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

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Valider la date et l'heure du serveur
  - Nom du serveur de mise à jour
- Configurer
  - Services AD, utilisateur et modèle de certificat
    - Activer et configurer les services Active Directory
    - Activer et configurer les services de certificats
    - Création d'un modèle de certificat pour CiscoRA
    - Rendre le modèle de certificat disponible pour l'émission
    - Création de compte CiscoRA Active Directory
  - Configuration de l'authentification IIS et de la liaison SSL
    - Activer l'authentification NTLM
    - Générer le certificat d'identité pour le serveur Web
    - Liaison SSL du serveur Web
  - Configuration CUCM
- Vérifier
  - Vérifier les certificats IIS
  - Vérification de la configuration CUCM
- Liens connexes

Introduction

Ce document décrit l'inscription et le renouvellement automatiques des certificats via la fonctionnalité CAPF Online pour Cisco Unified Communications Manager (CUCM).

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 / Microprogramme : 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 l’incidence possible des commandes.

Informations générales

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

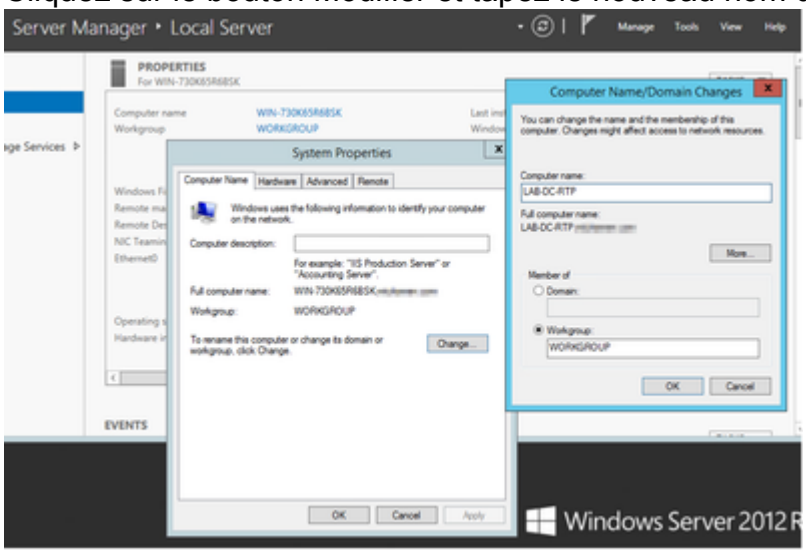
Valider la date et l'heure du serveur

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

Nom du serveur de mise à jour

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

1. Accédez à Local Server, sélectionnez le nom de l'ordinateur pour ouvrir les Propriétés système
2. Cliquez sur le bouton Modifier et tapez le nouveau nom de l'ordinateur.



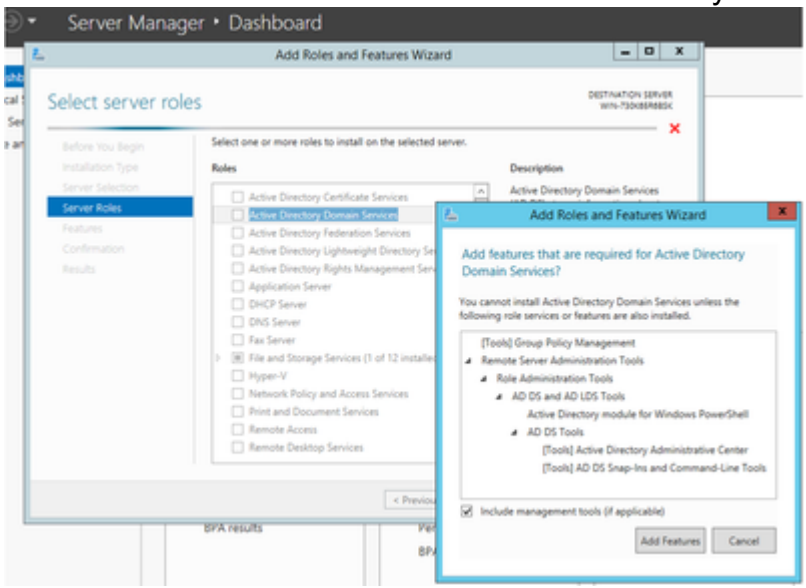
3. Redémarrez le serveur pour que les modifications soient appliquées.

Configurer

Services AD, utilisateur et modèle de certificat

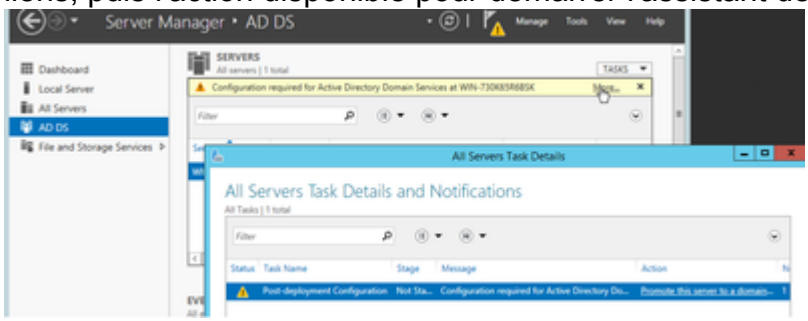
Activer et configurer les services Active Directory

1. Dans le Gestionnaire de serveur, sélectionnez Ajouter des rôles et des fonctionnalités, puis sélectionnez Installation basée sur les rôles ou basée sur les fonctionnalités.
2. Sélectionnez le serveur dans le pool (il ne doit y en avoir qu'un seul).
3. Sélectionnez Services de domaine Active Directory.

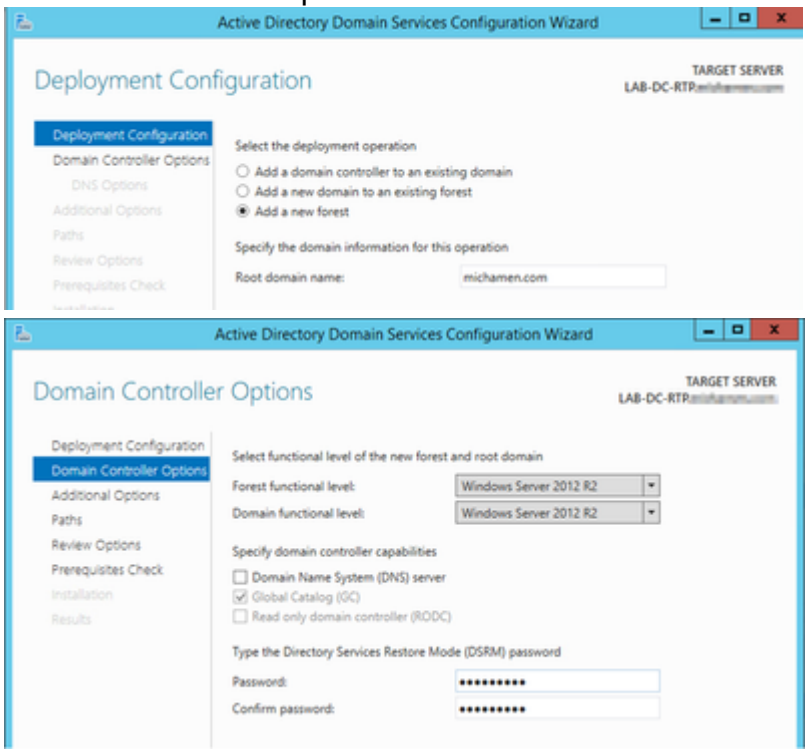


4. Cliquez sur le bouton Suivant, puis sur Installer.

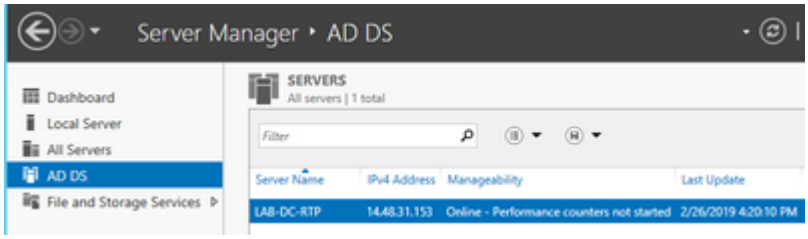
5. Cliquez sur le bouton Fermer une fois l'installation terminée.
6. Un onglet d'avertissement apparaît sous Gestionnaire de serveur > AD DS avec le titre Configuration requise pour les services de domaine Active Directory. Sélectionnez autres liens, puis l'action disponible pour démarrer l'assistant de configuration.



7. Complétez les invites de l'assistant de configuration de domaine, ajoutez une nouvelle forêt avec le nom de domaine racine souhaité et décochez la case DNS le cas échéant. Définissez le mot de passe DSRM.

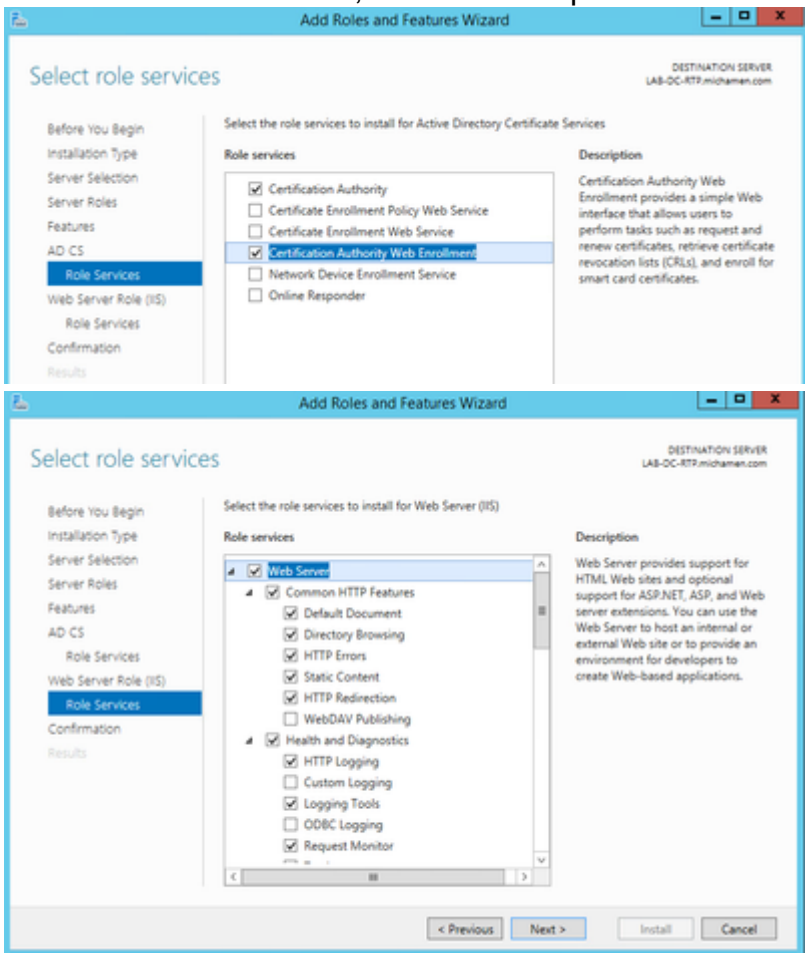


8. Spécifiez un nom de domaine NetBIOS (MICHAMEN1 utilisé dans ces travaux pratiques).
9. Terminez l'Assistant. Le serveur redémarre ensuite pour terminer l'installation.
10. Spécifiez le nouveau nom de domaine lors de votre prochaine connexion. Par exemple, MICHAMEN1\Administrateur.

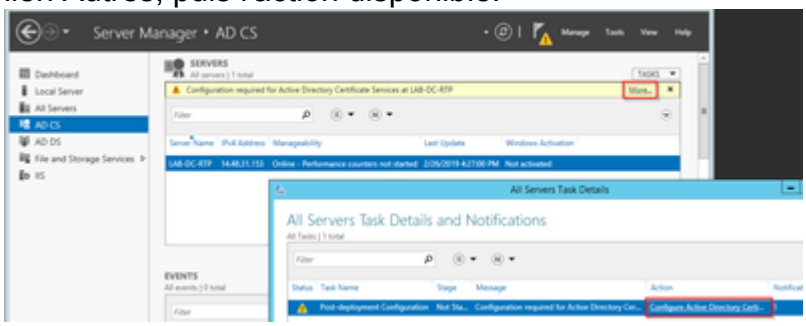


Activer et configurer les services de certificats

1. Dans le Gestionnaire de serveur, sélectionnez Ajouter des rôles et des fonctionnalités.
2. Sélectionnez Services de certificats Active Directory et ajoutez les fonctionnalités requises (toutes les fonctionnalités disponibles ont été sélectionnées dans les services de rôle qui ont été activés pour ces travaux pratiques).
3. Pour les services de rôle, vérifiez l'inscription Web de l'autorité de certification.



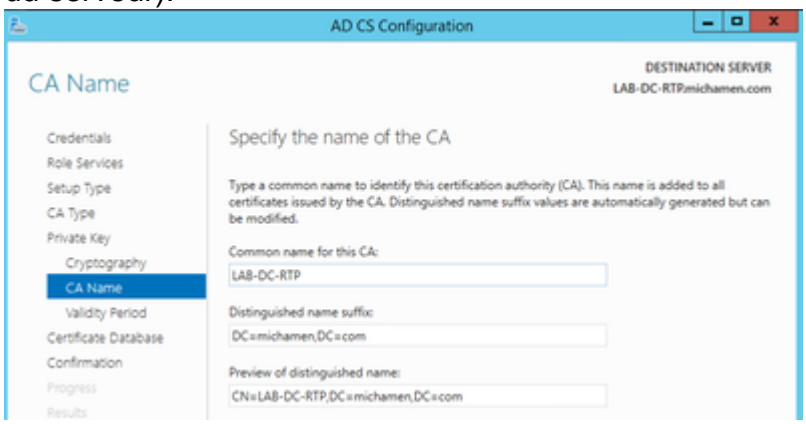
4. Un onglet d'avertissement doit apparaître sous Gestionnaire de serveur > AD DS avec le titre Configuration requise pour les services de certificats Active Directory ; Sélectionnez le lien Autres, puis l'action disponible.



Complétez ces étapes dans l'assistant Post Install Configuration d'AD-CS :

1. Sélectionnez les rôles d'inscription Web Autorité de certification et Autorité de certification.
2. Choisissez Enterprise CA avec les options suivantes :
3. Autorité de certification racine
4. Créez une nouvelle clé privée.

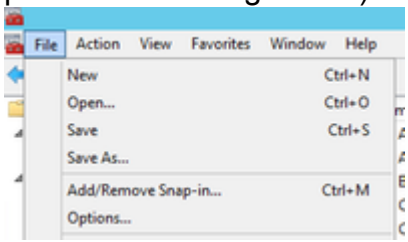
5. Utiliser la clé privée - SHA1 avec les paramètres par défaut.
6. Définissez un nom commun pour l'autorité de certification (doit correspondre au nom d'hôte du serveur).

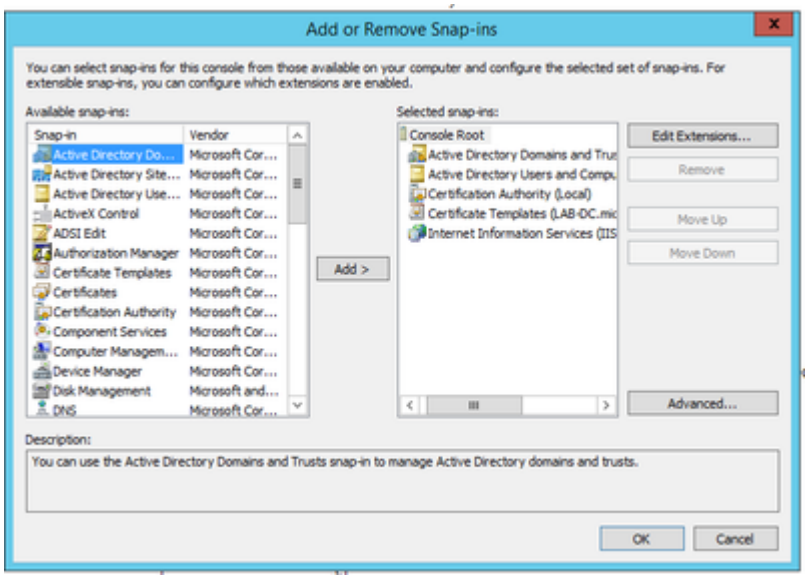


7. Définissez Validité pour 5 ans (ou plus si vous le souhaitez).
8. Sélectionnez le bouton Next dans le reste de l'assistant.

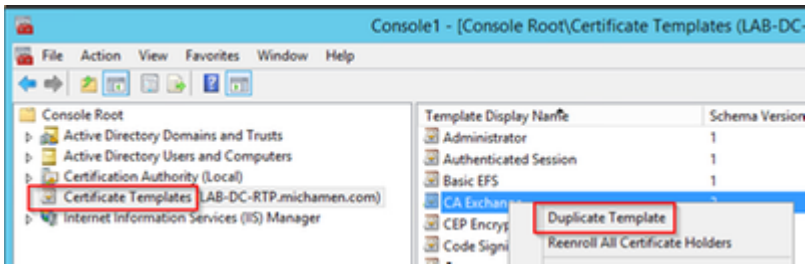
Création d'un modèle de certificat pour CiscoRA

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

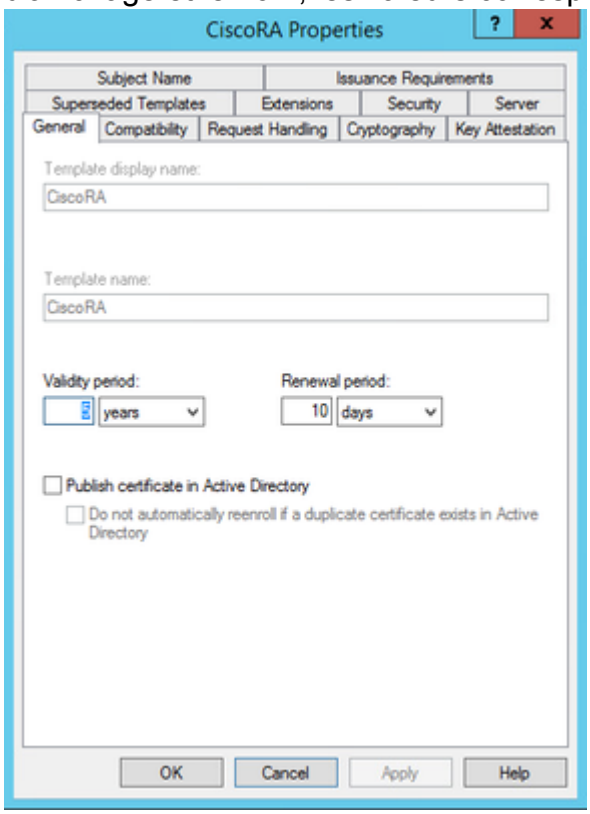




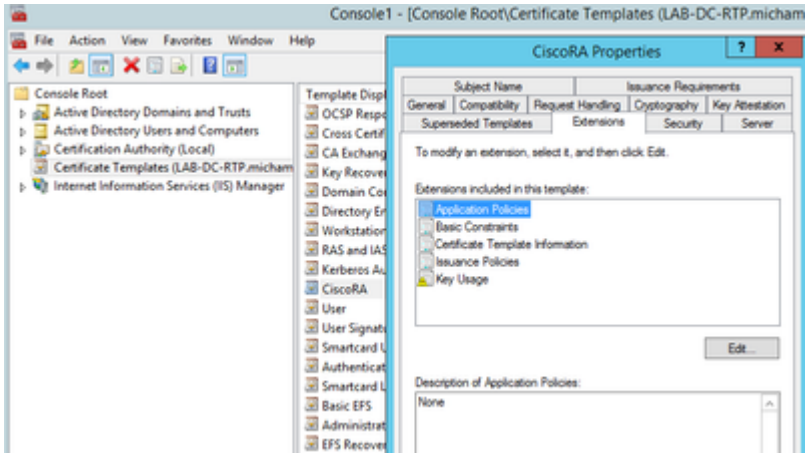
3. Sélectionnez File > Save et enregistrez cette session de console sur le bureau pour un accès rapide.
4. Dans les composants logiciels enfichables, sélectionnez Modèles de certificats.
5. Créez ou clonez un modèle (de préférence le modèle Autorité de certification racine si disponible) et nommez-le CiscoRA.



6. Cliquez avec le bouton droit sur le modèle et sélectionnez Propriétés.
7. 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 le modèle, le nom d'affichage et le nom, les valeurs correspondent.

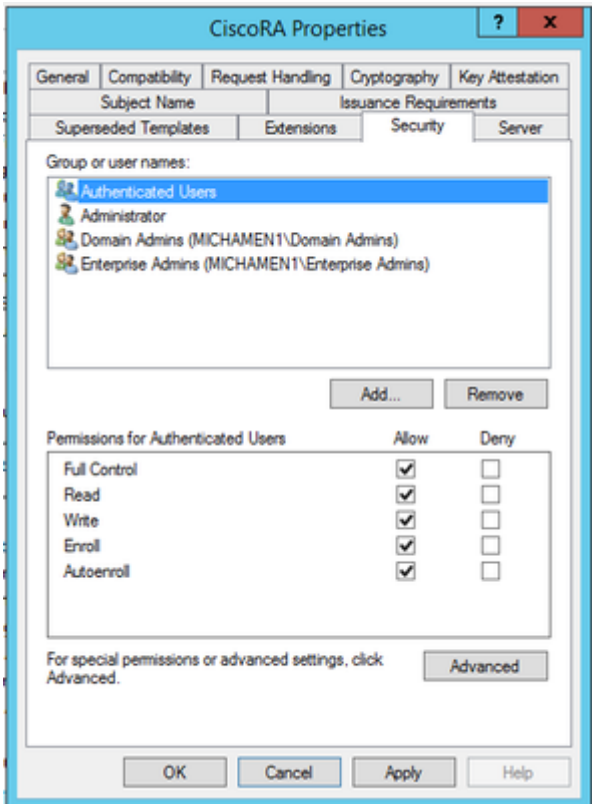


8. Sélectionnez l'onglet Extensions, mettez en surbrillance Application Policies, puis sélectionnez Edit.



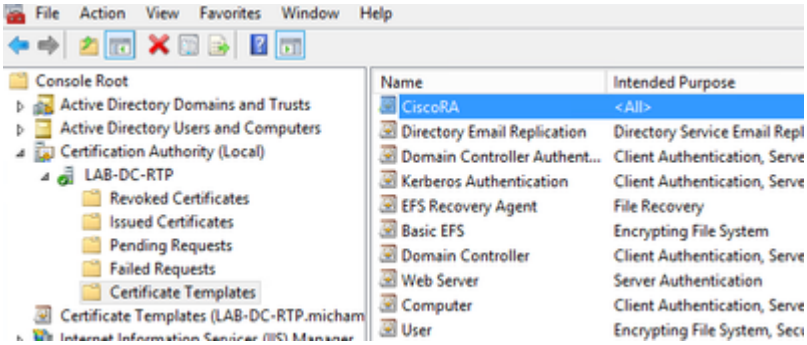
9. Supprimez toutes les stratégies affichées dans la fenêtre qui s'affiche.
10. Sélectionnez l'onglet Subject Name et sélectionnez la case d'option Supply in Request.
11. Sélectionnez l'onglet Sécurité et accordez des autorisations en fonction de vos besoins en termes de noms de groupes/d'utilisateurs.

Remarque : Dans cet exemple, des autorisations complètes ont été accordées à tous les niveaux pour plus de simplicité, mais cela a des implications en matière de sécurité. Dans un environnement de production, les autorisations d'écriture et d'inscription ne doivent être accordées qu'aux utilisateurs et aux groupes qui en ont besoin. Pour plus d'informations, reportez-vous à la documentation Microsoft.



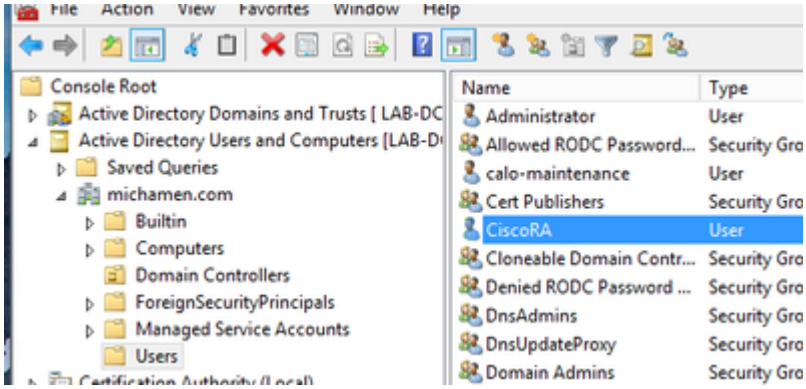
Rendre le modèle de certificat disponible pour l'émission

1. Dans les composants logiciels enfichables MMC, sélectionnez Autorité de certification et développez l'arborescence des dossiers pour localiser le dossier Modèles de certificats.
2. Cliquez avec le bouton droit de la souris dans l'espace blanc du cadre contenant le nom et l'objectif souhaité.
3. Sélectionnez Nouveau et Modèle de certificat à émettre.
4. Sélectionnez le nouveau modèle CiscoRA créé et modifié.



Création de compte CiscoRA Active Directory

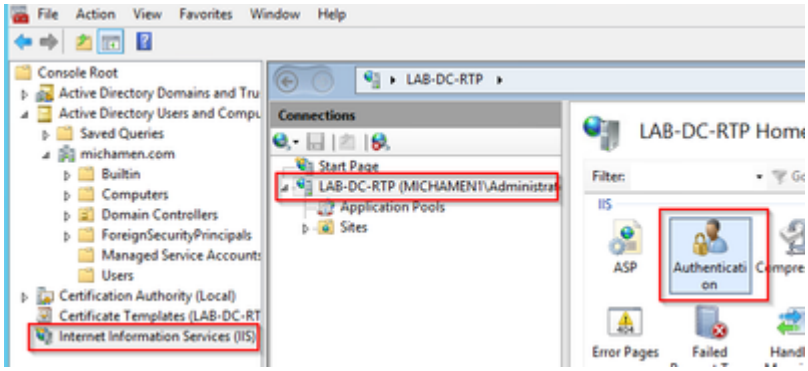
1. Accédez à Composants logiciels enfichables MMC et sélectionnez Utilisateurs et ordinateurs Active Directory.
2. Sélectionnez le dossier Users dans l'arborescence du volet le plus à gauche.
3. Cliquez avec le bouton droit dans l'espace blanc du cadre contenant Nom, Type et Description.
4. Sélectionnez Nouveau et Utilisateur.
5. Créez le compte CiscoRA avec le nom d'utilisateur/mot de passe (ciscora/Cisco123 a été utilisé pour ces travaux pratiques) et cochez la case Password never expires lorsqu'elle est affichée.



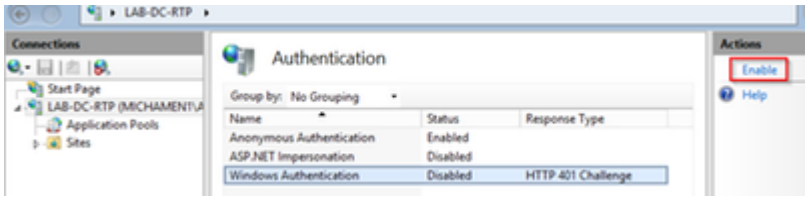
Configuration de l'authentification IIS et de la liaison SSL

Activer l'authentification NTLM

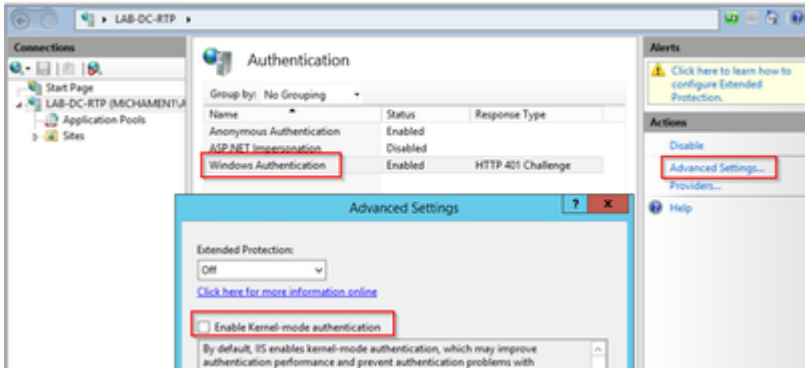
1. Accédez aux composants logiciels enfichables MMC et, sous le composant logiciel enfichable Gestionnaire des services Internet (IIS), sélectionnez votre nom de serveur.
2. La liste des fonctions s'affiche dans la trame suivante. Double-cliquez sur Authentification.



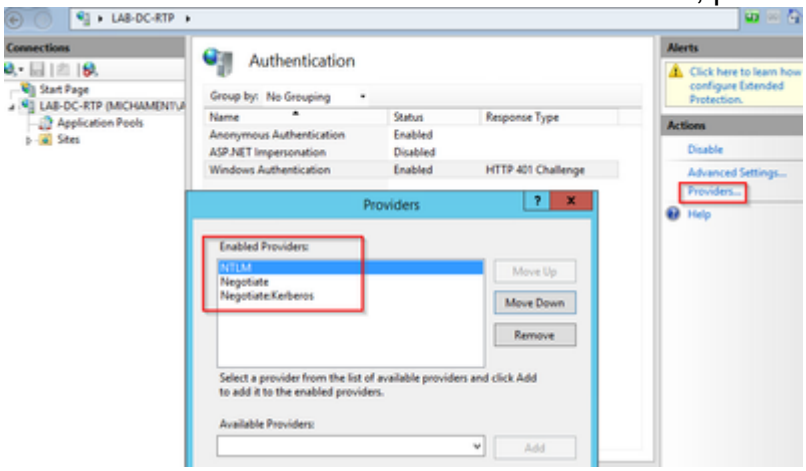
3. Sélectionnez Authentification Windows et, dans le cadre Actions (volet droit), sélectionnez Activer.



4. Sélectionnez Advanced Settings et désactivez la case à cocher Enable Kernel-mode authentication.



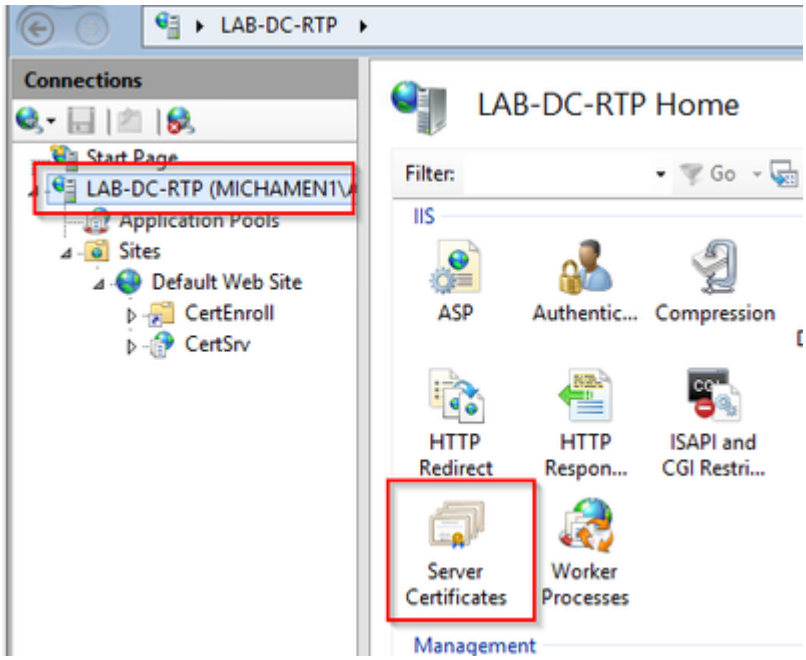
5. Sélectionnez Providers et mettez en ordre NTML, puis Negotiate.



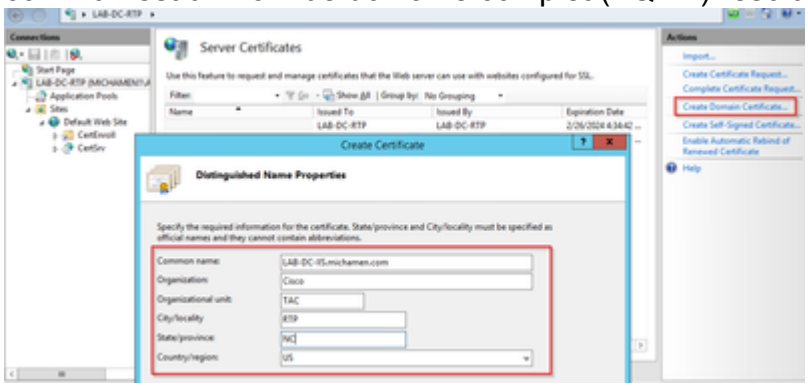
Générer le certificat d'identité pour le serveur Web

Si vous ne l'avez pas encore fait, générez 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.

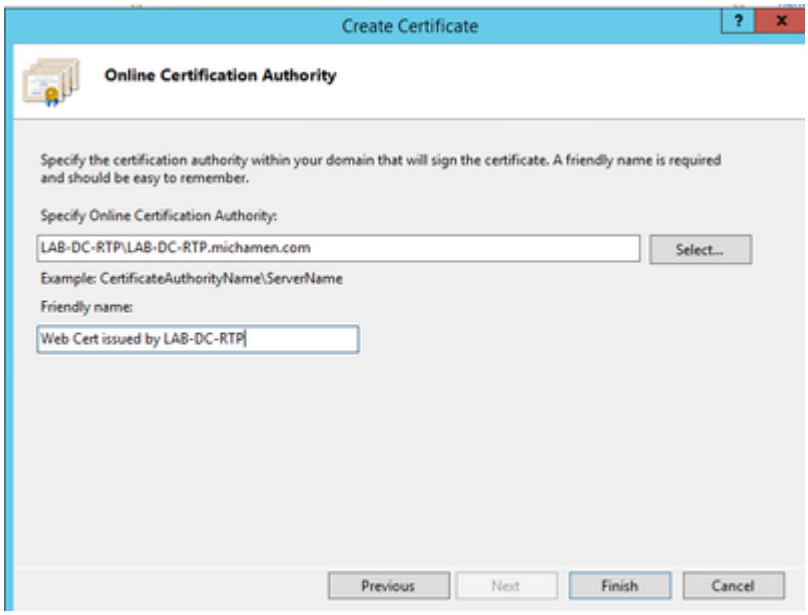
1. Sélectionnez votre serveur Web dans le composant logiciel enfichable IIS et double-cliquez sur Certificats de serveur.



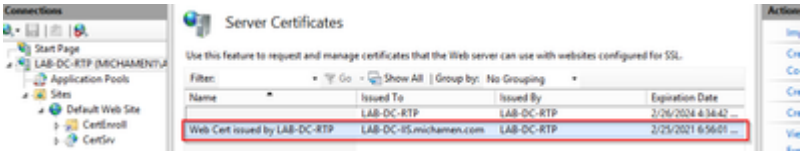
2. Par défaut, un certificat y est répertorié, à savoir le certificat CA racine auto-signé. Dans le menu Actions, sélectionnez Créer un certificat de domaine. Entrez les valeurs dans l'assistant de configuration pour créer votre nouveau certificat. Assurez-vous que le nom commun est un nom de domaine complet (FQDN) résoluble et sélectionnez Suivant.



3. Sélectionnez le certificat de votre autorité de certification racine comme émetteur et sélectionnez Terminer.

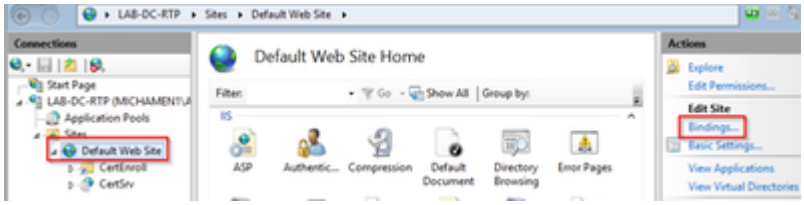


Le certificat CA et votre certificat d'identité de serveur Web sont répertoriés.

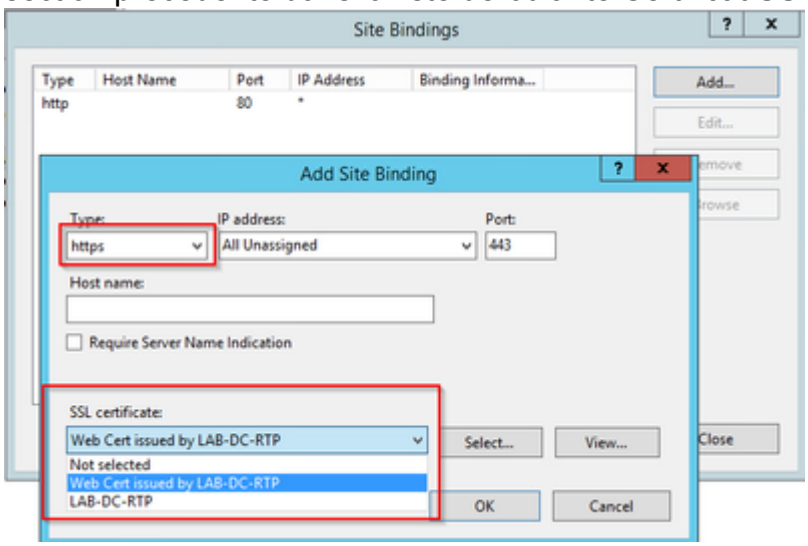


Liaison SSL du serveur Web

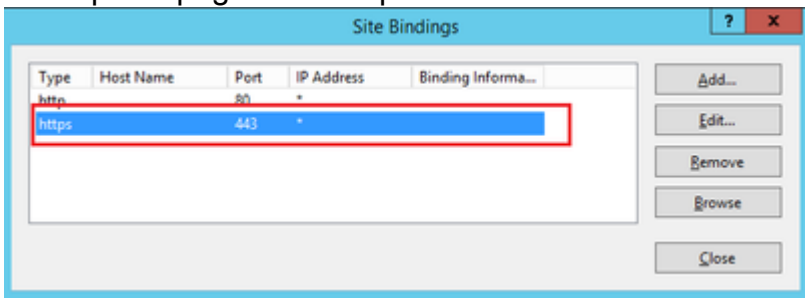
1. Sélectionnez un site dans l'arborescence (vous pouvez utiliser le site Web par défaut ou le rendre plus granulaire pour des sites spécifiques) et sélectionnez Liaisons dans le volet Actions. L'éditeur de liaisons qui s'affiche vous permet de créer, modifier et supprimer des liaisons pour votre site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

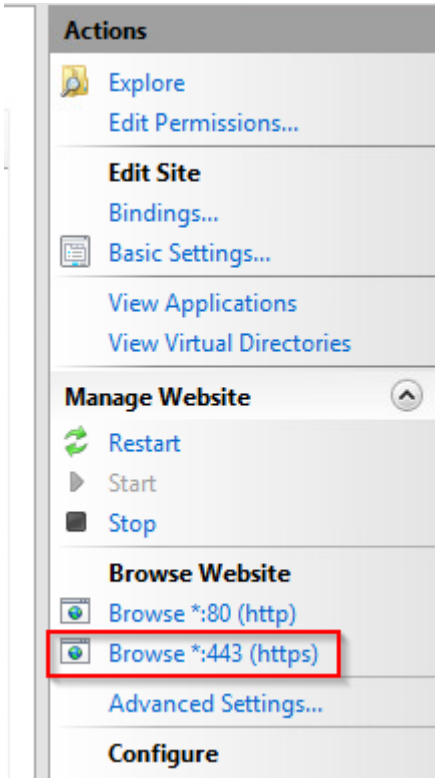


2. Les paramètres par défaut d'une nouvelle liaison sont définis sur HTTP sur le port 80. Pour Type, sélectionnez https. Sélectionnez le certificat auto-signé que vous avez créé dans la section précédente dans la liste déroulante Certificat SSL, puis cliquez sur OK.



3. 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.

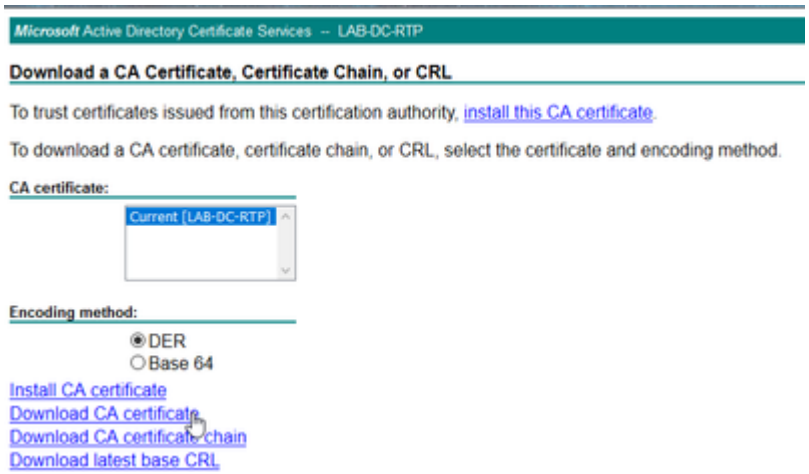




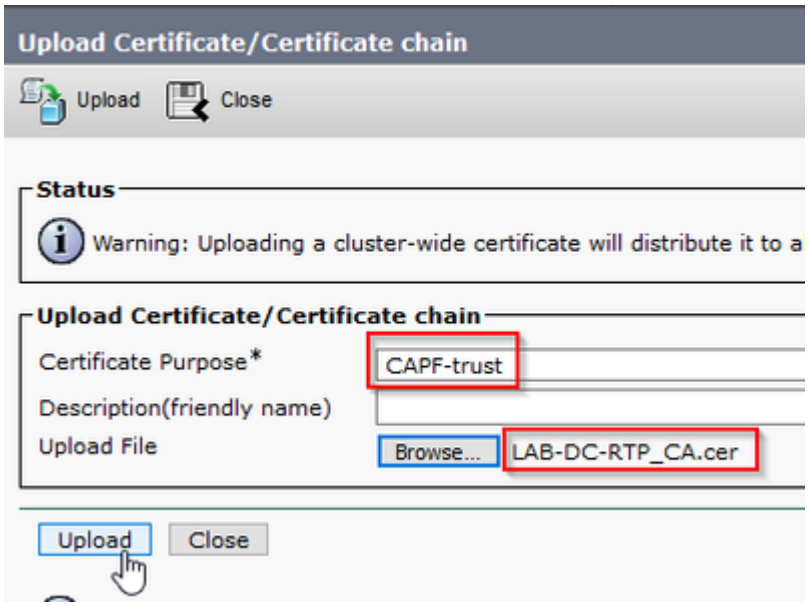
4. N'oubliez pas de redémarrer le service IIS après les modifications de configuration. Utilisez l'option Redémarrer du volet Actions.

Configuration CUCM

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

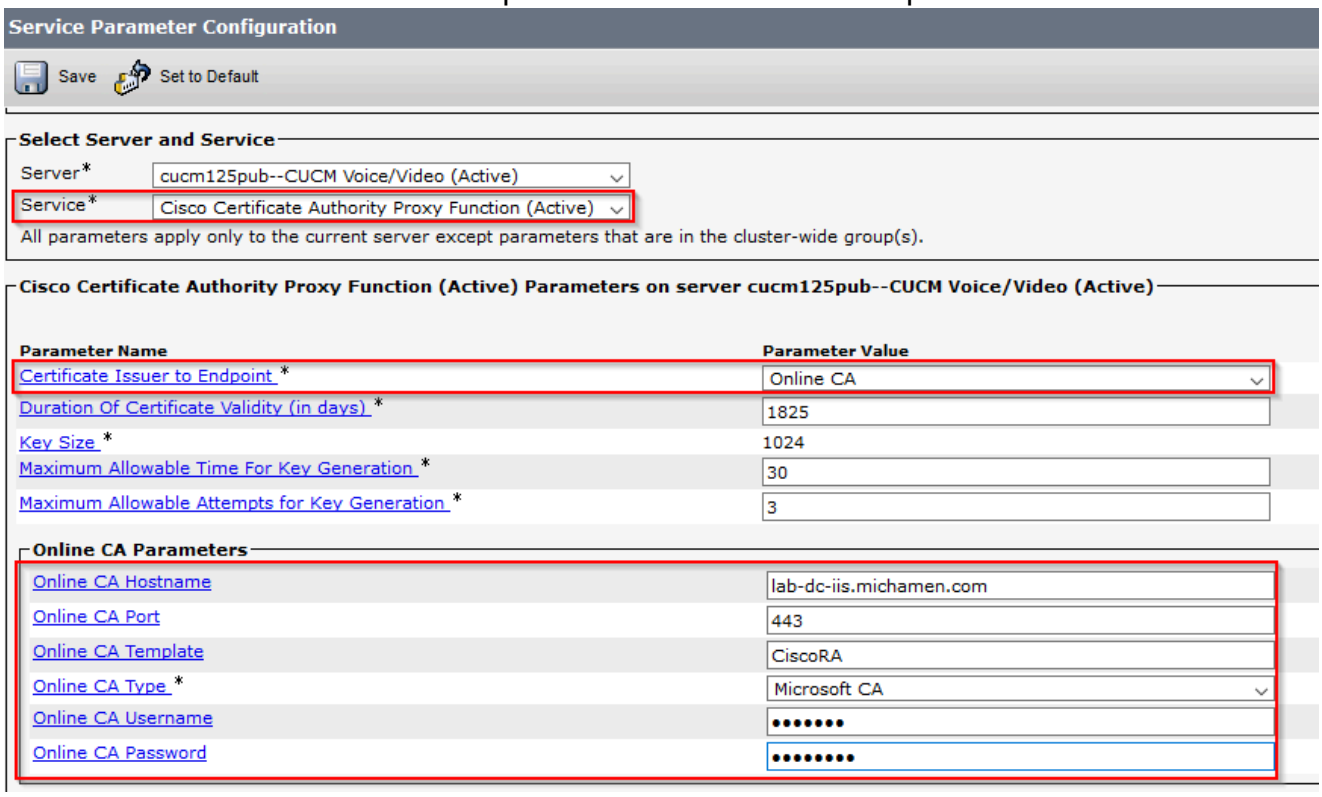


2. Accédez à Security > Certificate Management depuis la page OS Administration et sélectionnez le bouton Upload Certificate/Certificate chain pour télécharger le certificat CA avec l'objectif défini sur CAPF-trust.



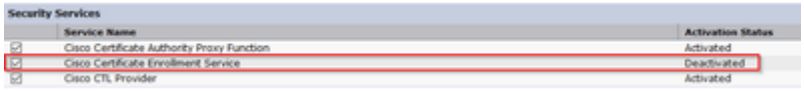
Téléchargez le même certificat CA que CallManager-trust car il est nécessaire si le chiffrement de signalisation sécurisé est activé pour les terminaux, ce qui est probable si le cluster est en mode mixte.

3. Accédez à System > Service Parameters. Sélectionnez le serveur de publication Unified CM dans le champ Serveur et la fonction Proxy de l'autorité de certification Cisco dans le champ Service.
4. Définissez la valeur de Certificate Issuer sur Endpoint sur Online CA et entrez les valeurs pour les 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.



5. Une fenêtre contextuelle vous informe que le service CAPF doit être redémarré.

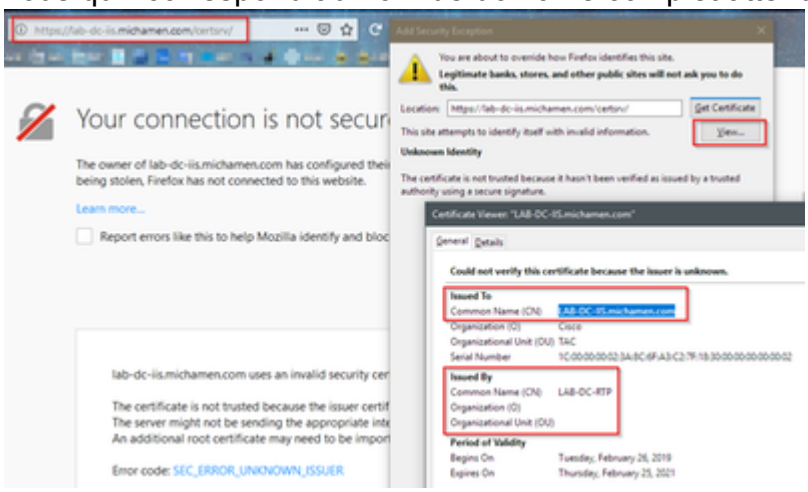
Commencez par activer le service d'inscription de certificat Cisco via Cisco Unified Serviceability > Tools > Service Activation, sélectionnez l'éditeur dans le champ server, activez la case à cocher Cisco Certificate Enrollment Service, puis cliquez sur le bouton Save.



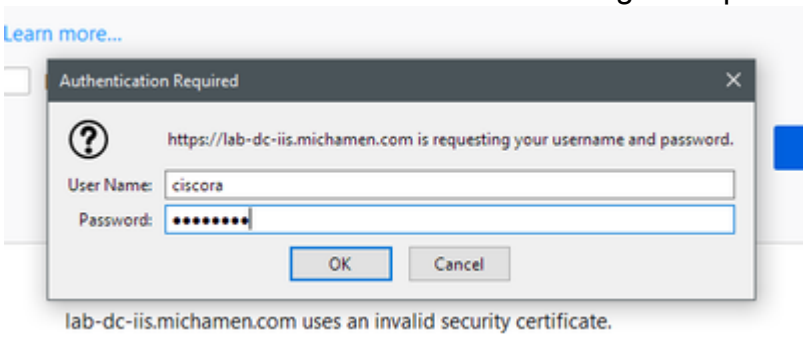
Vérifier

Vérifier les certificats IIS

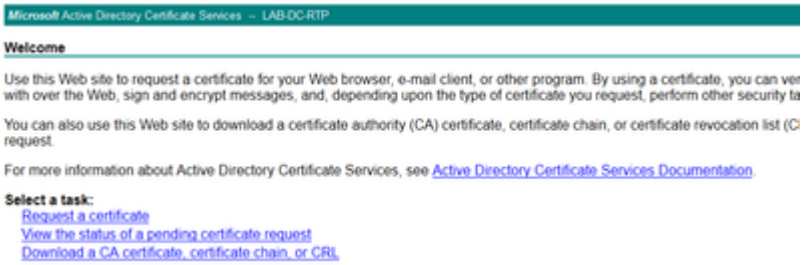
1. À partir d'un navigateur Web sur un PC connecté au serveur (de préférence sur le même réseau que le serveur de publication CUCM), accédez au nom de domaine complet de votre serveur (https://)YOUR_SERVER_FQDN/certsrv/).
2. L'alerte Certificat non approuvé s'affiche. Ajoutez l'exception et vérifiez le certificat. Assurez-vous qu'il correspond au nom de domaine complet attendu.



3. 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.



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



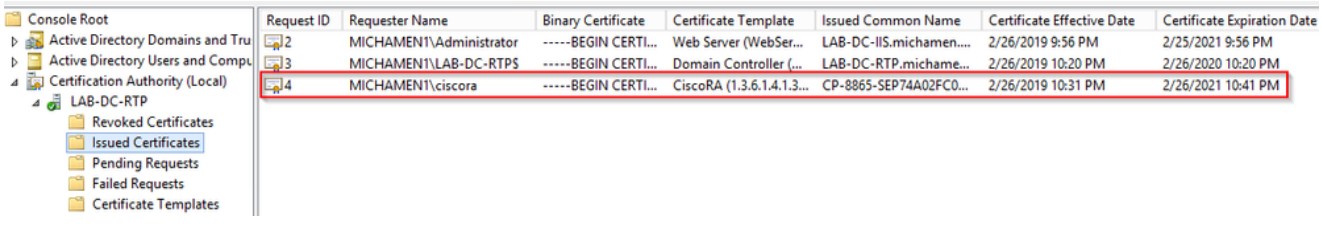
Vérification de la configuration CUCM

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

1. Ouvrez la page CallManager Administration, Device, puis Phone.
2. Cliquez sur le bouton Rechercher pour afficher les téléphones.
3. Sélectionnez le téléphone sur lequel vous souhaitez installer le contrôleur LSC.
4. Faites défiler jusqu'à Certification Authority Proxy Function (CAPF) Information.
5. Sélectionnez Install/Upgrade dans Certificate Operation (Opération de certificat).
6. Sélectionnez le mode d'authentification. (Par chaîne Null convient pour les tests.)
7. Faites défiler la page jusqu'en haut et sélectionnez save (enregistrer) puis Apply Config (Appliquer la configuration) pour le téléphone.
8. Après le redémarrage du téléphone et l'enregistrement, utilisez le filtre LSC Status pour confirmer que le LSC a été correctement installé.

Et continuez :

1. Côté serveur AD, ouvrez MMC et développez le composant logiciel enfichable Autorité de certification pour sélectionner le dossier Certificats émis.
2. L'entrée du téléphone s'affiche dans la vue récapitulative, avec les détails suivants :
   - ID de la demande : Numéro de séquence unique
   - Nom du demandeur : Le nom d'utilisateur du compte CiscoRA configuré doit être affiché.
   - Modèle de certificat : Le nom du modèle CiscoRA créé doit être affiché.
   - Nom usuel 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
- Documentation et assistance techniques

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.