WATCHDOC

FICHE PRATIQUE

Sécuriser Watchdoc / WSC à l'aide d'un certificat - Sécurisation https

DOXENSE Imprimez, respirez !

47, avenue de Flandre - 59290 Wasqhehal
65, rue de la Tombe Issoire - 75014 Paris

T +33 (0)3 62 21 14 00
www.doxense.com

Table des matières

Droits de reproduction

47, avenue de Flandre
59290 Wasquehal - FRANCE
contact@doxense.fr

Tel : +33(0)3.62.21.14.00
Fax : +33(0)3.62.21.14.01
www.doxense.fr

Watchdoc - Certificats - Sécuriser Watchdoc en https

Télécharger le .pdf

Principe

Watchdoc échange des informations avec différents périphériques (imprimantes, MFP, lecteurs de cartes) grâce à des interfaces telles que WSC, les WES, d'autres API (dont la Print API pour WPC et Skyprint) ainsi que la page "Mon compte".

Pour sécuriser ces pages accessibles via Internet, Watchdoc utilise le protocole TLS/SSL (via les ports 5744, 5753 et 5754) reposant sur des certificats auto-signés au format **.pfx**[1] (pkcs#12).

En tant qu'administrateur, vous pouvez gérer ces certificats (ou d'autres, signés par une autorité de certification) à l'aide de l'outil en ligne de commande Watchdoc Certificat Manager (WCM) présent par défaut dans le package d'installation Wathdoc.

Depuis la v. 6.1.0.5011, Watchdoc dispose d'une interface dédiée, plus simple à utiliser que l'outil WCM (cf. Gérer les certificats du serveur web).

La procédure suivante vous permet de sécuriser Watchdoc et WSC à l'aide de certificats fournis par votre autorité de certification.

Prérequis

Pour sécuriser Watchdoc, deux procédures sont possibles en fonction de la manière dont la D.S.I. souhaite procéder :

- vous générez une demande **CSR**[2] à l'aide de Watchdoc et demandez à la D.S.I. de votre organisation de signer le certificat ainsi obtenu. Dans ce cas, suivez

[1]Un fichier PKCS#12 ou .pfx est un fichier qui contient à la fois la clé privée et le certificat X.509. Il est prêt à être installé par le client sur des serveurs comme IIS, Tomkat ou Exchange. Avec un fichier PKCS#12, le client n'a plus à créer son propre CSR. Une autorité de certification s'en charge pour lui de manière entièrement sécurisée pendant le processus de demande de certificat. (Source : https://www.globalsign.com/fr/blog/fichier-pkcs12)

[2](Certificat Signing Request). Dans une infrastructure PKI (Public Key Infrastructure / Infrastructure à Clés Publiques), une demande de signature de certificat (en anglais CSR pour Certificate Signing Request) est un message envoyé à partir d'un demandeur à une autorité de certification afin de demander un certificat d'identité numérique. Le format le plus commun pour les CSR est la spécification PKCS#10.

toutes les étapes de la procédure décrite ci-dessous ;
- la D.S.I. de votre organisation vous fournit un certificat au format .pfx destiné à sécuriser Watchdoc et ses modules. Dans ce cas, suivez la procédure à partir de l'étape Activer le certificat .pfx sur WSC.

Par ailleurs, vérifiez que vous disposez bien des droits d'accès et d'utilisation aux deux outils suivants:
- Microsoft Active Directory Certificat Manager (Microsoft AD CS), rôle de serveur Windows permettant d'émettre et de gérer des certificats numériques dans un environnement Active Directory. Droit nécessaire si vous devez générer une demande CSR ;
- l'outil en ligne de commande Watchdoc Certificate Manager (WCM), disponible par défaut dans (C:\Program Files\Doxense\Watchdoc\wcm.exe).

Générer un certificat PFX avec WCM et Microsoft AD CS

Générer un CSR à l'aide de WCM

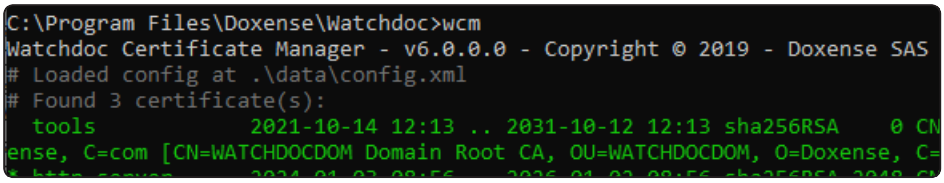
> Durant cette étape (2 min. environ), le service Watchdoc doit être arrêté. La page "Mon compte" n'est donc plus disponible.
> Et si le serveur fait office de serveur d'impression, le service d'impression n'est plus disponible non plus.

Pour cette première étape de création d'un certificat, il est important de réfléchir à l'url utilisée pour accéder à vos interfaces : souhaitez-vous utiliser le nom du serveur ou un alias ?

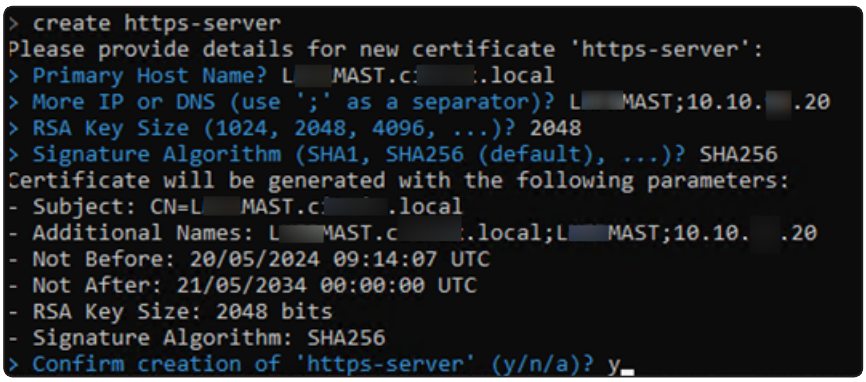
Pour générer le CSR, utilisez l'outil en ligne de commandes WCM (Watchdoc Certificate Manager) développé par Doxense.
Pour le lancer :
1. sur le serveur Watchdoc, en tant qu'administrateur, exécutez l'invite de commande Windows ;
2. placez-vous dans le dossier où Watchdoc est installé (C:\Program Files\Doxense\Watchdoc par défaut) ;
3. stoppez le service Watchdoc en saisissant la commande `net stop watchdoc` :

```
C:\Program Files\Doxense\Watchdoc>net stop watchdoc
The Watchdoc service is stopping....
The Watchdoc service was stopped successfully.
```

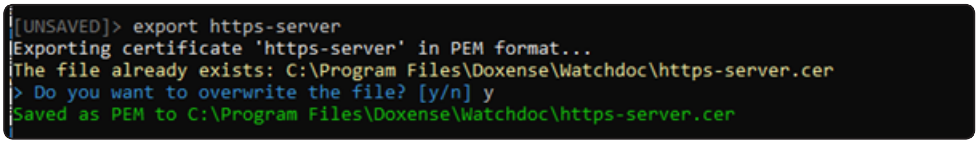
4. lancez l'outil wmc en saisissant la commande `wcm` :



5. créez le certificat du serveur https en saisissant la commande `create https-server` (n'oubliez pas le "s" de "https") et fournissez les informations suivantes :
   - **Primary host Name?** : indiquez le FQDN du serveur sur lequel vous vous trouvez ;
   - **More IP or DNS** (use ';' as a separator)? saisissez les IP de tous les serveurs qui vont utiliser ce certificat en les séparant par un point-virgule (par exemple : MASTERONE;127.0.0.1;localhost;watchdocadmin.domain.local;autres Alias;…)
   - **RSA key Size:** indiquez la taille de la clé de chiffrement RSA utilisée (par exemple 2048) ;
   - **Signature Algorithm:** indiquez l'algorithme de hashage utilisé (par exemple SHA256) ;
6. Après avoir vérifié le résumé de la commande, confirmez son exécution par la commande **y**
   Notez que la date d'expiration ne peut pas dépasser la date de validation du domaine.
   Notez également que les autorités de sécurité recommandent de changer les certificats tous les ans :

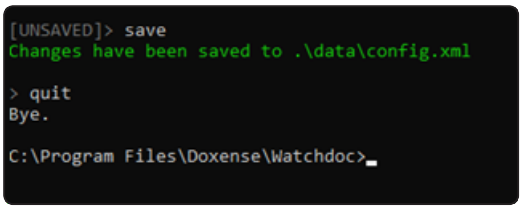


7. une fois le certificat signé, exportez-le en saisissant la commande **`export https-server`** :

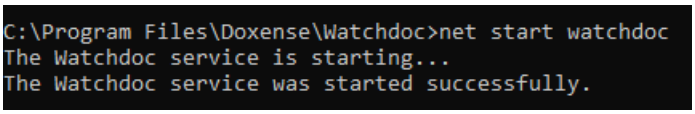


➔ par défaut, le certificat signé (.cer) est exporté dans le dossier C:\Program Files\Doxense\Watchdoc\. Vous aurez besoin de connaître l'emplacement de ce fichier pour la suite de la procédure.

8. sauvegardez les tâches réalisées en saisissant la commande **`save`** :

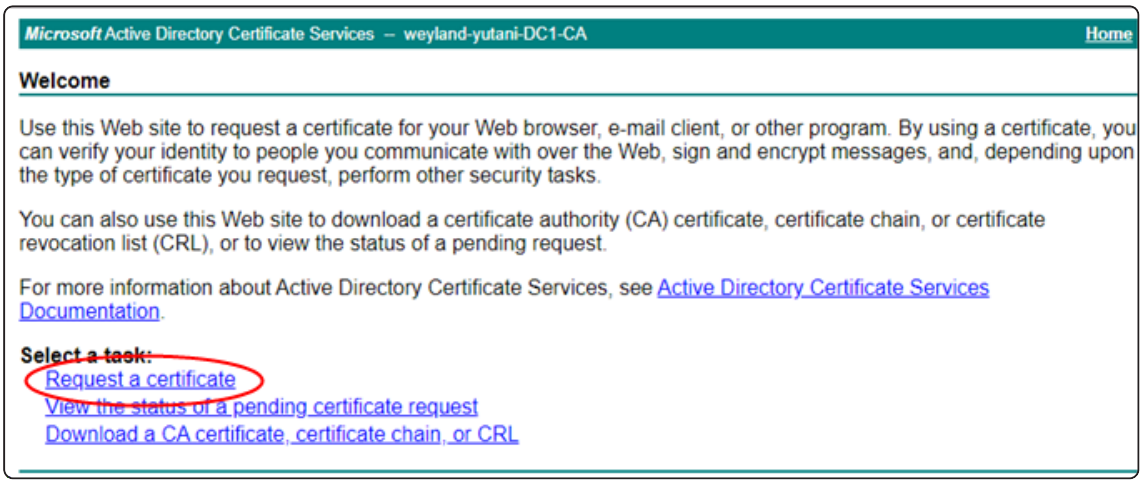


9. La sauvegarde effectuée, redémarrez Watchdoc en saisissant la commande **`net start watchdoc`** :

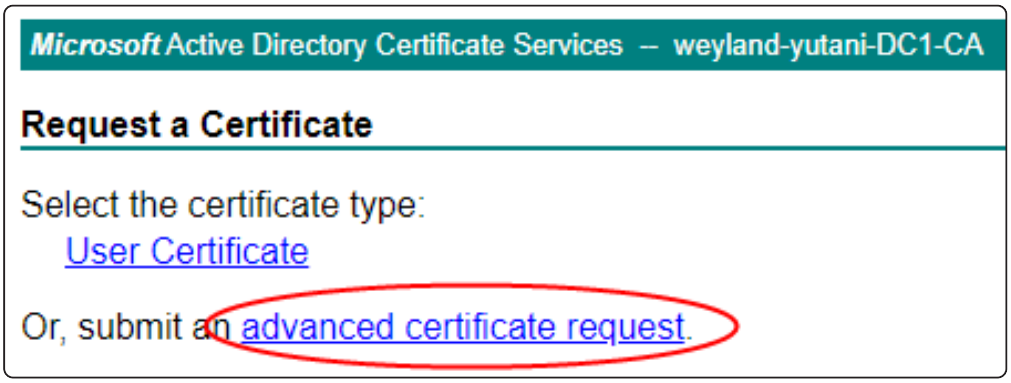


Faire valider le CSR par le domaine avec Microsoft AD CS[1]

1. Depuis un espace d'où le fichier .cer précédemment généré est accessible, lancez un navigateur avec un compte administrateur du domaine (compte ayant le droit de gestion des certificats) ;
2. dans ce navigateur, saisissez l'adresse permettant d'accéder au contrôleur de domaine (exemple : http://adresseDC/certsrv) ;
   ➔**Microsoft Active Directory Certificate Services** s'affiche :
3. dans la section **Select a task,** cliquez sur **Request a certificate** :



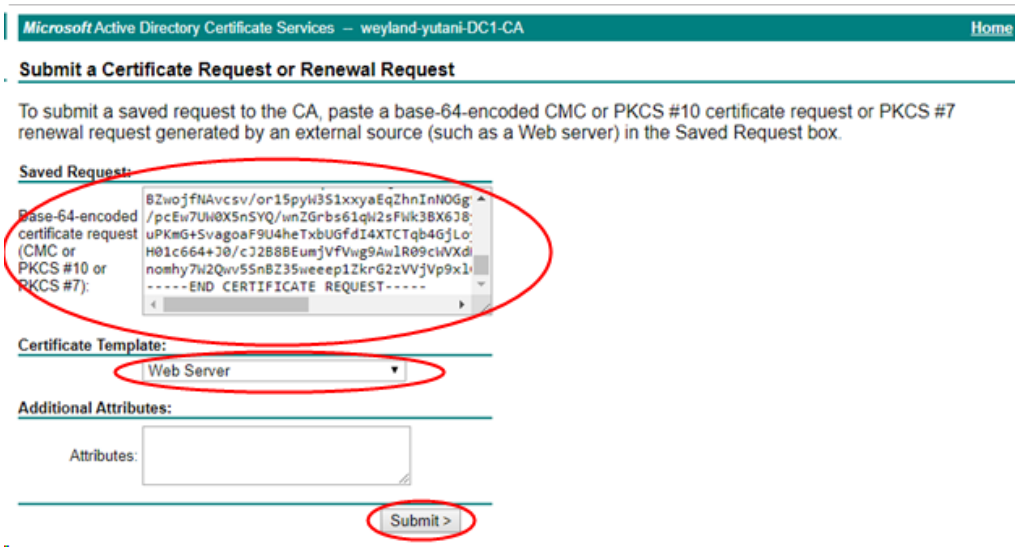
4. dans l'interface **Request a Certificate**, cliquez sur **advanced certificate request** :



5. ouvrez le fichier .csr dans un éditeur de texte et copiez-le ;
6. dans l'interface **Submit a Certificate Request or Renewal Request**, dans la zone de saisie **Saved Request**, collez le contenu du .csr en base 64 ;
7. dans la section **Certificate Template**, dans la liste déroulante, sélectionnez **Web Server** ;

[1]Microsoft Active Directory Certificate Services / Service de certificats Active Directory est un rôle Windows Server pour l'émission et la gestion des certificats d'infrastructure à clé publique (PKI) utilisés dans les protocoles de communication et d'authentification sécurisés. (Source : https://learn.microsoft.com)

8. cliquez sur **Submit** :



9. dans l'interface **Certificate Issued**, cochez le bouton-radio **Base 64 encoded** ;
10. cliquez ensuite sur **Download certificate** :

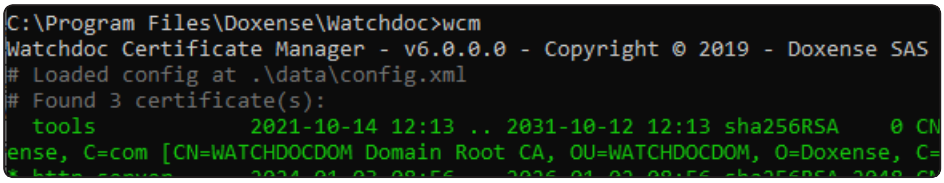
11. Sauvegardez le certificat signé téléchargé(extension .cer).

> Ne pas cliquer sur **Download certificate chain.**

Compléter et exporter le certificat

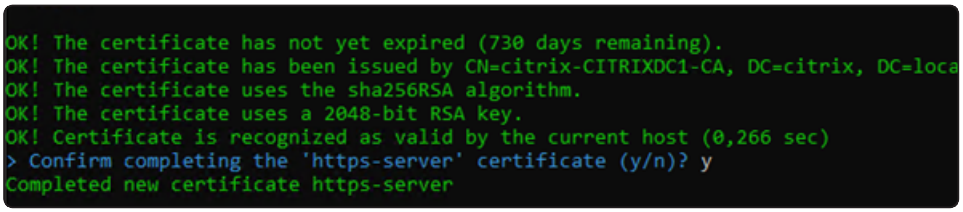
Pour compléter le certificat, utilisez WCM. Pour le lancer :

1. exécutez l'invite de commande Windows en tant qu'administrateur ;
2. placez-vous dans le dossier où Watchdoc est installé (C:\Program Files\Doxense\Watchdoc par défaut) ;
3. lancez l'outil WMC en saisissant la commande `wcm`:

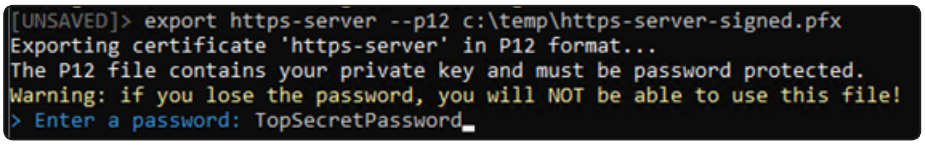


4. saisissez la commande **complete http-server <chemin vers votre certificat>** en indiquant le chemin vers le dossier dans lequel a été exporté le fichier .cer lors de la précédente étape :

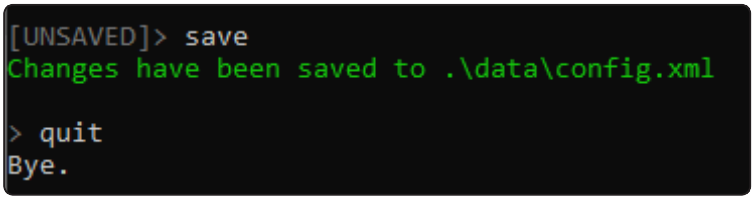
5. Si le certificat est bien validé, le message **OK! Certificate is recognized OK! Certificate is recognized as valid by the current host (0,266 sec)** s'affiche ;
6. Confirmez en saisissant la commande **y** :



7. Exportez ensuite le certificat en saisissant la commande **Export https-server -p12 c:\[chemind'export]** (indiquez le chemin du dossier dans lequel vous souhaitez enregistrer le certificat) ;
8. saisissez un mot de passe permettant de sécuriser le certificat :



9. Vérifiez dans le dossier de sauvegarde que le certificat (fichiers .pfx) s'y trouve bien. Il peut alors être activé sur WSC et Watchdoc.
10. Sauvegardez avec la commande **save** :
puis quittez l'outil WMC à l'aide de la commande **quit** ;



Activer le certificat .pfx sur WSC

Editer le fichier de configuration WSC

Pour compléter le certificat, utilisez WCM. Pour le lancer :

1. exécutez l'invite de commande Windows en tant qu'administrateur ;
2. placez-vous dans le dossier où WSC est installé (C:\Program Files\Doxense\Supervision par défaut) ;
3. stoppez le service WSC en saisissant la commande `net stop WatchdocTelemetryServer` :

```
C:\Program Files\Doxense\Watchdoc>net stop WatchdocTelemetryServer
The WatchdocTelemetryServer service is stopping.
The WatchdocTelemetryServer service was stopped successfully.
```

4. lancez l'outil WMC en saisissant la commande `wcm` :
5. saisissez la commande `-config` puis indiquez l'emplacement du fichier de configuration de la console de supervision (par défaut "c:\Program Files\Doxense\Supervision\data\wts_config.xml") :

```
C:\Program Files\Doxense\Watchdoc>wcm --config "c:\Program Files\Doxense\Supervision\data\wts_config.xml"
Watchdoc Certificate Manager - v6.0.0.0 - Copyright © 2019 - Doxense SAS
# Loaded config at c:\Program Files\Doxense\Supervision\data\wts_config.xml
# Found 1 certificate(s):
* http-server      2021-10-24 20:54 .. 2023-10-24 20:54 sha256RSA 1024 CN=LMFRMAST.citrix.local, OU=IT, O=DOXENSE,
LE, S=NORD, C=FR [CN=citrix-CITRIXDC1-CA, DC=citrix, DC=local]
```

Importer un certificat dans WSC

1. saisissez la commande`import http-server <emplacement_certificat>` `-password` en précisant l'emplacemenet où a été enregistré le fichier .pfx et le mot de passe saisi lorsque le certificat a été complété (cf. Compléter et exporter le certificat).
   (Attention ce n'est pas https-server **mais http -server**) :

```
> import http-server c:\temp\https-server-signed.pfx --password TopSecretPassword
Certificate 'http-server' already exists!
> Confirm replacing 'http-server' with a new certificate (y/n)? y
Showing details for imported certificate 'http-server'
[Version]
```

2. Saisissez la commande `Save` pour sauvegarder la configuration :

```
Configuration has been changed! Don't forget to 'save' or 'reload'
[UNSAVED]> save
Changes have been saved to c:\Program Files\Doxense\Supervision\data\wts_config.xml

> quit
Bye.
```

3. Redémarrez le service Console de supervision en saisissant la commande `net start WatchdocTelemetryServer` :

```
C:\Program Files\Doxense\Watchdoc>net start WatchdocTelemetryServer
The WatchdocTelemetryServer service is starting.....
The WatchdocTelemetryServer service was started successfully.
```

Valider le certificat

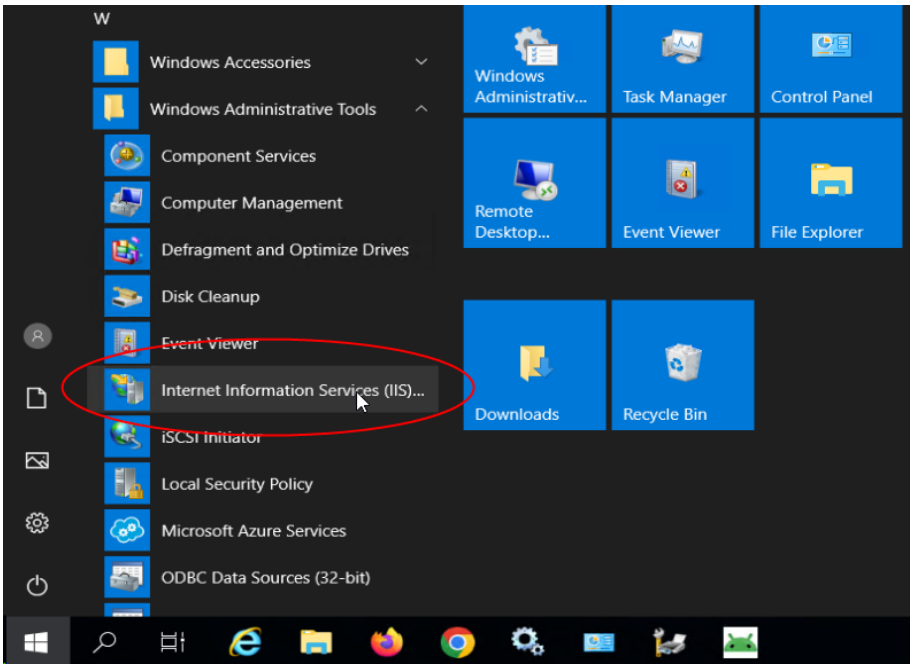
1. Depuis un poste de travail, à l'aide d'un navigateur, saisissez l'adresse de la Console de supervision (nom du serveur ou alias, selon ce qui a été déclaré dans le CSR) en HTTPS sur le port 5756.
2. Vérifiez qu'un cadenas apparait à côté de l'url et que vous n'avez aucun message d'alerte.
   Si c'est le cas, cela signifie que le site est sécurisé.

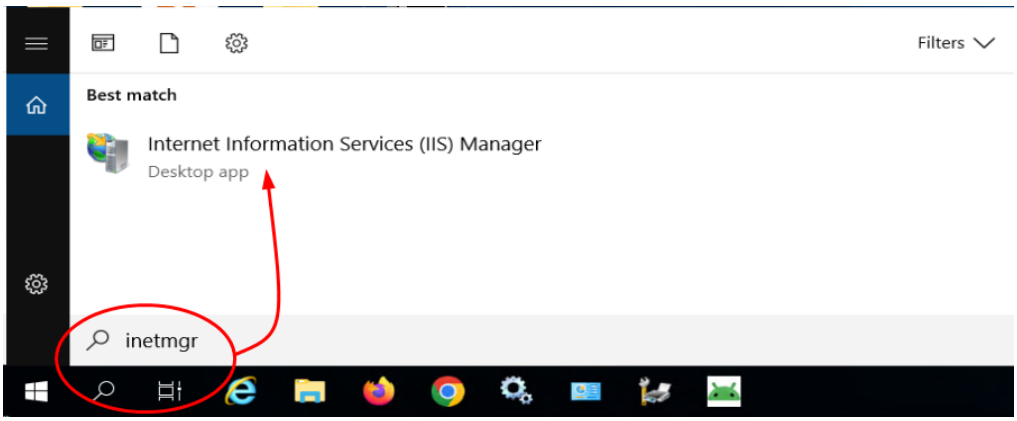
Activer le certificat PFX sur Watchdoc

Accéder au certificat dans

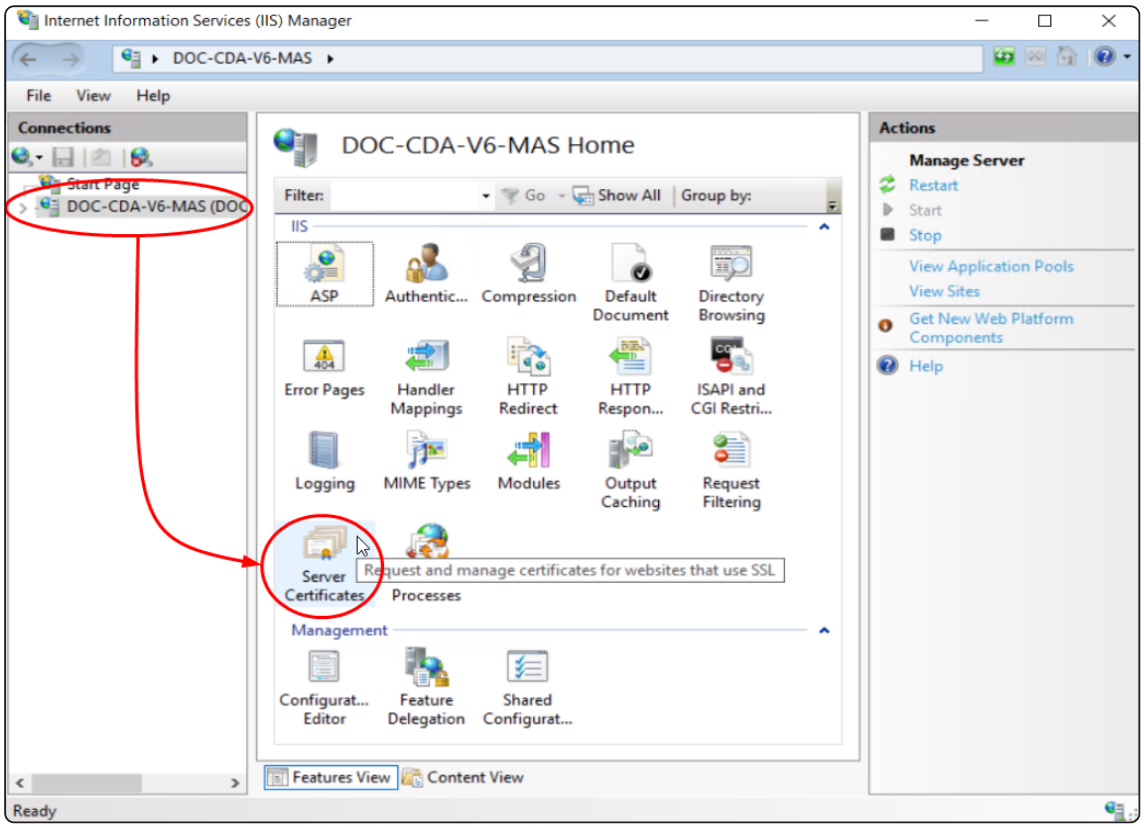
Watchdoc utilise Microsoft IIS pour la gestion de son site web. Il convient donc d'utiliser IIS services manager pour activer le certificat .pfx sur Watchdoc :

1. sur le serveur Watchdoc, en tant qu'administrateur, ouvrez IIS services manager depuis le menu (ou exécutez **inetmgr**depuis l'outil de rechercher MS Windows) :

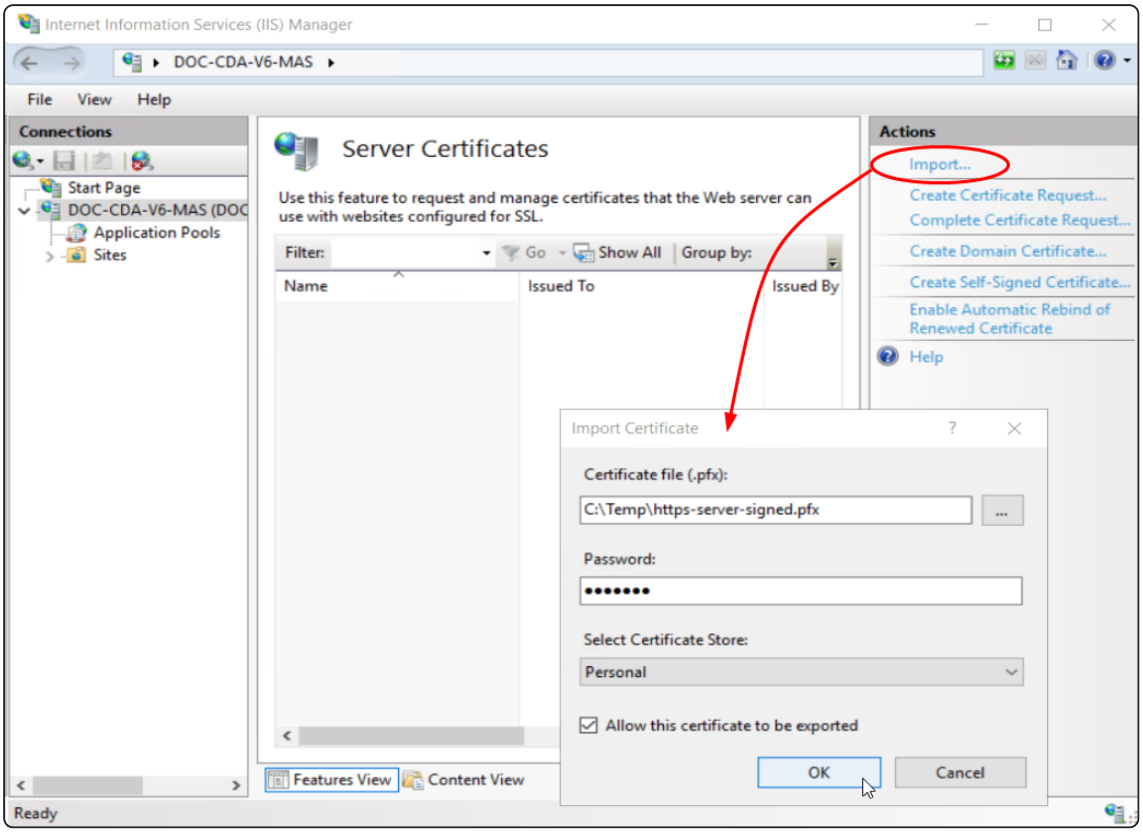




2. Sélectionnez le serveur Watchdoc dans la liste **Connections** ;
3. dans la liste des fonctions, sélectionnez **Server certificates** :

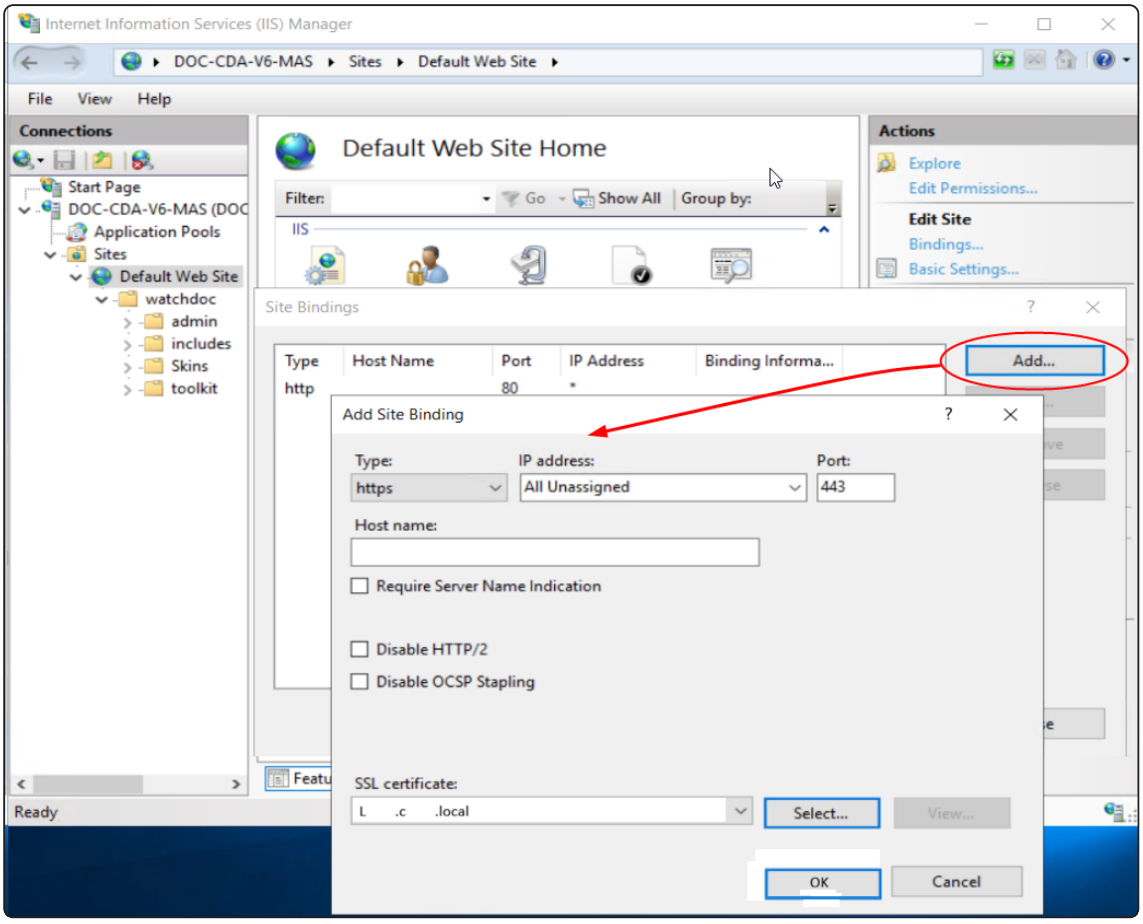


4. dans l'interface **Server Certificates**, dans la liste des **Actions**, cliquez sur **Import** :
5. parcourez ensuite l'espace de travail pour y sélectionner le fichier .pfx qui y a été enregistré ;
6. complétez le champ **Password** en saisissant le mot de passe défini pour le certificat ;
7. cliquez sur **OK** pour valider l'import :



➔le certificat apparaît alors dans la liste des certificats disponibles pour ce serveur web.

8. dans le menu **Connection**, sélectionnez le **Web Site** qui héberge Watchdoc (par défaut **Default Web Site**) :
9. dans la liste des options, cliquez sur **Edit Site** > **Bindings**
10. si le type **https** n'apparaît pas dans la liste, cliquez sur **Add** ;
11. dans l'interface **Add Site Binding**, indiquez :
    - type : https
    - IP address : All unassigned
    - Port : 443
    - SSL Certificate : sélectionnez le certificat précédemment ajouté :



Valider le certificat PFX sur Watchdoc

1. Depuis un poste de travail, à l'aide d'un navigateur, saisissez l'adresse de Watchdoc (nom du serveur ou alias, selon ce qui a été déclaré dans le CSR) en HTTPS.
2. Vérifiez qu'un cadenas apparait à côté de l'url et que vous n'avez aucun message d'alerte.
   Si c'est le cas, cela signifie que le site est sécurisé.
3. Cette vérification effectuée, supprimez le fichier .pfx là où il est enregistré car il contient le secret du certificat.