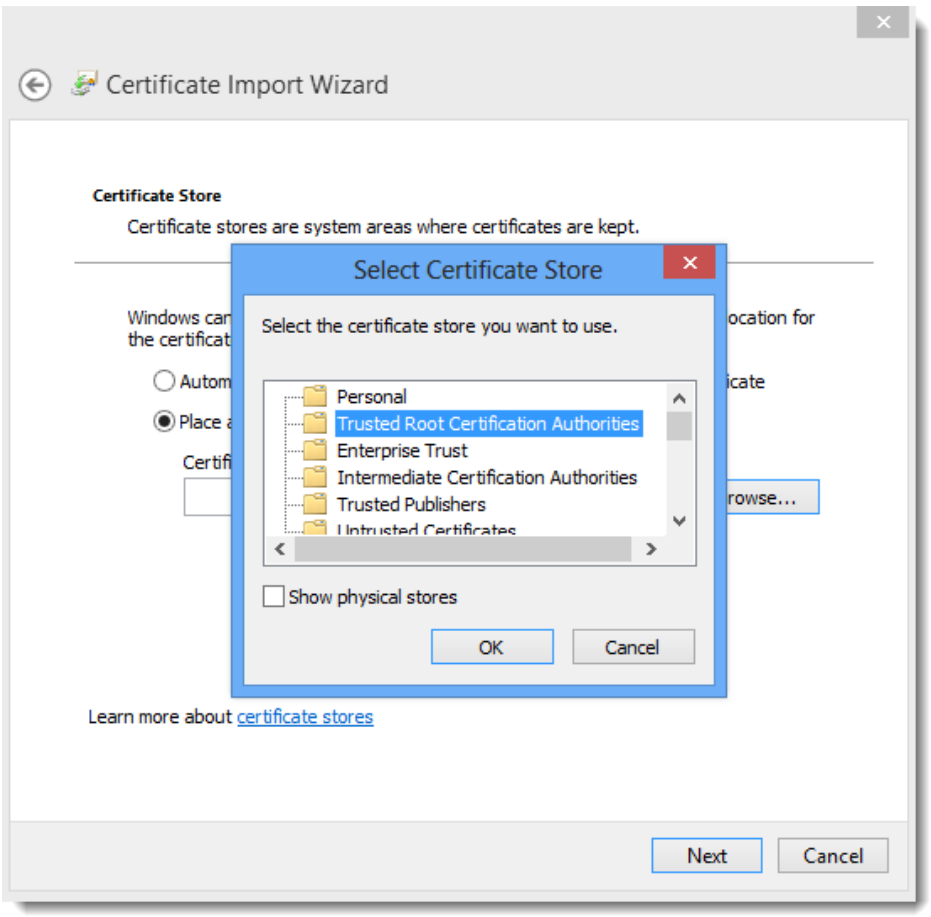
To install the certificate, you can follow these steps:

1. Using Internet Explorer, browser to the **Password Reset Portal** web site
2. When you see the following screen, click on the '**Continue to this website**' link



3. Now click on the '**Certificate error**' link at the top of your screen

4. The click on '**View Certificates**', then on the '**Install Certificate…**' button
5. Select the '**Local Machine**' Store Location, then click on the '**Next**' button
6. Select '**Place all certificates in the following store**' option, click on the '**Browse**' button, and select '**Trusted Root Certification Authorities**' as per the next screenshot



7. Now click on the '**OK**' button, then the '**Next**' and '**Finish**' buttons

After the certificate is installed, you can close and re-open your browser to the Password Reset Portal web site, and it should no longer see any errors about an untrusted certificate.

6 Active Directory Certificate Authority

To use the Password Reset Portal module, 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 required so LDAP over SSL can be used, which will honor any Domain Password Policies, or Fine-Grained Password Policies.

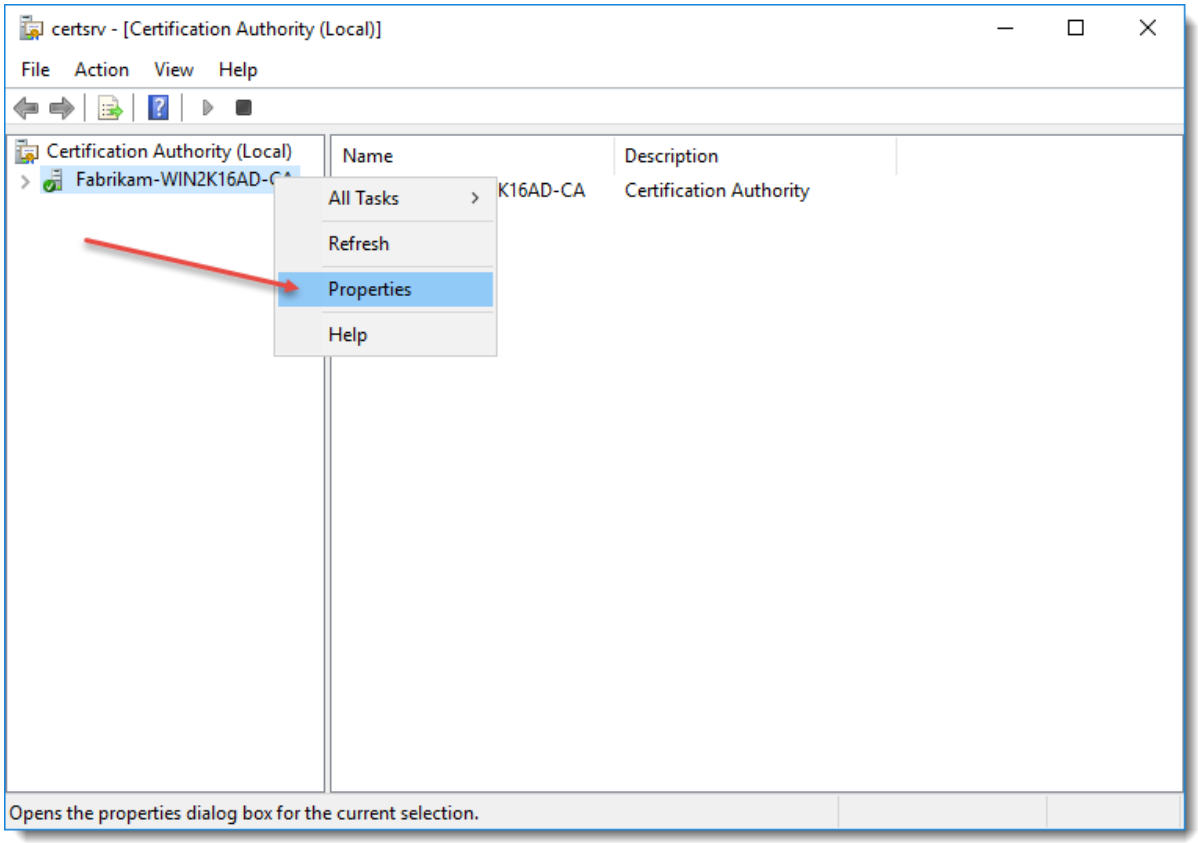
Please follow these step by step instructions to set up a Certificate Authority:
https://www.clickstudios.com.au/community/index.php?/topic/2934-how-to-set-up-a-internal-certificate-authority/

7 Certificate Considerations

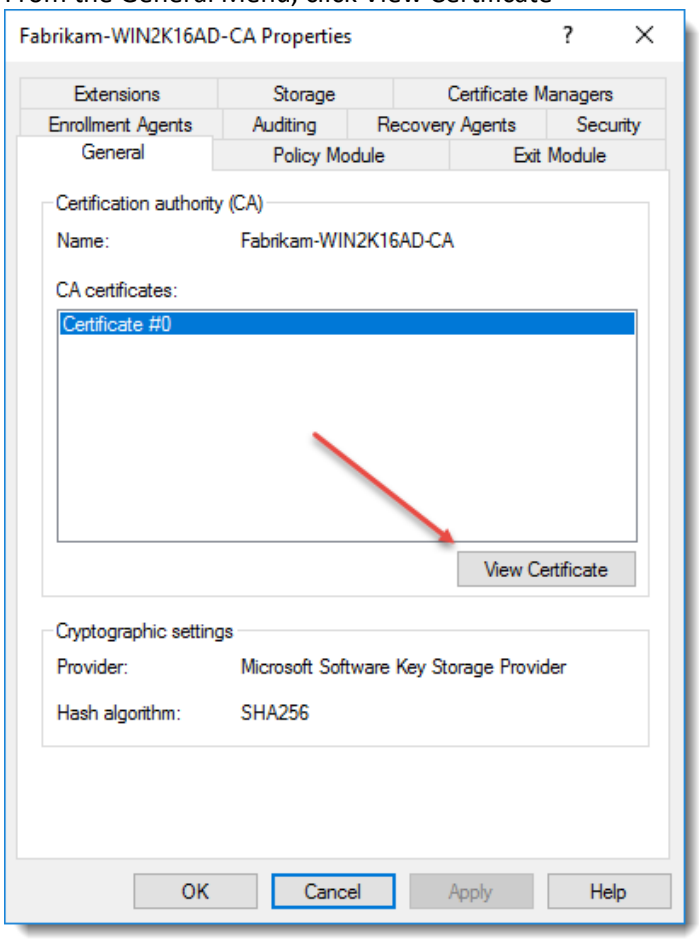
If you intend to use additional domains that your Passwordstate Web Server is not a member of, then you will need to export the CA certificate from these domains, and import them onto your Passwordstate web server. This is required so the API can securely communicate with these other domains. If this is a requirement for you, you can follow these steps:

Export the Domain CA Certificate

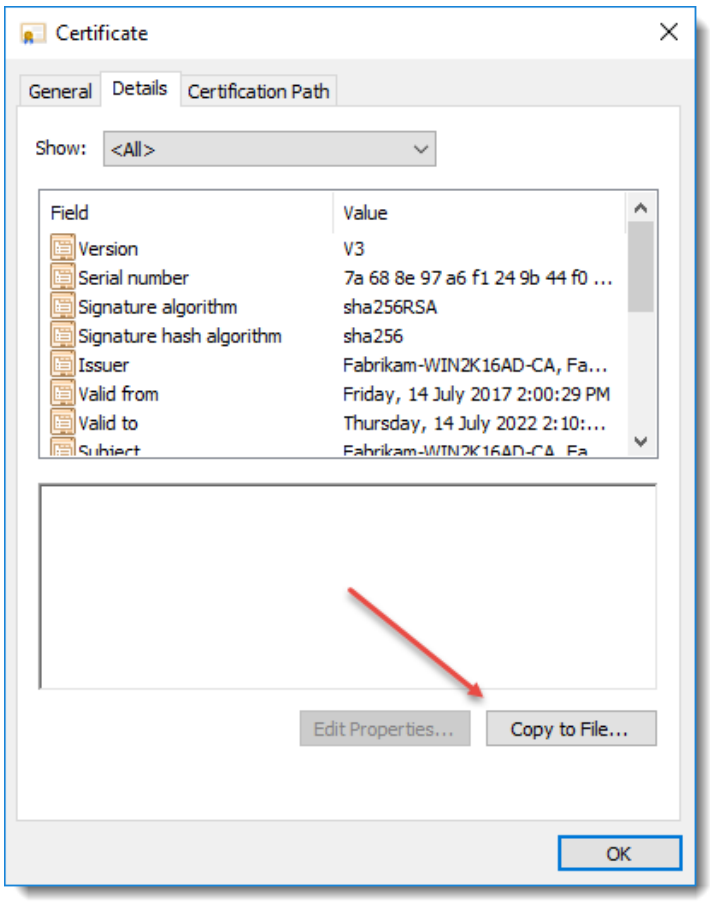
1. On your server that has the CA installed, Click Start > Control Panel -> System and Security -> Administrative Tools > Certificate Authority to open the CA Microsoft Management Console (MMC) GUI
2. Right-click the CA server and select Properties



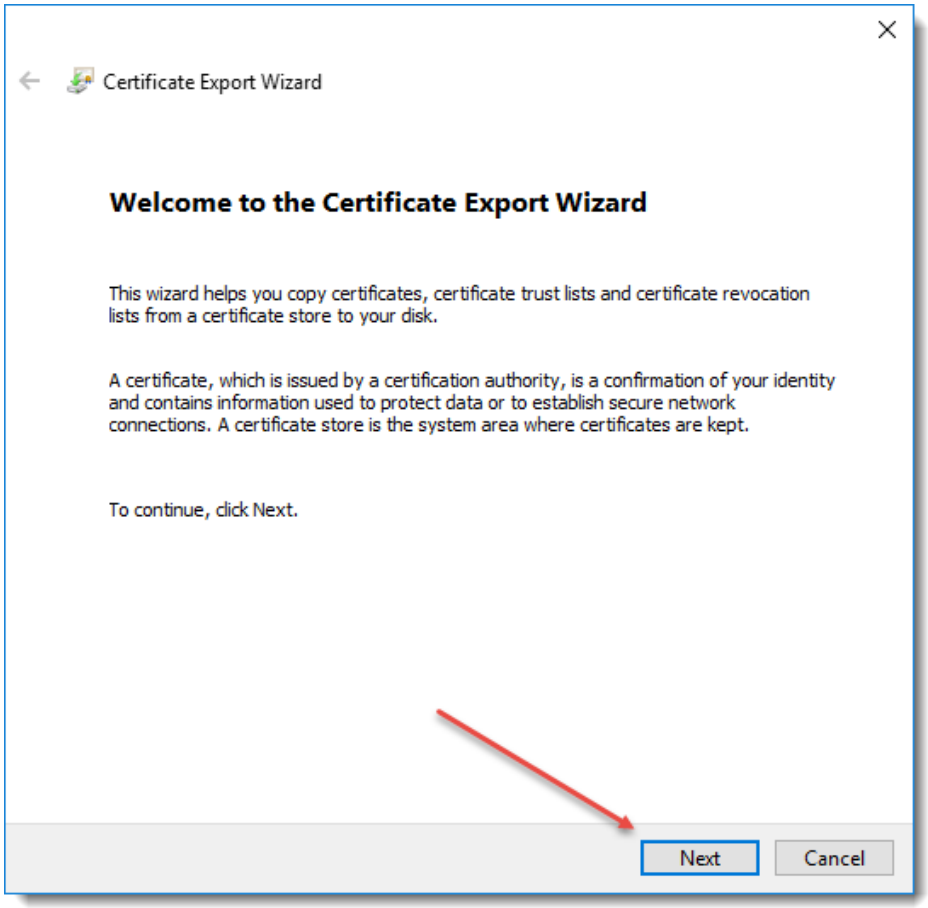
3. From the General Menu, click View Certificate



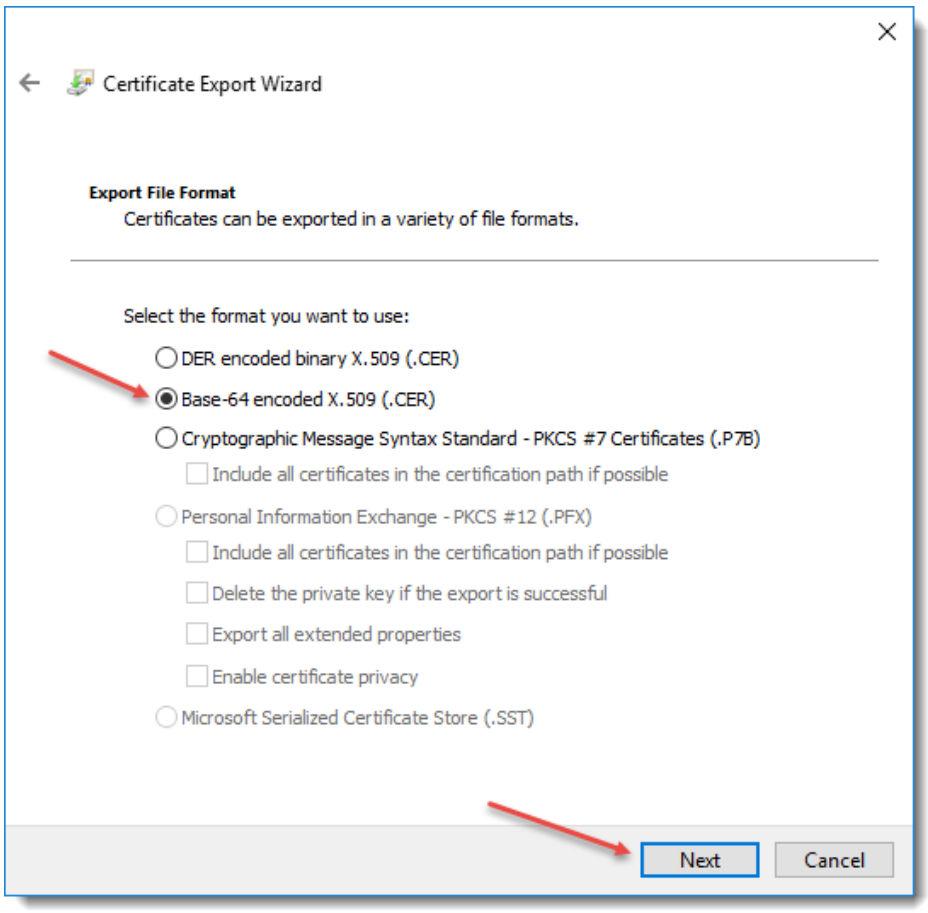
4. On the Details tab, click Copy to File



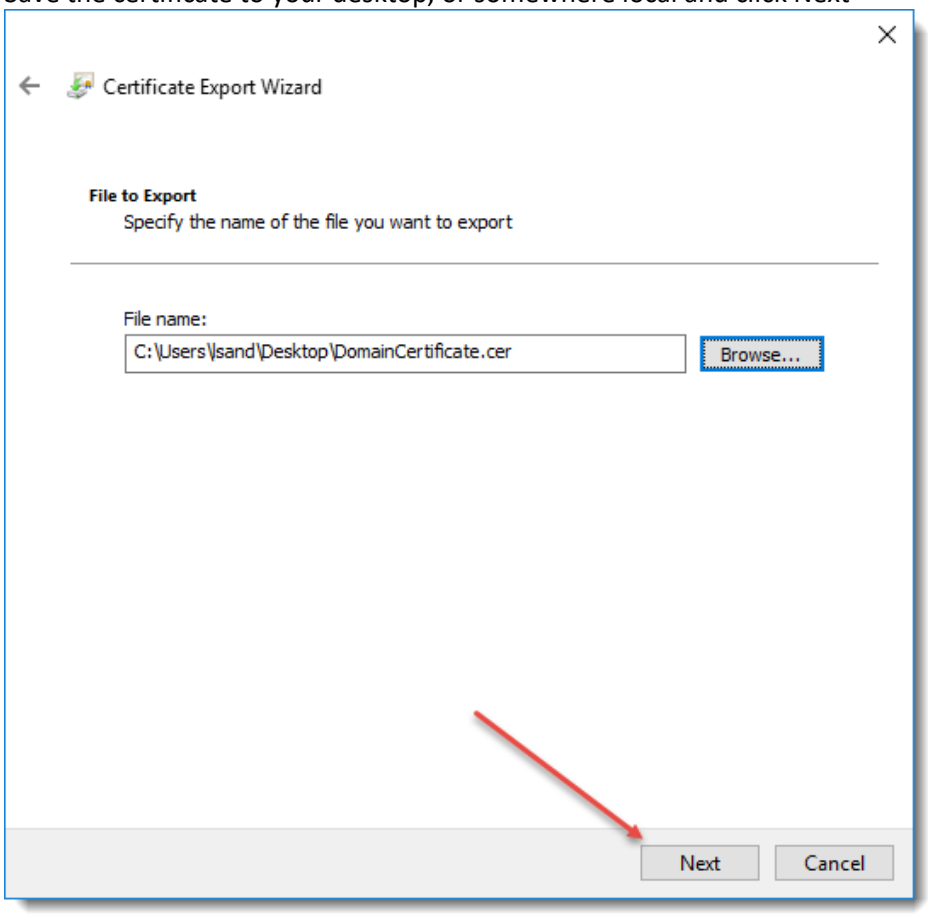
5. Click Next



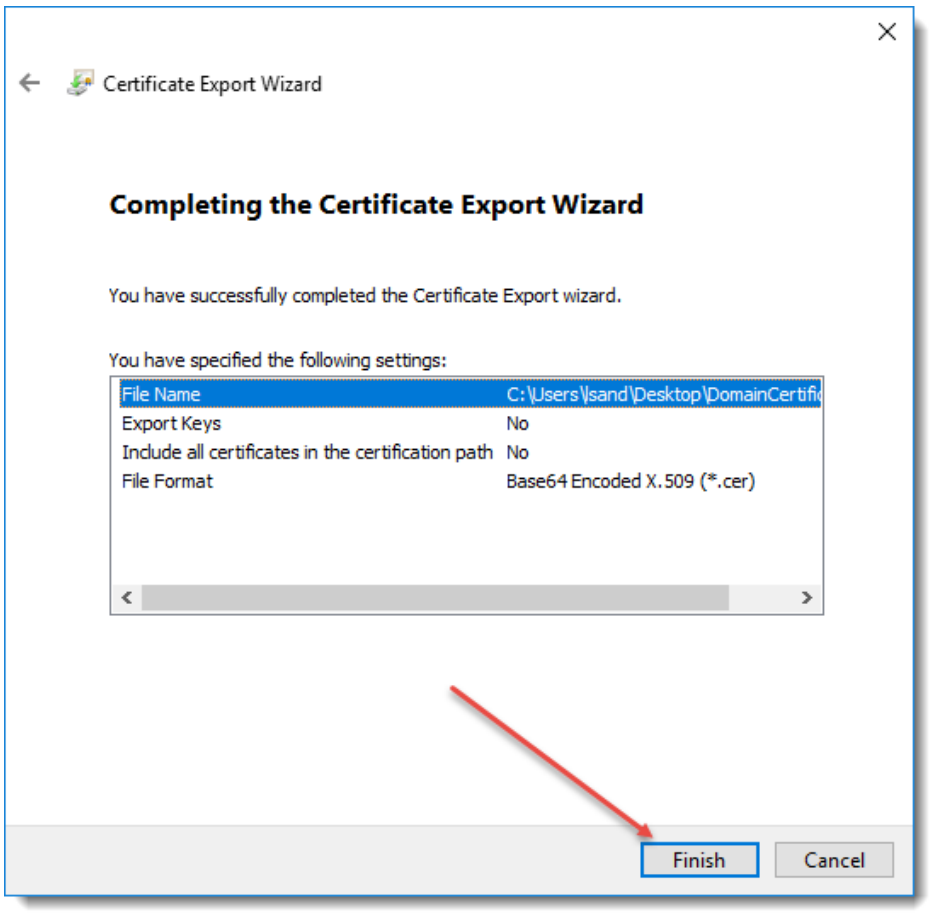
6. Choose Base-64 encoded X.509(.CER) and click Next



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



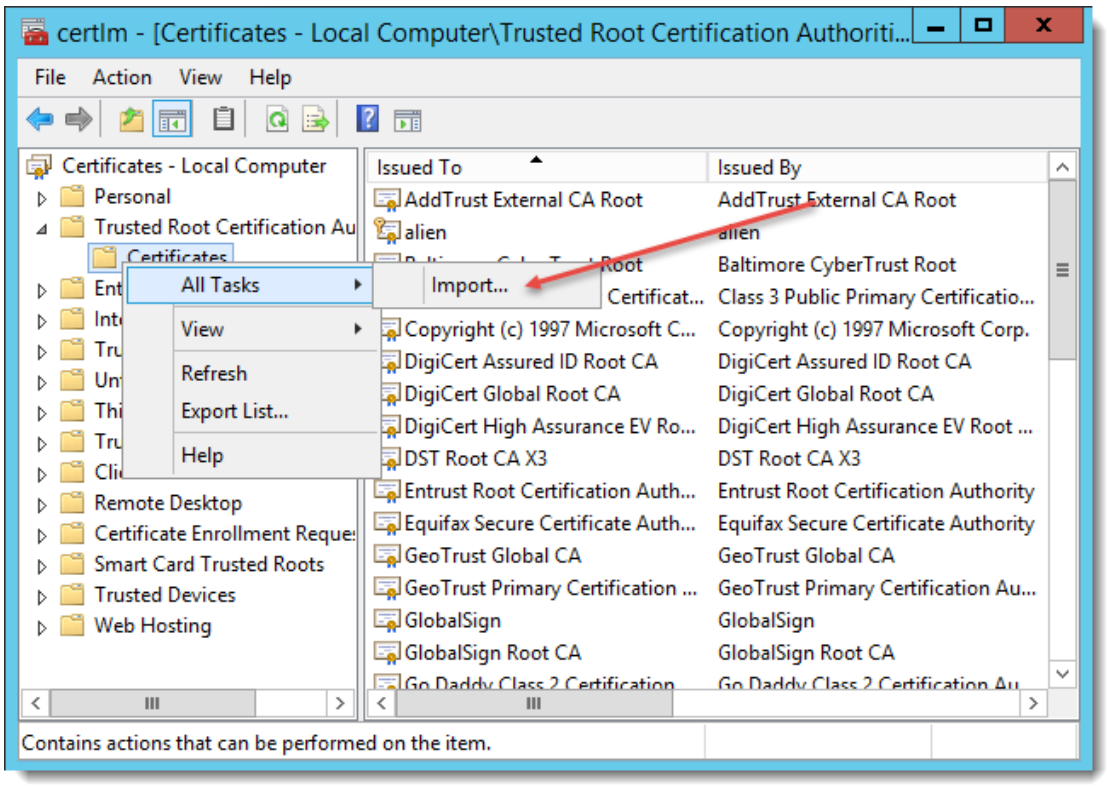
8. Click Finish



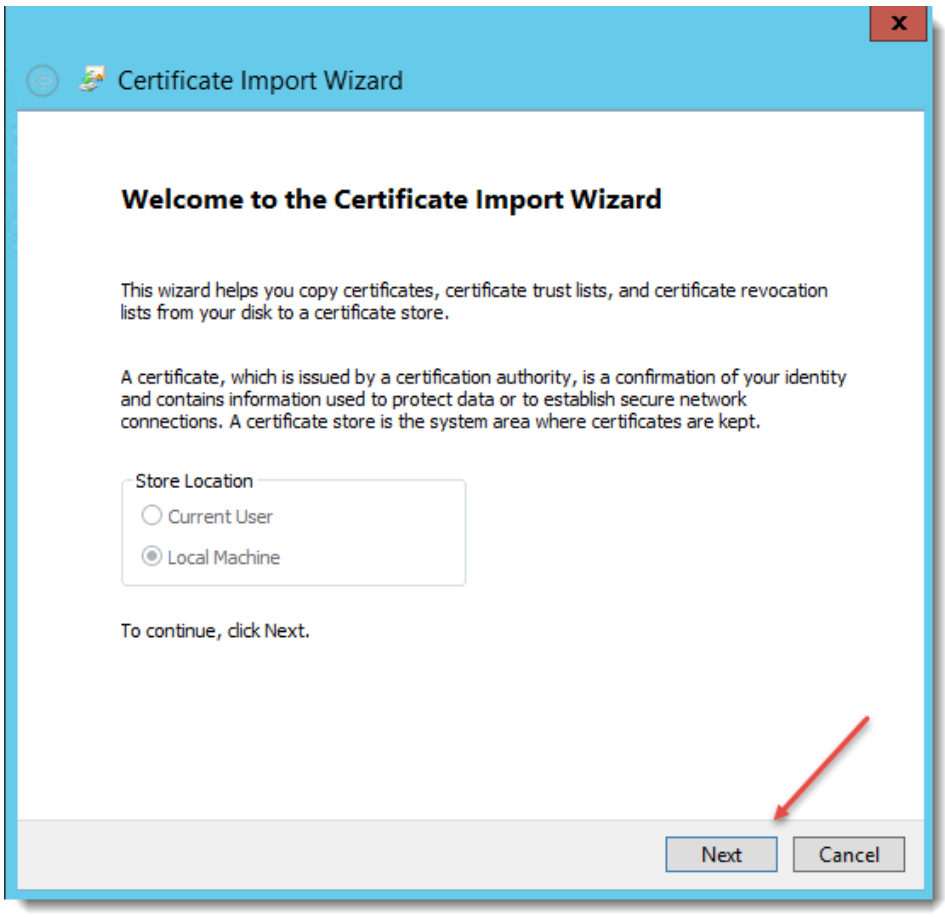
9. Transfer the certificate to your Passwordstate web server and close all windows.

Importing the Certificate into your Passwordstate web server

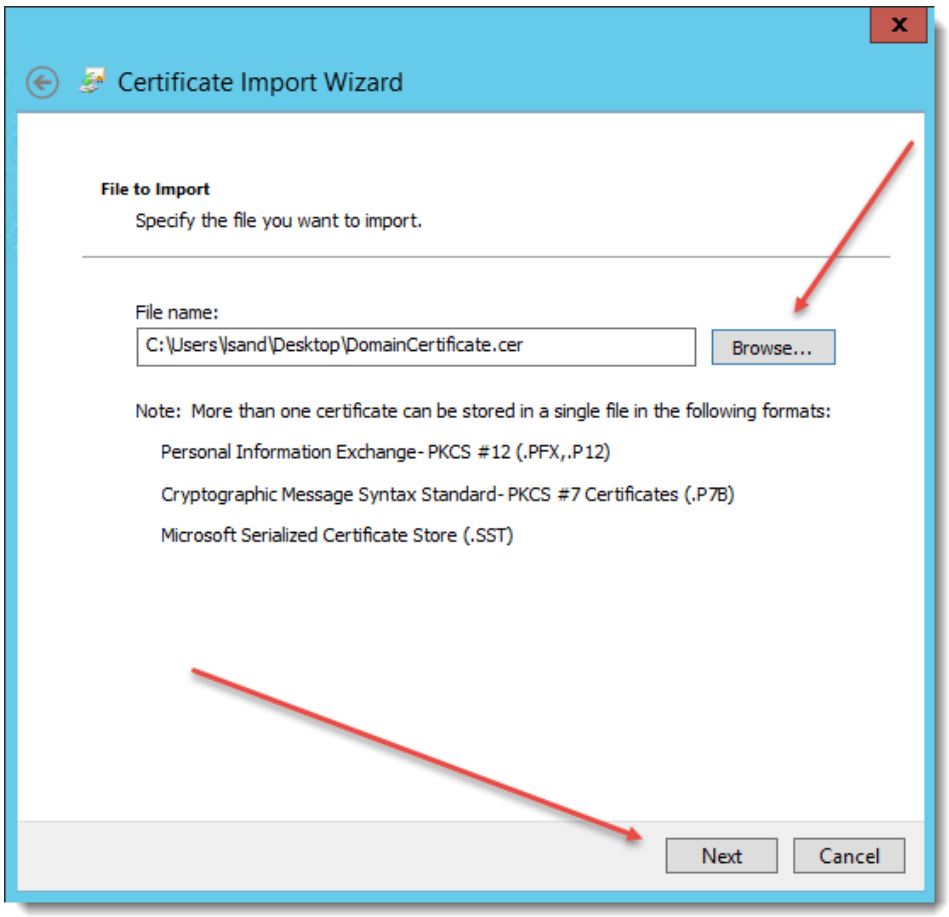
1. On your Passwordstate web server, open Certificate Manager for Local computer by typing certlm.msc into your Run command bar
2. Expand Trusted Root Certificate Authorities -> Certificates
3. Right Click Certificates and select All Tasks -> Import



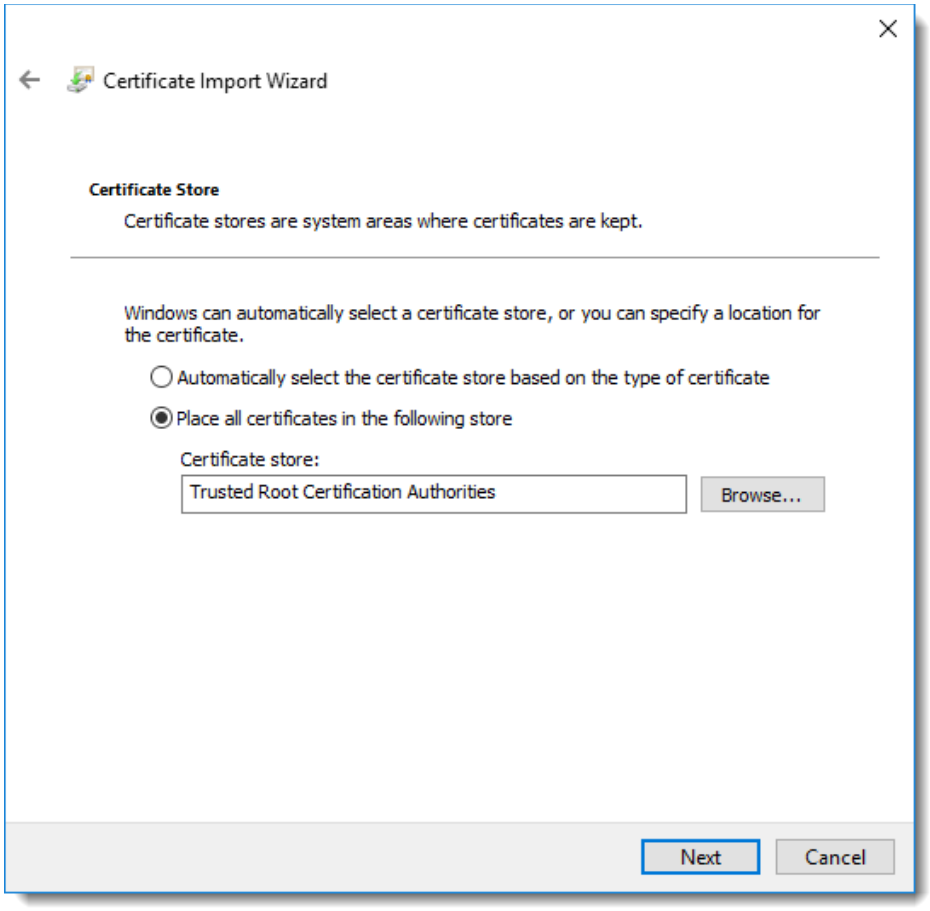
4. Click Next



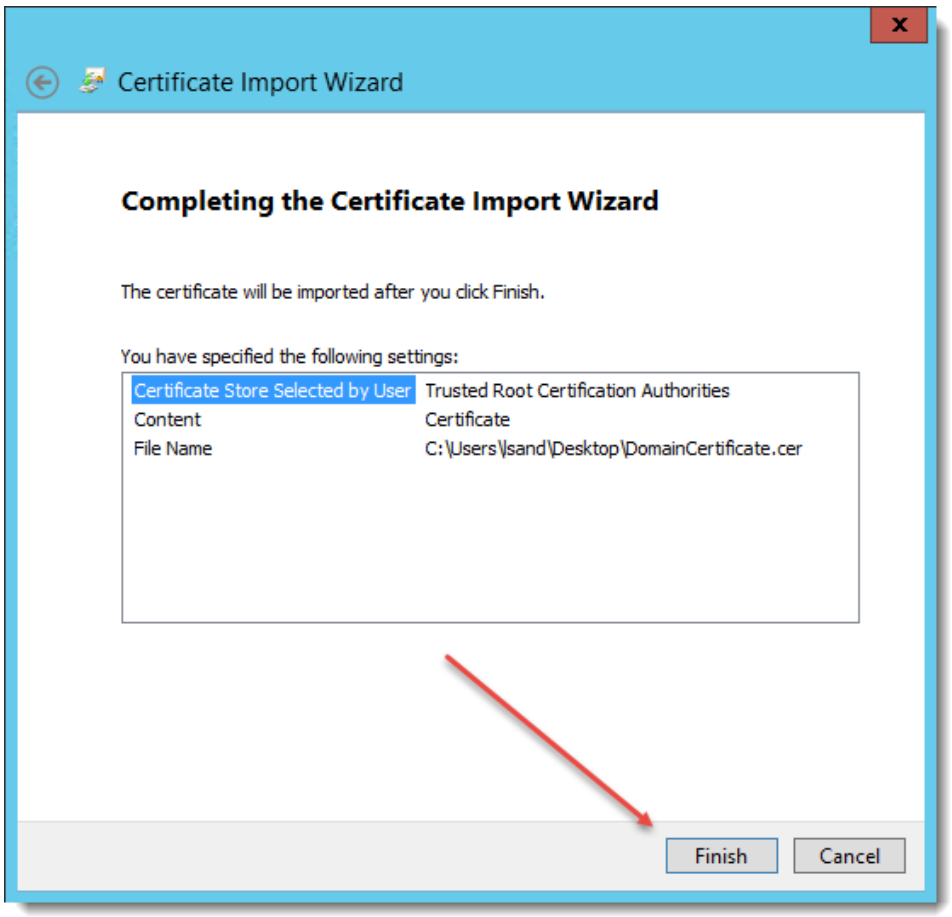
5. Browse to the certificate and click Next



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

8 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 API 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

- The Password Reset Portal only needs to communicate back to your Passwordstate API, so generally Port 443 is required to be open. If you are using a different port for your Passwordstate web site, then this port will instead need to be open

Passwordstate Web Site and API

- Port 636 - this is required for LDAP over SSL, so the Passwordstate UI and API can communicate with Active Directory to reset and unlock accounts
- Ports 135 and 49153 - this is required for the Passwordstate UI and Windows Service to query Event Logs on Domain Controllers for bad login attempts and account lockouts

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 from your Passwordstate web server to confirm if the ports are open or not (replace win2k16ad.fabrikam.com as appropriate for your Domain Controller):

```
test-netconnection -Computername win2k16ad.fabrikam.com -Port 636

test-netconnection -Computername win2k16ad.fabrikam.com -Port 135

test-netconnection -Computername win2k16ad.fabrikam.com -Port 49153
```

9 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. Please see instructions below for installing the credential provider, as well as recommendations for further securing your environment for its usage.

Installation Instructions

The Windows Credential Provider must be installed in silent mode, as 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.

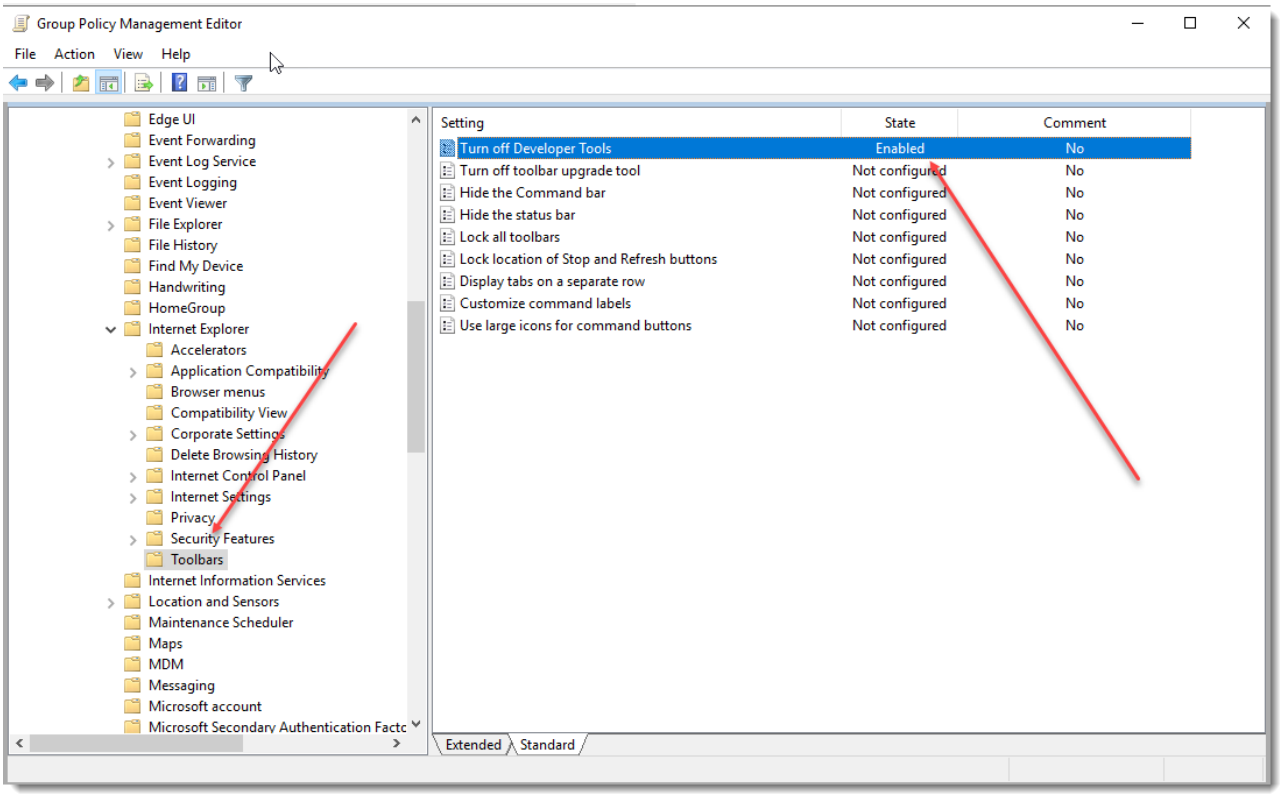
Security Recommendations

When the users clicks on the link "Reset Password/Unlock Account" from the Windows login screen, Internet Explorer will launch in Kiosk mode and navigate to your Password Reset Portal URL.

As there is no user profile loaded a at the Windows Login screen, it is recommended you apply a group policy setting to all desktops to prevent the usage of the Developer Tools in Internet Explorer.

The policy setting to enable is 'Turn off Developer Tools' and can be found in the policy section of Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Toolbars.

Below is a screenshot of this setting, and following is also further recommendations from Microsoft to further secure your environment if your security team deems appropriate - https://docs.microsoft.com/en-us/dynamics365/unified-operations/retail/dev-itpro/secure-retail-cloud-pos


Group Policy Management Editor
File Action View Help
Edge UI
Event Forwarding
Event Log Service
Event Logging
Event Viewer
File Explorer
File History
Find My Device
Handwriting
HomeGroup
Internet Explorer
Accelerators
Application Compatibility
Browser menus
Compatibility View
Corporate Settings
Delete Browsing History
Internet Control Panel
Internet Settings
Privacy
Security Features
Toolbars
Internet Information Services
Location and Sensors
Maintenance Scheduler
Maps
MDM
Messaging
Microsoft account
Setting
State
Comment
Turn off Developer Tools
Enabled
No
Turn off toolbar upgrade tool
Not configured
No
Hide the Command bar
Not configured
No
Hide the status bar
Not configured
No
Lock all toolbars
Not configured
No
Lock location of Stop and Refresh buttons
Not configured
No
Display tabs on a separate row
Not configured
No
Customize command labels
Not configured
No
Use large icons for command buttons
Not configured
No
Extended
Standard