Configurer l'inscription et le renouvellement automatiques des certificats via CAPF Online CA

Table des matières

Introduction

Ce document décrit l'inscription et le renouvellement automatiques des certificats via la fonction en ligne CAPF (Certificate Authority Proxy Function) pour Cisco Unified Communications Manager (CUCM).

Contribution de Michael Mendoza, ingénieur du centre d'assistance technique Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Solutions Cisco Unified Communications Manager
- Certificats X.509
- Windows Server
- Windows Active Directory (AD)
- Services Internet (IIS) Windows
- Authentification NT (nouvelle technologie) LAN Manager (NTLM)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CUCM version 12.5.1.10000-22
- Windows Server 2012 R2
- Téléphone IP CP-8865 / Firmware : SIP 12-1-1SR1-4 et 12-5-1SR2.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre lâ€™incidence possible des commandes.

Informations générales

Ce document couvre la configuration de la fonctionnalité et les ressources associées pour des recherches supplémentaires.

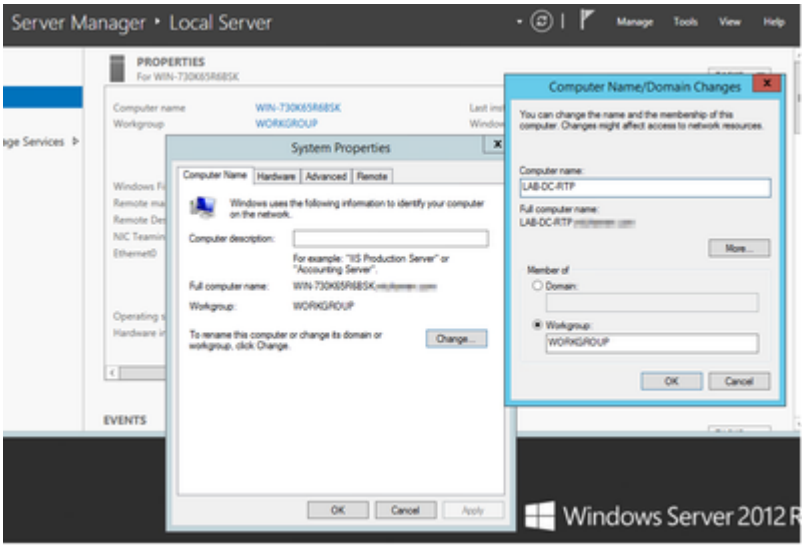
Valider la date et l'heure du serveur

Assurez-vous que le serveur Windows a la date, l'heure et le fuseau horaire corrects configurés car ils affectent les durées de validité du certificat de l'autorité de certification racine du serveur ainsi que les certificats émis par celui-ci.

Mettre à jour le nom du serveur

Par défaut, le nom d'ordinateur du serveur a un nom aléatoire tel que WIN-730K65R6BSK. La première chose à faire avant d'activer les services de domaine Active Directory est de vous assurer de mettre à jour le nom d'ordinateur du serveur avec ce que vous voulez que le nom d'hôte et le nom d'émetteur de l'autorité de certification racine du serveur soient à la fin de l'installation ; sinon, il faut beaucoup d'étapes supplémentaires pour modifier cela après l'installation des services Active Directory.

- Accédez à **Serveur local**, sélectionnez le nom de l'ordinateur pour ouvrir les **Propriétés système**
- Cliquez sur le bouton **Modifier** et tapez le nouveau nom de l'ordinateur :



- Redémarrez le serveur pour appliquer les modifications

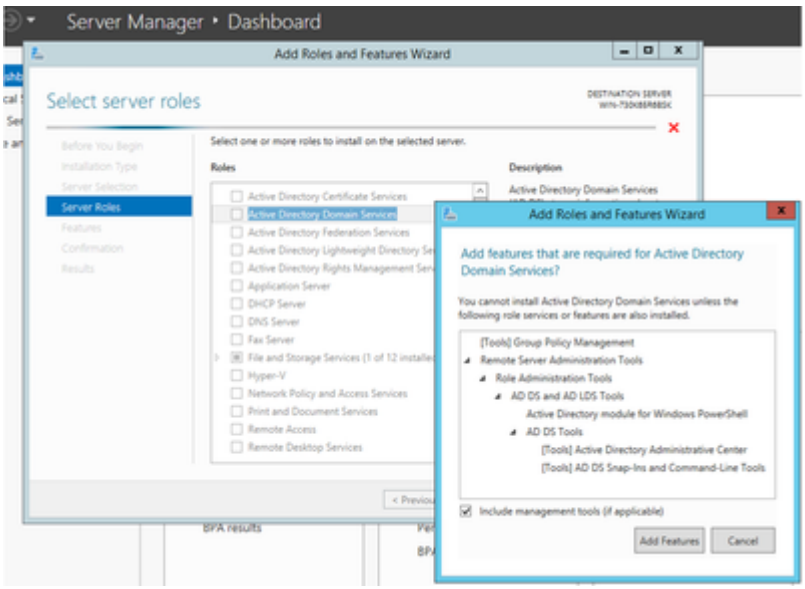
Configurer

Services AD, utilisateur et modèle de certificat

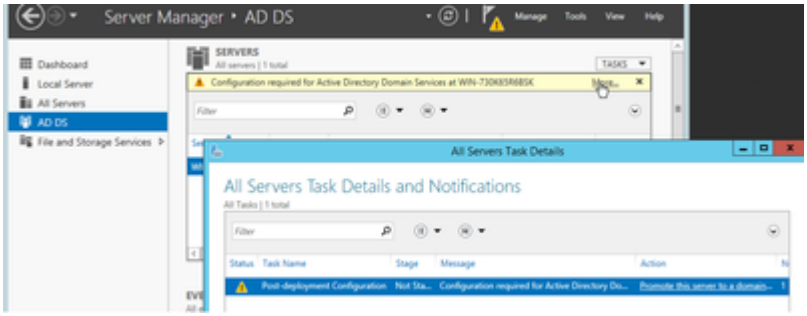
Activer et configurer les services Active Directory

- Dans le Gestionnaire de serveur, sélectionnez l'option **Ajouter des rôles et des fonctionnalités**, sélectionnez l'**installation basée sur les rôles ou sur les fonctionnalités** et choisissez le serveur dans

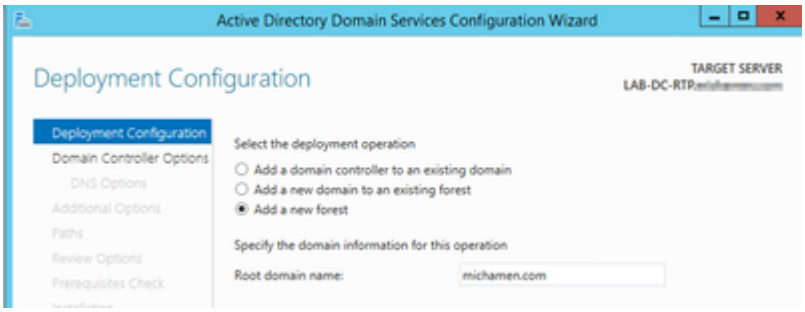
le pool (il ne doit y en avoir qu'un dans le pool), puis les services de domaine Active Directory :

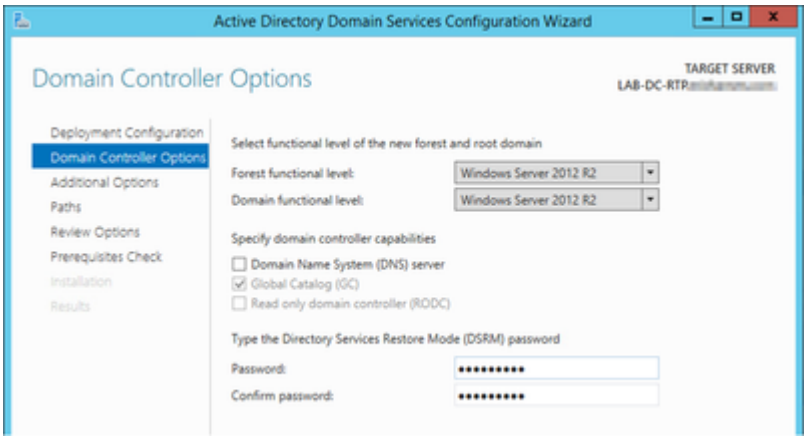


- Continuez à sélectionner le bouton **Next** , puis **Install**
- Cliquez sur le bouton **Fermer** une fois l'installation terminée
- Un onglet d'avertissement apparaît sous **Gestionnaire de serveur > AD DS** avec le titre Configuration requise pour les services de domaine Active Directory ; Sélectionnez **plus de** lien et l'action disponible pour démarrer l'Assistant de configuration :

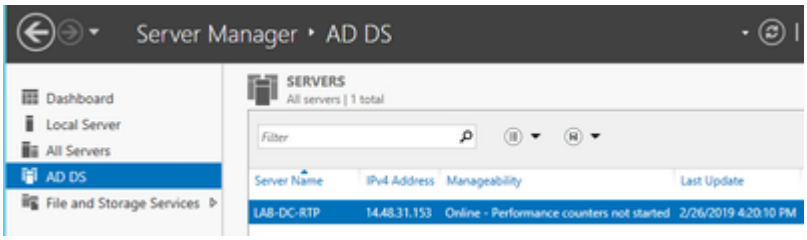


- Suivez les instructions de l'assistant de configuration de domaine, ajoutez une nouvelle forêt avec le nom de domaine racine souhaité (utilisé michamen.com pour ces travaux pratiques) et décochez la case DNS lorsque disponible, définissez le mot de passe DSRM (utilisé *C1sc0123 !* pour ces travaux pratiques) :



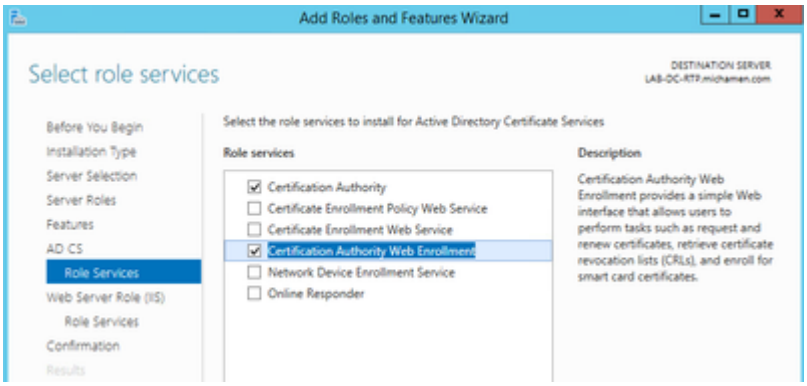


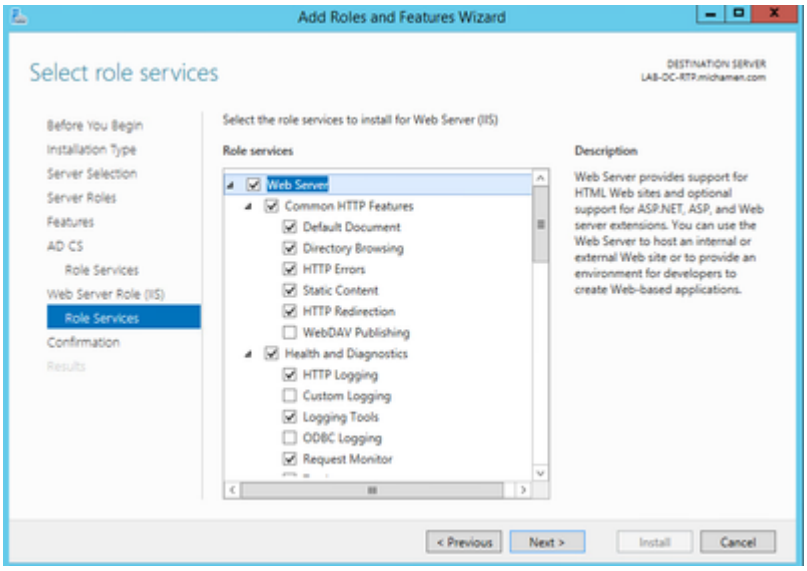
- Nécessité de spécifier un nom de domaine NetBIOS (MICHAMEN1 utilisé dans ces travaux pratiques).
- Suivez l'assistant jusqu'à la fin. Le serveur redémarre ensuite pour terminer l'installation.
- Lorsque vous devez spécifier le nouveau nom de domaine la prochaine fois que vous vous connectez. Par exemple MICHAMEN1\Administrateur.



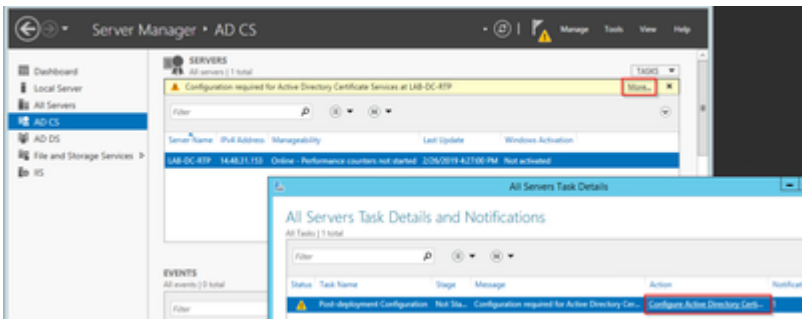
Activer et configurer les services de certificats

- Dans le Gestionnaire de serveur, sélectionnez Ajouter des rôles et des fonctionnalités
- Sélectionnez les services de certificats Active Directory et suivez les invites pour ajouter les fonctionnalités requises (toutes les fonctionnalités disponibles ont été sélectionnées dans les services de rôle qui ont été activés pour ces travaux pratiques)
- Pour les services de rôle, vérifiez l'inscription Web Autorité de certification

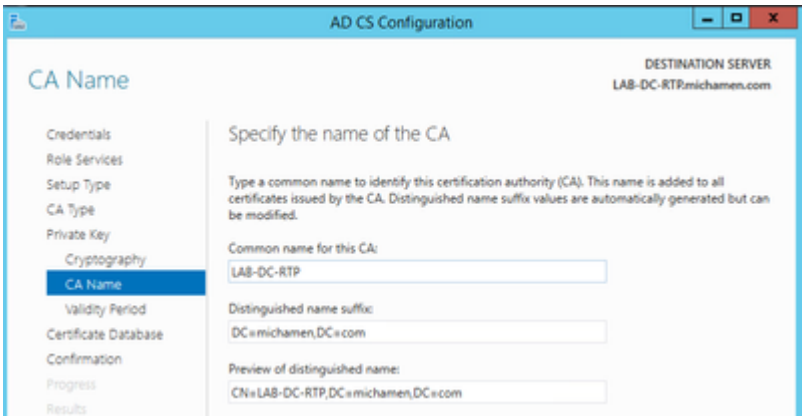




- Un onglet d'avertissement doit apparaître sous **Gestionnaire de serveur > AD DS** avec le titre Configuration requise pour les services de certificats Active Directory. Sélectionnez le lien **plus** et l'action disponible :



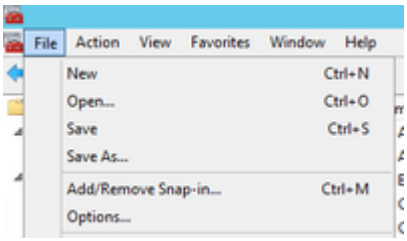
- Dans l'assistant Post Install Configuration d'AD-CS, parcourez les étapes suivantes :
- Sélectionnez les rôles d'**inscription Web Autorité de certification** et **Autorité de certification**
- Choisissez Enterprise CA avec les options suivantes :
- Autorité de certification racine
- Créer une nouvelle clé privée
- Utiliser la clé privée - SHA1 avec les paramètres par défaut
- Définissez un nom commun pour l'autorité de certification (doit correspondre au nom d'hôte du serveur) :

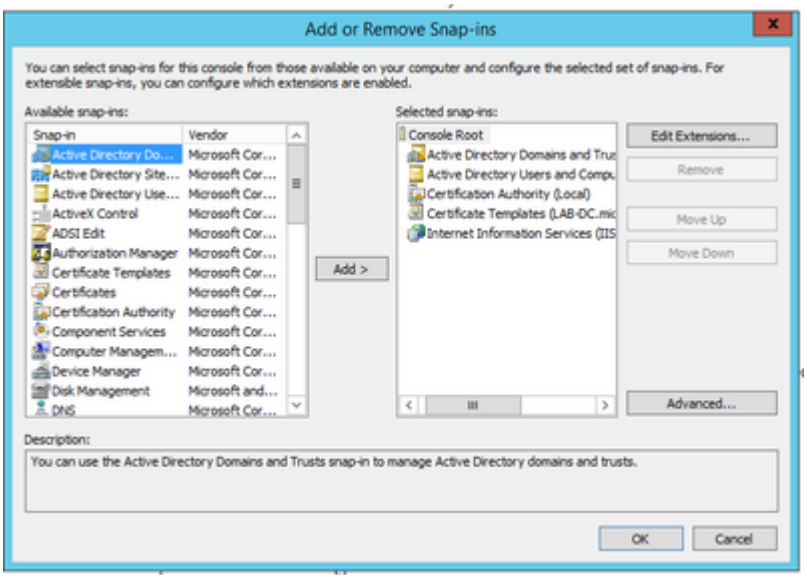


- Définir la validité pour 5 ans (ou plus si vous le souhaitez)
- Sélectionnez le bouton **Next** dans le reste de l'assistant

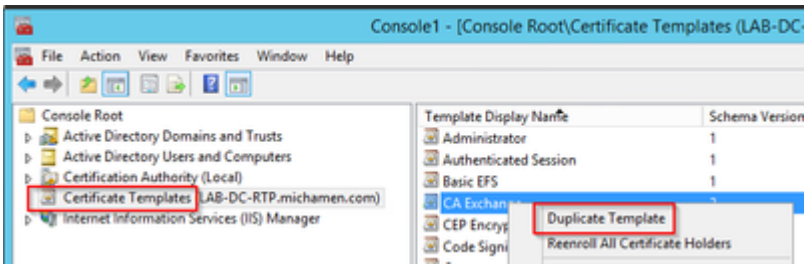
Création d'un modèle de certificat pour CiscoRA

- Ouvrez MMC. Sélectionnez le logo de démarrage de Windows et tapez *mmc* dans Exécuter
- Ouvrez une fenêtre MMC et ajoutez les composants logiciels enfichables suivants (utilisés à différents points de la configuration), puis sélectionnez **OK** :

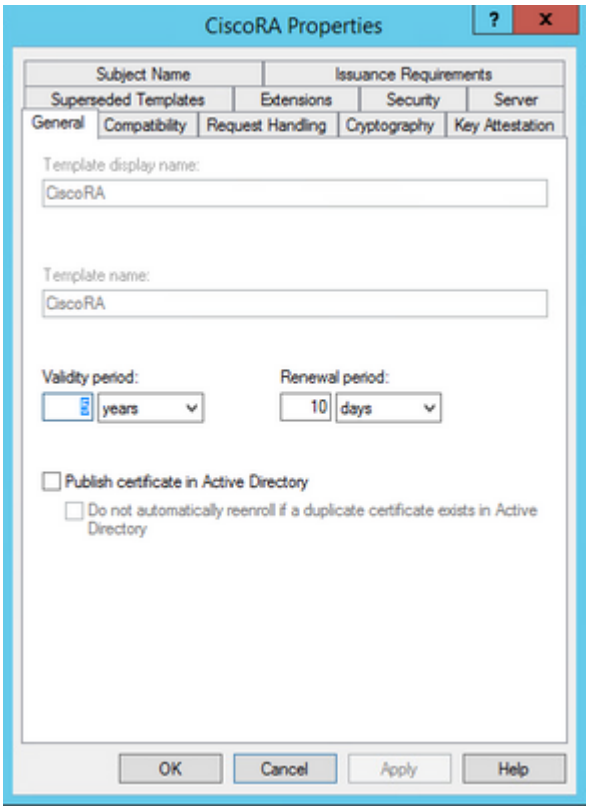




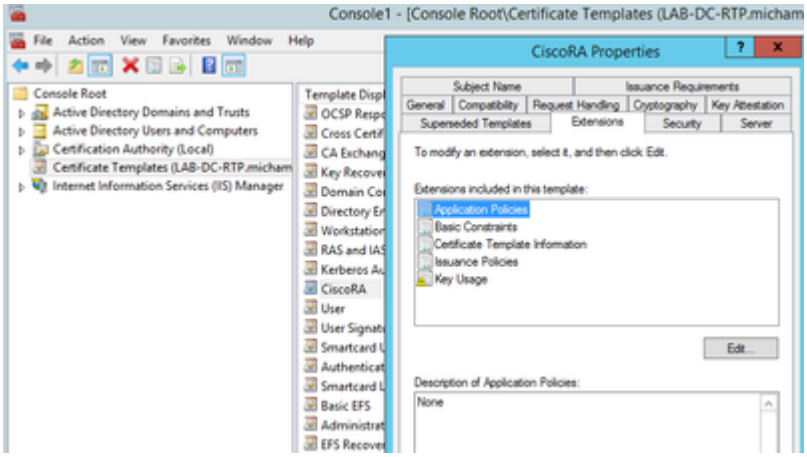
- Sélectionnez **Fichier > Enregistrer** et enregistrez cette session de console sur le bureau pour un accès rapide
- Dans les composants logiciels enfichables, sélectionnez **Modèles de certificats**
- Créez ou clonez un modèle (de préférence le modèle « *Autorité de certification racine* » si disponible) et nommez-le CiscoRA



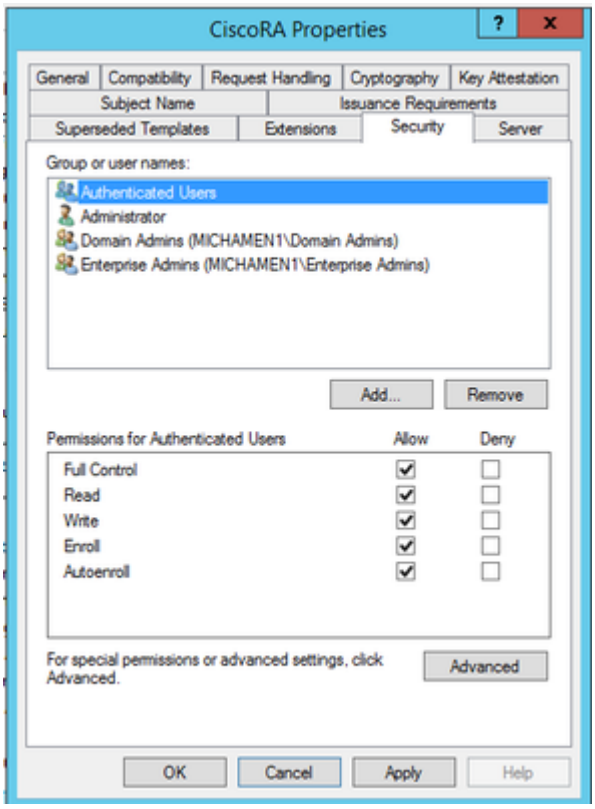
- Modifiez le modèle. Cliquez dessus avec le bouton droit et sélectionnez **Propriétés**
- Sélectionnez l'onglet **Général** et définissez la période de validité sur 20 ans (ou une autre valeur si vous le souhaitez). Dans cet onglet, assurez-vous que les valeurs « display name » et « name » du modèle correspondent



- Sélectionnez l'onglet **Extensions**, mettez en surbrillance **Stratégies d'application,** puis sélectionnez **Modifier**

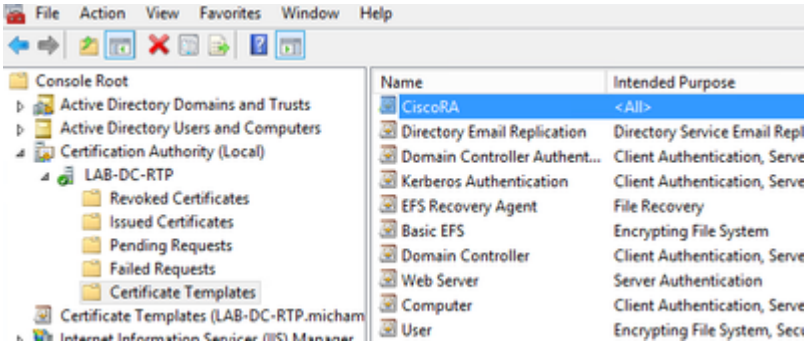


- Supprimez toutes les stratégies affichées dans la fenêtre qui s'affiche
- Sélectionnez l'onglet **Subject Name** et sélectionnez la case d'option **Supply in Request**
- Sélectionnez l'onglet **Sécurité** et accordez toutes les autorisations pour tous les groupes/noms d'utilisateurs affichés



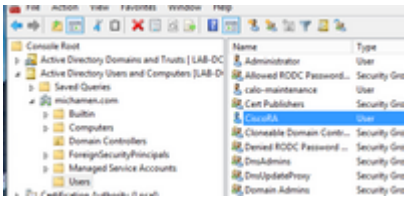
Rendre le modèle de certificat disponible pour l'émission

- Dans les composants logiciels enfichables MMC, sélectionnez **Autorité de certification** et développez l'arborescence des dossiers afin de localiser le dossier **Modèles de certificat**
- Cliquez avec le bouton droit de la souris dans l'espace blanc du cadre contenant le nom et l'objectif souhaité
- Sélectionnez **Nouveau** et **Modèle de certificat à émettre**
- Sélectionnez le modèle CiscoRA nouvellement créé et modifié



Création de compte CiscoRA Active Directory

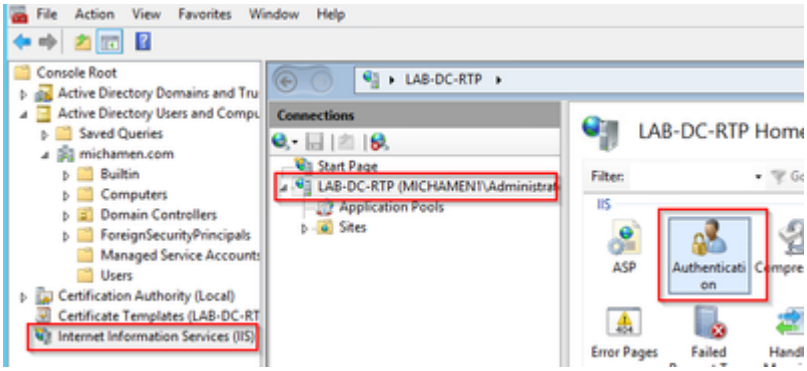
- Accédez aux composants logiciels enfichables MMC et sélectionnez **Utilisateurs et ordinateurs Active Directory**
- Sélectionnez le dossier **Users** dans l'arborescence du volet le plus à gauche
- Cliquez avec le bouton droit dans l'espace blanc du cadre contenant Nom, Type et Description
- Sélectionnez **Nouveau** et **Utilisateur**
- Créez le compte CiscoRA avec le nom dâ€™utilisateur/mot de passe (*ciscora/Cisco123* a été utilisé pour ces travaux pratiques) et activez la case à cocher Le **mot de passe nâ€™expire jamais** lorsquâ€™il est affiché



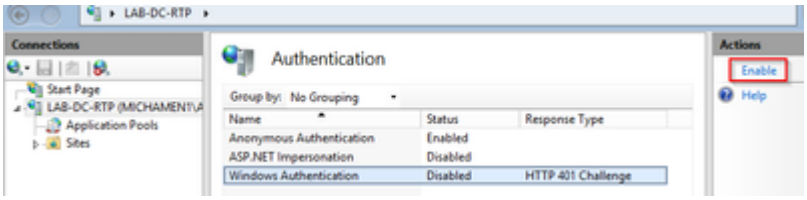
IIS Configuration de l'authentification et de la liaison SSL

Activer NTLM Authentification

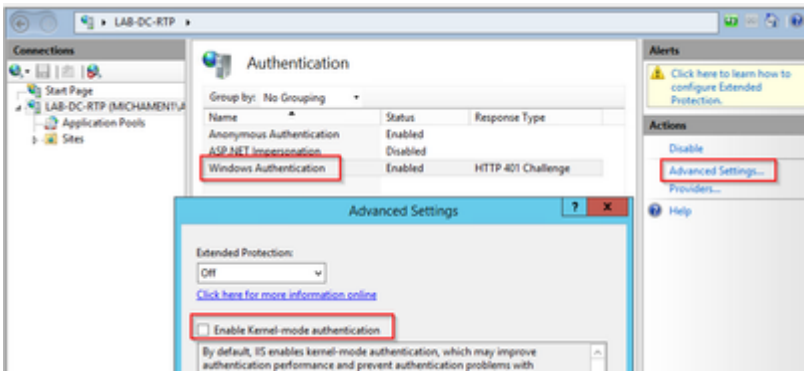
- Accédez aux composants logiciels enfichables MMC et, sous le composant logiciel enfichable Gestionnaire des services Internet (IIS), sélectionnez le nom de votre serveur
- La liste des fonctions s'affiche dans la trame suivante. Double-cliquez sur l'icône **Authentication** feature



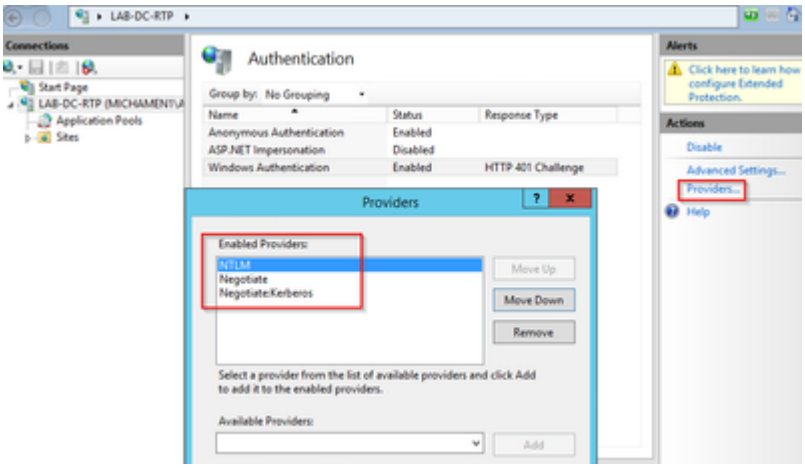
- Sélectionnez **Authentification Windows** et, dans le cadre Actions (volet droit), sélectionnez l'option **Activer**



- Le volet Actions affiche l'option **Paramètres avancés** ; sélectionnez-la et décochez **Activer l'authentification en mode noyau**



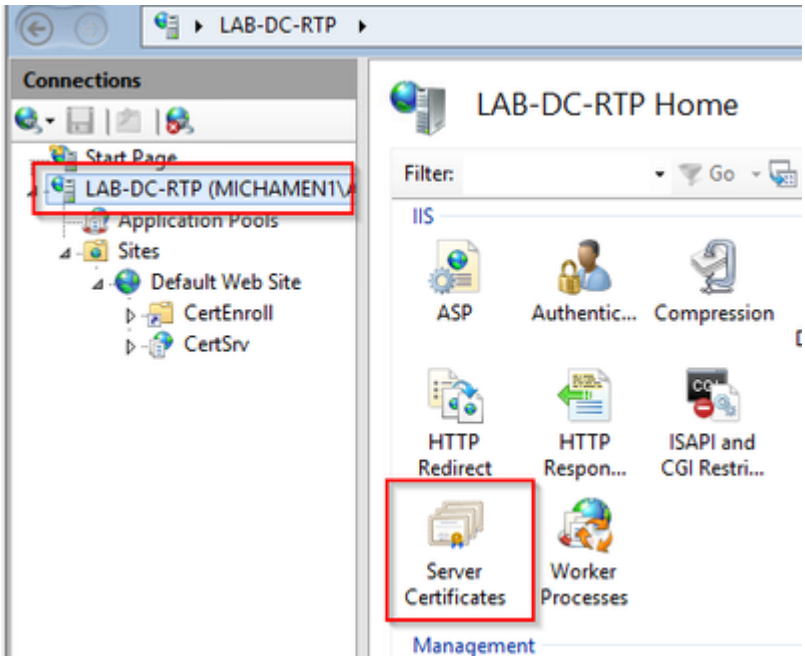
- Sélectionnez **Fournisseurs** et mettez en ordre **NTML** puis **Négocier.**



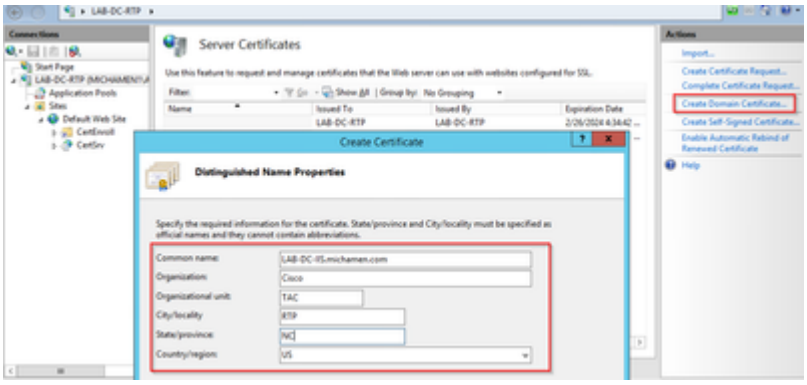
Générer le certificat d'identité pour le serveur Web

Si ce n'est pas déjà le cas, vous devez générer un certificat et un certificat d'identité pour votre service Web qui est signé par l'autorité de certification, car CiscoRA ne peut pas s'y connecter si le certificat du serveur Web est auto-signé :

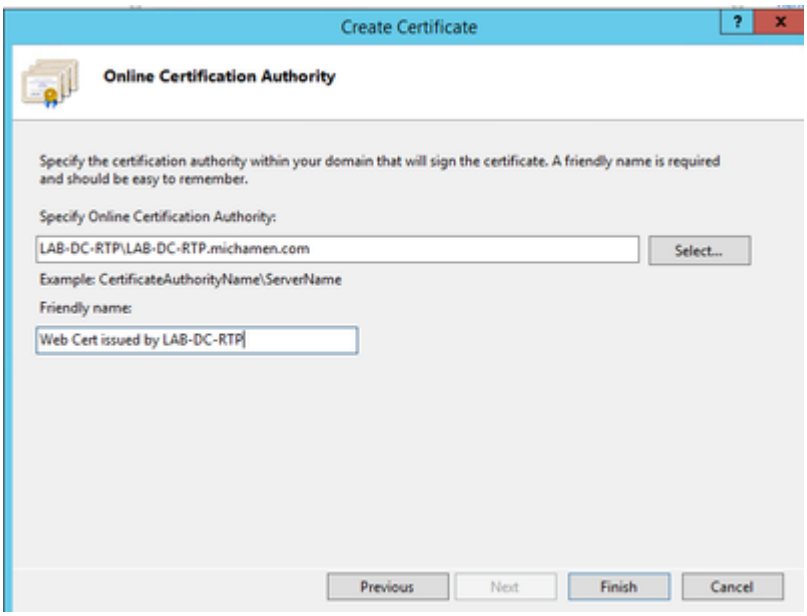
- Sélectionnez votre serveur Web à partir du **composant logiciel enfichable IIS** et double-cliquez sur l'icône de fonction **Certificats de serveur** :



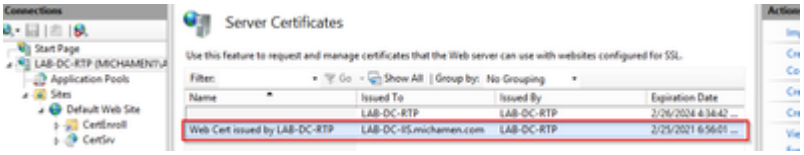
- Par défaut, vous pouvez voir un certificat répertorié ici ; qui est le certificat CA racine auto-signé ; Dans le menu **Actions** sélectionnez l'option **Créer un certificat de domaine**. Entrez les valeurs dans l'assistant de configuration afin de créer votre nouveau certificat. Assurez-vous que le nom commun est un nom de domaine complet (FQDN) résoluble, puis sélectionnez **Suivant** :



- Sélectionnez le certificat de votre autorité de certification racine comme émetteur et sélectionnez **Terminer** :

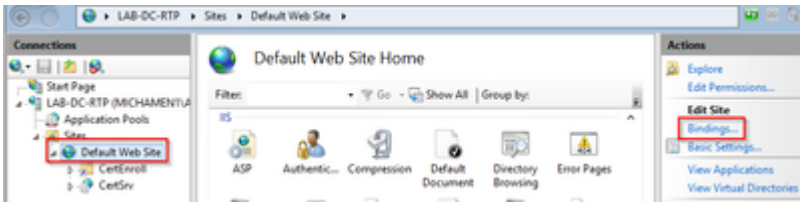


- Vous pouvez voir le certificat CA et le certificat d'identité de votre serveur Web répertoriés :



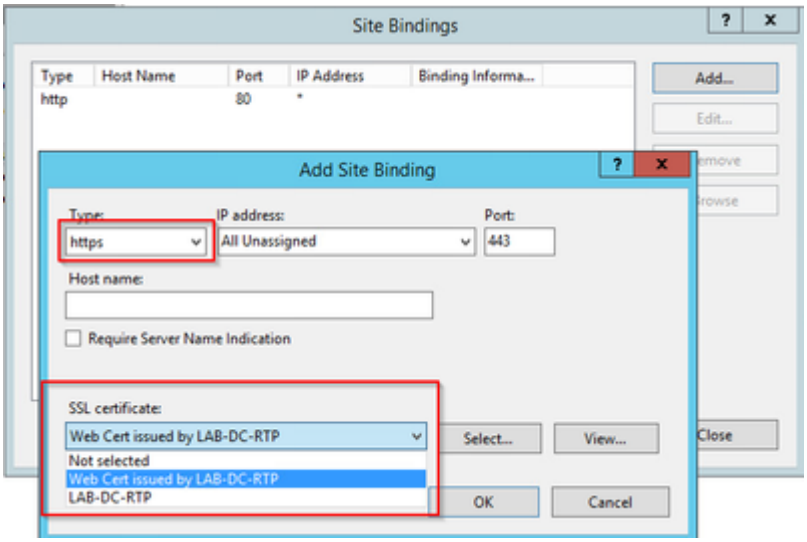
Liaison SSL du serveur Web

- Sélectionnez un site dans l'arborescence (vous pouvez utiliser le site Web par défaut ou le rendre plus granulaire pour des sites spécifiques) et sélectionnez **Liaisons** dans le volet Actions. L'éditeur de liaisons qui s'affiche vous permet de créer, de modifier et de supprimer des liaisons pour votre site Web. Sélectionnez **Add** afin d'ajouter votre nouvelle liaison SSL au site.

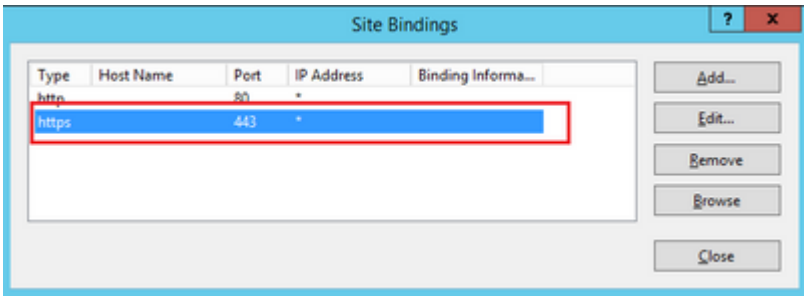


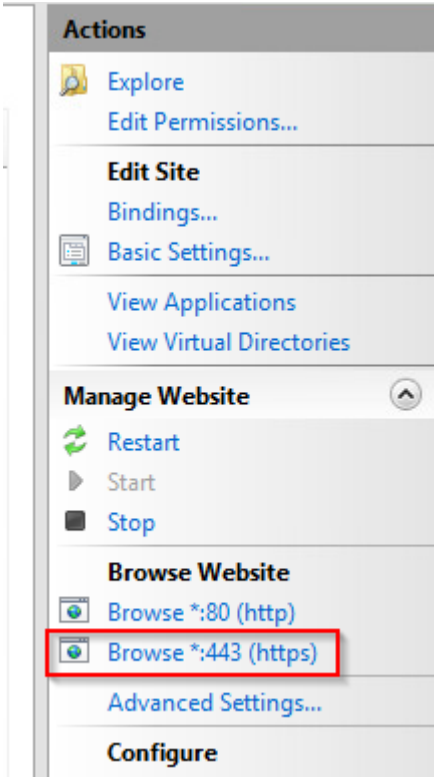
- Les paramètres par défaut d'une nouvelle liaison sont définis sur HTTP sur le port 80. Sélectionnez **https** dans la liste déroulante **Type**. Sélectionnez le certificat auto-signé que vous avez créé dans la

section précédente dans la liste déroulante **SSL Certificate**, puis sélectionnez **OK**.



- Maintenant, vous avez une nouvelle liaison SSL sur votre site et tout ce qui reste est de vérifier qu'il fonctionne en sélectionnant **Browse * : 443 (https)** option du menu et assurez-vous que la page Web IIS par défaut utilise HTTPS :



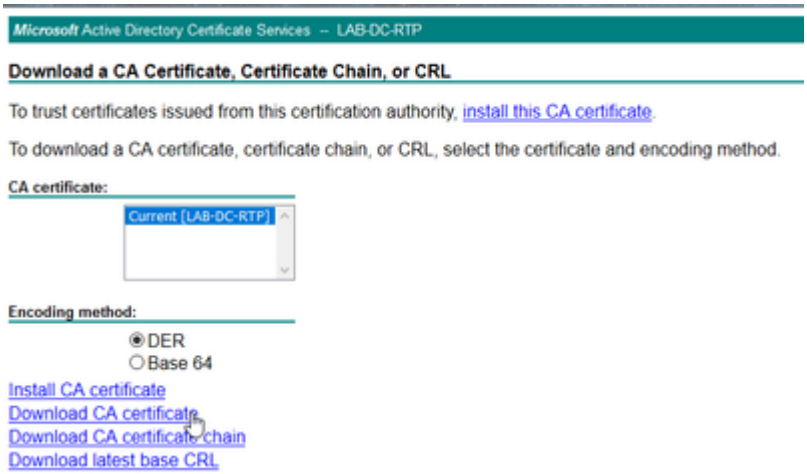


- N'oubliez pas de redémarrer le service IIS après les modifications de configuration. Utilisez l'option

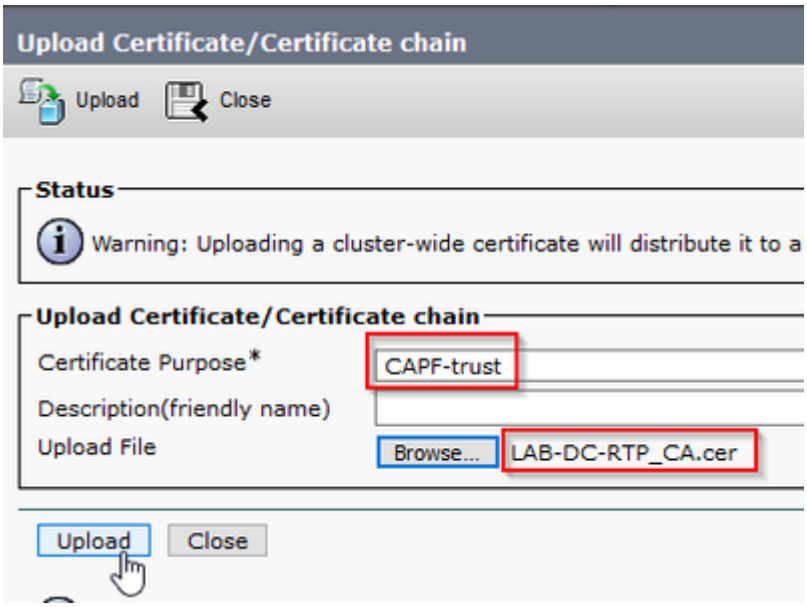
Redémarrer du volet Actions.

Configuration CUCM

- Accédez à votre page Web AD CS (https://YOUR_SERVER_FQDN/certsrv/) et téléchargez le certificat CA

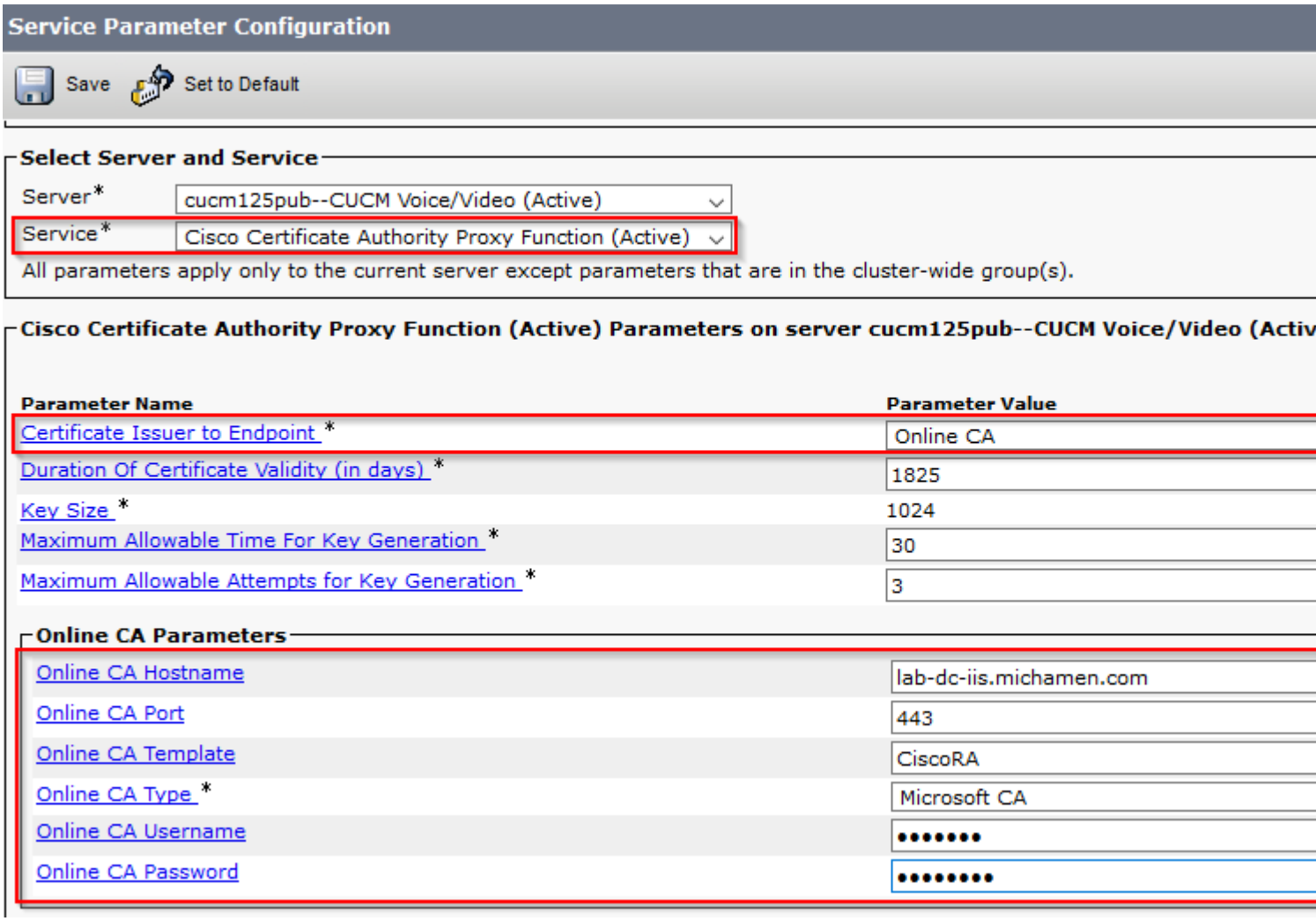


- Accédez à **Security > Certificate Management** à partir de la page OS Administration et sélectionnez le bouton **Upload Certificate/Certificate chain** afin de télécharger le certificat CA avec le *but* défini sur *CAPF-trust.*

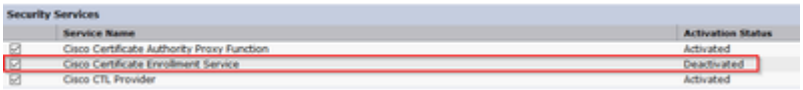


... À ce stade, il est également conseillé de télécharger le même certificat d'autorité de certification que *CallManager-trust* car il est nécessaire si le chiffrement de signalisation sécurisé est activé (ou sera activé) pour les points d'extrémité ; ce qui est probable si le cluster est en mode mixte.

- Accédez à **System > Service Parameters.** Sélectionnez le serveur Unified CM Publisher dans le champ Server et **Cisco Certificate Authority Proxy Function** dans le champ Service
- Définissez la valeur de Certificate Issuer sur Endpoint sur Online CA et saisissez les valeurs des champs Online CA Parameters. Veillez à utiliser le nom de domaine complet du serveur Web, le nom du modèle de certificat créé précédemment (CiscoRA), le type d'autorité de certification en tant qu'autorité de certification Microsoft et utilisez les informations d'identification du compte utilisateur CiscoRA créé précédemment



- Une fenêtre contextuelle vous informe que le service CAPF doit être redémarré. Mais d'abord, activez le service d'inscription de certificat Cisco via **Cisco Unified Serviceability > Tools > Service Activation**, sélectionnez l'éditeur dans le champ Server et cochez la case Cisco Certificate Enrollment Service, puis sélectionnez le bouton **Save** :



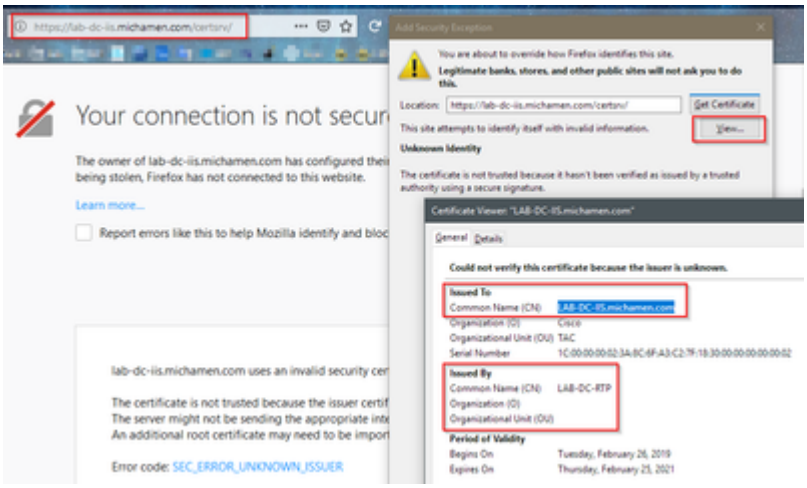
Vérifier

Vérifier les certificats IIS

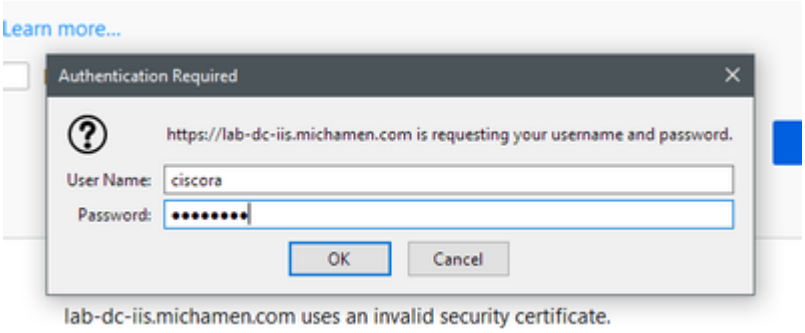
- À partir d'un navigateur Web sur un PC connecté au serveur (de préférence sur le même réseau que le serveur de publication CUCM), accédez à l'URL suivante :

  https://YOUR_SERVER_FQDN/certsrv/

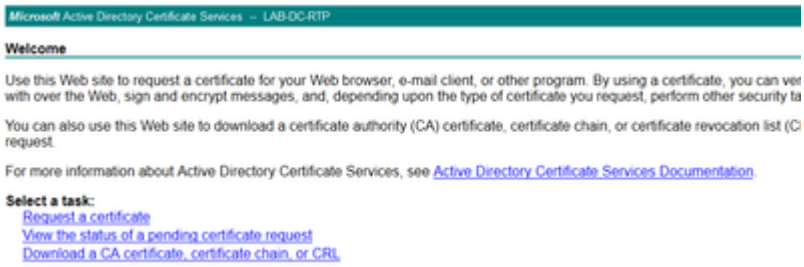
- L'alerte Certificat non approuvé s'affiche. Ajoutez l'exception et vérifiez le certificat. Vérifiez qu'il correspond au nom de domaine complet attendu :



- Après avoir accepté l'exception, vous devez vous authentifier ; à ce stade, vous devez utiliser les informations d'identification configurées pour le compte CiscoRA précédemment :



- Après l'authentification, vous devez pouvoir afficher la page d'accueil AD CS (Active Directory Certificate Services) :



Vérification de la configuration CUCM

Suivez les étapes habituelles pour installer un certificat LSC sur l'un des téléphones.

Étape 1. Ouvrez la page CallManager Administration, Device, puis Phone

Étape 2. Cliquez sur le bouton **Rechercher** pour afficher les téléphones

Étape 3. Sélectionnez le téléphone sur lequel vous souhaitez installer le contrôleur LSC

Étape 4. Faites défiler jusqu'à Certification Authority Proxy Function (CAPF) Information

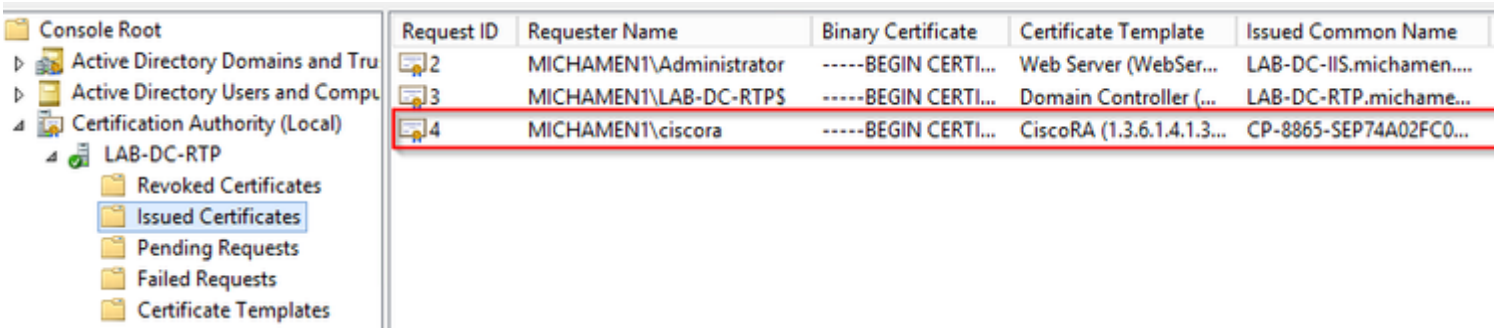
Étape 5. Sélectionnez Installation/Mise à niveau dans l'opération de certificat.

Étape 6. Sélectionnez le mode d'authentification. (Par chaîne Null convient pour les tests)

Étape 7. Faites défiler la page jusqu'en haut et sélectionnez **save** puis **Apply Config** pour le téléphone.

Étape 8. Une fois le téléphone redémarré et réenregistré, utilisez le filtre d'état LSC pour confirmer que le contrôleur LSC a été correctement installé.

- Du côté du serveur AD, ouvrez MMC et développez le composant logiciel enfichable Autorité de certification pour sélectionner le dossier Certificats émis
- L'entrée du téléphone s'affiche. Dans la vue récapitulative, voici quelques-uns des détails affichés :
  - ID de la demande : numéro d'ordre unique
  - Requester Name : le nom d'utilisateur du compte CiscoRA configuré doit être affiché
  - Modèle de certificat : le nom du modèle CiscoRA créé doit être affiché
  - Nom commun émis : le modèle du téléphone ajouté au nom du périphérique doit être affiché
  - Date d'effet et d'expiration du certificat



Liens connexes

- **Dépannage de CAPF Online CA**
- **Assistance et documentation techniques - Cisco Systems**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.