Xorble Web Service Proxy installation

Introduction to Web Services Proxy

The Xorble Web Service Proxy component implements the X.509 Certificate Enrollment Policy Protocol (MS-XCEP) and WS-Trust X.509v3 Token Enrollment Extensions (MS-WSTEP) protocols that allows Windows clients to auto enrol for both user and computer certificates.

The protocol allows clients to query for the list of certificate profiles (templates) available and then automatically enrol for them. Configuration for XCEP and WSTEP are both done using Group Policy and hence there is no per user or computer configuration.

By using the web services proxy, customers can deploy and use certificates without needing to manage an internal PKI. In addition, encryption certificates are automatically published to Active Directory and to an Internet based repository allowing easier user to user secure messaging using S/MIME.

Xorble Web Service Pre-Requisites

- Network Connectivity to Xorble
- Windows Server 2012 R2 Member Server with IIS
- Install Xorble Web Service Proxy
- DNS TXT Records
- User Authentication Certificates for Each Domain (UPN, machine and email suffixes)
- Web Server Certificate and ISS Configuration
- Xorble CA Certificate Publishing to Active Directory
- Configuring Auto Enrolment in Active Directory

Installation Details

Network Connectivity to Xorble

Xorble is designed to enable customers all over the world to connect to the service using an internet connection. Customers need to use the internet to establish a connection to the service.

Customers planning to use Xorble should assess their existing and forecasted internet connectivity needs as a part of the deployment project.

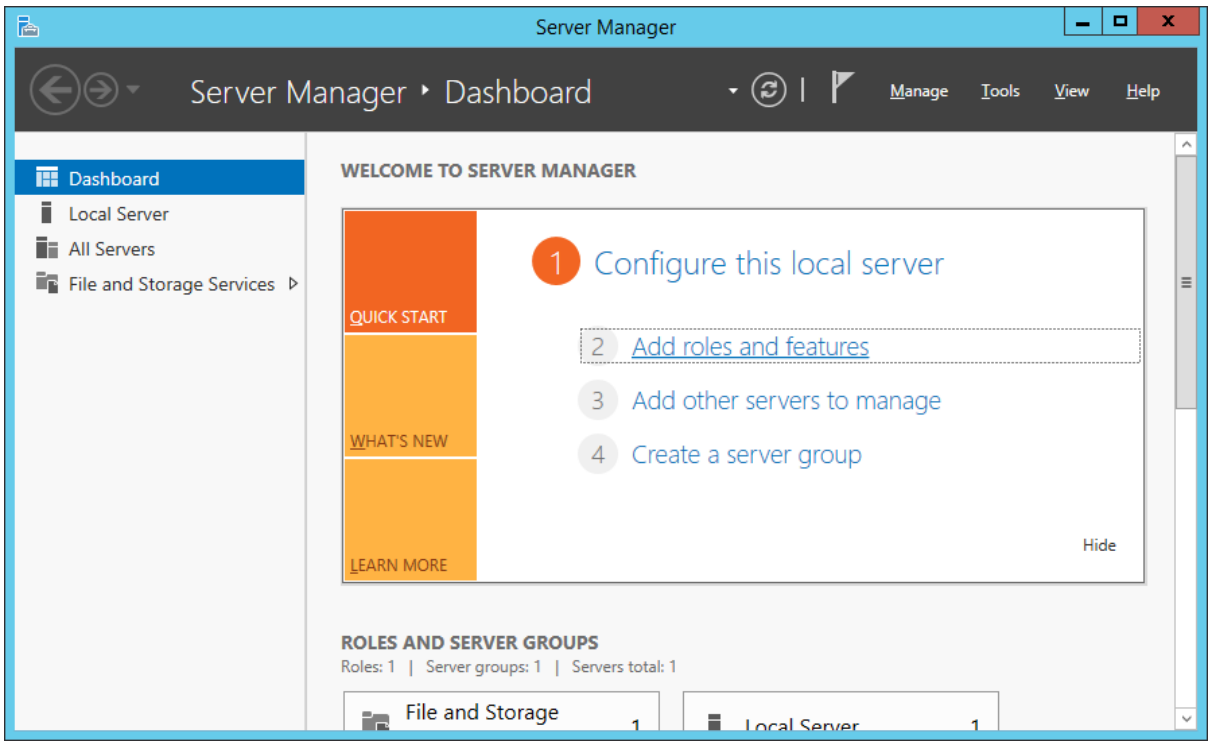
Most organisations network environments can be accommodated with minor changes to network egress - Xorble is a web based service and needs several URLs to be permitted to the Internet. The URLs that are required are:

URL	Description
www.xorble.com	Main web site and WebAPI URL
pki{N}.xorble.com	Location for certificate revocation list, published CA information and end entity (user) certificates. N can be from 0 to 63.
ocsp{N}.xorble.com	Location for the Online Certificate Status Protocol endpoint. N can be from 0 to 63.

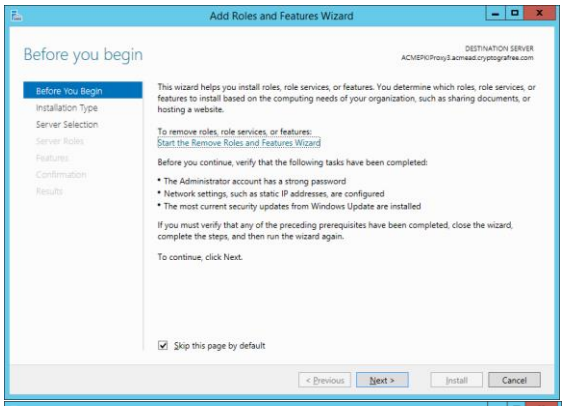
The IP addresses of the above URLs will change over time as additional services are deployed. Xorble also extensively utilises the Azure Content Delivery Network (CDN) to cache content locally to end users and the IP addresses of the CDN vary over time and location.

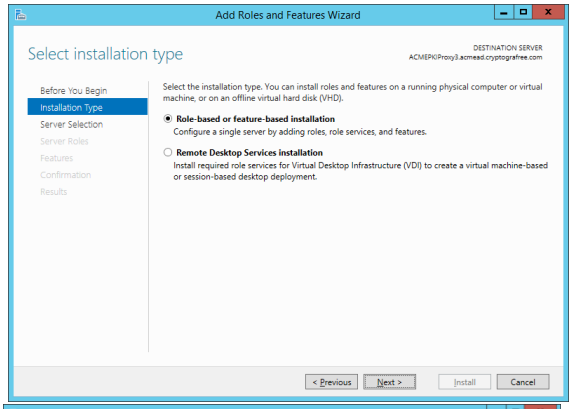
Installing Internet Information Services (IIS)

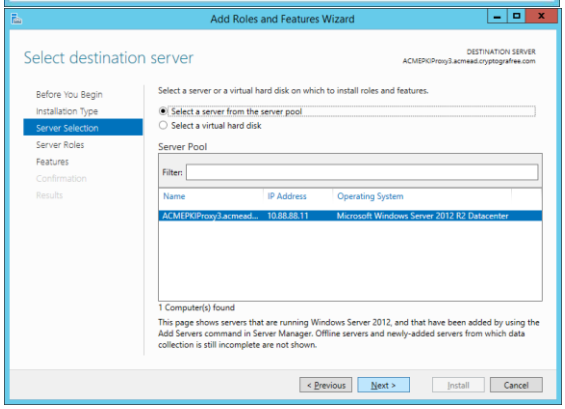
Start server manager and select ***Add roles and features*** as below:

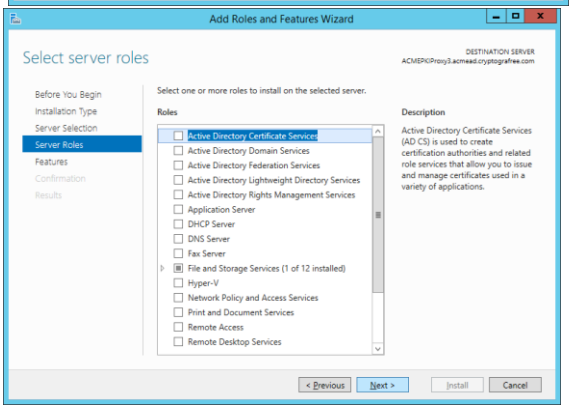


Select Next, Next, Next,

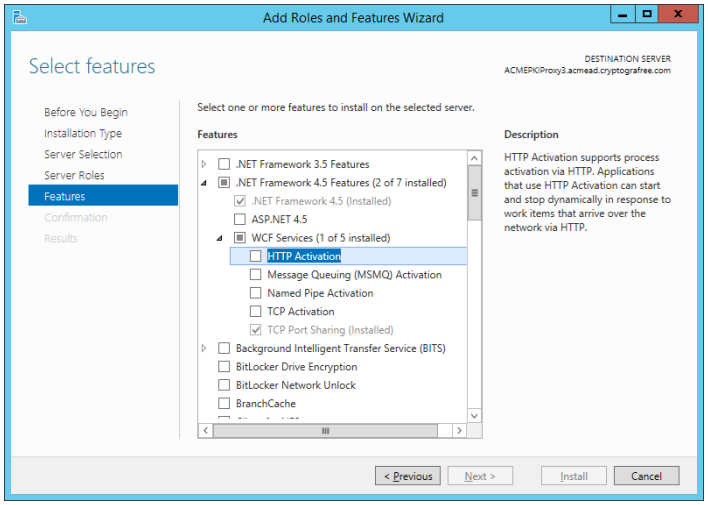




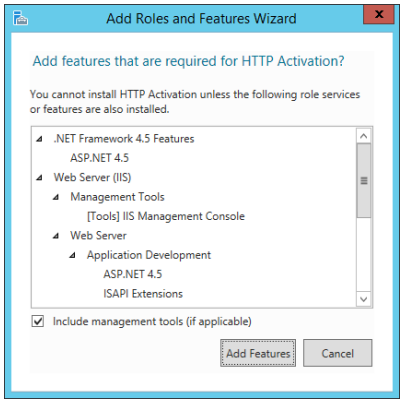




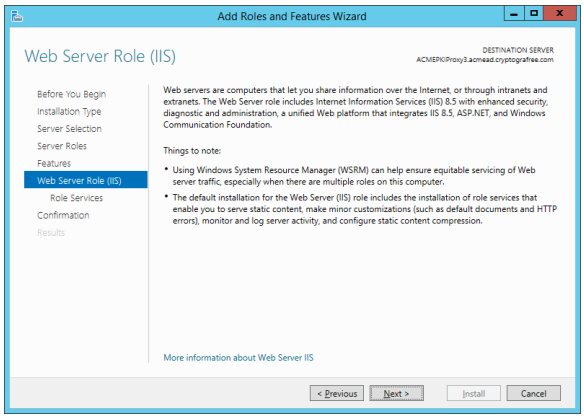
Expand **.NET Framework 4.5 features**, **WCF Services**, and Select **HTTP Activation**:

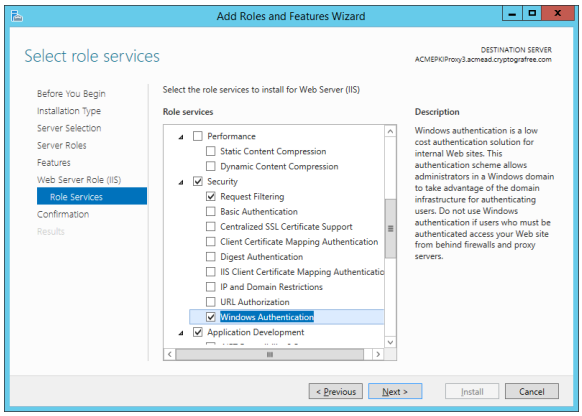


Select **Add features**:

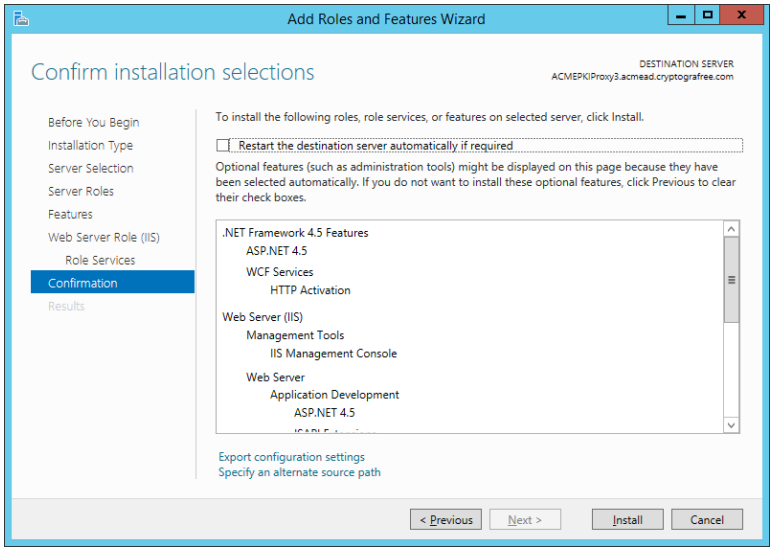


Select **Next, Next** and then Add **Windows Authentication** to the list of installed IIS role services and **Next**.

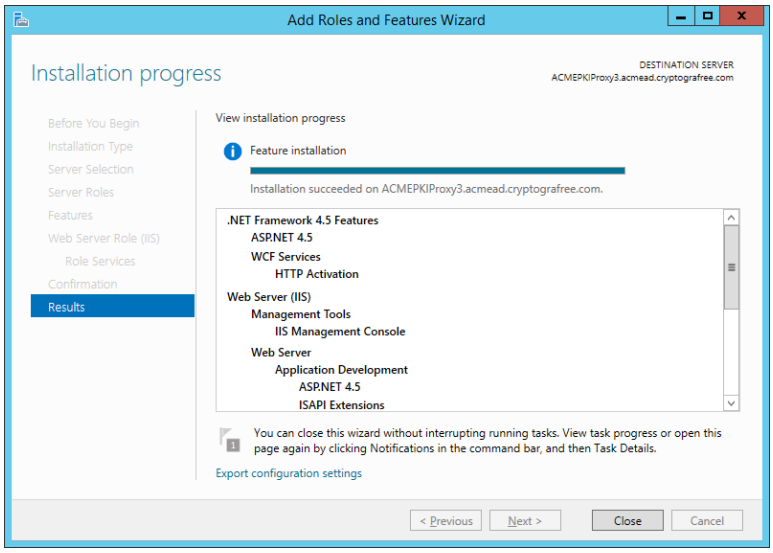




Select **Install** to install IIS, with WCF HTTP Activation.



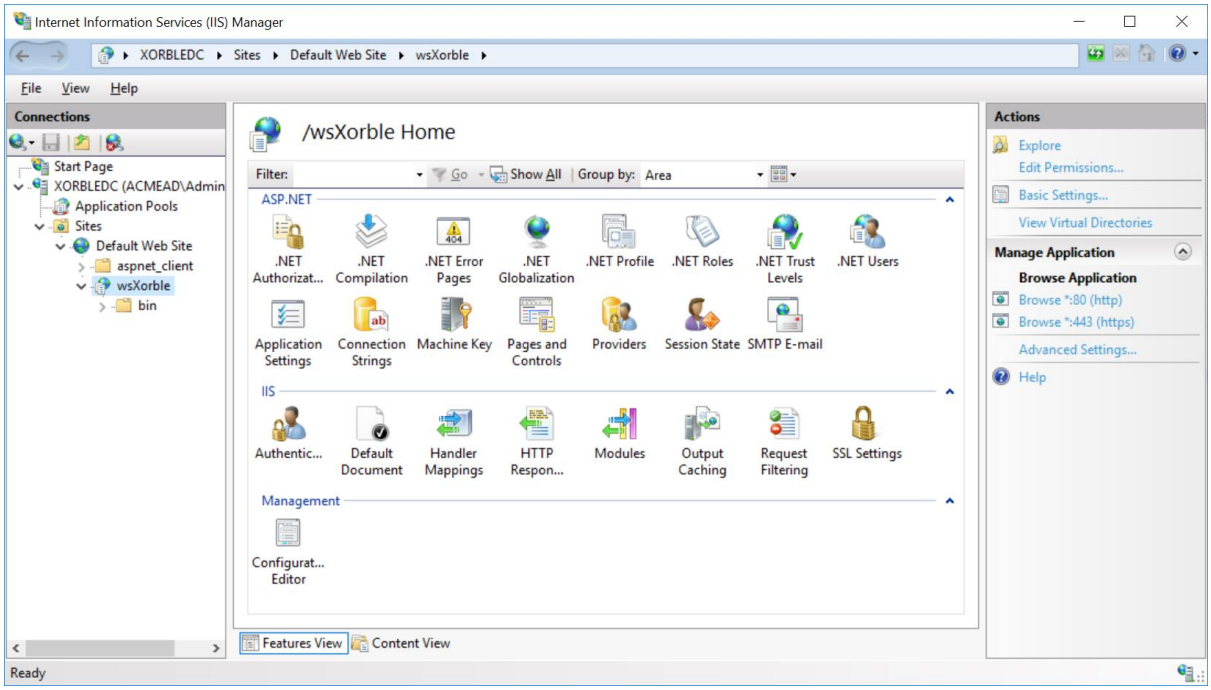
Wait for the installation to complete and **Close**.



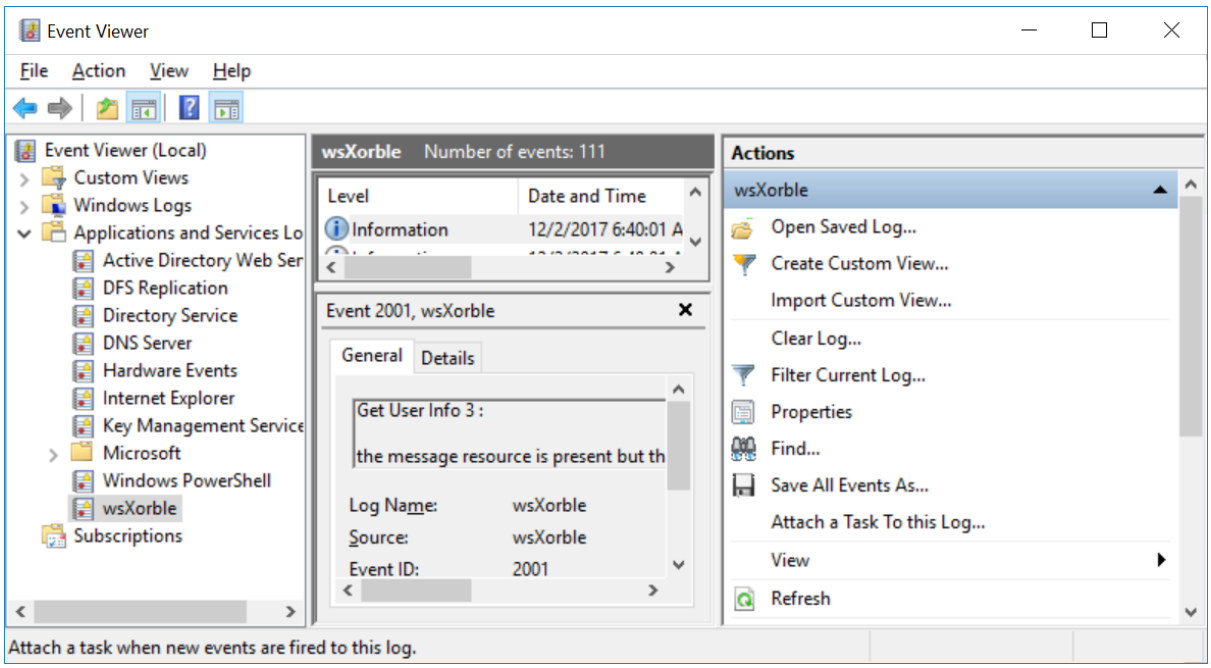
Install wsXorbleSetupProject.MSI

Download the wsXorbleSetupProject.msi file to the server and run it. This will install the Xorble Web Services Proxy component on the server.

This installs components to the “C:\Program Files (x86)\wsXorble” folder and creates a Web Application called wsXorble as shown below:



It also creates an event log called wsXorble as shown below:



Configure Xorble Authentication Certificates

Client certificate(s) are used to allow the Web Services Proxy to authenticate to Xorble in order to enrol for user and computer certificates. The identities associated with these certificates have to be configured to allow them to “enrol on behalf of” other users. Xorble uses DNS TXT records to control the authorisation process for these identities so that only identities that have a matching correct DNS TXT record can perform the enrolment for other users and computers.

Xorble will also only permit certificates to be issued to users and computers whose domain name matches the enrolment certificate identity.

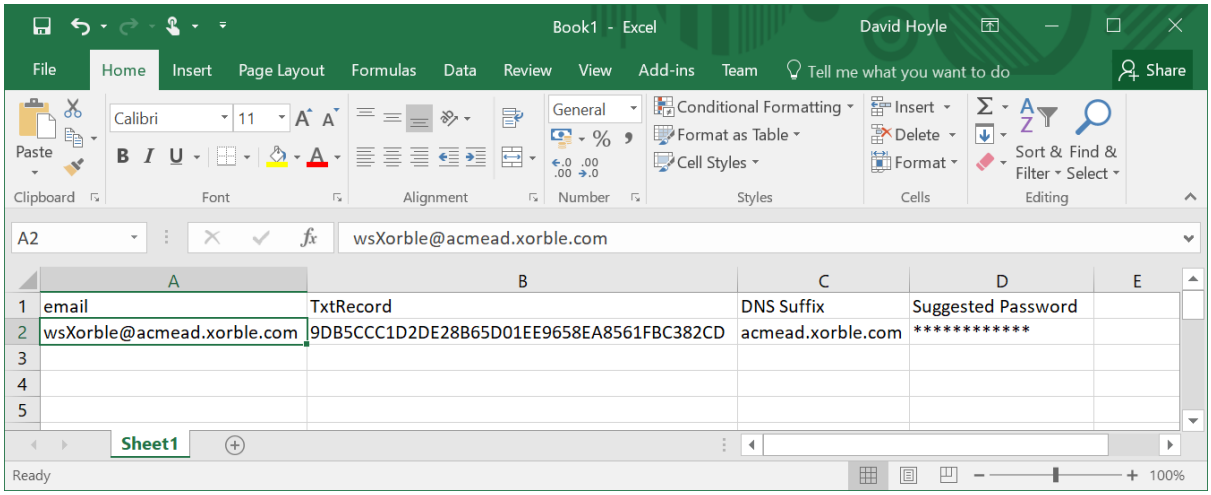
Obtain Active Directory DNS TXT Record List

The PowerShell script queries Active Directory for all name suffixes that will need a corresponding TXT record creating. The script first reads the list of all domain in the forest, then reads the domain suffix list and finally enumerates all email address suffixes – this last query can take some run to run.

Start a PowerShell in the "C:\Program Files (x86)\wsXorble" folder and run the FindDNSTXTRecords.ps1 PowerShell script and redirect the output to a CSV file called DNSTXTRecords.csv.

```
cd "C:\Program Files (x86)\wsXorble"

.\FindDNSTXTRecords.ps1 > DNSTXTRecords.csv

Domain Suffix List

Alternative UPN Suffix List

... Finding user emails - this make take some time ...

Email Suffix List



Press Enter to continue...:
```

Open the CSV (Tab delimited) file called DNSTXTRecords.csv in Excel or equivalent as shown below:



For each item in the file, create a DNS TXT record (using your DNS management tool) and set the value of this TXT record to the following string:

```
8:Request_Web,Domain Users,Domain Computers,Domain Controllers
```

The following example shows a typical configuration of the TXT records:

DNS ENTRY	TYPE	PRIORITY	TTL	DESTINATION/TARGET
3EDB21E8EDC8F8C43DEF4241A1D20EEDE1CDE693	TXT/SPF			8:Request_Web Domain...
95888A9EB3636A5381669059CFA67D2858DA3B5A.acmead	TXT/SPF			8:Request_Web Domain...

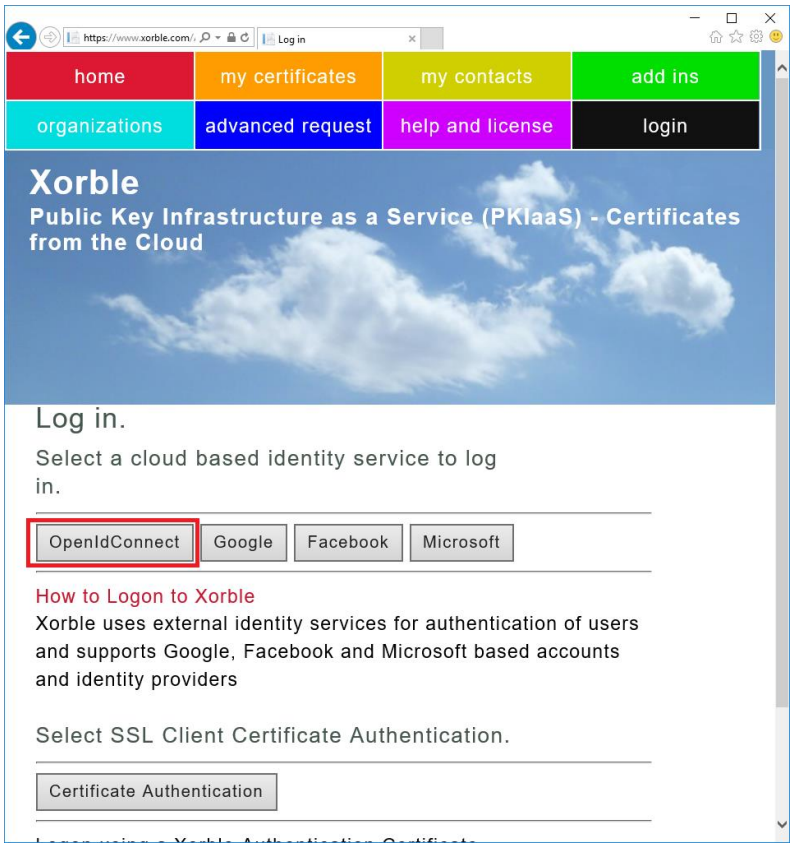
Register Additional Email Proxy Addresses

It is recommended that the identity use for this process is called wsXorble. In order to be able to enrol for a certificate using this name, probably the simplest way is to create a corresponding Azure Active Directory (AAD) account for each of the identities in the above CSV.

Enroll for Web Services Authentication Certificates

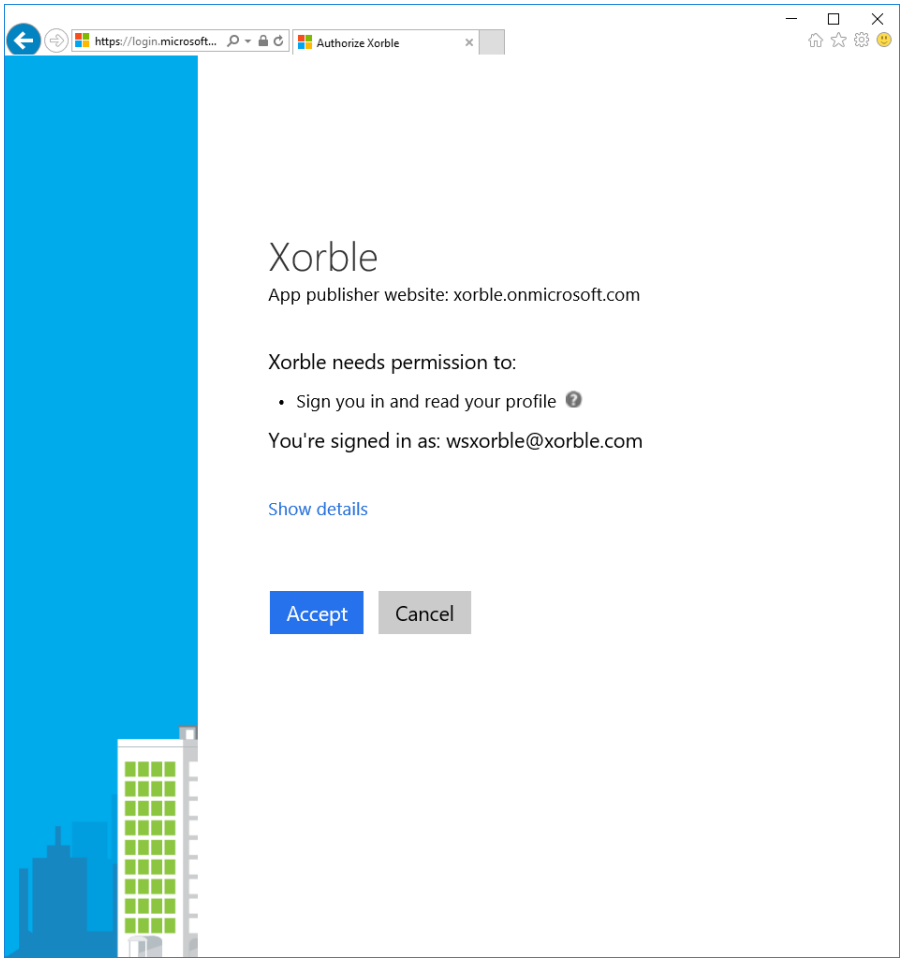
In order to authenticate the web services proxy an authentication certificate is required. Start a browser using InPrivate (to stop it automatically logging in) and go to https://www.xorble.com/MyCerts/CertsIndexView

Select OpenIDConnect as shown below to logon using the AAD Account:

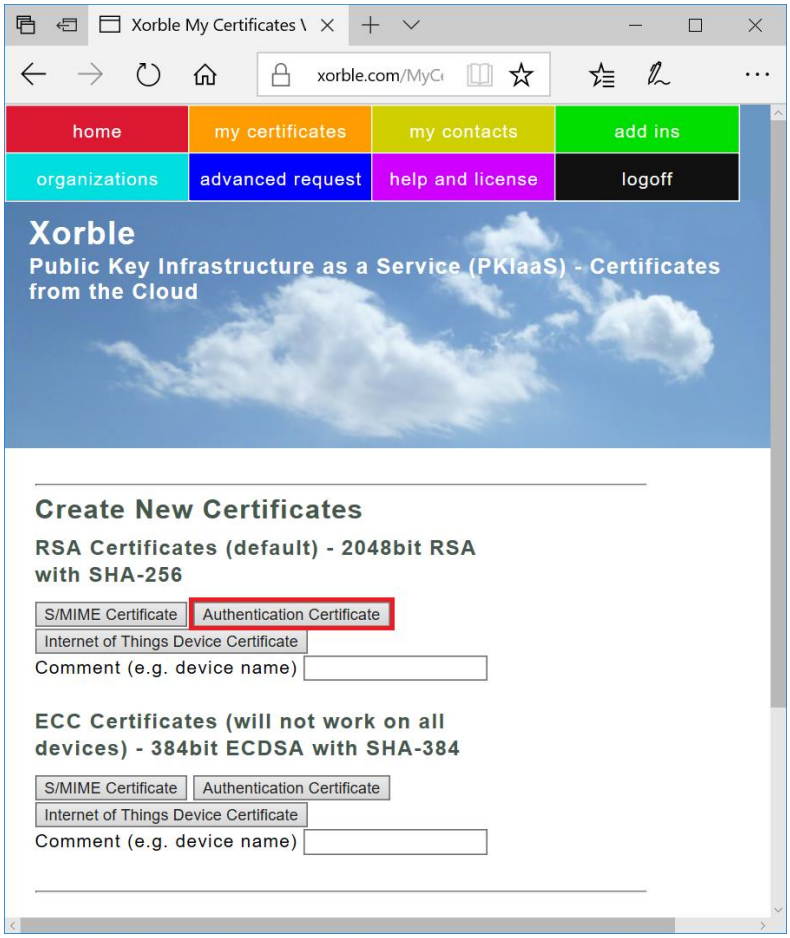


Enter the AAD account details to logon.

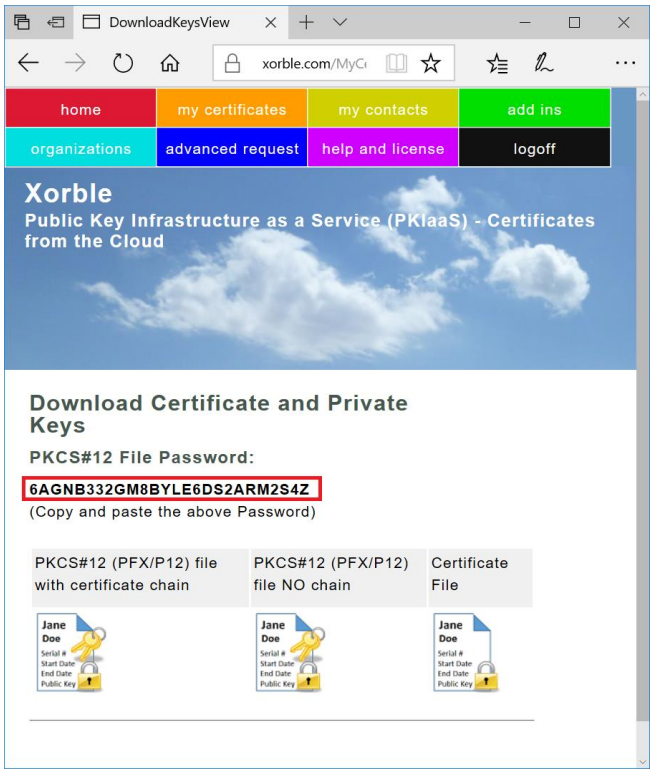
Select **Yes** to allow Xorble to see the email address of this user.



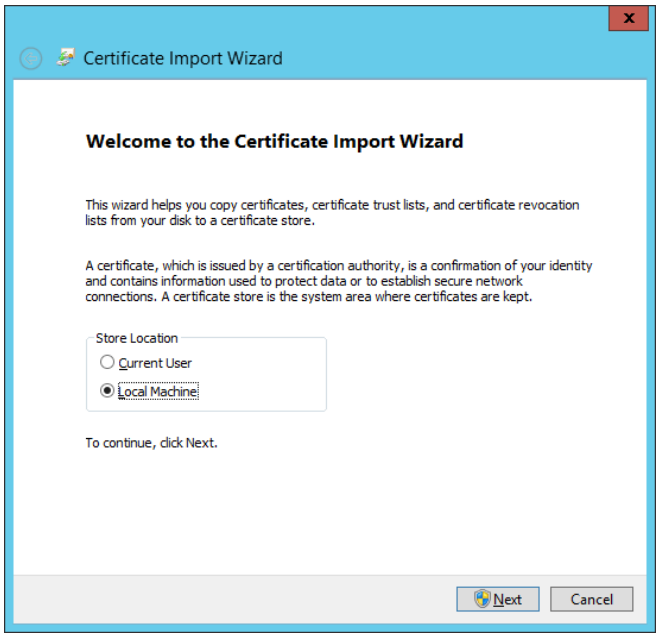
You should now be authenticated to Xorble as the wsXorble identity. Select **Authentication Certificate** as shown below to create a new Authentication certificate for the identity.


Xorble My Certificates \
xorble.com/MyC
home
my certificates
my contacts
add ins
organizations
advanced request
help and license
logoff
Xorble
Public Key Infrastructure as a Service (PKIaaS) - Certificates from the Cloud
Create New Certificates
RSA Certificates (default) - 2048bit RSA with SHA-256
S/MIME Certificate
Authentication Certificate
Internet of Things Device Certificate
Comment (e.g. device name)
ECC Certificates (will not work on all devices) - 384bit ECDSA with SHA-384
S/MIME Certificate
Authentication Certificate
Internet of Things Device Certificate
Comment (e.g. device name)

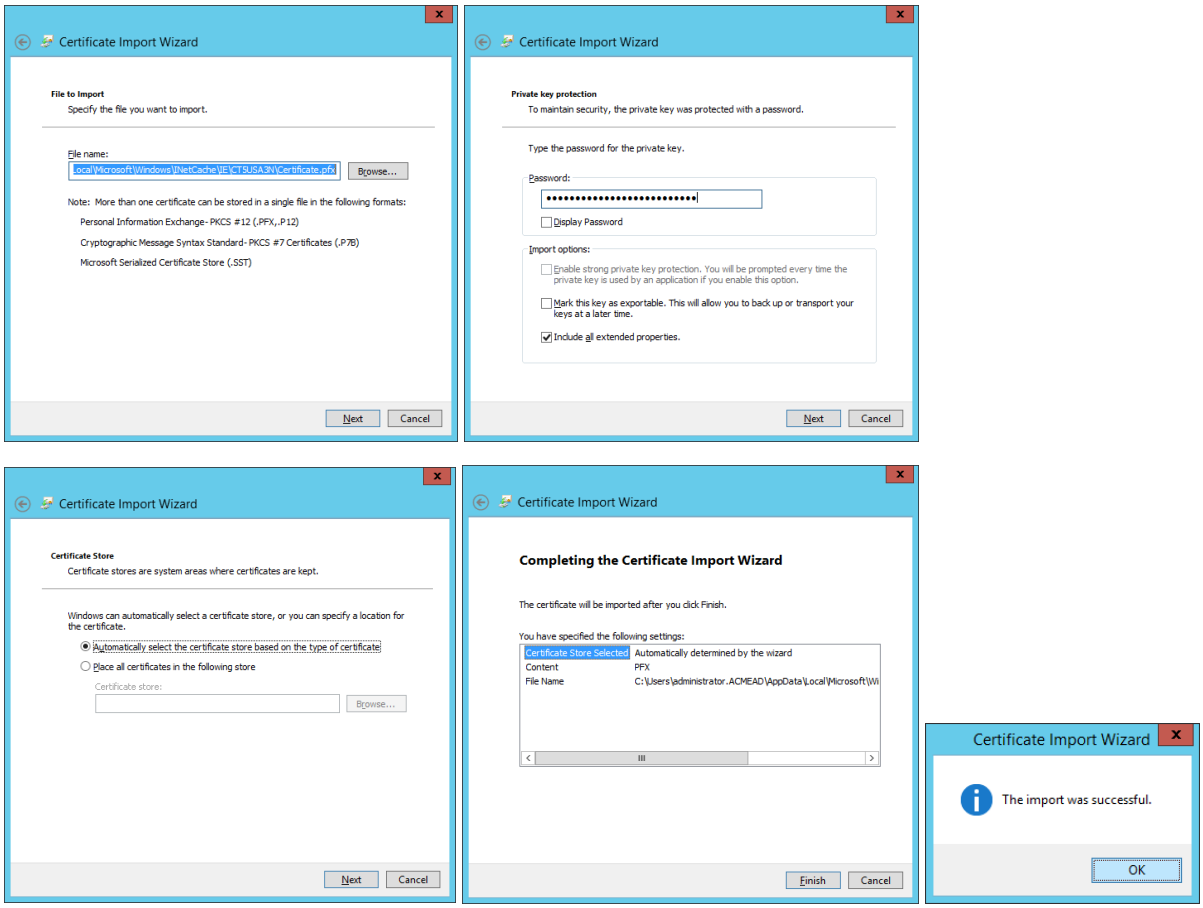
This will create an authentication certificate for the identity – copy and paste the password and then click on the certificate to download as shown below:



Select Open when the download is complete and then select **Local Machine** and then **Next** as shown below:



Select **Next** and then enter the **Password, Next, Next** and **Finish** as below.

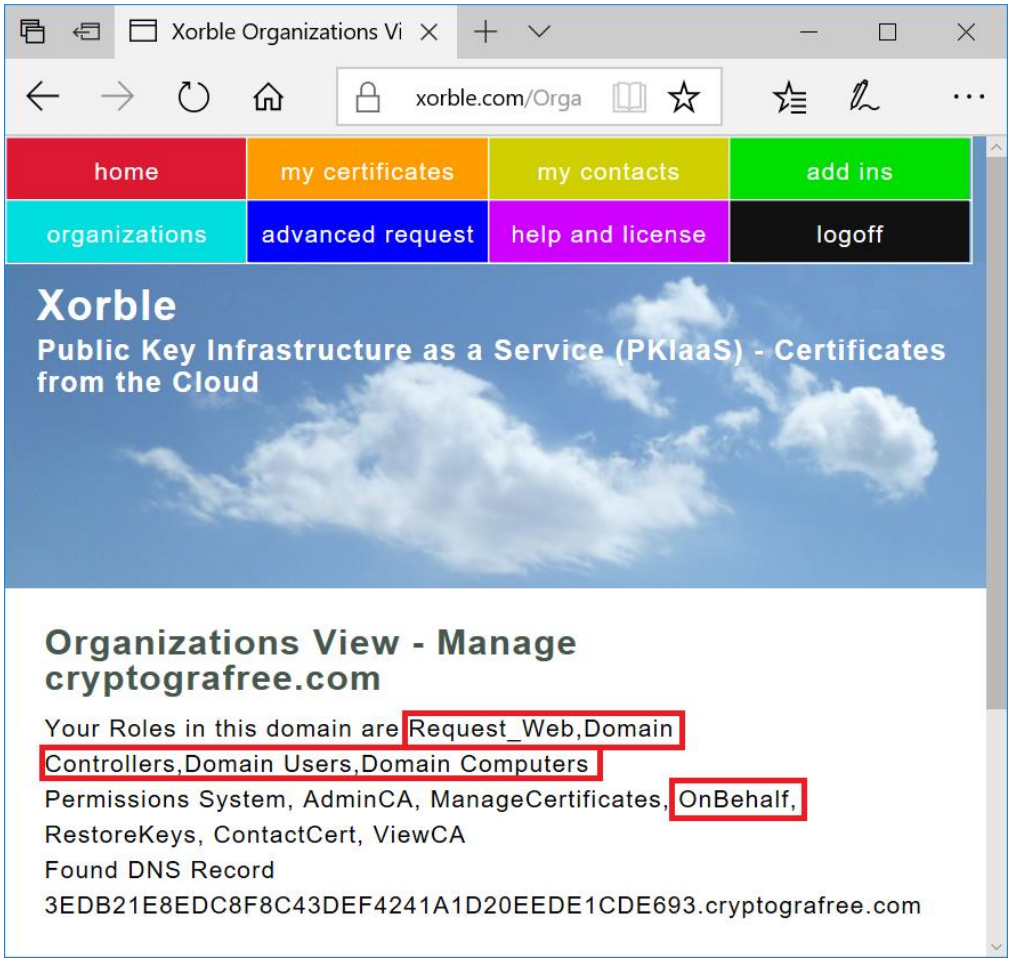


Repeat this process for each of the email addresses in the DNSTXTRecords .CSV file.

Check the New wsXorble Identity Permissions

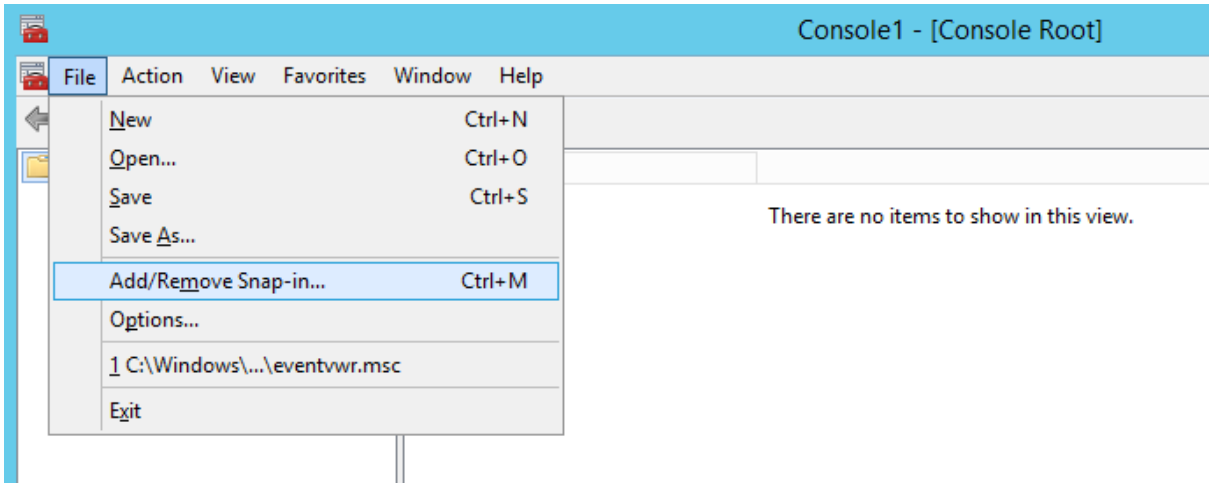
Open the URL https://www.xorble.com/Organizations/OrganizationsView and logon using the wsXorble account that was previously created.

You should see that the account has OnBehalf permissions and has roles that include Web request, Domain Users, Domain Computers and Domain Controllers as shown below:

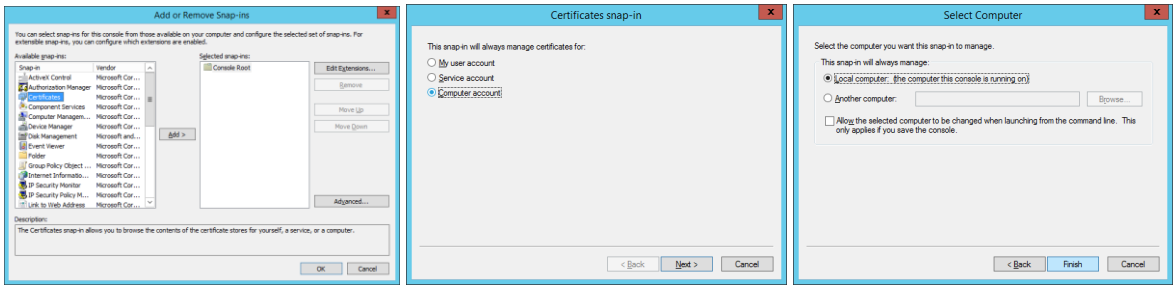


Setting Permissions on the Certificate Private Keys

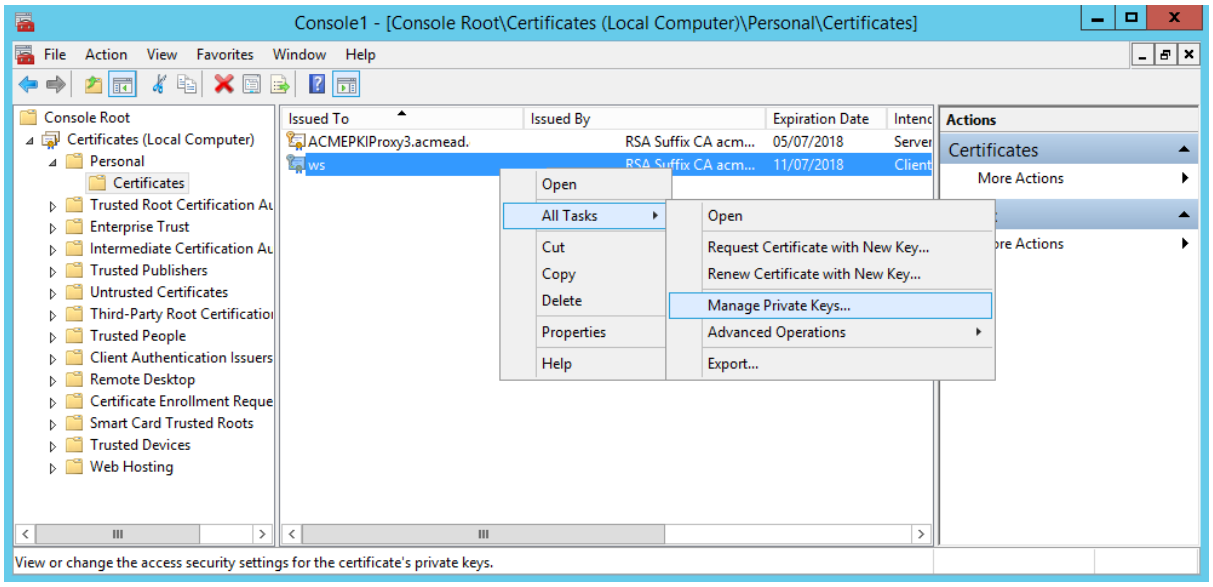
Open **MMC.EXE** and then select **Add/Remove Snap-in…**



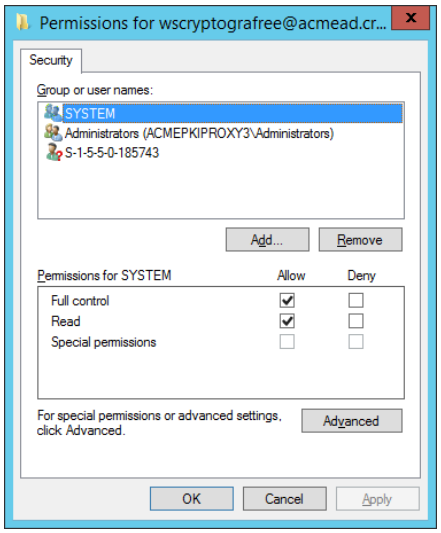
Select **Certificates** and **Add** and then **Computer account** and **Next** and **Finish** and **OK.**



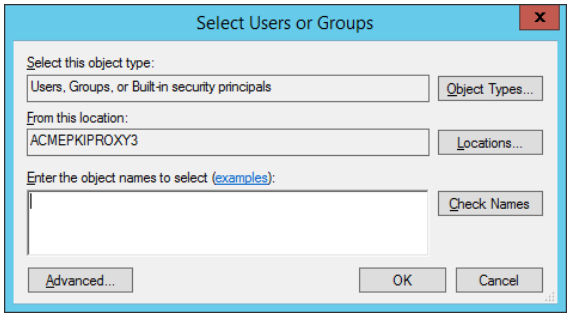
Open the Certificates, Personal, Certificates. Right click on the wsXorble certificate and select **All Tasks**, **Manage Private Keys** as below:

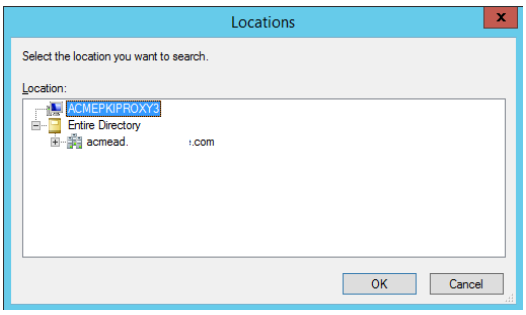


In the permissions dialog, select **Add**.

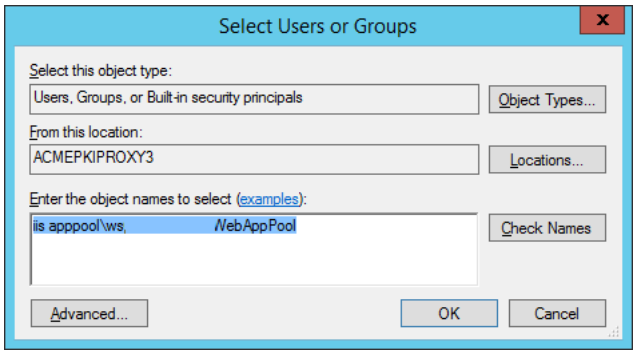


Select **Locations** and select the current server and **OK**.





Enter the string "**iis apppool\wsXorbleWebAppPool**" and then **OK, OK**.



Repeat this process for each of the certificates.

Publish Xorble Certificates to Active Directory

Start a PowerShell in the "C:\Program Files (x86)\wsXorble" folder.

Run the following command to publish and run the FindDNSTXTRecords.ps1 PowerShell

```
cd "C:\Program Files (x86)\wsXorble"

.\FindDNSTXTRecords.ps1 -ADPublish $true

Domain Suffix List


Get Domain Suffix List

Get Alternative UPN Suffix List

... Finding user emails - this make take some time ...

Downloadfile http://pki{N}.xorble.com/aia/Xorble rsa root ca.cer

ldap:///CN=Xorble RSA Root CA,CN=Certification Authorities,CN=Public Key
Services,CN=Services,CN=Configuration,DC

=acmead,DC=Xorble,DC=com?cACertificate


Certificate added to DS store.
```

```
ldap:///CN=Xorble RSA Root CA,CN=AIA,CN=Public Key
Services,CN=Services,CN=Configuration,DC=acmead,DC=cryptografr

ee,DC=com?cACertificate


Certificate added to DS store.


CertUtil: -dsPublish command completed successfully.

Downloadfile http://pki{N}.xorble.com/aia/Xorble ecc root ca.cer

ldap:///CN=Xorble ECC Root CA,CN=Certification Authorities,CN=Public Key
Services,CN=Services,CN=Configuration,DC

=acmead,DC=Xorble,DC=com?cACertificate


Certificate added to DS store.


ldap:///CN=Xorble ECC Root CA,CN=AIA,CN=Public Key
Services,CN=Services,CN=Configuration,DC=acmead,DC=cryptografr

ee,DC=com?cACertificate


Certificate added to DS store.


CertUtil: -dsPublish command completed successfully.

Downloadfile http://pki{N}.xorble.com/aia/Xorble rsa organisation ca.cer

ldap:///CN=Xorble RSA Organisation CA,CN=AIA,CN=Public Key
Services,CN=Services,CN=Configuration,DC=acmead,DC=cry

ptografree,DC=com?cACertificate


Certificate added to DS store.


CertUtil: -dsPublish command completed successfully.

Downloadfile http://pki{N}.xorble.com/aia/Xorble ecc organisation ca.cer

ldap:///CN=Xorble ECC Organisation CA,CN=AIA,CN=Public Key
Services,CN=Services,CN=Configuration,DC=acmead,DC=cry

ptografree,DC=com?cACertificate
```

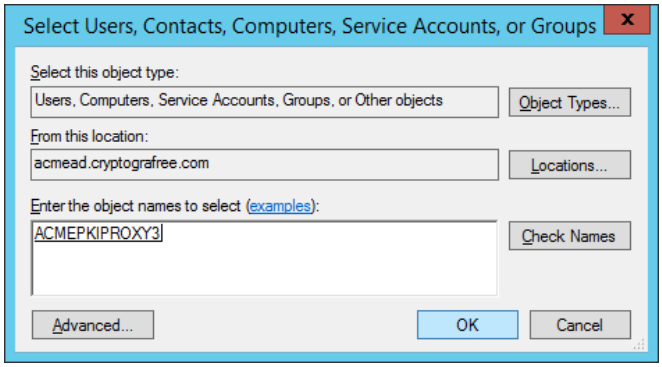
```
Certificate added to DS store.

Downloadfile http://pki{N}.xorble.com/aia/Xorble rsa suffix ca acmead.........com.cer

ldap:///CN=NTAuthCertificates,CN=Public Key
Services,CN=Services,CN=Configuration,DC=acmead,DC=Xorble,DC=com?cACe

rtificate

Certificate added to DS store.

CertUtil: -dsPublish command completed successfully.

ldap:///CN=Xorble RSA Suffix CA acmead.Xorble.co-00109,CN=AIA,CN=Public Key
Services,CN=Services,CN=Config

uration,DC=acmead,DC=Xorble,DC=com?cACertificate

Certificate added to DS store.

CertUtil: -dsPublish command completed successfully.

Press Enter to continue...:
```

After running the above, the Xorble certificates will e trusted by all members of the forest.

Adding Web Services Proxy Server to Certificate Publishers Group

Need to add the computer account for the wsXorble server into the Certificate Publishers group within AD and reboot this server.

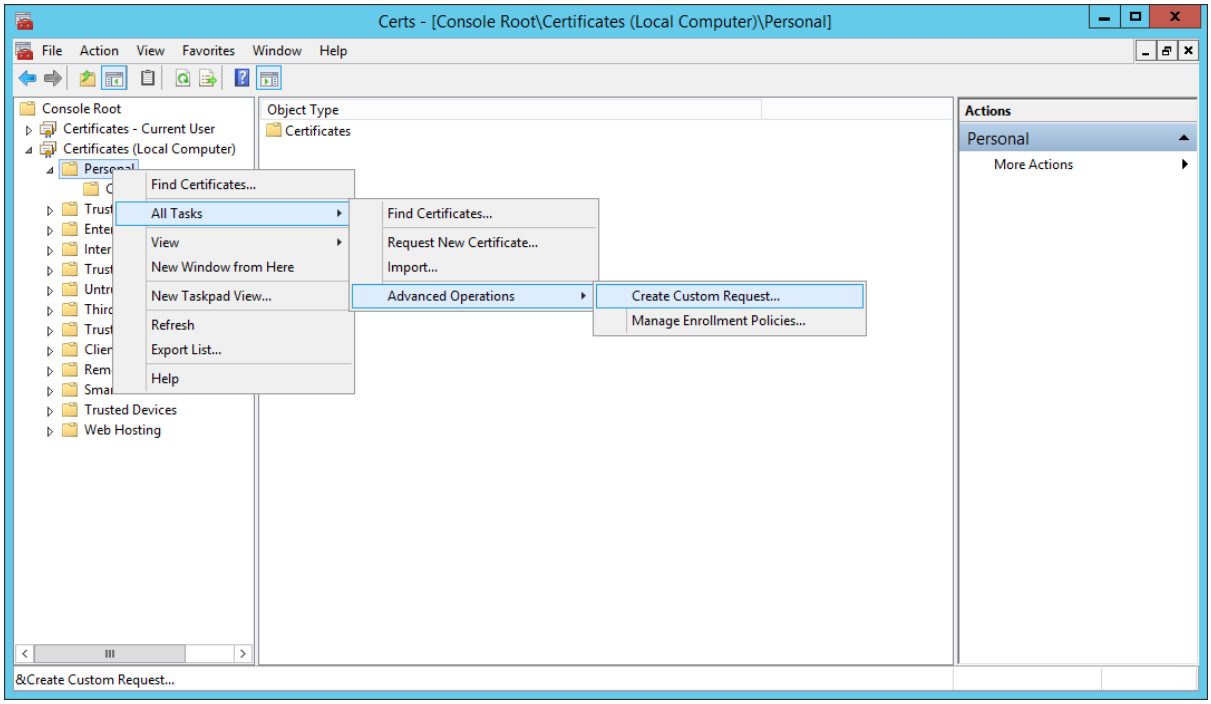
Open Active Directory Users and Computers. Navigate to the Users container and open the “Cert Publishers” group. Select the Members tab and then Add. Select Object Types and add computers. Enter the wsXorble server name and OK as shown below:



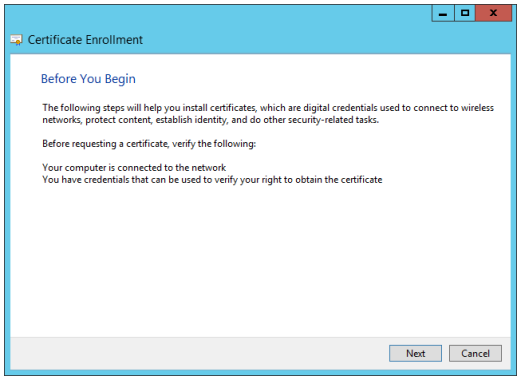
Configuring Web Server Certificate for Web Services Proxy

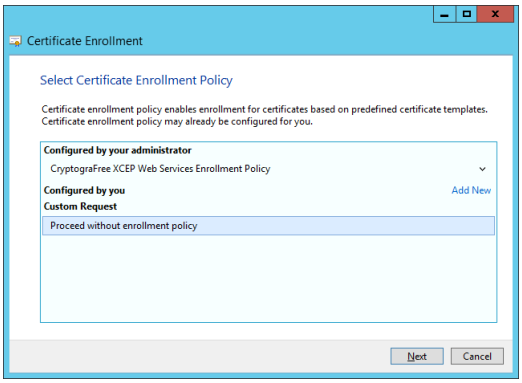
The Web Service requires a Web Server certificate. The web server certificate can be issued by any public CA including Xorble.

To enrol for the web server certificate, open the computer certificate store as shown below. Start a Custom Certificate Request:

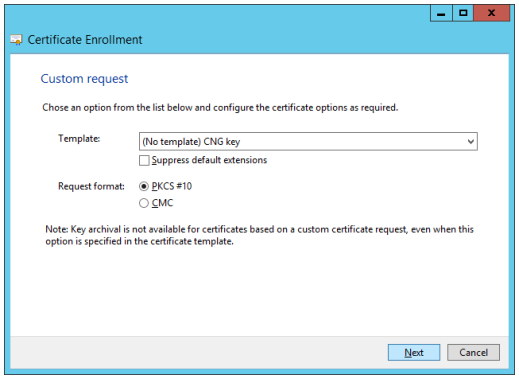


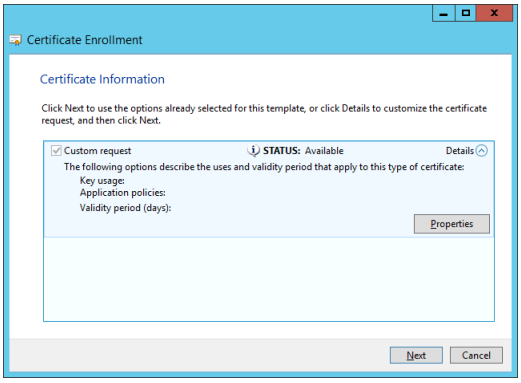
Select **Next**, **Proceed without enrolment policy** and **Next**.



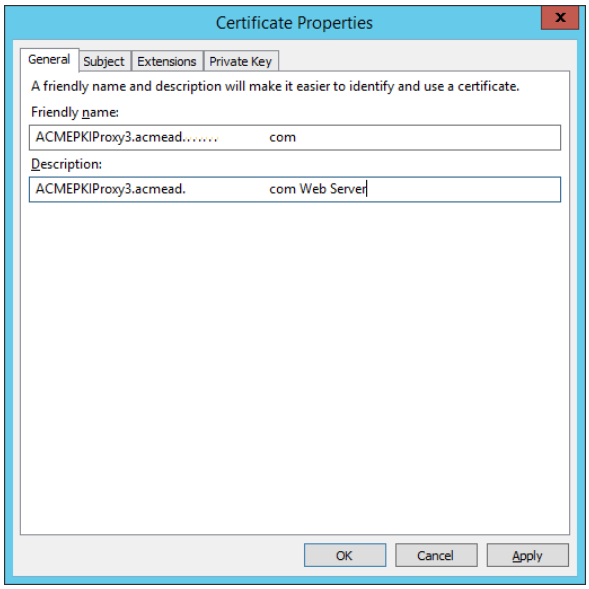


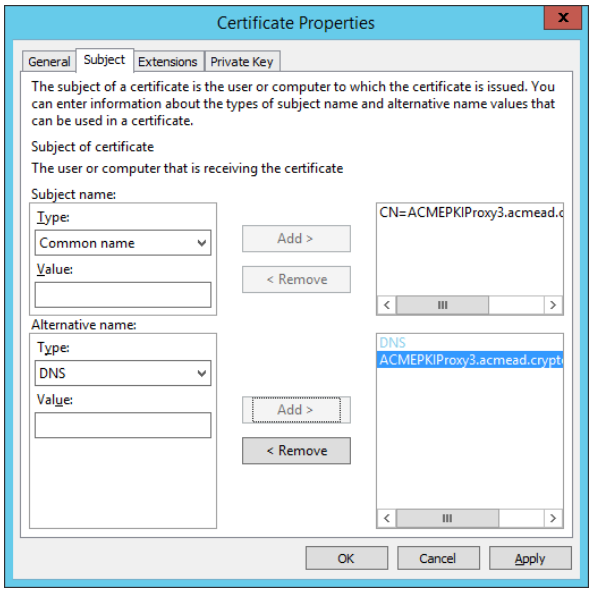
Select **Next** and the select **Properties**.



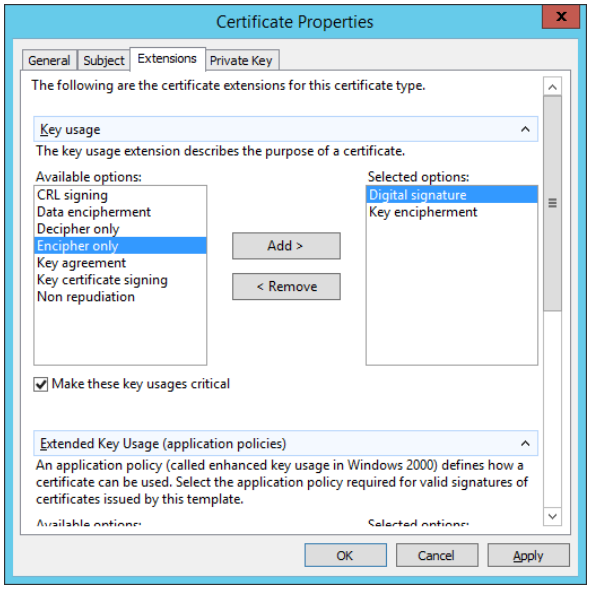


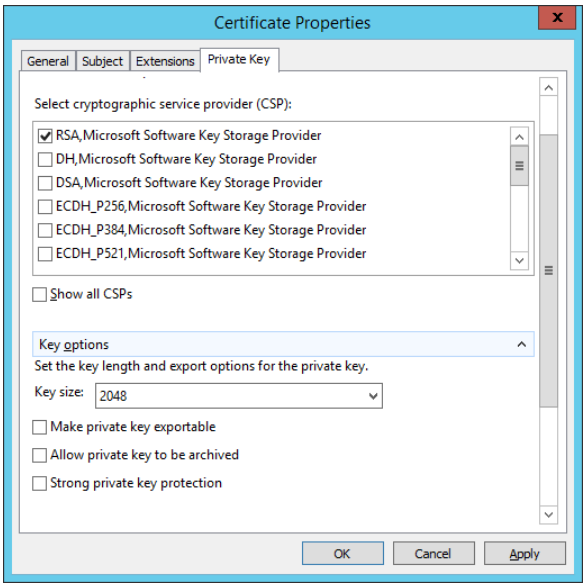
In the certificate request properties, enter the computer name as the friendly name and description and also set this as the Common name and DNS name on the request as shown below:



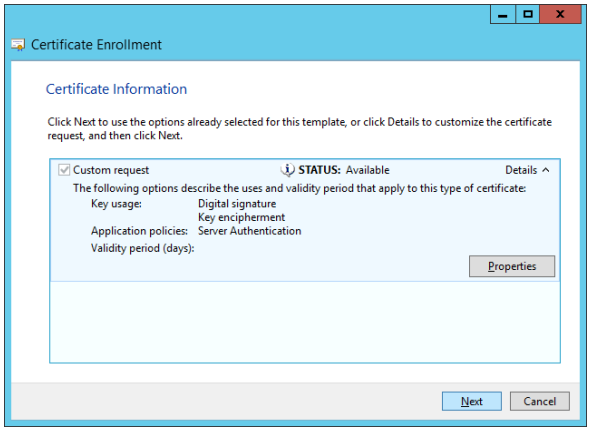


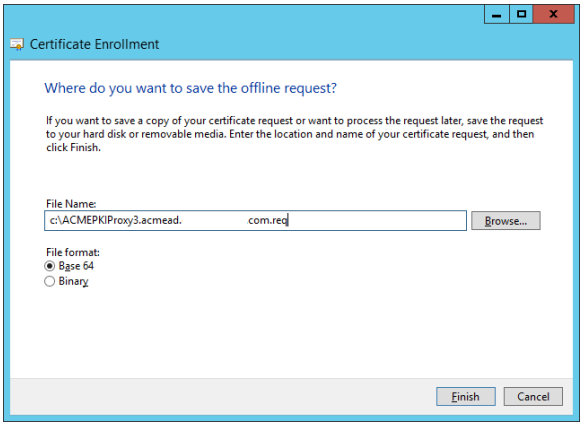
Set the key usage extensions as below and also set the Key size to **2048** bits.



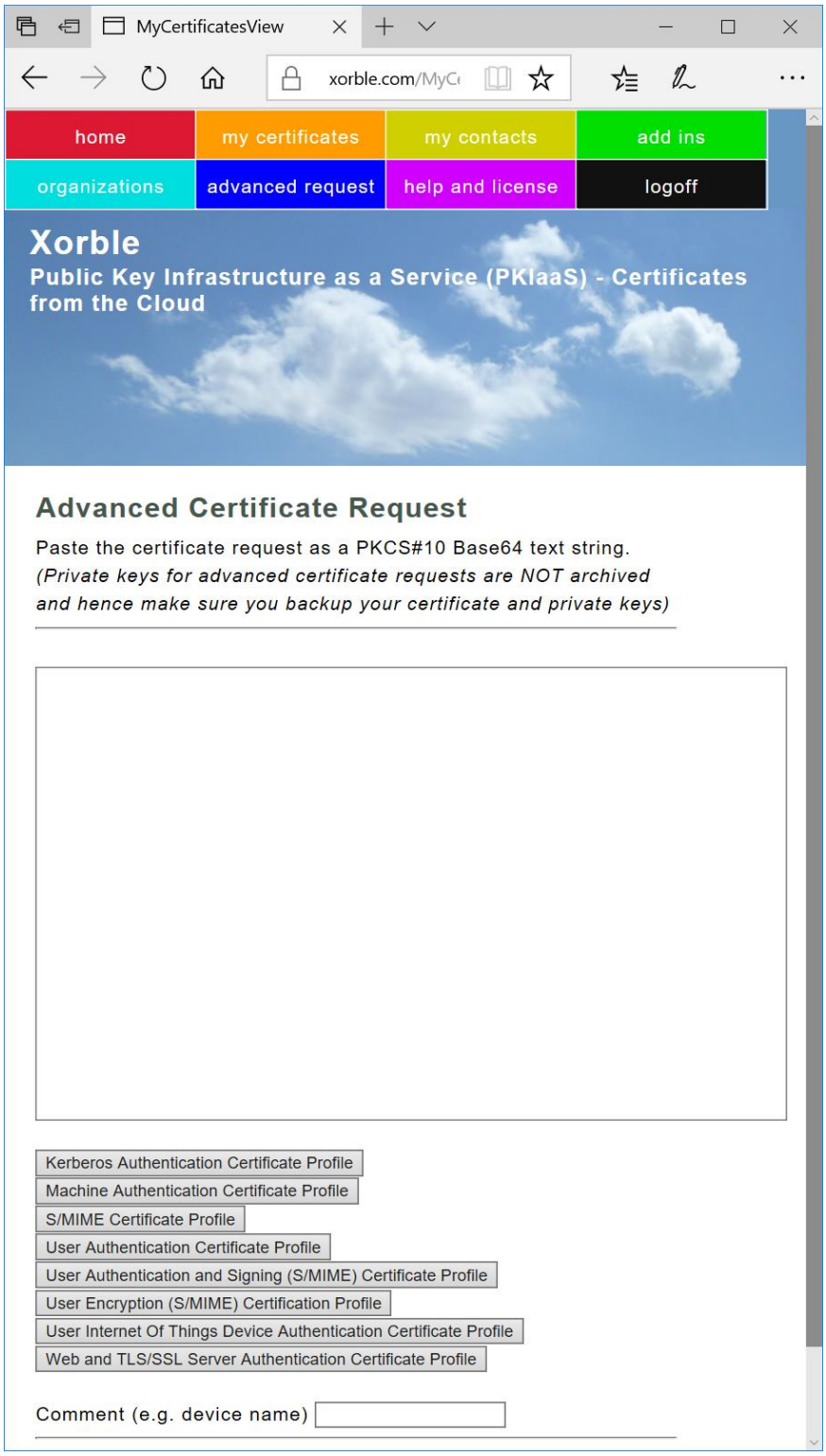


Select **OK**, **Next** and then set the file name before selecting **Finish** as below:





Open the browser and go to https://www.xorble.com advanced request

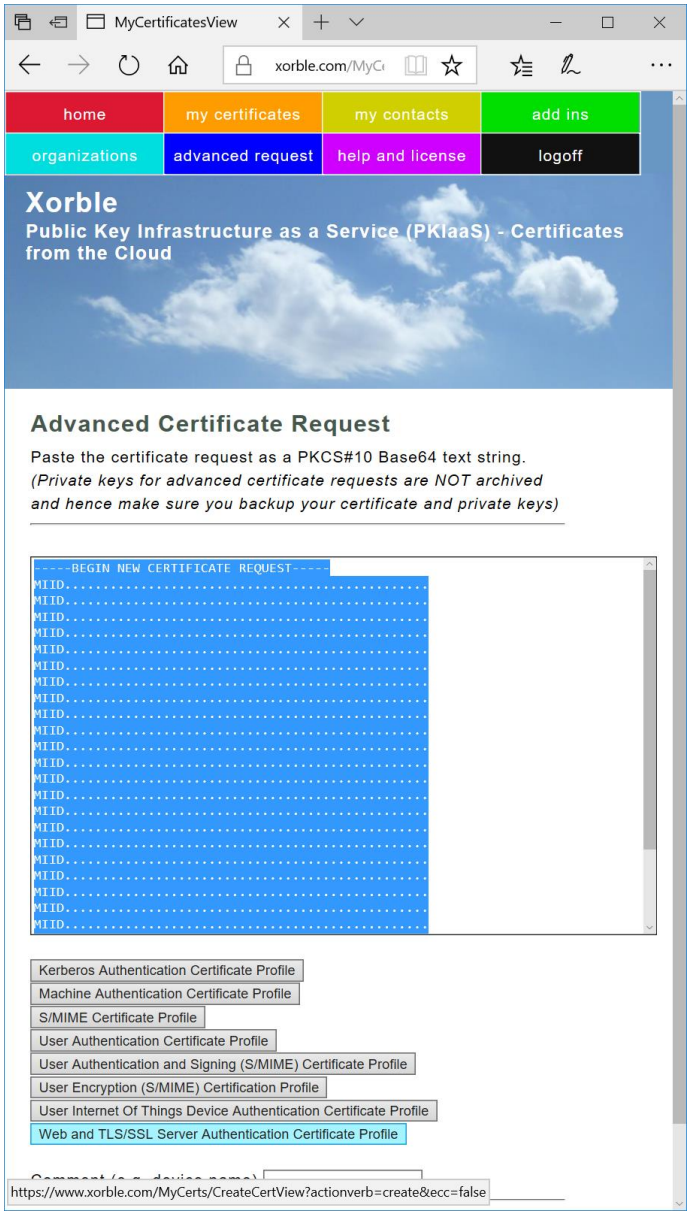


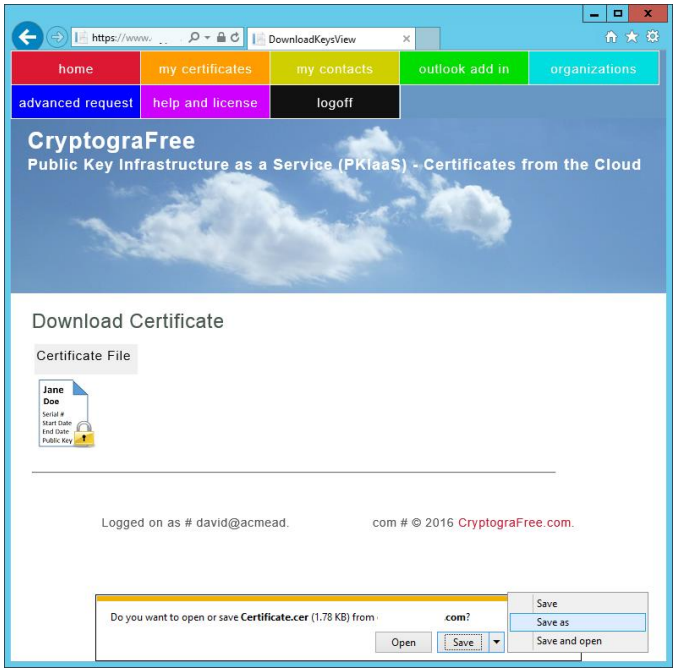
Copy and paste the request file:

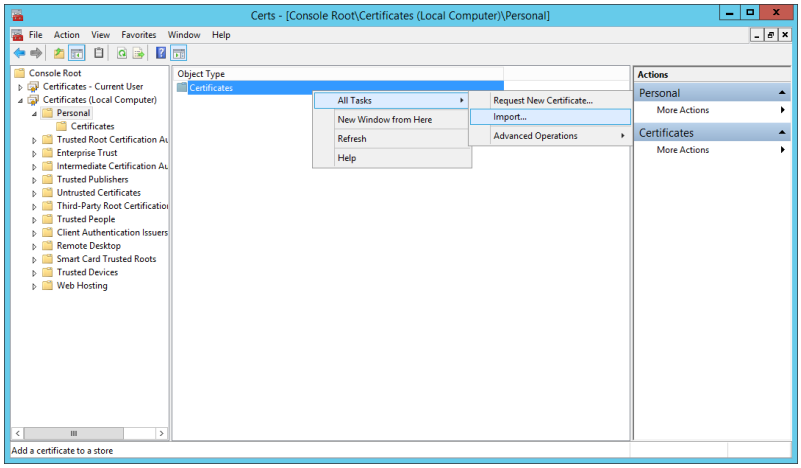
ACMEPKIProxy3.acmead. req - Notepad

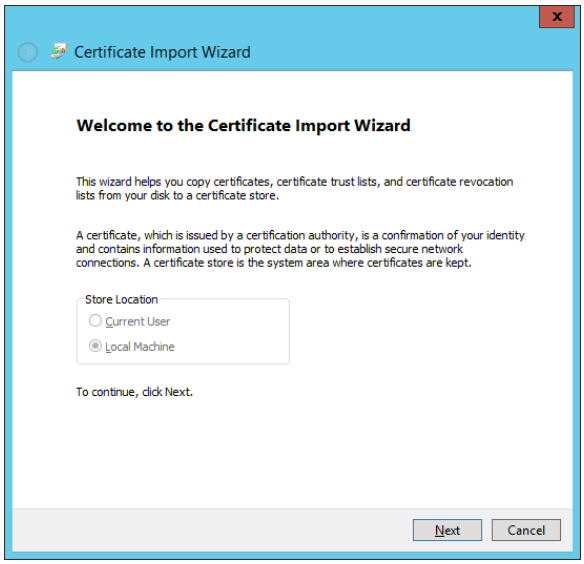
File Edit Format View Help

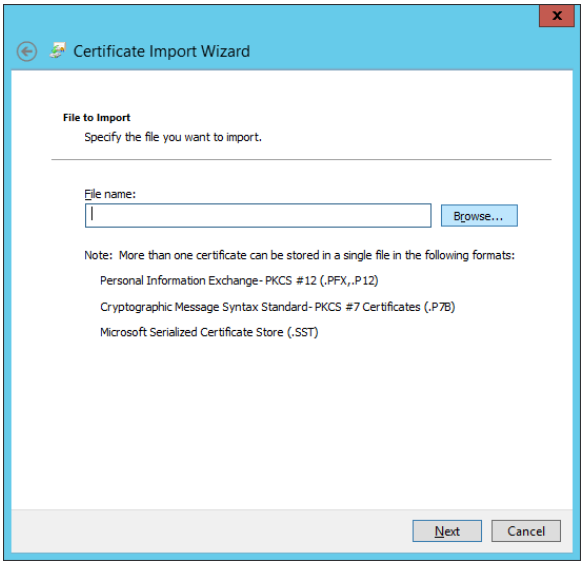

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIID/zCCAucCAQAwMTEvMC0GA1UEAwwmQUNNRVBLSVByb3h5My5hY211YWQuY3J5
cHRvZ3JhZnJlZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC1
s7CosOBPid+hdJhj0yQQ1KVCOgsG363rsL6c/vIYMq7rs7sPIeBcV1yg+ykejI8+
BMvqIjtQtt0uGsJq8/imuBptxn1Ad93AQaoHbg5tuqVkqh5VJQ6I4DMpoet5AD/e
BdWrJRMPGsknc0Crm8JZKRWz75iyG4C+qhfh1QvoEkjJ3G2H3FhhsLSfJuTTk+Vq
O2UhEMMSYaB9h2jbFA9dcj2BwyXZpr/qmyjuGPtRhTyTJbKR5sgciAy4O2yRMxut
7A0NfnTm6Rm0RX2T+yUe/ms5C11C7HtYUPkWCUqXxIIqS0kW9ag/ibPy+kvAsIFA
sKpPb7LYUYNqc1xaHx2DAgMBAAGgggGHMBoGCisGAQQBgjcNAgMxDBYKNi4zLjk2
MDAuMjBZBgkrBgEEAYI3FRQxTDBKAgEFDCZBQ01FUEtJUHJveHkzLmFjbWVhZC5j
cnlwdG9ncmFmcmVlLmNvbQwUQUNNRUFEXGFkbWluaXN0cmF0b3IMB01NQy5FWEUw
ZgYKKwYBBAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMAbwBm
AHQAdwBhAHIAZQAgAEsAZQB5ACAAUwB0AG8AcgBhAGcAZQAgAFAAcgBvAHYAaQBk
AGUAcgMBADCBpQYJKoZIhvcNAQkOMYGXMIGUMDEGA1UdEQQqMCiCJkFDTUVQS0lQ
cm94eTMuYWNtZWFkLmNyeXB0b2dyYWZyZWUuY29tMA4GA1UdDwEB/wQEAwIFoDAT
BgNVHSUEDDAKBggrBgEFBQcDATAbBgkrBgEEAYI3FQoEDjAMMAoGCCsGAQUFBwMB
MB0GA1UdDgQWBBSgEr7rsWKQhIpS56qeMWhbPsKRvjANBgkqhkiG9w0BAQsFAAOC
AQEAJzRW1wDZtPXY+nhhkW7pFKgYOqYEHnZJwK34Ud3w6KSuoHDNfLF7+USeYNWw
ObkA4QTeDwZ0b4H4CXoOnwzu8AwdSztGoQAMkHzpUjDuS143ejnpGXFBBTH0mUuA
GS/tzxTAlIo+KXDMYHCihURj1EKdCOfoR+jGHlyB3PnVpSzl52csctoKb/l05IBc
v0zavQTartbFjTR3+KIM+9DhhJ/BcbPAeKKYz2T1iybIQem5WdX3x0hpecW0IOq4
TAcZa8R1a2wZa3XPn43YI/0WrJFp6uTq88gSpfXi1zgvVIJOhe2IIHzbbNNsLmr1
uYMP5LXI/k4HiY4ZkjlM8bP8tg==
-----END NEW CERTIFICATE REQUEST-----
```

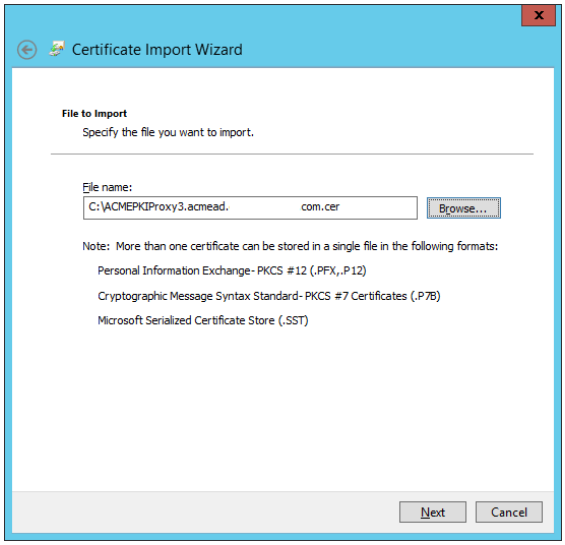

MyCertificatesView
xorble.com/MyC
home
my certificates
my contacts
add ins
organizations
advanced request
help and license
logoff
Xorble
Public Key Infrastructure as a Service (PKIaaS) - Certificates from the Cloud
Advanced Certificate Request
Paste the certificate request as a PKCS#10 Base64 text string.
(Private keys for advanced certificate requests are NOT archived and hence make sure you backup your certificate and private keys)
-----BEGIN NEW CERTIFICATE REQUEST-----
MIID
Kerberos Authentication Certificate Profile
Machine Authentication Certificate Profile
S/MIME Certificate Profile
User Authentication Certificate Profile
User Authentication and Signing (S/MIME) Certificate Profile
User Encryption (S/MIME) Certification Profile
User Internet Of Things Device Authentication Certificate Profile
Web and TLS/SSL Server Authentication Certificate Profile
https://www.xorble.com/MyCerts/CreateCertView?actionverb=create&ecc=false

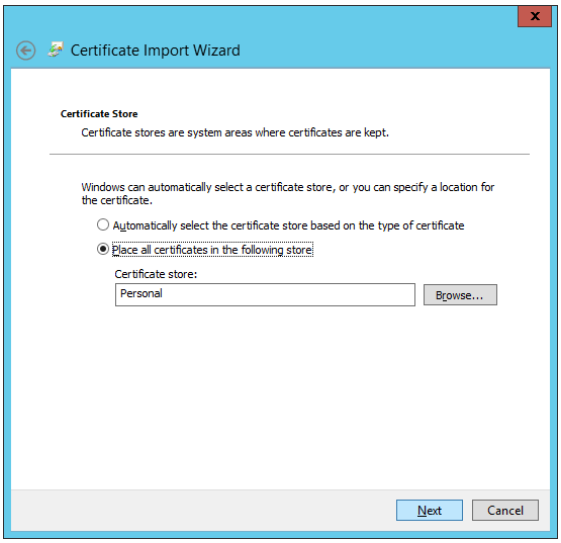

DownloadKeysView
home
my certificates
my contacts
outlook add in
organizations
advanced request
help and license
logoff
CryptograFree
Public Key Infrastructure as a Service (PKIaaS) - Certificates from the Cloud
Download Certificate
Certificate File
Logged on as # david@acmead.
com # © 2016 CryptograFree.com.
Do you want to open or save Certificate.cer (1.78 KB) from
.com?
Open
Save
Save
Save as
Save and open

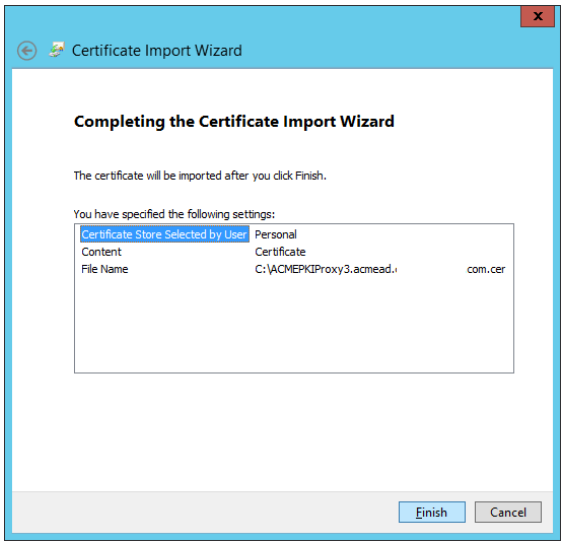

Certs - [Console Root\Certificates (Local Computer)\Personal]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatio
Trusted People
Client Authentication Issuers
Remote Desktop
Smart Card Trusted Roots
Trusted Devices
Web Hosting
Object Type
Certificates
All Tasks
New Window from Here
Refresh
Help
Request New Certificate...
Import...
Advanced Operations
Actions
Personal
More Actions
Certificates
More Actions
Add a certificate to a store


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
Local Machine
To continue, click Next.
Next
Cancel


Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
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

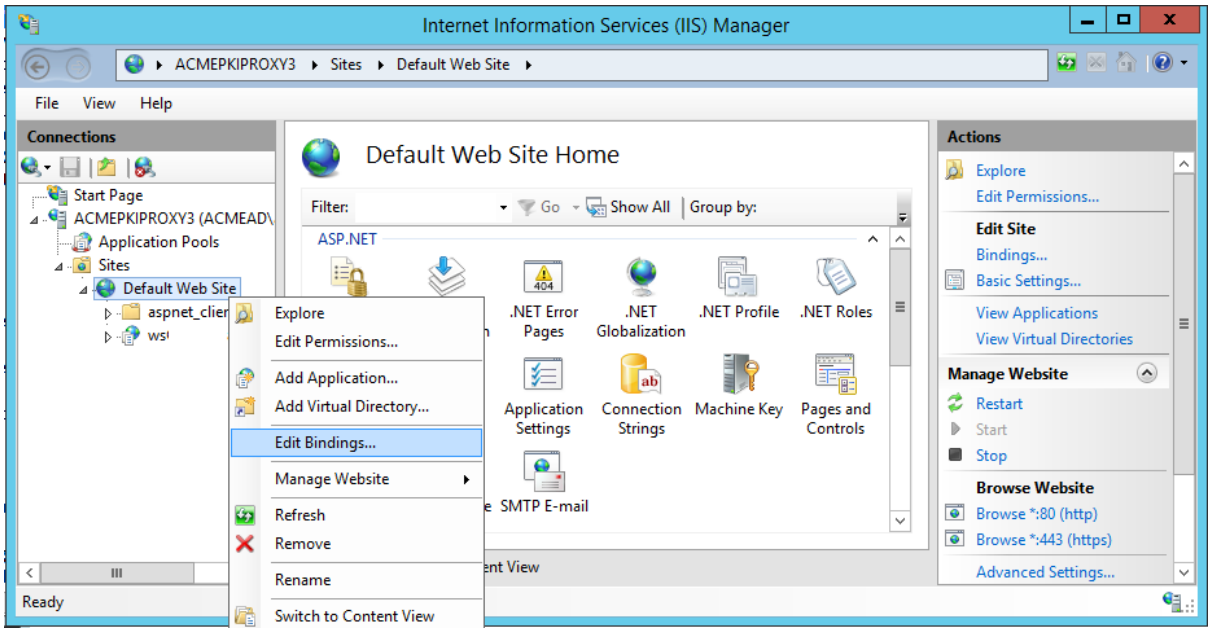

Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
C:\ACMEPKIProxy3.acmead. com.cer
Browse...
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Next
Cancel


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.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Personal
Browse...
Next
Cancel

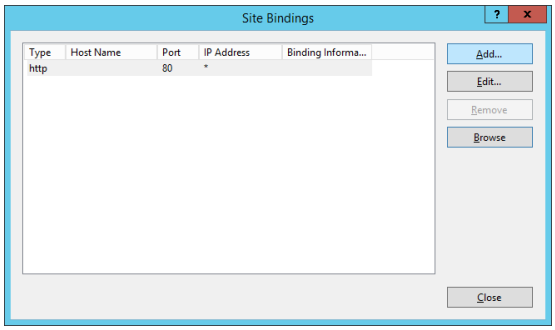

Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User Personal
Content Certificate
File Name C:\ACMEPKIProxy3.acmead. com.cer
Finish
Cancel

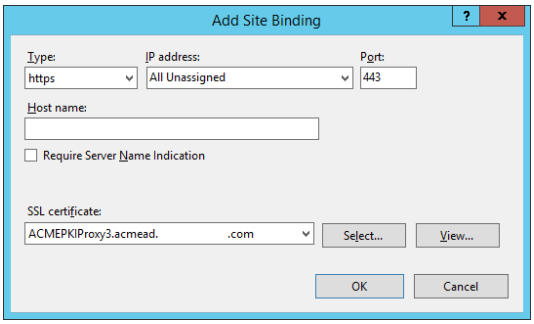
Add HTTPS Binding to IIS

After enrolling for a web server certificate, the web services proxy need also to be configured to use HTTPS. Open the Internet Information Services MMC and select the Default Web Site. Right click and select **Edit Bindings** as below:



Select Add and then select **https** as the type and select the web server certificate as below and **OK**.

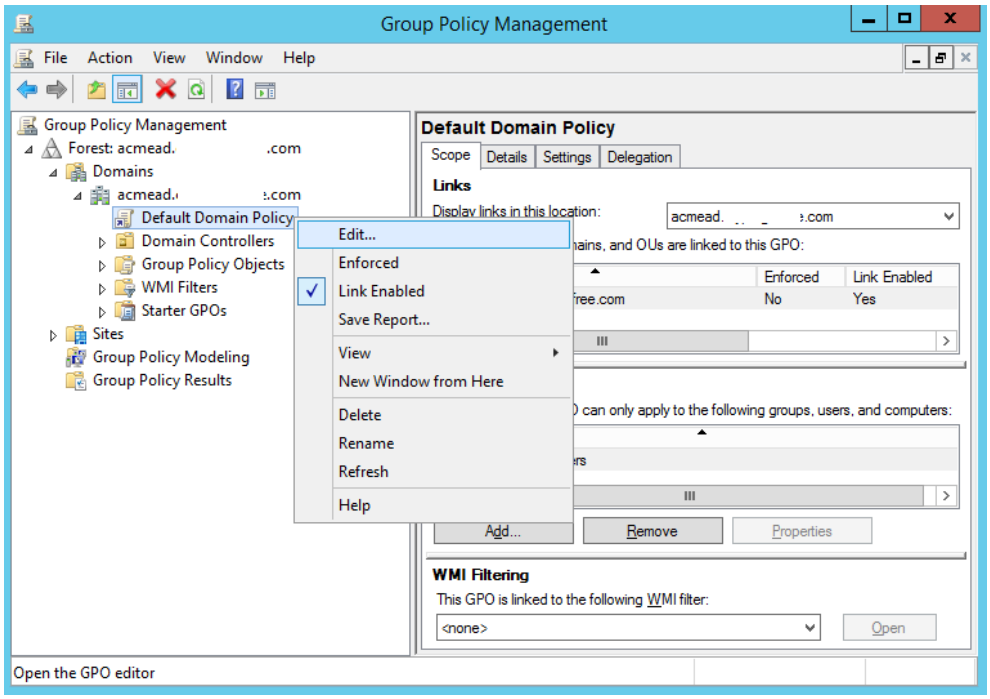




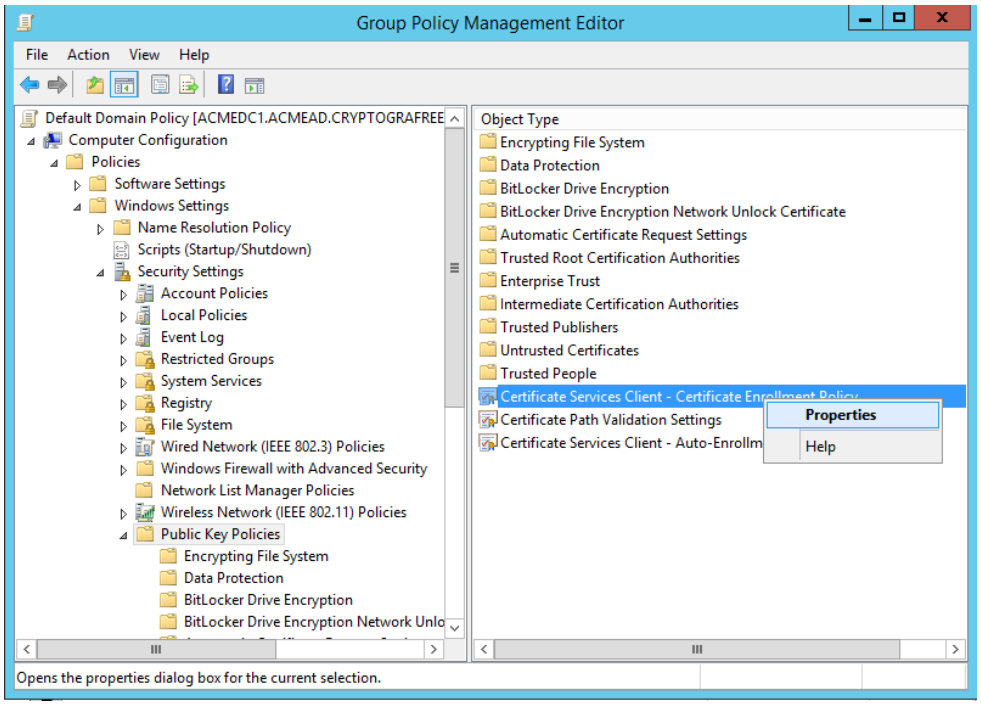
Configuring PKI Web Services Group Policy

On a Domain Controller, start the Group Policy Management MMC.

Select the Default Domain Policy and **Edit** as below.

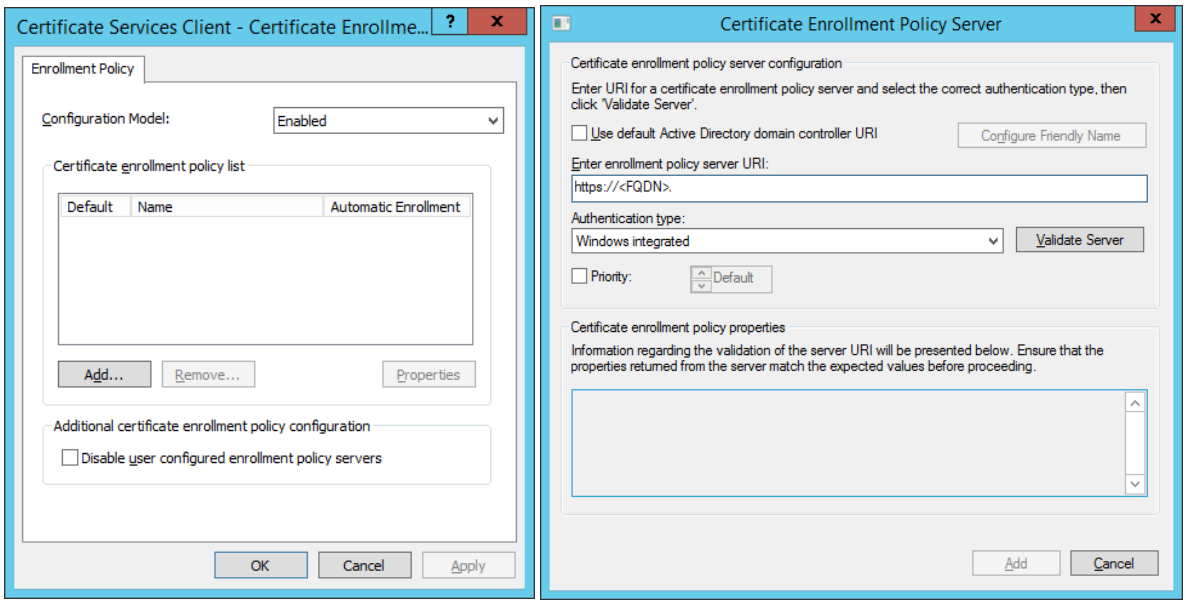


Navigate to the Computer Public Key Policies and select Certificate Enrollment Policy **Properties** as below:

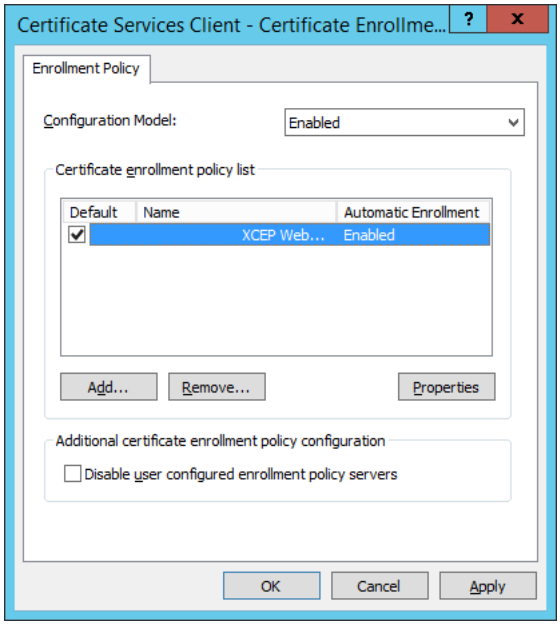


Select Add and then enter the following URL (with the FQDN replaced by the Web Services Proxy Server name and then select **Validate Server**.

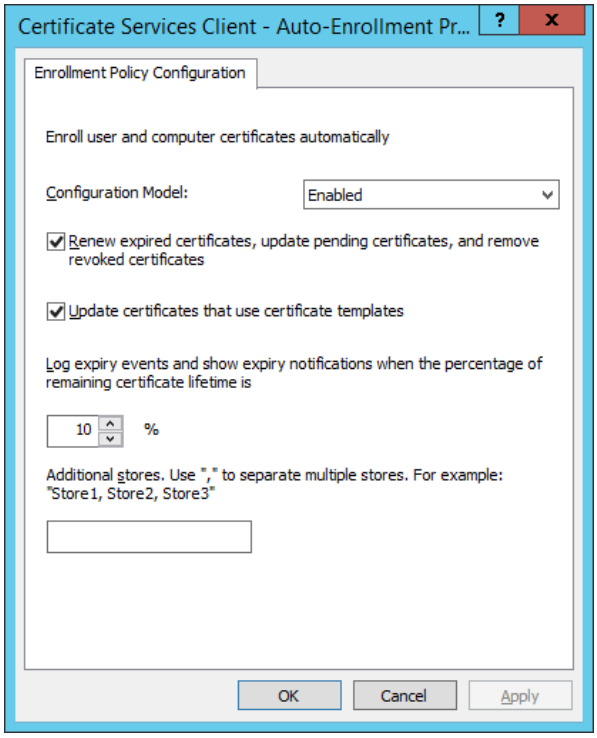
https://<FQDN>/wsXorble/wsXorbleXCEP.svc/XCEP



Select **Add** and then set this as the **Default** and **OK**.



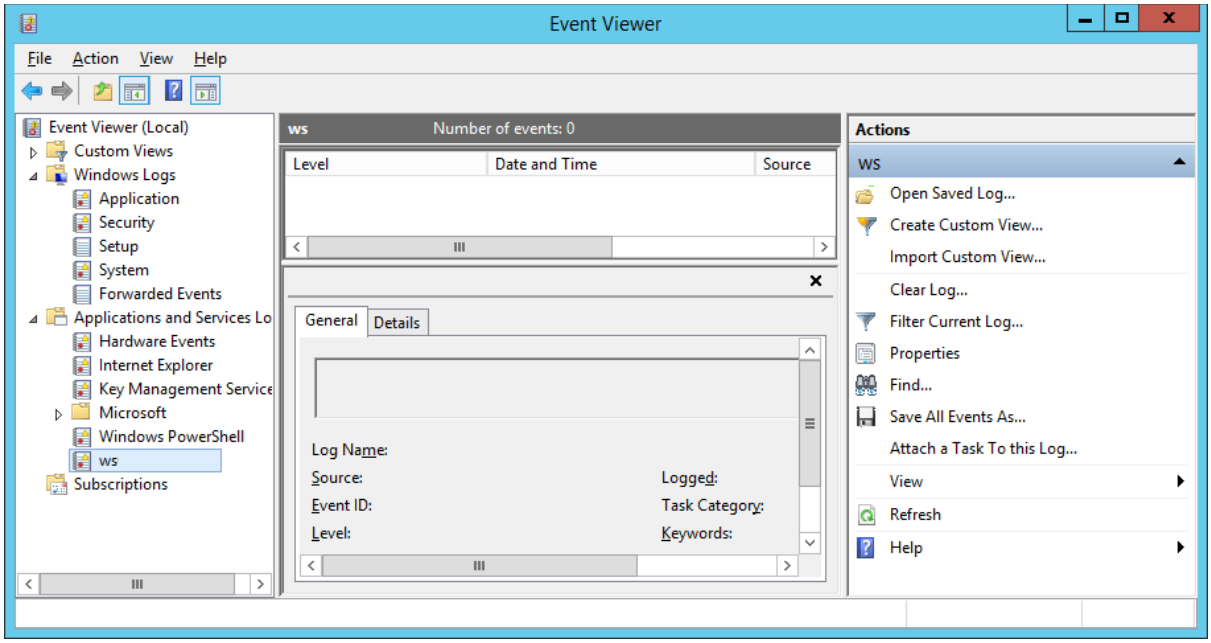
Open the auto enrolment settings and set as follows:



Repeat the above steps but this time set the User group policy.

Testing and Debugging the Web Services Proxy

The web services proxy logs events into an event log called wsXorble. By default, only errors and warning are written to this event log.



The Web Service Proxy log can be configured to log informational massages by adjusting the DebugLevel parameter in the web.config file for the service. Setting this to 4 will enable full logging.

```
<add key="DebugLevel" value="4" />
```