SERVICE SUPPORT AND BUSINESS APPLICATIONS
LOGISTICS APPLICATION SERVICES

How to use SSL/TLS to secure your LOGFAS sites

Last updated: 22-NOV-2018
Applies to: LOGFAS 6.3.1.

Table of contents

Document change log			
Version	Comments	Date	Author
1.0	Initial version	12 FEB 2019	J.Ramon Garcia Viejo
1.1	Support team revision	28 FEB 2019	
1.2	Final revision	28 FEB 2019	Lukasz Pajak

1 References

001 Enter ref. here

1 Purpose

002 How to use SSL/TLS to secure your LOGFAS sites

2 Applicability

003 LOGFAS 6.4.1.and earlier versions up to 6.3.1

3 Overview

3.2 General Overview

004 Using SSL/TLS (to secure your LOGFAS sites) is recomended to protect user's privacy.

005 This document explains how to configure Secure Sockets Layer (SSL) for the Internet information Services (IIS) site hosting ADAMSWEB and/or EVEWEB.

006 The required changes only affect server-platform installations; Client-workstation configurations are not affected when a proper certificate is used on the server.

3.3 Requirements

007 Local administrator permissions/rights at the target LOGFAS server.

008 LOGFAS ADAMSWEB and/or EVEWEB suscessfully deployed to the LOGFAS server.

4 How to set up SSL on IIS

009 If you need to configure SSL on your LOGFAS server, it's important to realize that the implementation of SSL has changed from IIS 6.0 and above.

0010 Depending on the scope and/or usage of ADAMWEB/EVEWEB some of the following steps will be optional. Note that those steps will be explained using the IIS Manager GUI although the same outcome could be achieved through other Microsoft/Windows tools and commands (i.e. AppCmd.exe, WMI scripts, PowerShell.exe, Certmgr.msc, etc.).

0011 The main steps are:

- Step 1 - Get an appropriated PKI certificate.
- Step 2 - Create an HTTPS binding at the IIS site.
- Step 3 - Configure SSL settings for the IIS site.
- Step 4 - Test SSL by making a request to the IIS site.

0012 Optional steps will be:

- Step 5 - Removing PKI certificate(s).
- Etc.

IMPORTANT NOTE

- The certificates deployed with ADAMSWEB and/or EVEWEB should be deleted (applicable to LOGFAS 6.4.1 and earlier versions up to 6.3.1)

4.1 Step 1.0 - Get an appropriated PKI certificate

0013 Depending on the scope and usage of ADAMWEB/EVEWEB the PKI certificate could be Self-Signed or issued by the Certification Authority (CA) of the Active Directory (AD) Domain.

0014

0015 In both cases the aim will be to obtain a Personal Information Exchange format certificate (PFX) protected with a password-based symmetric key. PFX is a predecessor to PKCS#12; It defines a file format that can be used for secure storage of certificates, containing both private and public keys, plus all of the certificates in a certification path.

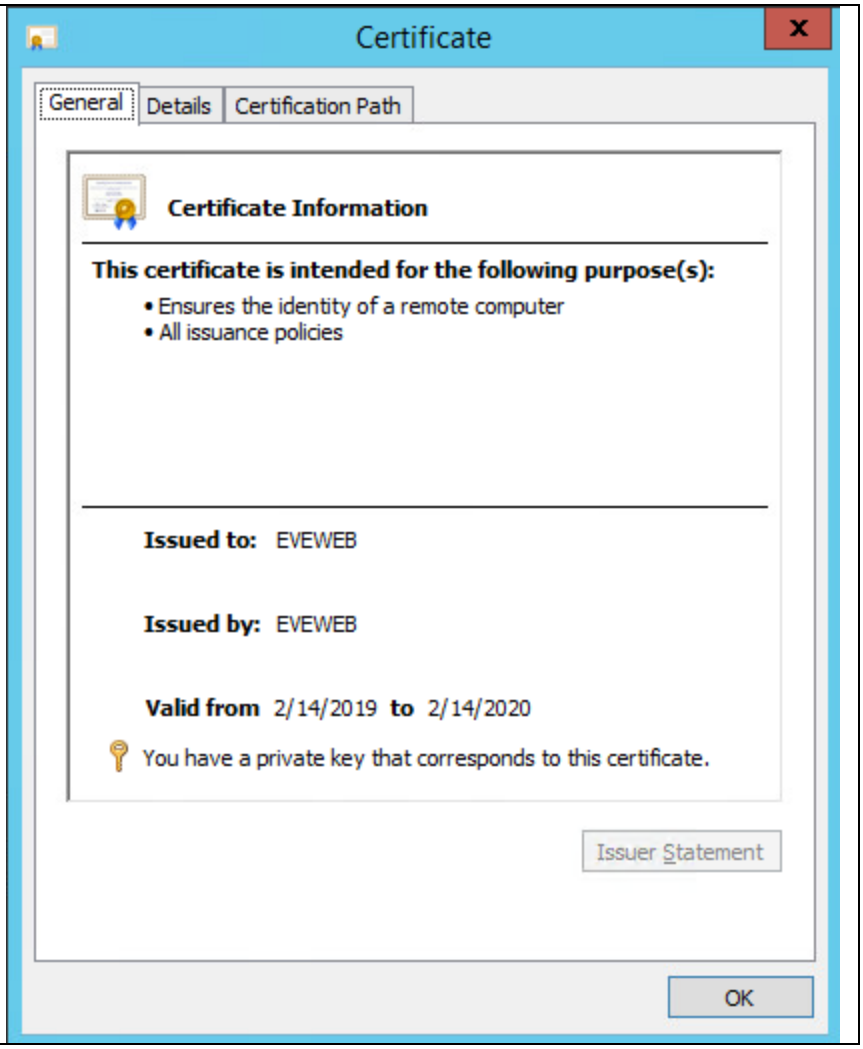
0016

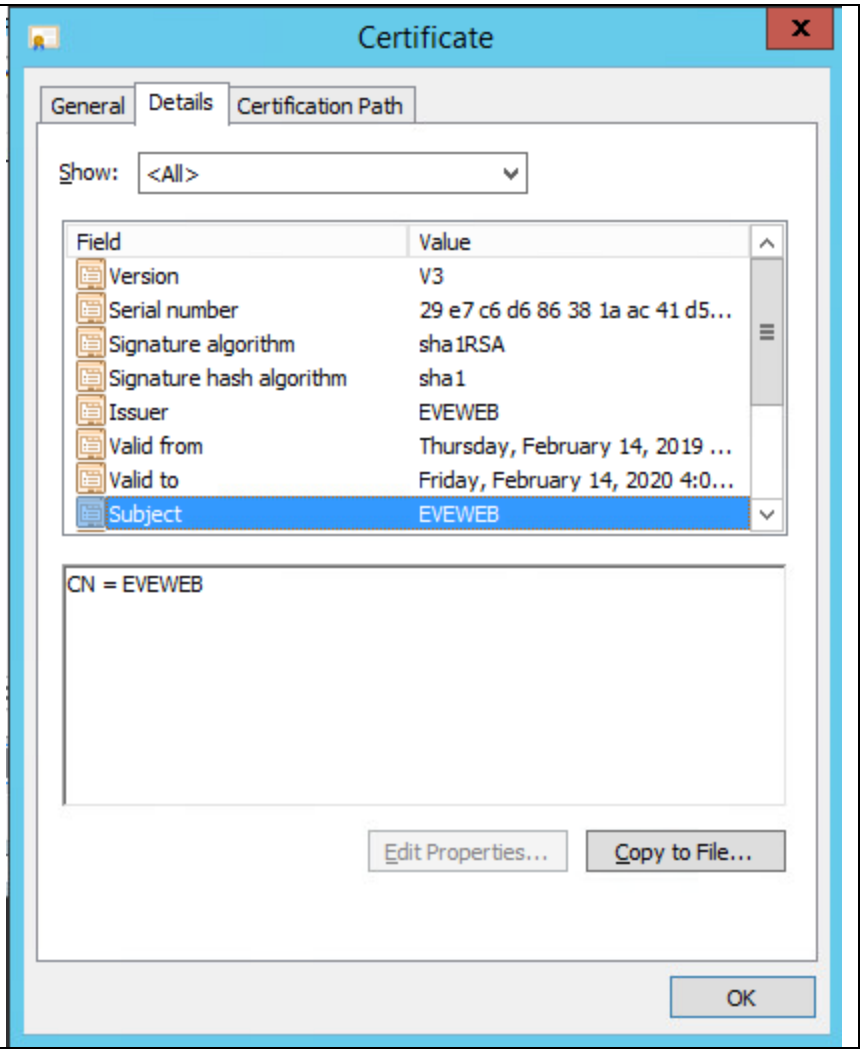
0017 When choosing a certificate, consider the following: Do you want end users to be able to verify your server's identity with your certificate? If yes, then either create a certificate request and send that request to a known certificate authority (CA) such as VeriSign or GeoTrust, or obtain a certificate from an online CA in your intranet domain. There are three things that a browser usually verifies in a server certificate:

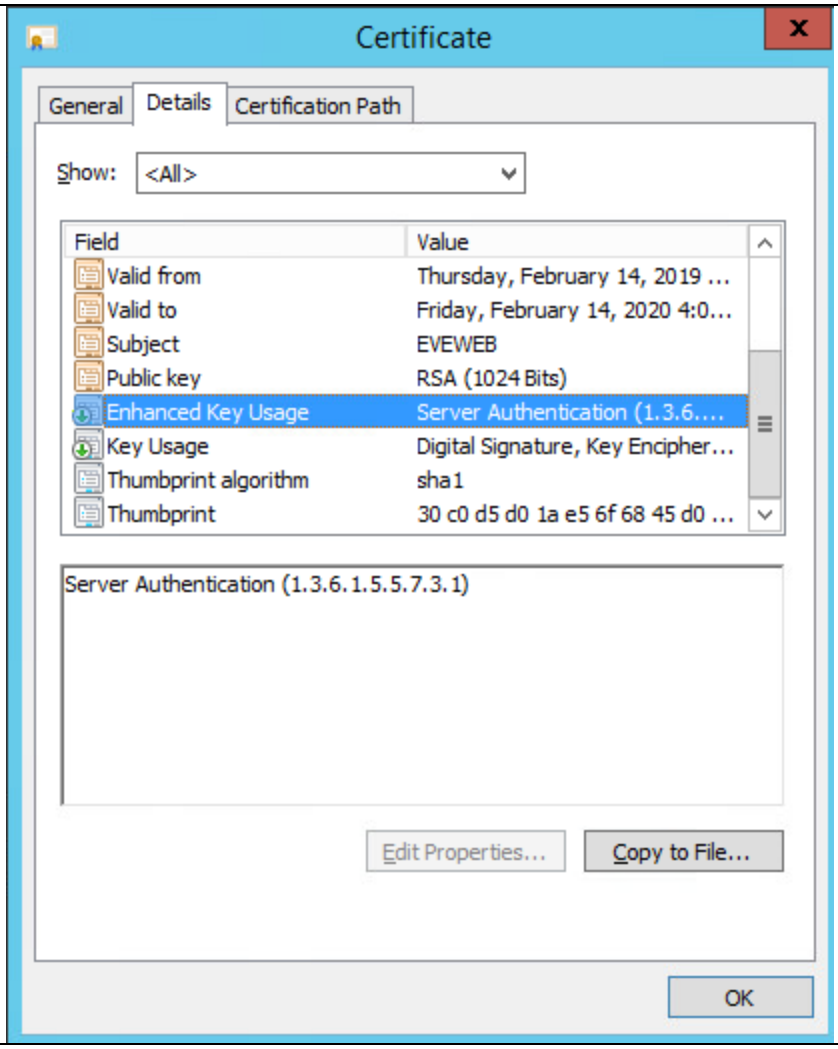
- That the current date and time is within the "Valid from" and "Valid to" date range on the certificate.
- That the certificate's "Common Name" (CN) matches the host header in the request. For example, if the client is making a request to https://www.contoso.com/, then the CN must be www.contoso.com.
- That the issuer of the certificate is a known and trusted CA.

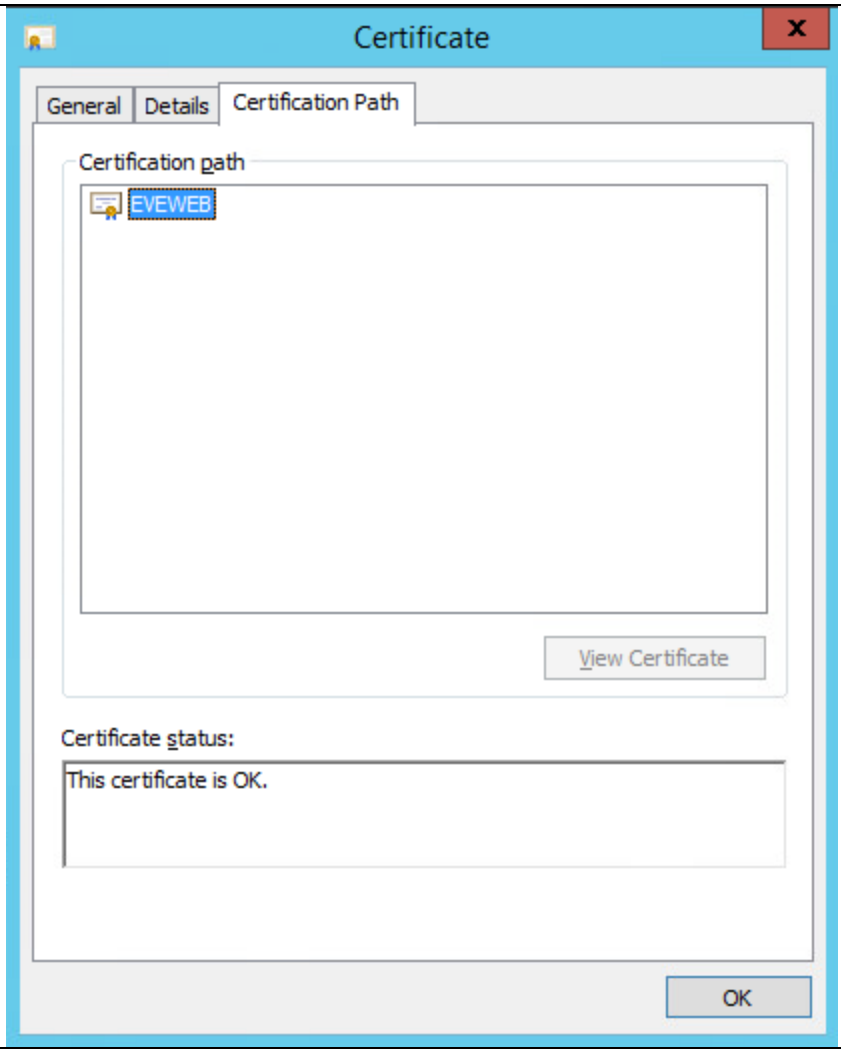
0018 If one or more of these checks fails, the browser prompts the user with warnings. If you have an Internet site or an intranet site where your end users are not people you know personally, then you should always ensure that these three parameters are valid.

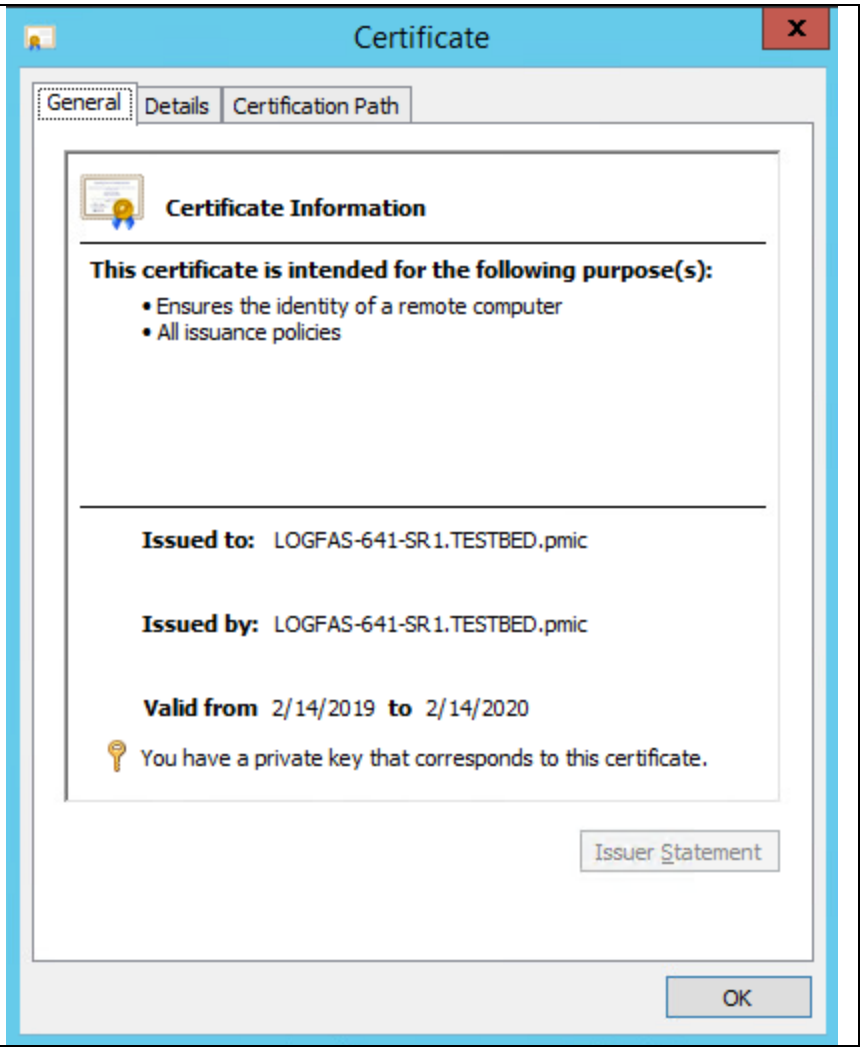
0019 Self-signed certificates are certificates created on your computer. They're useful in environments where it's not important for an end user to trust your server, such as a test environment.

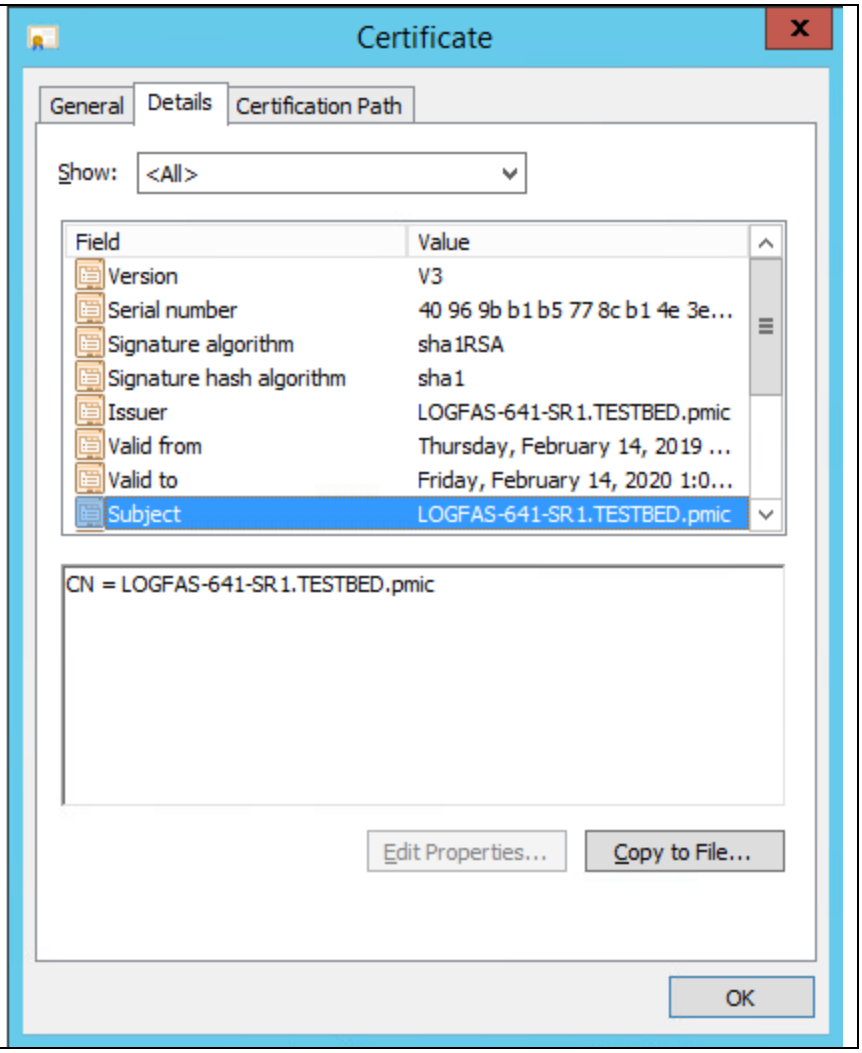
Example of Self-Signed certificate deployed upon installation of EVEWEB.	

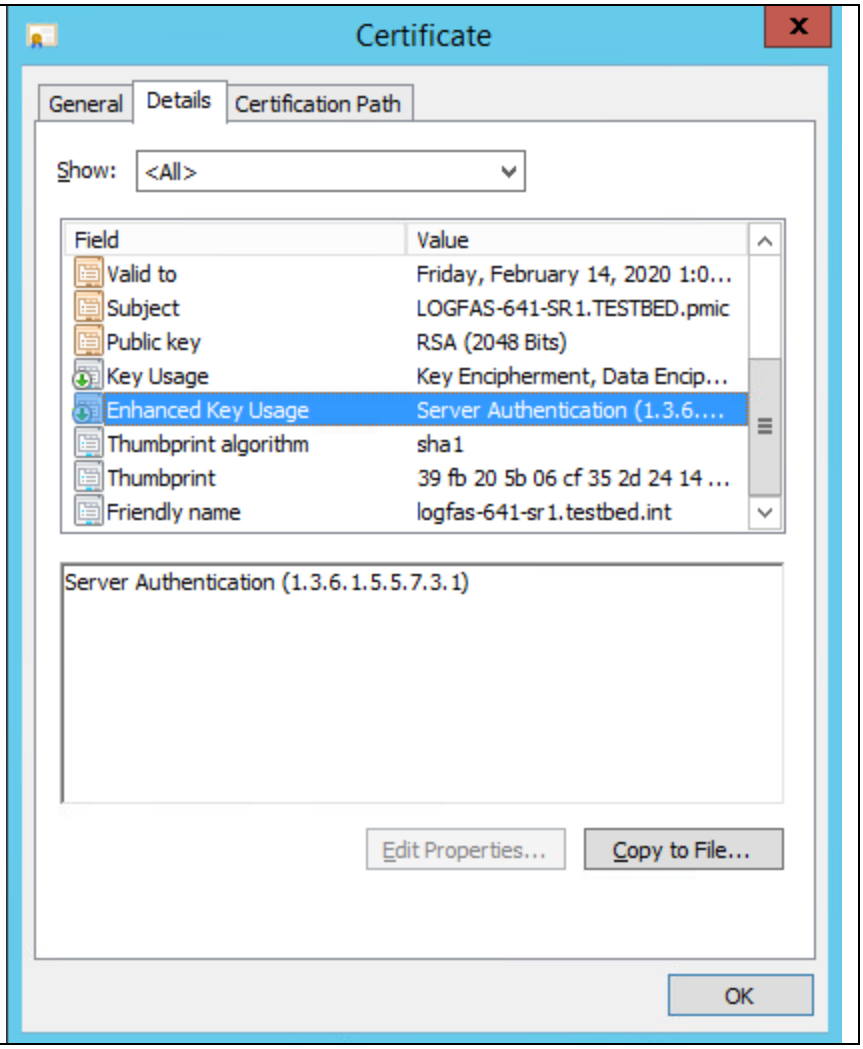

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
29 e7 c6 d6 86 38 1a ac 41 d5...
Signature algorithm
sha1RSA
Signature hash algorithm
sha1
Issuer
EVEWEB
Valid from
Thursday, February 14, 2019 ...
Valid to
Friday, February 14, 2020 4:0...
Subject
EVEWEB
CN = EVEWEB
Edit Properties...
Copy to File...
OK

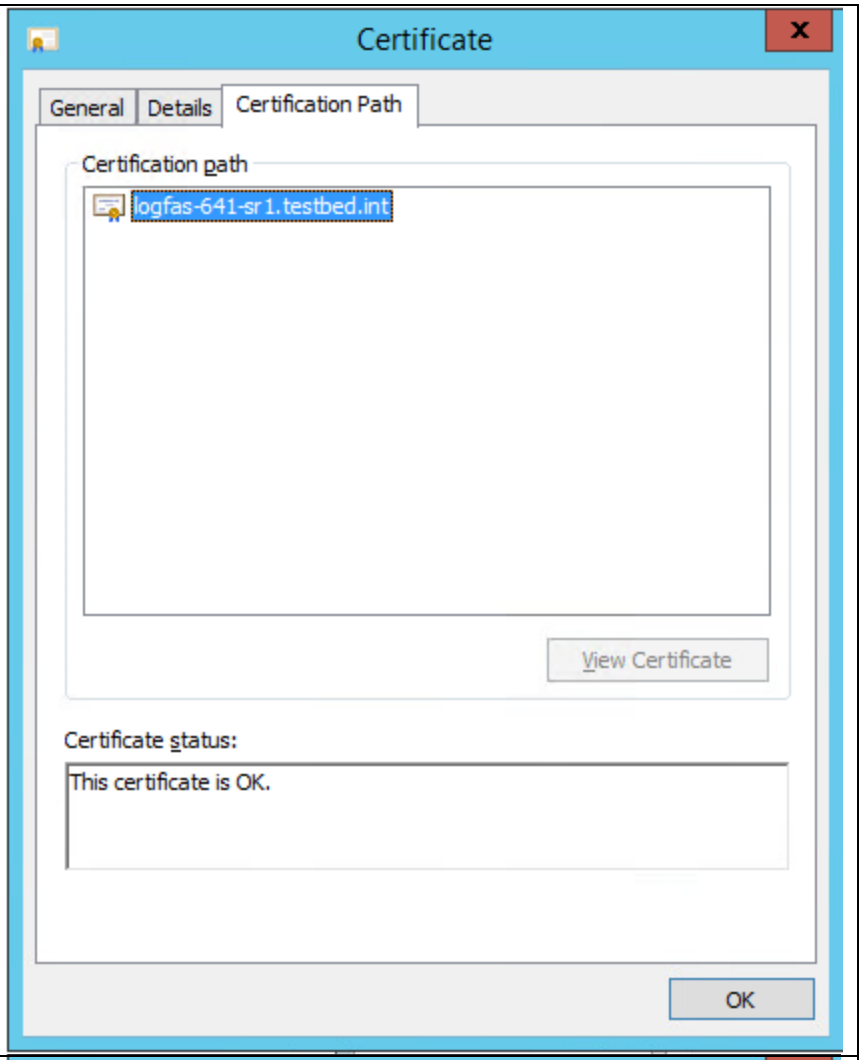

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Valid from
Thursday, February 14, 2019 ...
Valid to
Friday, February 14, 2020 4:0...
Subject
EVEWEB
Public key
RSA (1024 Bits)
Enhanced Key Usage
Server Authentication (1.3.6....
Key Usage
Digital Signature, Key Encipher...
Thumbprint algorithm
sha1
Thumbprint
30 c0 d5 d0 1a e5 6f 68 45 d0 ...
Server Authentication (1.3.6.1.5.5.7.3.1)
Edit Properties...
Copy to File...
OK

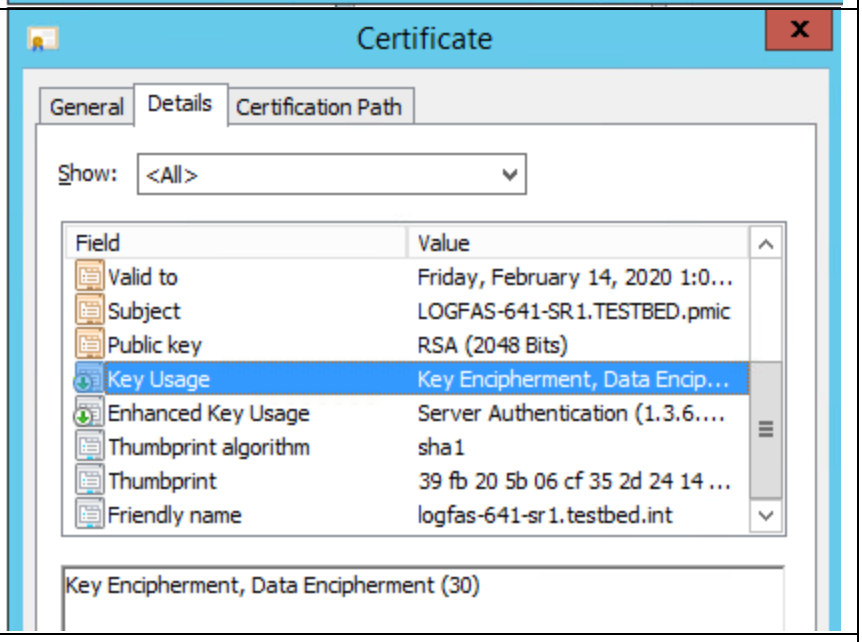

Certificate
General
Details
Certification Path
Certification path
EVEWEB
View Certificate
Certificate status:
This certificate is OK.
OK

Example of IIS self-signed certificate	


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
40 96 9b b1 b5 77 8c b1 4e 3e...
Signature algorithm
sha1RSA
Signature hash algorithm
sha1
Issuer
LOGFAS-641-SR1.TESTBED.pmic
Valid from
Thursday, February 14, 2019 ...
Valid to
Friday, February 14, 2020 1:0...
Subject
LOGFAS-641-SR1.TESTBED.pmic
CN = LOGFAS-641-SR1.TESTBED.pmic
Edit Properties...
Copy to File...
OK


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Valid to
Friday, February 14, 2020 1:0...
Subject
LOGFAS-641-SR1.TESTBED.pmic
Public key
RSA (2048 Bits)
Key Usage
Key Encipherment, Data Encip...
Enhanced Key Usage
Server Authentication (1.3.6....
Thumbprint algorithm
sha1
Thumbprint
39 fb 20 5b 06 cf 35 2d 24 14 ...
Friendly name
logfas-641-sr1.testbed.int
Server Authentication (1.3.6.1.5.5.7.3.1)
Edit Properties...
Copy to File...
OK


Certificate
General
Details
Certification Path
Certification path
logfas-641-sr1.testbed.int
View Certificate
Certificate status:
This certificate is OK.
OK


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Valid to
Friday, February 14, 2020 1:0...
Subject
LOGFAS-641-SR1.TESTBED.pmic
Public key
RSA (2048 Bits)
Key Usage
Key Encipherment, Data Encip...
Enhanced Key Usage
Server Authentication (1.3.6....
Thumbprint algorithm
sha1
Thumbprint
39 fb 20 5b 06 cf 35 2d 24 14 ...
Friendly name
logfas-641-sr1.testbed.int
Key Encipherment, Data Encipherment (30)

0020

0021 The following matrix display one example of usage;

Table 1 - LOGFAS Installation Summary

Procedure Step Description	Demo	Production
1. **Removing a previous version of LOGFAS**. If a previous version of LOGFAS is installed, you will need to remove it. Follow the section "*Uninstalling LOGFAS (Client & Server)*".[1] If this is a clean installation then proceed to the following step below.	✓	✓
2. **Preparing LOGFAS Server for the Domain**. Have your Domain Administrator create a service account for the POSTGRESQL service and issue the SETSPN commands as explained in "*Preparing LOGFAS Server for the Domain with SETSPN*" section.	x	✓
3. **Creating SSL Certificates for LOGFAS Server**. If you don't have valid SSL certificate(s) for you server you must install OpenSSL and generate them. The procedures can be found below in "*Installing OpenSSL & Creating Certificates*" section.	x	✓
4. **LOGFAS Client and Server Software Installation**. Install the LOGFAS software as explained in "*LOGFAS Software Installation Procedures*" section.	✓	✓
5. **LOGFAS Server Post-Installation Configuration**. To configure the database Service, database, PGADMIN and SSPI, follow the steps described in "*LOGFAS Server Post-Installation Procedures*" section.	x	✓

4.1.1 Step 1.1 - Get an appropriated PKI certificate from Certification Authority (CA)

0022 Note that NATO/National policies and proceses related to the management of PKI certificates could be stablished/enforced on your environment. The following CA steps are just an example for informational purposes.

0023

0024 Requesting a certificate from the CA using the Web browser.

0025

0026 Who is my CA? How to find the Certificate Authority enabled for the Active Directory environment.

0027

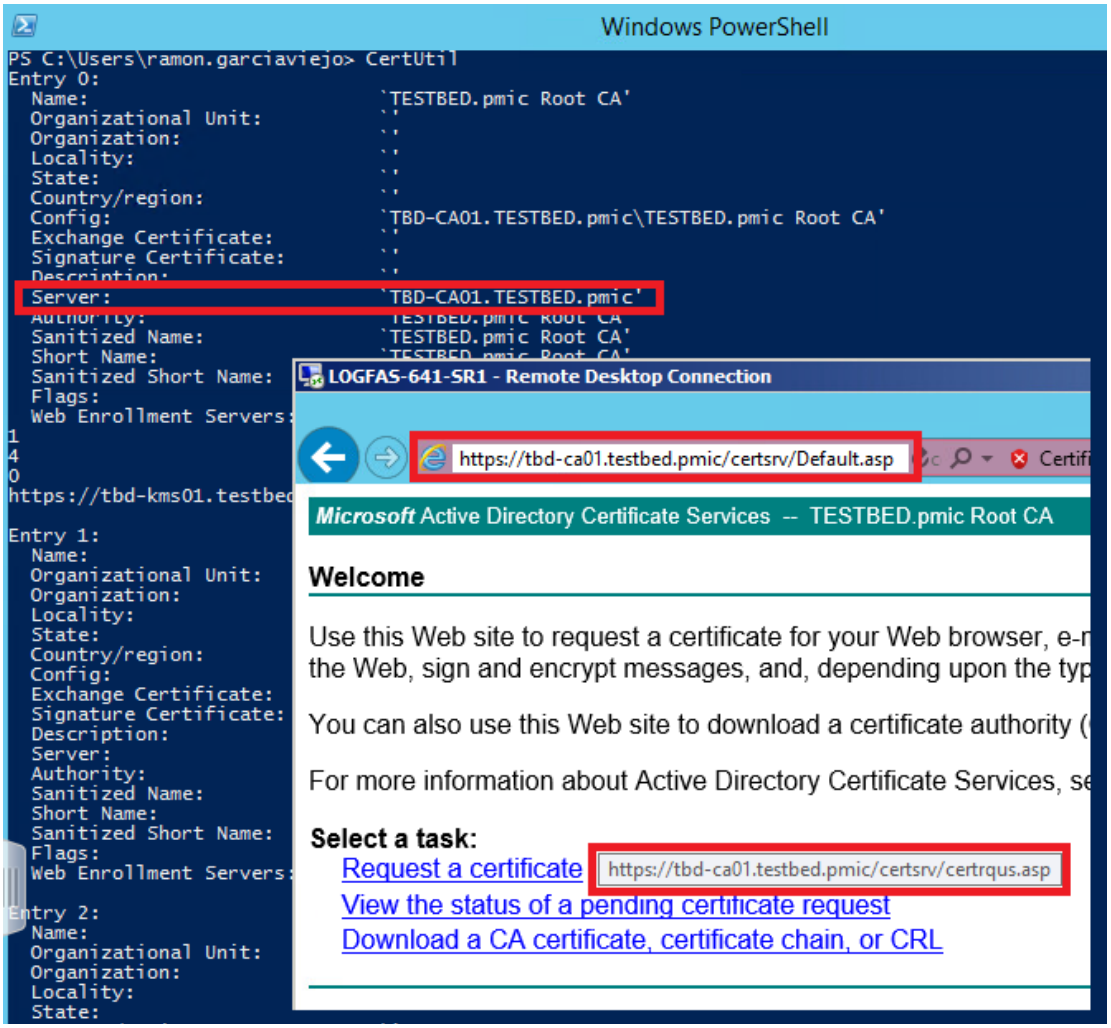
0028 At the target LOGFAS server: Use the CertUtil utility from a cmd or PowerShell command prompt to determine the CA information and the server(s) hosting the service.

```
PS C:\Windows\System32> CertUtil
```

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certutil#BKMK_CAInfo

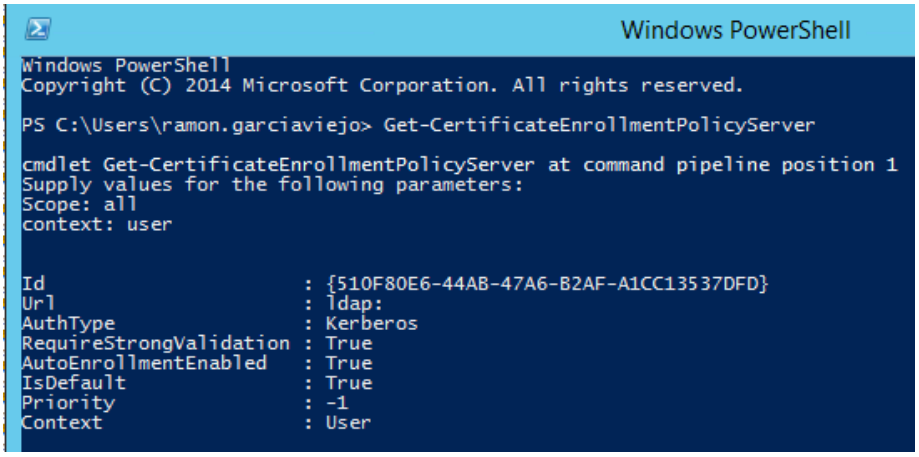
[1] This is only applicable to releases of 6.3.1 or later. Prior releases must first follow migration procedures outlined in the 6.3.1 installation package.

0029 If the CA has enabled the Web enrollment, It should be possible to request/download a certificate using the Web browser. The CA URL should be: **https://<fully qualified Domain name>/certsrv**



0030 Below PowerShell command should display the CA policy server information. The Id value should match with the one displayed –later on- during the certificate enrollment.

```
PS C:\Windows\System32> Get-CertificateEnrollmentPolicyServer
```



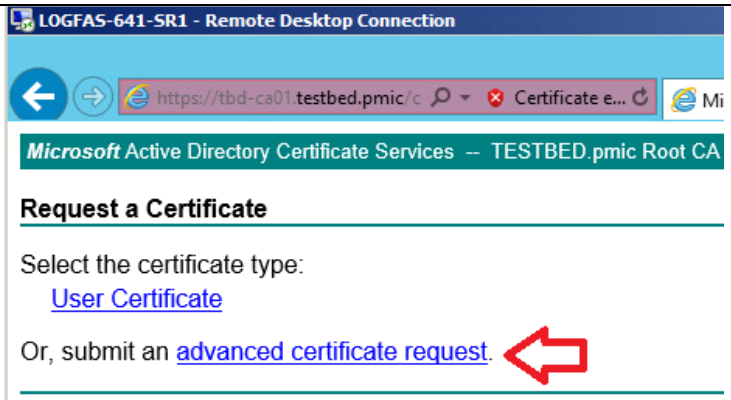
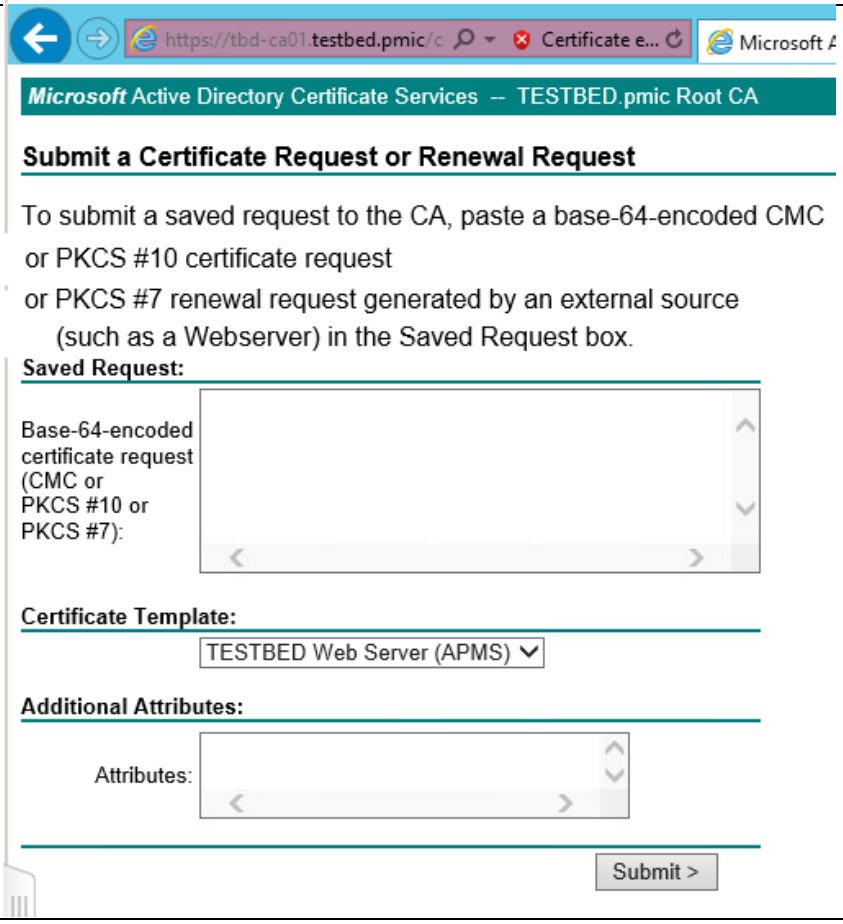
https://docs.microsoft.com/en-us/powershell/module/pkiclient/get-certificateenrollmentpolicyserver?view=win10-ps

0031 Log on to the LOGFAS server where you want to install a certificate.

0032 Start Internet Explorer, and then connect to the computer hosting Certificate Services (for example, https://<servername>/certsrv).

IMPORTANT NOTE

- Note the use of https (TCP port 443) and not http.

0033 On the Microsoft Certificate Services Welcome page, click Request a certificate. 0034 On the Request a Certificate page, click "Or, submit an advanced certificate request"	
0035 Depending on the CA settings you could have access to the full functionallity. In the following example we have limited rights and it is only allowed to paste the contents of a previously generated certificate request.	

0036 On the Advanced Certificate Request page, click Create and submit a request to this CA.

0037 On the Advanced Certificate Request page, do the following:

0038 Under Identifying Information, in the Name field, enter a unique name, for example, the fully qualified domain name (FQDN) of the computer you are requesting the certificate for. For the remaining fields, enter the applicable information.

Note

Event ID 20052 of type Error is generated if the FQDN entered into the Name field does not match the computer's name.

4.1.2 Requesting a certificate from the CA using the Certificate Management tool.

IMPORTANT NOTE

- On Windows 2012R1/Win8 and/or later Operating Systems: You can use **certlm.msc** (Certificates Local Machine) to open the computer certificate store. Note that certmgr.msc (Certificates User) will open the user certificate store. Otherwise use mmc.exe to access to the Local machine certificate store.

```
C:\Windows\System32> certlm.msc
```

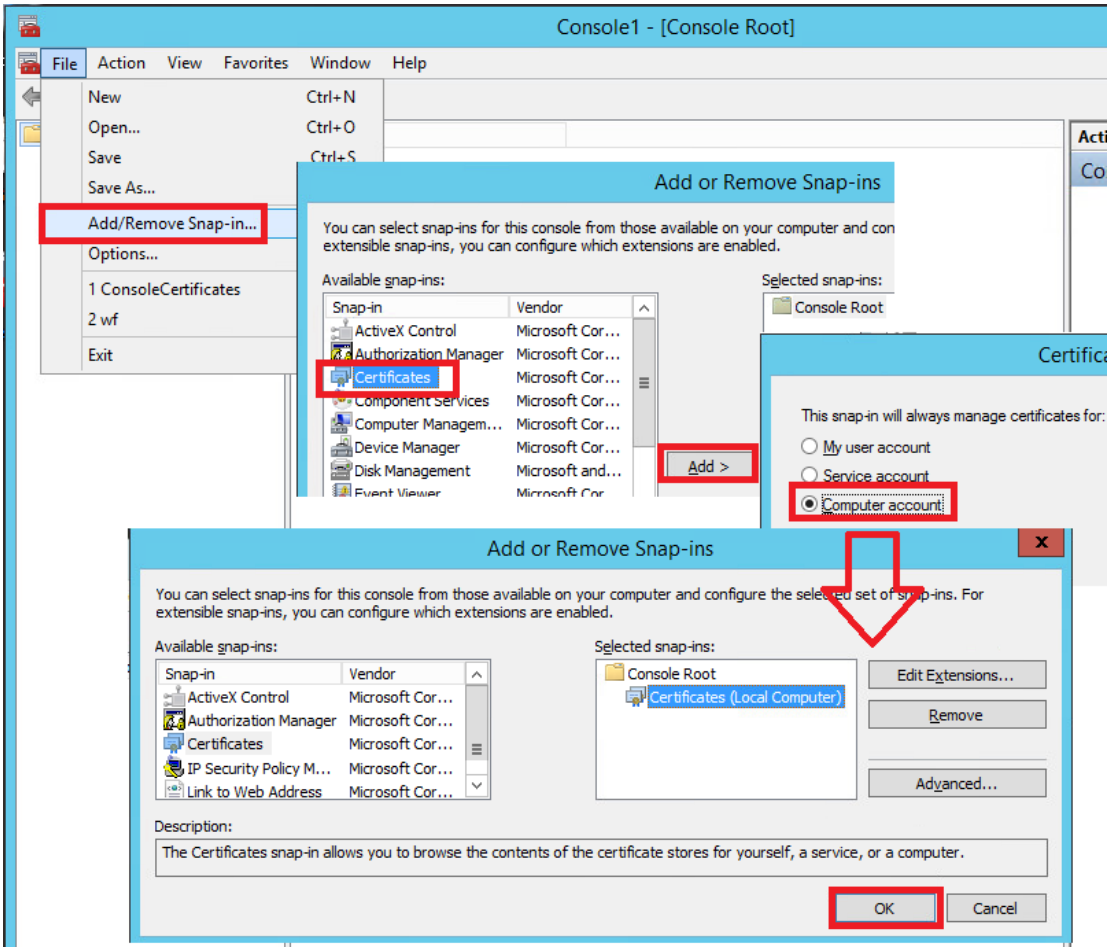
0039 start / mmc.exe / File / Add-Remove Snap-in…/ Certificates / Add

IMPORTANT NOTE

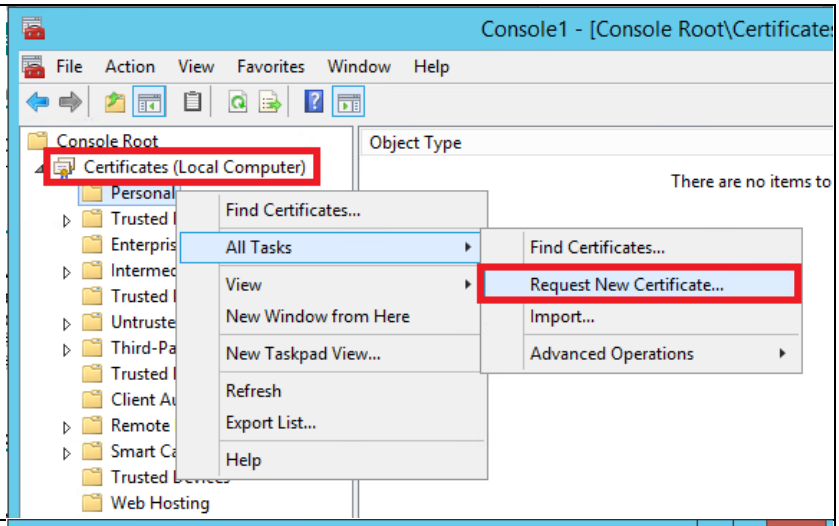
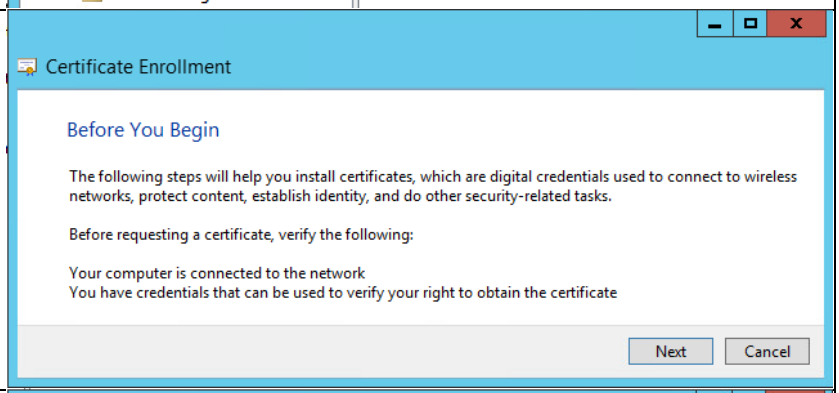
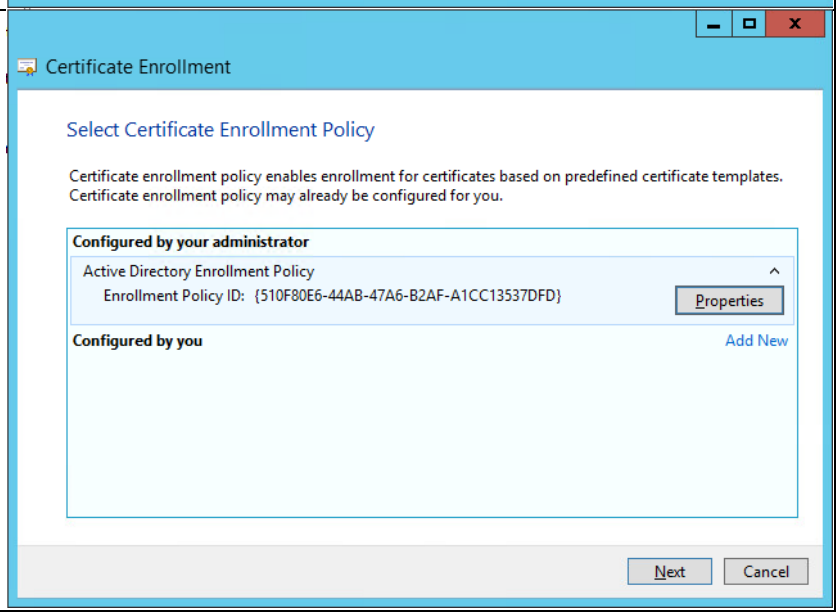
User must have granted permissions as a "local administrator" to manage the certificates of the local computer (all computer's users affected)

0040 mmc console -> certificates >request a new certificate…

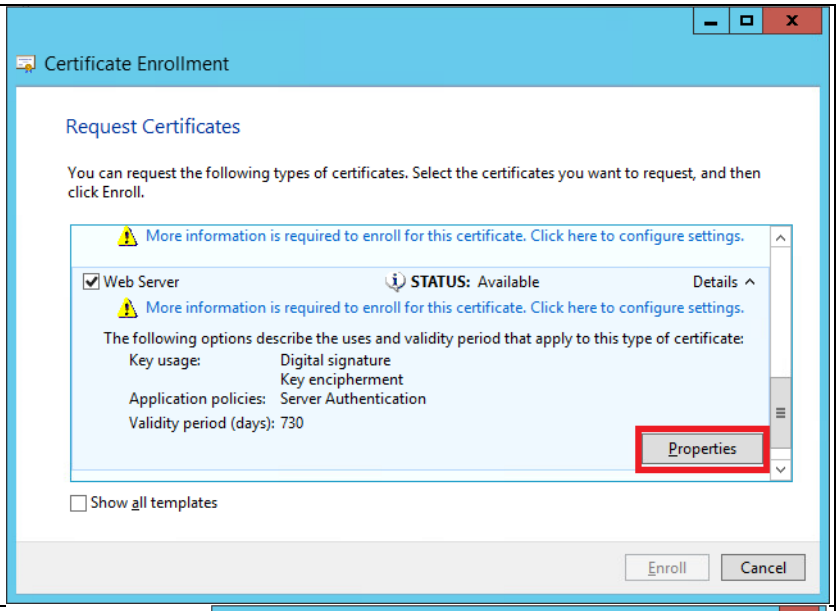
0041



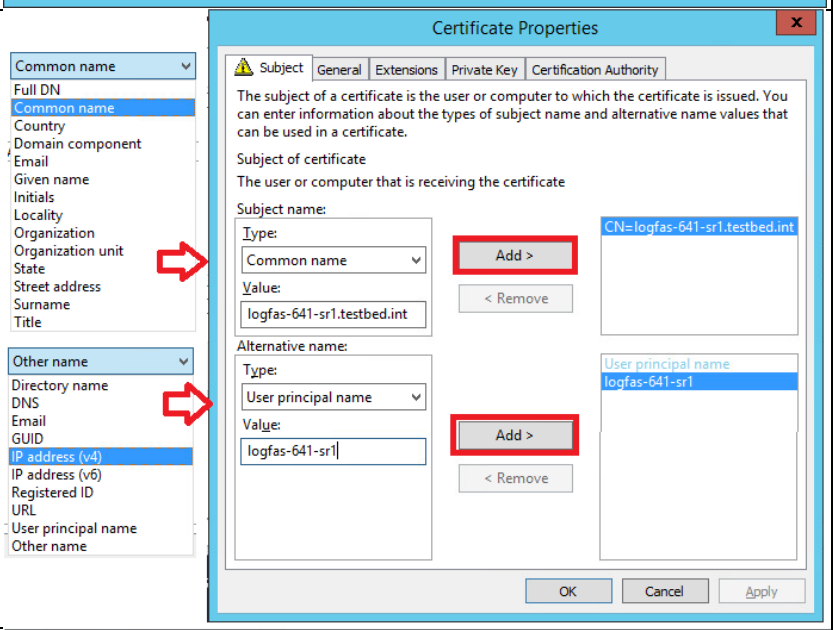
0042 The following steps are just one example about how to request a certificate from your CA.

0043 At the local computer certificates: request a new certificate.	
0044 Click “Next” to continue.	
0045 Optional: Click “Properties” to get more details.	

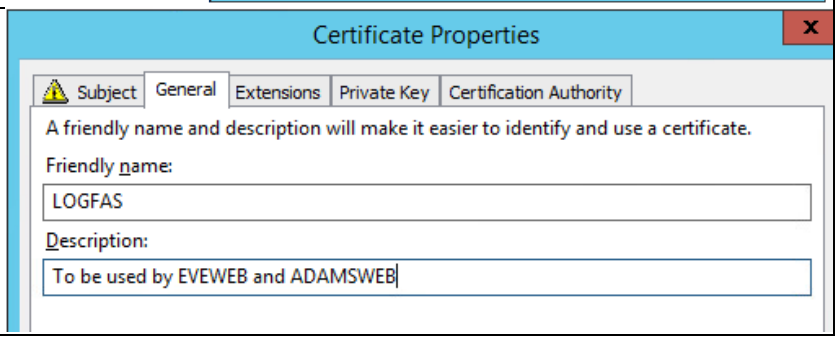
0046 Once selected the certificates' template Click "Properties" to fill in required values.

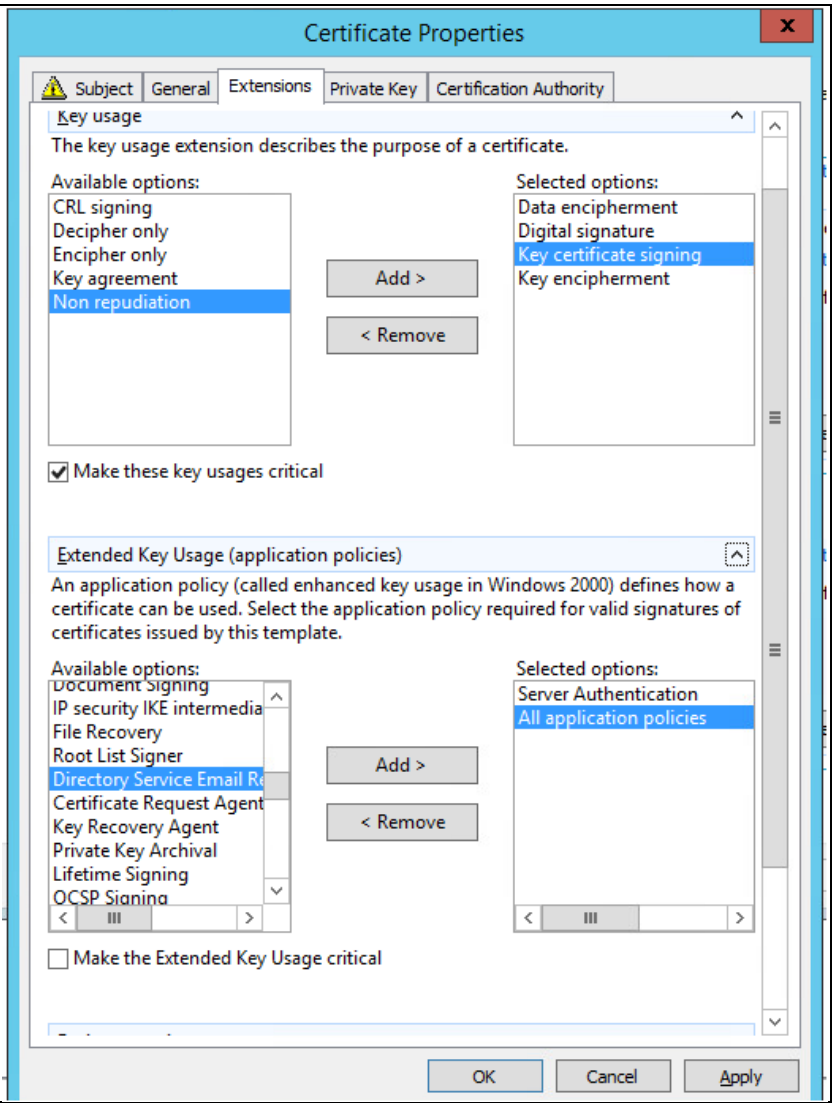


0047 Give a Subject name and optionally an alternative name (e.g. adding localhost will not raise certificate' errors when browsing https:\\localhost\)

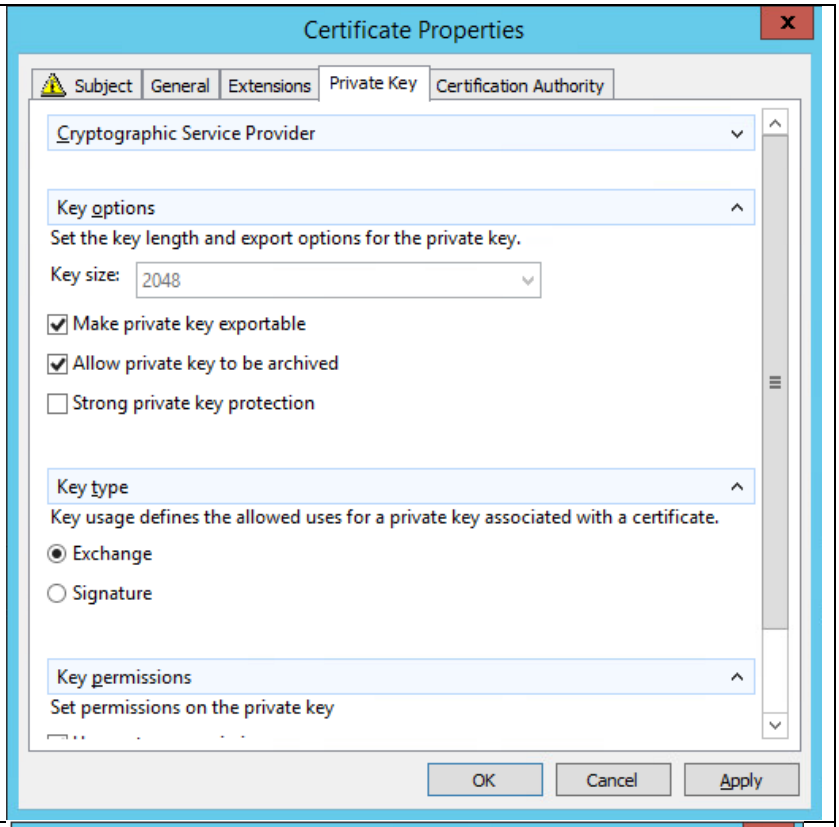


0048 A friendly name helps to identify the certificate.



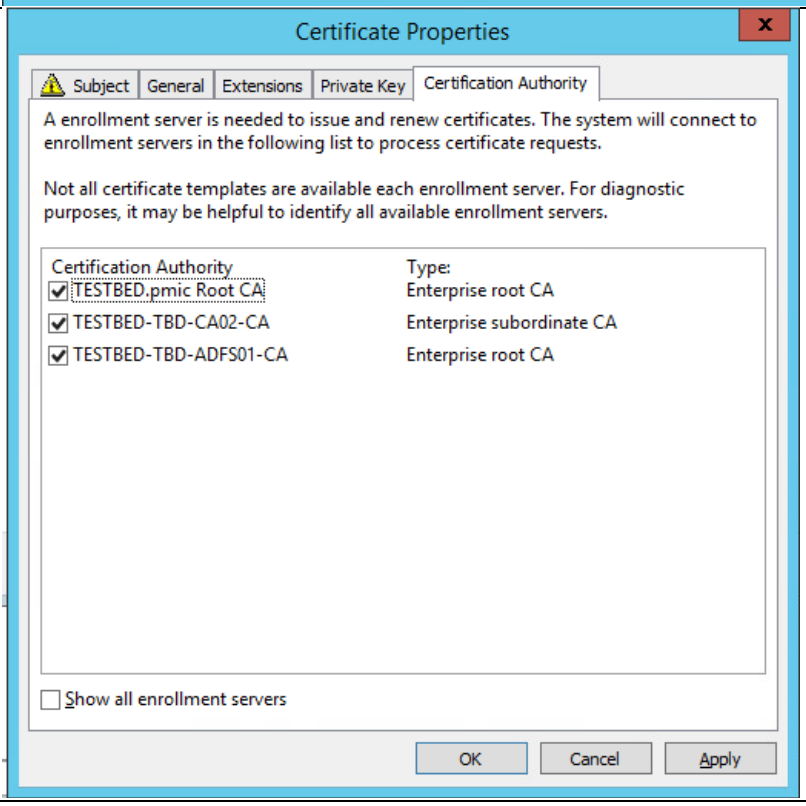
0049 Add any required extensions.	

0050 Set the restrictions for the private key.



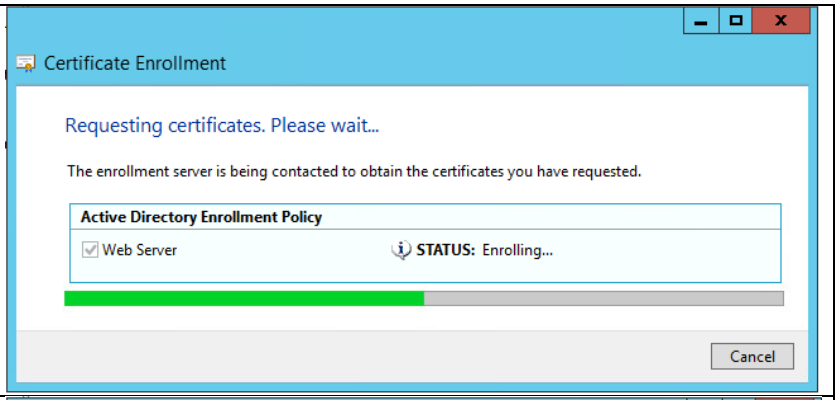
0051 The CAs for enrolment will be listed and at least one of then must be selected.

0052 Click “Apply”.



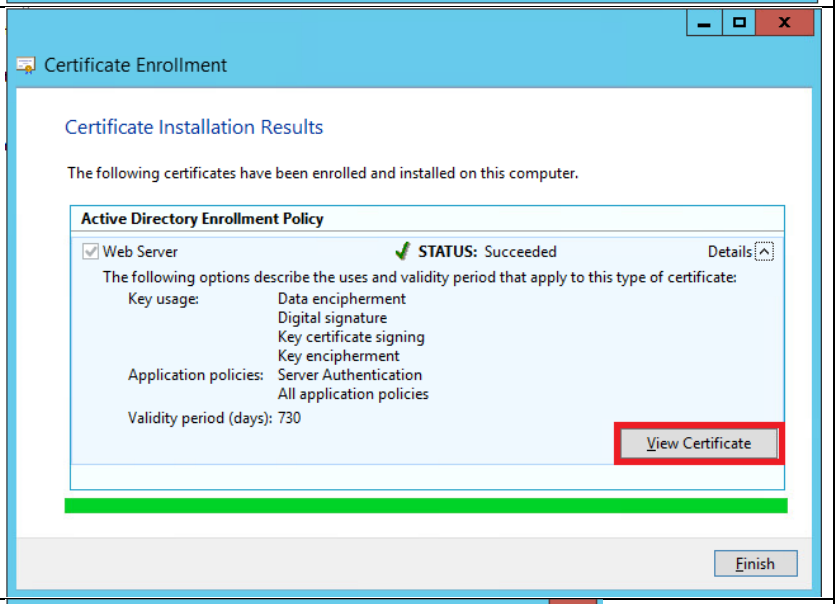
0053 The enrolment process starts to contact the CA.

0054 Depending on the CA settings the request could be waiting for manual intervention (authorization process) or it will be processed in case that automatic enrrollment is available.



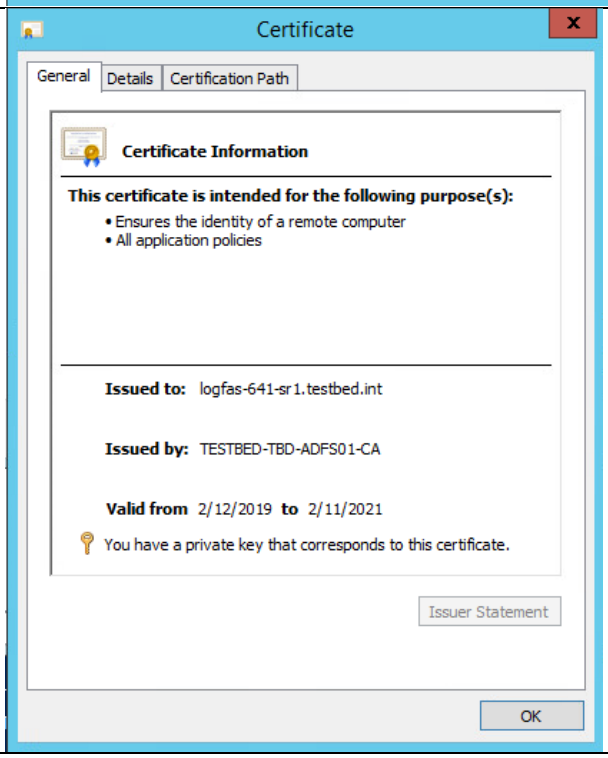
0055 Once the request was processed and authorized a certificate will be issued.

0056 Optionally: Click on "View Certificate" to check its properties and export it to a file.pfx



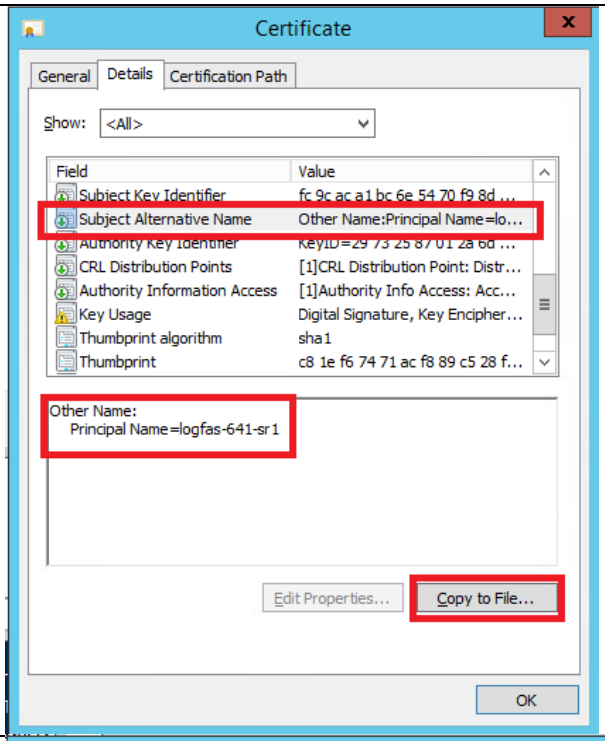
0057 The picture shows how a certificate should look like when Clicking on the buttom "View certificate"

0058 It is important to notice the existence of a private key

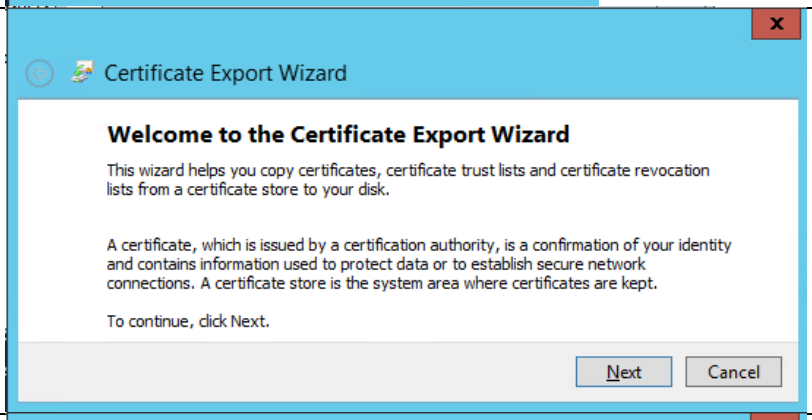


0059 Review other values

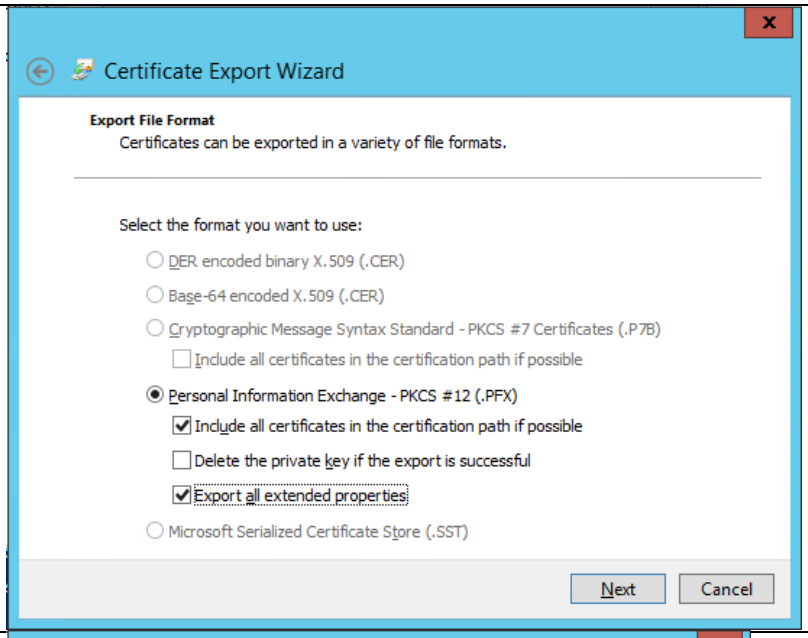
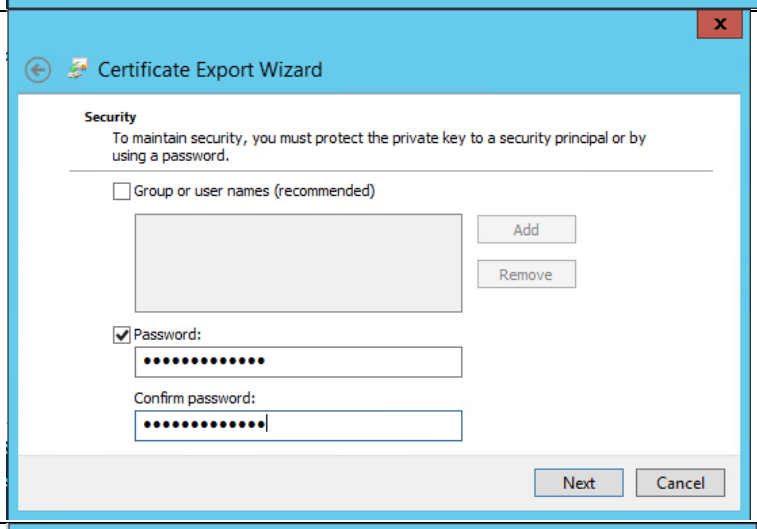
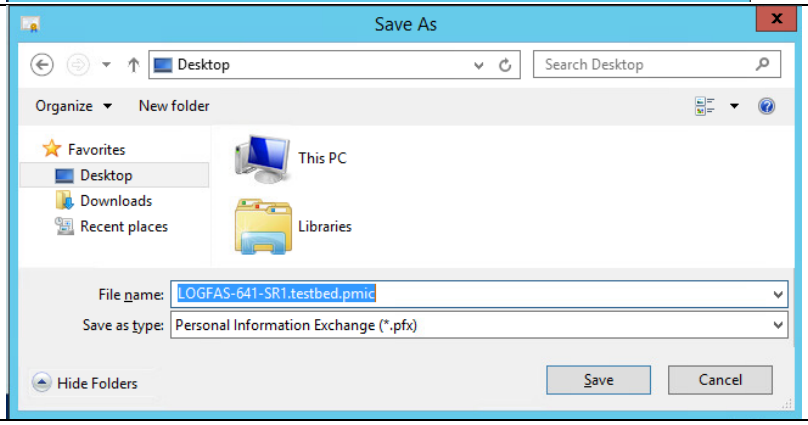
0060 Clicking “Copy to File” allows to export the certificate to a .pfx file. The export could be done later on using the Certificate Manager.

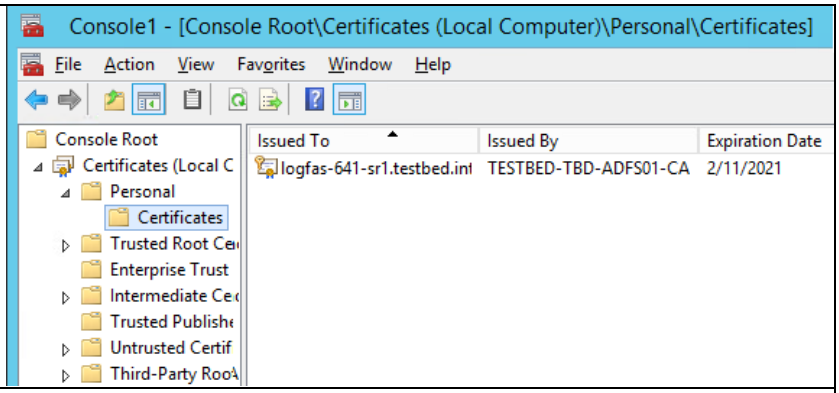
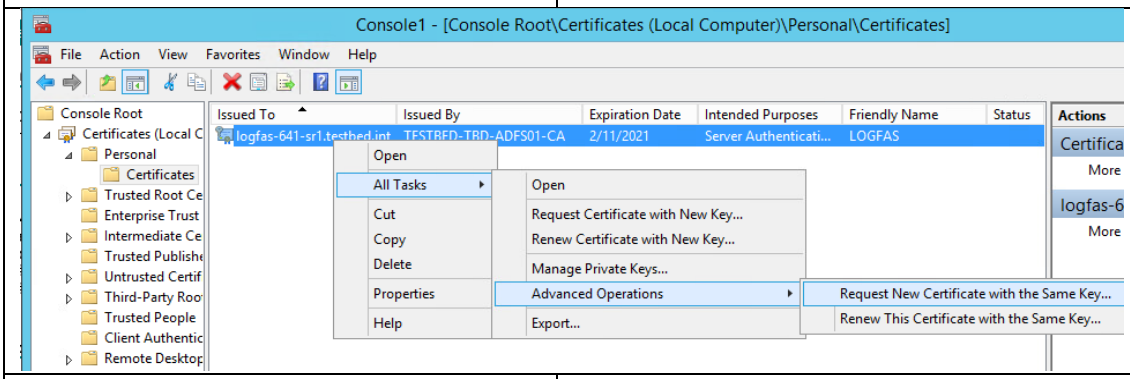


0061 In this case the buttom “Copy to File” was clicked to export the certificate.



0062 Make sure to export the private key.

0063 Check all of the possible options but DO NOT delete the private key unless the certificate does not need to be installed on the computer used to submit the request.	
0064 Using password will be recommended but note that without the password it won't be possible to import the certificate.	
0065 Click "Save" to continue with the export. The expected result will be to get a pop-up window saying "The export was successful" 0066 **0067**	

0068 At this time the requested certificate is available at two locations: 0069 Installed at the Personal store of the Local Computer 0070 And as .pfx file at the specified location (i.e. user's Desktop) because it was exported.	
0071 Explore the task available for the certificate.	
	

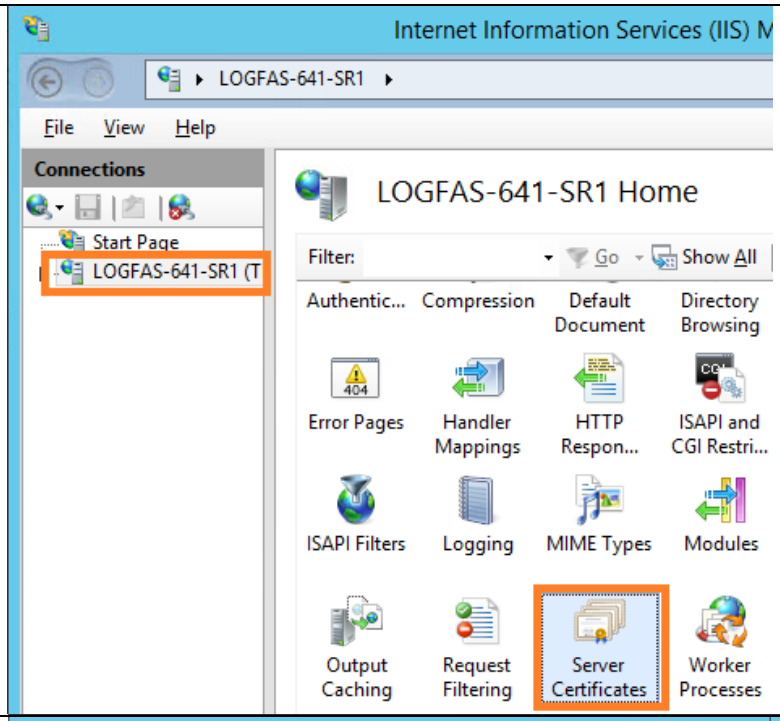
4.1.3 Step 1.2 Get an appropriated PKI certificate (Self-Signed)

0072 How to create a Self-Signed certificate using the IIS manager that will be used on the same computer hosting LOGFAS ADAMSWEB/EVEWEB.

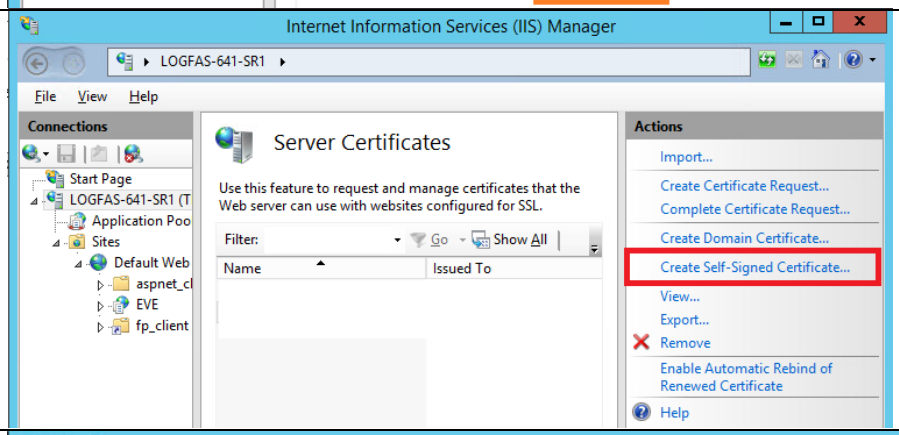
0073

0074

0075 Select the server node in the treeview and double-click the Server Certificates feature in the listview:

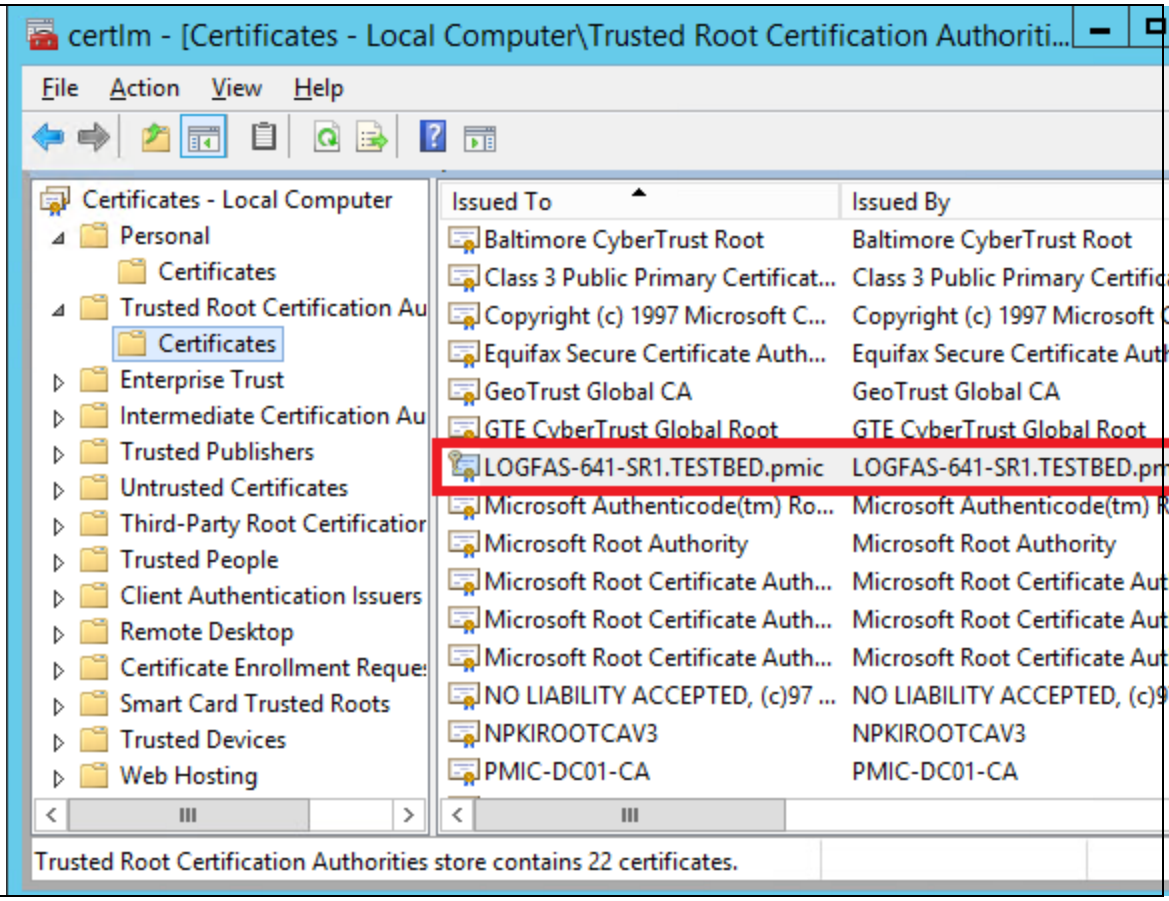


0076 Click "Create Self-Signed Certificate..." in the Actions pane.



0077

0078



0079 Enter a friendly name for the new certificate and click OK.

0080 Now you have a self-signed certificate. The certificate is marked for "Server Authentication" use that could be used as a server-side certificate for HTTP SSL encryption and for authenticating the identity of the server.

0081 Note that Viewing the certificate will also allow to export it.

4.2 Step 2. Create an HTTPS binding at the IIS site

0082 The default IIS binding settings are set to HTTP on port 80.

0083

0084 Select the the parent, ADAMSWEB and/or EVEWEB site in the tree view and click Bindings... in the Actions pane. This brings up the bindings editor that lets you create, edit, and delete bindings for your Web site.

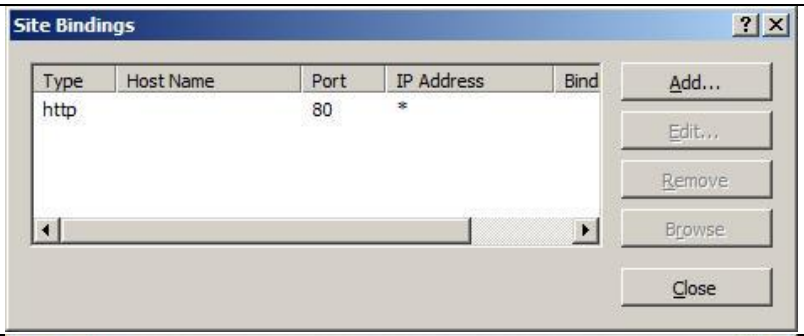
0085

0086 Using a unique certificate assigned to the parent site will make sense on most scenarios.

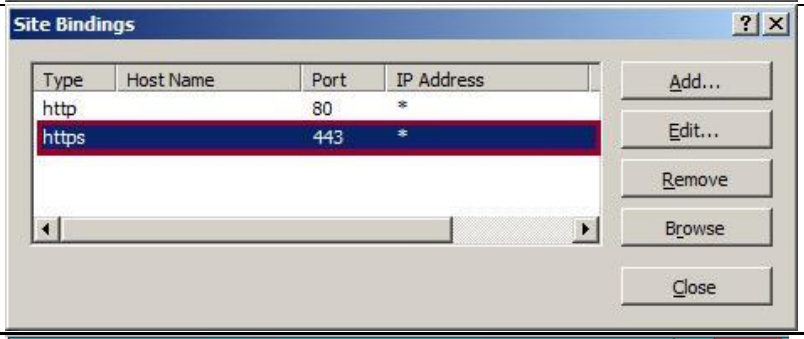
0087 Click Add... to add your new SSL binding to the site (TCP port 443) and assign the proper certificate.

0088

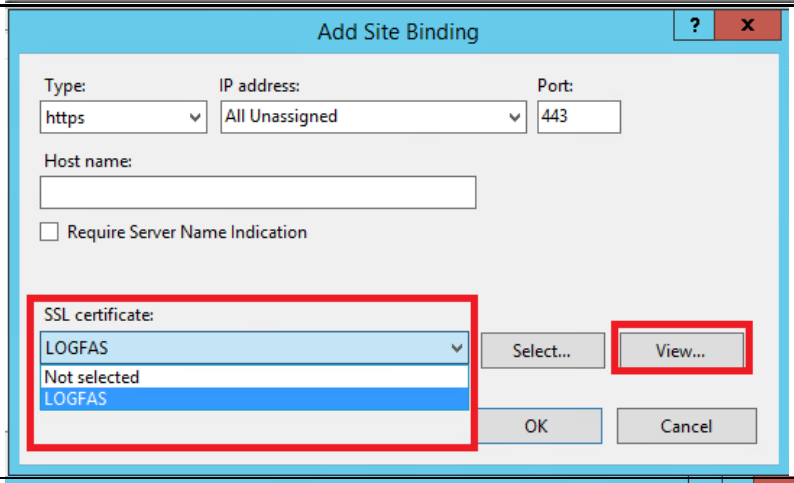
0089



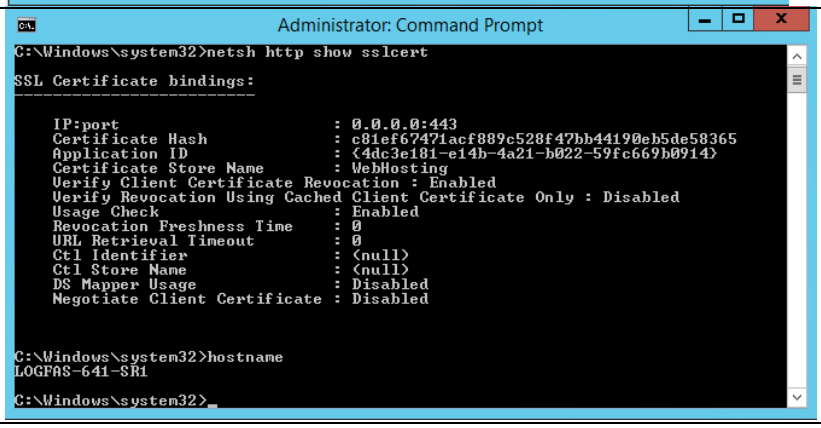
0090 It is possible to change the certificate: Select https in the Type drop-down list and Click Edit.

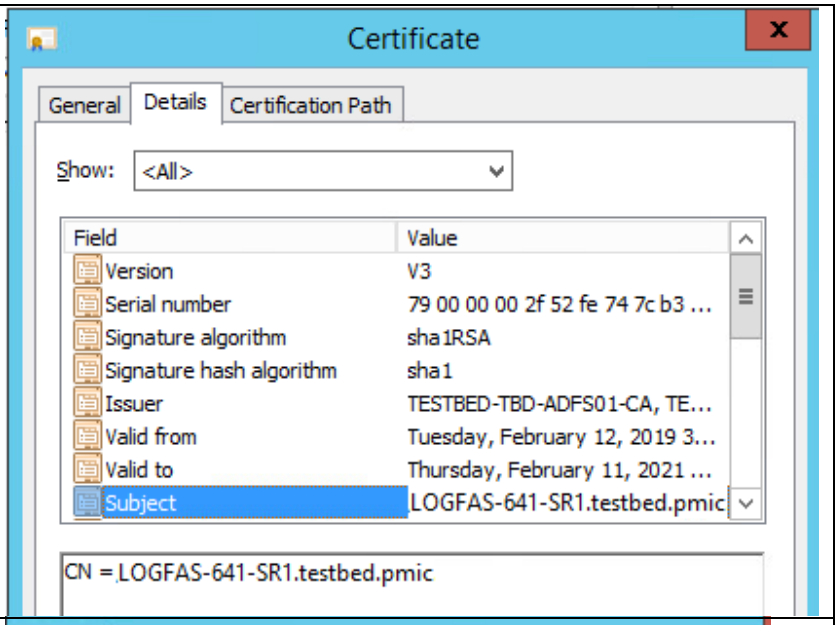
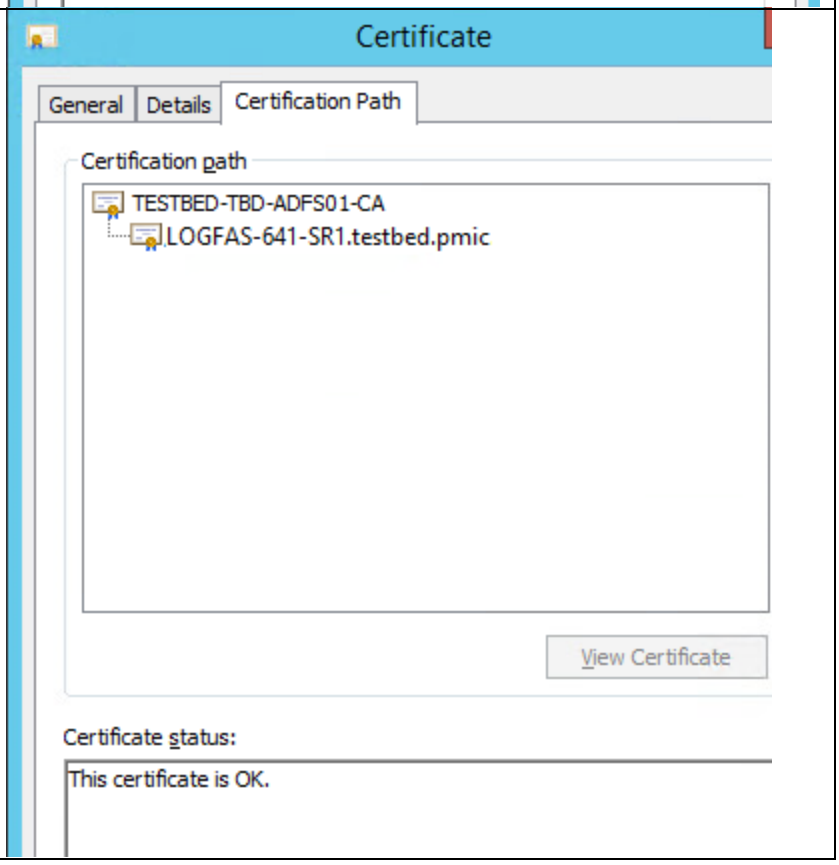


0091 Select the required certificate issued by your CA and/or Self-Signed and then click OK.

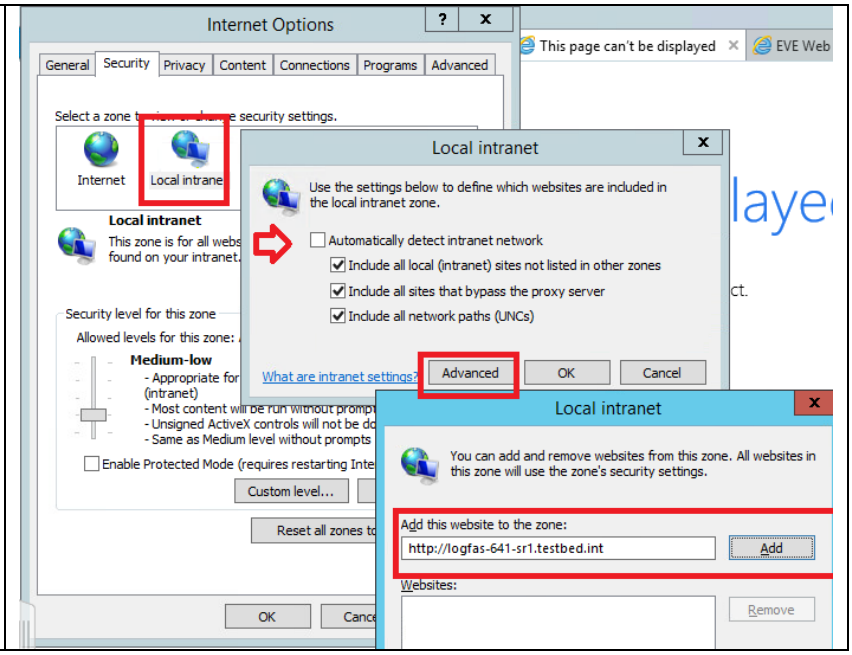


0092 The SSL binding is –now- available on your site and all that remains is to verify that it works.



0093 Use the IIS manager to browse the site (or use the subject of the certificate to build the required URL) **https://logfas-641-sr1.testbed.pmic/eve/**	
0094	

0095

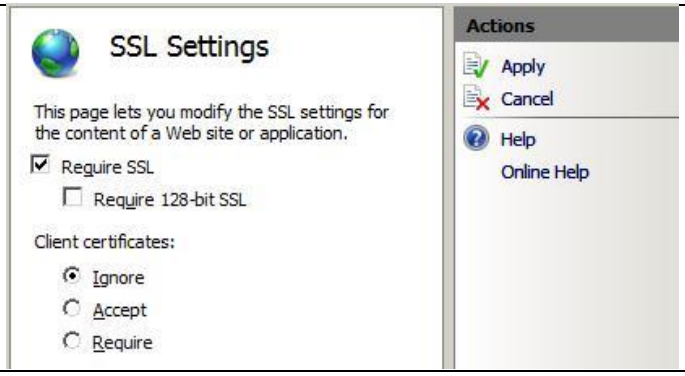


4.3 Step 3. Configure SSL settings for the IIS site

0096 Configure SSL settings if you want your site to require SSL, or to interact in a specific way with client certificates. Click the site node in the tree view to go back to the site's home page. Double-click the SSL Settings feature in the middle pane.

0097 If the box "Require SSL" is checked then HTTPS browsing will be required for that website. Furthermore, a 403.4 Forbidden error message will be raised when the user tries to browse the website over HTTP.

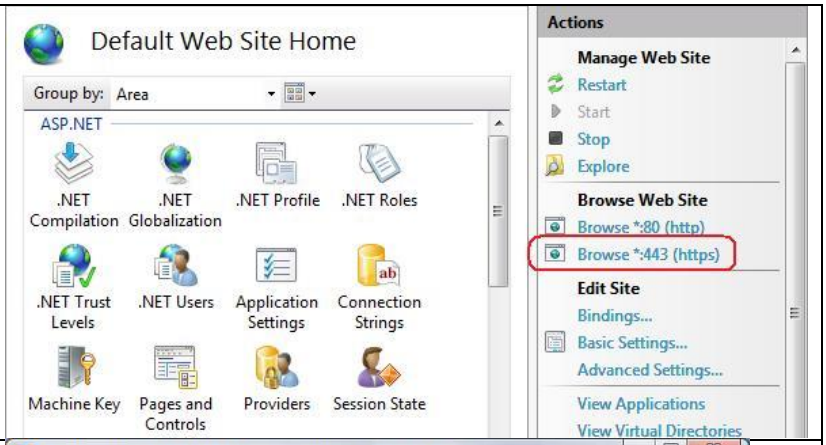
0098 Check recommended configuration values at the LOGFAS ADAMSWEB/EVEWEB installation guide.



4.4 Step 4. Test SSL by making a request to the IIS site

0099 Depending on the scope and usage of ADAMWEB/EVEWEB the PKI certificate could be Self-Signed or issued by the Certification Authority (CA) of the Active Directory (AD) Domain.

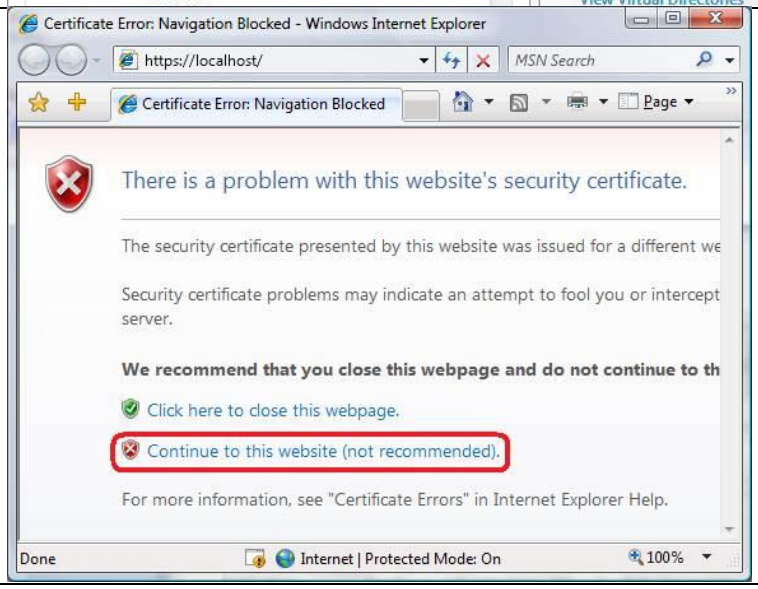
00100 Verify the SSL Binding: In the Actions pane, under Browse Web Site, click the link associated with the binding you just created.



00101 Internet Explorer (IE) 7 and above: it will display an error page because the self-signed certificate was issued by your computer, not by a trusted Certificate Authority (CA). IE 7 and above will trust the certificate if it was imported on the Trusted Root Certification Authorities (certificates store) of the local computer, or at the Group Policy for the domain.

00102 Click "Continue to this website (not recommended)" will allow to continue navigating to the site.

00103



4.5 Step 5. Install the public server's certificate to the client's certificate store

00104 Browse to the URL of the server's Web site (i.e. ADAMSWEB and/or EVEWEB), ignore the error, click on the certificate icon, view it and install it onto the Trusted Root Certification Authorities.

The URL should match with the subject's name of the server's certificate

- Include example here

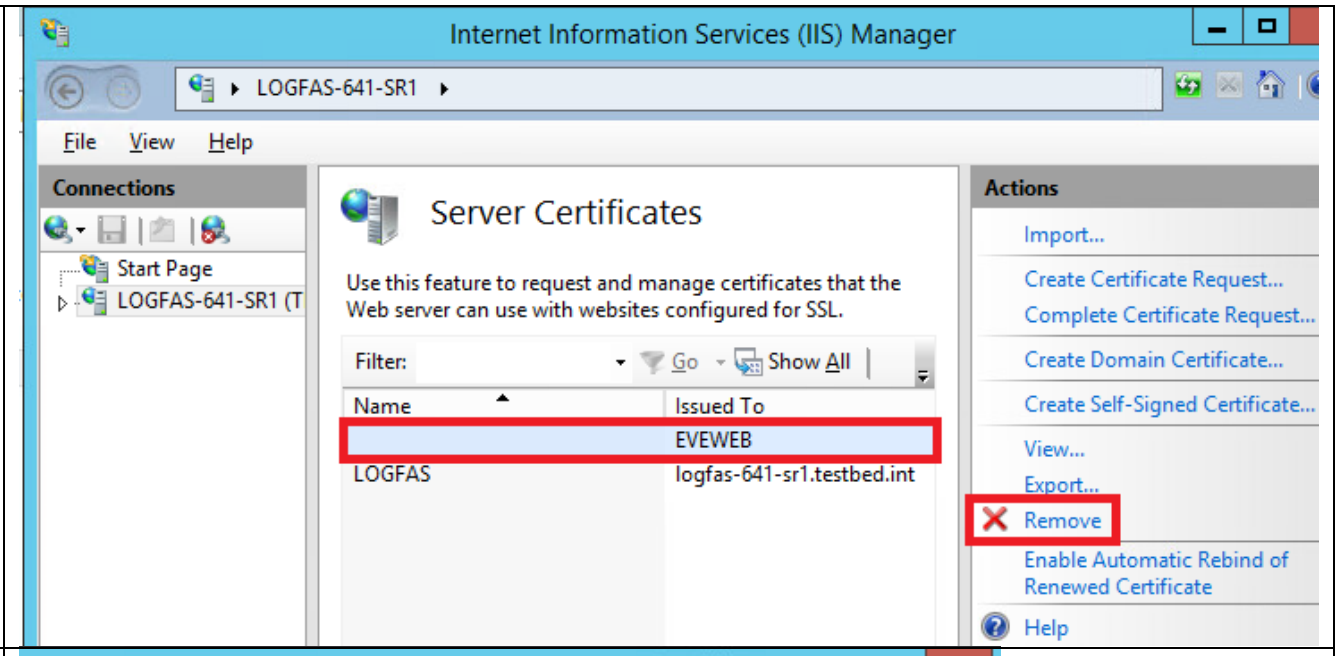
5 Step x. Removing PKI certificate(s)

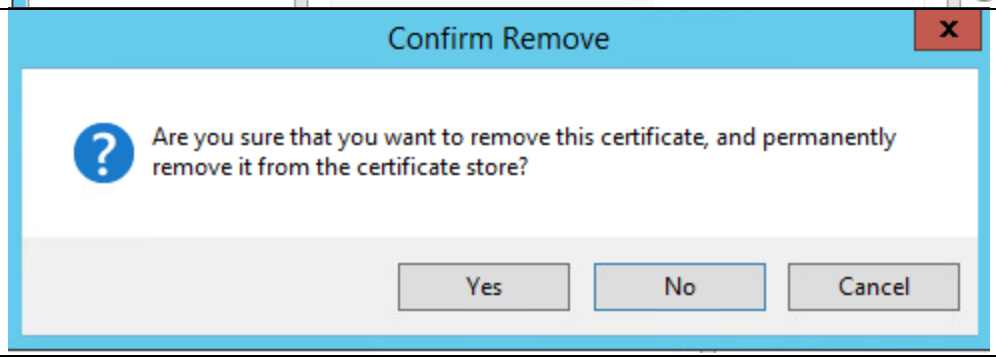
IMPORTANT NOTE

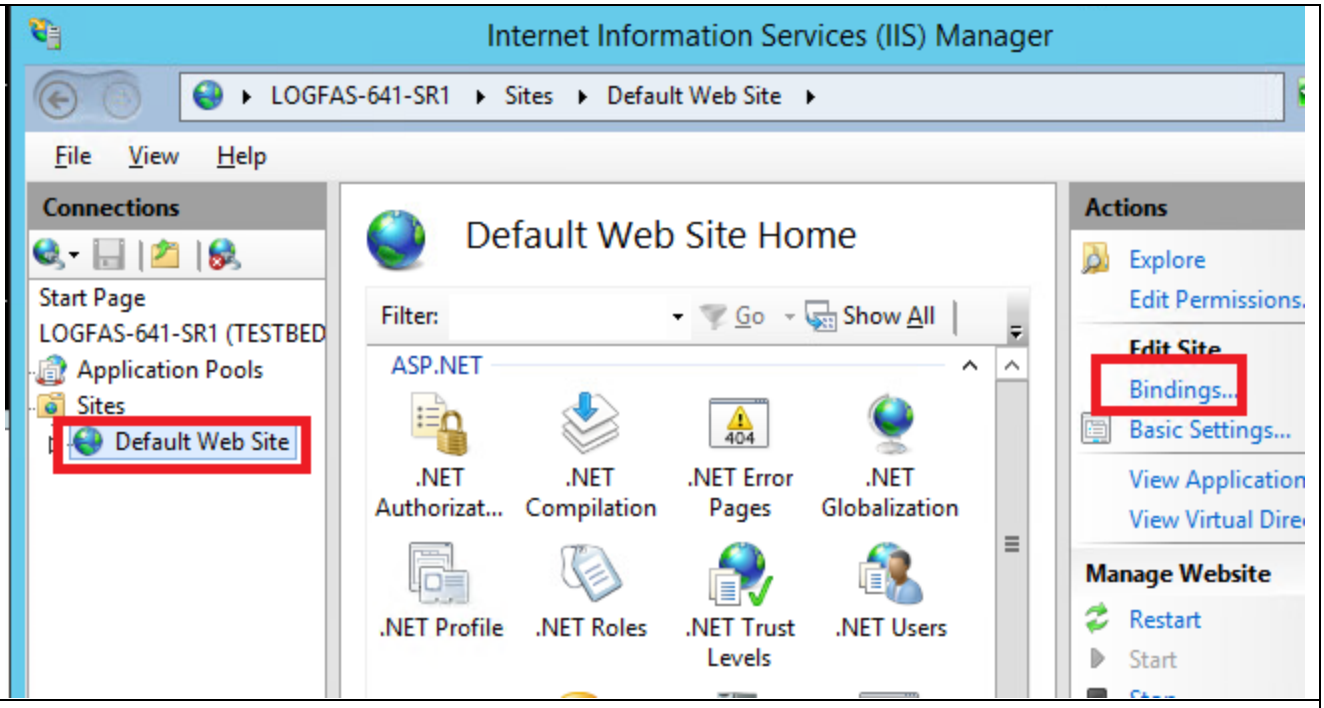
- The certificates deployed with ADAMSWEB and/or EVEWEB should be deleted (applicable to LOGFAS 6.4.1 and earlier versions up to 6.3.1)

00105 the Check the certificate in used by IIS

00106 Use the Internet Information Services (IIS) Manager as previously directed, but remove the certificate or binding instead of adding it.








```
C:\> netsh http show sslcert
```

00107 Remove the computer certificate by using a Windows command (CMD Run As Administrator).

1. https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/configuring-http-and-https
2. https://docs.microsoft.com/en-us/windows/desktop/http/netsh-commands-for-http
3. Windows XP / Server 2003

```
C:\> httpcfg delete ssl -i 0.0.0.0:443
```

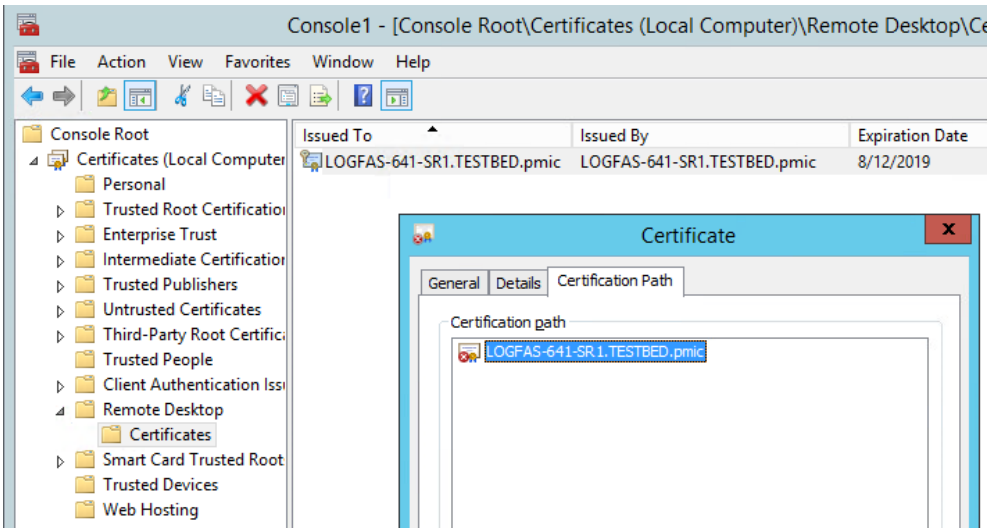
00108 Windows Vista / Windows 7

```
C:\> netsh http delete sslcert ipport=0.0.0.0:443
```

00109

00110

00111 The Certificate Manager tool (Certmgr.exe) manages certificates, certificate trust lists (CTLs), and certificate revocation lists (CRLs).



2

[1] Read how to customize the configuration file at the “EVE Web - Installation Manual.docx”, section “Web.config file configuration (optional)” that was supplied along with the product.