

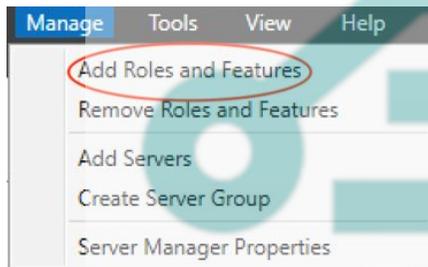
# ADCS (Active Directory Certificate Services) 2016

## Introduction

L'Active Directory Certificate Services (AD CS) est un rôle de Windows Serveur lié à l'active directory qui a pour but de créer, gérer des certificats numériques au sein du système informatique de l'entreprise.

## Installation et configuration

- Pour débiter l'installation, il faut se rendre dans le "Server Manager"
- Dans l'onglet "Manage" sélectionner "Add Roles and Features"



- Sélectionner le serveur sur lequel vous souhaitez installer l'ADCS
- Sélectionner "Active Directory Certificate Services"

### Roles



- Cliquer sur "Next" plusieurs fois
- Sélectionner les services : "Certification Authority" et "Certification Authority Web Enrollment"

Select the role services to install for Active Directory Certificate Services

Role services

- Certification Authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Certification Authority Web Enrollment
- Network Device Enrollment Service
- Online Responder

Description

Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.

- Pour le service “Certification Authority Web Enrollment” le Web Server Role (IIS) est nécessaire.

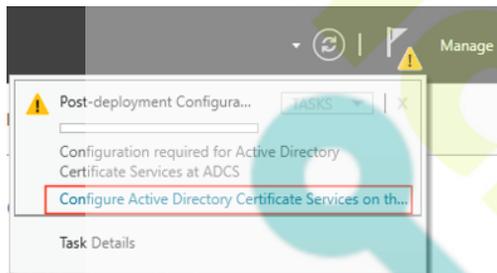
Select the role services to install for Web Server (IIS)

Role services

- ▲  Web Server
  - ▲  Common HTTP Features
    - Default Document
    - Directory Browsing
    - HTTP Errors
    - Static Content
    - HTTP Redirection
    - WebDAV Publishing
  - ▲  Health and Diagnostics
    - HTTP Logging
    - Custom Logging
    - Logging Tools
    - ODBC Logging
    - Request Monitor
    - Tracing
  - ▲  Performance
    - Static Content Compression
    - Dynamic Content Compression
  - ▲  Security

- Terminer en cliquant sur “Install”
- Une fois l’installation terminée, il faut passer à la configuration de l’Active Directory Certificate Services”

- Sélectionner “configure Active Directory Certificate Services”



- Dans la partie “Credentials” entrer l'utilisateur en charge de l'administration du service.
- Sélectionner les services : “Certification Authority” et “Certification Authority Web Enrollment”

Select Role Services to configure

- Certification Authority
- Certification Authority Web Enrollment
- Online Responder
- Network Device Enrollment Service
- Certificate Enrollment Web Service
- Certificate Enrollment Policy Web Service

- Sélectionner “Entreprise CA”

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

- Enterprise CA  
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.
- Standalone CA  
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

- Sélectionner Root CA

#### Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

- Root CA  
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.
- Subordinate CA  
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

- Sélectionner “Create a new private key” pour générer une nouvelle clé privée.

#### Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

- Create a new private key  
Use this option if you do not have a private key or want to create a new private key.
- Use existing private key  
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

- Choisir un fournisseur de chiffrement, la longueur de la clé et l’algorithme qui sera utilisé pour signer les certificats délivrés par l’Autorité de Certificat.

#### Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider	Key length: 2048
Select the hash algorithm for signing certificates issued by this CA: SHA256 SHA384 SHA512 SHA1 MD5	
<input type="checkbox"/> Allow administrator interaction when the private key is accessed by the CA.	

- Spécifier le nom de votre CA (Autorité de Certificat)

#### Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA: exemple-ADCS-CA
Distinguished name suffix: DC=exemple,DC=com
Preview of distinguished name: CN=exemple-ADCS-CA,DC=exemple,DC=com

- Choisir la durée de validité des certificats générés par la CA.

#### Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):

5	Years
---	-------

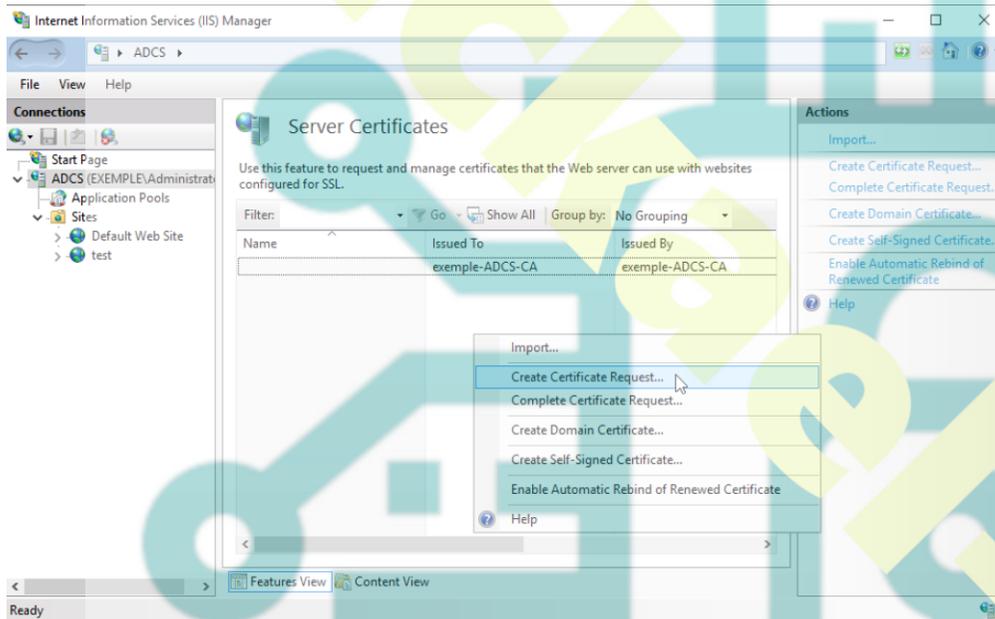
CA expiration Date: 9/11/2023 4:32:00 PM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

- Spécifier le chemin d'accès pour la base de données des certificats.
- Cliquer sur "Configurer" pour lancer la configuration de L'ADCS comprenant les paramètres précédemment ajoutés.
- L'installation et la configuration des deux Services sont terminés.

## Utilisation du service "Certification Authority Web Enrollment"

- Ouvrir votre IIS (Internet Information Service) Manager.
- Sélectionner "Create Certificate Request" pour faire la demande de certificat



- Remplir les informations en liens avec votre site et votre entreprise.

**Distinguished Name Properties**

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	<input type="text" value="test.exemple.com"/>
Organization:	<input type="text" value="Société"/>
Organizational unit:	<input type="text" value="IT"/>
City/locality:	<input type="text" value="Lille"/>
State/province:	<input type="text" value="ILE-DE-FRANCE"/>
Country/region:	<input type="text" value="FR"/>

- Sélectionner un fournisseur de chiffrement et la “Bit Length”.

Request Certificate



### Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider:

Microsoft RSA SChannel Cryptographic Provider

Bit length:

2048

- Enregistrer le texte fichier généré sur le bureau.

Request Certificate



### File Name

Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request:

C:\Users\Administrator\Desktop\demande\_de\_certificat.txt



- Utiliser le navigateur, et accéder au site <http://adcs/certsrv> . Rentrer l'identifiant et mot de passe du compte de gestion de l'ADCS.

- Sur la page, dans SELECT A TASK, sélectionner “Request a certificate”
- Puis sélectionner “Submit an advanced certificate request”

### Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

- Sélectionner “Submit a certificate request by using a base-64-encoded....”

### Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

[Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal](#)

- Coller l'intégralité du fichier texte généré précédemment, puis sélectionner la template “Web Server” et enfin cliquer sur Submit.

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #7 renewal request generated by an external source (such as a Request box).

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
IzmLFGIGjbcBUDEVeS+dyHst3mo/ZQp3LBvKg3d1:
7BHqIDqy1Ugo0Rj3gLNLsphF75PrKY1bIQDavVhc:
x0yZScLmTwRkmqRkXt5+bzHz5K1Pt8ku8Dg1zXR/!
NRax1JqzMeLf3BFWJv0/Z7CwaH3tbkPo
-----END NEW CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

- Télécharger le certificat en cliquant sur “Download certificate”

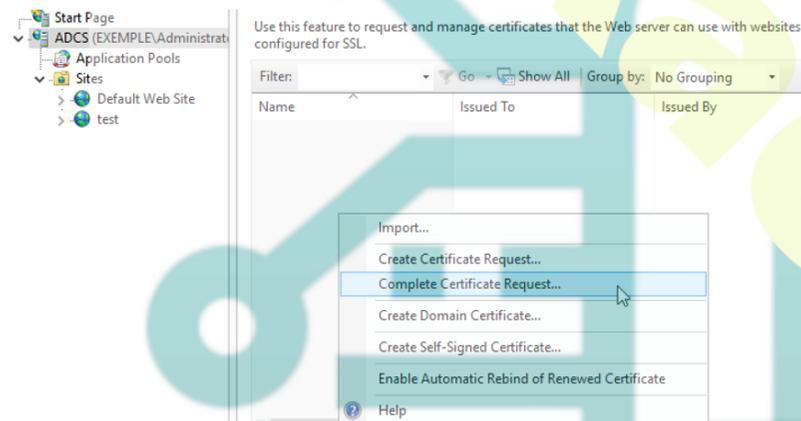
### Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

 [Download certificate](#)  
[Download certificate chain](#)

- Aller dans L'IIS Manager du serveur hébergeant le futur site web. Sélectionner “Complete Certificate Request”.



- Entrer le chemin d'accès au certificat et un nom pour celui-ci.

### Complete Certificate Request

 **Specify Certificate Authority Response**

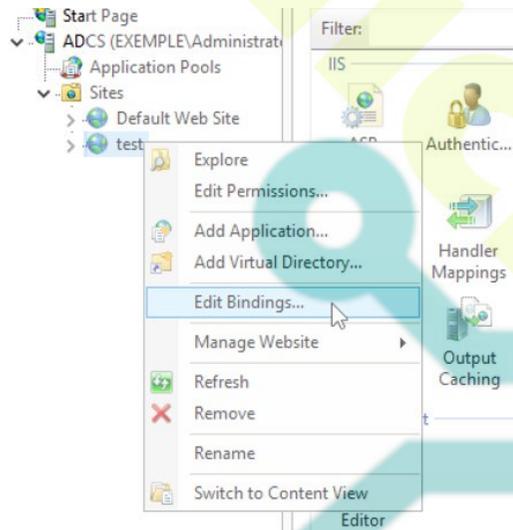
Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:  
 ...

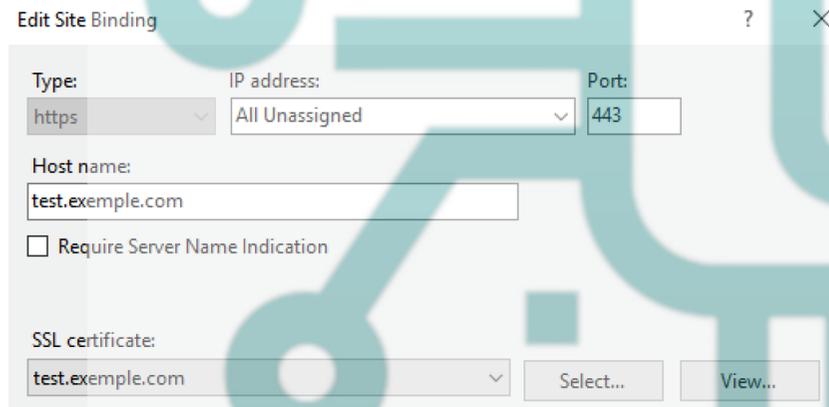
Friendly name:

Select a certificate store for the new certificate:

- Cliquer sur “Edit Bindings”



- Sélectionner le certificat SSL ajouté à l'étape précédente dans la liste déroulante.



- Un redémarrage du serveur web peut être nécessaire pour que la configuration soit prise en compte.