

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

1 References	3
1 Purpose	3
2 Applicability	3
3 Overview	3
3.2 General Overview	3
3.3 Requirements	3
4 How to set up SSL on IIS	3
4.1 Step 1.0 - Get an appropriated PKI certificate	5
4.1.1 Step 1.1 - Get an appropriated PKI certificate from Certification Authority (CA)	14
4.1.2 Requesting a certificate from the CA using the Certificate Management tool	18
4.1.3 Step 1.2 Get an appropriated PKI certificate (Self-Signed)	28
4.2 Step 2. Create an HTTPS binding at the IIS site	31
4.3 Step 3. Configure SSL settings for the IIS site	34
4.4 Step 4. Test SSL by making a request to the IIS site	35
5 Step x. Removing PKI certificate(s)	
2	

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	Certificate X
EVEWEB.	General Details Certification Path
	Certificate Information
	This certificate is intended for the following purpose(s):
	Ensures the identity of a remote computer All issuance policies
	Issued to: EVEWEB
	Issued by: EVEWEB
	Valid from 2/14/2019 to 2/14/2020
	eq: product of the set of t
	Issuer <u>S</u> tatement
	ОК

Certificate X
General Details Certification Path
Show: <all></all>
Field Value ^
Version V3 Serial number 29 e7 c6 d6 86 38 1a ac 41 d5 Signature algorithm sha 1RSA Signature hash algorithm sha 1 Issuer EVEWEB
Valid from Thursday, February 14, 2019
Subject EVEWEB
CN = EVEWEB Edit Properties
ОК

Cer	tificate
General Details Certification Path]
Show: <all></all>	~
Field Valid from Valid to Subject Public key Enhanced Key Usage Key Usage Thumbprint algorithm	Value ^ Thursday, February 14, 2019 Friday, February 14, 2020 4:0 EVEWEB RSA (1024 Bits) Server Authentication (1.3.6 Digital Signature, Key Encipher sha1 30 c0 d5 d0 1a e5 6f 68 45 d0
Server Authentication (1.3.6.1.5.5	
Ē	dit Properties <u>C</u> opy to File OK

Certificate X
General Details Certification Path
Certification path
<u>V</u> iew Certificate
Certificate <u>s</u> tatus:
This certificate is OK.
ОК

Example of IIS self-signed certificate	Certificate X		
	General Details Certification Path		
	Certificate Information		
	This certificate is intended for the following purpose(s):		
	Ensures the identity of a remote computer All issuance policies		
	Issued to: LOGFAS-641-SR1.TESTBED.pmic		
	Issued by: LOGFAS-641-SR1.TESTBED.pmic		
	Valid from 2/14/2019 to 2/14/2020		
	You have a private key that corresponds to this certificate.		
	Issuer <u>S</u> tatement		
	ОК		

. Co	ertificate X
General Details Certification Pa	th
Show: <all></all>	~
Field	Value ^
 Version Serial number Signature algorithm Signature hash algorithm 	V3 40 96 9b b1 b5 77 8c b1 4e 3e sha1RSA sha1
Issuer Valid from Valid to	LOGFAS-641-SR 1.TESTBED.pmic Thursday, February 14, 2019 Friday, February 14, 2020 1:0
E Subject	LOGFAS-641-SR1.TESTBED.pmic 🗸
CN = LOGFAS-641-SR 1.TESTBED	D.pmic
	Edit Properties Copy to File
	ОК

Cer	tificate x
General Details Certification Path]
Show: <all></all>	~
Field Valid to Subject Public key Key Usage Enhanced Key Usage Thumbprint algorithm Friendly name	Value ^ Friday, February 14, 2020 1:0 LOGFAS-641-SR1.TESTBED.pmic LOGFAS-641-SR1.TESTBED.pmic RSA (2048 Bits) Key Encipherment, Data Encip Server Authentication (1.3.6 Sha1 39 fb 20 5b 06 cf 35 2d 24 14 Ionfas 641-sr1 testbed int X
Server Authentication (1.3.6.1.5.5	.7.3.1)
Ē	lit Properties
	ОК

Certificate X
General Details Certification Path
Certification path
Image: Certificate gtatus: This certificate is OK.
ОК
Certificate X
General Details Certification Path
Field Value A Valid to Friday, February 14, 2020 1:0 Encipherment, 2020 1:0 Subject LOGFAS-641-SR 1.TESTBED.pmic Encipherment, 2020 1:0 Public key RSA (2048 Bits) Encipherment, Data Encip Enhanced Key Usage Server Authentication (1.3.6) Encipherment, Data Encip Thumbprint algorithm sha1 Encipherment, 2020 1:0 Friendly name Logfas-641-sr 1.testhed.int X
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.	RemovingapreviousversionofLOGFAS.If a previous version of LOGFAS is installed, you will need to removeit. Follow the section "Uninstalling LOGFAS (Client & Server)".1 If thisis a clean installationthen proceed to the following step below.	\checkmark	\checkmark
2.	PreparingLOGFASServerfortheDomain.Have your DomainAdministratorcreate a service account for thePOSTGRESQL service and issue the SETSPN commands as explained in "Preparing LOGFAS Server for the Domain with SETSPN" section.	x	\checkmark
3.	CreatingSSLCertificatesforLOGFASServer.If you don't have validSSL certificate(s) for you server you must installOpenSSL and generate them. The procedures can be found below in"Installing OpenSSL & Creating Certificates" section.	x	\checkmark
4.	LOGFAS Client and Server Software Installation. Install the LOGFAS software as explained in <i>"LOGFAS Software Installation Procedures"</i> section.	\checkmark	~
5.	LOGFASServerPost-InstallationConfiguration.To configure the databaseService, database, PGADMIN and SSPI,follow the steps described in "LOGFAS Server Post-InstallationProcedures" section.	x	\checkmark

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

0022 Note that NATO/National policies and processes 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/windowscommands/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: <u>https://<fully qualified Domain name>/certsrv</u>

	Windows PowerShell
PS C:\Users\ramon.garciav	riejo> CertUtil
Name:	`TESTBED.pmic Root CA'
Organizational Unit:	
Locality:	5 T
State:	
Config:	`TBD-CA01.TESTBED.pmic\TESTBED.pmic Root CA'
Exchange Certificate:	
Description:	N 1
Server:	`TBD-CA01.TESTBED.pmic'
Sanitized Name:	`TESTBED.pmic Root CA'
Short Name: Sanitized Short Name:	TESTRED parc Root CA'
Flags:	
Web Enrollment Servers:	
4	< 🕀 🖉 https://tbd-ca01.testbed.pmic/certsrv/Default.asp 🕼 🔎 👻 Certifi
0 https://tbd-kms01.testbed	
	Microsoft Active Directory Certificate Services TESTBED.pmic Root CA
Entry 1: Name:	
Organizational Unit:	Welcome
Locality:	
State:	Use this Web site to request a certificate for your Web browser, e-r
Country/region: Config:	the Web, sign and encrypt messages, and, depending upon the typ
Exchange Certificate:	
Description:	You can also use this Web site to download a certificate authority (
Server:	
Sanitized Name:	For more information about Active Directory Certificate Services, se
Short Name: Sanitized Short Name:	Coloré o fosku
Flags:	Deguest a contificate https://https://https://article.top/article.top/
Web Enrollment Servers:	request a certificate inters://too-cavitestoeo.pmic/certstv/certrqus.asp
Entry 2:	view the status of a pending certificate request
Organizational Unit:	Download a CA certificate, certificate chain, or CRL
Organization:	
State:	

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

Σ	Windows PowerShell
Windows PowerShell Copyright (C) 2014 Micro	osoft Corporation. All rights reserved.
PS C:\Users\ramon.garcia	aviejo> Get-CertificateEnrollmentPolicyServer
cmdlet Get-CertificateEr Supply values for the fo Scope: all context: user	nrollmentPolicyServer at command pipeline position 1 llowing parameters:
Id Url AuthType RequireStrongValidation AutoEnrollmentEnabled IsDefault Priority Context	: {510F80E6-44AB-47A6-B2AF-A1CC13537DFD} : ldap: : Kerberos : True : True : True : True : -1 : User

https://docs.microsoft.com/en-us/powershell/module/pkiclient/getcertificateenrollmentpolicyserver?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, <u>https://<servername>/certsrv</u>).

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. On the Request a Certificate page, click "Or, submit an advanced certificate request"	 ➡ LOGFAS-641-SR1 - Remote Desktop Connection ← → ▲ https://tbd-ca01.testbed.pmic/c ♀ ▼ Certificate e C ▲ Mi Microsoft Active Directory Certificate Services TESTBED.pmic Root CA Request a Certificate Select the certificate type: User Certificate 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.	Additional Attributes: Attribu

- 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 **certIm.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

						Console1 - [Console Root]	
	File	Action	View	Favorites	Window	Help	
4		New			Ctrl+N		
		Open			Ctrl+O		Acti
		Save			Ctrl+S		Co
		Save As.				Add or Remove Snap-ins	CU.
		Add/Rer Options.	nove Sna 	ap-in	You can extensibl	n select snap-ins for this console from those available on your computer and con ible snap-ins, you can configure which extensions are enabled.	
		1 Conso	eCertific	ates	Available	le snap-ins: Selected snap-ins:	
		2 wf			Snap-in Activ	in Vendor ^ Console Root	
		Exit			Aut	thorization Manager Microsoft Cor Certif	fica
					Com Com Dev Dev Even	remeates Microsoft Cor imponent services Microsoft Cor imputer Manager Microsoft Cor wicrosoft Cor Microsoft Cor sk Management Microsoft Cor went Viewer Microsoft Cor	for:
						Add or Remove Snap-ins	
			You can extensib	select snap-i le snap-ins, y	ns for this co you can confi	console from those available on your computer and configure the selected set of symp-ins. For figure which extensions are enabled.	
			Available	snap-ins:		Selected snap-ins:	
			Shap-ir	n iveX Control	Micro	rosoft Cor	
			Aut	horization Ma	anager Micro	rosoft Cor	
			Cer	tificates	Micro Micro	rosoft Cor	
			Link	to Web Add	ress Micro	rosoft Cor Advanced	
			Descripti	ion:			
			The Ce	rtificates sna	p-in allows yo	you to browse the contents of the certificate stores for yourself, a service, or a computer.	
						OK Cancel	

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

0043 At the local computer certificates:	Console1 - [Console Root\Certificate
request a new certificate.	🚟 File Action View Favorites Window Help
	Console Root Certificates (Local Computer) Personal Find Certificates Certificates (Local Computer) All Tasks Find Certificates
	▷ Conterned View ► Request New Certificate
	▷ Outruste New Window from Here Import ▷ Third-Pa New Taskpad View Advanced Operations ○ Trusted Refresh ○ Client Au Refresh ▷ Remote Export List ▷ Smart Ce Uate
	Trusted Levee
0044 Click "Next" to continue.	Certificate Enrollment
	Before You Begin The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks. Before requesting a certificate, verify the following: Your computer is connected to the network You have credentials that can be used to verify your right to obtain the certificate
	Next Cancel
0045 Optional: Click "Properties" to get more details.	X
	Select Certificate Enrollment Policy
	Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.
	Configured by your administrator
	Active Directory Enrollment Policy Enrollment Policy ID: {510F80E6-44AB-47A6-B2AF-A1CC13537DFD} Properties
	Configured by you Add New

0046 Once selected the certificates'	
template Click "Properties" to fill in	📮 Certificate Enrollment
required values.	Request Certificates You can request the following types of certificates. Select the certificates you want to request, and then click Enroll. Image: More information is required to enroll for this certificate. Click here to configure settings. Image: More information is required to enroll for this certificate. Click here to configure settings. Image: More information is required to enroll for this certificate. Click here to configure settings. Image: More information is required to enroll for this certificate. Click here to configure settings. The following options describe the uses and validity period that apply to this type of certificate: Key usage: Digital signature Key encipherment Application policies: Server Authentication Validity period (days): 730 Image: Properties Properties Image: Server Authentication Properties
	<u>Enroll</u> Cancel
0047 Give a Subject name and optionally	Certificate Properties X
an alternative name (e.g. adding	Common name V Asubject General Extensions Private Key Certification Authority EulIDM
localhost will not raise certificate'	Common name Common name Country Country Coun
errors when browsing	Domain component Email Subject of certificate
https:\\localhost\)	Given name The user or computer that is receiving the certificate Initials Locality Subject name:
	Organization Organization unit
	State Value: <a>Remove
	Title
	Other name V Directory name User principal nam
	DNS Email Value:
	GUID Add > IP address (v4) D address (v5)
	Registered ID URL
	User principal name Other name
	OK Cancel Apply
0048 A friendly name helps to identify	Certificate Properties
the certificate.	
	A friendly name and description will make it easier to identify and use a certificate
	Friendly name:
	LOGFAS
	Description:
	To be used by EVEWEB and ADAMSWEB

0049 Add any required extensions.	Certificate Properties	x
	Subject General Extensions Private Key Certification Authority Key usage ^	
	The key usage extension describes the purpose of a certificate. Available options: Selected options: CRL signing Decipher only Encipher only Key agreement Data encipherment Digital signature Key certificate signing Key encipherment Non repudiation	
	Make these key usages critical Extended Key Usage (application policies) An application policy (called enhanced key usage in Windows 2000) defines how a	
	certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.	=
	Available options: Selected options: Document Signing IP security IKE intermedia File Recovery Root List Signer Directory Service Email R Add > Certificate Request Agent Key Recovery Agent Private Key Archival	
	Lifetime Signing V OCSP Signing V < III	
	· · · ·	~
	OK Cancel Appl	у

0050 Set the restrictions for the private	Certificate Properties
key.	A Subject General Extensions Private Key Certification Authority
	Cryptographic Service Provider
	Key options
	Set the key length and export options for the private key.
	Key size: 2048
	Make private key exportable
	Allow private key to be archived
	Key type
	Key usage defines the allowed uses for a private key associated with a certificate.
	Exchange
	○ Signature
	Key permissions ^ Set permissions on the private key
	OK Cancel <u>Apply</u>
0051 The CAs for enrolment will be listed	Certificate Properties
0051 The CAs for enrolment will be listed and at least one of then must be	Certificate Properties
0051 The CAs for enrolment will be listed and at least one of then must be selected.	Certificate Properties X <u>A enrollment server is needed to issue and renew certificates. The system will connect to </u>
 0051 The CAs for enrolment will be listed and at least one of then must be selected. 0052 Click "Apply". 	Certificate Properties X Subject General Extensions Private Key Certification Authority A enrollment server is needed to issue and renew certificates. The system will connect to enrollment servers in the following list to process certificate requests.
 0051 The CAs for enrolment will be listed and at least one of then must be selected. 0052 Click "Apply". 	Subject General Extensions Private Key Certification Authority A enrollment server is needed to issue and renew certificates. The system will connect to enrollment servers in the following list to process certificate requests. Not all certificate templates are available each enrollment server. For diagnostic purposes, it may be helpful to identify all available enrollment servers.
 0051 The CAs for enrolment will be listed and at least one of then must be selected. 0052 Click "Apply". 	Certificate Properties Subject General Extensions Private Key Certification Authority A enrollment server is needed to issue and renew certificates. The system will connect to enrollment servers in the following list to process certificate requests. Not all certificate templates are available each enrollment servers. Image: Not all certification Authority Certification Authority Type:
 0051 The CAs for enrolment will be listed and at least one of then must be selected. 0052 Click "Apply". 	Certificate Properties Subject General Extensions Private Key Certification Authority A enrollment server is needed to issue and renew certificates. The system will connect to enrollment servers in the following list to process certificate requests. Not all certificate templates are available each enrollment servers. Certification Authority Type: Image: TestBED.pmic Root CA
 0051 The CAs for enrolment will be listed and at least one of then must be selected. 0052 Click "Apply". 	Certificate Properties Subject General Extensions Private Key Certification Authority A enrollment server is needed to issue and renew certificates. The system will connect to enrollment servers in the following list to process certificate requests. Not all certificate templates are available each enrollment servers. Certification Authority Type: TESTBED.pmic Root CA Enterprise root CA TESTBED-TBD-CA02-CA Enterprise subordinate CA TESTBED-TBD-ADES01-CA
 0051 The CAs for enrolment will be listed and at least one of then must be selected. 0052 Click "Apply". 	Certificate Properties Subject General Extensions Private Key Certification Authority A enrollment server is needed to issue and renew certificates. The system will connect to enrollment servers in the following list to process certificate requests. Not all certificate templates are available each enrollment server. For diagnostic purposes, it may be helpful to identify all available enrollment servers. Certification Authority Type: Image:
 0051 The CAs for enrolment will be listed and at least one of then must be selected. 0052 Click "Apply". 	Certificate Properties Subject General Extensions Private Key Certification Authority A enrollment server is needed to issue and renew certificates. The system will connect to enrollment servers in the following list to process certificate requests. Not all certificate templates are available each enrollment server. For diagnostic purposes, it may be helpful to identify all available enrollment servers. Certification Authority Type: TESTBED.pmic Root CA Enterprise root CA TESTBED-TBD-CA02-CA Enterprise subordinate CA TESTBED-TBD-ADFS01-CA Enterprise root CA
 0051 The CAs for enrolment will be listed and at least one of then must be selected. 0052 Click "Apply". 	Certificate Properties Subject General Extensions Private Key Certification Authority A enrollment server is needed to issue and renew certificates. The system will connect to enrollment servers in the following list to process certificate requests. Not all certificate templates are available each enrollment server. For diagnostic purposes, it may be helpful to identify all available enrollment servers. Certification Authority Type: TESTBED.pmic Root CA Enterprise root CA TESTBED-TBD-CA02-CA Enterprise subordinate CA TESTBED-TBD-ADFS01-CA Enterprise root CA
 0051 The CAs for enrolment will be listed and at least one of then must be selected. 0052 Click "Apply". 	Certificate Properties Subject General Extensions Private Key Certification Authority A enrollment server is needed to issue and renew certificates. The system will connect to enrollment servers in the following list to process certificate requests. Not all certificate templates are available each enrollment server. For diagnostic purposes, it may be helpful to identify all available enrollment servers. Certification Authority Type: TESTBED.pmic Root CA Enterprise root CA TESTBED-TBD-CA02-CA Enterprise subordinate CA TESTBED-TBD-ADFS01-CA Enterprise root CA
 0051 The CAs for enrolment will be listed and at least one of then must be selected. 0052 Click "Apply". 	Certificate Properties Subject General Extensions Private Key Certification Authority A enrollment server is needed to issue and renew certificates. The system will connect to enrollment servers in the following list to process certificate requests. Not all certificate templates are available each enrollment server. For diagnostic purposes, it may be helpful to identify all available enrollment servers. Certification Authority Type: TESTBED.pmic Root CA Enterprise root CA TESTBED-TBD-CA02-CA Enterprise subordinate CA TESTBED-TBD-ADFS01-CA Enterprise root CA
 0051 The CAs for enrolment will be listed and at least one of then must be selected. 0052 Click "Apply". 	Certificate Properties Subject General Extensions Private Key Certification Authority A enrollment server is needed to issue and renew certificates. The system will connect to enrollment servers in the following list to process certificate requests. Not all certificate templates are available each enrollment server. For diagnostic purposes, it may be helpful to identify all available enrollment servers. Certification Authority Type: TESTBED.pmic Root CA Enterprise root CA TESTBED-TBD-CA02-CA Enterprise subordinate CA TESTBED-TBD-ADFS01-CA Enterprise root CA
0051 The CAs for enrolment will be listed and at least one of then must be selected. 0052 Click "Apply".	Subject General Extensions Private Key Certification Authority A enrollment server is needed to issue and renew certificates. The system will connect to enrollment servers in the following list to process certificate requests. Not all certificate templates are available each enrollment server. For diagnostic purposes, it may be helpful to identify all available enrollment servers. Certification Authority Type: TESTBED.pmic Root CA Enterprise root CA TESTBED-TBD-CA02-CA Enterprise subordinate CA TESTBED-TBD-ADFS01-CA Enterprise root CA
0051 The CAs for enrolment will be listed and at least one of then must be selected. 0052 Click "Apply".	Certificate Properties Subject General Extensions Private Key Certification Authority A enrollment server is needed to issue and renew certificates. The system will connect to enrollment servers in the following list to process certificate requests. Not all certificate templates are available each enrollment server. For diagnostic purposes, it may be helpful to identify all available enrollment servers. Certification Authority Type: TESTBED.pmic Root CA Enterprise root CA TESTBED-TBD-CA02-CA Enterprise subordinate CA TESTBED-TBD-ADFS01-CA Enterprise root CA TESTBED-TBD-ADFS01-CA Enterprise root CA Show all enrollment servers Enterprise root CA
0051 The CAs for enrolment will be listed and at least one of then must be selected. 0052 Click "Apply".	Certificate Properties X Subject General Extensions Private Key Certification Authority A enrollment server is needed to issue and renew certificates. The system will connect to enrollment servers in the following list to process certificate requests. Not all certificate templates are available each enrollment server. For diagnostic purposes, it may be helpful to identify all available enrollment servers. Certification Authority Type: TESTBED.pmic Root CA Enterprise root CA TESTBED-TBD-CA02-CA Enterprise subordinate CA TESTBED-TBD-ADFS01-CA Enterprise root CA TESTBED-TBD-ADFS01-CA Enterprise root CA Show all enrollment servers OK

 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. 	Certificate Enrollment Requesting certificates. Please wait The enrollment server is being contacted to obtain the certificates you have requested. Active Directory Enrollment Policy Web Server Cancel Cancel
 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 	Certificate Enrollment Certificate Installation Results The following certificates have been enrolled and installed on this computer. Active Directory Enrollment Policy Web Server The following options describe the uses and validity period that apply to this type of certificate: Key usage: Data encipherment Digital signature Key certificate signing Key encipherment Application policies Validity period (days): 730 Yiew Certificate Einish
 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 	Certificate X General Details Certification Path Image: Certificate Information This certificate is intended for the following purpose(s): • • Ensures the identity of a remote computer • All application policies • All application policies Issued to: logfas-641-sr 1.testbed.int Issued to: logfas-641-sr 1.testbed.int Issued by: TESTBED-TBD-ADFS01-CA Valid from 2/12/2019 to You have a private key that corresponds to this certificate. Issuer Statement

0059 Review other values	Certificate X
0060 Clicking "Copy to File" allows to	General Details Certification Path
export the certificate to a .pfx file. The	
export could be done later on using	
the Certificate Manager.	Field Value Subject Key Identifier fc 9c ac a1 bc 6e 54 70 f9 8d
	Subject Alternative Name Other Name:Principal Name=Io Other Name:Principal Name=Io
	CRUCING TRANSPORTED TO THE STATE OF THE STA
	Image: Second State Sta
	Thumbprint algorithm sha 1 Thumbprint c8 1e f6 74 71 ac f8 89 c5 28 f V
	Other Name
	Principal Name=logfas-641-sr1
	Edit Properties
	ОК
0061 In this case the huttom "Convite	
File" was clicked to export the	
certificate	
certificate.	Welcome to the Certificate Export Wizard
	This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
	A certificate, which is issued by a certification authority, is a confirmation of your identity
	connections. A certificate store is the system area where certificates are kept.
	To continue, click Next.
	<u>N</u> ext Cancel
0062 Make sure to export the private	×
key.	📀 🍠 Certificate Export Wizard
	Export Private Key You can choose to export the private key with the certificate.
	Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
	Do you want to export the private key with the certificate?
	<u>Yes, export the private key</u>
	○ No, do not export the private key
	<u>N</u> ext Cancel

0063 Check all of the possible options	X
but DO NOT delete the private key	📀 🍠 Certificate Export Wizard
unless the certificate does not need to be installed on the computer used to	Export File Format Certificates can be exported in a variety of file formats.
submit the request.	Select the format you want to use: DER encoded binary X.509 (.CER) Bage-64 encoded X.509 (.CER) Oryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) Include all certificates in the certification path if possible Personal Information Exchange - PKCS #12 (.PFX) Include all certificates in the certification path if possible Delete the private key if the export is successful Export all extended properties Microsoft Serialized Certificate Store (.SST)
0064 Using password will be	×
recommended but note that without	📀 🔄 Certificate Export Wizard
the password it won't be possible to import the certificate.	Security To maintain security, you must protect the private key to a security principal or by using a password. Group or user names (recommended) Add Remove Password: Confirm
0065 Click "Save" to continue with the	Save As
export. The expected result will be to	€ · ↑ ■ Desktop ♥ C Search Desktop ₽
get a pop-up window saying "The	Organize ▼ New folder
export was successful" 0066 0067	Favorites This PC Desktop Downloads Recent places Libraries
	File name: LOGFAS-641-SR1.testbed.pmic
	Save as type: Personal Information Exchange (*.pfx)

0008 At this time the requested	🚡 Consc	ole1 - [Console	Root\Certificat	tes (Loca	al Computer)\Personal\	Certificates]
certificate is available at two locations	S: <u>नि</u> <u>F</u> ile <u>A</u> c	tion <u>V</u> iew Fav	v <u>o</u> rites <u>W</u> indow	<u>H</u> elp		
0069 Installed at the Personal store of the	e 🔿 🖄	D	🗟 🛿 🖬			
Local Computer	Console ⊿ 🗊 Certif	Root iicates (Local C	lssued To 🛱 logfas-641-sr1.te	stbed.in1	Issued By TESTBED-TBD-ADFS01-CA	Expiration Date 2/11/2021
location (i.e. user's Desktop) becaus it was exported.	ie	Certificates rusted Root Cen nterprise Trust termediate Cec rusted Publishe ntrusted Certif hird-Party Roo				
0071 Explore the task available for the		,				
certificate						
Consolat Consola P	oot\Cortificator (Loca					
Console1 - [Console Ro	oot\Certificates (Loca	I Computer)\Perso	onal\Certificates]			
Console1 - [Console Ro	oot\Certificates (Loca	I Computer)\Perso	onal\Certificates]			
Image: Second	oot\Certificates (Loca	I Computer)\Perso	onal\Certificates]	Status	Actions	
Console 1 - [Console Ro File Action View Favorites Window Help ← → △ □ 《 □ 《 □ 》 □ ↓ □ Console Root ↓ Certificates (Local C ↓ □ Personal	OOT\Certificates (Loca Expiration Date 01-CA 2/11/2021	I Computer)\Perso Intended Purposes Server Authenticati.	Friendly Name LOGFAS	Status	Actions Certifica	
Console1 - [Console Ro File Action View Favorites Window Help File Console Root Console Root Certificates Certificates Open All Tasks	Oot\Certificates (Loca Expiration Date 01-CA 2/11/2021 Open	I Computer)\Perso	Friendly Name	Status	Actions Certifica More	
Console 1 - [Console Ro File Action View Favorites Window Help Image: Second Seco	oot\Certificates (Loca Expiration Date 01-CA 2/11/2021 Open Request Certificate with N	I Computer)\Perso Intended Purposes Server Authenticati.	Friendly Name	Status	Actions Certifica More logfas-6	
Console 1 - [Console Ro File Action View Favorites Window Help Image: Second Seco	oot\Certificates (Loca Expiration Date 01-CA 2/11/2021 Open Request Certificate with Nenew	I Computer)\Perso Intended Purposes Server Authenticati lew Key w Key	Friendly Name	Status	Actions Certifica More logfas-6 More	
Console 1 - [Console Ro File Action View Favorites Window Help File Action View Favorites View Favorites Console Root Console Root Issued To Issued By Certificates Cortificates Open Open Cut Cut Cut Cut Intermediate Ce Cut Copy Delete Vurtured Publisht Delete Delete	oot\Certificates (Loca Expiration Date 01-CA 2/11/2021 Open Request Certificate with N Renew Certificate with Ne Manage Private Keys	I Computer)\Perso Intended Purposes Server Authenticati. iew Key w Key	Friendly Name LOGFAS	Status	Actions Certifica More logfas-6 More	
 Console 1 - [Console Rot File Action View Favorites Window Help File Action View Favorites Window Help Console Rot Console Rot Certificates (Local Personal Certificates Trusted Rot Ce Enterprise Trust Intremediate Ce Trusted Publisht Untrusted Certifi Third-Party Roo 	oot\Certificates (Loca Expiration Date 01-CA 2/11/2021 Open Request Certificate with Ne Renew Certificate with Ne Manage Private Keys Advanced Operations	I Computer)\Perso Intended Purposes Server Authenticati. Iew Key w Key	Priendly Name Friendly Name LOGFAS	Status ste with the S	Actions Certifica More logfas-6 More ame Key	
 Console 1 - [Console Rot File Action View Favorites Window Help File Action View Favorites Window Help Console Rot Certificates (Local Certificates (Local Certificates (Local Certificates (Local Certificates (Local Certificates (Local Trusted Rot Ce Enterprise Trust Intermediate Ce Trusted Publishe Untrusted Certifi Third-Party Roo Trusted People Client Authentic 	oot\Certificates (Loca Expiration Date 01-CA 2/11/2021 Open Request Certificate with N Renew Certificate with Ne Manage Private Keys Advanced Operations Export	I Computer)\Perso	Priendly Name Friendly Name LOGFAS Request New Certificat	Status ste with the Sa	Actions Certifica More logfas-6 More Jame Key me Key	
 Console 1 - [Console Rot File Action View Favorites Window Help File Action View Favorites Window Help Console Rot Certificates (Local Personal Certificates (Local Prosentiate Ce Enterprise Trust Intermediate Ce Trusted Publish Untrusted Certifi Third-Party Roor Trusted People Client Authentic Remote Desktop 	Oot\Certificates (Loca Expiration Date 01-CA 2/11/2021 Open Request Certificate with N Renew Certificate with Ne Manage Private Keys Advanced Operations Export	I Computer)\Perso	Priendly Name . LOGFAS Request New Certificat Renew This Certificat	Status ste with the Sa	Actions Certifica More logfas-6 More same Key me Key	
Console 1 - [Console Ro File Action View Favorites Window Help File Action View Favorites Window Help Console Root Issued To Issued By Console Root Issued To Issued By Certificates Certificates Open Cut Cut Cut Intermediate Ce Cut Copy Trusted Publisht Open Delete Cient Authentic Remote Desktop Help	Oot\Certificates (Loca Expiration Date 01-CA 2/11/2021 Open Request Certificate with N Renew Certificate with Ne Manage Private Keys Advanced Operations Export	I Computer)\Perso	Friendly Name LOGFAS	Status ste with the S a with the Sa	Actions Certifica More logfas-6 More iame Key me Key	
Console 1 - [Console Ro File Action View Favorites Window Help File Action View Favorites Window Help Console Root Issued To Issued By Console Root Issued To Issued To Trusted Publisht Cut Copy Delete Properties Help Client Authentic Remote Desktop Help	oot\Certificates (Loca Expiration Date 01-CA 2/11/2021 Open Request Certificate with Ne Manage Private Keys Advanced Operations Export	I Computer)\Perso	Friendly Name LOGFAS Request New Certificat Renew This Certificat	Status ste with the Sa	Actions Certifica More logfas-6 More iame Key me Key	

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





- 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	Site Bindings			
binding to the site (TCP port 443) and assign the proper certificate	Type Host Name Port IP Address Bind Add			
0088	Edit			
0089	<u>R</u> emove			
	Browse			
	Glose			
0090 It is possible to change the	Site Bindings	×		
certificate: Select https in the Type	Type Host Name Port IP Address <u>A</u> dd			
drop-down list and Click Edit.	http 80 * https 443 * <u>E</u> dit			
	Remove			
	Browse			
	Glose			
0091 Select the required certificate issued	Add Site Binding	Γ		
by your CA and/or Self-Signed and	Type: IP address: Port:			
then click OK.	https v All Unassigned v 443			
	Host name:			
	Require Server Name Indication			
	SSL certificate:			
	LOGFAS View View View			
	LOGFAS OK Cancel			
		×		
0092 The SSL binding is –now- available	Administrator: Command Prompt C:\Windows\system32>netsh http show sslcert			
on your site and all that remains is to SSL Certificate bindings:				
verity that it works.	IP:port : 0.0.0.0:443 Certificate Hash : c8lef6747lacf889c528f47bb44190eb5de58365 Application ID : t4dc3el81-e14b-4a21-b022-59fc669b0914) Certificate Store Name : WebHosting Uerify Client Certificate Revocation : Enabled Uerify Revocation Using Cached Client Certificate Only : Disabled Usage Check : Enabled Revocation Freshness Time : 0 URL Retrieval Timeout : 0 Ctl Identifier : (null) Ctl Identifier : (null) DS Mapper Usage : Disabled Negotiate Client Certificate : Disabled Ctl Ident Certificate : Disabled Negotiate Client Certificate : Disabled			
	c:\windows\system32>hostname LOGFAS-641-SR1 C:\Windows\system32>_	~		

0093 Use the IIS manager to browse the	Certificate X
site (or use the subject of the	
certificate to build the required URL)	General Details Certification Path
https://logfas-641-sr1.testbed.pmic/eve/	Show: <all> Field Value Version V3 Serial number 79 00 00 00 2f 52 fe 74 7c b3 Signature algorithm sha 1RSA Signature hash algorithm sha 1 Issuer TESTBED-TBD-ADFS01-CA, TE Valid from Tuesday, February 12, 2019 3 Valid to Thursday, February 11, 2021 Subject LOGFAS-641-SR1.testbed.pmic</all>
0094	
	General Details Certification Path Certification gath Image: TESTBED-TBD-ADFS01-CA Ima



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		Actions		
HTTPS browsing will be required for that	SSL Settings	Apply		
website. Furthermore, a 403.4 Forbidden error	ermore, a 403.4 Forbidden error This page lets you modify the SSL settings for			
message will be raised when the user tries to	the content of a Web site or application.	😧 Help		
browse the website over HTTP.	Require SSL	Online Help		
0098 Check recommended configuration values at	Client certificates:			
the LOGFAS ADAMSWEB/EVEWEB installation	• Ignore			
guide.	C Accept			
	C Require			

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.



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.



2]	Ir	nternet Inforr	nation Ser	vices (IIS) Ma	nager	
	€ ► LOGFAS-641-SR1 ► Sites ► Default Web Site ►					
<u>F</u> ile <u>V</u> iew <u>H</u>	<u>H</u> elp					
Connections	De	Default Web Site Home			Actions	
Start Page LOGFAS-641-SR1	(TESTBED Filter: ools ASP.NET	ingen er	• 7 <u>9 G</u> o •	Show <u>A</u> ll	Ŧ	Edit Permissions.
i Sites	eb Site	.NET	.NET Error	.NET		Basic Settings View Application
	Authorizat	Compilation	Pages	Globalization	=	View Virtual Dire
	.NET Profile	.NET Roles	.NET Trust Levels	.NET Users		RestartStart
			-			Chara Chara
C:\> net	tsh http show sslcer	t				

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

- 1. <u>https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/configuring-http-and-https</u>
- 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).

	Console1 - [Console Root\Cert	ificates (Local Computer)\Rer	note Desktop\Ce
🔚 File Action View Favorites	Window H	Help		
🗢 🔿 🖄 🖬 🗶 🛛	1 🔒 🛛 🗖	1 1 1		
Console Root	Issued To	.	Issued By	Expiration Date
⊿ 🚽 Certificates (Local Computer	🛱 LOGFAS-6	41-SR1.TESTBED.pmic	LOGFAS-641-SR1.TESTBED.pmic	8/12/2019
📔 Personal				
Trusted Root Certification		_		
Enterprise Trust		08	Certificate	×
Intermediate Certification			10 H B H	
Trusted Publishers		General Details	ertification Path	
Untrusted Certificates		Certification path		
Third-Party Root Certifici		I OGEAS-641	-SR 1. TESTBED. pmic	
Irusted People				
Client Authentication Issi				
⊿ Remote Desktop				
Smart Card Trusted Root				
Web Hesting				
web Hosting				

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.