Damaris

Procedure

Update SSL Certificate

Update SSL Certificate

Procedure

Version	Auteur : modifications	Date
1.00	AA: Document Creation	20/04/2020
2.00	AA: Add Windows and Apache Servers Upgrade	18/06/2020

Table des matières

1 - INTRODUCTION

Periodically, we need to update our managed servers with a new ssl certificate.

This document describes how to install new certificate on existing servers.

2 – THE CONTEXT

At Damaris we deployed different server types:

- Linux tomcat
- Linux Apache
- Linux PHPBB
- Linux Vsftpd
- Windows tomcat
- Windows Filezilla

So, this document will explain how to upgrade for each server type.

3 - PREREQUISITES

Before starting, you should verify several prerequisites.

- Do you have new ssl certificate, for each server type?
  - keystore_damarisxx.jks: Keystore
  - damarisproxx.key: Private key
  - damarisproxx.pem: Certificate
- Do you have access to all servers to be upgraded?
- Current list of servers to be upgraded
- Take care of best timing because of server unavailability for users

4 – SSL UPGRADE PROCEDURE

4.1 – LINUX TOMCAT

Please get the new keystore and its password.

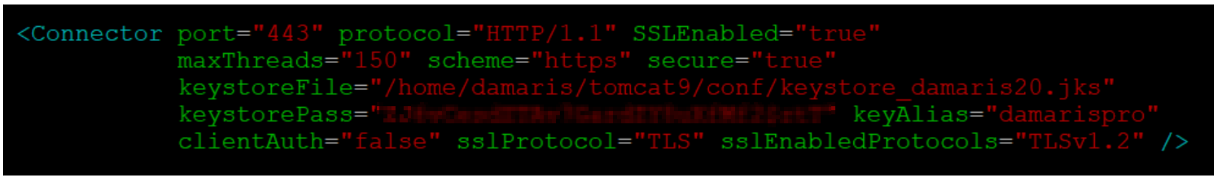
Login on the target server.

Go to /tomcat9/conf folder and copy the new keystore on it.

Modify conf/server.xml file by adapting the following information:

- KeystoreFile: with the new keystore filename
- KeystorePass: with the new keystore's password
- keyAlias: Please check if it contains the right value
- Please add the following tag: **sslEnabledProtocols="TLSv1.2"**

You will get this type of section:



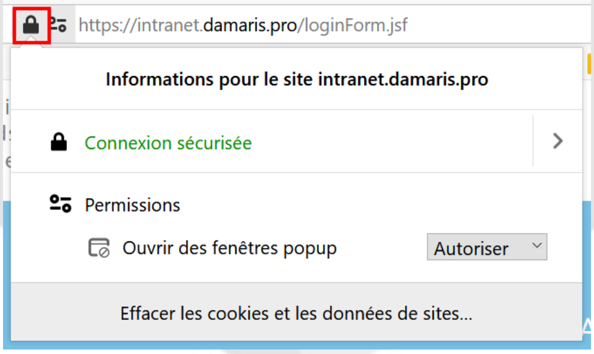
```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
           maxThreads="150" scheme="https" secure="true"
           keystoreFile="/home/damaris/tomcat9/conf/keystore_damaris20.jks"
           keystorePass="[redacted]" keyAlias="damarispro"
           clientAuth="false" sslProtocol="TLS" sslEnabledProtocols="TLSv1.2" />
```

Restart tomcat by running as root:

```
systemctl restart tomcat
```

Test connection from a browser.

After accessing to web page, please click on key icon near URL.



https://intranet.damaris.pro/loginForm.jsf

Informations pour le site intranet.damaris.pro

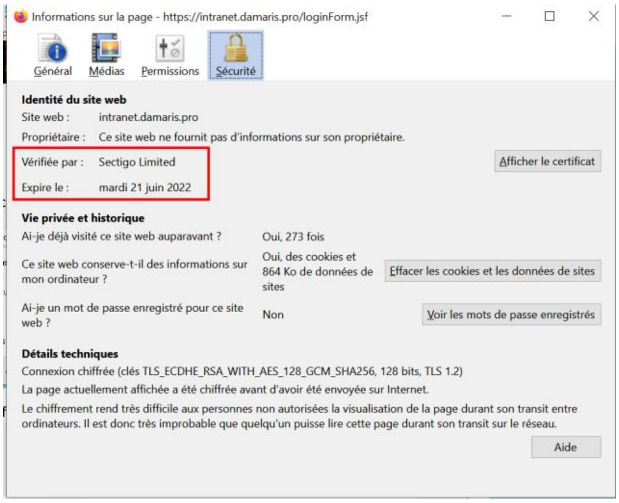
Connexion sécurisée

Permissions

Ouvrir des fenêtres popup: Autoriser

Then, click on right arrow and "More information" button.

You will get this kind of window:



Informations sur la page - https://intranet.damaris.pro/loginForm.jsf

Identité du site web

Site web : intranet.damaris.pro

Propriétaire : Ce site web ne fournit pas d'informations sur son propriétaire.

Vérifiée par : Sectigo Limited

Expire le : mardi 21 juin 2022

Vie privée et historique

Ai-je déjà visité ce site web auparavant ? Oui, 273 fois

Ce site web conserve-t-il des informations sur mon ordinateur ? Oui, des cookies et 864 Ko de données de sites

Ai-je un mot de passe enregistré pour ce site web ? Non

Détails techniques

Connexion chiffrée (clés TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bits, TLS 1.2)

La page actuellement affichée a été chiffrée avant d'avoir été envoyée sur Internet.

Le chiffrement rend très difficile aux personnes non autorisées la visualisation de la page durant son transit entre ordinateurs. Il est donc très improbable que quelqu'un puisse lire cette page durant son transit sur le réseau.

The most important information here is Expire date.

4.2 – LINUX VSFTPD

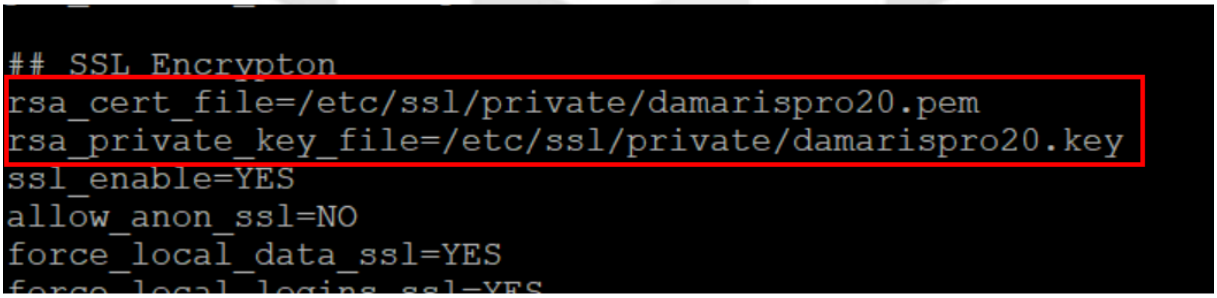
Please get ssl key and certificate files.

Connect to target Linux server.

Please copy (As root or sudo) key and certificate files into /etc/ssl/private directory.

Please modify /etc/vsftpd/vsftpd.conf file by updating file names for key and certificate:

- rsa_cert_file
- rsa_private_key=



```
## SSL Encrypton
rsa_cert_file=/etc/ssl/private/damarispro20.pem
rsa_private_key_file=/etc/ssl/private/damarispro20.key
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
```

Please restart vsftpd by running as root:

```
systemctl restart vsftpd
```

4.3 – WINDOWS TOMCAT

Please get the new keystore and its password.

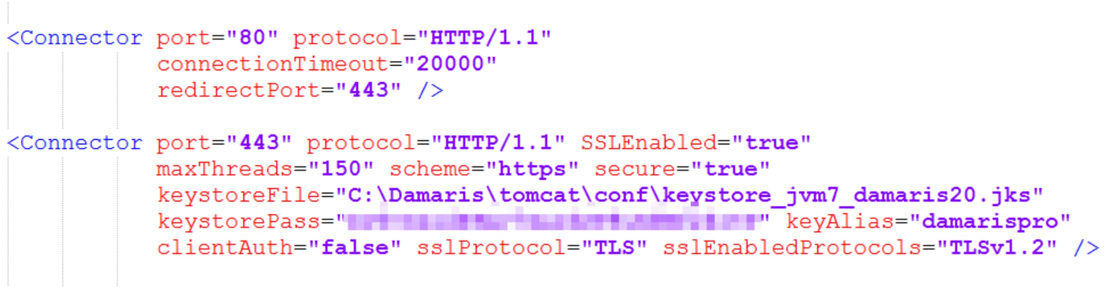
Login on the target server.

Go to /tomcat/conf folder and copy the new keystore on it.

Modify conf/server.xml file by adapting the following information:

- KeystoreFile: with the new keystore filename
- KeystorePass: with the new keystore's password
- keyAlias: Please check if it contains the right value
- Please add the following tag: **sslEnabledProtocols="TLSv1.2"**

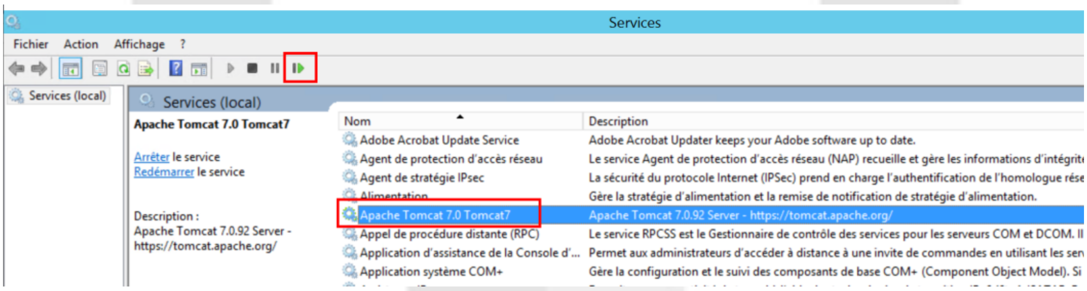
You will get this type of section:



```
<Connector port="80" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="443" />

<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
           maxThreads="150" scheme="https" secure="true"
           keystoreFile="C:\Damaris\tomcat\conf\keystore_jvm7_damaris20.jks"
           keystorePass="[redacted]" keyAlias="damarispro"
           clientAuth="false" sslProtocol="TLS" sslEnabledProtocols="TLSv1.2" />
```

Restart Apache tomcat Windows Service using Services.msc:



Apache Tomcat 7.0 Tomcat7

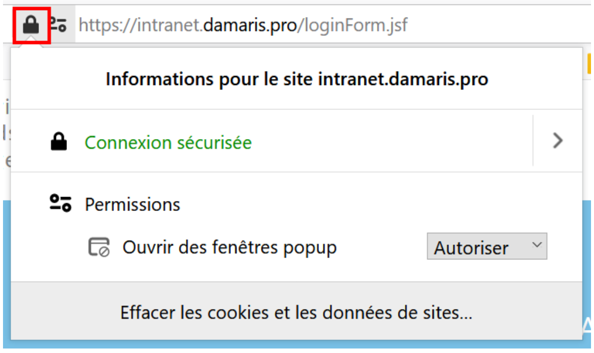
Arrêter le service
Redémarrer le service

Description :
Apache Tomcat 7.0.92 Server - https://tomcat.apache.org/

Nom	Description
Adobe Acrobat Update Service	Adobe Acrobat Updater keeps your Adobe software up to date.
Agent de protection d'accès réseau	Le service Agent de protection d'accès réseau (NAP) recueille et gère les informations d'intégrit
Agent de stratégie IPsec	La sécurité du protocole Internet (IPSec) prend en charge l'authentification de l'homologue rése
Alimentation	Gère la stratégie d'alimentation et la remise de notification de stratégie d'alimentation.
Apache Tomcat 7.0 Tomcat7	Apache Tomcat 7.0.92 Server - https://tomcat.apache.org/
Appel de procédure distante (RPC)	Le service RPCSS est le Gestionnaire de contrôle des services pour les serveurs COM et DCOM. Il
Application d'assistance de la Console d'...	Permet aux administrateurs d'accéder à distance à une invite de commandes en utilisant les serv
Application système COM+	Gère la configuration et le suivi des composants de base COM+ (Component Object Model). Si

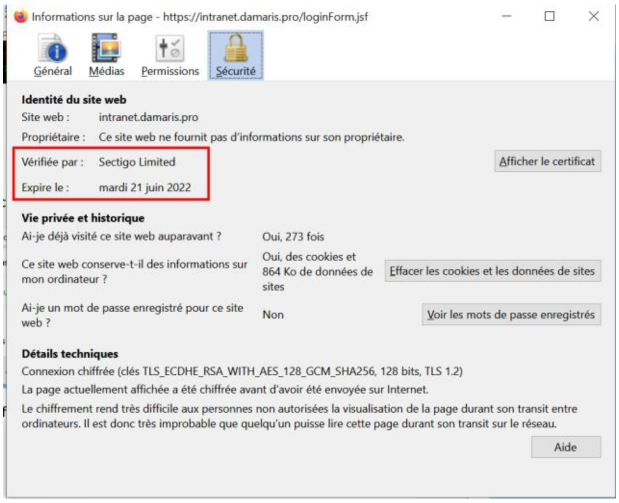
Test connection from a browser.

After accessing to web page, please click on key icon near URL.


https://intranet.damaris.pro/loginForm.jsf
Informations pour le site intranet.damaris.pro
Connexion sécurisée
Permissions
Ouvrir des fenêtres popup
Autoriser
Effacer les cookies et les données de sites…

Then, click on right arrow and "More information" button.

You will get this kind of window:



Informations sur la page - https://intranet.damaris.pro/loginForm.jsf

Identité du site web

Site web : intranet.damaris.pro

Propriétaire : Ce site web ne fournit pas d'informations sur son propriétaire.

Vérifiée par : Sectigo Limited

Expire le : mardi 21 juin 2022

Vie privée et historique

Ai-je déjà visité ce site web auparavant ? Oui, 273 fois

Ce site web conserve-t-il des informations sur mon ordinateur ? Oui, des cookies et 864 Ko de données de sites

Ai-je un mot de passe enregistré pour ce site web ? Non

Détails techniques

Connexion chiffrée (clés TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bits, TLS 1.2)

La page actuellement affichée a été chiffrée avant d'avoir été envoyée sur Internet.

Le chiffrement rend très difficile aux personnes non autorisées la visualisation de la page durant son transit entre ordinateurs. Il est donc très improbable que quelqu'un puisse lire cette page durant son transit sur le réseau.

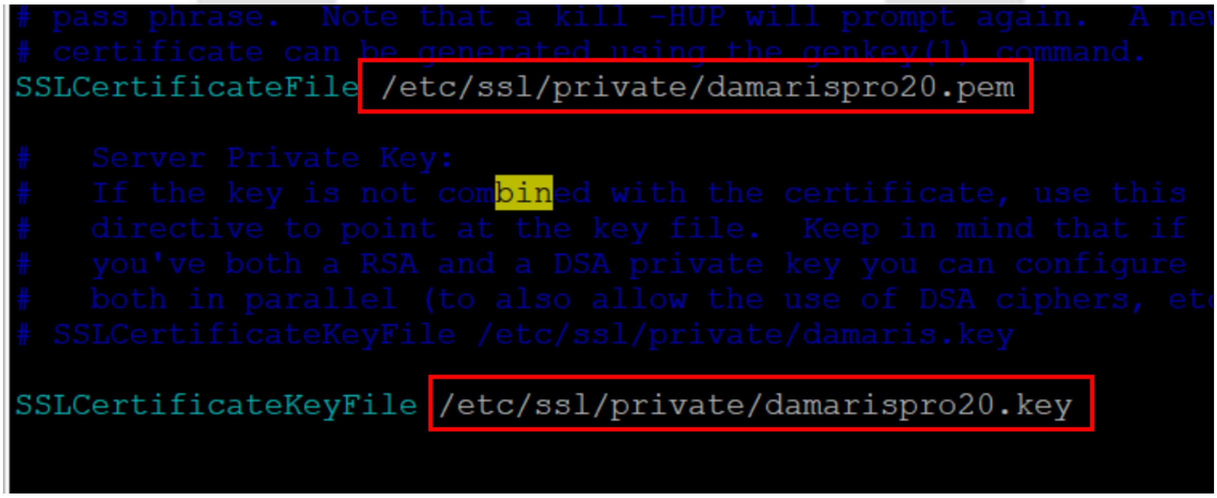
The most important information here is Expire date.

4.4 – LINUX APACHE

Please copy the following files in: /etc/ssl/private/

- damarispro20.pem
- damarispro20.key

Then, please modify the following file for Apache server: /etc/httpd/conf.d/ssl.conf

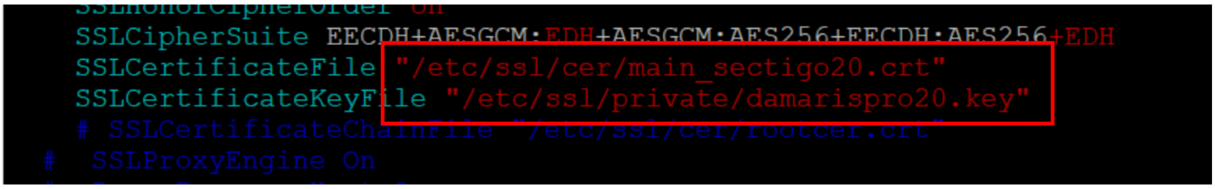


```
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/ssl/private/damarispro20.pem

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc
# SSLCertificateKeyFile /etc/ssl/private/damaris.key

SSLCertificateKeyFile /etc/ssl/private/damarispro20.key
```

If you use PHPBB (https://forum.damaris.pro) please modify also /etc/httpd/conf.d/forum.conf

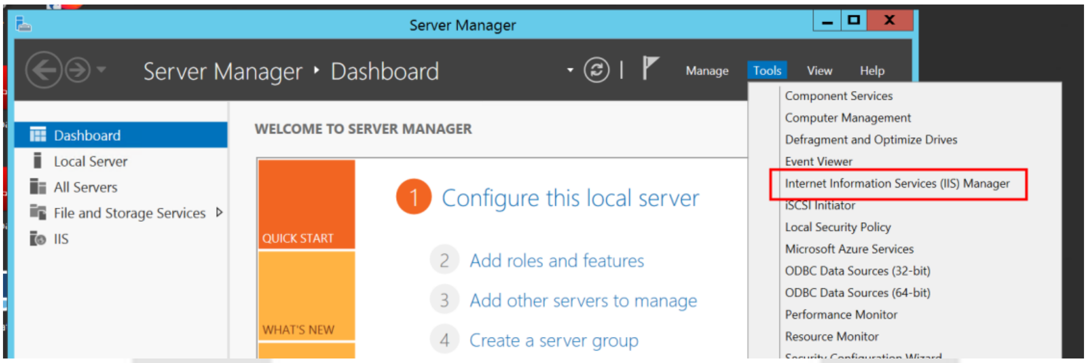


```
    SSLHonorCipherOrder on
    SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
    SSLCertificateFile "/etc/ssl/cer/main_sectigo20.crt"
    SSLCertificateKeyFile "/etc/ssl/private/damarispro20.key"
    # SSLCertificateChainFile "/etc/ssl/cer/rootcer.crt"
  #  SSLProxyEngine On
```

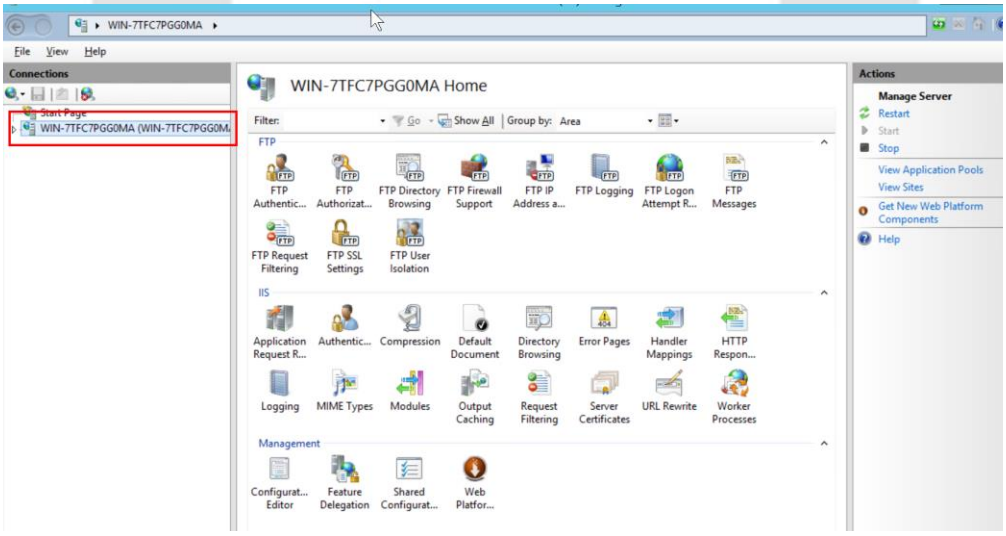
4.3 – WINDOWS IIS

To install a new certificate on a Windows IIS server, please copy the following file to the target server: damarisproxx.p12

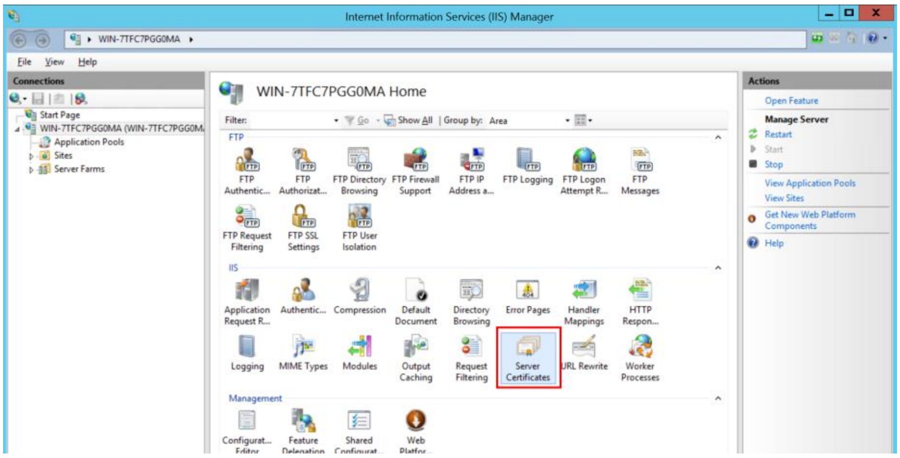
Then, please go to IIS configuration tool:


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
Component Services
Computer Management
Defragment and Optimize Drives
Event Viewer
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Resource Monitor
Security Configuration Wizard

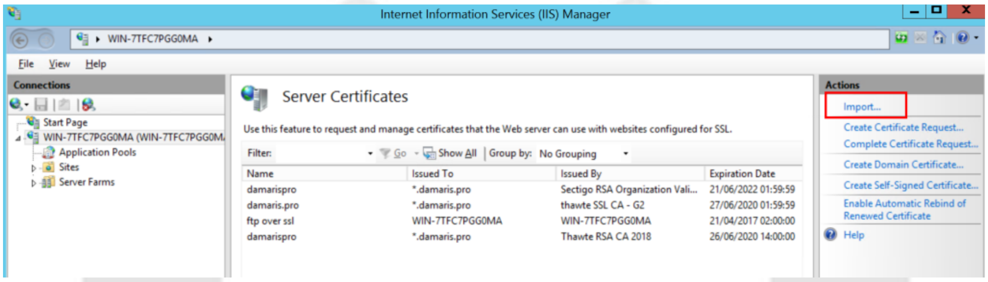
Please choose the Web server:



Choose server's Certificates by double clicking the icon:



Use the "Import" Action:


Internet Information Services (IIS) Manager
WIN-7TFC7PGG0MA
File View Help
Connections
Start Page
WIN-7TFC7PGG0MA (WIN-7TFC7PGG0MA
Application Pools
Sites
Server Farms
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help

Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

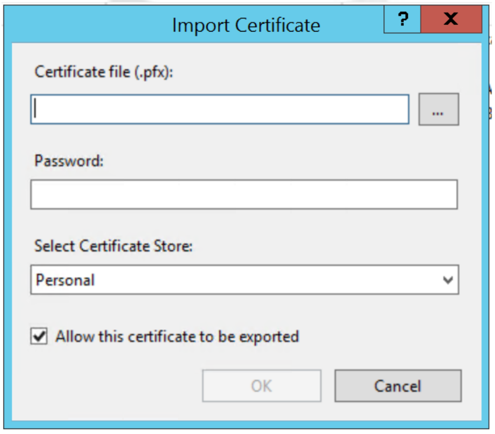
Filter: Go Show All | Group by: No Grouping

Name	Issued To	Issued By	Expiration Date
damarispro	*.damaris.pro	Sectigo RSA Organization Vali...	21/06/2022 01:59:59
damaris.pro	*.damaris.pro	thawte SSL CA - G2	27/06/2020 01:59:59
ftp over ssl	WIN-7TFC7PGG0MA	WIN-7TFC7PGG0MA	21/04/2017 02:00:00
damarispro	*.damaris.pro	Thawte RSA CA 2018	26/06/2020 14:00:00

In the popup, please Certificate file. You should indicate .p12 instead of .pfx.

You also need to know certificate's password.

Use "Personal" Store.



Import Certificate

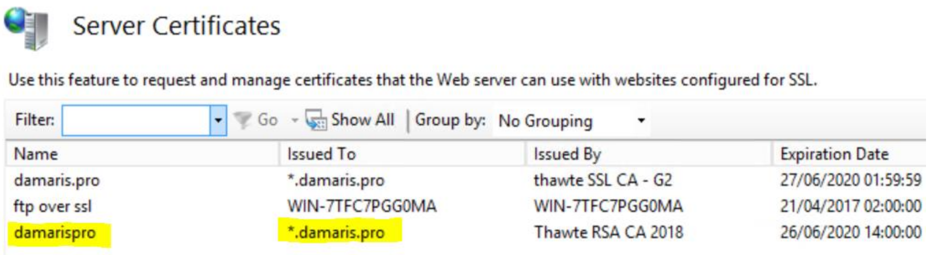
Certificate file (.pfx):

Password:

Select Certificate Store: Personal

☑ Allow this certificate to be exported

You will find the new certificate in the list:



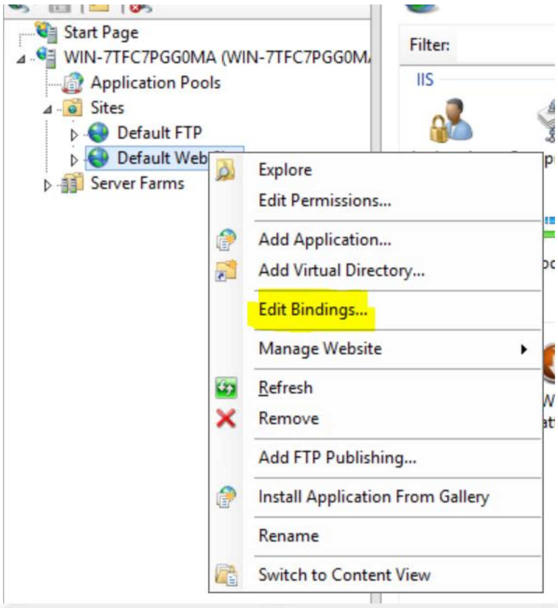
Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter: Go Show All | Group by: No Grouping

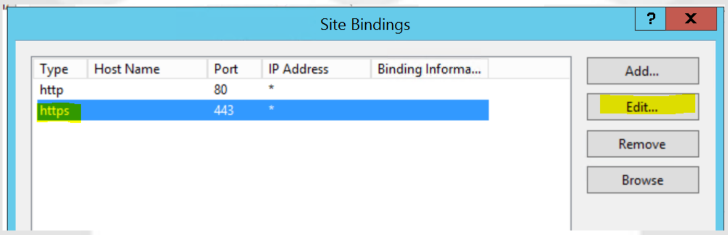
Name	Issued To	Issued By	Expiration Date
damaris.pro	*.damaris.pro	thawte SSL CA - G2	27/06/2020 01:59:59
ftp over ssl	WIN-7TFC7PGG0MA	WIN-7TFC7PGG0MA	21/04/2017 02:00:00
damarispro	*.damaris.pro	Thawte RSA CA 2018	26/06/2020 14:00:00

Go to the default Web server:



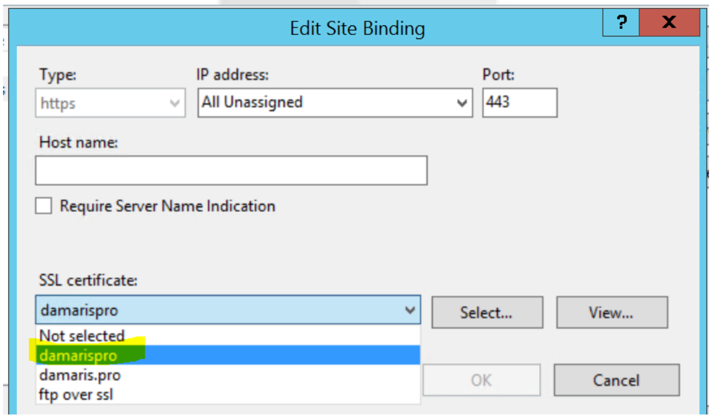
And edit its bindings.

Please select the https protocol and click on "Edit" button:


Site Bindings

Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	*	

Select the new certificate you installed on the server.


Edit Site Binding

Type: https

IP address: All Unassigned

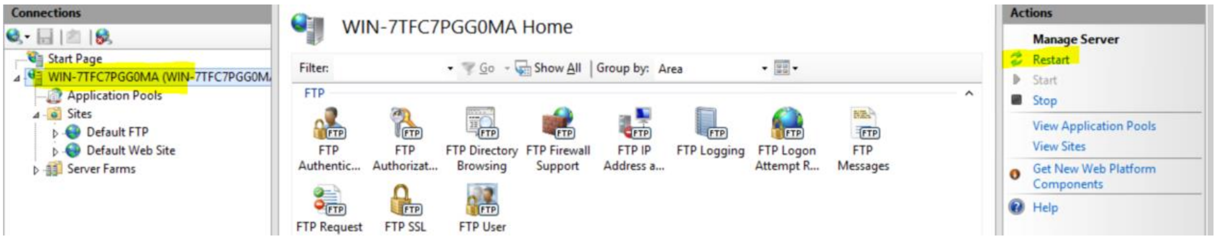
Port: 443

Host name:

□ Require Server Name Indication

SSL certificate: damarispro

To finish the setup, please restart IIS service:


Connections
Start Page
WIN-7TFC7PGG0MA (WIN-7TFC7PGG0M/
Application Pools
Sites
Default FTP
Default Web Site
Server Farms
WIN-7TFC7PGG0MA Home
Filter:
Go
Show All
Group by:
Area
FTP
FTP Authentic...
FTP Authorizat...
FTP Directory Browsing
FTP Firewall Support
FTP IP Address a...
FTP Logging
FTP Logon Attempt R...
FTP Messages
FTP Request
FTP SSL
FTP User
Actions
Manage Server
Restart
Start
Stop
View Application Pools
View Sites
Get New Web Platform Components
Help