



WLC : Mise en place d'un certificat

>>> Installation d'un certificat délivré par une autorité de certification.

Description :

Le but de cet article est d'expliquer comment générer un CSR depuis le contrôleur wifi, de générer un certificat via une autorité de certification sous Windows Serveur et installer le certificat afin d'obtenir une interface web d'administration du contrôleur wifi en HTTPS avec un certificat signé.

WLC : Mise en place d'un certificat

>>> **Installation d'un certificat délivré par une autorité de certification.**

Sommaire :

- I) Introduction
 - II) Certificat Racine
 - 1) Vérification du certificat
 - 2) récupération du certificat racine
 - 3) Conversion du certificat racine
 - 4) Installation du certificat racine
 - 5) Vérification du certificat
 - 6) Vérification de l'heure
 - III) Générer le CSR
 - IV) Générer et signer le certificat
 - 1) Générer le certificat
 - 2) Conversion du certificat
 - 3) Installation du certificat
 - V) Vérification du certificat
-

I) Introduction

Je ne vais pas rappeler comment fonctionne le fonctionnement des certificats, déjà expliqué dans l'article 292.

Voici le résumer de la procédure :

1. Vérifier le certificat en place sur le contrôleur
2. Récupérer le certificat racine de l'autorité de certification
3. Convertir le certificat racine
4. Installer le certificat racine sur le contrôleur
5. Vérifier qu'il est bien installé
6. Générer une demande CSR
7. Générer un certificat sur l'autorité de certification
8. Convertir le certificat
9. Installer le certificat

Informations : Le contrôleur wifi, ne supporte que les certificats de type PEM. Une autorité de certification Windows ne sait malheureusement pas générer de tel certificats. Il vous faudra donc installer OpenSSL sur votre serveur Windows ou sur votre PC afin de convertir les certificats dans le format demandé.

II) Certificat Racine

1) Vérification du certificat

Nous commençons donc par vérifier le certificat en place.

- Connectez-vous sur la page d'administration du contrôleur Wifi.
- Cliquez sur **"Management"** dans la barre du haut.
- Puis cliquez sur **"HTTP-HTTPS"** dans le menu de gauche.
- Vous pouvez observer que le certificat actuel est au nom de Cisco Systems avec un CN "169.254.1.1".

The screenshot shows the Cisco WLC Management interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT (highlighted), COMMANDS, HELP, and FEEDBACK. The left sidebar shows a tree view with categories like Management, Summary, SNMP, HTTP-HTTPS (selected), IPSEC, Telnet-SSH, Serial Port, Local Management Users, User Sessions, Logs, Mgmt Via Wireless, Cloud Services, Software Activation, and Tech Support. The main content area is titled 'HTTP-HTTPS Configuration' and lists various settings with dropdown menus: HTTP Access (Disabled), HTTPS Access (Enabled), WebAuth SecureWeb (Enabled), HTTPS Redirection (Enabled), Web Session Timeout (30 Minutes), 2-Factor Authentication (Disabled), and Last Login Information Display (Disabled). Below this is the 'Current Certificate' section, which displays details for the 'bsnSslWebadminCert': Type (3rd Party), Serial Number (292021E8), Validity (From Oct 11 00:00:01 2020 GMT to Oct 11 00:00:01 2030 GMT), Subject Name (C=US, O=Cisco Systems Inc., OU=DeviceSSL (WebAdmin), CN=169.254.1.1), Issuer Name (C=US, O=Cisco Systems Inc., OU=DeviceSSL (WebAdmin), CN=169.254.1.1), MD5 Fingerprint (db:32:17:a3:53:6e:ce:ad:bb:f5:9d:0e:ae:65:df:65), and SHA1 Fingerprint (c5:25:f4:e0:ab:28:15:8a:76:30:ab:c0:4f:61:ea:99:7b:c4:36:ed). There is a checkbox for 'Download SSL Certificate' and a note stating '* Controller must be rebooted for the new certificate to take effect.' A footer note mentions '1. Controller must be rebooted for the WebAuth SecureWeb configuration change to take effect.'

2) récupération du certificat racine

Nous allons maintenant récupérer le certificat racine depuis l'autorité de certification.

- Connectez-vous à l'interface WEB de l'autorité pour moi : "http://ad.idum.local/certsrv/" et authentifiez-vous avec un compte ayant les droits de générer les certificats.

ad.idum.local/certsrv/

- Cliquez sur **"Télécharger un certificat d'autorité de certification, une chaîne de certificats ou une liste de révocation des certificats"**.

The screenshot shows the Microsoft Active Directory Certificate Services (CA-INTRA) website. The header includes 'Services de certificats Microsoft Active Directory -- CA-INTRA' and a 'Accueil' link. The main content area is titled 'Bienvenue !' and contains the following text: 'Utilisez ce site Web pour demander un certificat pour votre navigateur Web, votre programme client de messagerie électronique ou un autre programme. En utilisant un certificat, vous pouvez confirmer votre identité aux personnes avec lesquelles vous communiquez sur le Web, signer et chiffrer des messages et, selon le type de certificat que vous demandez, effectuer d'autres tâches sécurisées.' Below this, it states: 'Vous pouvez également utiliser ce site Web pour télécharger un certificat d'autorité de certification, une chaîne de certificats ou une liste de révocation des certificats, ou vous pouvez afficher le statut d'une requête en attente.' At the bottom, it says: 'Pour obtenir plus d'informations sur les Services de certificats Active Directory, voir [Documentation sur les Services de certificats Active Directory](#).' The page also includes a section 'Sélectionnez une tâche :' with three links: 'Demander un certificat', 'Afficher le statut d'une requête de certificat en attente', and 'Télécharger un certificat d'autorité de certification, une chaîne de certificats ou une liste de révocation des certificats'.

- Sélectionnez le certificat, sélectionnez la méthode DER, et cliquez sur "**Télécharger la chaine de certificats d'autorité de certification**".

Services de certificats Microsoft Active Directory – CA-INFRA Accueil

Télécharger un certificat d'autorité de certification, une chaîne de certificats ou la liste de révocation des certificats

Pour approuver les certificats approuvés par l'autorité de certification, [Installer ce certificat d'autorité de certification](#)

Pour sélectionner un certificat d'autorité de certification, une chaîne de certificats ou une liste de révocation des certificats, sélectionnez un certificat et une méthode de chiffrement.

Certificat de l'autorité de certification :

Actuel [CA-INFRA]

méthode de codage :

☒ DER
☐ Base 64

[Installer un certificat d'autorité de certification](#)
[Télécharger un certificat de l'autorité de certification](#)
[Télécharger la chaîne de certificats d'autorité de certification](#)
[Télécharger la dernière Liste de révocation des certificats de base](#)
[Télécharger la dernière Liste de révocation des certificats delta](#)

3) Conversion du certificat racine

Comme expliqué dans l'introduction, le contrôleur wifi ne supporte que le format PEM. Il faut donc convertir le certificat racine de P7B en PEM.

- Installez "**OpenSSL**" sur votre PC.
- Puis tapez la commande ci-dessous pour convertir le certificat racine.

```
OpenSSL> pkcs7 -in C:\Certs\CA-root-infra-local.p7b -inform DER -print_certs -text -out C:\Certs\CA-root-infra-local.pem
```

```
OpenSSL> pkcs7 -in C:\Certs\CA-root-infra-local.p7b -inform DER -print_certs -text -out C:\Certs\CA-root-infra-local.pem
```

4) Installation du certificat racine

- Retournez sur la page d'administration du contrôleur Wifi.
- Cliquez sur "**Commands**" dans le menu du haut.
- Cliquez sur "**Download File**".
- Sélectionnez :
 - Le file type : "**Vendor CA Certificate**"
 - Le type de transfert que vous souhaitez
 - L'adresse IP du serveur TFTP ou FTP
 - Le chemin
 - Et le nom du fichier PEM
- Cliquez sur "**Download**".

CISCO Save Configuration | Ping | Logout | Refresh

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | **COMMANDS** | HELP | FEEDBACK User: admin(ReadWrite) | Home

Commands

[Download File](#)
[Upload File](#)
[Reboot](#)
[Restart](#)
[Config Boot](#)
[Scheduled Reboot](#)
[Reset to Factory Default](#)
[Set Time](#)
[Login Banner](#)

Download file to Controller

File Type

Vendor CA Certificate

Transfer Mode

TFTP

Server Details

IP Address(Ipv4/Ipv6)

172.16.1.69

Maximum retries (1 to 254)

10

Timeout (1 to 254 seconds)

6

File Path

/

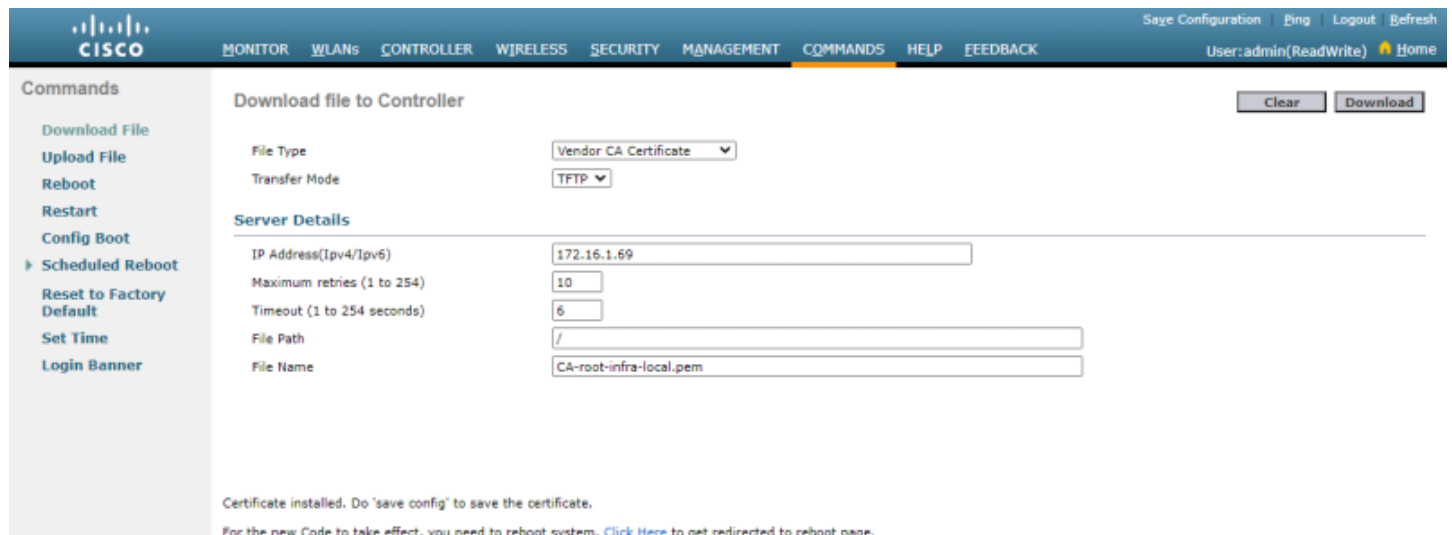
File Name

CA-root-infra-local.pem

Clear

Download

- Si l'opération se déroule bien, le contrôleur vous demandera de redémarrer.



Commands

- Download File
- Upload File
- Reboot
- Restart
- Config Boot
- Scheduled Reboot
- Reset to Factory Default
- Set Time
- Login Banner

Download file to Controller

File Type: Vendor CA Certificate

Transfer Mode: TFTP

Server Details

IP Address(Ipv4/Ipv6): 172.16.1.69

Maximum retries (1 to 254): 10

Timeout (1 to 254 seconds): 6

File Path: /

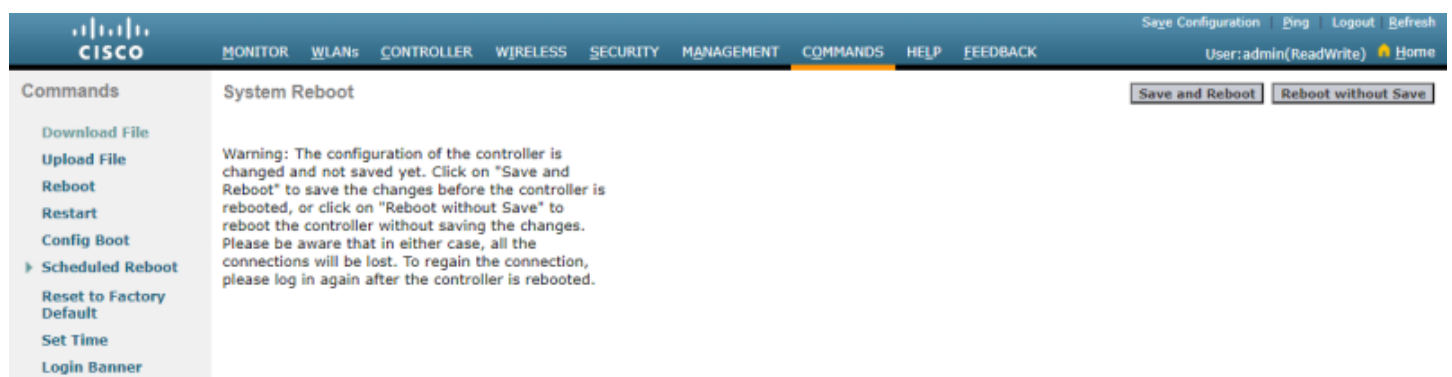
File Name: CA-root-infra-local.pem

Clear Download

Certificate installed. Do 'save config' to save the certificate.

For the new Code to take effect, you need to reboot system. [Click Here](#) to get redirected to reboot page.

- Cliquez sur **"Save and Reboot"**



Commands

- Download File
- Upload File
- Reboot
- Restart
- Config Boot
- Scheduled Reboot
- Reset to Factory Default
- Set Time
- Login Banner

System Reboot

Save and Reboot Reboot without Save

Warning: The configuration of the controller is changed and not saved yet. Click on "Save and Reboot" to save the changes before the controller is rebooted, or click on "Reboot without Save" to reboot the controller without saving the changes. Please be aware that in either case, all the connections will be lost. To regain the connection, please log in again after the controller is rebooted.

5) Vérification du certificat

On vérifie que le certificat racine est bien en place.

- Cliquez sur **"Security"** dans la barre du haut.
- Cliquez sur **"Advanced"** dans le menu de gauche.
- Puis sur **"Vendor Certs"**
- Et enfin sur **"CA certificate"**
- Vous pouvez observer que le certificat est au nom de : **"DC=local, DC=idum, DC=infra, CN=CA-INFRA"**

CISCO MONITOR WLANs CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration Ping Logout Refresh User: admin(ReadWrite) Home

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Auth Cached Users
 - Fallback
 - DNS
 - Downloaded AVP
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
 - Advanced EAP
 - Priority Order
 - Certificate
 - Access Control Lists
 - Wireless Protection Policies
 - Web Auth
 - TrustSec
 - Local Policies
 - Umbrella
 - Advanced
 - CIDS
 - Sensors
 - Shunned Clients
 - Vendor Certs
 - CA Certificate
 - ID Certificate

CA Certification

IPSec Certificate [Delete IPSec Certificate](#)

Name: _____
 Serial Number: _____
 Valid: _____
 Subject Name: _____
 Issuer Name: _____
 Signature Algorithm: _____
 MD5 Fingerprint: _____
 SHA1 Fingerprint: _____

EAP Certificate

Name: bsnSslEapCaCert
 Serial Number: 31000000020B958756E32E66DC000000000002
 Valid: From Sep 26 15:40:35 2020 GMT To Sep 26 15:50:35 2022 GMT
 Subject Name: DC=local, DC=idum, DC=infra, CN=CA-INFRA
 Issuer Name: DC=local, DC=idum, CN=CA-IDUM
 Signature Algorithm: sha256WithRSAEncryption
 MD5 Fingerprint: e2:6e:5c:a6:1f:e9:fc:c6:73:30:18:d0:a7:25:a1:c0
 SHA1 Fingerprint: bc:10:d0:3f:82:4d:89:2c:47:ca:20:fb:8b:2c:77:e4:a6:ce:41:c7

6) Vérification de l'heure

Pour tout ce qui touche au certificat, l'heure des équipements sont important.

- Cliquez sur **"Commands"** en haut de la page.
- Cliquez sur **"Set Time"**.
- puis vérifiez le **"Current Time"** de votre contrôleur.

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY **COMMANDS** HELP FEEDBACK

Commands

- Download File
- Upload File
- Reboot
- Restart
- Config Boot
- Scheduled Reboot
- Reset to Factory Default
- Set Time
- Login Banner

Set Time

Current Time Fri Jan 6 00:21:18 2006

Date

Month
 Day
 Year

Time

Hour

III) Générer le CSR

Nous allons maintenant générer la demande de certificat.

- Cliquez sur **"Security"** en haut de la page.
- Cliquez sur **"Certificate"** sur la gauche.
- Puis sur **"CSR"**.
- Sélectionnez le type de certificat : **"CSR WebAdmin"**.
- Remplissez les champs.

- Et cliquez sur **"Generate"**.

The screenshot shows the Cisco Security configuration interface. The left sidebar contains a tree view with categories like AAA, Local EAP, Advanced EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth, TrustSec, Umbrella, and Advanced. The main area is titled 'CSR' and contains a form for generating a Certificate Signing Request. The form fields are: Certificate Type (dropdown: CSR WebAdmin), Country Code (text: FR), State (text: Loire-Atlantique), City (text: Nantes), Organization (text: IDUM), Department (text: Wireless), Common Name (text: wlc.idum.local), E-mail (text: n.salmon@idum.local), and Key Type (dropdown: RSA). A 'Generate' button is at the top right. Below the form, a note reads: 'Download CSR certificate file at Commands-> Upload File -> CSR Certificate once CSR is generated here.'

- Cliquez sur **"Commands"** en haut de la page.

- Puis sur **"Upload"** à gauche.

- Sélectionnez :

- Le type de fichier : **"CSR WebAdmin Certificate"**
- L'adresse IP
- Le chemin
- Le nom du fichier

- Puis cliquez sur **"Upload"**.

The screenshot shows the Cisco Commands configuration interface. The left sidebar contains a tree view with categories like Download File, Upload File, Reboot, Restart, Config Boot, Scheduled Reboot, Reset to Factory Default, Set Time, and Login Banner. The main area is titled 'Upload file from Controller' and contains a form for uploading a file. The form fields are: File Type (dropdown: CSR WebAdmin Certificate), Transfer Mode (dropdown: TFTP), IP Address(Ipv4/Ipv6) (text: 172.16.1.69), File Path (text: /), and File Name (text: CSRwebadmin.csr). 'Clear' and 'Upload' buttons are at the top right.

IV) Générer le certificat

1) Générer le certificat

- Retournez sur la page WEB de l'autorité de Certification.

- Cliquez sur **"Demander un Certificat"**.

Bienvenue !

Utilisez ce site Web pour demander un certificat pour votre navigateur Web, votre programme client de messagerie électronique ou un autre programme. En utilisant un certificat, vous pouvez confirmer votre identité aux personnes avec lesquelles vous communiquez sur le Web, signer et chiffrer des messages et, selon le type de certificat que vous demandez, effectuer d'autres tâches sécurisées.

Vous pouvez également utiliser ce site Web pour télécharger un certificat d'autorité de certification, une chaîne de certificats ou une liste de révocation des certificats, ou vous pouvez afficher le statut d'une requête en attente.

Pour obtenir plus d'informations sur les Services de certificats Active Directory, voir [Documentation sur les Services de certificats Active Directory](#).

Sélectionnez une tâche :[Demander un certificat](#)[Afficher le statut d'une requête de certificat en attente](#)[Télécharger un certificat d'autorité de certification, une chaîne de certificats ou une liste de révocation des certificats](#)

- Cliquez sur **"Soumettez une demande de certificat en utilisant un fichier CMC ou PKCS #10 codé en base 64, ou soumettez une demande en utilisant un fichier PKCS #7 codé en base 64."**

Demande de certificat avancée

La stratégie de l'autorité de certification détermine le type de certificats que vous pouvez demander. Cliquez sur l'une des options suivantes pour :

[Créer et soumettre une demande de requête auprès de cette autorité de certification.](#)[Soumettez une demande de certificat en utilisant un fichier CMC ou PKCS #10 codé en base 64 ou soumettez une demande en utilisant un fichier PKCS #7 codé en base 64.](#)

- Ouvrez dans un éditeur de texte le fichier CSR.
- Copiez tout le contenu.
- Collez le contenu dans la zone **"Demande enregistrée"**.
- Sélectionnez le modèle de Certificat.
- Ajoutez les attributs supplémentaires ci-dessous :

```
san:ipaddress=172.16.99.200&dns=wlc.idum.local&dns=wlc.infra.local
```

- Cliquez sur **"Envoyer"**

Pour résumer :

- Spécifiez l'adresse IP du contrôleur de la page administration.
- Spécifiez le nom DNS du contrôleur (nom qui sera utilisé dans le navigateur pour joindre la page d'administration du contrôleur).

Information : Dans mon cas le nom de domaine est idum.local, mais je possède aussi un sous-domaine infra.local

Soumettre une demande de certificat ou de renouvellement

Afin de soumettre une demande enregistrée à l'autorité de certification, collez une demande de certificat CMC ou PKCS #10 codé en base 64 ou une demande de renouvellement PKCS #7 générée par une source externe (telle qu'un serveur Web) dans la zone Demande enregistrée.

Demande enregistrée :

Base-64-encoded
Requête de certificat
(CMC ou
PKCS #10 ou
PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC0TCCBkCAQAwYsGTAxBgNVBAgHEExvaXJlLUF0bGdudG1xdWUxOzANBgNV
BACiMBk5b2R1czENPAsGA1UECgwsSURVTTERMA8GA1UECmV1Z2lyZ3VxL3h3ZAV
BgNVBA8wIDN5Yy5pZHVtLmVxY2FzPS15IAAY3KoZihvcNAQkBFhNuLnNhbG1vbkbBp
ZHVtLmVxY2FzPS15IAAY3KoZihvcNAQkBFhNuLnNhbG1vbkbBpZHVtLmVxY2FzPS15IAAY3KoZihvcNAQkBFhNuLnNhbG1vbkbBp
gYpXNn+fI28m5Jnflj+uy2tTYjxtH7XVNI2VKu/b8AusHRpeqsVy6YEqK/cc0PU2
pvIDBL3dg016seCLxjYdZaQ1pHprUeekOXdx7e3381IGR319Qu5+5Gc6XPgn/N
QP96cokC//8HErXq+P54tLVXGv365vqrzrCkOxH6p11D+KCKOG3Hf5+o1an9mFke
+gr6Lm60s8cpV37t+5N1T6gV7kUMDA4+uAEIY72pteztv6Tfay7k4cXje8viQ0/k
p2ekyyDt1fn51k+7bRLg9Nz1JzWfukFRuARCAIkTykxBMFzTkQeoqIUrZb5Kx4uq
CCBua3v5+hmoVQIDAQABoAAuQVY7KoZihvcNAQkBFhNuLnNhbG1vbkbBpZHVtLmVxY2FzPS15IAAY3KoZihvcNAQkBFhNuLnNhbG1vbkbBp
n/7zlnL7aL3Qw5MOLDc9T4hEfGUHVP/D9YIAh4Ydn6r2x16JzHe8UA5A1ehq+oB8
nuuUJAS/01TjWmU5u4x81bVxAS957pDAaz9zIdU3b9M3f3qDksUomYmZ07Gm98K6
N0Zw+kIdEKVnHHz1U0zDdzxEBAzWkTppzt980PnxY2Uo60EDX2RD7C8kF05xsKj
0TK1hnCOBwYVhFGHBFHdcHvX6TTxGdrCdro+SZFr25VfqaFjDPWzDz4RR32HpyH
7Pfp5FOxdzfkYvq35ZzONTpMz15g7tF5Sj1OcmV/18hrZ0p0K41keJw/xPBhCn
Ph3ARsc=
-----END CERTIFICATE REQUEST-----
```

Modèle de certificat :

IDUM Serveur Web

Attributs supplémentaires :

Attributs :

Envoyer >

- Sélectionnez la méthode DER, et cliquez sur "**Télécharger la chaîne de certificats**"

Certificat émis

Le certificat que vous avez demandé a été émis.

☒ Codé DER ou ☐ Codé en base 64



[Télécharger le certificat](#)

[Télécharger la chaîne de certificats](#)

2) Conversion du certificat

Comme précédemment, utilisez OpenSSL pour convertir le certificat P7B en PEM. Utilisez la commande suivante :

```
OpenSSL> pkcs7 -in C:\Certs\cert_webadmin.p7b -inform DER -print_certs -text -out C:\Certs\Cert_webadmin.pem
```

```
OpenSSL> pkcs7 -in C:\Certs\cert_webadmin.p7b -inform DER -print_certs -text -out C:\Certs\Cert_webadmin.pem
```

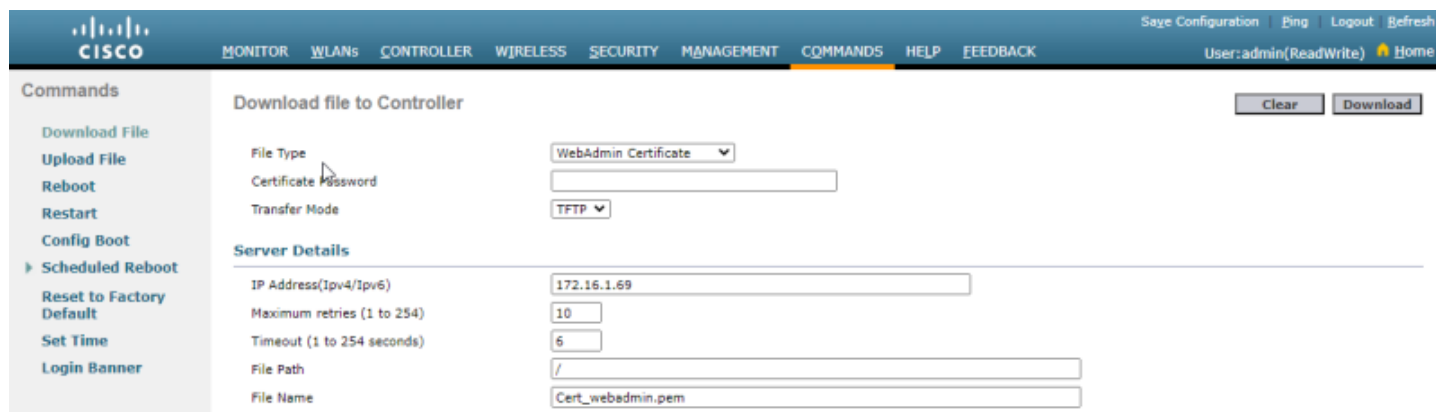
3) Installation du certificat

- Dans "**Commands**" en haut de la page, puis dans "**Download File**".

- Sélectionnez :

- Le file type : "**WebAdmin Certificate**"
- Le type de transfert que vous souhaitez
- L'adresse IP du serveur TFTP ou FTP
- Le chemin
- Et le nom du fichier PEM

- Cliquez sur "**Download**"

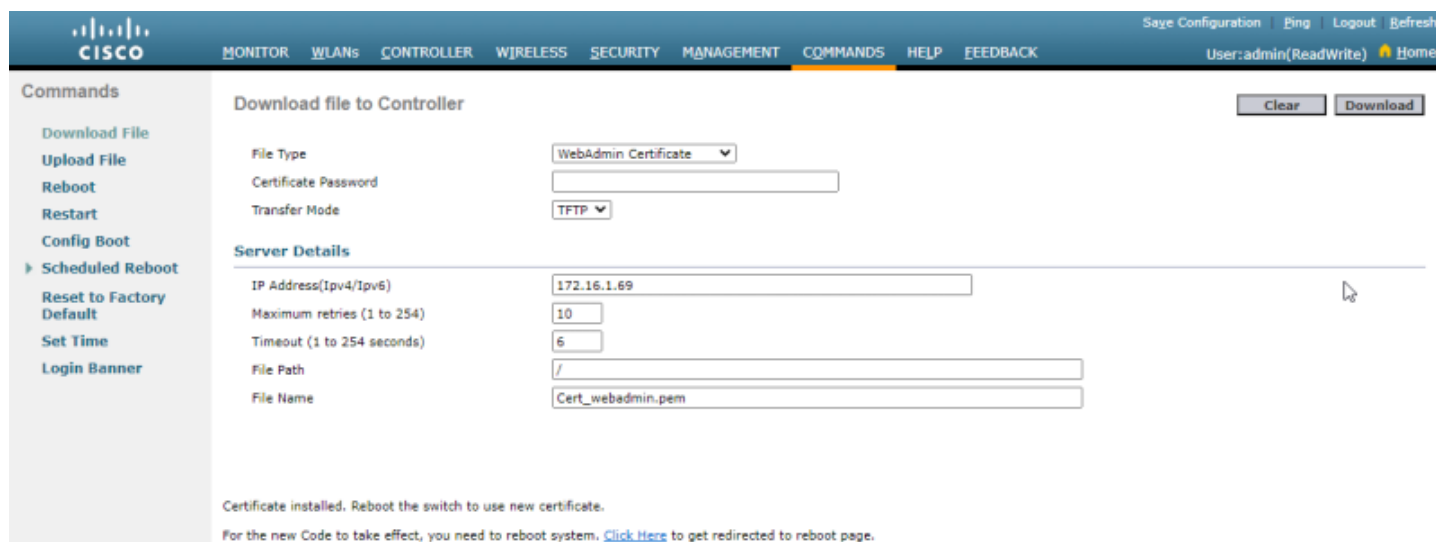


The screenshot shows the Cisco WLC Command Line Interface. The 'Commands' menu on the left includes 'Download File', 'Upload File', 'Reboot', 'Restart', 'Config Boot', 'Scheduled Reboot', 'Reset to Factory Default', 'Set Time', and 'Login Banner'. The 'Download file to Controller' form has the following fields:

- File Type: WebAdmin Certificate (dropdown)
- Certificate Password: (text input)
- Transfer Mode: TFTP (dropdown)
- Server Details:
 - IP Address(Ipv4/Ipv6): 172.16.1.69
 - Maximum retries (1 to 254): 10
 - Timeout (1 to 254 seconds): 5
 - File Path: /
 - File Name: Cert_webadmin.pem

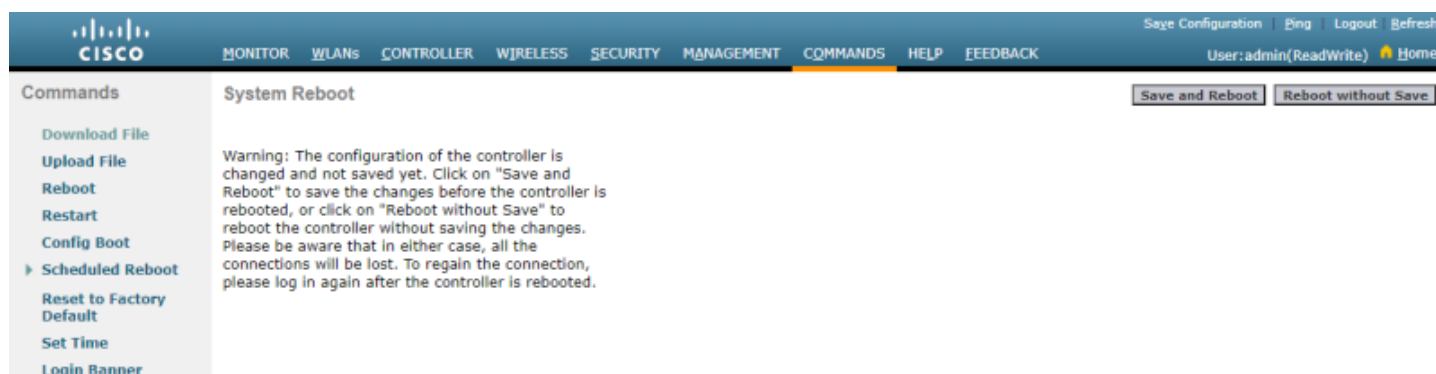
Buttons: Clear, Download

- Si l'opération se déroule bien, le contrôleur vous demandera de redémarrer.



The screenshot shows the same Cisco WLC Command Line Interface. The 'Download file to Controller' form is identical to the previous one. Below the form, a message states: 'Certificate installed. Reboot the switch to use new certificate. For the new Code to take effect, you need to reboot system. [Click Here](#) to get redirected to reboot page.'

- Cliquez sur "Save and Reboot"



The screenshot shows the Cisco WLC Command Line Interface. The 'System Reboot' form has the following fields:

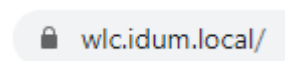
- Warning: The configuration of the controller is changed and not saved yet. Click on "Save and Reboot" to save the changes before the controller is rebooted, or click on "Reboot without Save" to reboot the controller without saving the changes. Please be aware that in either case, all the connections will be lost. To regain the connection, please log in again after the controller is rebooted.

Buttons: Save and Reboot, Reboot without Save

V) Vérification du certificat

Pour conclure cet article, la vérification pour valider que le certificat est bien installé :

- Attendez que le contrôleur Wifi ait redémarré.
- Fermer et rouvrez le navigateur sur la page administration.
- Vérifier que votre navigateur vous informe bien que le certificat est valide avec un cadenas.



- Cliquez dessus pour voir l'information "Certificat (valide)"

La connexion est sécurisée



Vos informations, comme vos mots de passe ou vos numéros de carte de paiement, sont privées lorsqu'elles sont transmises à ce site. [En savoir plus](#)



Certificat (Valide)

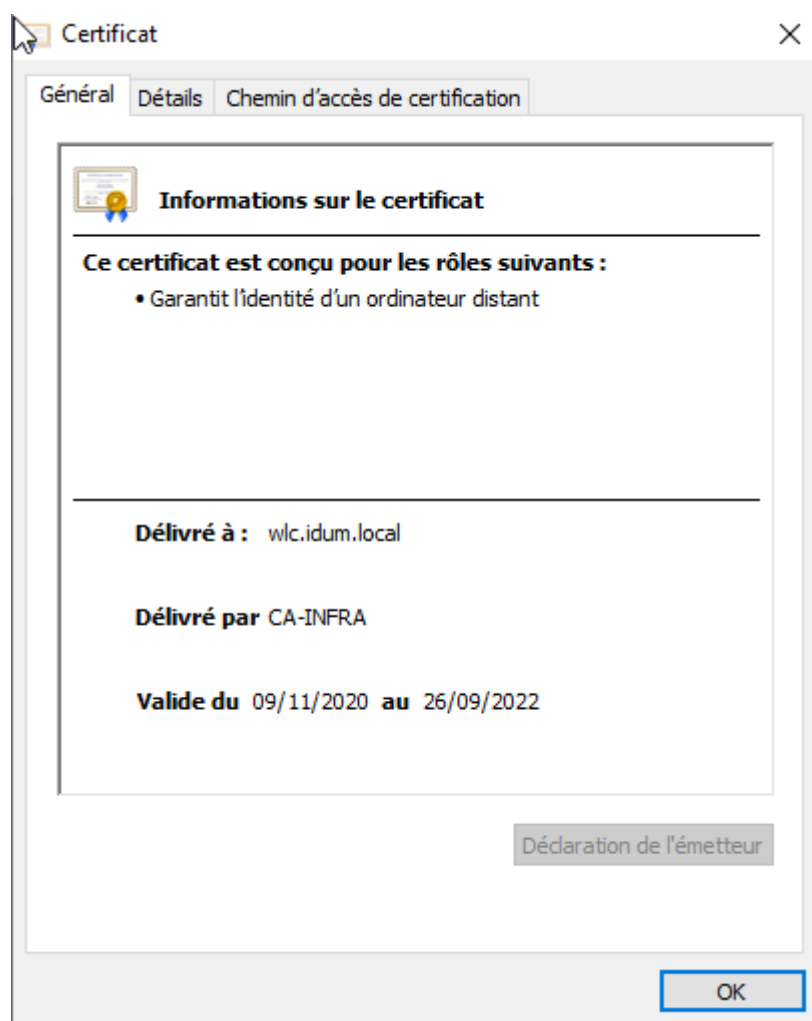


Cookies (0 en cours d'utilisation)



Paramètres de site

- Cliquez dessus afin de voir le détail et vérifier que le certificat est bien signé par votre autorité de certification.



- N'hésitez pas aussi à regarder dans le menu "**Management**" puis "**HTTP-HTTPS**"

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration Ping Logout Refresh

User: admin(ReadWrite) Home

Management

Summary

SNMP

HTTP-HTTPS

IPSEC

Telnet-SSH

Serial Port

Local Management Users

User Sessions

Logs

Mgmt Via Wireless

Cloud Services

Software Activation

Tech Support

HTTP-HTTPS Configuration

Apply Delete Certificate Regenerate Certificate

HTTP Access Disabled

HTTPS Access Enabled

WebAuth SecureWeb Enabled

HTTPS Redirection Enabled

Web Session Timeout 30 Minutes

2-Factor Authentication Disabled

Last Login Information Display Disabled

Current Certificate

Name: bsnSslWebadminCert

Type: 3rd Party

Serial Number: 1900000006FB850FF7B82A8EDF00000000006

Valid: From Nov 9 18:20:20 2020 GMT Until Sep 26 15:50:35 2022 GMT

Subject Name: ST=Loire-Atlantique, L=Nantes, O=IDUM, OU=Wireless, CN=wlc.idum.local, emailAddress=n.salmon@idum.local

Issuer Name: DC=local, DC=idum, DC=infra, CN=CA-INFRA

MD5 Fingerprint: 29:e2:09:e6:5e:67:24:a4:c0:62:5b:c3:e6:d8:2c:dc

SHA1 Fingerprint: 0c:7b:49:75:bf:4a:d6:4a:79:3c:a9:5d:5d:fe:d2:05:c2:74:bb:a8

☐ Download SSL Certificate

* Controller must be rebooted for the new certificate to take effect.

1. Controller must be rebooted for the WebAuth SecureWeb configuration change to take effect.

Il vous restera à faire la même chose pour le Webauth si vous l'utilisez.

Attention : N'oubliez pas que le certificat Racine doit être installé sur le PC afin de pouvoir authentifier et valider le certificat.

28 décembre 2020 -- N.Salmon -- article_353.pdf



Idum