MOBOTIX HUB – Guide des certificats

V2.03

Contenu

Droits d'auteur, marques de commerce et clause de non-responsabilité

Marques

MOBOTIX HUB est une marque déposée de MOBOTIX AG.

Microsoft et Windows sont des marques déposées de Microsoft Corporation. App Store est une marque de service d' Apple Inc. Android est une marque commerciale de Google Inc.

Toutes les autres marques commerciales mentionnées dans ce document sont des marques commerciales de leurs propriétaires respectifs.

Démenti

Ce texte n'est destiné qu'à des fins d'information générale, et son préparation a fait l'objet d'un soin particulier.

Tout risque découlant de l'utilisation de ces informations incombe au destinataire, et rien dans les présentes ne doit être interprété comme constituant une quelconque garantie.

MOBOTIX AG se réserve le droit d'effectuer des adaptations sans préavis.

Tous les noms de personnes et d'organisations utilisés dans les exemples de ce texte sont fictifs. Toute ressemblance avec une organisation ou une personne réelle, vivante ou morte, est purement fortuite et involontaire.

Ce produit peut utiliser des logiciels tiers pour lesquels des conditions générales spécifiques peuvent s'appliquer. Dans ce cas, vous trouverez plus d'informations dans le fichier 3rd_party_software_terms_and_conditions.txt situé dans le dossier d'installation de votre système MOBOTIX.

À propos de ce guide

Ce guide vous présente le chiffrement et les certificats, ainsi que les procédures étape par étape sur l'installation de certificats dans un environnement de groupe de travail Windows.

MOBOTIX vous recommande de mettre en place une infrastructure à clé publique (PKI) pour la création et la distribution de certificats. Une PKI est un ensemble de rôles, de politiques, de matériel, de logiciels et de procédures nécessaires à la création, à la gestion, à la distribution, à l'utilisation, au stockage et à la révocation de certificats numériques et à la gestion du chiffrement à clé publique. Dans un domaine Windows, il est recommandé d'établir une infrastructure à clé publique à l'aide des services de certificats Active Directory (AD CS).
Si vous n'êtes pas en mesure de créer une PKI, soit parce que vous avez différents domaines sans confiance entre eux, soit parce que vous n'utilisez pas de domaines du tout, il est possible de créer et de distribuer manuellement des certificats.
AVERTISSEMENT : La création et la distribution manuelles de certificats ne sont pas recommandées comme moyen sécurisé de distribution de certificats. Si vous choisissez la distribution manuelle, vous êtes responsable de la sécurité permanente des certificats privés. Lorsque vous assurez la sécurité des certificats privés, les

Quand avez-vous besoin d'installer des certificats ?

Tout d'abord, décidez si votre système a besoin d'une communication cryptée.

N'utilisez pas de certificats avec chiffrement du serveur d'enregistrement si vous utilisez une ou plusieurs intégrations qui ne prennent pas en charge la communication HTTPS. Il s'agit, par exemple, d'intégrations tierces du SDK MIP qui ne prennent pas en charge HTTPS.

À moins que votre installation ne soit effectuée dans un réseau physiquement isolé, il est recommandé de sécuriser la communication à l'aide de certificats.

Ce document décrit quand utiliser les certificats :

- Si votre système MOBOTIX HUB VMS est configuré dans un environnement de groupe de travail Windows
- Avant d'installer ou de mettre à niveau vers MOBOTIX HUB VMS 2019 R1 ou une version ultérieure, si vous souhaitez activer le chiffrement pendant l'installation.
- Avant d'activer le chiffrement, si vous avez installé MOBOTIX HUB VMS 2019 R1 ou une version ultérieure sans chiffrement
- Lorsque vous renouvelez ou remplacez des certificats en raison de leur expiration

Introduction aux certificats

Le protocole HTTPS (Hypertext Transfer Protocol Secure) est une extension du protocole HTTP (Hypertext Transfer Protocol) pour la communication sécurisée sur un réseau informatique. En HTTPS, le protocole de communication est chiffré à l'aide de TLS (Transport Layer Security) ou de son prédécesseur, SSL (Secure Sockets Layer).

Dans les machines virtuelles Mobotix Hub, la communication sécurisée est obtenue à l'aide de TLS/SSL avec chiffrement asymétrique (RSA). TLS/SSL utilise une paire de clés, l'une privée et l'autre publique, pour authentifier, sécuriser et gérer les connexions sécurisées.

Une autorité de certification (CA) est toute personne qui peut émettre des certificats racines. Il peut s'agir d'un service Internet qui émet des certificats racines, ou de toute personne qui génère et distribue manuellement un certificat. Une autorité de certification peut émettre des certificats pour des services Web, c'est-à-dire pour tout logiciel utilisant la communication https. Ce certificat contient deux clés, une clé privée et une clé publique. La clé publique est installée sur les clients d'un service web (service clients) par l'installation d'un certificat public. La clé privée est utilisée pour signer les certificats de serveur qui doivent être installés sur le serveur.
Chaque fois qu'un client de service appelle le service Web, celui-ci envoie le certificat du serveur, y compris la clé publique, au client. Le client de service peut valider le certificat du serveur à l'aide du certificat d'autorité de certification publique déjà installé. Le client et le serveur peuvent désormais utiliser les certificats de serveur public et privé pour échanger une clé secrète et établir ainsi une connexion TLS/SSL sécurisée.

Pour les certificats distribués manuellement, les certificats doivent être installés avant que le client puisse effectuer une telle vérification.

Pour plus d'informations sur TLS, consultez Sécurité de la couche transport.

Dans les machines virtuelles Mobotix Hub, vous pouvez activer le chiffrement TLS/SSL aux emplacements suivants :

- Dans la communication entre le serveur de gestion et les serveurs d'enregistrement, les serveurs d'événements et les serveurs mobiles
- Sur le serveur d'enregistrement, dans la communication avec les clients, les serveurs et les intégrations qui récupèrent les flux de données du serveur d'enregistrement.
- Dans la communication entre les clients et le serveur mobile

Dans ce guide, les éléments suivants sont appelés clients :

- MOBOTIX HUB Desk Client
- Client de gestion
- Serveur de gestion (pour le Moniteur système et pour les images et les clips vidéo AVI dans les notifications par e-mail)
- Serveur mobile MOBOTIX HUB
- Serveur d'événements MOBOTIX HUB
- MOHUB MOBOTIX LPR
- Pont de réseau ouvert MOBOTIX

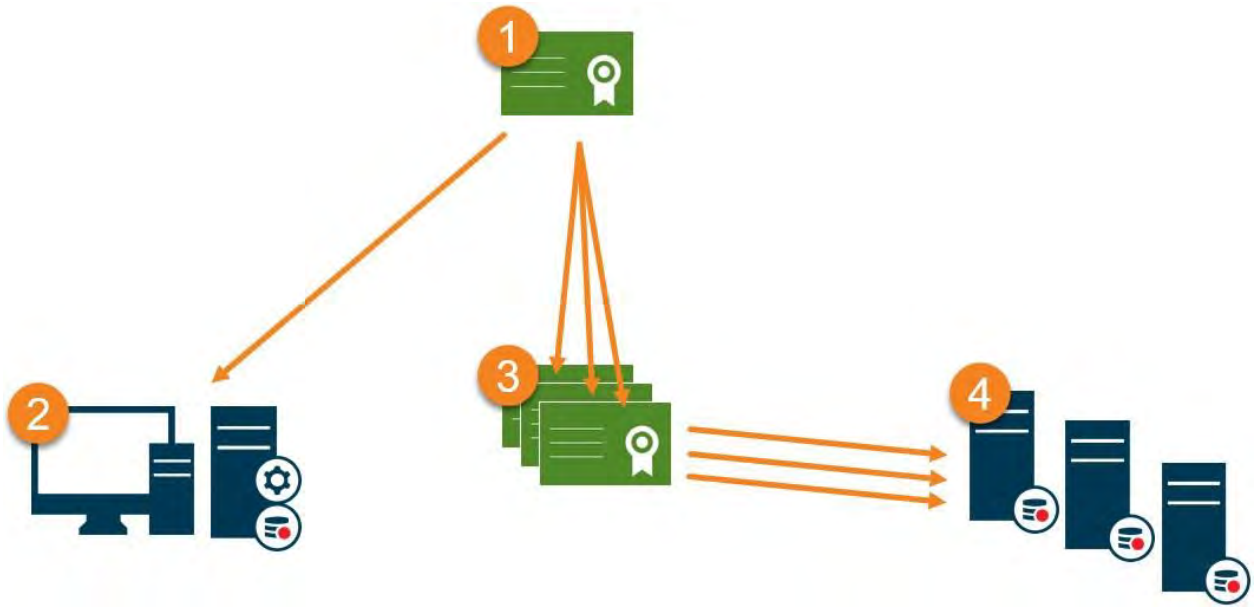
- Serveur DLNA MOBOTIX HUB
- Sites qui récupèrent des flux de données à partir du serveur d'enregistrement via Milestone Interconnect
- Intégrations SDK MIP tierces prenant en charge HTTPS

Pour les solutions créées avec MIP SDK 2018 R3 ou version antérieure qui

- Si les intégrations sont effectuées à l'aide des bibliothèques MIP SDK, elles doivent être reconstruites avec
- Si les intégrations communiquent directement avec les API du serveur d'enregistrement sans
- En cas de doute, demandez à votre fournisseur qui a

Distribution des certificats

Le graphique illustre le concept de base de la signature, de l'approbation et de la distribution des certificats dans les machines virtuelles MOBOTIX HUB.



1 Une autorité de certification (CA) est toute personne qui peut émettre des certificats racines. Un certificat d'autorité de certification agit en tant que tiers de confiance , approuvé à la fois par le sujet/propriétaire (serveur) et par la partie qui vérifie le certificat (clients) (voir Créer un certificat d'autorité de certification à la page 17).

2 Le certificat public doit être approuvé sur tous les ordinateurs clients. De cette façon, les clients peuvent vérifier la validité des certificats émis par l'autorité de certification (voir Installer les certificats sur les clients à la page 19).

3 Le certificat CA est utilisé pour émettre des certificats d'authentification de serveur privé aux serveurs (voir Créer un certificat SSL à la page 27).

❹ Les certificats SSL privés créés doivent être importés dans le magasin de certificats Windows sur tous les serveurs (voir Importer un certificat SSL à la page 29).

Conditions requises pour le certificat SSL privé :

- Attribué au serveur afin que le nom d'hôte du serveur soit inclus dans le certificat, soit en tant qu'objet (propriétaire), soit dans la liste des noms DNS auxquels le certificat est émis
- Approuvé sur tous les ordinateurs exécutant des services ou des applications qui communiquent avec le service sur les serveurs, en faisant confiance au certificat de l'autorité de certification utilisé pour émettre le certificat SSL.
- Le compte de service qui exécute le serveur doit avoir accès à la clé privée du certificat sur le serveur.

Les certificats ont une date d'expiration. Vous ne recevrez pas d'avertissement lorsqu'un certificat est sur le point d'expirer. Si un certificat expire, les clients ne feront plus confiance au serveur avec le certificat expiré et ne pourront donc pas communiquer avec lui.
Pour renouveler les certificats, suivez les étapes de ce guide comme vous l'avez fait lors de la création des certificats.

Vue d'ensemble des scénarios et des procédures utilisés avec les certificats

Les procédures de configuration de la communication sécurisée dans un environnement MOBOTIX HUB VMS sont différentes selon le type de serveur nécessitant une communication sécurisée.

Les procédures sont également différentes dans un réseau WORKGROUP par rapport à un réseau DOMAIN.

Les types d'applications clientes MOBOTIX HUB VMS qui sont utilisés dans le système déterminent également certaines des procédures requises pour les communications sécurisées.

> L'utilisation de certificats pour la communication du serveur peut généralement être ignorée sur une installation de serveur unique , sauf pour servir de protection supplémentaire lors de la communication avec le serveur de gestion.

Cette liste présente les différents scénarios :

- Serveur mobile MOBOTIX HUB

  Dans les machines virtuelles Mobotix Hub, le chiffrement est activé ou désactivé par serveur mobile. Vous pouvez activer ou désactiver le chiffrement lors de l'installation du produit MOBOTIX HUB VMS ou à l'aide du configurateur de serveur. Lorsque vous activez le chiffrement sur un serveur mobile, vous utilisez ensuite une communication chiffrée avec tous les clients, services et intégrations qui récupèrent les flux de données.

  Le serveur mobile se connecte au client mobile MOBOTIX HUB et au client Web MOBOTIX HUB. Les navigateurs, les systèmes d'exploitation et les appareils mobiles qui hébergent ces clients tiennent à jour une liste de certificats racines d'autorité de certification approuvés. Seule l'autorité connaît sa clé privée, mais tout le monde connaît sa clé publique, qui est similaire à n'importe quel certificat particulier .

  Ces clients ont donc déjà des clés de certificat installées et fonctionnent avec la plupart des certificats tiers disponibles pour l'installation sur le serveur mobile lui-même.

  Étant donné que chaque autorité de certification tierce a ses propres exigences pour demander un certificat, il est préférable d' examiner les exigences individuelles directement auprès de l'autorité de certification.

  Ce document décrit comment créer une demande de certificat sur le serveur mobile et installer le certificat une fois qu'il a été émis par l'autorité de certification.

  Voir:

  Installez les certificats pour la communication avec le serveur mobile à la page 40

- Serveur de gestion et serveur d'enregistrement MOBOTIX HUB

  Vous pouvez chiffrer la connexion bidirectionnelle entre le Serveur de gestion et le Serveur d'enregistrement. Lorsque vous activez le chiffrement sur le Serveur de gestion, il s'applique aux connexions de tous les Serveurs d'enregistrement qui se connectent au Serveur de gestion. Si vous activez le chiffrement sur le Serveur de gestion, vous devez également l'activer sur tous les serveurs d'enregistrement. Avant d'activer le chiffrement, vous devez installer des certificats de sécurité sur le Serveur de gestion et sur tous les serveurs d'enregistrement, y compris les serveurs d'enregistrement de basculement.

  - Certificat d'autorité de certification d'un tiers ou d'un organisme commercial

    Le processus de demande de certificats auprès d'autorités de certification tierces pour une utilisation avec les serveurs de gestion et les serveurs d'enregistrement est le même qu'avec le serveur mobile. La seule différence est la configuration avec le configurateur de serveur.

    Voir:

    Installez des certificats d'autorité de certification tiers ou commerciaux pour la communication avec le serveur de gestion ou le serveur d'enregistrement à la page 57

  - Domaine

    Lorsque les points de terminaison client et serveur fonctionnent tous dans un environnement de domaine avec sa propre infrastructure d'autorité de certification, il n'est pas nécessaire de distribuer des certificats d'autorité de certification aux postes de travail clients. Tant que vous disposez d'une stratégie de groupe au sein du domaine, celle-ci gérera la distribution automatique de tous les certificats d'autorité de certification approuvés à tous les utilisateurs et ordinateurs du domaine.

    Le processus de demande de certificat et d'installation d'un certificat de serveur est le même que dans un groupe de travail.

    Voir:

    Installez des certificats dans un domaine pour la communication avec le Serveur de gestion ou le Serveur d'enregistrement à la page 86

  - Groupe de travail

    Lorsque vous utilisez un environnement de groupe de travail, il est supposé qu'il n'existe pas d'infrastructure d'autorité de certification. Pour distribuer des certificats, il est nécessaire de créer une infrastructure d'autorité de certification. Il est également nécessaire de distribuer les clés de certificat aux postes de travail clients. À l'exception de ces exigences, le processus de demande et d'installation d'un certificat sur un serveur est similaire à celui du domaine et des scénarios tiers.

    Voir:

    Installez les certificats dans un environnement de groupe de travail pour la communication avec le serveur de gestion ou le serveur d'enregistrement à la page 104

- Serveur d'événements MOBOTIX HUB

  Vous pouvez chiffrer la connexion bidirectionnelle entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements, y compris le serveur LPR. Lorsque vous activez le chiffrement sur le serveur d'événements , il s'applique aux connexions de tous les composants qui se connectent au serveur d'événements. Avant d'activer le chiffrement, vous devez installer des certificats de sécurité sur le serveur d'événements et tous les composants de connexion.

  Voir:

  Installez les certificats pour la communication avec le serveur d'événements à la page 126

- Client

  Dans les scénarios Tiers/commercial et Domaine, les clients n'ont pas besoin d'installer de clés de certificat. Vous devez uniquement installer les clés de certificat client dans un environnement de groupe de travail.

  Lorsque vous activez le chiffrement sur un serveur d'enregistrement, la communication avec tous les clients, serveurs et intégrations qui récupèrent les flux de données à partir du serveur d'enregistrement est chiffrée.

  Dans ce document, ils sont appelés « clients » du serveur d'enregistrement :

  - MOBOTIX HUB Desk Client
  - Client de gestion
  - Serveur de gestion (pour le Moniteur système et pour les images et les clips vidéo AVI dans les notifications par e-mail)
  - Serveur mobile MOBOTIX HUB
  - Serveur d'événements MOBOTIX HUB
  - MOHUB MOBOTIX LPR
  - Pont réseau MOBOTIX
  - Serveur DLNA MOBOTIX HUB
  - Sites qui récupèrent des flux de données à partir du serveur d'enregistrement via MOBOTIX Interconnect
  - Certaines intégrations tierces du SDK MIP

- 

  Pour les solutions créées avec MIP SDK 2018 R3 ou version antérieure qui accède aux serveurs d'enregistrement : si les intégrations sont effectuées à l'aide des bibliothèques MIP SDK, elles doivent être reconstruites avec MIP SDK 2019 R1 ; si les intégrations communiquent directement avec les API du serveur d'enregistrement sans utiliser les bibliothèques MIP SDK, les intégrateurs doivent ajouter eux-mêmes la prise en charge HTTPS.

  Voir:

  Quels clients ont besoin de certificats ? à la page 11

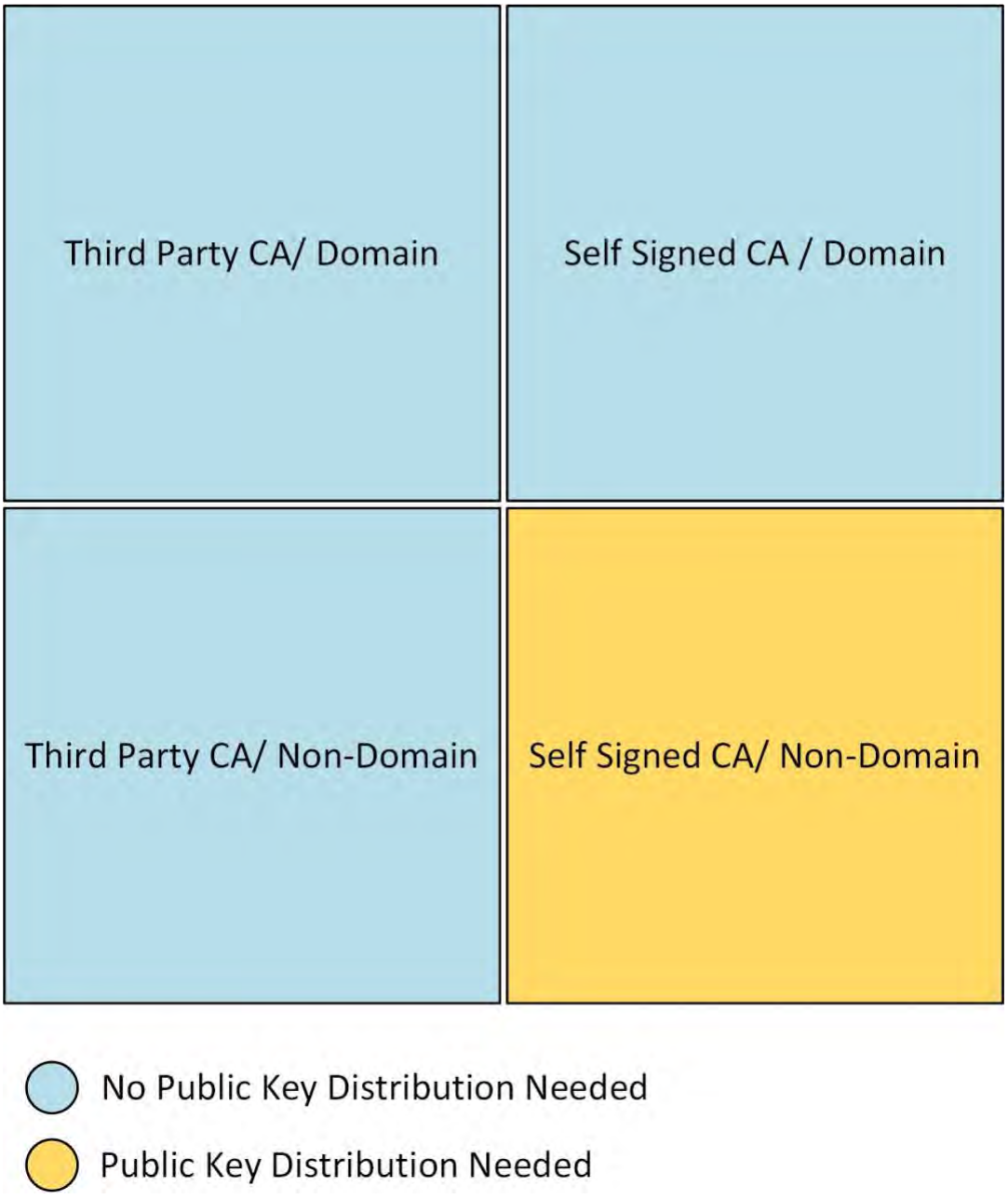
  Importer les certificats clients à la page 129

Quels clients ont besoin de certificats ?

Quels clients ont besoin d'installer des certificats ? Comment planifions-nous cela ? Que pouvons-nous faire pour nous préparer ?

Les clients basés sur un navigateur Web et les clients distribués via un service ou un magasin public de distribution d'applications tiers, par exemple Google Play ou Apple AppStore, ne doivent pas nécessiter l'installation d'un certificat. MOBOTIX HUB Mobile n'utilisera pas les certificats installés. MOBOTIX HUB Mobile ne peut utiliser que des certificats de tiers de confiance.

Si les serveurs MOBOTIX HUB (Serveur de gestion et Serveur d'enregistrement) sont installés sur des ordinateurs connectés au Domaine, et que les utilisateurs qui se connectent au Client de bureau sont tous des utilisateurs du Domaine, le Domaine se chargera de la distribution de toutes les clés publiques et de l'authentification nécessaires à l'établissement de communications sécurisées.



Ce n'est que dans un scénario où les services de certificats Active Directory (AD CS) sont utilisés pour créer des certificats auto-signés et où les ressources (utilisateurs et ordinateurs) fonctionnent dans un environnement hors domaine qu'il serait nécessaire de distribuer des clés publiques aux postes de travail clients.

Voir aussi Installer des certificats sur les clients à la page 19 et Importer des certificats clients à la page 129.

Configurateur de serveur (expliqué)

Utilisez le configurateur de serveur pour sélectionner des certificats sur des serveurs locaux pour une communication chiffrée et enregistrer les services de serveur afin de les rendre aptes à communiquer avec les serveurs.

Les types de serveurs suivants dans les MOBOTIX HUB VMS nécessitent des certificats pour une communication sécurisée :

- Serveurs de gestion
- Serveurs d'enregistrement
- Serveurs d'événements
- Serveurs mobiles

Ces serveurs fonctionnent avec le configurateur de serveur pour gérer les communications sécurisées. Utilisez le configurateur de serveur pour déterminer si les serveurs MOBOTIX HUB utilisent ou non des communications cryptées sécurisées et pour gérer les certificats utilisés par les serveurs MOBOTIX HUB.

Le configurateur de serveur est installé par défaut sur tout ordinateur hébergeant un serveur MOBOTIX HUB.

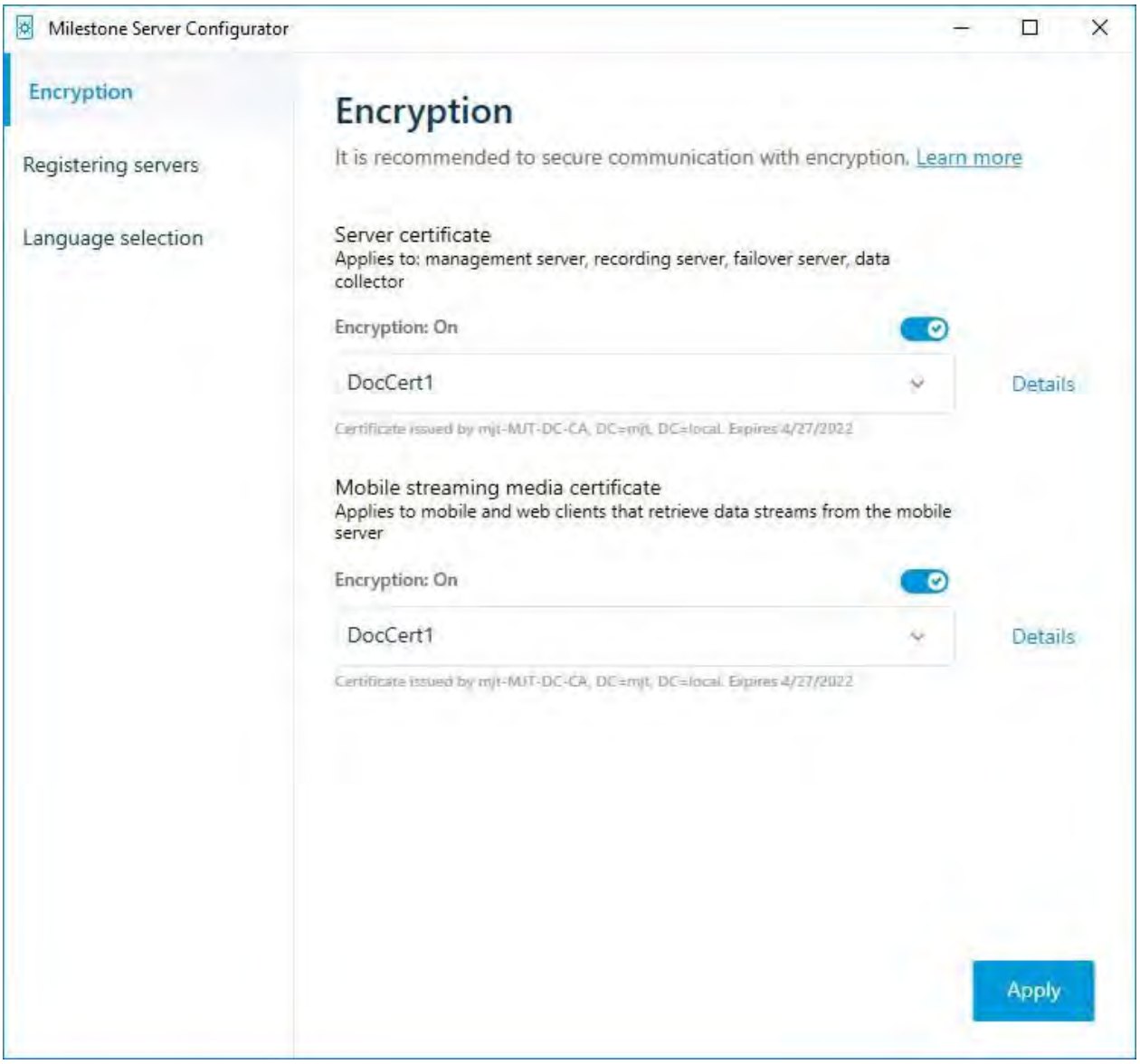
Ouvrez le configurateur de serveur à partir de :

- Le menu Démarrer de

  Windows

  ou

- Le gestionnaire de serveur MOBOTIX HUB en cliquant avec le bouton droit de la souris sur l'icône du gestionnaire de serveur dans la barre des tâches de l'ordinateur et en sélectionnant Configurateur de serveur



Utilisez le configurateur de serveur pour choisir les certificats que les serveurs MOBOTIX HUB utilisent pour sécuriser les communications avec leurs applications clientes et pour vérifier que les paramètres de cryptage sont correctement configurés.

Dans la section **Chiffrement** du configurateur de serveur, définissez les types de chiffrement suivants :

- **Certificat de serveur**

  Sélectionnez le certificat à utiliser pour chiffrer la connexion bidirectionnelle entre le serveur de gestion et les serveurs suivants :

  - Serveur d'enregistrement
  - Serveur d'événements
  - Serveur de journaux
  - Serveur LPR
  - Serveur mobile

- **Serveur d'événements et add-ons**

  Sélectionnez le certificat à utiliser pour chiffrer la connexion bidirectionnelle entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements, y compris le serveur LPR.

- **Certificat de diffusion multimédia en continu**

  Sélectionnez le certificat à utiliser pour chiffrer la communication entre les serveurs d'enregistrement et tous les clients, serveurs et intégrations qui récupèrent les flux de données à partir des serveurs d'enregistrement.

- **Certificat de diffusion multimédia mobile**

  Sélectionnez le certificat à utiliser pour chiffrer la communication entre le serveur mobile et les clients mobiles et Web qui récupèrent les flux de données à partir du serveur mobile.

Dans la section **Enregistrement des serveurs** du configurateur de serveurs, enregistrez les serveurs qui s'exécutent sur l'ordinateur auprès du serveur de gestion désigné.

Pour enregistrer les serveurs, vérifiez l'adresse du serveur de gestion et sélectionnez **Enregistrer**.

Scripts PowerShell

Vous pouvez utiliser PowerShell et le module PSTools de Milestone pour installer, intégrer, simplifier, surveiller et automatiser la maintenance continue et les processus de configuration requis des systèmes MOBOTIX HUB VMS de grande taille, complexes et techniquement avancés.

Néanmoins, MOBOTIX recommande aux administrateurs, installateurs et techniciens de savoir comment configurer manuellement l'environnement MOBOTIX HUB VMS de leur client. Vous apprendrez avec l'expérience à utiliser des scripts PowerShell à la place des configurations manuelles. Vous pouvez trouver des scripts PowerShell aux emplacements suivants :

- Processus/Vidéo PowerShell pour serveur mobile et permet de chiffrer
- Dépôt Github pour les informations, la documentation et les scripts Milestone PSTools.

Création et distribution manuelles de certificats

Important à savoir :

> ⚠ La création et la distribution manuelles de certificats ne sont pas recommandées en tant que moyen sécurisé de distribution de certificats. Si vous choisissez la distribution manuelle, vous êtes responsable de la sécurité des certificats privés à tout moment. Lorsque vous assurez la sécurité des certificats privés , les ordinateurs clients qui font confiance aux certificats sont moins vulnérables aux attaques.

Dans certaines situations, Windows Update peut supprimer périodiquement des certificats qui ne proviennent pas d'une « autorité de certification tierce de confiance ».

Pour vous assurer que vos certificats ne sont pas supprimés par Windows Update, vous devez activer l' **option Désactiver la mise à jour automatique des certificats racines**. Avant d'effectuer cette modification, vous devez vous assurer qu'elle respecte la politique de sécurité de votre entreprise.

1. Pour ce faire, ouvrez l' **éditeur de stratégie de groupe local** sur l'ordinateur (cliquez sur la barre de démarrage de Windows et tapez **gpedit.msc**).
2. Dans l'Éditeur de **stratégie de groupe local** Windows, accédez à **Configuration de l'ordinateur** > **Modèles d'administration** > Gestion des communications Internet > système **>** Paramètres de communication Internet**.**
3. Double-cliquez sur **Désactiver la mise à jour automatique du certificat racine** et sélectionnez **Activé**.
4. Cliquez sur **OK**.

Notez que ce paramètre peut être contrôlé par une stratégie de domaine. Dans ce cas, il doit être désactivé à ce niveau.

Votre certificat reste désormais sur l'ordinateur même s'il ne provient pas d'une « autorité de certification tierce approuvée », car Windows Update ne contacte pas le site Web Windows Update pour voir si Microsoft a ajouté l'autorité de certification à sa liste d'autorités de confiance.

Création d'un certificat d'autorité de certification

Sur un ordinateur à accès restreint et non connecté à votre système MOBOTIX HUB, exécutez ce script une fois pour créer un certificat d'autorité de certification.

> ⚠ L'ordinateur que vous utilisez pour créer des certificats doit exécuter Windows 10 ou Windows Server OS 2016 ou plus récent.

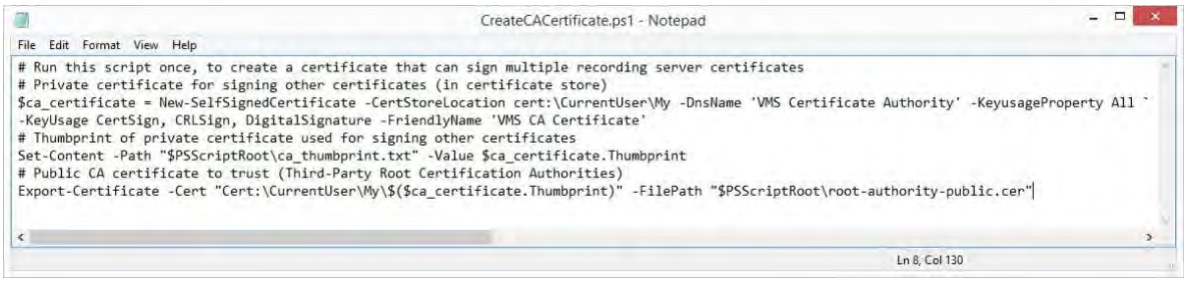
N'oubliez pas que lorsque vous créez des certificats de cette manière, ceux-ci sont liés à l'ordinateur sur lequel ils sont installés. Si le nom de l'ordinateur change, le VMS ne pourra pas démarrer tant que les certificats n'auront pas été recréés et réinstallés sur l'ordinateur.

Ce script crée deux certificats :

- Un certificat privé n'existe dans le magasin des certificats personnels que pour l'utilisateur actuel après l'exécution du script . Il est recommandé de créer une sauvegarde conservée sur un support (USB) dans un endroit sûr, et de préférence deux sauvegardes conservées dans des endroits physiquement différents. À l'exception des sauvegardes, ce certificat ne doit jamais quitter l'ordinateur sur lequel vous l'avez créé
- Un certificat public : à importer en tant que certificat approuvé sur tous les ordinateurs clients

1. Dans l'annexe A, à la fin de ce guide, vous trouverez un script pour créer le certificat CA. Copiez le contenu.
2. Ouvrez le Bloc-notes et collez le contenu.

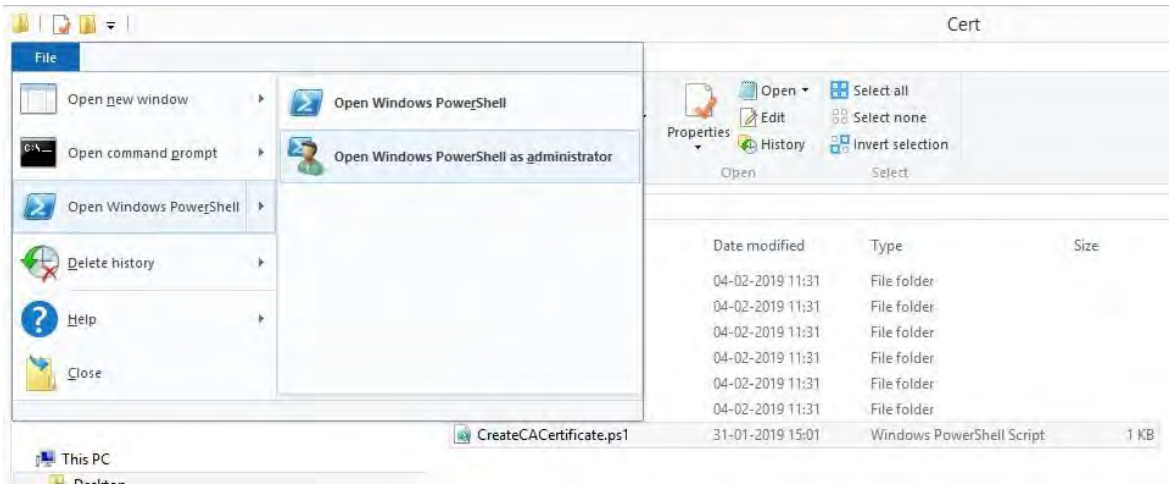
   Il est très important que les lignes se brisent aux mêmes endroits qu'à l'annexe A. Vous pouvez ajouter les sauts de ligne dans le Bloc-notes ou réouvrir ce PDF avec Google Chrome, copier à nouveau le contenu et le coller dans le Bloc-notes.



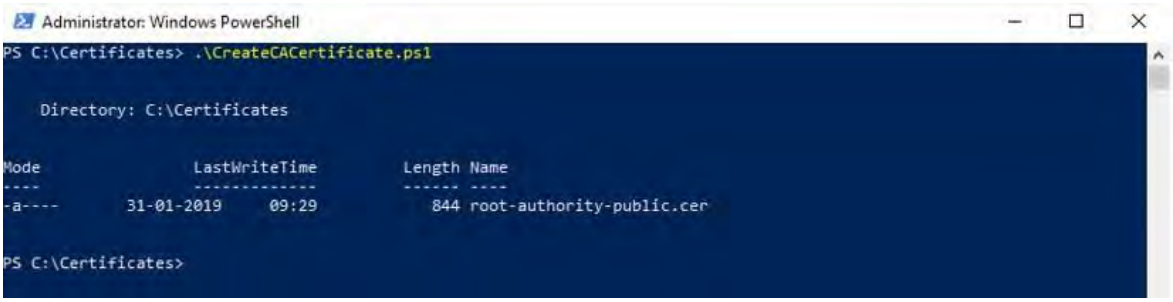
3. Dans le Bloc-notes, cliquez sur **Fichier** -> **Enregistrer sous**, nommez le fichier **CreateCACertificate.ps1** et enregistrez-le localement, comme suit :

   C :\Certificates\CreateCACertificate.ps1.

4. Dans l'Explorateur de fichiers, allez dans C :\Certificates et sélectionnez le **fichier CreateCACertificate.ps1**.
5. Dans le menu **Fichier**, sélectionnez **Ouvrir Windows PowerShell**, puis **Ouvrir Windows PowerShell en tant qu'administrateur**.



6. Dans PowerShell, à l'invite, entrez **.\CreateCACertificate.ps1** et appuyez sur **Entrée**.



7. Vérifiez que le **fichier root-authority-public.cer** apparaît dans le dossier dans lequel vous avez exécuté le script.

> Il se peut que vous demandiez à votre ordinateur de modifier la stratégie d'exécution PowerShell. Si oui, entrez **Set-ExecutionPolicy RemoteSigned**. Appuyez sur **Entrée** et sélectionnez **A**.

Installer les certificats sur les clients

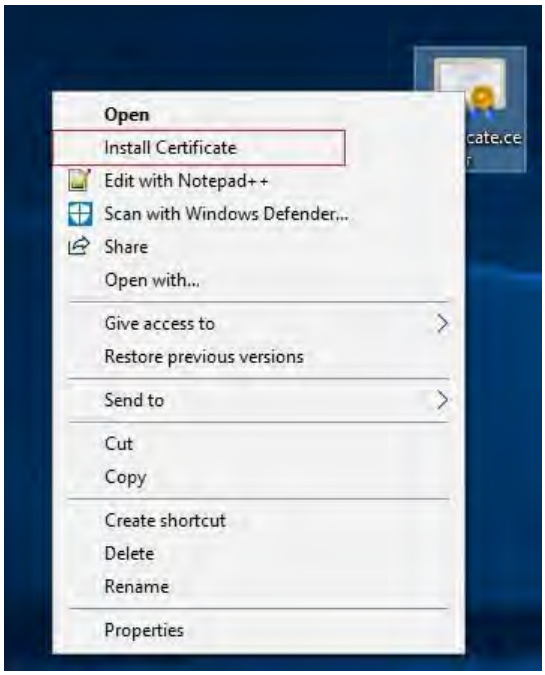
Après avoir créé le certificat d'autorité de certification, vous devez approuver le certificat d'autorité de certification public en l'installant sur tous les ordinateurs qui agissent en tant que clients du service, conformément aux descriptions de la section Introduction aux certificats à la page 5.

> Reportez-vous à la section Importer des certificats client à la page 129 pour une procédure alternative à l'installation manuelle des certificats sur les clients.

1. Copiez le fichier root-authority-public.cer de l'ordinateur sur lequel vous avez créé le certificat d'autorité de certification (C :\Certificates\root-authority-public.cer) sur l'ordinateur sur lequel le client MOBOTIX HUB est installé.

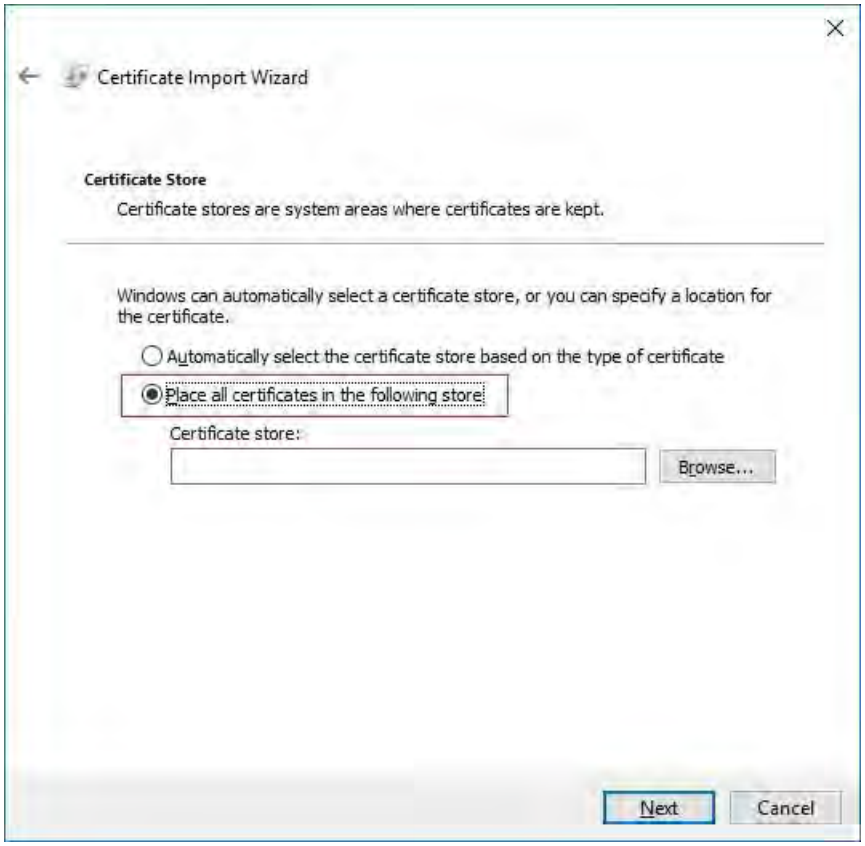
   > ⚠ Pour plus d'informations sur les services client et serveur, ainsi que sur les intégrations qui nécessitent le certificat, consultez Présentation des certificats à la page 5.

2. Cliquez avec le bouton droit de la souris sur le certificat et sélectionnez Installer le **certificat**.



3. Dans l' **Assistant Importation de certificat**, choisissez d'installer le certificat dans le magasin de l' **ordinateur local** et cliquez sur **Suivant**.

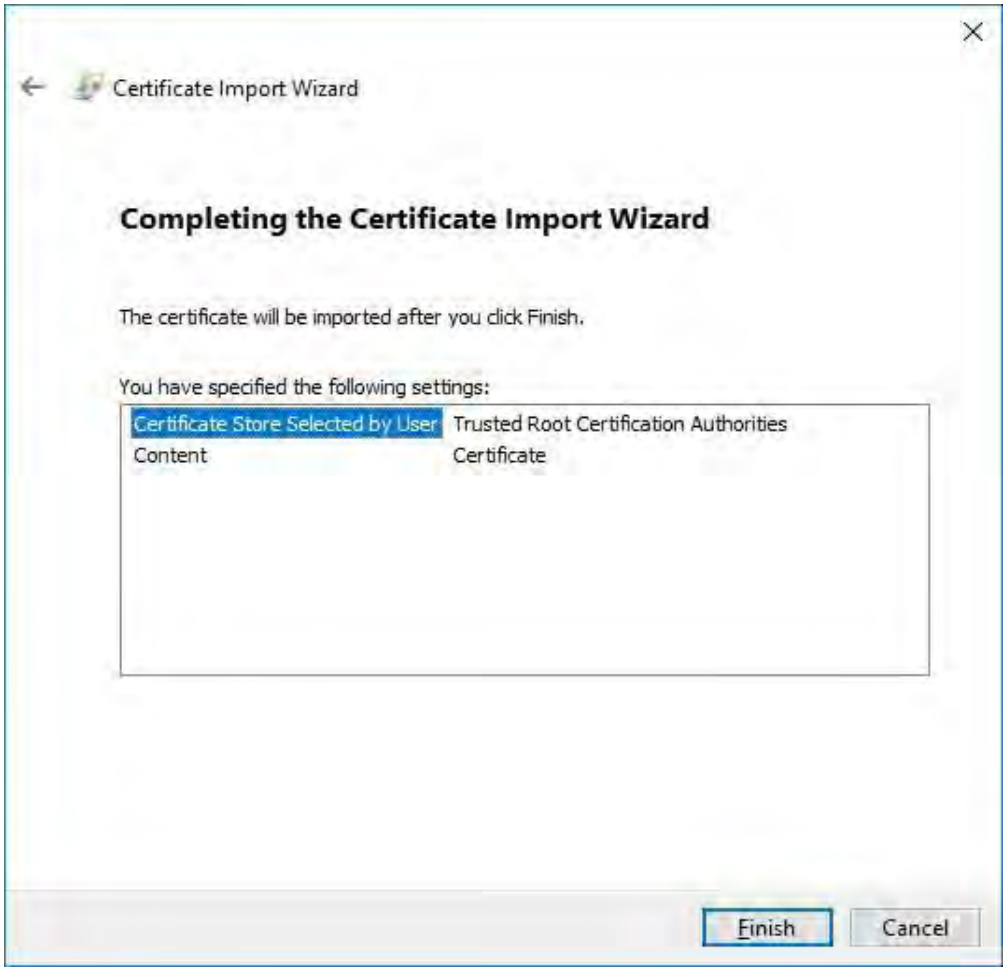
4. Sélectionnez cette option pour localiser manuellement le magasin dans lequel le certificat sera installé.



5. Cliquez sur **Parcourir**, sélectionnez **Autorités de certification racine approuvées** , puis cliquez sur **OK**. Cliquez ensuite sur **Suivant**.

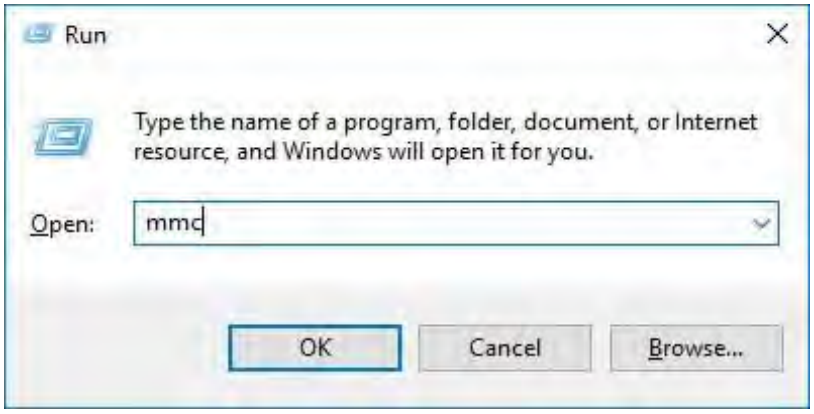
6. Dans la boîte de dialogue **Fin de l'assistant d'importation de certificat**, cliquez sur **Terminer**.

Si vous recevez un avertissement de sécurité indiquant que vous êtes sur le point d'installer un certificat racine, cliquez sur **Oui** pour continuer.

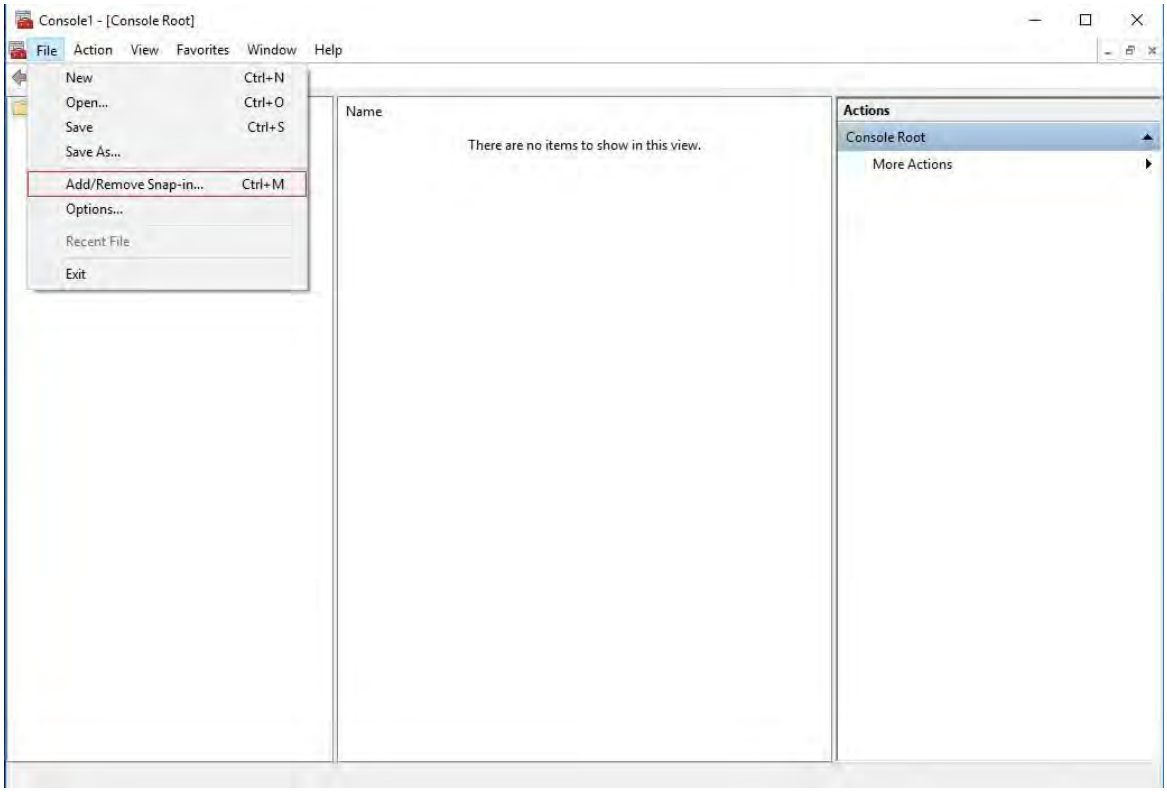


7. Vous recevrez une boîte de dialogue de confirmation de la réussite de l'importation.

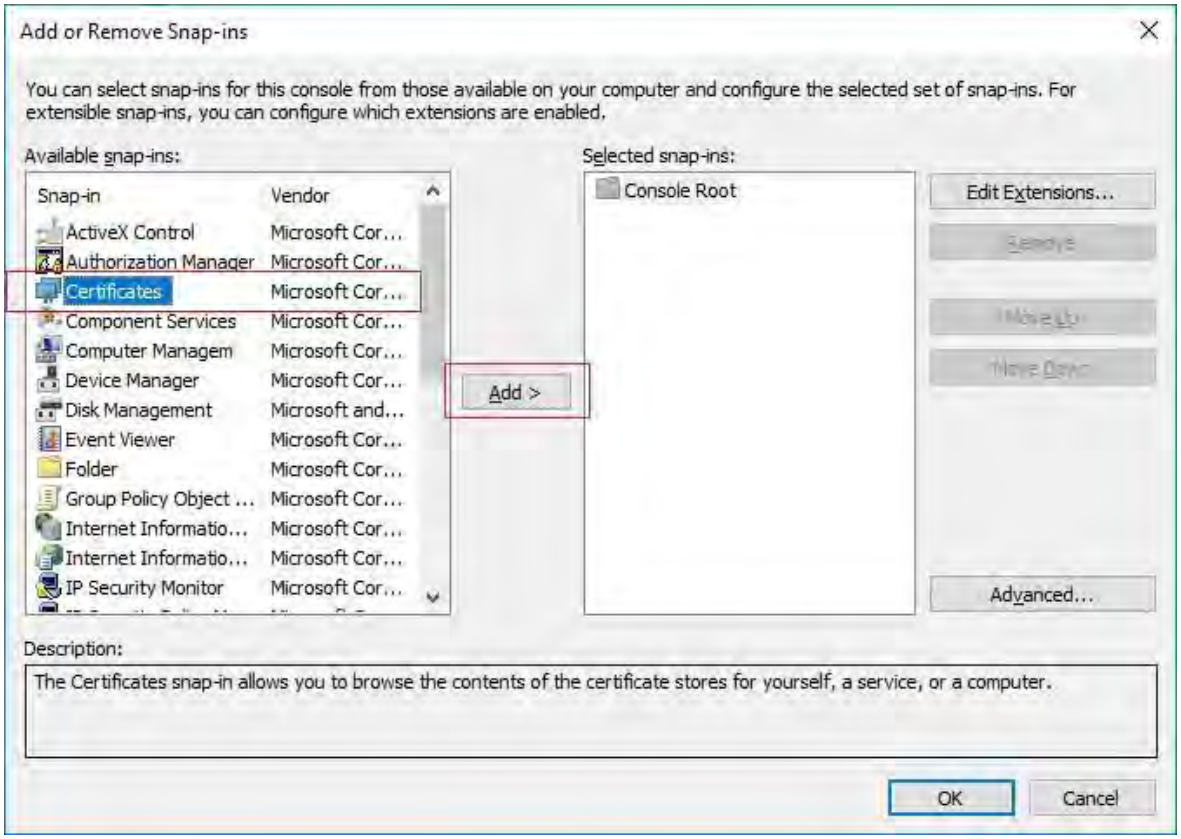
8. Pour vérifier que le certificat est importé, démarrez Microsoft Management Console.



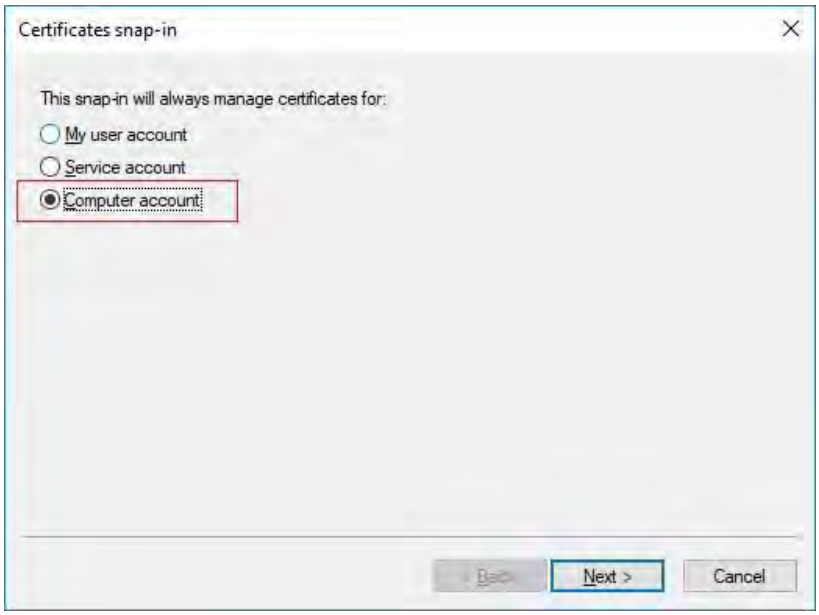
9. Dans Microsoft Management Console, dans le menu Fichier, sélectionnez **Ajouter/Supprimer un composant logiciel enfichable...**.



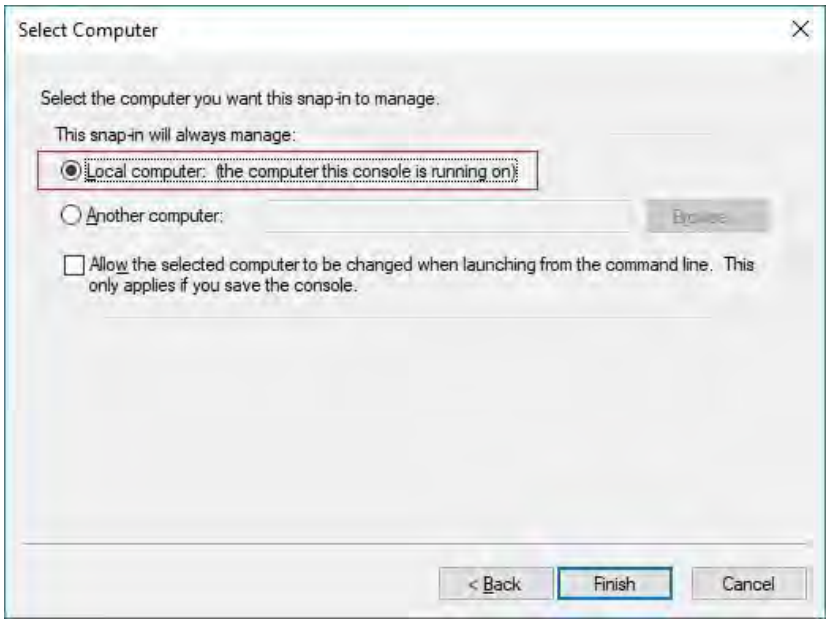
10. Sélectionnez le composant logiciel enfichable Certificats et cliquez sur **Ajouter**.



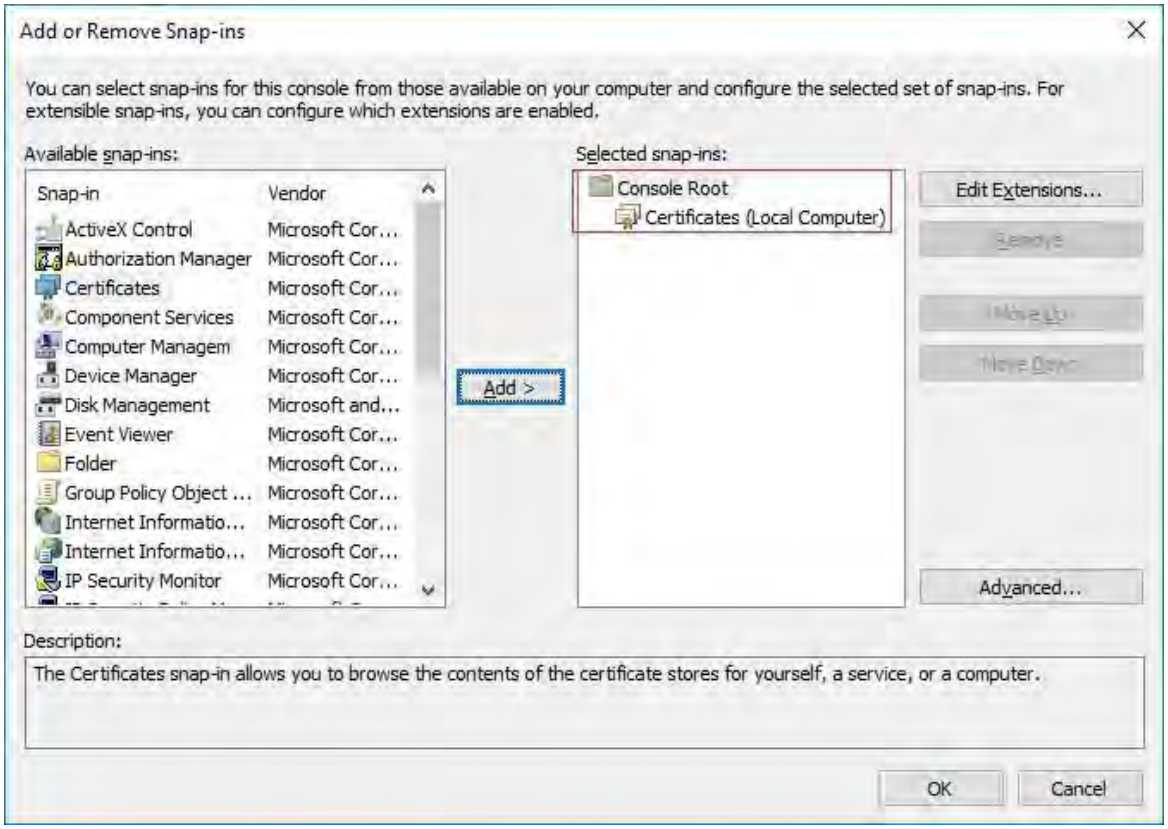
11. Sélectionnez que le composant logiciel enfichable doit gérer les certificats pour le **compte Ordinateur**.



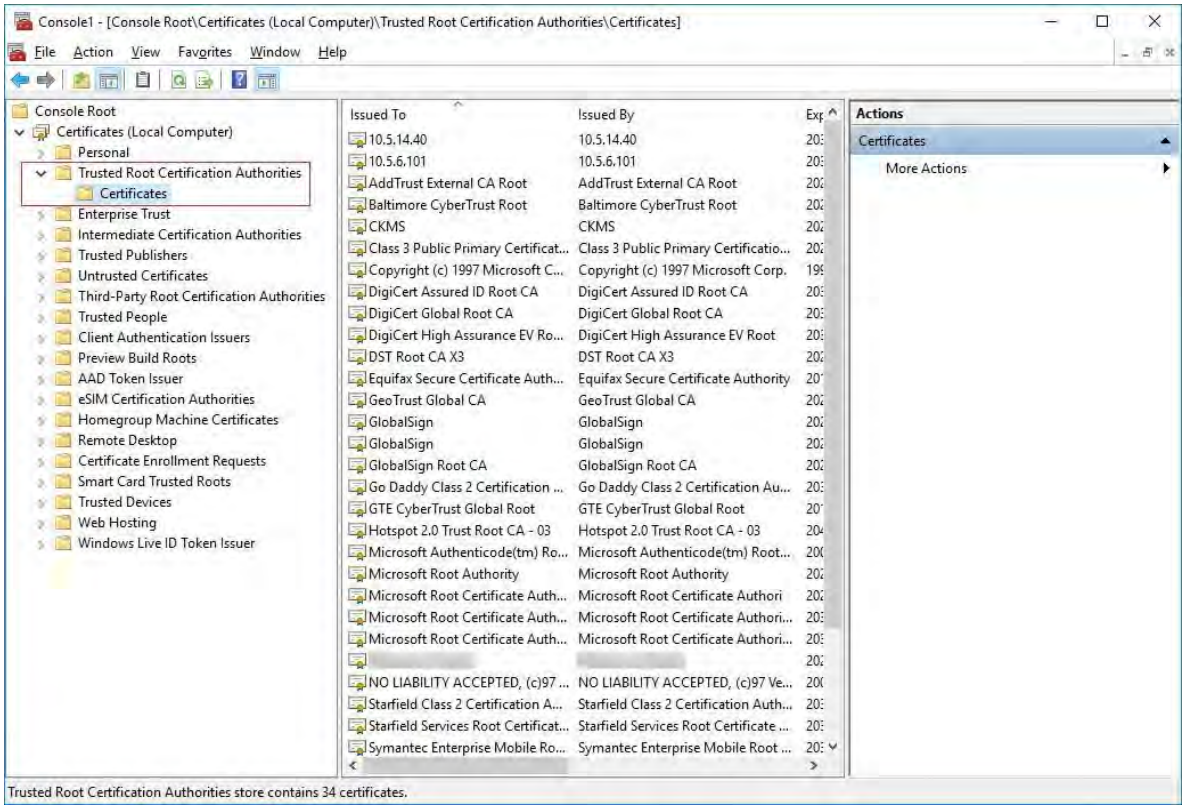
12. Sélectionnez **Ordinateur local** comme ordinateur que vous souhaitez que le composant logiciel enfichable gère et cliquez sur **Terminer**.



13. Cliquez sur **OK** une fois le composant logiciel enfichable ajouté.



14. Vérifiez que le certificat est répertorié dans la vue centrale des autorités de **certification racine approuvées** sous-arbre.



15. Répétez les étapes sur l'ordinateur suivant qui s'exécute en tant que client du service où le chiffrement est activé, jusqu'à ce que vous ayez installé le certificat sur tous les ordinateurs appropriés.

Créer un certificat SSL

Une fois que vous avez installé le certificat d'autorité de certification sur tous les clients, vous êtes prêt à créer des certificats à installer sur tous les ordinateurs qui exécutent des serveurs (serveurs d'enregistrement, serveurs de gestion, serveurs mobiles ou serveurs de basculement).

Si vous souhaitez configurer un serveur de gestion de basculement, vous devez créer un autre certificat SSL. Pour plus d'informations, reportez-vous à la section Création d'un certificat SSL pour le serveur de gestion du basculement à la page 38.

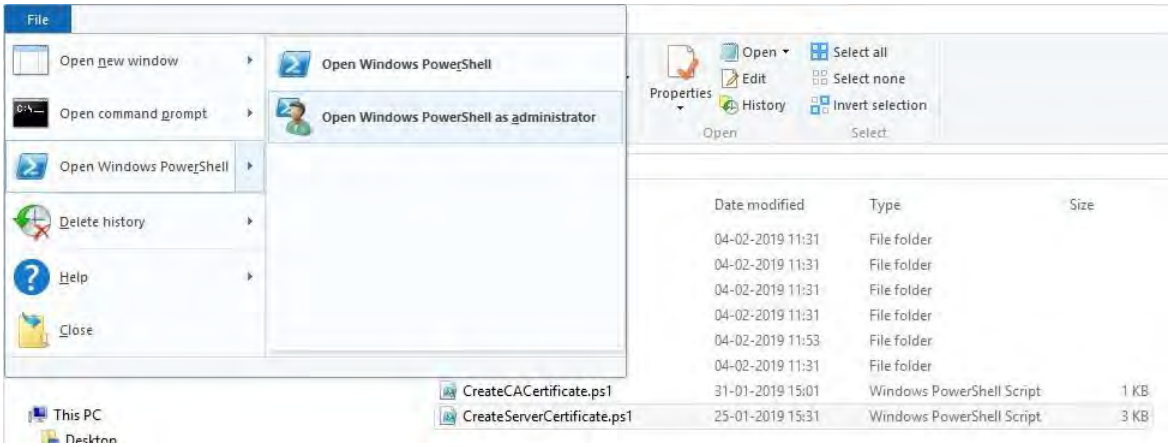
Sur l'ordinateur sur lequel vous avez créé le certificat d'autorité de certification, à partir du dossier dans lequel vous l'avez placé, exécutez le script de **certificat de serveur** pour créer des certificats SSL pour tous les serveurs.

L'ordinateur que vous utilisez pour créer des certificats doit exécuter Windows 10 ou Windows Server 2016 ou une version ultérieure.

1. L'annexe B à la fin de ce guide vous propose un script de création de certificats de serveur.
2. Ouvrez le Bloc-notes et collez le contenu.

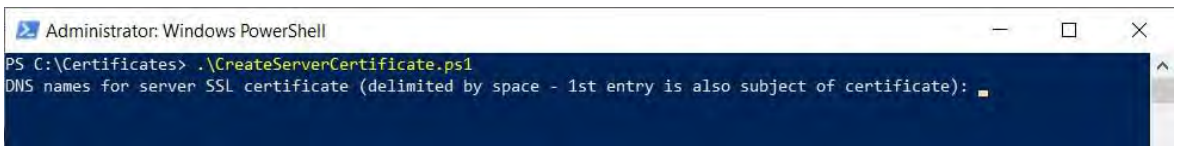
> ⚠ Il est très important que les lignes se brisent aux mêmes endroits qu'à l'annexe B. Vous pouvez ajouter les sauts de ligne dans le Bloc-notes ou réouvrir ce PDF avec Google Chrome, copier à nouveau le contenu et le coller dans le Bloc-notes.

3. Dans le Bloc-notes, cliquez sur **Fichier** -> **Enregistrer sous**, nommez le fichier **CreateServerCertificate.ps1** et enregistrez-le localement dans le même dossier que le certificat de l'autorité de certification, comme suit :
   C :\Certificates\CreateServerCertificate.ps1.
4. Dans l'Explorateur de fichiers, accédez à C :\Certificates et sélectionnez le **fichier CreateServerCertificate.ps1**.
5. Dans le menu **Fichier**, sélectionnez **Ouvrir Windows PowerShell**, puis **Ouvrir Windows PowerShell en tant qu'administrateur**.



6. Dans PowerShell, à l'invite, entrez **.\CreateServerCertificate.ps1** et appuyez sur **Entrée**.
7. Entrez le nom DNS du serveur. Si le serveur a plusieurs noms, par exemple pour une utilisation interne et externe, ajoutez-les ici, séparés par un espace. Appuyez sur **Entrée**.

> ✓ Pour trouver le nom DNS, ouvrez l'Explorateur de fichiers sur l'ordinateur exécutant le service Serveur d'enregistrement. Cliquez avec le bouton droit de la souris sur **Ce PC** et sélectionnez **Propriétés**. Utilisez le nom complet de l'**ordinateur**.



8. Entrez l'adresse IP du serveur. Si le serveur dispose de plusieurs adresses IP, par exemple pour une utilisation interne et externe, ajoutez-les ici, séparées par un espace. Appuyez sur **Entrée**.

   Pour trouver l'adresse IP, vous pouvez ouvrir l'invite de commande sur l'ordinateur exécutant le service Serveur d'enregistrement. Entrez **ipconfig /all**. Si vous avez installé le système MOBOTIX HUB, vous pouvez ouvrir le client de gestion, accéder au serveur et trouver l'adresse IP dans l' **onglet Infos**.

9. Spécifiez un mot de passe pour le certificat et appuyez sur **Entrée** pour terminer la création.

   Vous utilisez ce mot de passe lorsque vous importez le certificat sur le serveur.

   Un fichier Subjectname.pfx apparaît dans le dossier dans lequel vous avez exécuté le script.

10. Exécutez le script jusqu'à ce que vous ayez des certificats pour tous vos serveurs.

Importer un certificat SSL

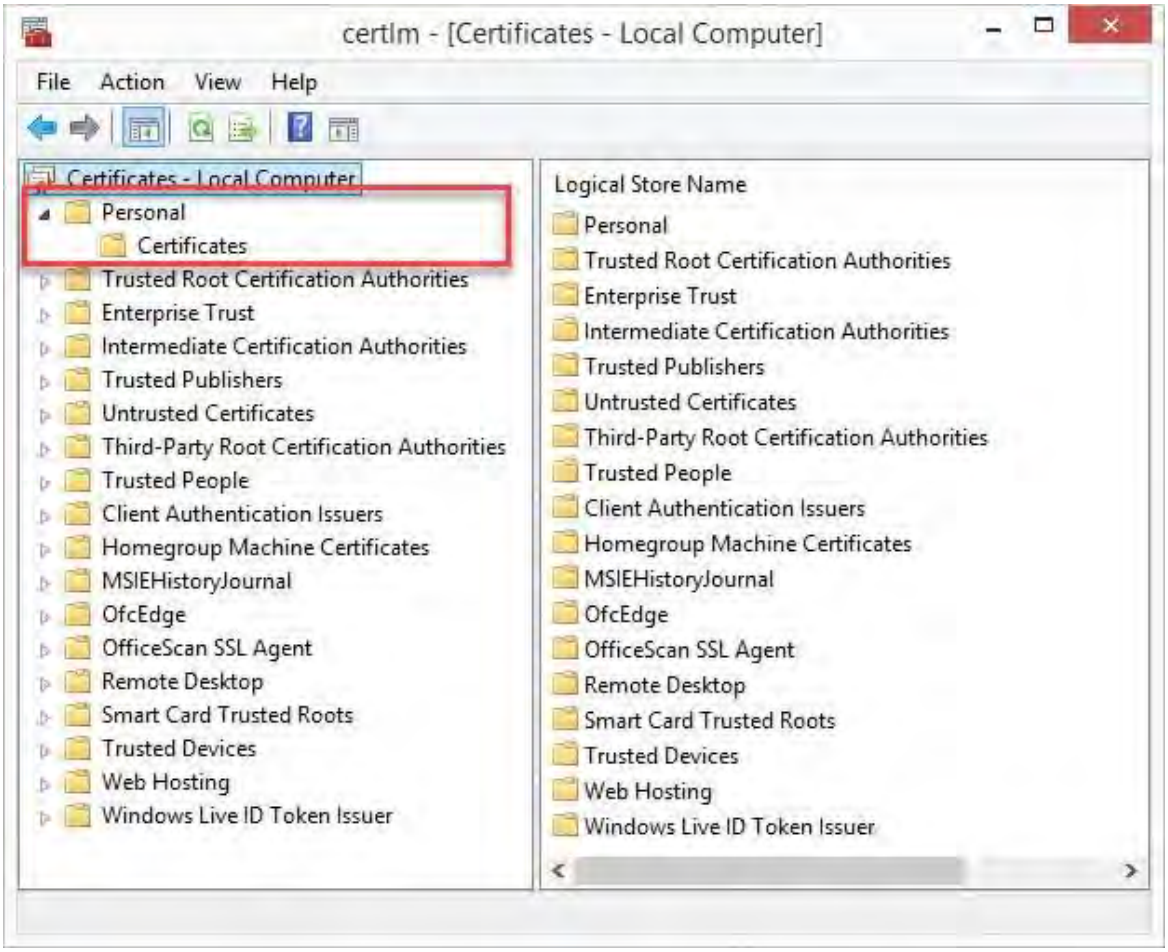
Après avoir créé les certificats SSL, installez-les sur les ordinateurs qui exécutent le service serveur.

1. Copiez le fichier Subjectname.pfx approprié à partir de l'ordinateur sur lequel vous avez créé le certificat sur l'ordinateur de service serveur correspondant.

   N'oubliez pas que chaque certificat est créé sur un serveur spécifique.

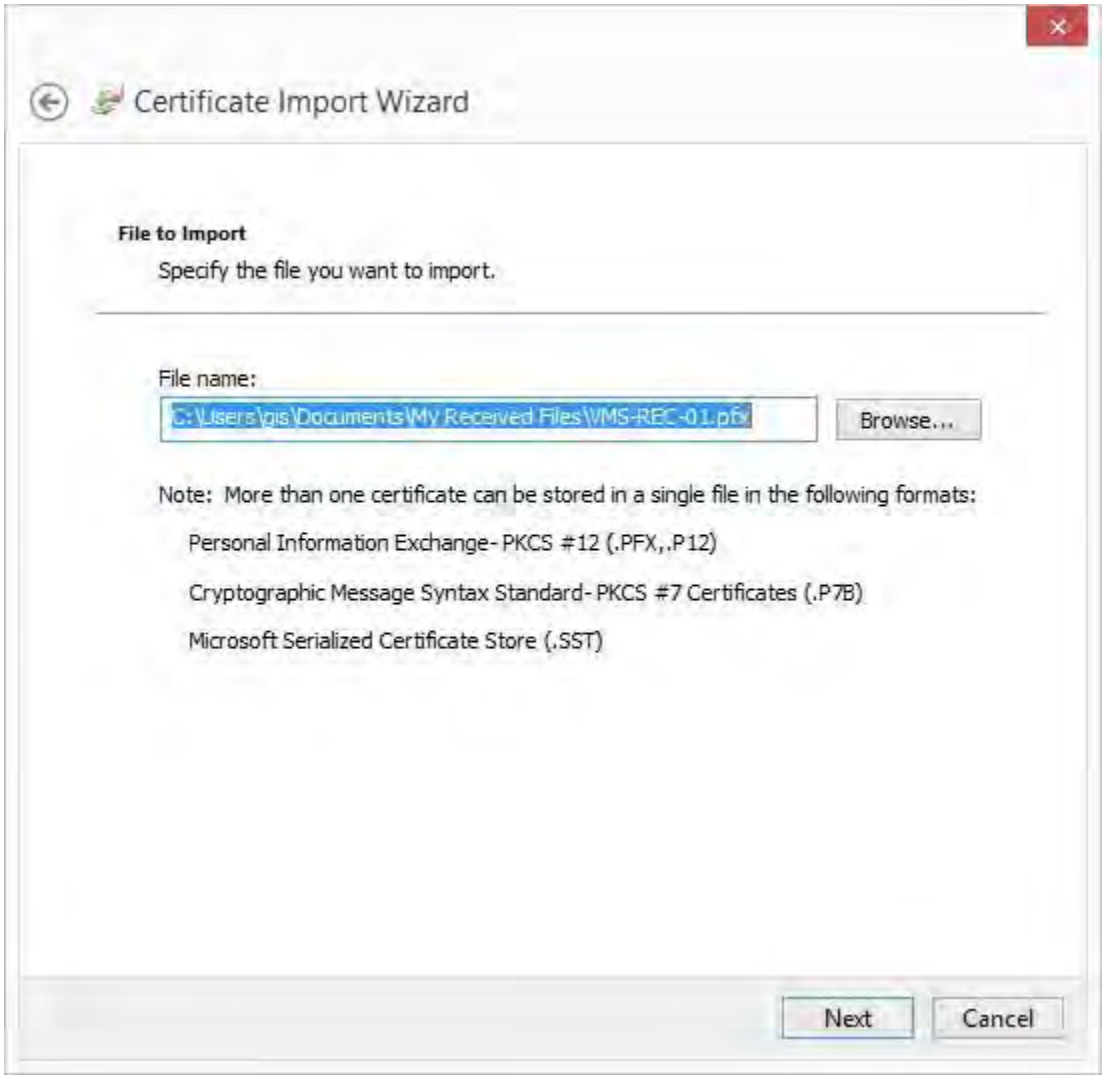
2. Sur l'ordinateur de service serveur, démarrez **Gérer les certificats de l'ordinateur**.

3. Cliquez sur **Personnel**, cliquez avec le bouton droit de la souris sur **Certificats** et sélectionnez **Toutes les tâches** > **importer**.

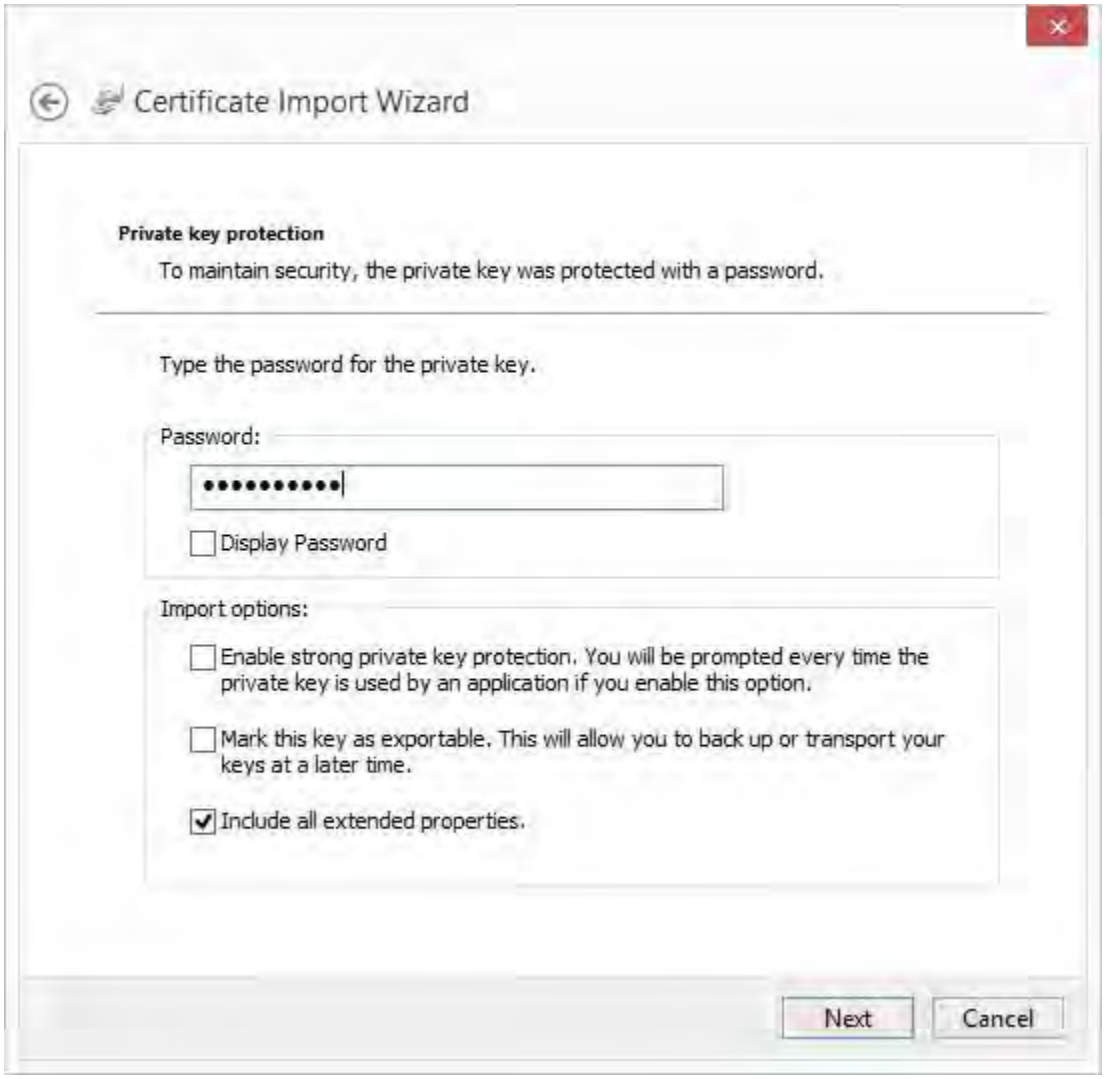


4. Sélectionnez cette option pour importer le certificat dans le magasin de la **machine locale** et cliquez sur **Suivant**.

5. Accédez au fichier de certificat et cliquez sur **Suivant**.



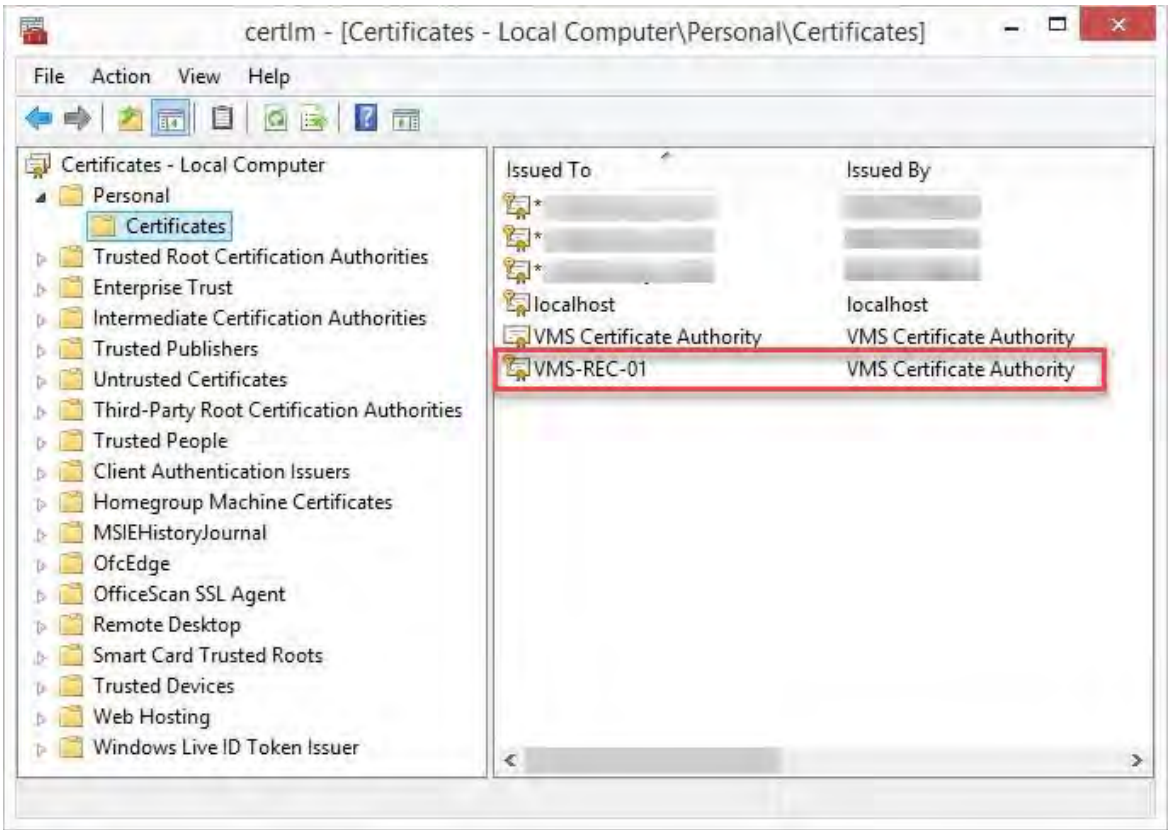
6. Entrez le mot de passe de la clé privée que vous avez spécifiée lors de la création du certificat de serveur, puis cliquez sur **Suivant**.



7. Placez le fichier dans le **magasin de certificats** : **Personnel,** puis cliquez sur **Suivant**.

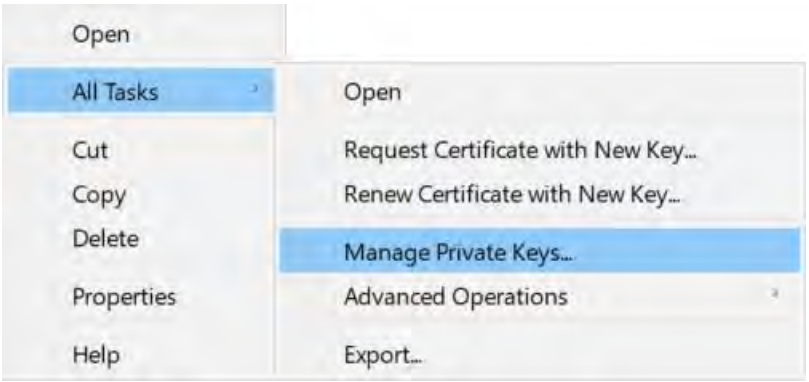
8. Vérifiez les informations et cliquez sur **Terminer** pour importer le certificat.

9. Le certificat importé apparaît dans la liste.

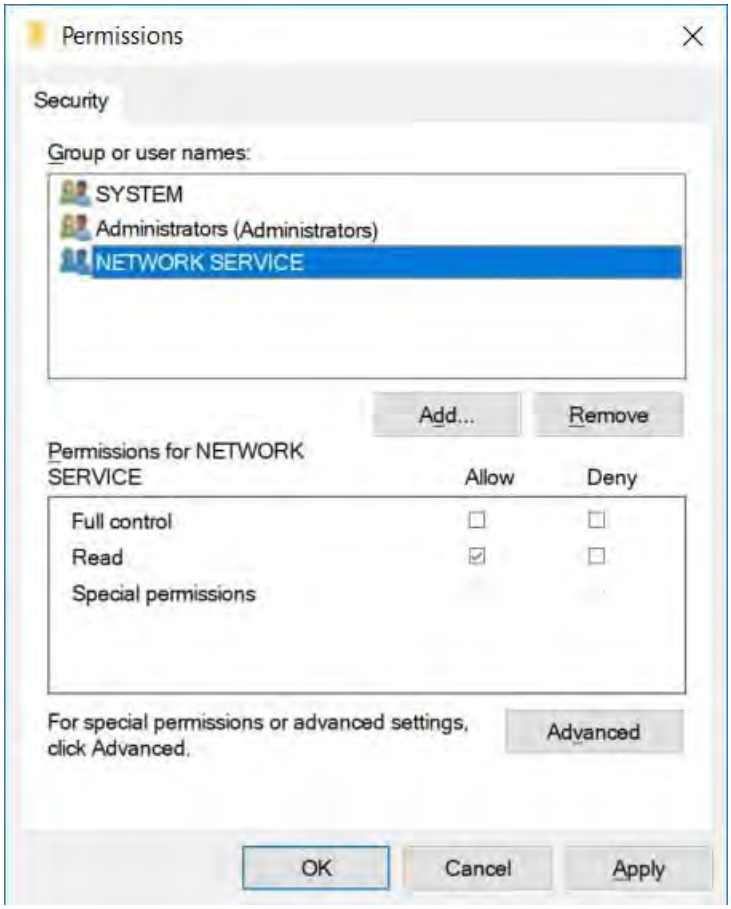


10. Pour autoriser un service à utiliser la clé privée du certificat, cliquez avec le bouton droit sur le certificat et sélectionnez **Toutes les tâches** >

    Gérer les clés privées.



11. Ajoutez l'autorisation de lecture pour l'utilisateur exécutant les services MOBOTIX HUB VMS qui doit utiliser le certificat de serveur .



12. Passez à l'ordinateur suivant jusqu'à ce que vous ayez installé tous les certificats de serveur.

Création d'un certificat SSL pour le serveur de gestion de basculement

Le basculement du serveur de gestion MOBOTIX HUB est configuré sur deux ordinateurs. Pour vous assurer que les clients font confiance au serveur de gestion en cours d'exécution, installez le certificat SSL sur l'ordinateur principal et l'ordinateur secondaire.

Pour créer et installer le certificat SSL pour le cluster de basculement, vous devez d'abord installer le certificat d'autorité de certification.

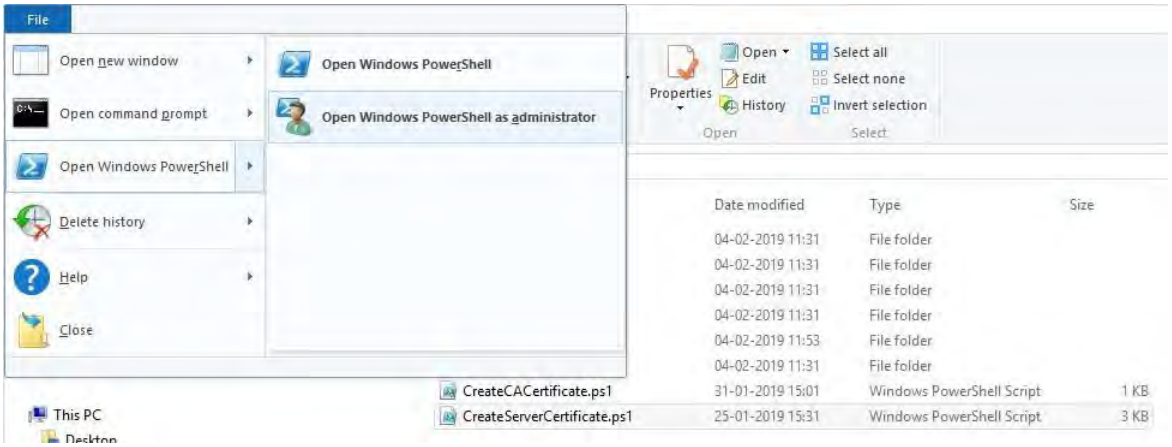
Sur l'ordinateur sur lequel vous avez créé le certificat d'autorité de certification, à partir du dossier dans lequel vous avez placé le certificat d'autorité de certification, exécutez le script de **certificat du serveur de gestion du basculement** afin de créer un certificat SSL pour l'ordinateur principal et l'ordinateur secondaire.

> ⚠ L'ordinateur que vous utilisez pour créer des certificats doit exécuter Windows 10 ou Windows Server 2016 ou une version ultérieure.

1. Dans l'annexe C de ce guide, copiez le script de création des certificats de serveur de gestion de basculement.
2. Ouvrez le Bloc-notes et collez le script.

   > ⚠ Il est très important que les lignes se brisent aux mêmes endroits que ceux indiqués en annexe C. Vous pouvez ajouter les sauts de ligne dans le Bloc-notes ou réouvrir ce PDF avec Google Chrome, copier à nouveau le contenu et le coller dans le Bloc-notes.

3. Dans le Bloc-notes, sélectionnez **Fichier** -> **Enregistrer sous**, nommez le fichier **CreateFailoverCertificate.ps1** et enregistrez-le localement dans le même dossier que le certificat de l'autorité de certification :
   Exemple : C :\Certificates\CreateFailoverCertificate.ps1.
4. Dans l'Explorateur de fichiers, accédez à C :\Certificates et sélectionnez le **fichier CreateFailoverCertificate.ps1**.
5. Dans le menu **Fichier**, sélectionnez **Ouvrir Windows Powershell**, puis **Ouvrir Windows PowerShell en tant qu'administrateur**.



6. Dans PowerShell, entrez **.\CreateFailoverCertificate.ps1** à l'invite et appuyez sur **Entrée**.

7. Spécifiez les noms de domaine complets et les noms d'hôte de l'ordinateur principal et de l'ordinateur secondaire, séparés par une virgule.

   Exemple : pc1host,pc1host.domain,pc2host,pc2host.domain.

   Appuyez sur **Entrée**.

8. Spécifiez l'adresse IP virtuelle du cluster de basculement. Appuyez sur **Entrée**.
9. Spécifiez un mot de passe pour le certificat et appuyez sur **Entrée** pour terminer la création.

   Vous utilisez ce mot de passe lorsque vous importez le certificat sur le serveur.

   Le fichier [virtualIP].pfx apparaît dans le dossier dans lequel vous avez exécuté le script.

Importez le certificat de la même manière que vous importeriez un certificat SSL, voir Importer un certificat SSL à la page 29. Importez le certificat sur les ordinateurs principal et secondaire.

Installer des certificats pour la communication avec le serveur mobile

Pour utiliser un protocole HTTPS afin d'établir une connexion sécurisée entre le serveur mobile et les clients et services, vous devez appliquer un certificat valide sur le serveur. Le certificat confirme que le titulaire du certificat est autorisé à établir des connexions sécurisées.

Dans les machines virtuelles Mobotix Hub, le chiffrement est activé ou désactivé par serveur mobile. Vous pouvez activer ou désactiver le chiffrement lors de l'installation du produit MOBOTIX HUB VMS ou à l'aide du configurateur de serveur. Lorsque vous activez le chiffrement sur un serveur mobile, vous utilisez ensuite une communication chiffrée avec tous les clients, services et intégrations qui récupèrent les flux de données.

Lorsque vous configurez le chiffrement pour un groupe de serveurs, il doit être activé à l'aide d'un certificat appartenant au même certificat d'autorité de certification ou, si le chiffrement est désactivé, il doit être désactivé sur tous les ordinateurs du groupe de serveurs.

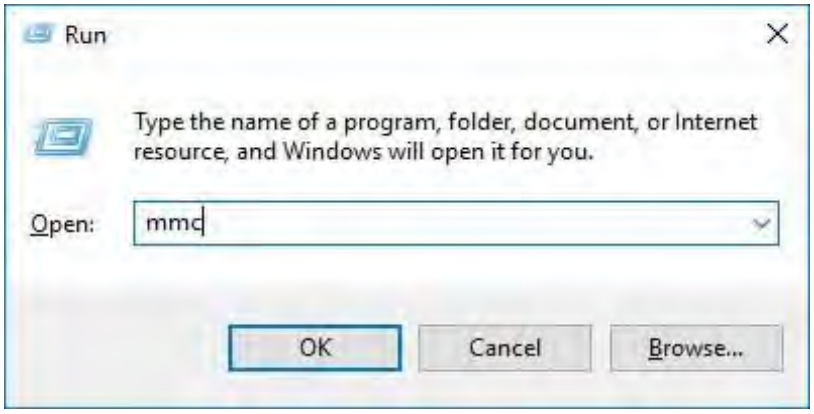
Les certificats émis par l'autorité de certification (CA) ont une chaîne de certificats et à la racine de cette chaîne se trouve le certificat racine de l'autorité de certification. Lorsqu'un appareil ou un navigateur voit ce certificat, il compare son certificat racine avec ceux préinstallés sur le système d'exploitation (Android, iOS, Windows, etc.). Si le certificat racine est répertorié dans la liste des certificats préinstallés, le système d'exploitation garantit à l'utilisateur que la connexion au serveur est suffisamment sécurisée. Ces certificats sont délivrés pour un nom de domaine et ne sont pas

Ajouter un certificat d'autorité de certification au serveur

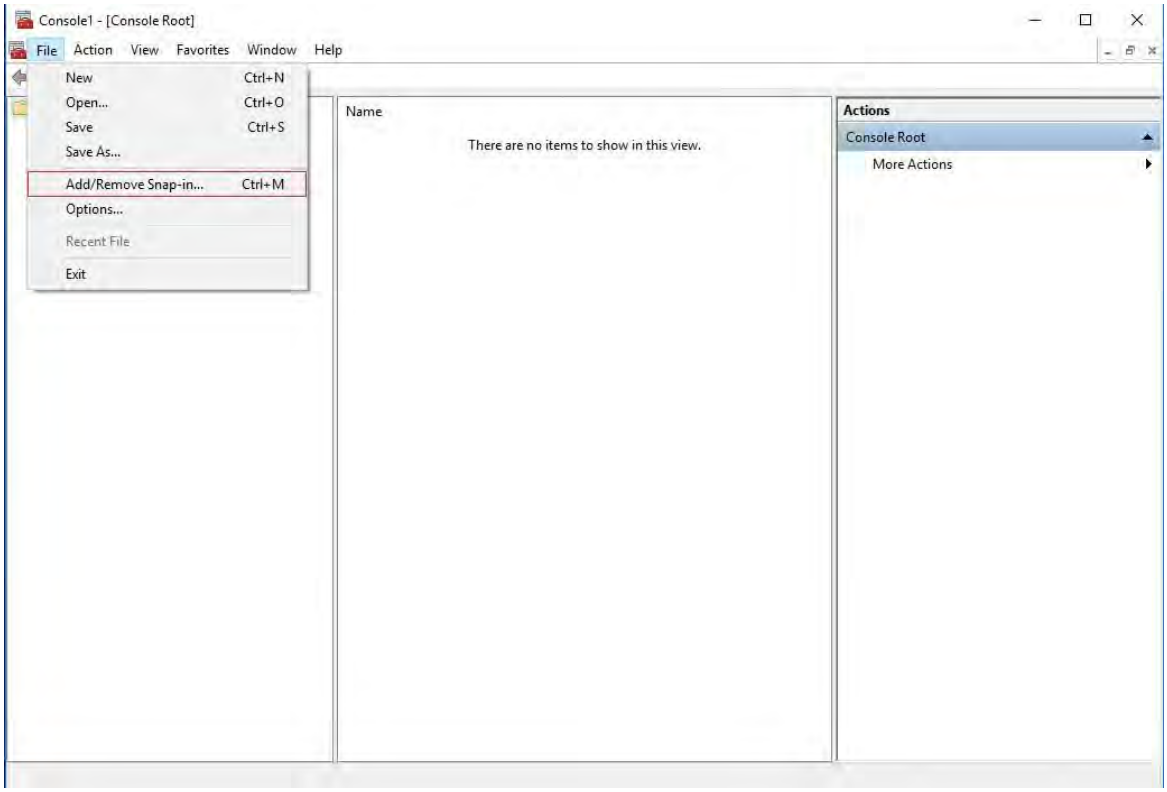
Ajoutez le certificat d'autorité de certification au serveur mobile en procédant comme suit.

Des paramètres spécifiques dépendent de l'autorité de certification. Reportez-vous à la documentation de votre autorité de certification avant de continuer.

1. Sur l'ordinateur qui héberge le serveur mobile, ouvrez la console de gestion Microsoft.

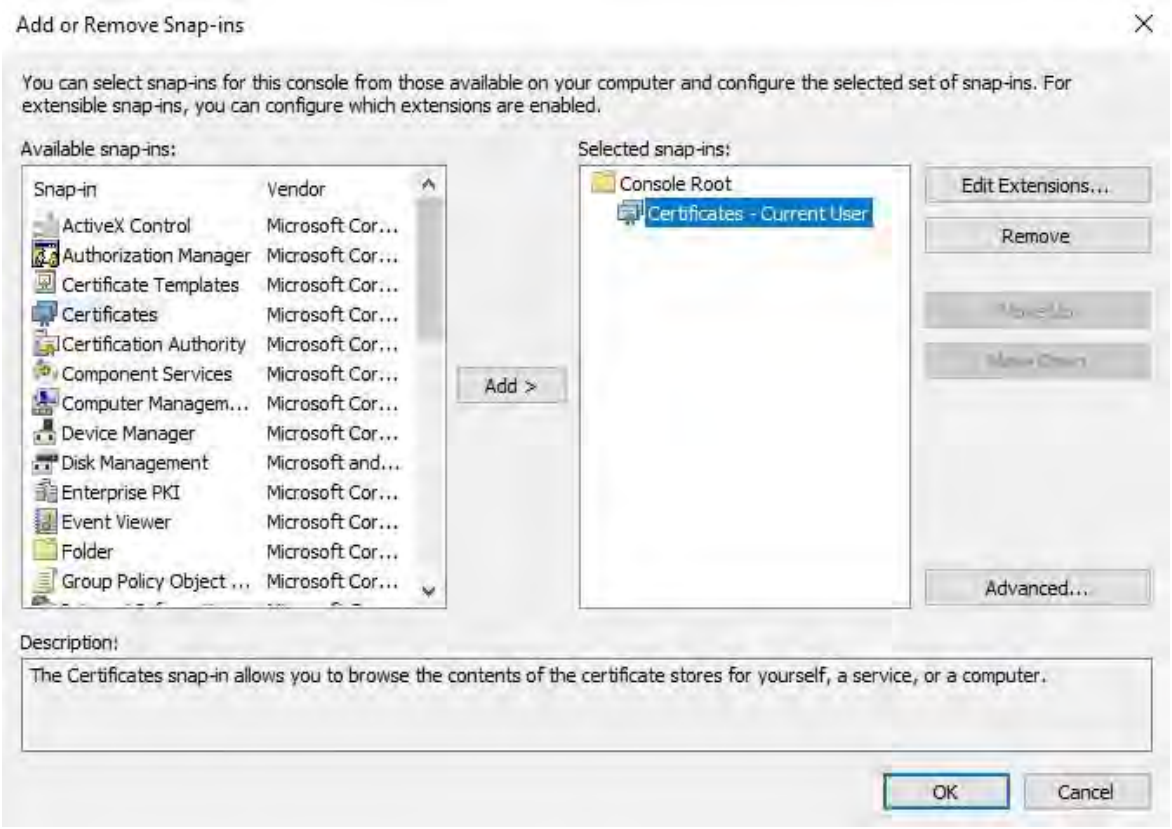


2. Dans Microsoft Management Console, dans le menu Fichier, sélectionnez **Ajouter/Supprimer un composant logiciel enfichable...**.

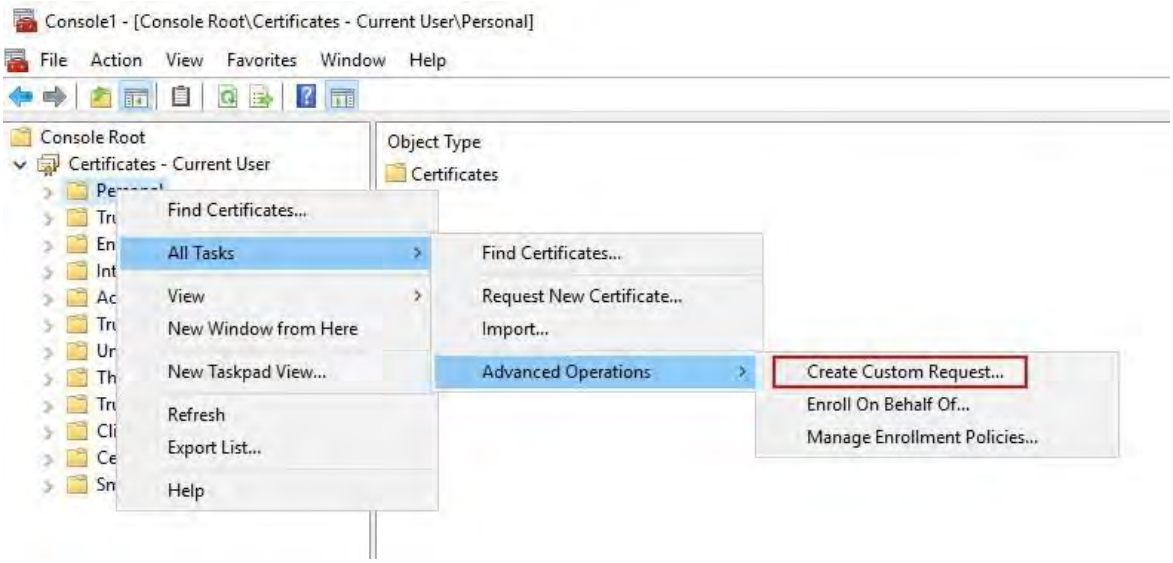


3. Sélectionnez le composant logiciel enfichable Certificats et cliquez sur **Ajouter**.

   Cliquez sur **OK**.

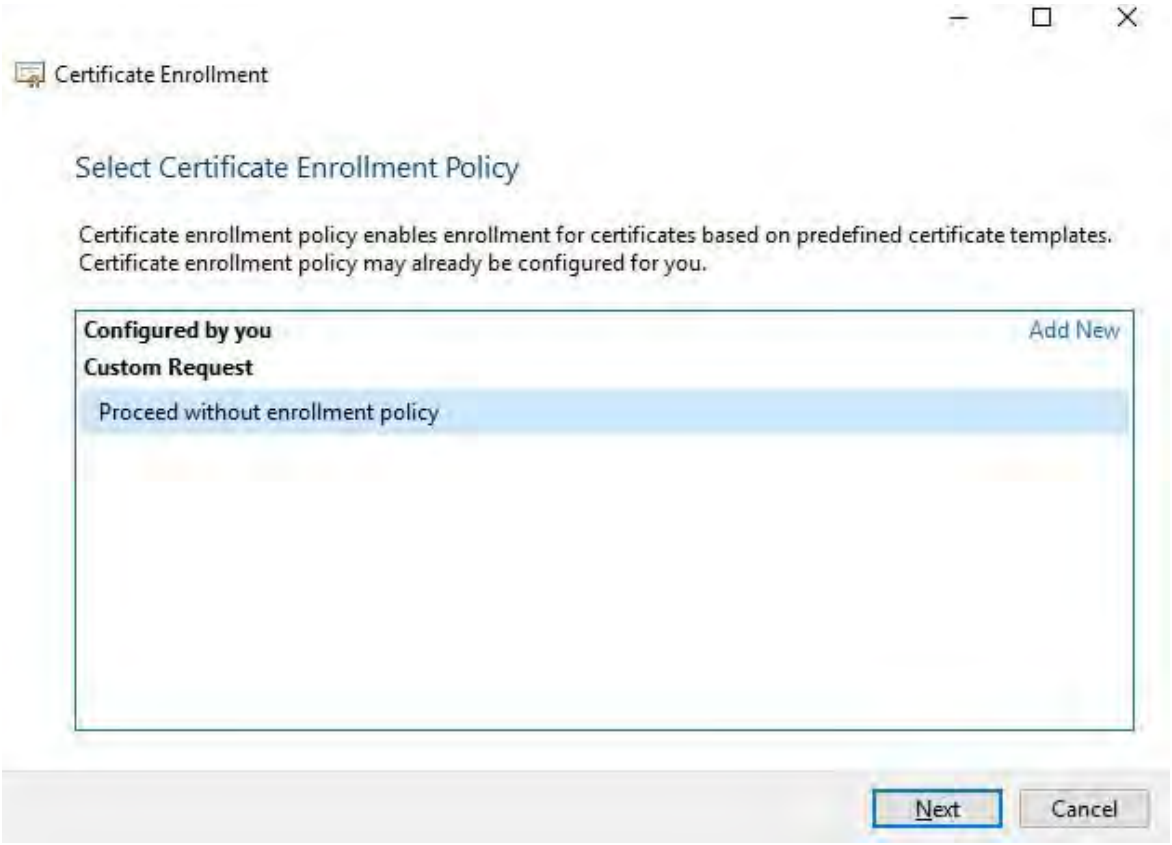


4. Développez l'objet Certificates. Cliquez avec le bouton droit de la souris sur le **dossier Personnel** et sélectionnez **Toutes les tâches** > **Opérations avancées** > **Créer une demande personnalisée**.

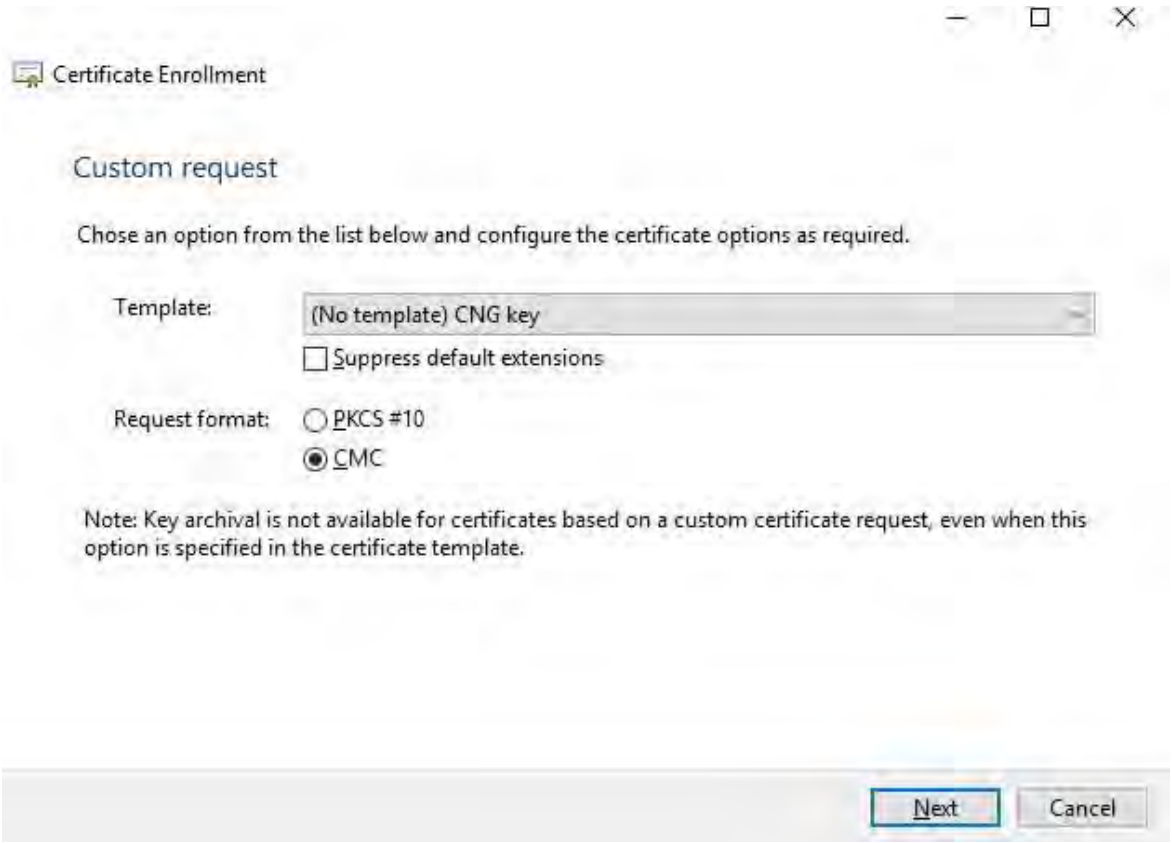


5. Cliquez sur **Suivant** dans l' Assistant **Inscription de certificat** et sélectionnez **Continuer sans stratégie d'inscription**.

   Cliquez sur **Suivant**.



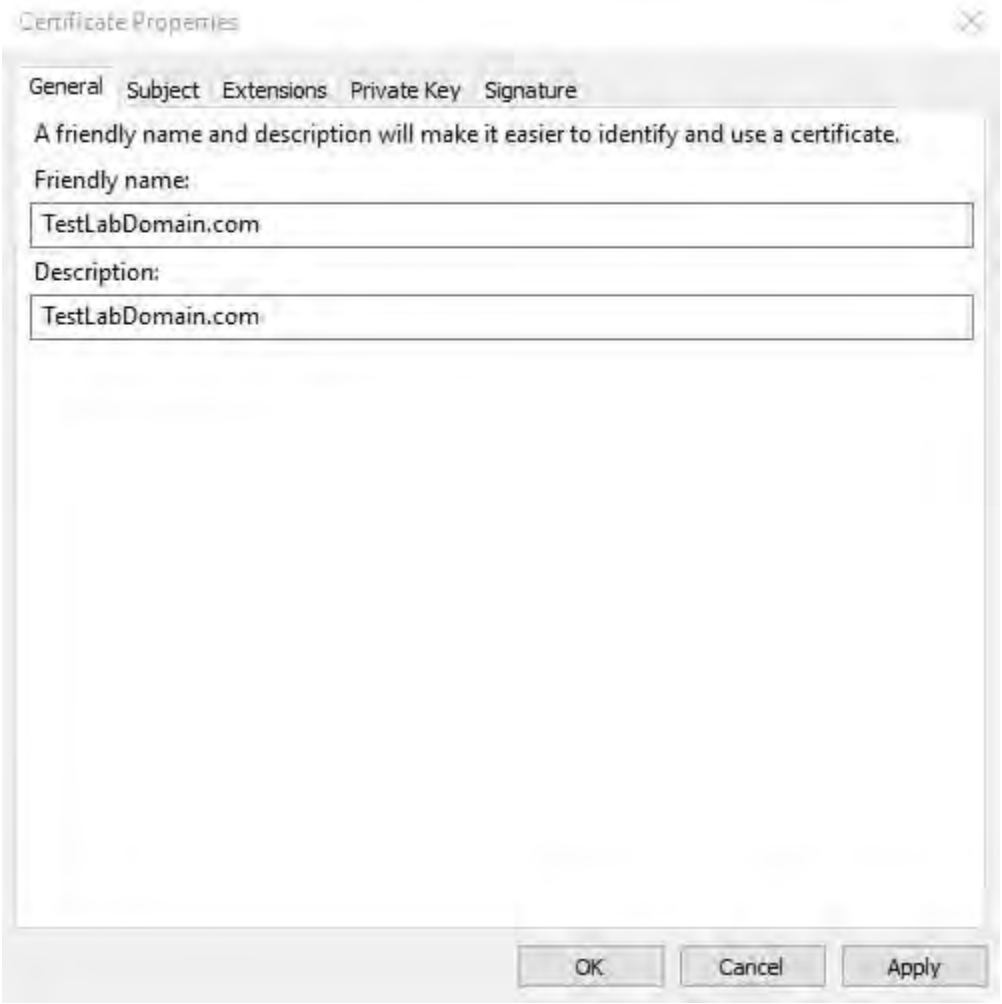
6. Sélectionnez le **modèle de clé CNG (sans modèle)** et le format de demande **CMC**, puis cliquez sur **Suivant**.



Le format de la demande dépend de l'autorité de certification. Si le format choisi est incorrect, l'autorité de certification émettra une erreur lors de l'envoi de la demande de signature de certificat (CSR). Vérifiez auprès de l'autorité de certification pour vous assurer que vous faites le bon choix.

7. Développez le champ d'affichage des **détails** de la demande personnalisée, puis cliquez sur **Propriétés**.

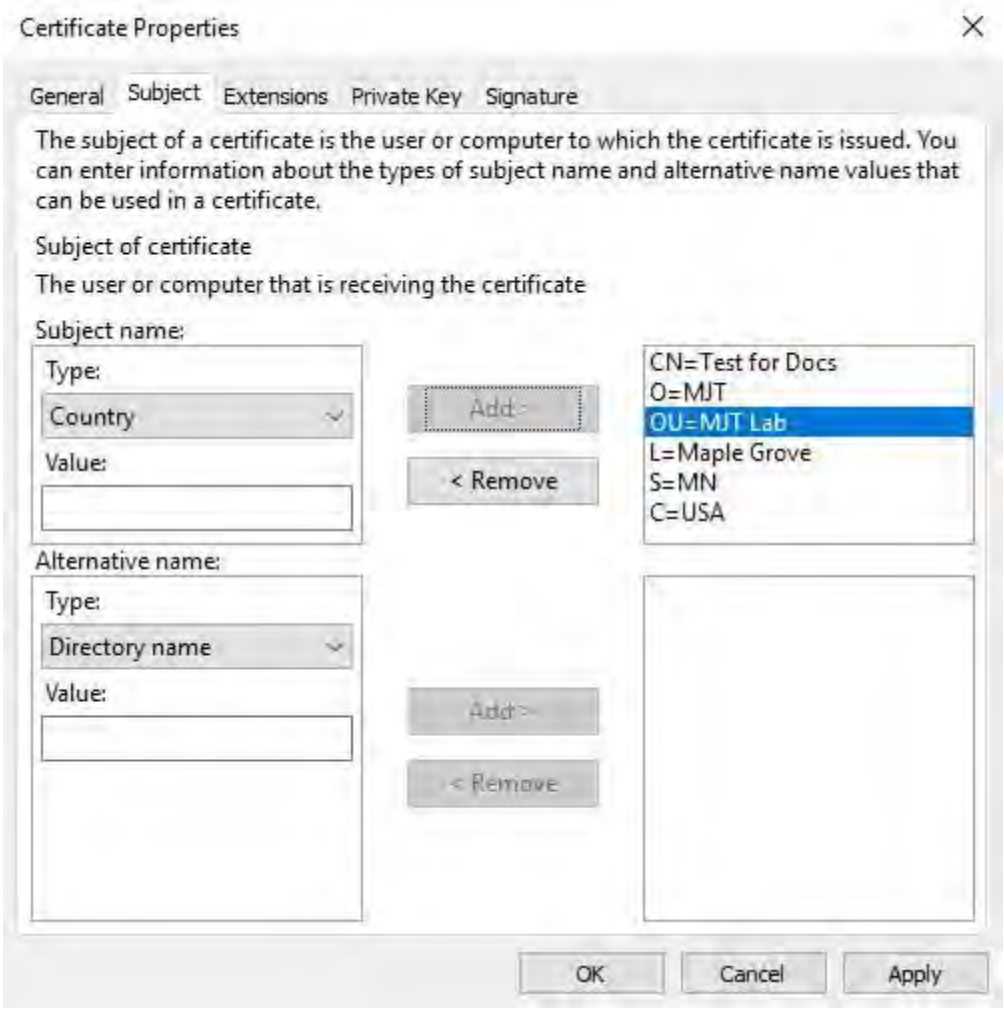
8. Dans l' **onglet Général**, remplissez les champs **Nom convivial** et **Description** avec le nom de domaine enregistré auprès de l'autorité de certification.



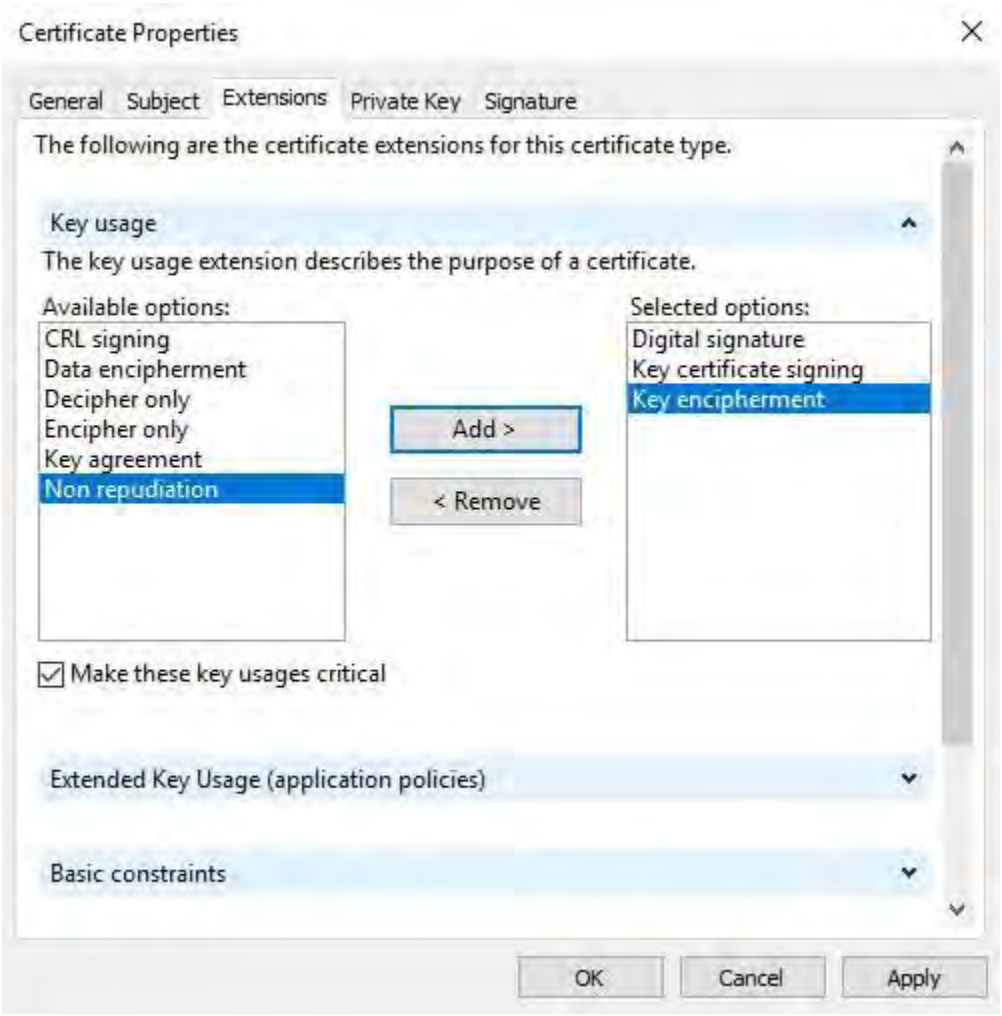
9. Dans l' **onglet Objet**, entrez les paramètres requis par l'autorité de certification spécifique.

   Par exemple, le nom de l'objet **Type** et **Valeur** sont différents pour chaque autorité de certification. Par exemple, les informations requises suivantes :

   - Nom commun:
   - Organisation:
   - Unité organisationnelle :
   - Ville/Localité :
   - État/Province :
   - Pays/Région :



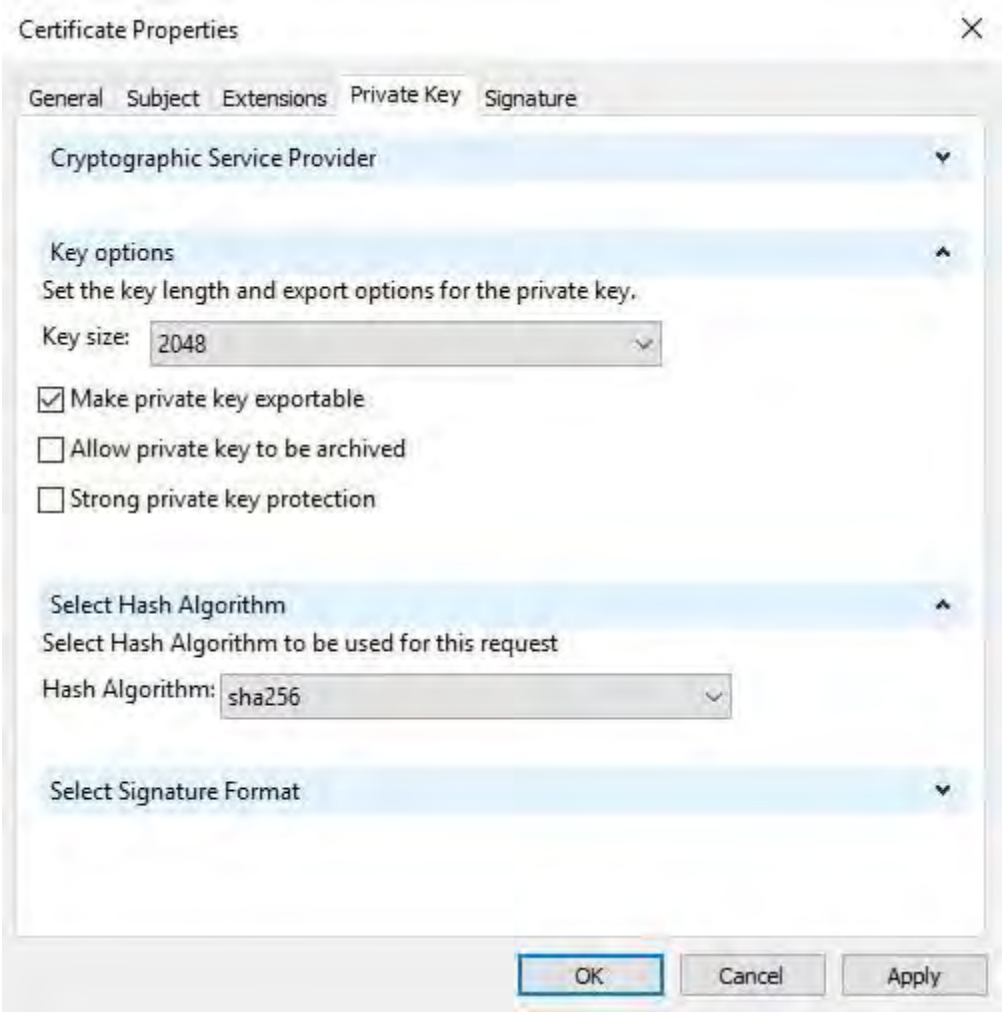
10. Certaines autorités de certification n'ont pas besoin d'extensions. Toutefois, si nécessaire, accédez à l' **onglet Extensions** et développez le menu Utilisation des **clés** . Ajoutez les options requises de la liste des **options disponibles** à la liste **des options sélectionnées**.



11. Sous l' **onglet Clé privée**, développez le menu Options de clé .

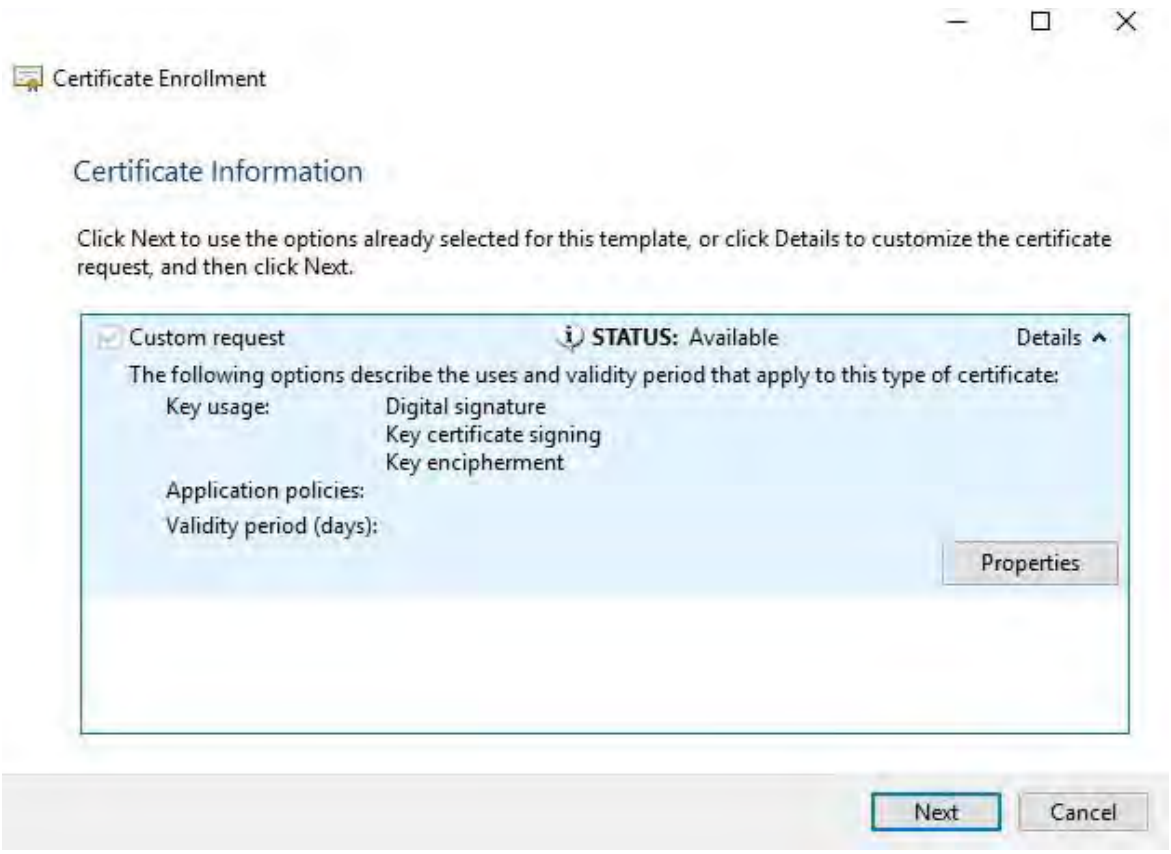
    Définissez la taille de la clé sur 2048 et sélectionnez l'option permettant d'exporter la clé privée.

    La variable de taille de clé est déterminée par l'autorité de certification, donc une clé de taille supérieure peut être requise. D'autres options, telles qu'un algorithme de hachage spécifique (sha256), peuvent également être requises. Ajustez toutes les options requises avant de passer à l'étape suivante.



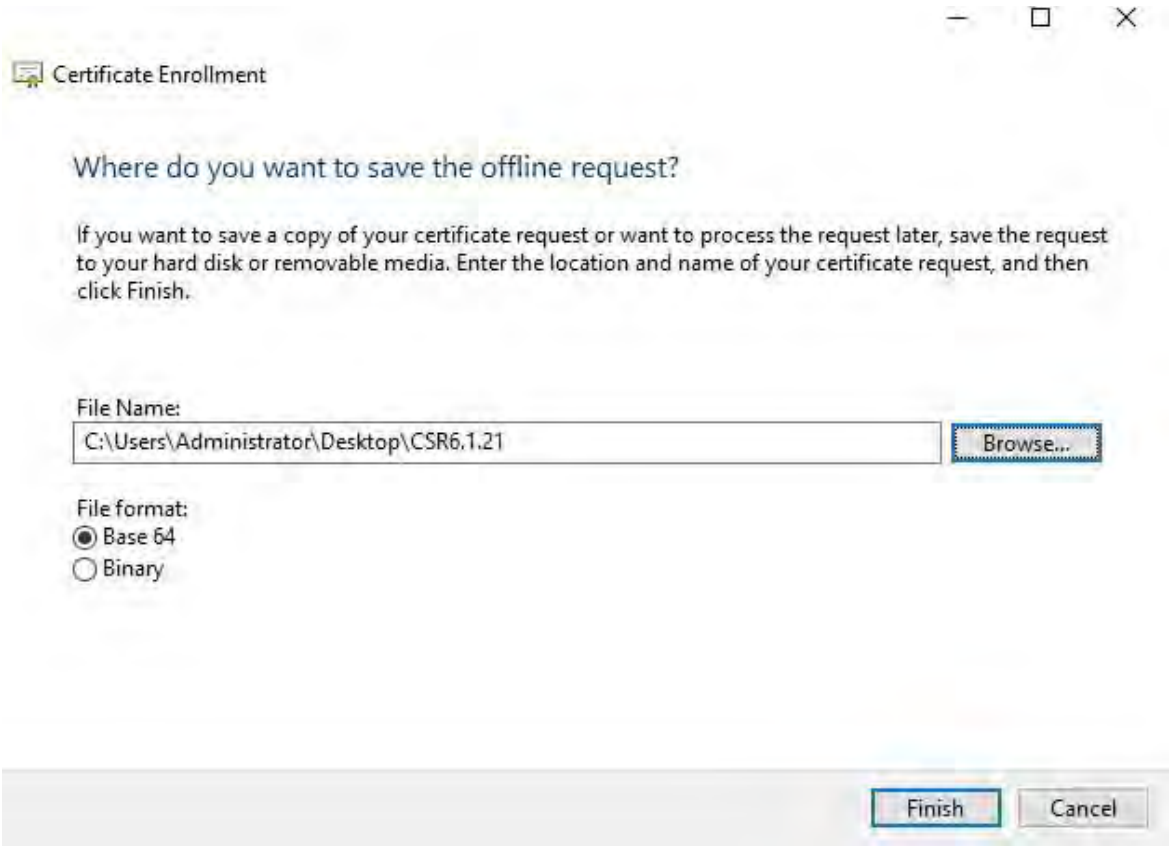
12. À moins que l'autorité de certification n'exige une signature, l'étape suivante consiste à cliquer sur **OK**.

13. Une fois que toutes les propriétés du certificat ont été définies, cliquez sur **Suivant** dans l' **onglet Inscription au certificat**
sorcier.



14. Sélectionnez un emplacement pour enregistrer la demande de certificat et un format. Naviguez jusqu'à cet emplacement et spécifiez un nom pour le fichier .req. Le format par défaut est la base 64, mais certaines autorités de certification exigent le format binaire.

15. Cliquez sur **Terminer**.



Un fichier .req est généré, que vous devez utiliser pour demander un certificat signé.

Téléchargez le fichier .req pour recevoir un certificat signé en retour

Chaque autorité de certification a un processus différent pour télécharger des fichiers .req afin de recevoir un certificat signé en retour. Reportez-vous à la documentation de votre autorité de certification pour plus d'informations sur la récupération d'un certificat signé.

Lorsque vous travaillez avec le serveur mobile, il est recommandé d'utiliser une autorité de certification tierce. Dans la plupart des situations d'autorité de certification tierce, il est nécessaire de télécharger un fichier .ZIP et d'extraire le contenu sur l'ordinateur qui héberge le serveur mobile.

Il existe plusieurs types de fichiers qui peuvent être inclus dans le contenu du fichier .ZIP extrait.

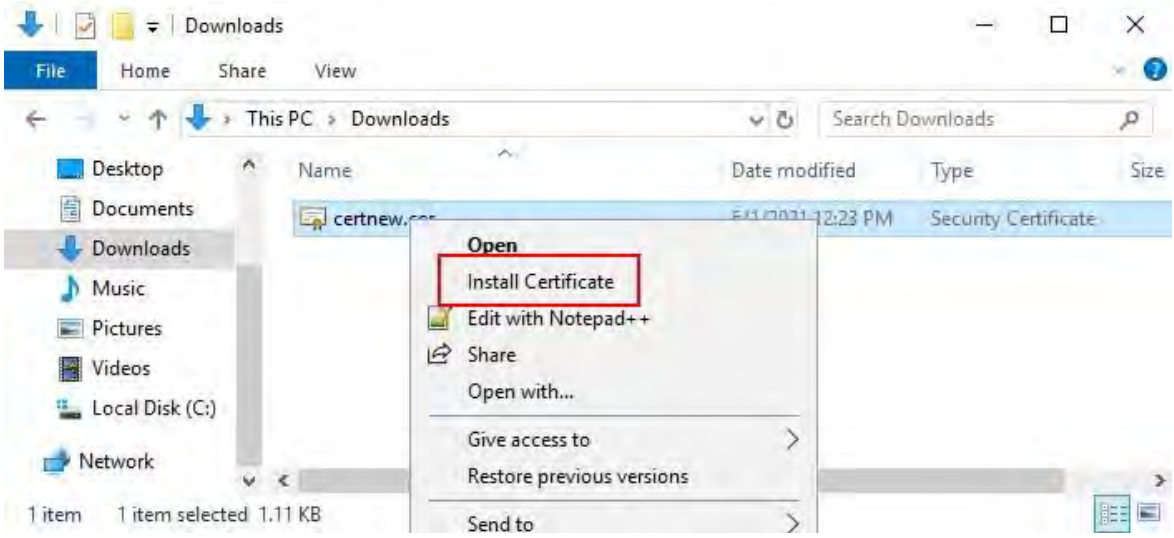
. CER ou . Les fichiers CRT peuvent être installés à l'aide d'un processus similaire. Cliquez avec le bouton droit de la souris sur le fichier et choisissez Installer le **certificat**
dans le menu contextuel.

Les étapes suivantes utilisent un fichier . Fichier CER d'une autorité de certification interne.

Votre autorité de certification aura besoin du contenu du fichier .req. On vous demandera de copier tout le texte du fichier .req, y compris les lignes de début et de fin, et de coller le texte dans un champ disponible sur un portail géré par l'autorité de certification.

1. Naviguez jusqu'à l'emplacement du fichier .req et ouvrez-le dans le Bloc-notes, puis collez le texte dans un champ mis à disposition sur un portail géré par votre autorité de certification.

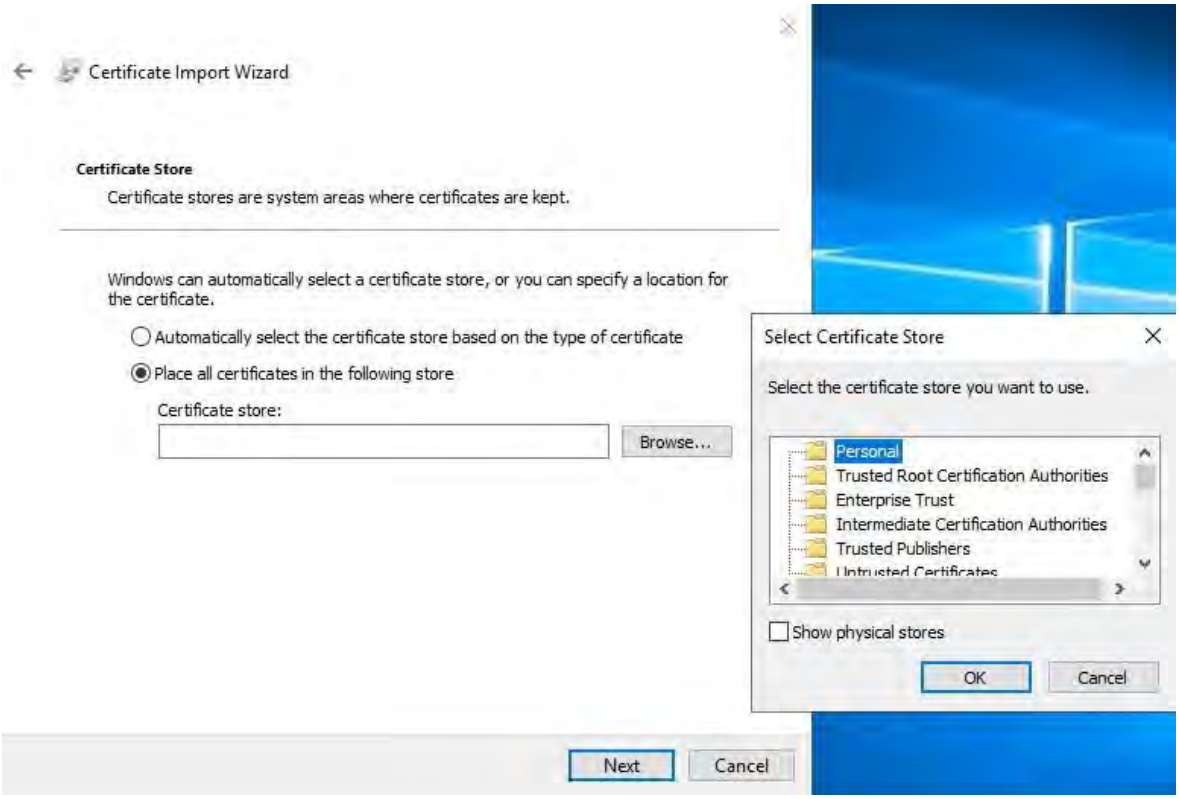
2. Lorsque vous recevez le certificat de votre autorité de certification, accédez au dossier des téléchargements (ou à l'endroit où vous choisissez de stocker le dossier sur l'ordinateur), cliquez avec le bouton droit sur le certificat et sélectionnez Installer le **certificat**.



3. Acceptez l'avertissement de sécurité s'il apparaît.

   Sélectionnez cette option pour installer le certificat pour l'ordinateur local et cliquez sur **Suivant**.

4. Choisissez un emplacement de stockage, accédez au magasin de certificats personnel, puis cliquez sur **Suivant**.



5. Terminez l' assistant **d'installation du certificat**.

Activer le chiffrement sur le serveur mobile

Une fois le certificat installé sur l'ordinateur qui héberge le serveur mobile, procédez comme suit.

1. Sur un ordinateur sur lequel un serveur mobile est installé, ouvrez le **configurateur de serveur** à partir de :

   - Le menu Démarrer de Windows

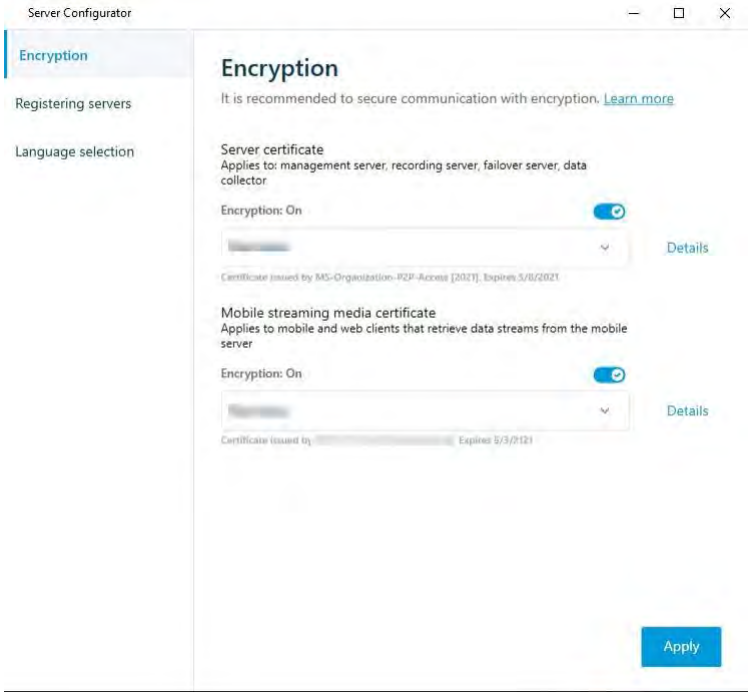
   ou

   - Le Gestionnaire de serveur mobile en cliquant avec le bouton droit de la souris sur l'icône Gestionnaire de serveur mobile dans la barre des tâches de l'ordinateur

2. Dans le **configurateur de serveur**, sous **Certificat de média de streaming mobile**, activez **le cryptage**.
3. Cliquez sur **Sélectionner un certificat** pour ouvrir une liste avec les noms d'objet uniques des certificats qui ont une clé privée et qui sont installés sur l'ordinateur local dans le magasin de certificats Windows.
4. Sélectionnez un certificat pour chiffrer la communication du client mobile MOBOTIX HUB et du client Web MOBOTIX HUB avec le serveur mobile.

   Sélectionnez **Détails** pour afficher les informations du Magasin de certificats Windows concernant le certificat sélectionné.

L'utilisateur du service Mobile Server a accès à la clé privée. Il est nécessaire que ce certificat soit approuvé sur tous les clients.



5. Cliquez sur **Appliquer**.

Lorsque vous appliquez des certificats, le service Mobile Server redémarre.

Pour plus d'informations, vous pouvez consulter :

Vidéo sur le processus Powershell.

Livre blanc sur les certificats avec le serveur mobile.

Installer des certificats d'autorité de certification tiers ou commerciaux pour la communication avec le serveur de gestion ou le serveur d'enregistrement

Les serveurs de gestion et les serveurs d'enregistrement n'exigent pas de certificats d'autorité de certification tiers ou commerciaux de confiance pour le chiffrement, mais vous pouvez choisir d'utiliser ces certificats si cela fait partie de votre politique de sécurité, et ils seront automatiquement approuvés par les postes de travail et les serveurs clients.

Le processus est identique à l'installation du certificat Mobile Server.

Lorsque vous configurez le chiffrement pour un groupe de serveurs, il doit être activé à l'aide d'un certificat appartenant au même certificat d'autorité de certification ou, si le chiffrement est désactivé, il doit être désactivé sur tous les ordinateurs du groupe de serveurs.

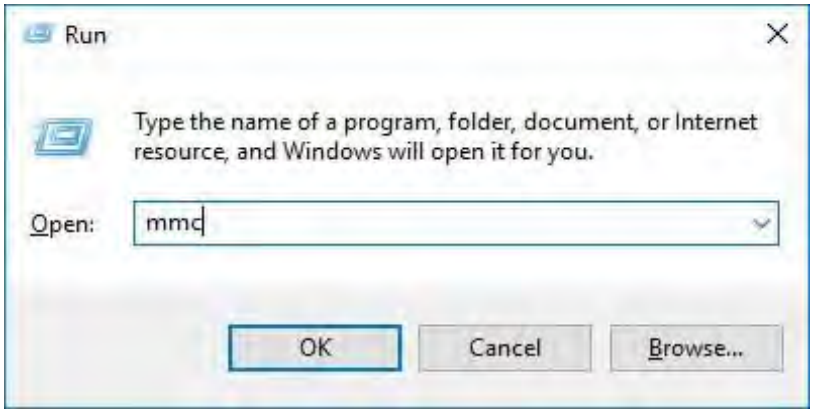
Les certificats émis par l'autorité de certification (CA) ont une chaîne de certificats et à la racine de cette chaîne se trouve le certificat racine de l'autorité de certification. Lorsqu'un appareil ou un navigateur voit ce certificat, il compare son certificat racine avec ceux préinstallés sur le système d'exploitation (Android, iOS, Windows, etc.). Si le certificat racine est répertorié dans la liste des certificats préinstallés, le système d'exploitation garantit à l'utilisateur que la connexion au serveur est suffisamment sécurisée. Ces certificats sont délivrés pour un nom de domaine et ne sont pas

Ajouter un certificat d'autorité de certification au serveur

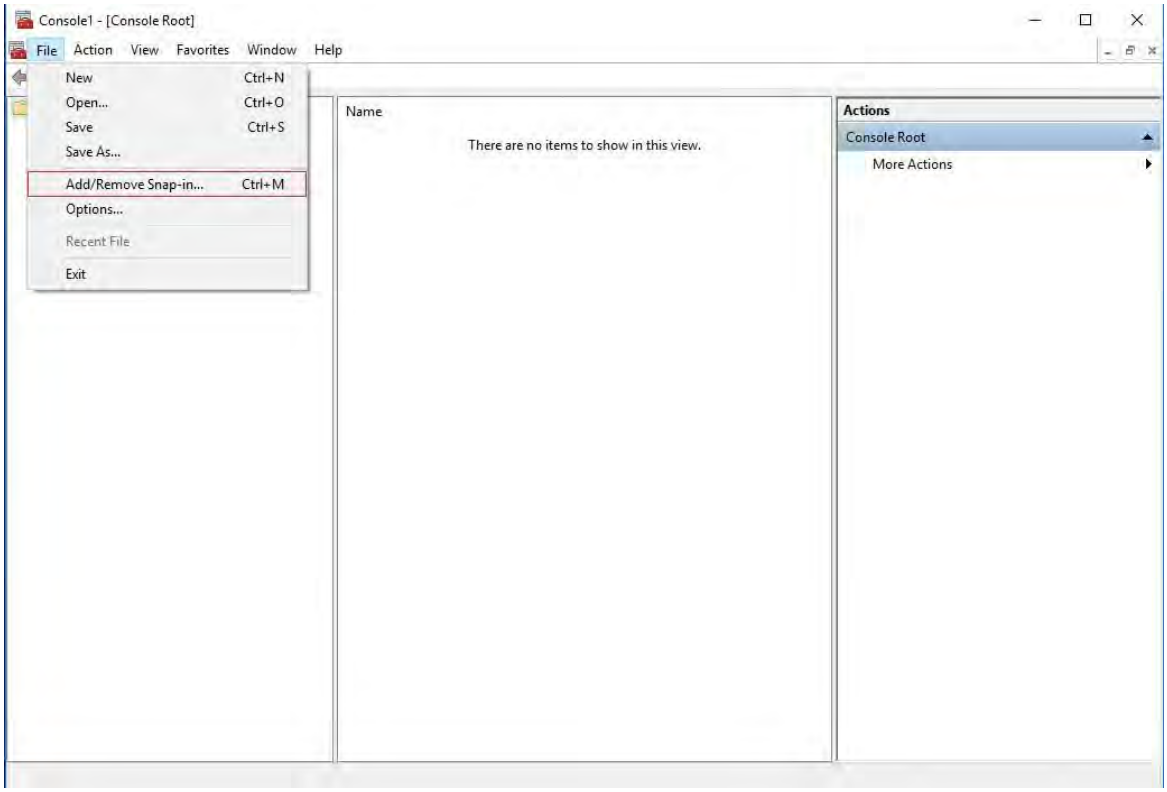
Ajoutez le certificat de l'autorité de certification au serveur en procédant comme suit.

Des paramètres spécifiques dépendent de l'autorité de certification. Reportez-vous à la documentation de votre autorité de certification avant de continuer.

1. Sur l'ordinateur qui héberge le serveur MOBOTIX HUB, ouvrez la console de gestion Microsoft.

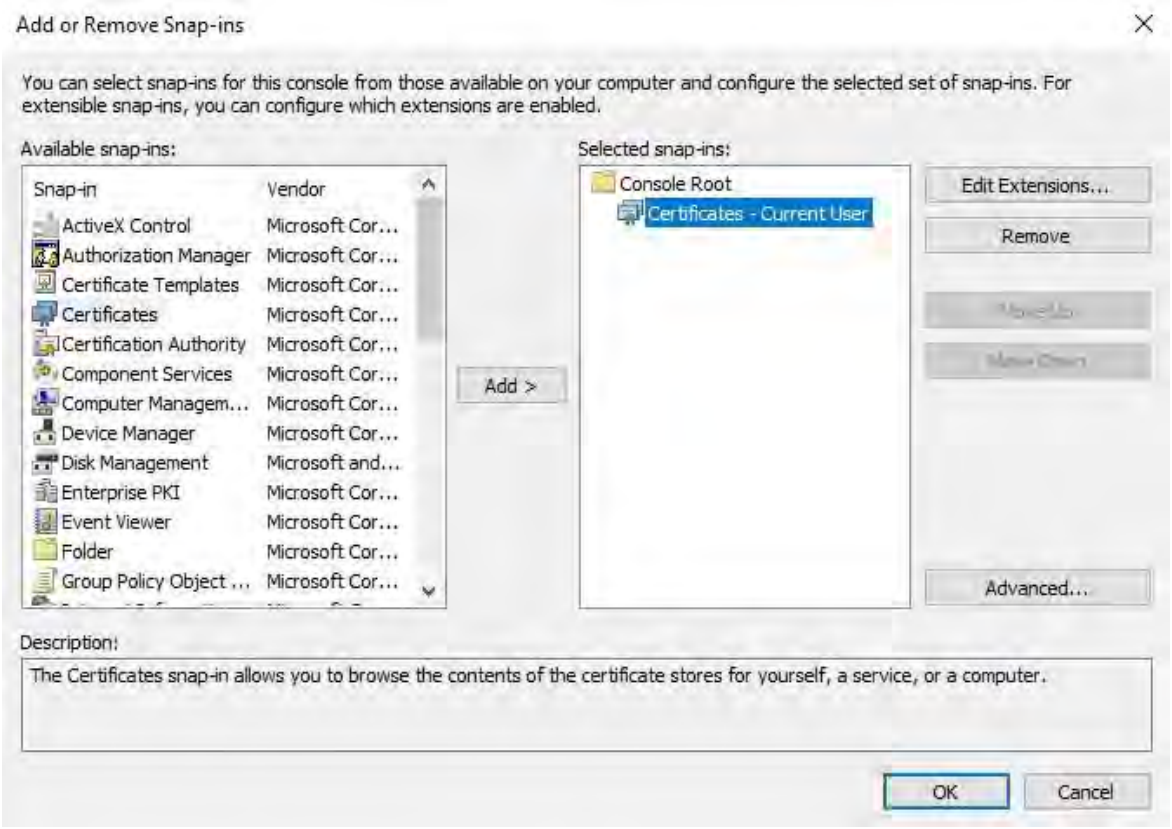


2. Dans Microsoft Management Console, dans le menu Fichier, sélectionnez **Ajouter/Supprimer un composant logiciel enfichable...**.

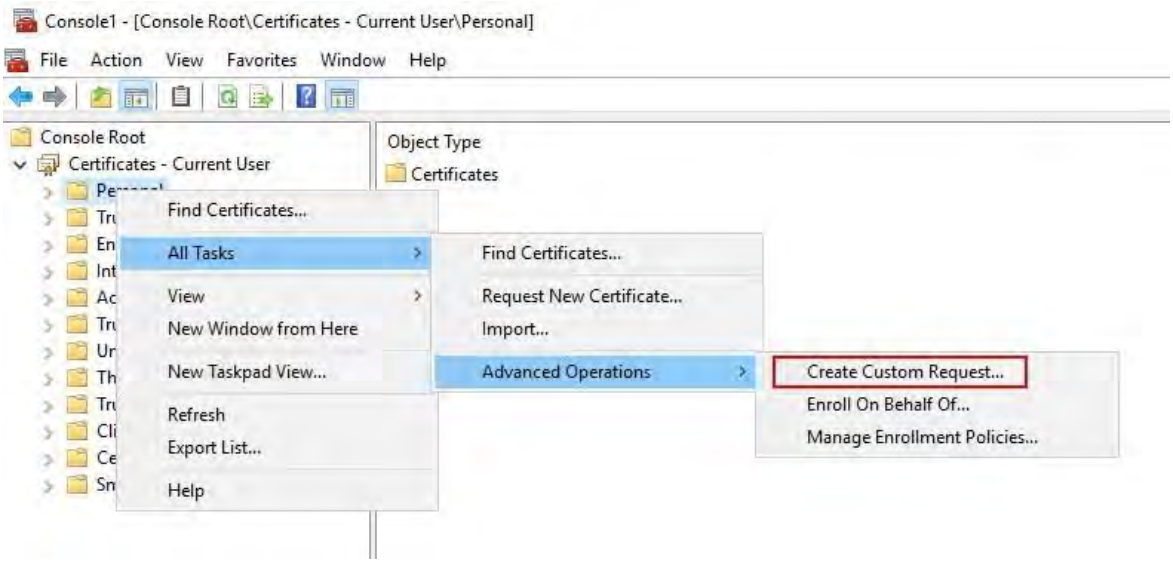


3. Sélectionnez le composant logiciel enfichable Certificats et cliquez sur **Ajouter**.

   Cliquez sur **OK**.

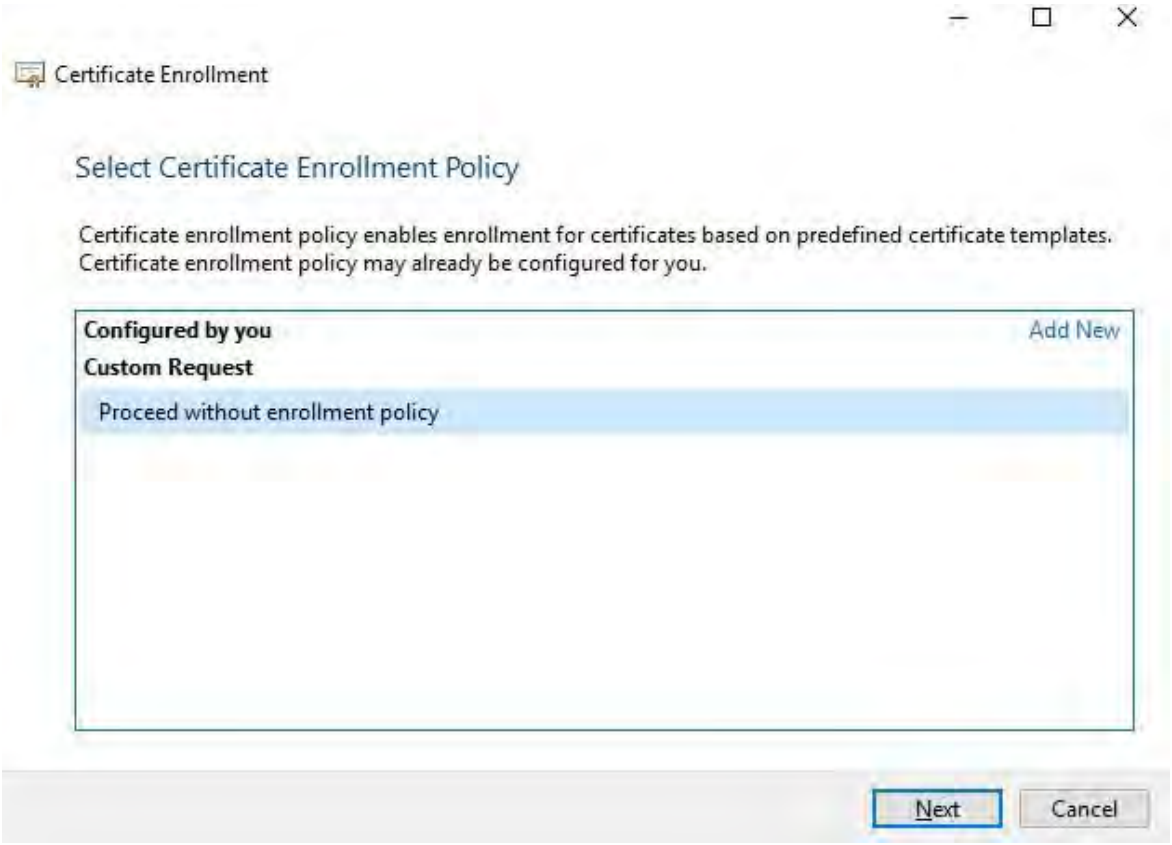


4. Développez l'objet Certificates. Cliquez avec le bouton droit de la souris sur le **dossier Personnel** et sélectionnez **Toutes les tâches** > **Opérations avancées** > **Créer une demande personnalisée**.

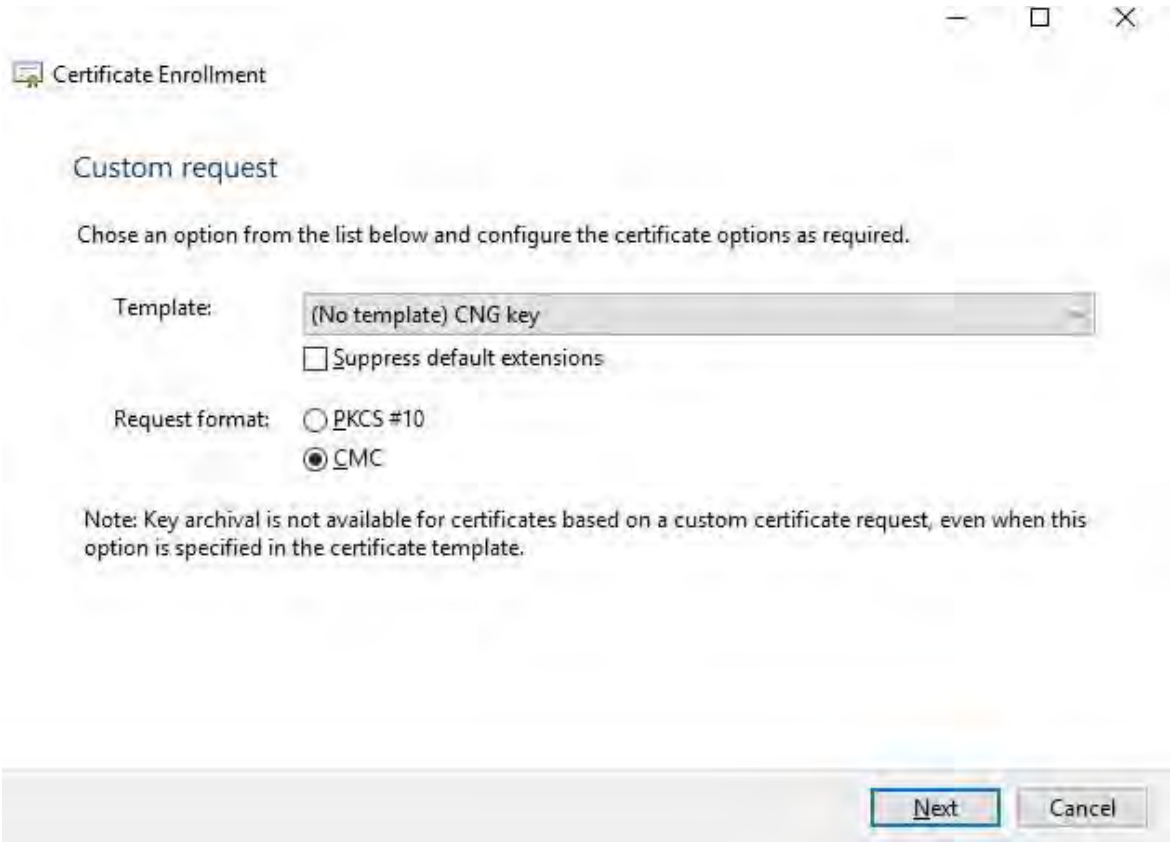


5. Cliquez sur **Suivant** dans l' Assistant **Inscription de certificat** et sélectionnez **Continuer sans stratégie d'inscription**.

   Cliquez sur **Suivant**.



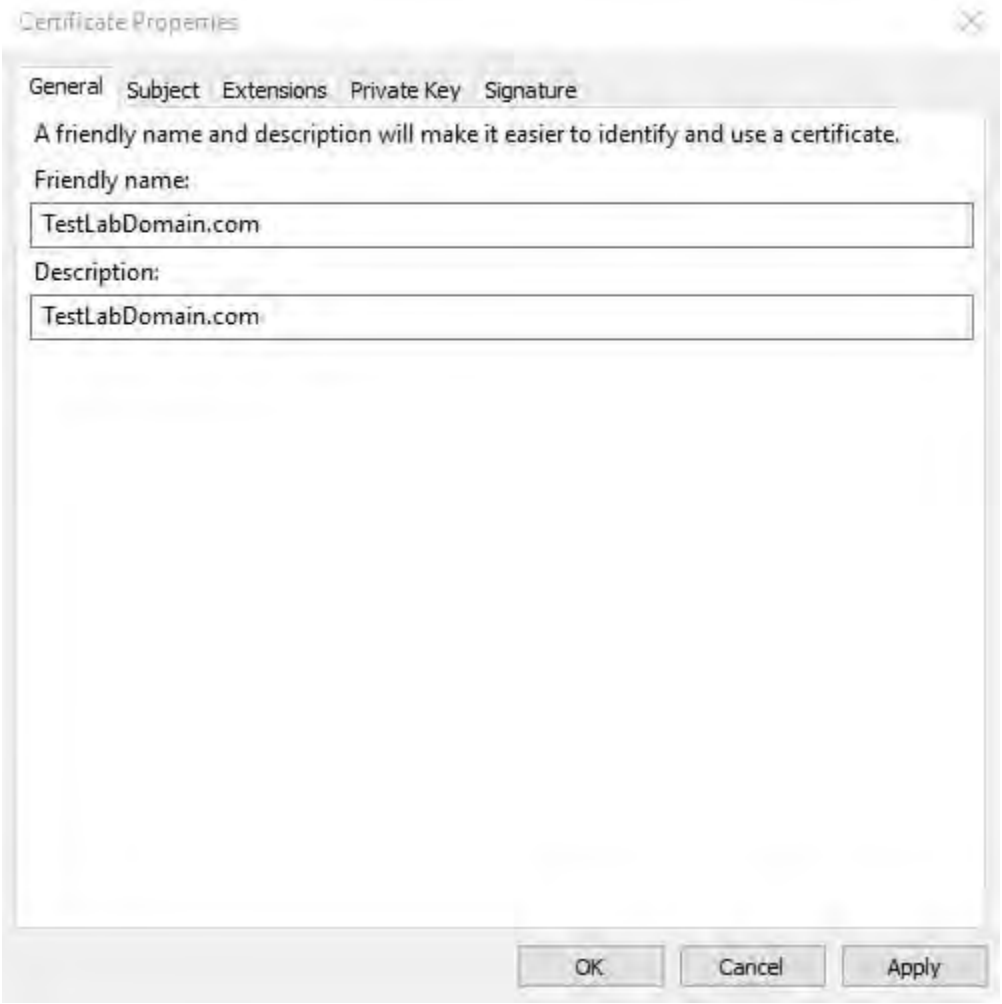
6. Sélectionnez le **modèle de clé CNG (sans modèle)** et le format de demande **CMC**, puis cliquez sur **Suivant**.



Le format de la demande dépend de l'autorité de certification. Si le format choisi est incorrect, l'autorité de certification émettra une erreur lors de l'envoi de la demande de signature de certificat (CSR). Vérifiez auprès de l'autorité de certification pour vous assurer que vous faites le bon choix.

7. Développez le champ d'affichage des **détails** de la demande personnalisée, puis cliquez sur **Propriétés**.

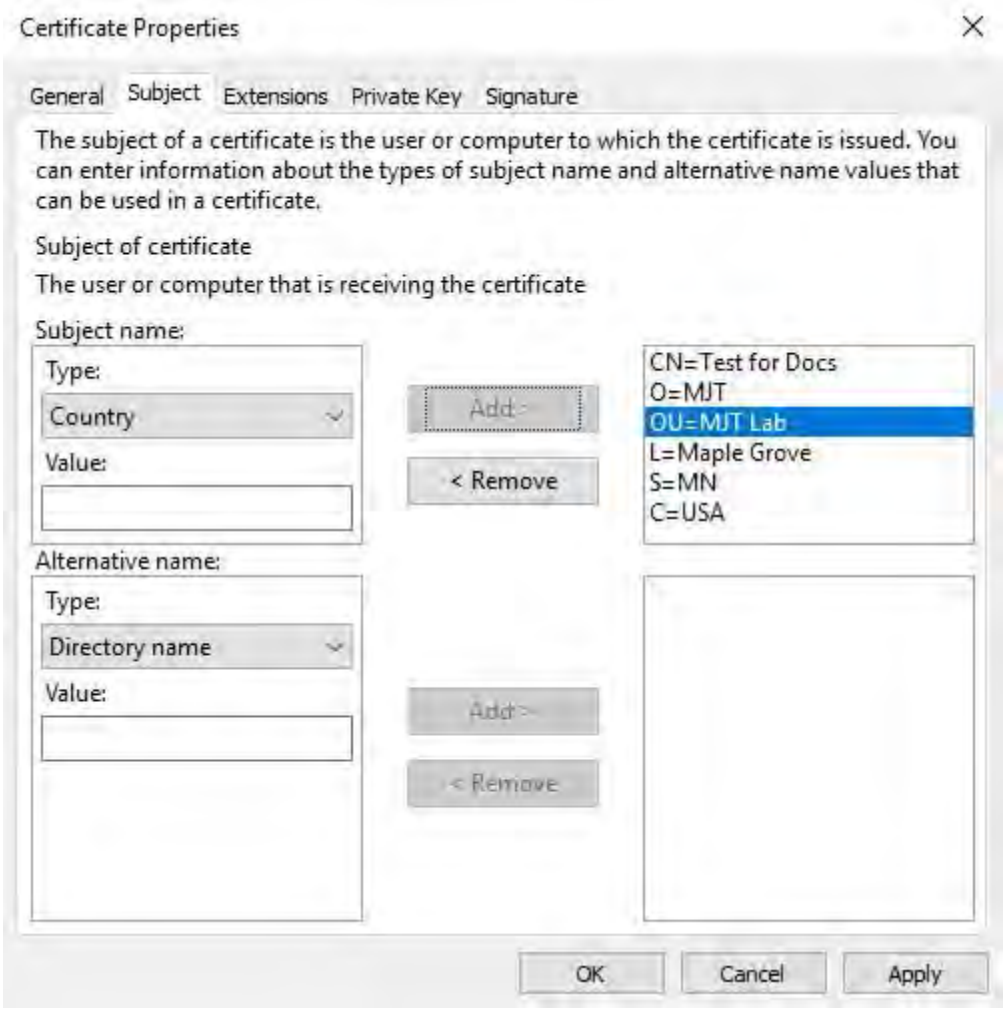
8. Dans l' **onglet Général**, remplissez les champs **Nom convivial** et **Description** avec le nom de domaine enregistré auprès de l'autorité de certification.



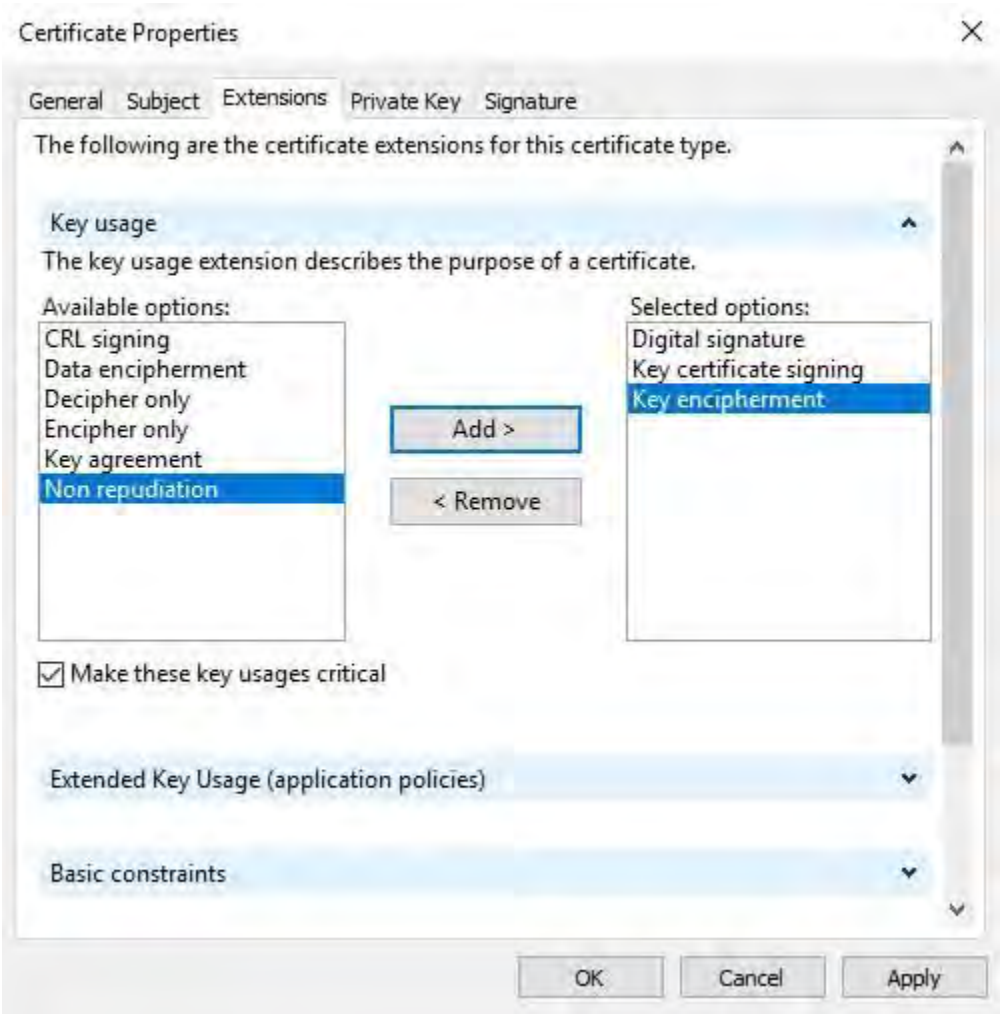
9. Dans l' **onglet Objet**, entrez les paramètres requis par l'autorité de certification spécifique.

   Par exemple, le nom de l'objet **Type** et **Valeur** sont différents pour chaque autorité de certification. Par exemple, les informations requises suivantes :

   - Nom commun:
   - Organisation:
   - Unité organisationnelle :
   - Ville/Localité :
   - État/Province :
   - Pays/Région :



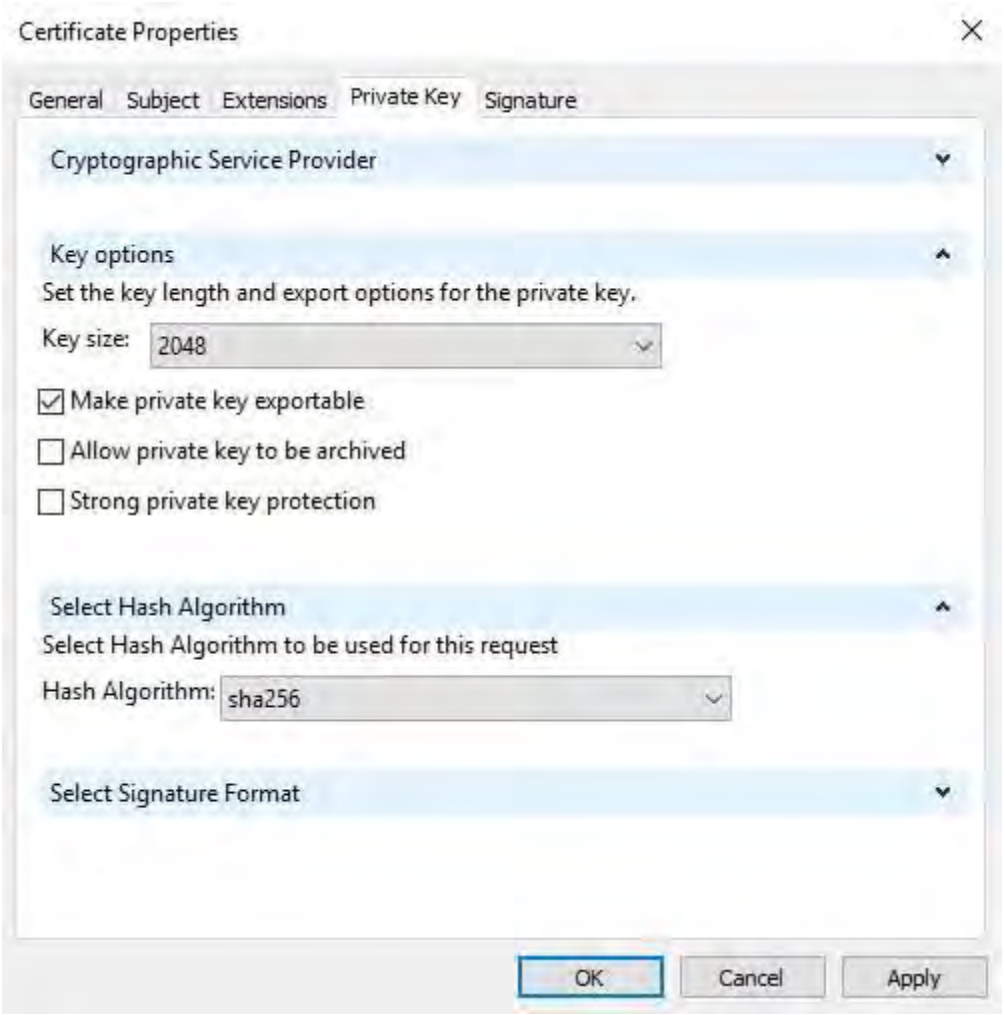
10. Certaines autorités de certification n'ont pas besoin d'extensions. Toutefois, si nécessaire, accédez à l' **onglet Extensions** et développez le menu Utilisation des **clés** . Ajoutez les options requises de la liste des **options disponibles** à la liste **des options sélectionnées**.



11. Sous l' **onglet Clé privée**, développez le menu Options de clé .

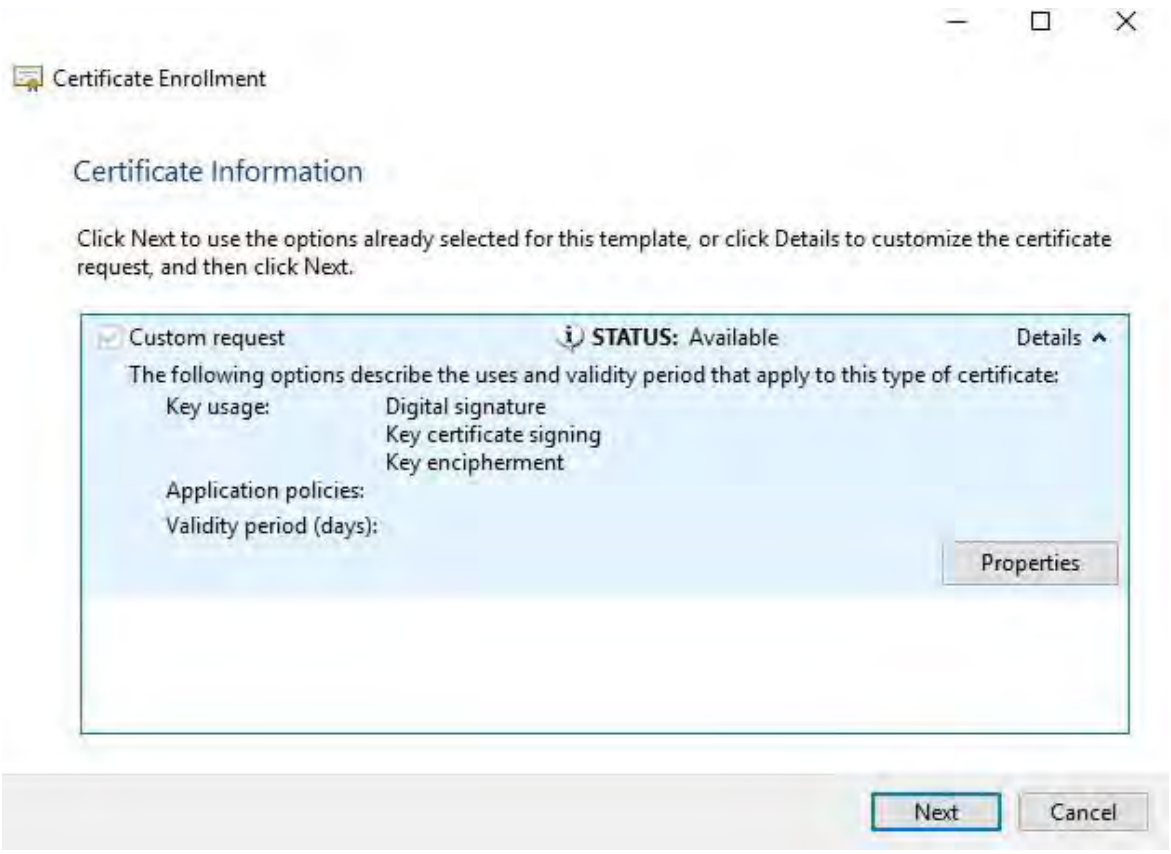
    Définissez la taille de la clé sur 2048 et sélectionnez l'option permettant d'exporter la clé privée.

    La variable de taille de clé est déterminée par l'autorité de certification, donc une clé de taille supérieure peut être requise. D'autres options, telles qu'un algorithme de hachage spécifique (sha256), peuvent également être requises. Ajustez toutes les options requises avant de passer à l'étape suivante.



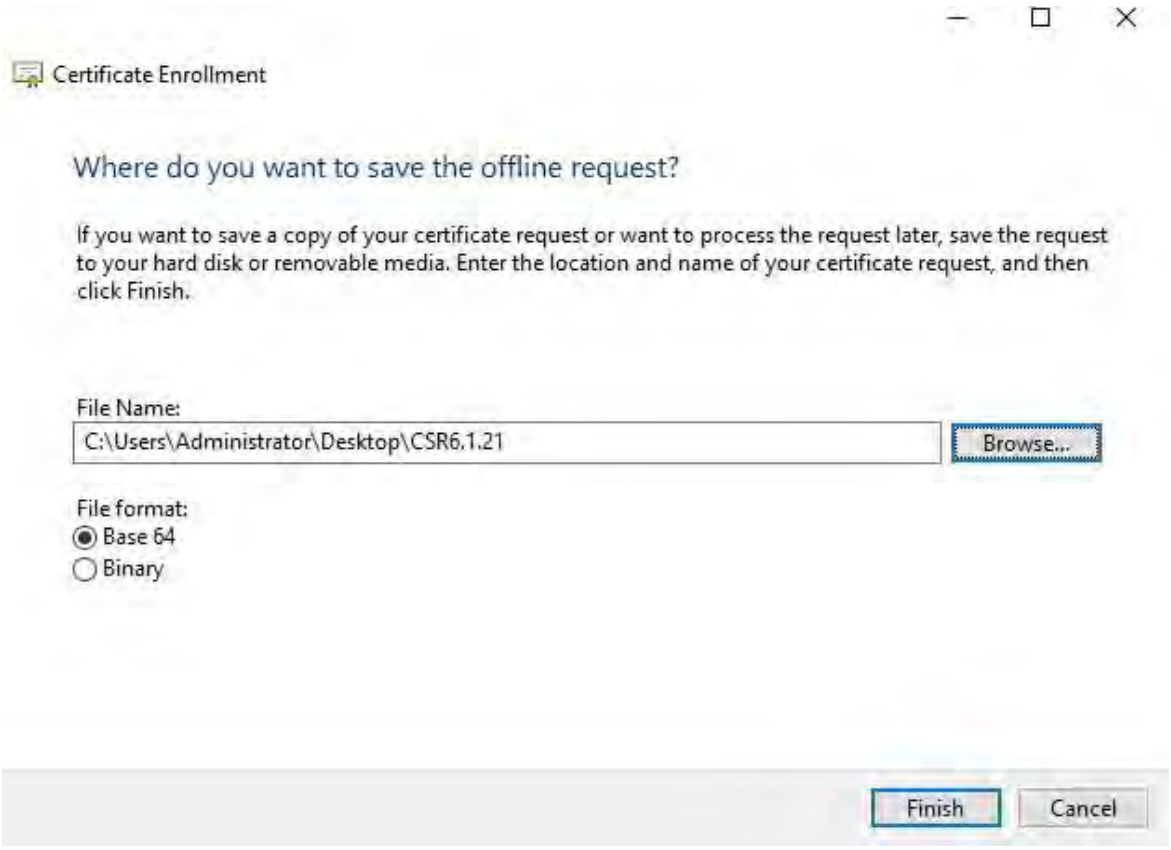
12. À moins que l'autorité de certification n'exige une signature, l'étape suivante consiste à cliquer sur **OK**.

13. Une fois que toutes les propriétés du certificat ont été définies, cliquez sur **Suivant** dans l' **onglet Inscription au certificat**
sorcier.



14. Sélectionnez un emplacement pour enregistrer la demande de certificat et un format. Naviguez jusqu'à cet emplacement et spécifiez un nom pour le fichier .req. Le format par défaut est la base 64, mais certaines autorités de certification exigent le format binaire.

15. Cliquez sur **Terminer**.



Un fichier .req est généré, que vous devez utiliser pour demander un certificat signé.

Téléchargez le fichier .req pour recevoir un certificat signé en retour

Chaque autorité de certification a un processus différent pour télécharger des fichiers .req afin de recevoir un certificat signé en retour. Reportez-vous à la documentation de votre autorité de certification pour plus d'informations sur la récupération d'un certificat signé.

Dans la plupart des situations d'autorité de certification tierce, il est nécessaire de télécharger un fichier .ZIP et d'extraire le contenu sur l'ordinateur qui héberge le serveur MOBOTIX HUB.

Il existe plusieurs types de fichiers qui peuvent être inclus dans le contenu du fichier .ZIP extrait.

. CER ou . Les fichiers CRT peuvent être installés à l'aide d'un processus similaire. Cliquez avec le bouton droit de la souris sur le fichier et choisissez Installer le **certificat**
dans le menu contextuel.

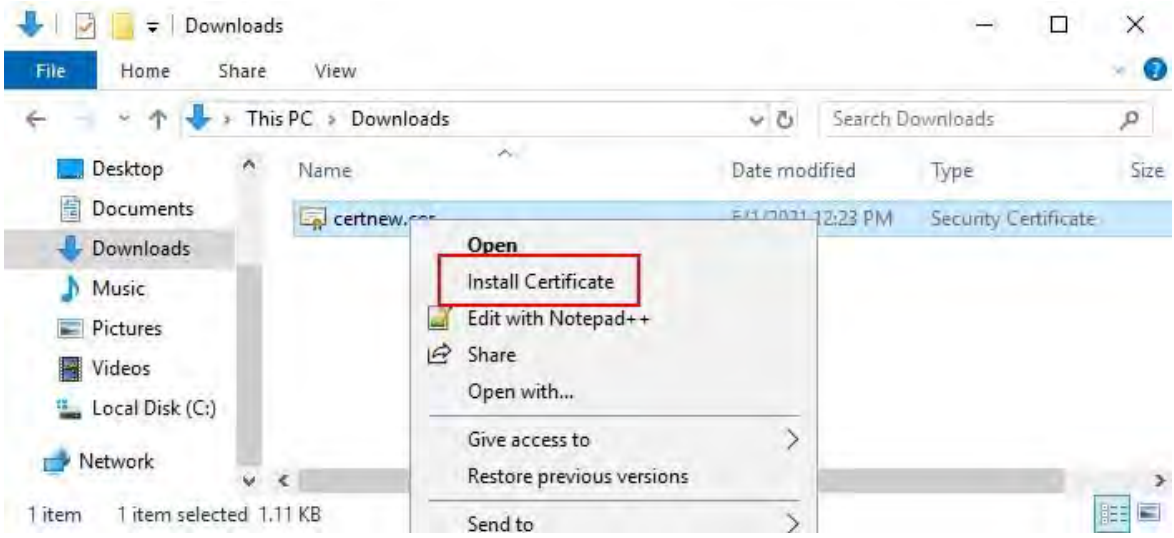
Les étapes suivantes utilisent un fichier . Fichier CER d'une autorité de certification interne.

Votre autorité de certification aura besoin du contenu du fichier .req. On vous demandera de copier tout le texte du fichier .req, y compris les lignes de début et de fin, et de coller le texte dans un champ disponible sur un portail géré par

l'autorité de certification.

1. Naviguez jusqu'à l'emplacement du fichier .req et ouvrez-le dans le Bloc-notes, puis collez le texte dans un champ mis à disposition sur un portail géré par votre autorité de certification.

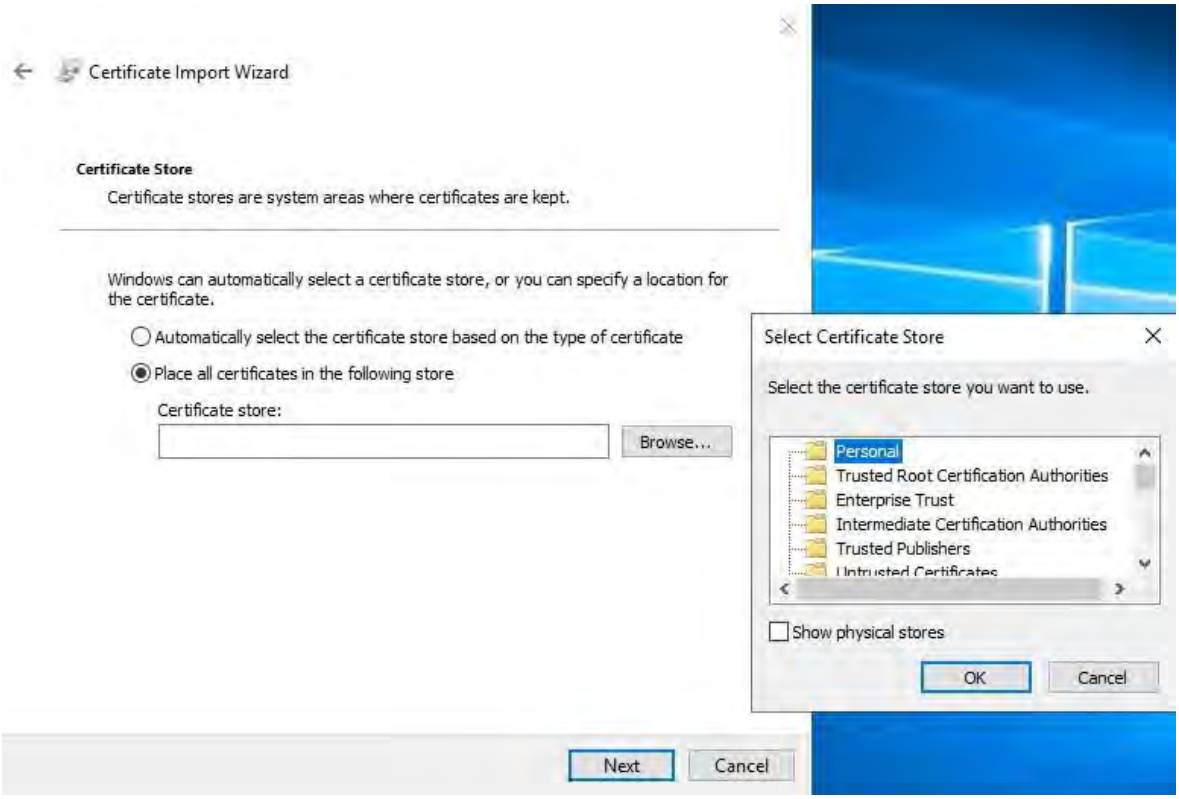
2. Lorsque vous recevez le certificat de votre autorité de certification, accédez au dossier des téléchargements (ou à l'endroit où vous choisissez de stocker le dossier sur l'ordinateur), cliquez avec le bouton droit sur le certificat et sélectionnez Installer le **certificat**.



3. Acceptez l'avertissement de sécurité s'il apparaît.

   Sélectionnez cette option pour installer le certificat pour l'ordinateur local et cliquez sur **Suivant**.

4. Choisissez un emplacement de stockage, accédez au magasin de certificats personnel, puis cliquez sur **Suivant**.



5. Terminez l' assistant **d'installation du certificat**.

Activer le chiffrement vers et depuis le serveur de gestion

Vous pouvez chiffrer la connexion bidirectionnelle entre le serveur de gestion et le collecteur de données associé lorsque vous disposez d'un serveur distant du type suivant :

- Serveur d'enregistrement
- Serveur d'événements
- Serveur de journaux
- Serveur LPR
- Serveur mobile

Si votre système contient plusieurs serveurs d'enregistrement ou des serveurs distants, vous devez activer le chiffrement sur chacun d' entre eux.

Lorsque vous configurez le chiffrement pour un groupe de serveurs, il doit être activé à l'aide d'un certificat appartenant au même certificat d'autorité de certification ou, si le chiffrement est désactivé, il doit être désactivé sur tous les ordinateurs du groupe de serveurs.

Conditions préalables:

- Un certificat d'authentification de serveur est approuvé sur l'ordinateur qui héberge le serveur de

gestion Tout d'abord, activez le chiffrement sur le serveur de gestion.

Escalier:

1. Sur un ordinateur sur lequel un serveur de gestion est installé, ouvrez le **configurateur de serveur** à partir de :

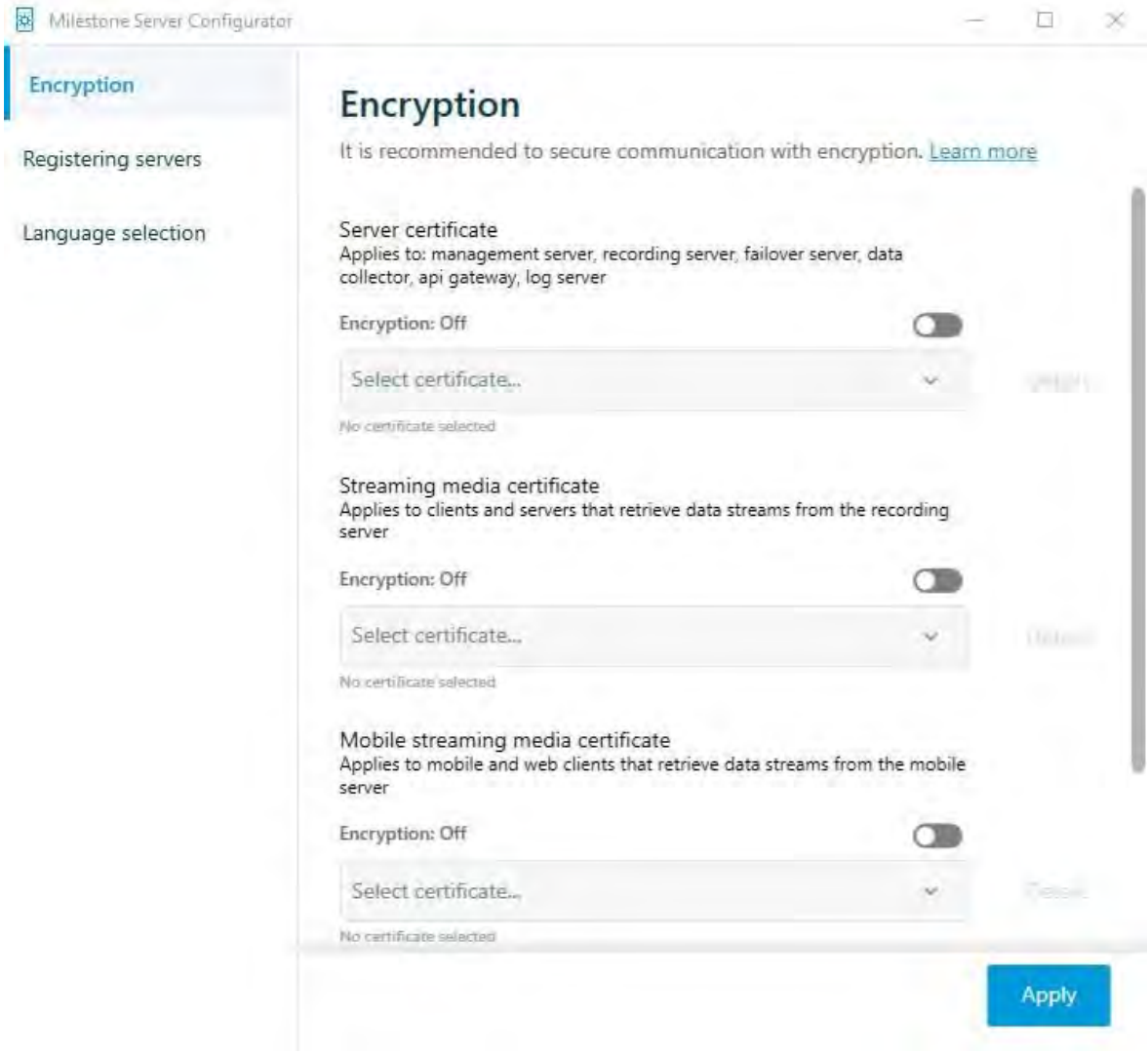
    - Le menu Démarrer de Windows

    ou

    - Le Gestionnaire du serveur de gestion en cliquant avec le bouton droit de la souris sur l'icône du Gestionnaire du Gestionnaire du Serveur de gestion dans la barre des tâches de l 'ordinateur

2. Dans le **configurateur de serveur**, sous **Certificat de serveur**, activez **le cryptage**.
3. Cliquez sur **Sélectionner un certificat** pour ouvrir une liste avec les noms d'objet uniques des certificats qui ont une clé privée et qui sont installés sur l'ordinateur local dans le magasin de certificats Windows.
4. Sélectionnez un certificat pour chiffrer la communication entre le serveur d'enregistrement, le serveur de gestion, le serveur de basculement et le serveur de collecte de données.

Sélectionnez **Détails** pour afficher les informations du Magasin de certificats Windows concernant le certificat sélectionné.



5. Cliquez sur **Appliquer**.

Pour terminer l'activation du chiffrement, l'étape suivante consiste à mettre à jour les paramètres de chiffrement sur chaque serveur d'enregistrement et chaque serveur doté d'un collecteur de données (serveur d'événements, serveur de journaux, serveur LPR et serveur mobile).

Installer les services de certificats Active Directory

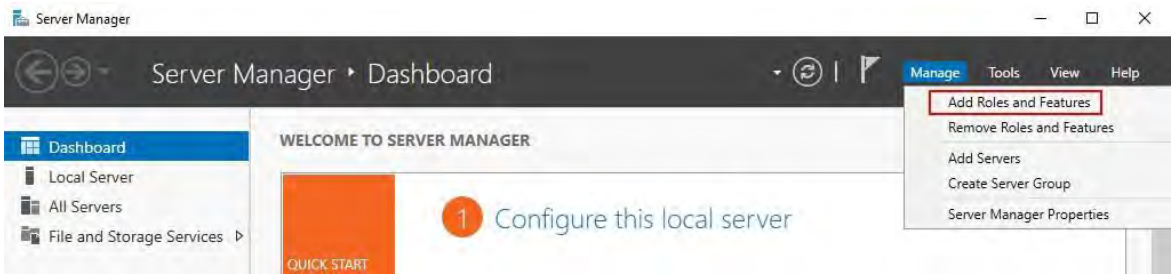
Les services de certificats Active Directory (AD CS) sont un produit Microsoft qui exécute des fonctionnalités d'infrastructure à clé publique (PKI). Il agit comme un rôle serveur qui vous permet de construire une infrastructure à clé publique (PKI) et de fournir une cryptographie à clé ouverte, une authentification informatisée et des capacités de marquage avancées pour votre association.

Dans ce document, AD CS est utilisé lors de l'installation de certificats :

- Dans un environnement de domaine (voir Installer des certificats dans un domaine pour la communication avec le Serveur de gestion ou le Serveur d'enregistrement à la page 86)
- Dans un environnement de groupe de travail (voir Installer des certificats dans un environnement de groupe de travail pour la communication avec le serveur de gestion ou le serveur d'enregistrement à la page 104)

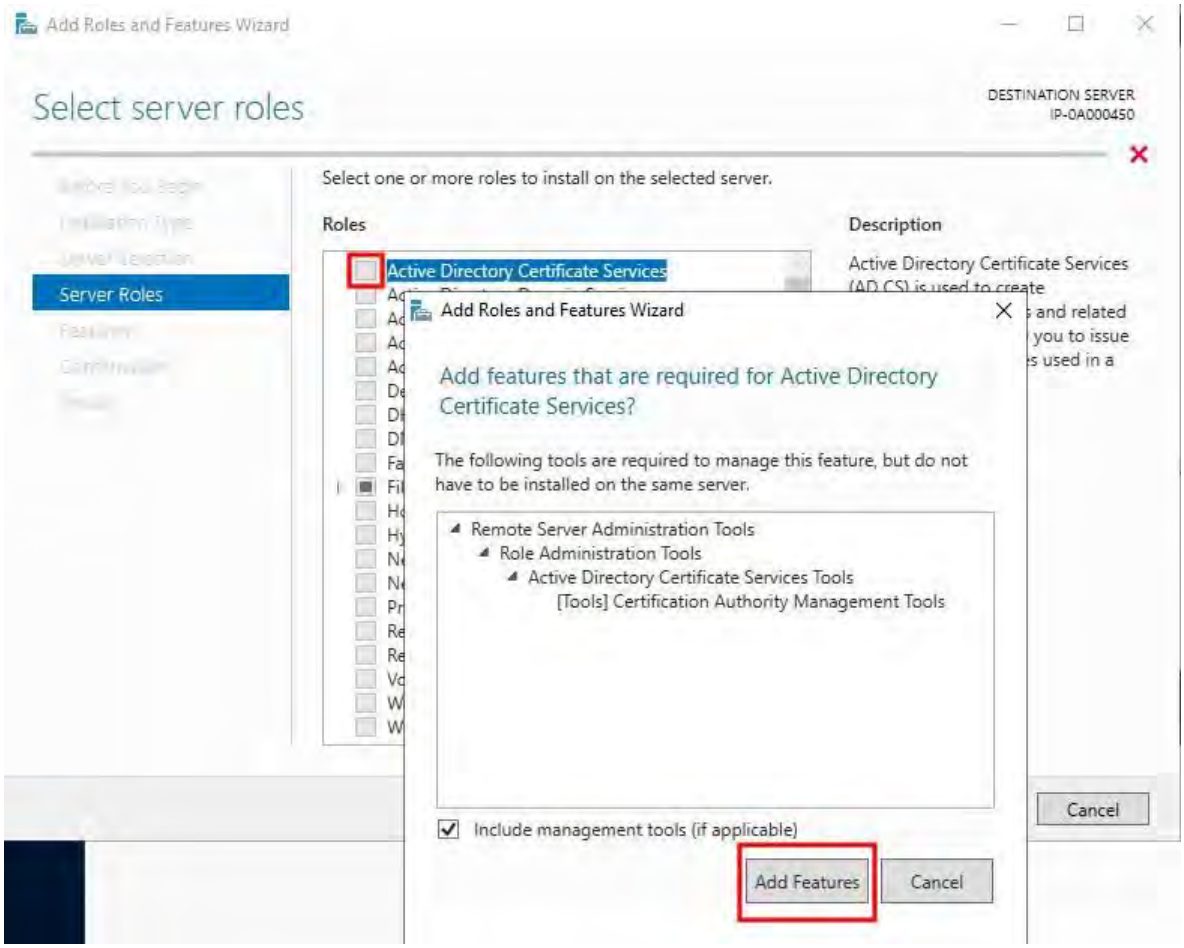
Pour installer AD CS :

1. Dans l' application **Gestionnaire de serveur**, sélectionnez **Gérer** > **Ajouter des rôles et des fonctionnalités**.



2. Dans **Avant de commencer**, cliquez sur **Suivant**.
3. Dans **Type d'installation**, sélectionnez **Installation basée sur les rôles ou sur les fonctionnalités**, puis cliquez sur **Suivant**.
4. Dans **Sélection du serveur**, sélectionnez le serveur local comme destination de l'installation, puis cliquez sur **Suivant**.

5. Dans **Rôles serveur**, sélectionnez le **rôle Services de certificats Active Directory**. Passez en revue la liste des fonctionnalités à installer et cliquez sur **Ajouter des fonctionnalités**.



Cliquez sur **Suivant**.

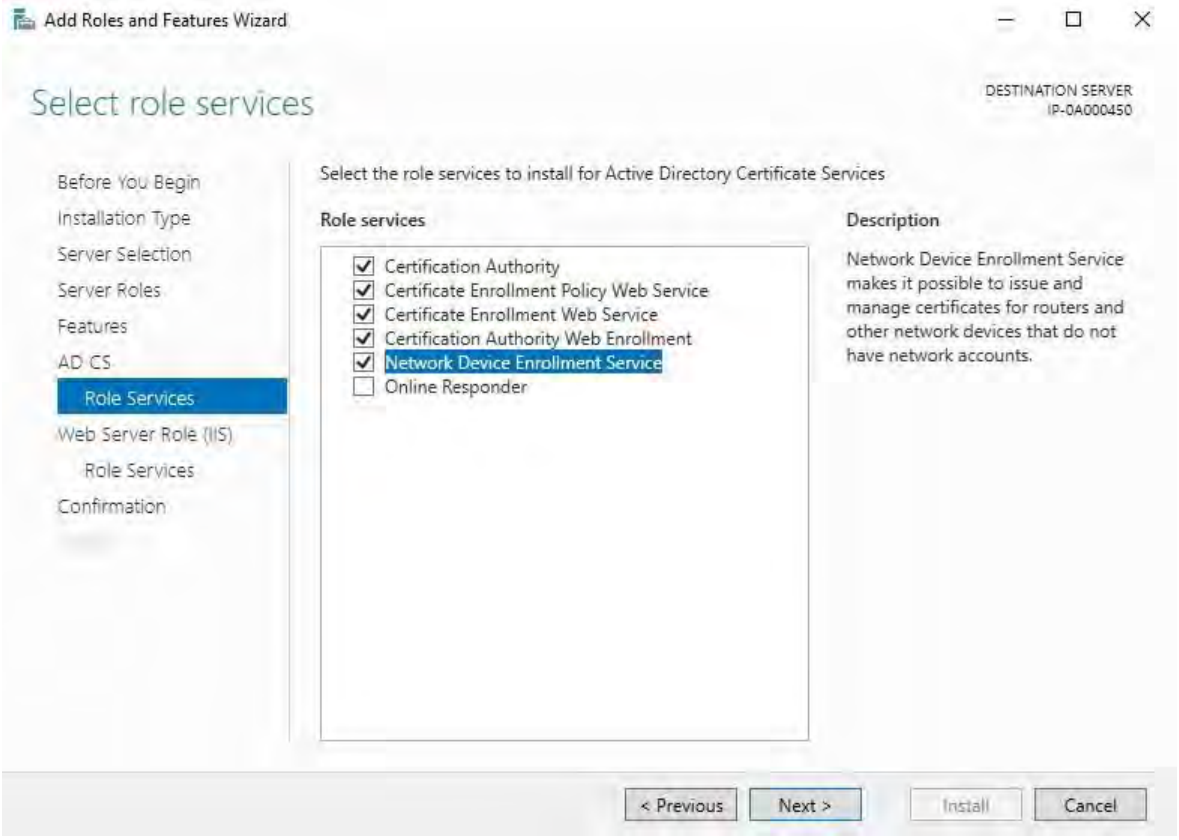
6. Dans **Fonctionnalités**, cliquez sur **Suivant**. Toutes les fonctionnalités requises sont sélectionnées pour l'installation.

7. Dans **AD CS,** lisez la description des services certifiés Active Directory, puis cliquez sur **Suivant**.

8. Dans Services de rôle, sélectionnez les éléments suivants :

   - **Autorité de certification**
   - **Service Web de politique d'inscription à la certification**
   - **Service Web d'inscription à la certification**
   - **Inscription Web de l'autorité de certification**
   - **Service d'inscription des périphériques réseau**

   Lorsque vous sélectionnez chacun des services de rôle, ajoutez les fonctionnalités requises pour prendre en charge l'installation de chaque service.

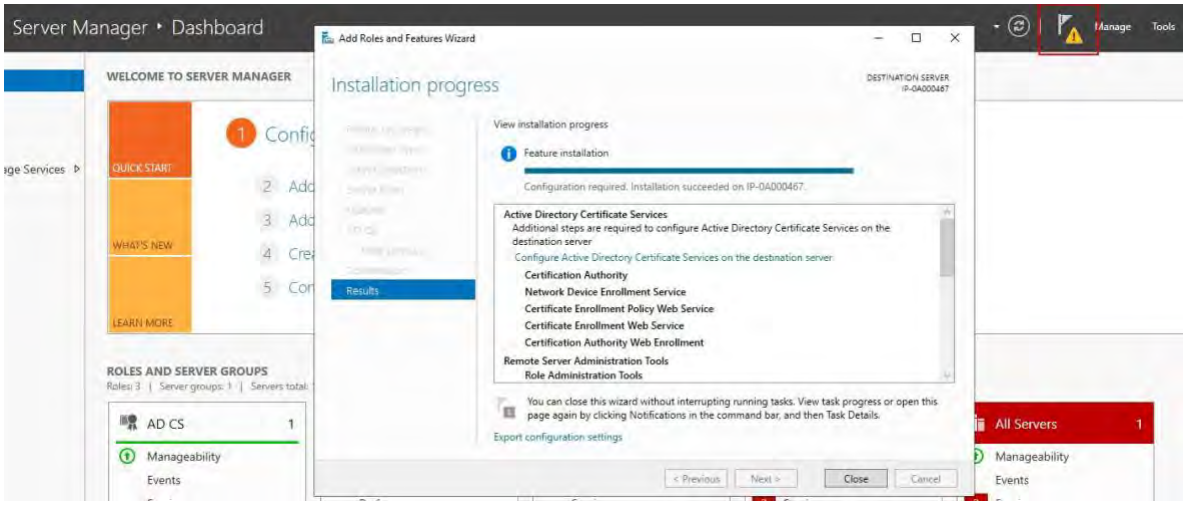


   Cliquez sur **Suivant**.

9. Dans **Confirmation**, sélectionnez **Redémarrer automatiquement le serveur de destination si nécessaire**, puis cliquez sur **Installer**.

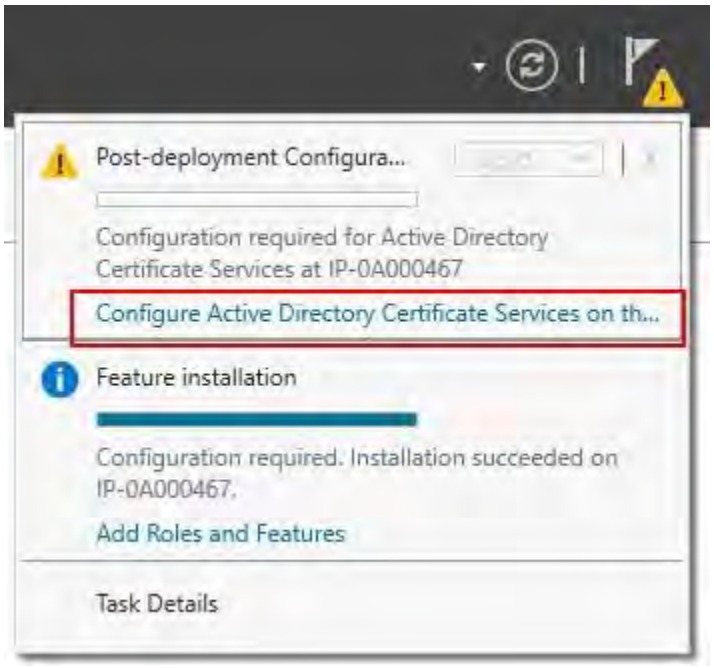
10. Une fois l'installation terminée, cliquez sur le **bouton Fermer**.

    Sélectionnez l'**indicateur de notification** dans l' application **Gestionnaire de serveur**.



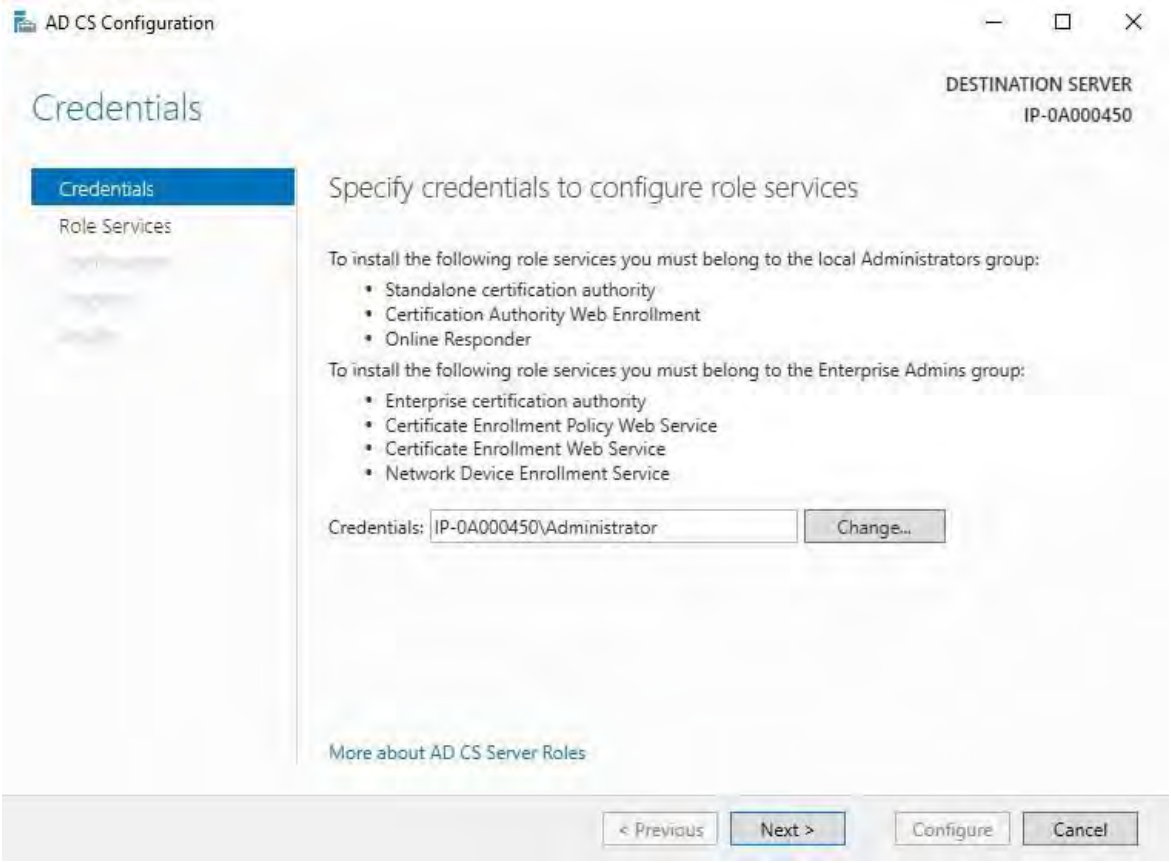
11. Un message pour commencer la configuration post-déploiement est répertorié sous l' **indicateur de notification**.

    Cliquez sur le lien pour commencer la configuration des services installés.



12. L'Assistant **de configuration des services de certificats Active Directory** démarre.

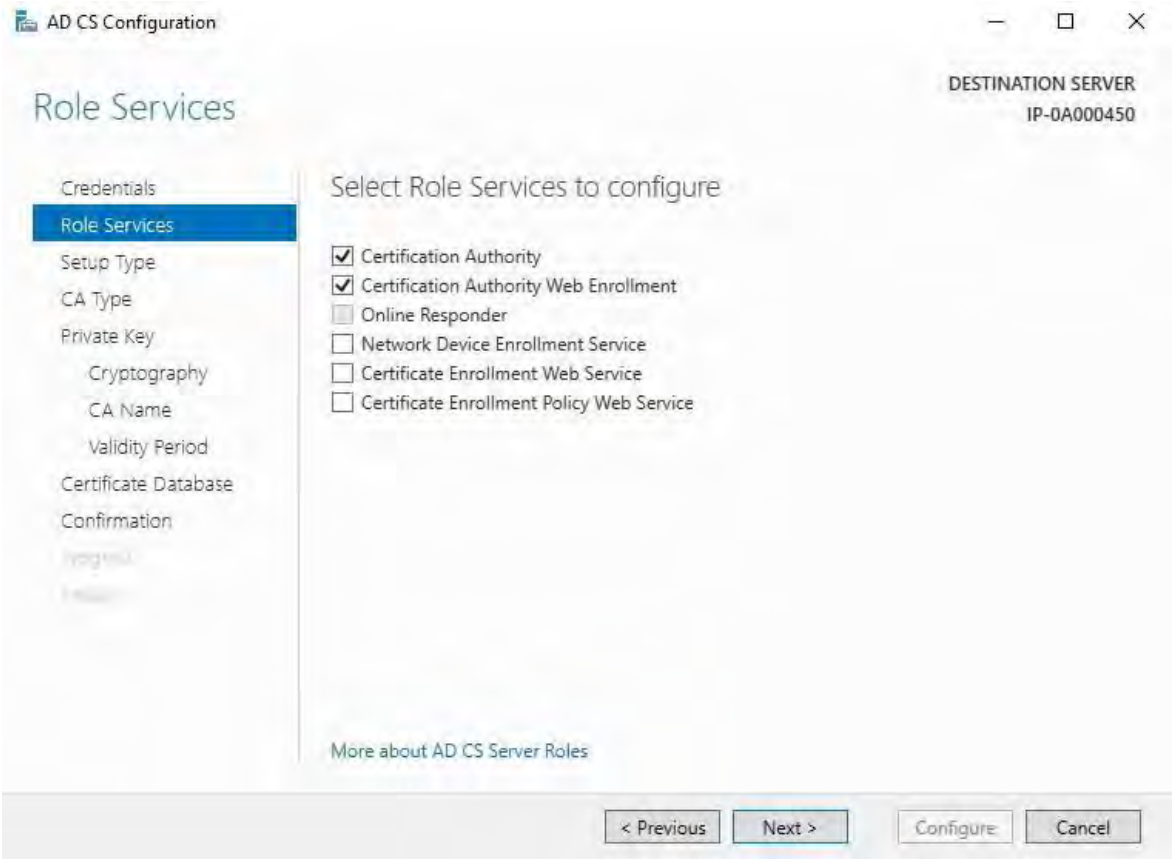
    Dans **Informations d'identification**, sélectionnez le compte d'utilisateur requis pour exécuter les services installés. Comme indiqué dans le texte, l'appartenance aux groupes d'administrateurs locaux et d'administrateurs d'entreprise est requise. Entrez les informations de compte requises et cliquez sur **Suivant**.



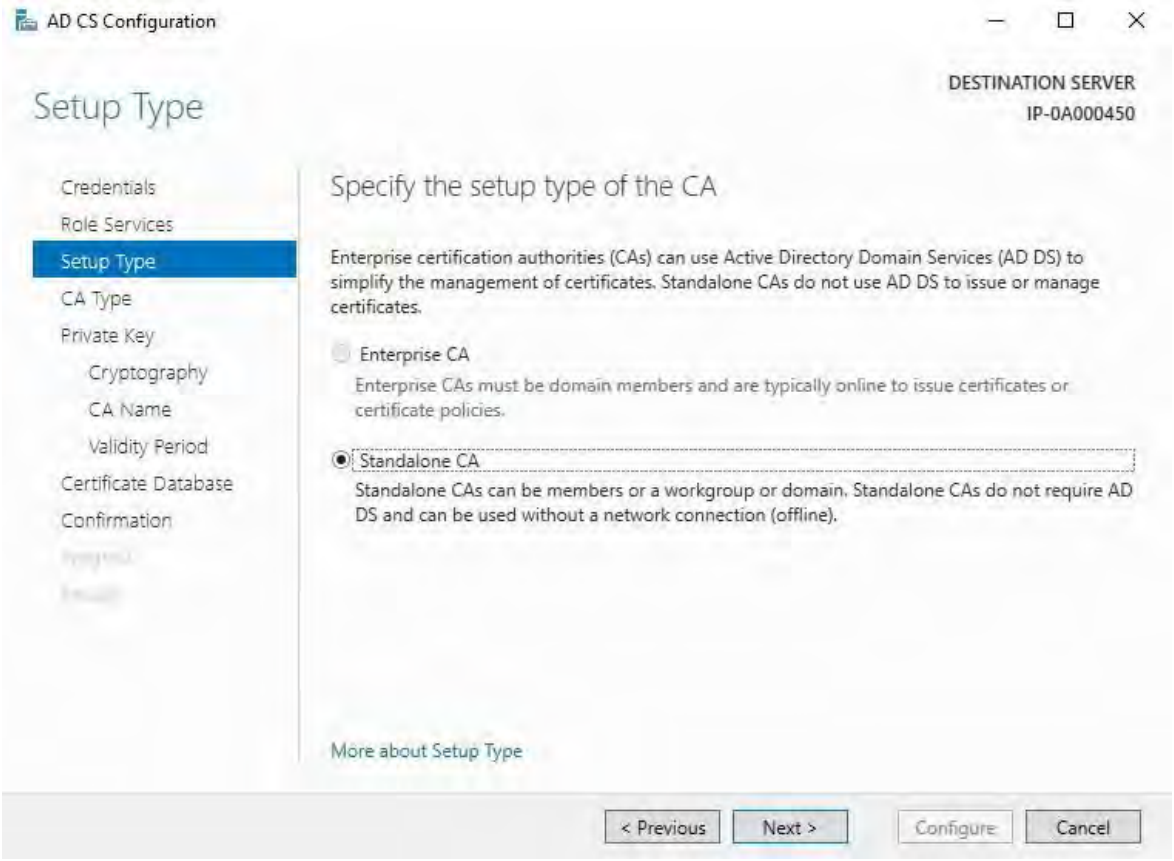
13. Dans **Services de rôle**, sélectionnez les services suivants :

    - **Autorité de certification**
    - **Inscription Web de l'autorité de certification**

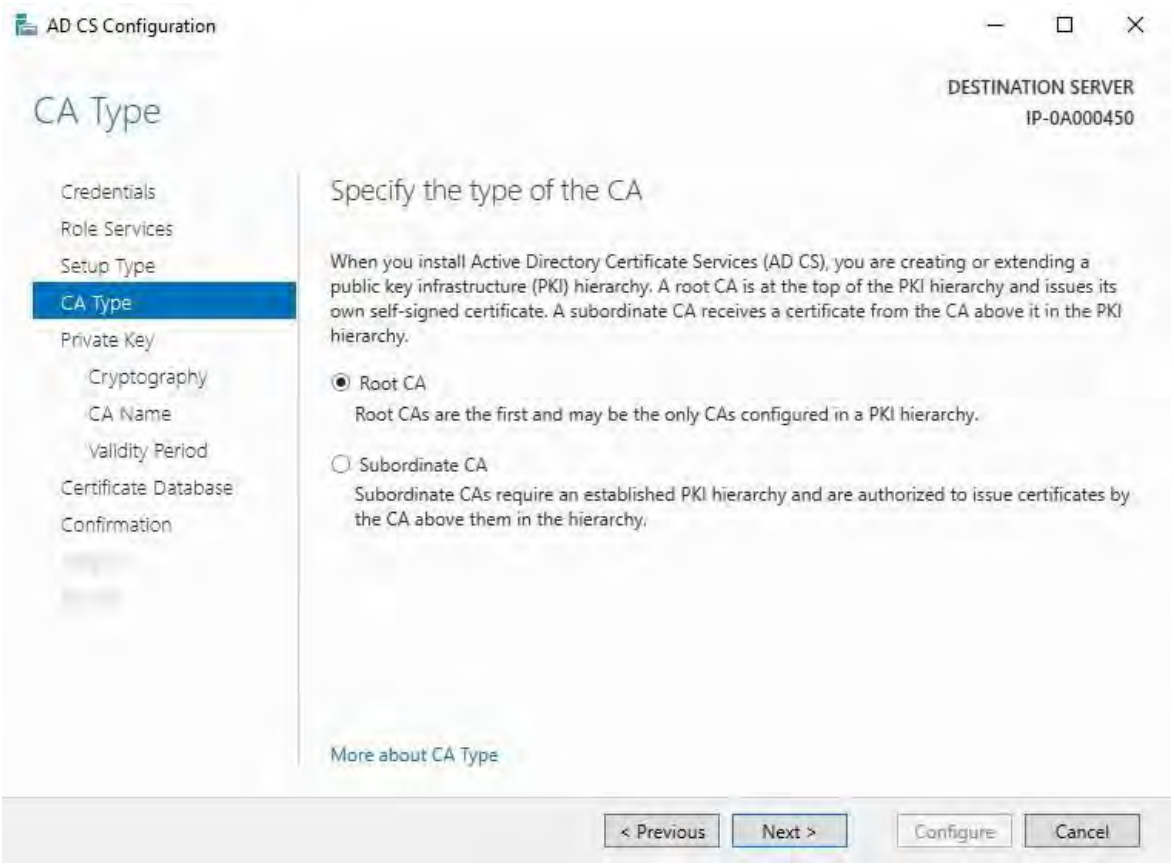
    Cliquez sur **Suivant**.



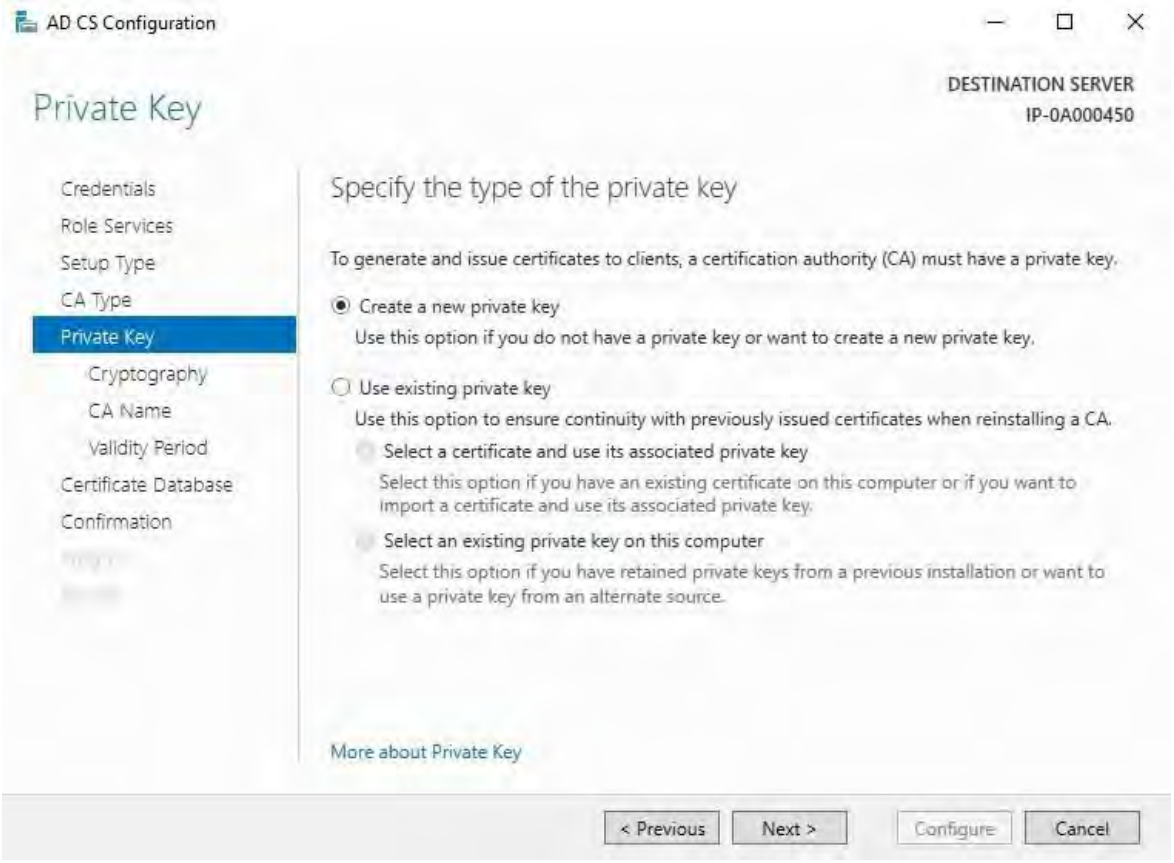
14. Dans **Type d'installation**, sélectionnez l' **option Autonome CA** et cliquez sur **Suivant**.



15. Dans Type d'**autorité de certification**, sélectionnez l'option d'installation d'une autorité de **certification racine**, puis cliquez sur **Suivant**.

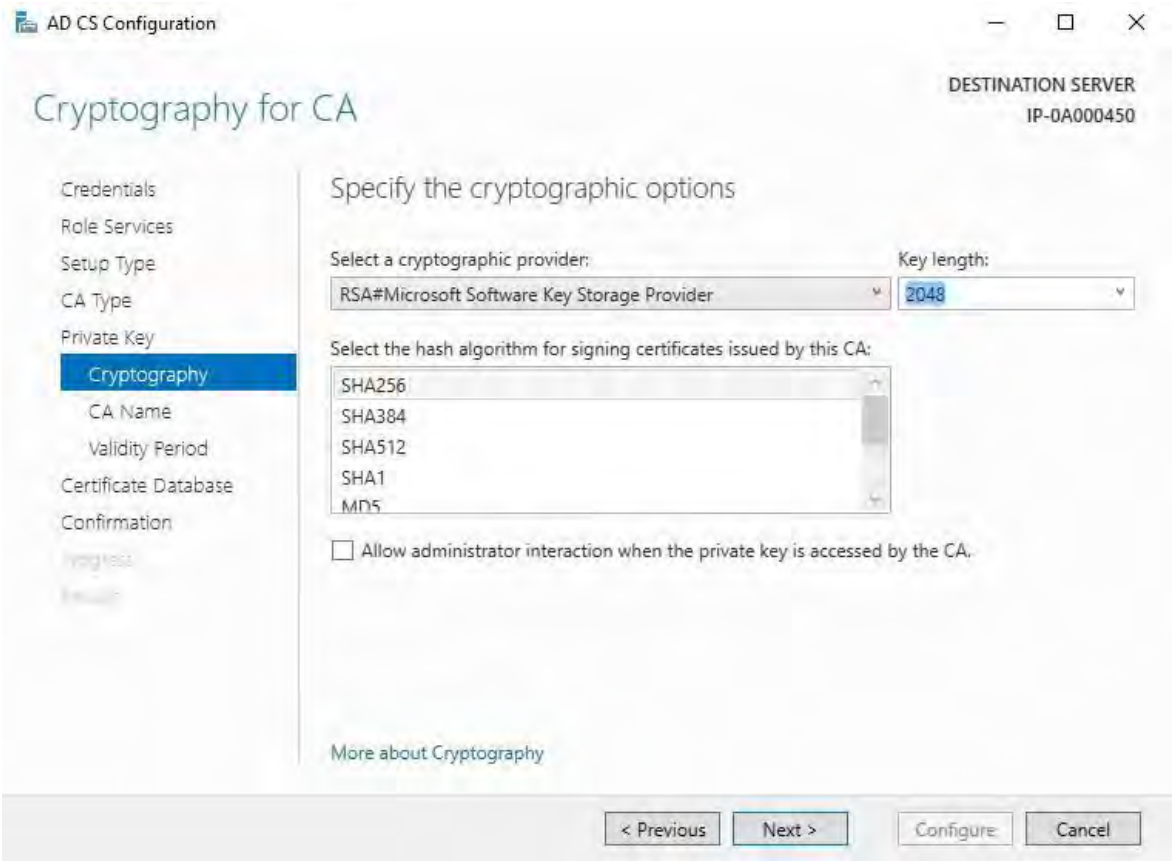


16. Dans **Clé privée**, sélectionnez l'option de création d'une clé privée, puis cliquez sur **Suivant**.



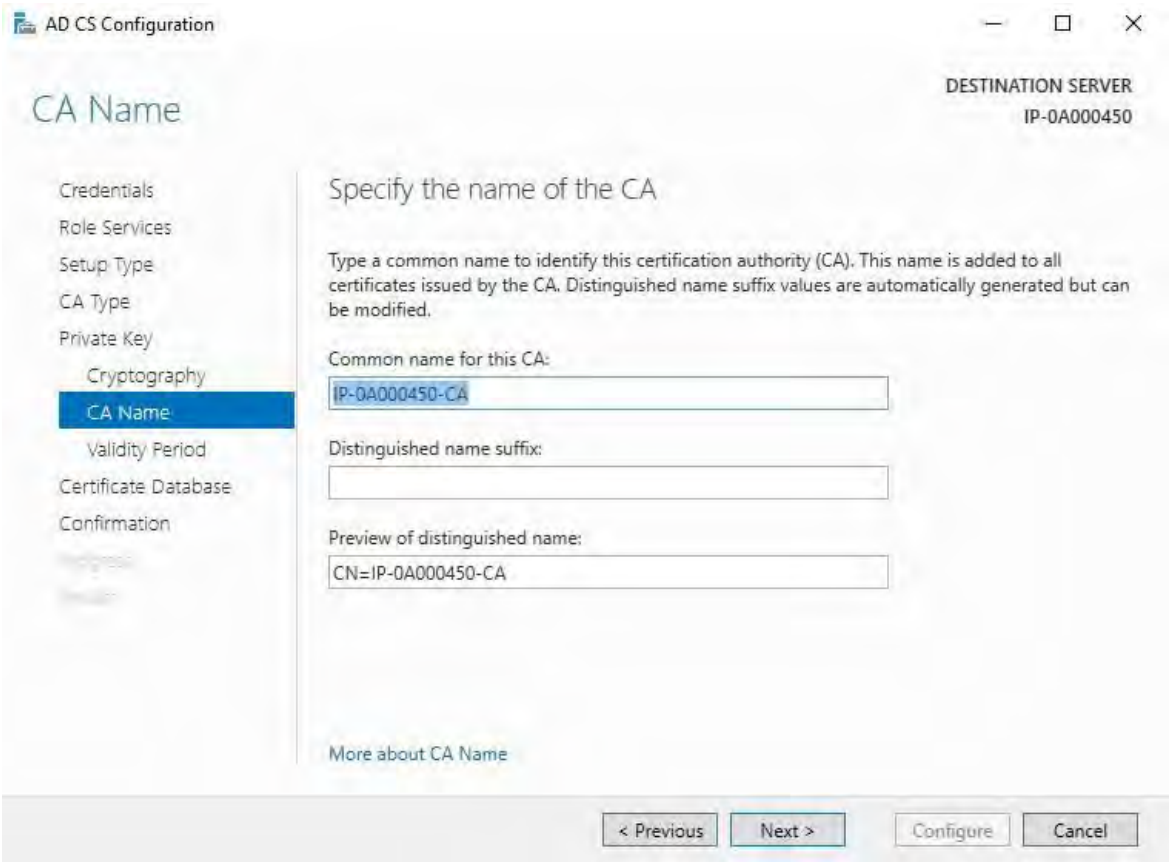
17. Dans **Cryptographie**, sélectionnez **RSA#Microsoft Software Key Storage Provider** pour l'option de fournisseur de chiffrement avec une **longueur de clé** de 2048 et un algorithme de hachage de SHA256.

    Cliquez sur **Suivant**.

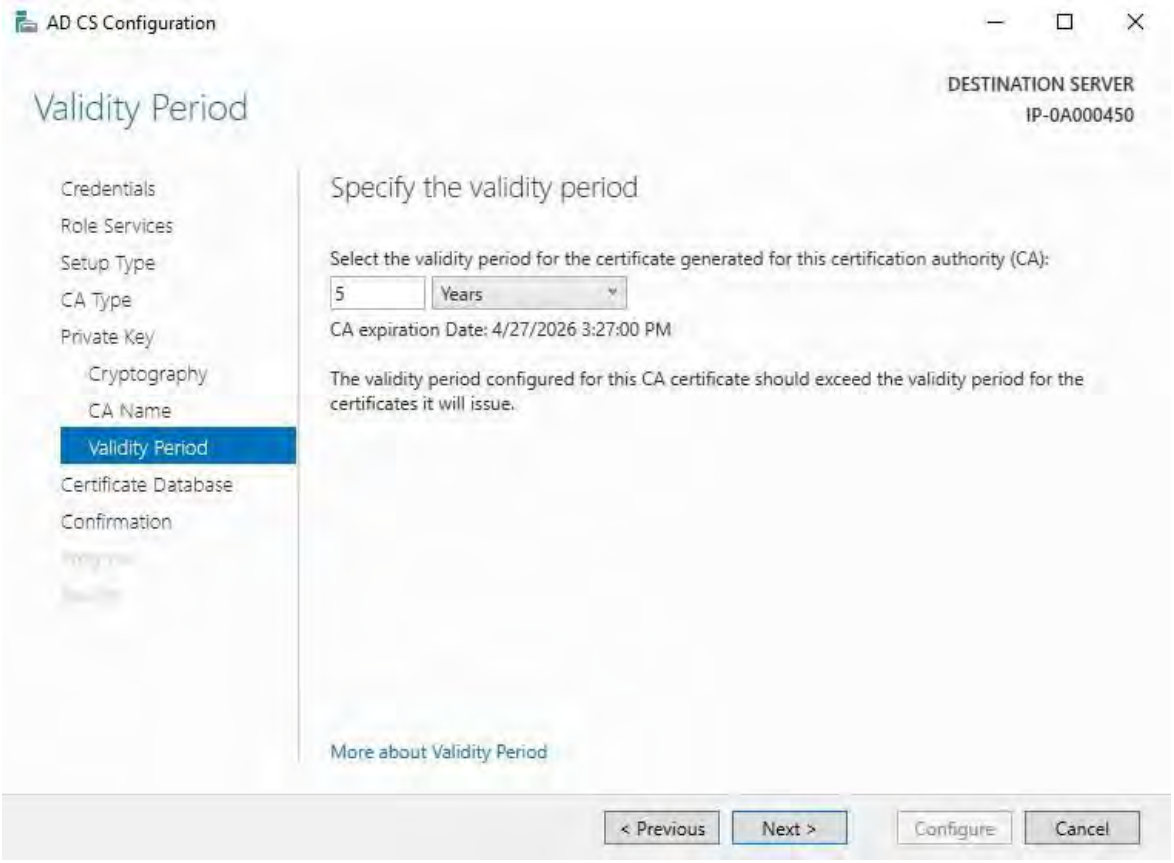


18. Dans **Nom de l'autorité de certification**, entrez le nom de l'autorité de certification et cliquez sur **Suivant**.

    Par défaut, le nom est « localhost-CA » - en supposant que le nom de l'ordinateur du serveur local est « localhost ».



19. Dans **Période de validité**, sélectionnez la période de validité par défaut de 5 ans, puis cliquez sur **Suivant**.



20. Dans **Base de données de** certificats, entrez les emplacements de la base de données et de la base de données de journaux.

    Les emplacements de base de données par défaut pour le magasin de certificats sont les suivants :
    `C:\Windows\system32\CertLog`

    Cliquez sur **Suivant**.

21. Dans **Confirmation**, passez en revue les options de configuration sélectionnées et cliquez sur **Configurer** pour commencer le processus de configuration.

22. Une fois la configuration terminée, cliquez sur **Fermer**.

    Lorsque vous êtes invité à configurer des services de rôle supplémentaires, cliquez sur **Non**.

23. Redémarrez le serveur local pour vous assurer qu'il est prêt à servir de serveur de certificats Active Directory.

Installer des certificats dans un domaine pour la communication avec le Serveur de gestion ou le Serveur d'enregistrement

Lorsque les points de terminaison client et serveur fonctionnent tous dans un environnement de domaine, il n'est pas nécessaire de distribuer des certificats d'autorité de certification aux postes de travail clients. La stratégie de groupe au sein du domaine gère la distribution automatique de tous les certificats d'autorité de certification approuvés à tous les utilisateurs et ordinateurs du domaine.

En effet, lorsque vous installez une autorité de certification racine d'entreprise, celle-ci utilise la stratégie de groupe pour propager son certificat dans le magasin de certificats des autorités de certification racines approuvées pour tous les utilisateurs et ordinateurs du domaine.

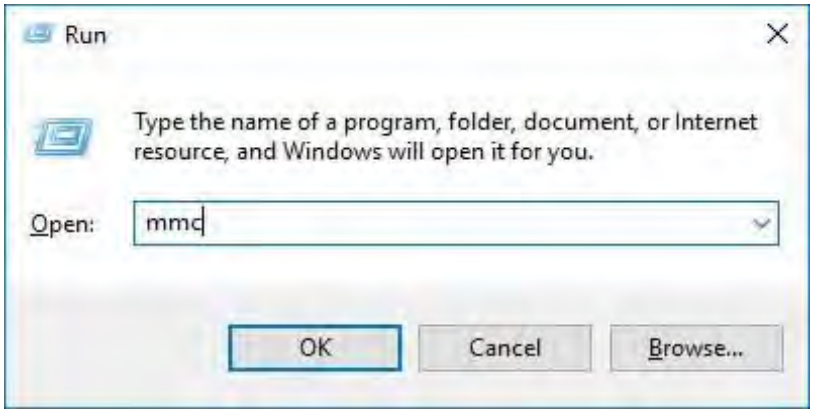
Vous devez être un administrateur de domaine ou un administrateur disposant d'un accès en écriture à Active Directory pour installer une autorité de certification racine d'entreprise.

Microsoft fournit une documentation complète pour les systèmes d'exploitation Windows Server, qui comprend des modèles pour les certificats de serveur, l'installation de l'autorité de certification et le déploiement de certificats, qui se trouve dans la présentation du déploiement de certificats de serveur de Microsoft.

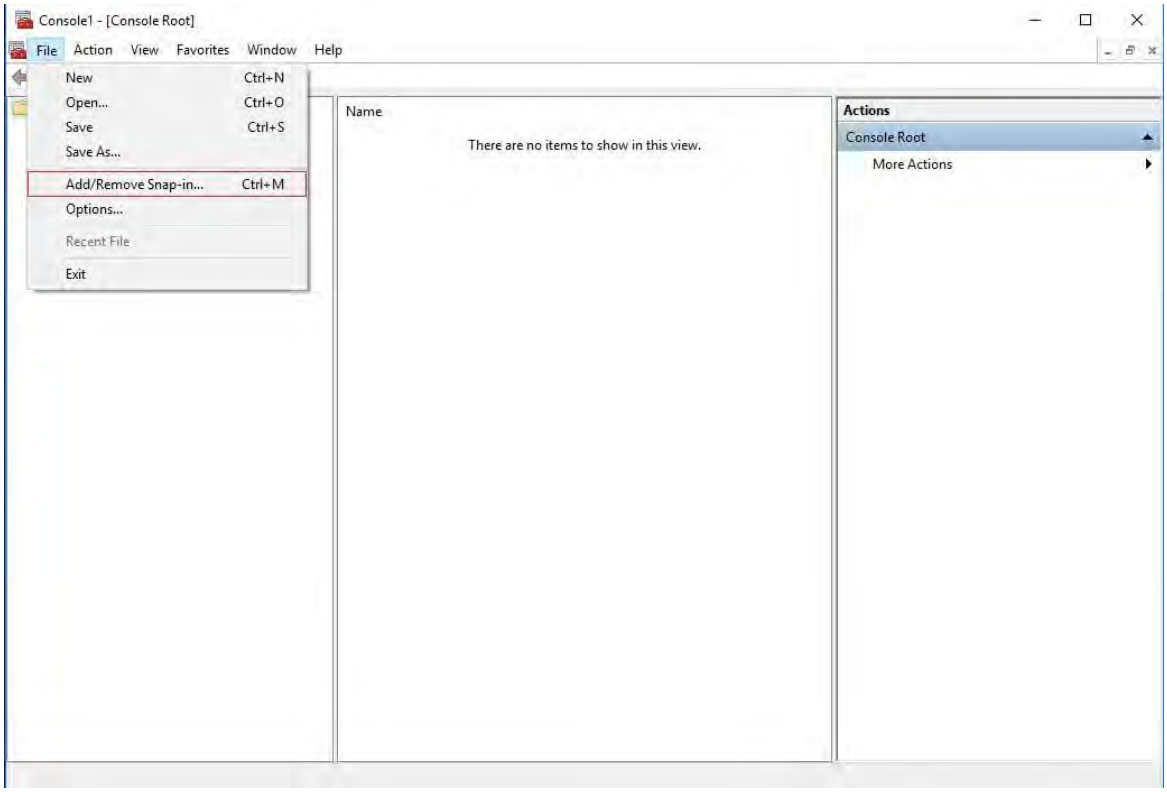
Ajouter un certificat d'autorité de certification au serveur

Ajoutez le certificat de l'autorité de certification au serveur en procédant comme suit.

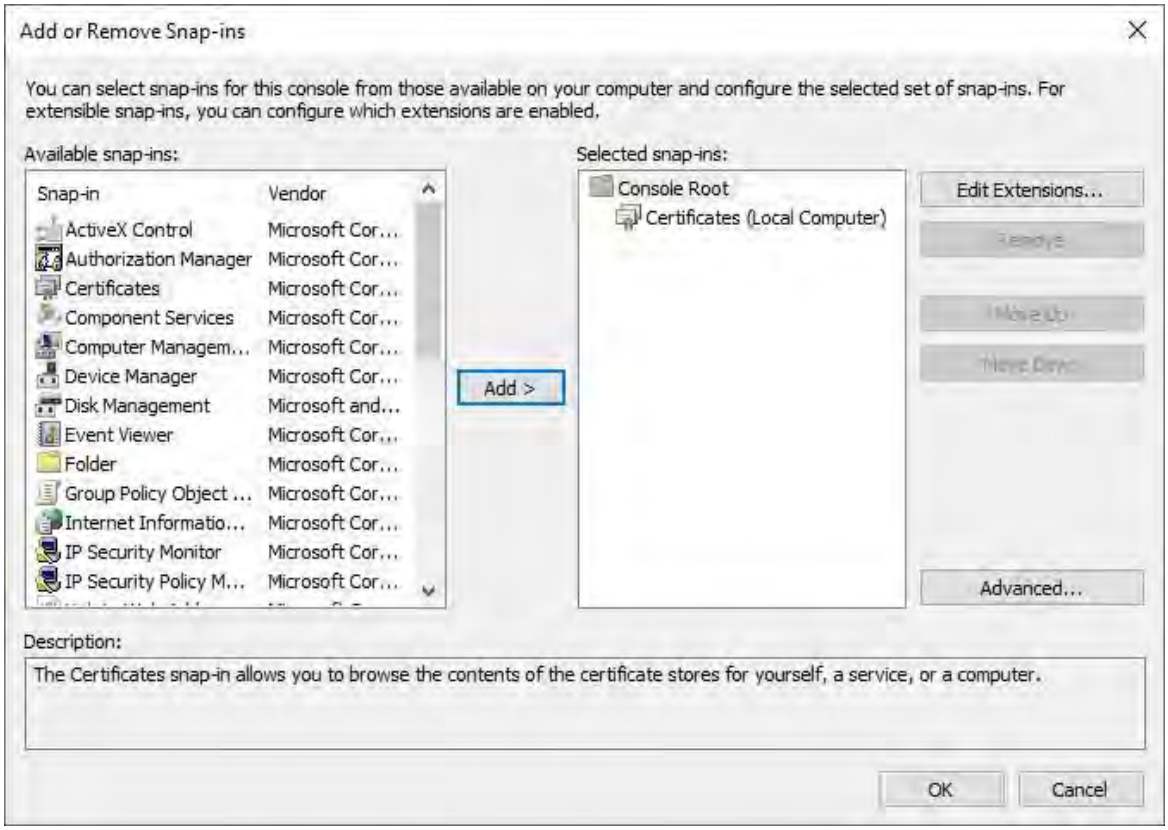
1. Sur l'ordinateur qui héberge le serveur MOBOTIX HUB, ouvrez la console de gestion Microsoft.



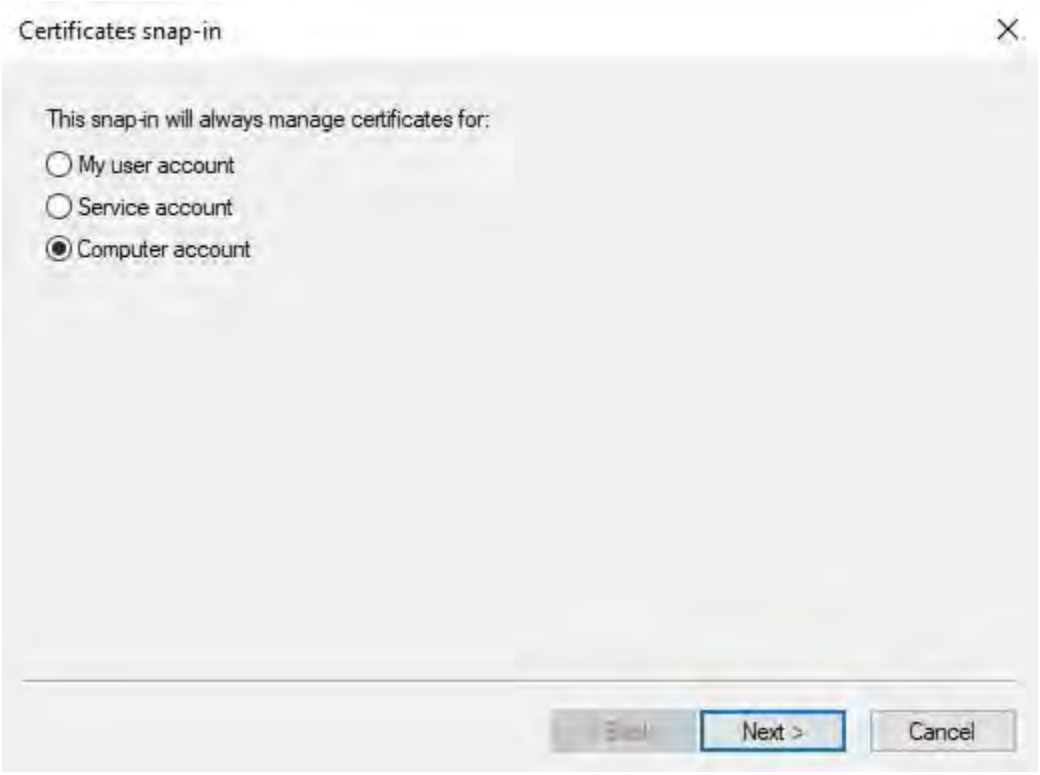
2. Dans Microsoft Management Console, dans le menu Fichier, sélectionnez **Ajouter/Supprimer un composant logiciel enfichable...**.



3. Sélectionnez le composant logiciel enfichable Certificats et cliquez sur **Ajouter**

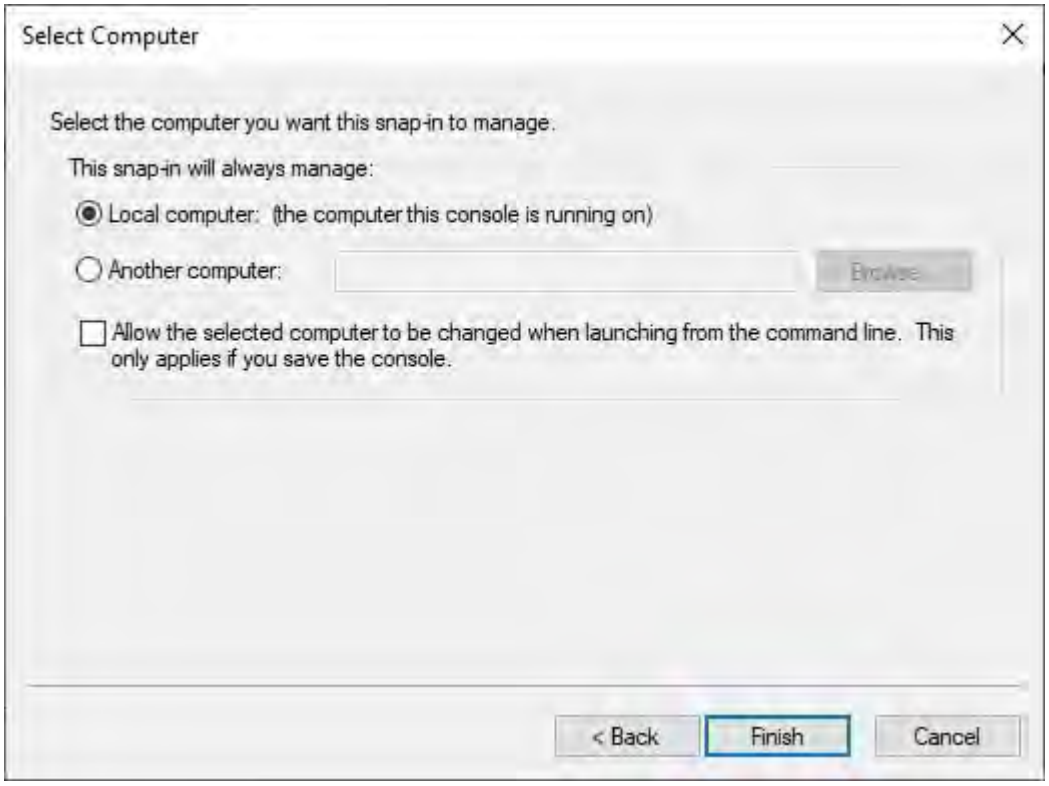


4. Dans **le composant logiciel enfichable Certificats**, sélectionnez **Compte d'ordinateur**.

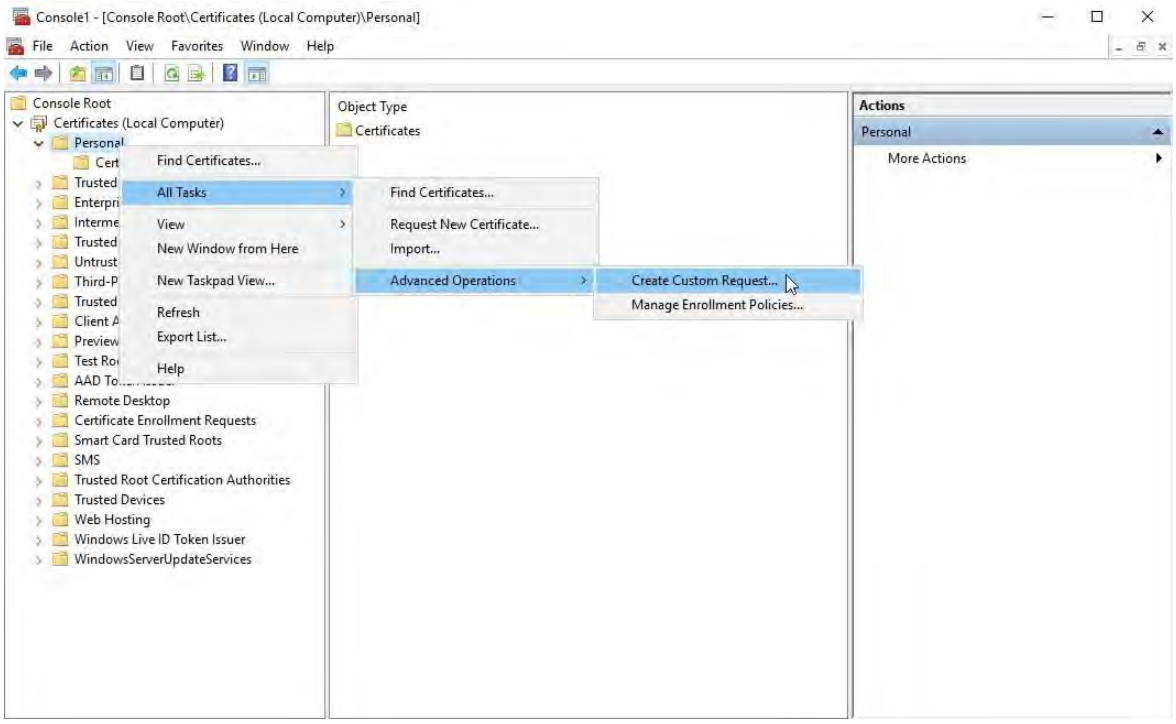


5. Dans **Sélectionner un ordinateur**, sélectionnez **Ordinateur local**.

   Sélectionnez **Terminer**, puis **OK.**



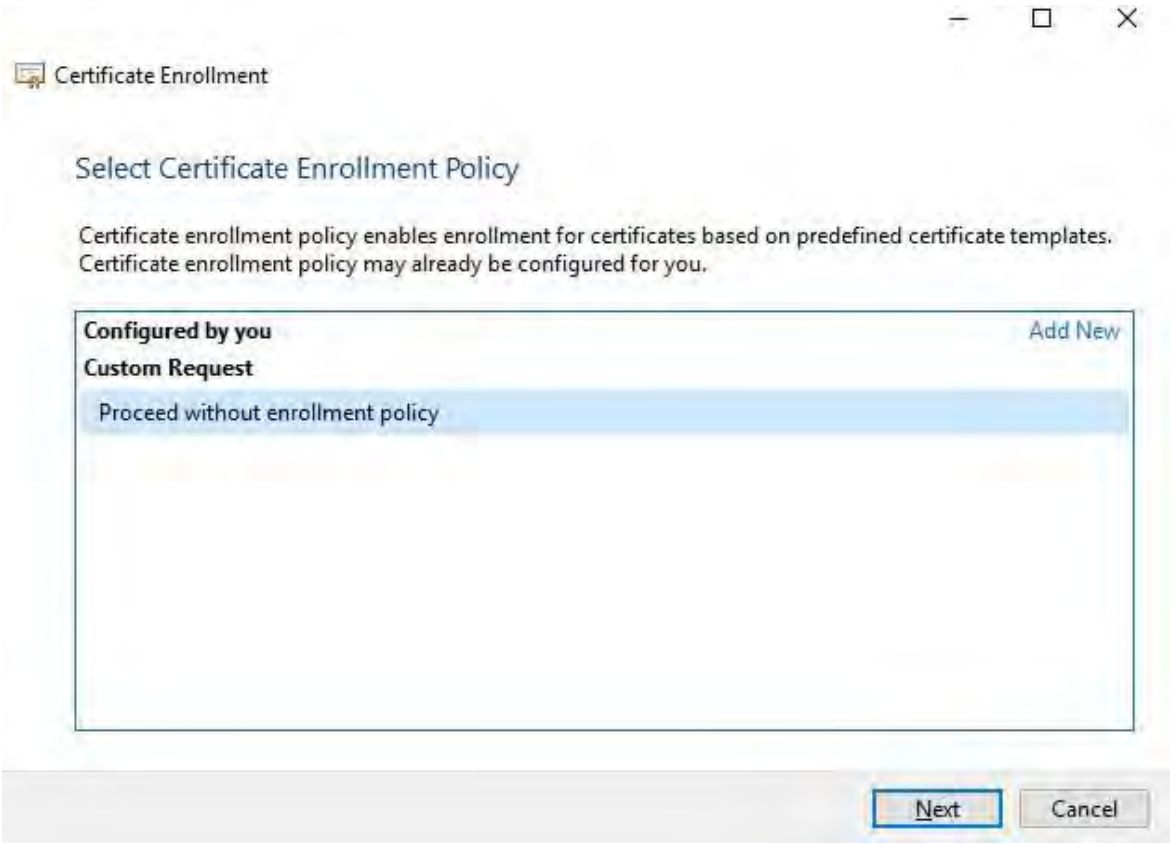
6. Développez l'objet Certificates. Cliquez avec le bouton droit de la souris sur le **dossier Personnel** et sélectionnez **Toutes les tâches** > **Opérations avancées** > **Créer une demande personnalisée**.



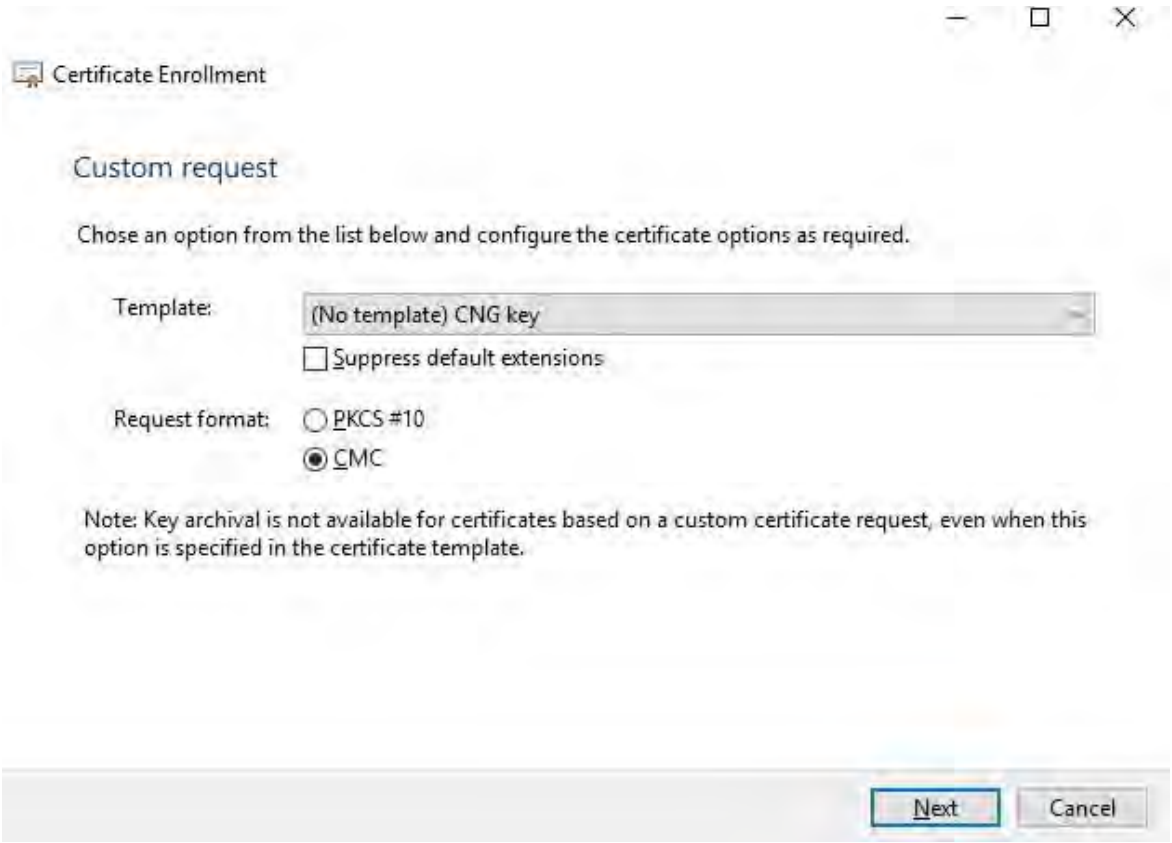
7. Cliquez sur **Suivant** dans l' Assistant **Inscription de certificat** et sélectionnez **Continuer sans stratégie d'inscription**.

   Si votre stratégie de groupe contient déjà une politique d'inscription de certificat, vous devez confirmer le reste de ce processus auprès de votre équipe d'administration de domaine avant de continuer.

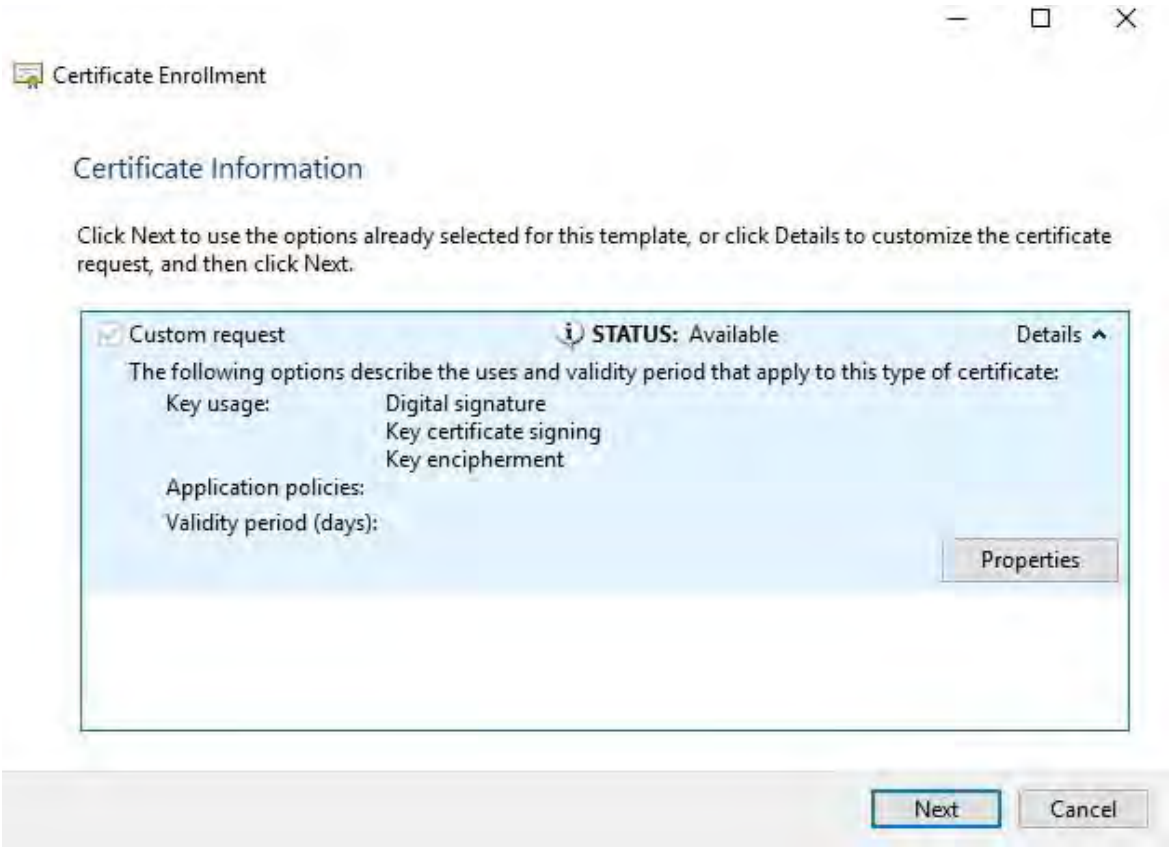
   Cliquez sur **Suivant**.



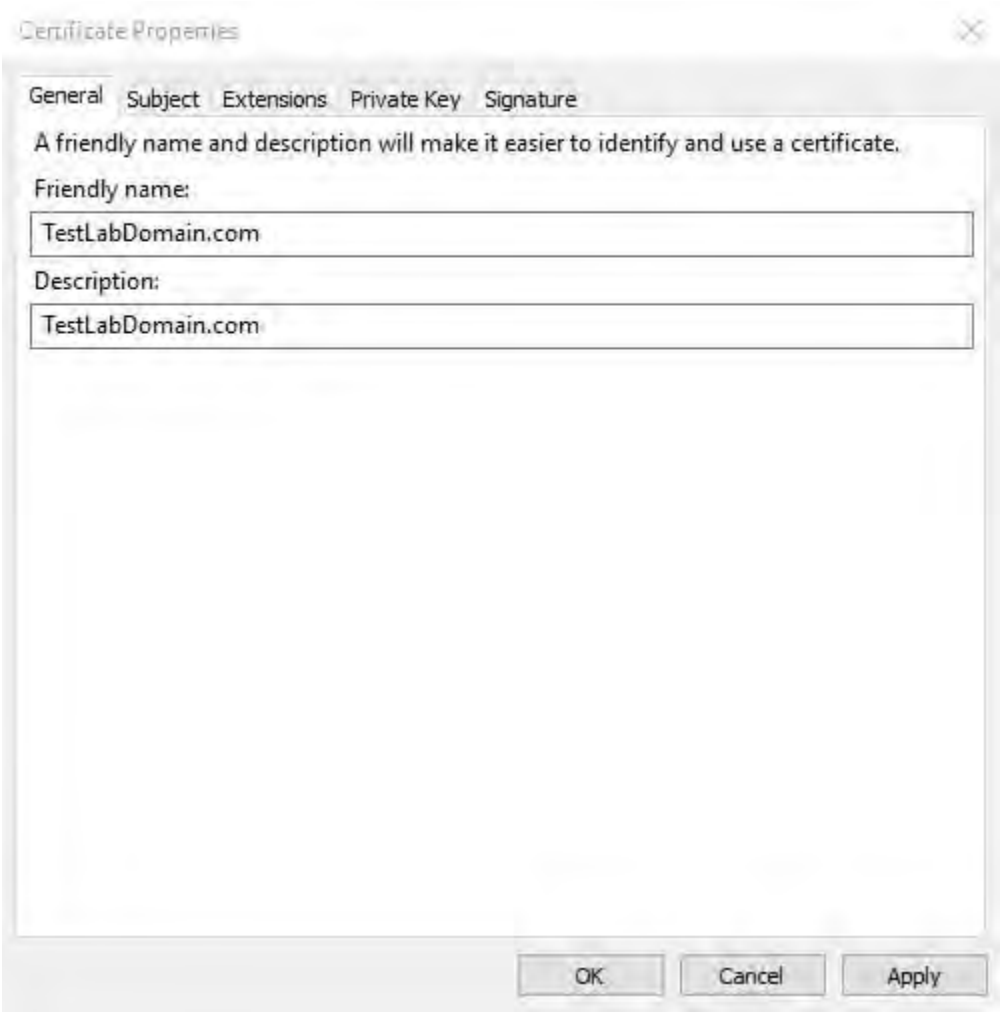
8. Sélectionnez le **modèle de clé CNG (sans modèle)** et le format de demande **CMC**, puis cliquez sur **Suivant**.



9. Développez le champ d'affichage des **détails** de la demande personnalisée, puis cliquez sur **Propriétés**.



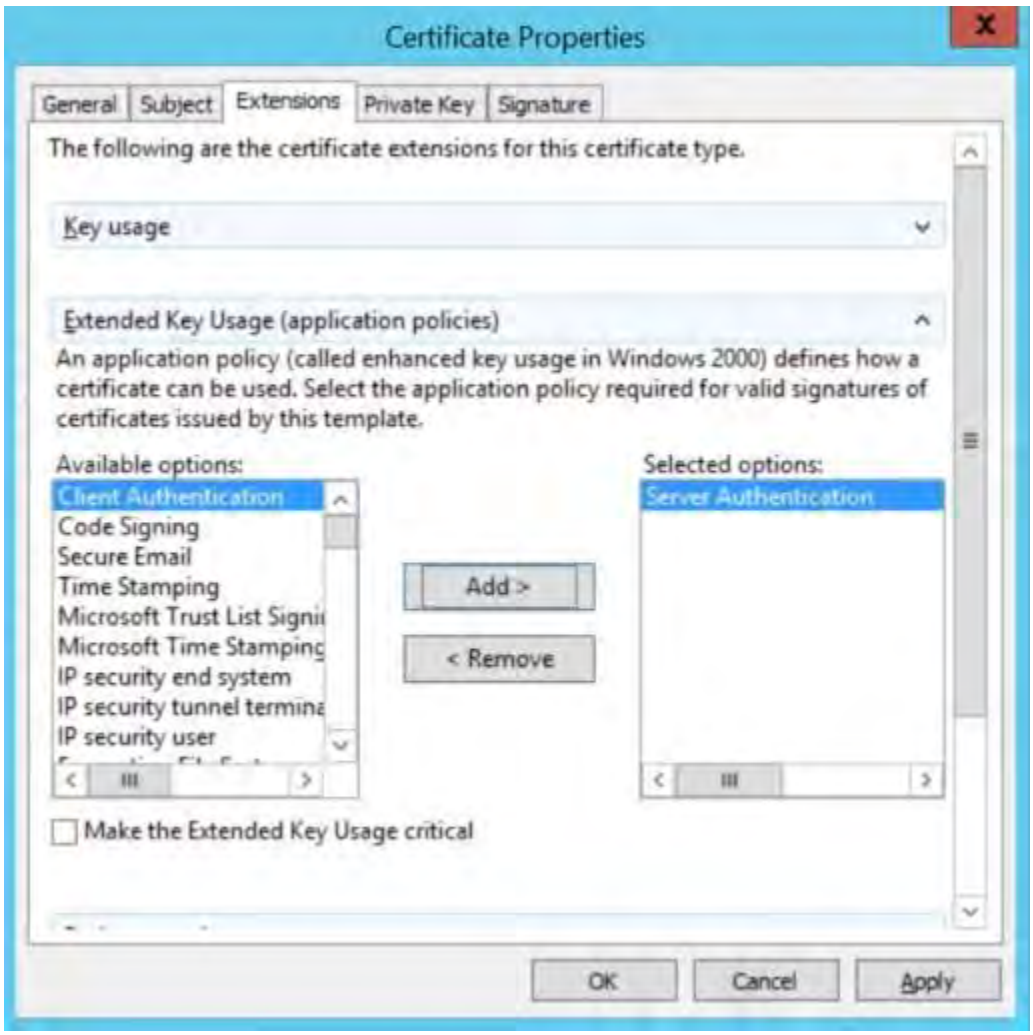
10. Sous l' **onglet Général**, renseignez les champs **Nom convivial** et **Description** avec le nom de domaine, le nom de l'ordinateur ou l'organisation.



11. Dans l' **onglet Objet**, entrez les paramètres requis pour le nom de l'objet.

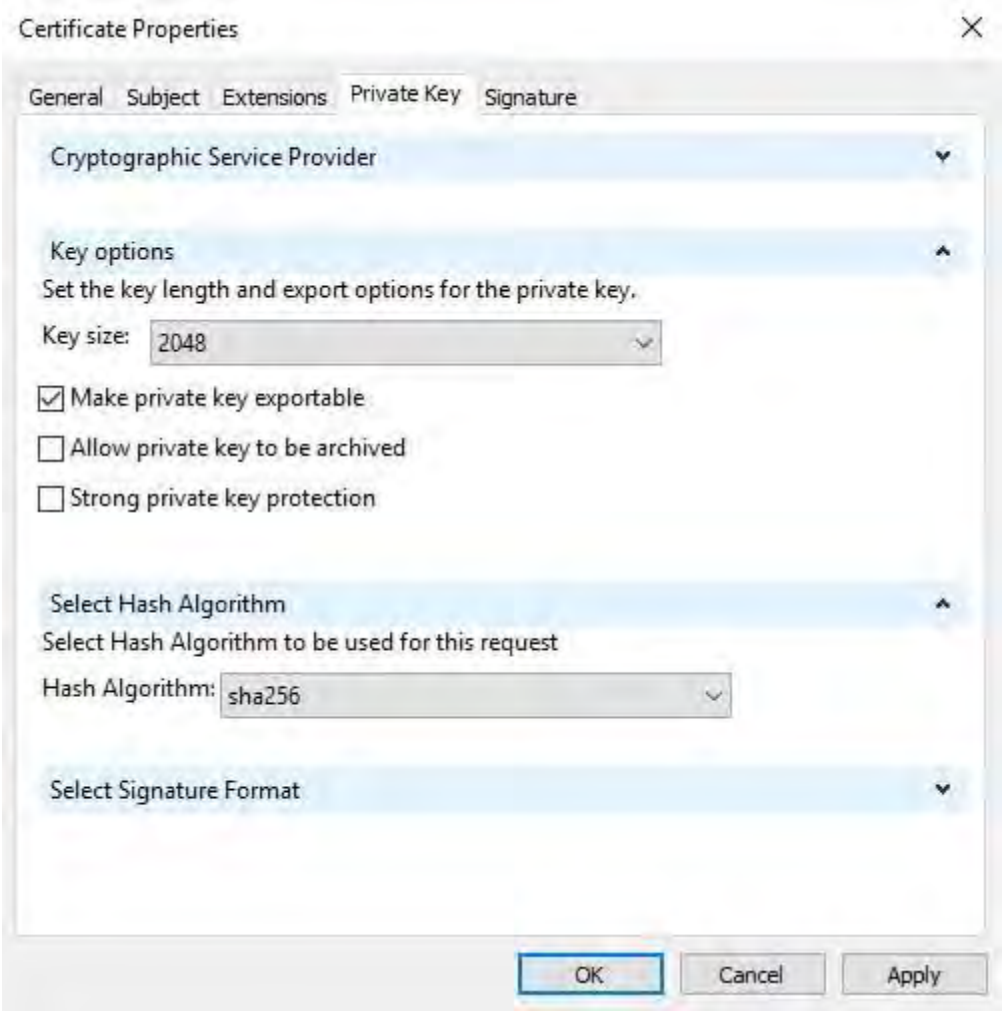
    Dans le champ **Nom d'objet Type**, entrez dans **Nom commun** le nom d'hôte de l'ordinateur sur lequel le certificat sera installé.

12. Dans l' **onglet Extensions**, développez le menu **Utilisation étendue des clés (stratégies d'application).** Ajoutez l'**authentification du serveur** dans la liste des options disponibles.



13. Sous l' **onglet Clé privée**, développez le menu Options de clé .

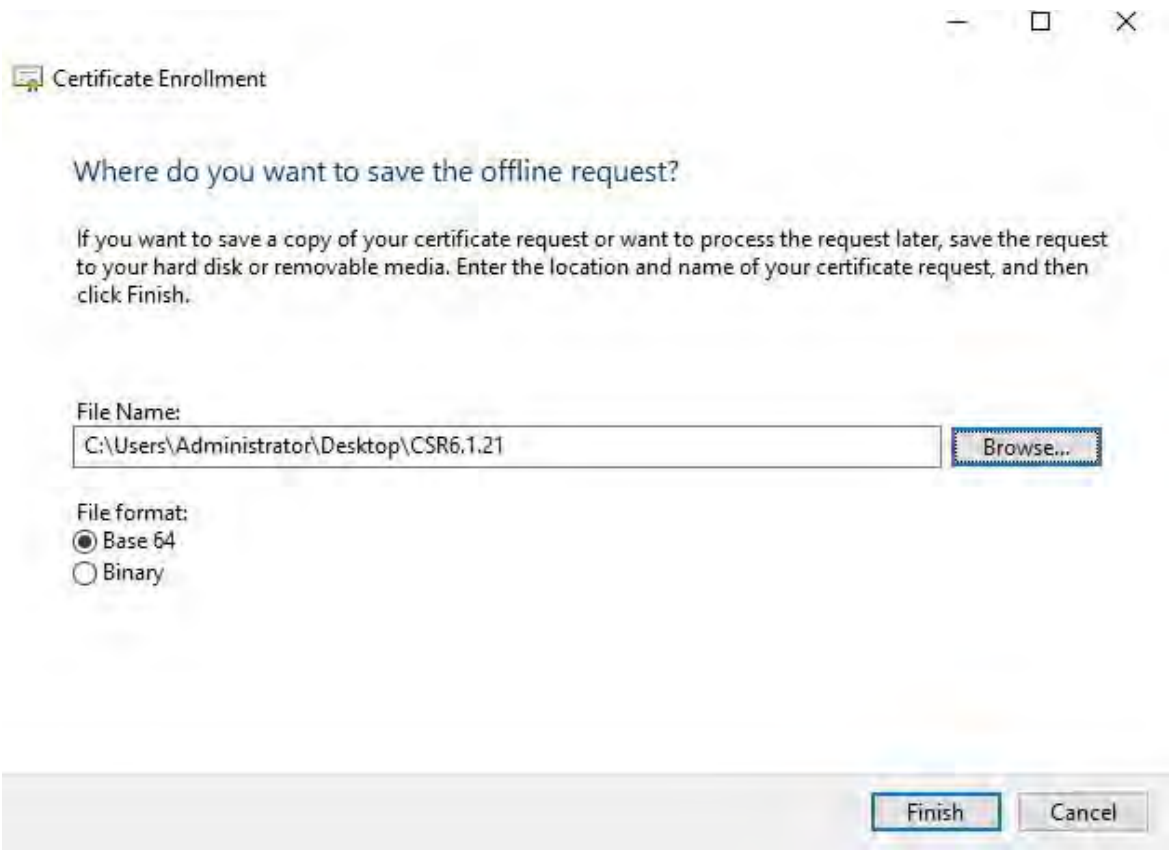
    Définissez la taille de la clé sur 2048 et sélectionnez l'option permettant d'exporter la clé privée. Cliquez sur **OK**.



14. Une fois que toutes les propriétés du certificat ont été définies, cliquez sur **Suivant** dans l' Assistant **Inscription de certificat**.

15. Sélectionnez un emplacement pour enregistrer la demande de certificat et un format. Naviguez jusqu'à cet emplacement et spécifiez un nom pour le fichier .req. Le format par défaut est la base 64.

16. Cliquez sur **Terminer**.



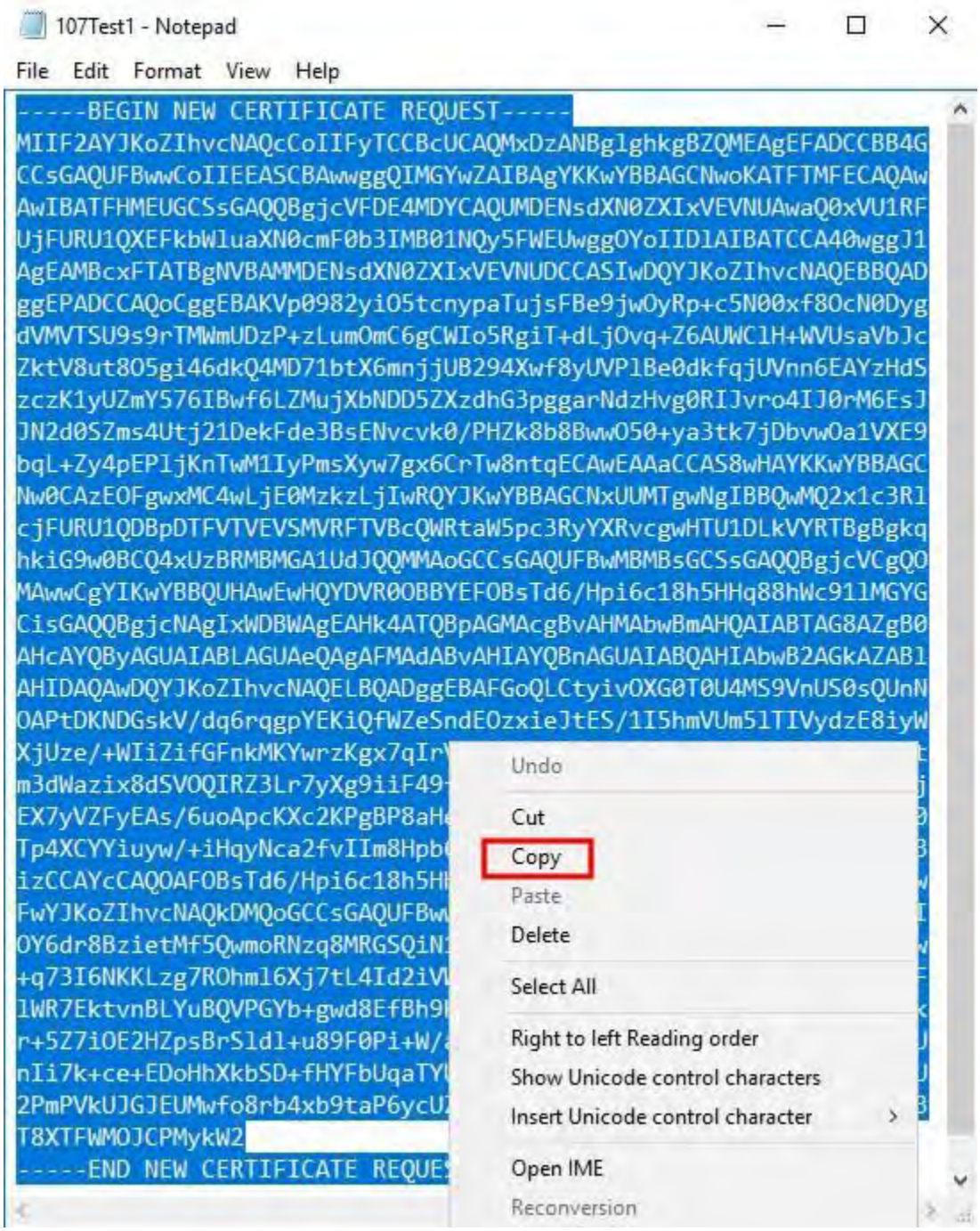
Un fichier .req est généré, que vous devez utiliser pour demander un certificat signé.

Téléchargez le fichier .req pour recevoir un certificat signé en retour

Vous devez copier l'intégralité du texte du fichier .req, y compris les lignes de début et de fin, et coller le texte dans l' autorité de certification interne des services de certificats Active Directory au sein du réseau. Voir Installer les services de certificats Active Directory à la page 74.

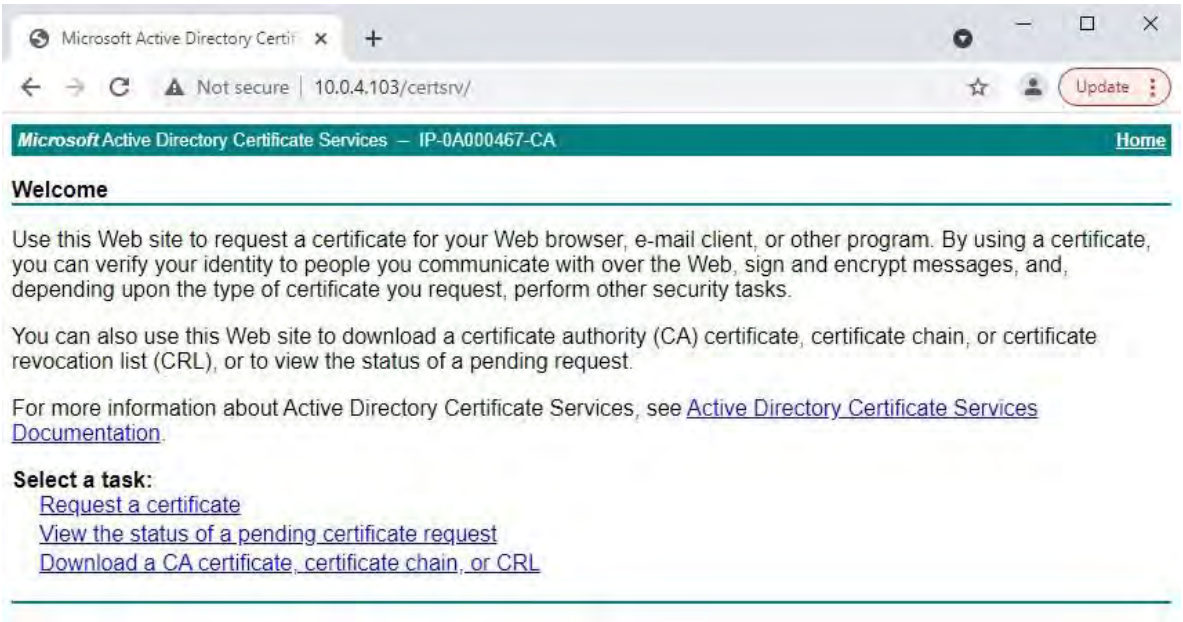
À moins que votre domaine n'ait récemment installé les services de certificats Active Directory ou qu'il n' ait été installé uniquement à cet effet, vous devrez soumettre cette demande en suivant une procédure distincte configurée par votre équipe d'administration de domaine. Veuillez confirmer ce processus avec eux avant de continuer.

1. Naviguez jusqu'à l'emplacement du fichier .req et ouvrez-le dans le Bloc-notes.



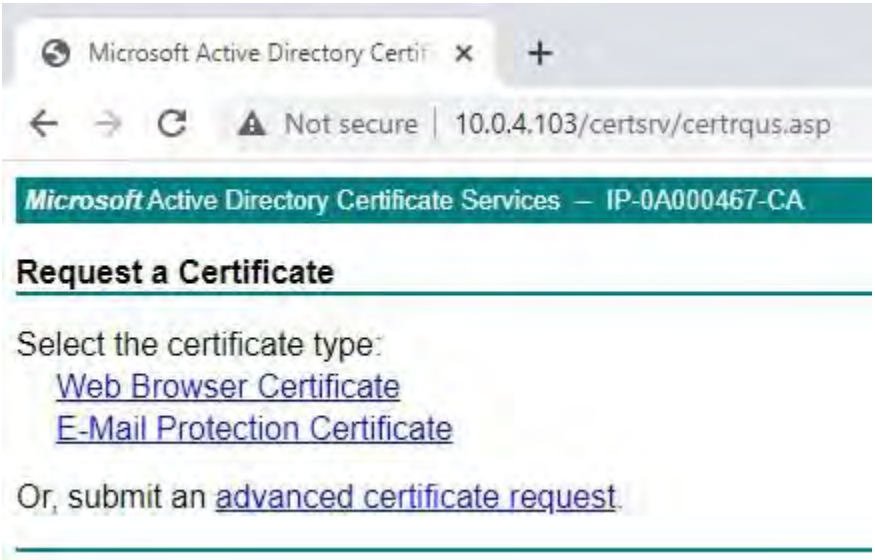
2. Copiez l'intégralité du contenu du fichier. Cela inclut les lignes pointillées marquant le début et la fin de la demande de certificat.

3. Ouvrez un navigateur Web et entrez l'adresse de l'autorité de certification de domaine.



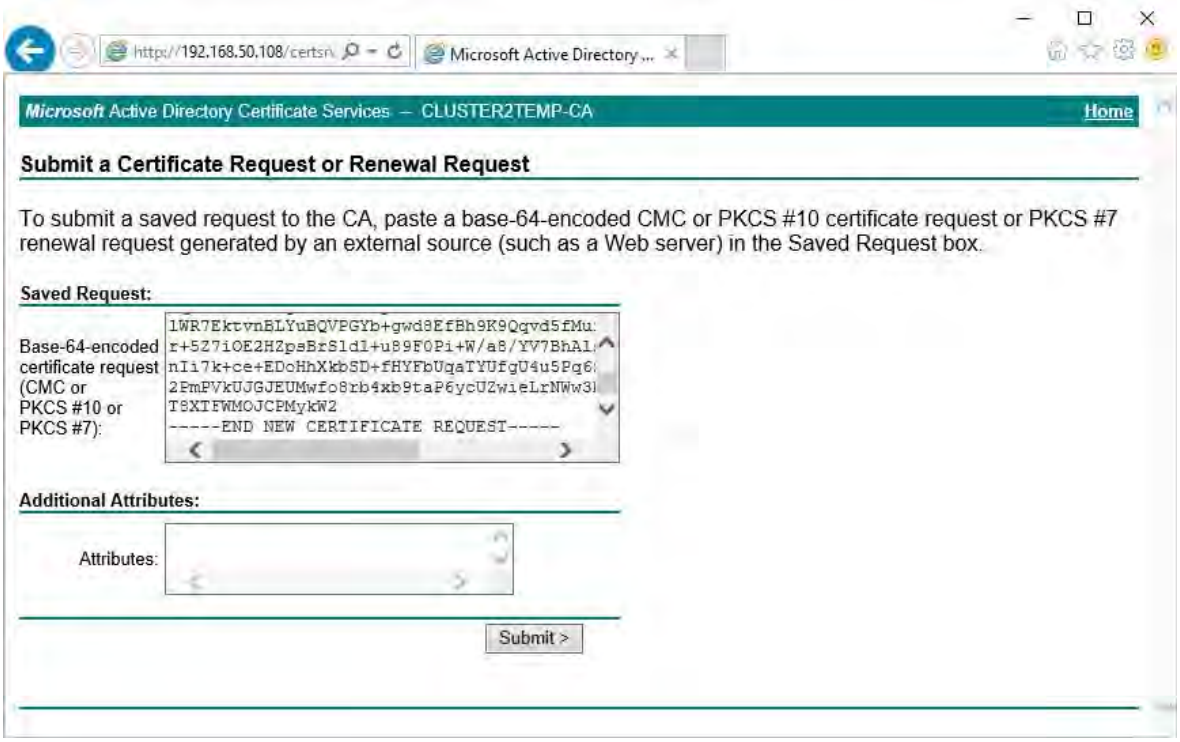
4. Cliquez sur le **lien Demander un certificat**.

5. Cliquez sur le lien de demande de **certificat avancé** .



6. Collez le contenu du fichier .req dans le formulaire. S'il est nécessaire de sélectionner un modèle de certificat, sélectionnez

   Serveur Web dans la liste Modèle de certificat.



7. Cliquez sur **Soumettre**.

   Le site affiche un message indiquant que le certificat sera émis dans quelques jours.

Votre équipe d'administration de domaine distribuera et installera probablement le certificat pour vous. Toutefois, si le certificat vous est livré, vous pouvez l'installer manuellement.

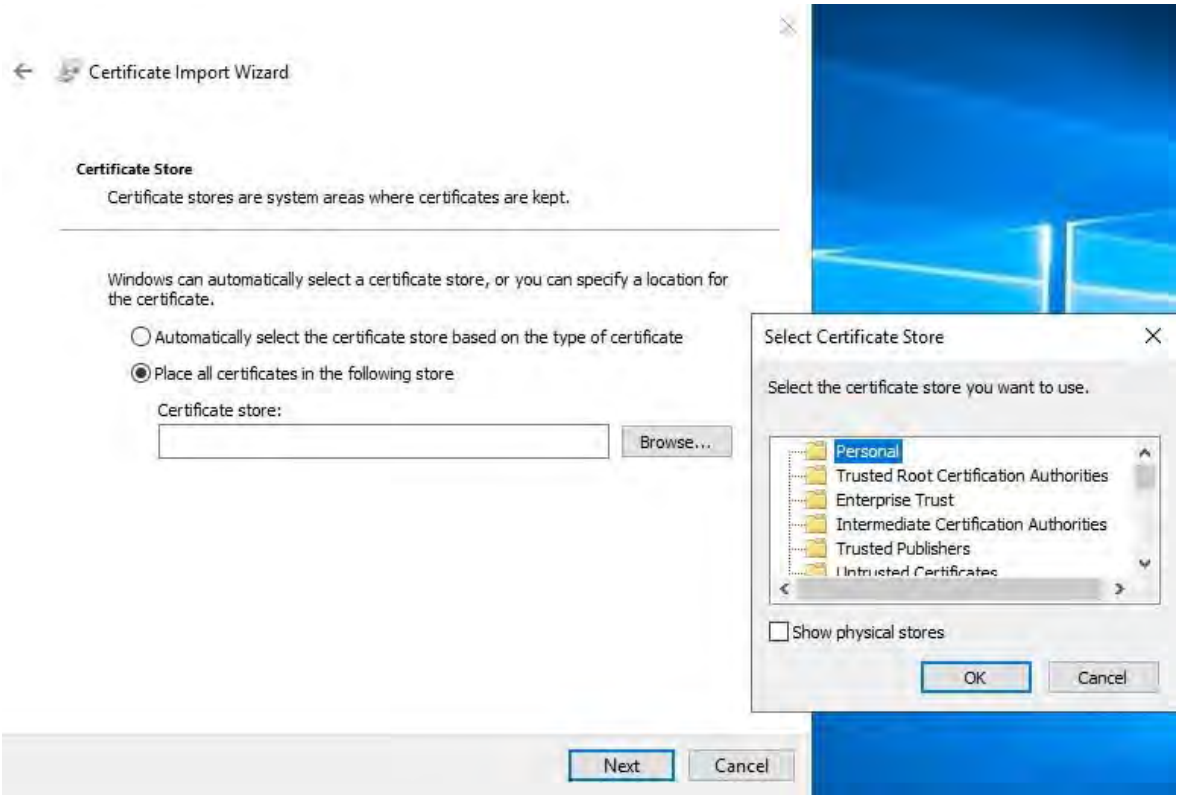
Installer le certificat manuellement

Si le certificat vous est remis, vous pouvez l'installer manuellement.

1. Recherchez le fichier de certificat sur l'ordinateur qui héberge le Serveur de gestion ou le Serveur d'enregistrement.
2. Cliquez avec le bouton droit sur le certificat et sélectionnez Installer le **certificat**.
3. Acceptez l'avertissement de sécurité s'il apparaît.

   Sélectionnez cette option pour installer le certificat de l'utilisateur actuel et cliquez sur **Suivant**.

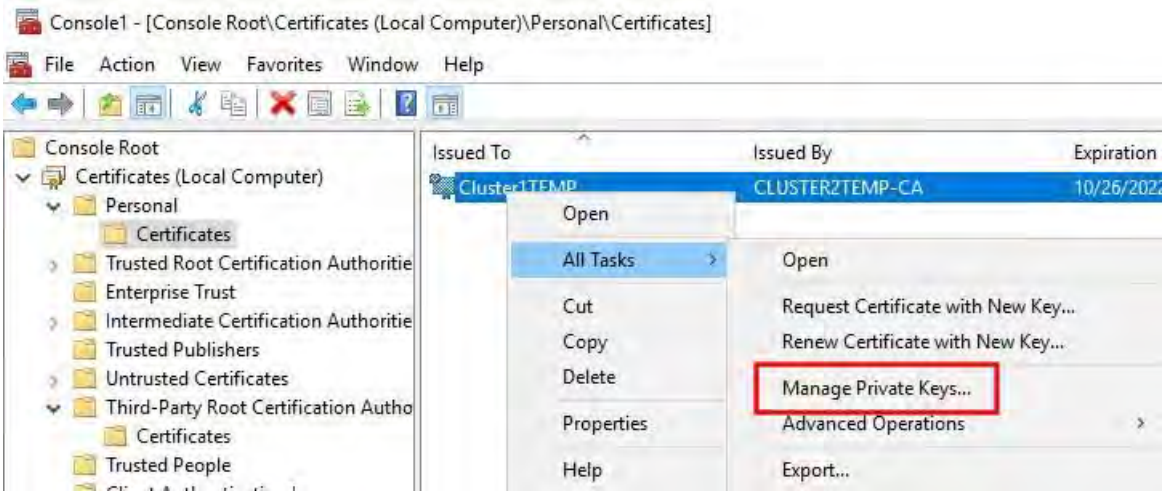
4. Choisissez un emplacement de stockage, accédez au magasin de certificats personnel, puis cliquez sur **Suivant**.



5. Terminez l' assistant **d'installation du certificat**.

6. Accédez au composant logiciel enfichable Certificats Microsoft Management Console (MMC).

7. Dans la console, accédez au magasin personnel où le certificat est installé. Cliquez avec le bouton droit de la souris sur le certificat et sélectionnez **Toutes les tâches** > **Gérer les clés privées**.



8. Vérifiez que le compte qui exécute le logiciel MOBOTIX HUB Management Server, Recording Server ou Mobile Server figure dans la liste des utilisateurs autorisés à utiliser le certificat.

   Assurez-vous que l'utilisateur dispose des autorisations Contrôle total et Lecture activées.

   > Par défaut, le logiciel MOBOTIX HUB utilise le compte NETWORK SERVICE. Dans un environnement de domaine, les comptes de service sont couramment utilisés pour installer et exécuter les services MOBOTIX HUB . Vous devrez en discuter avec votre équipe d'administration de domaine et faire ajouter les autorisations appropriées aux comptes de service s'ils n'ont pas déjà été configurés correctement. Confirmez-le avant de continuer.

Activer le chiffrement du serveur pour les serveurs de gestion et les serveurs d'enregistrement

Une fois le certificat installé avec les propriétés et les autorisations appropriées, procédez comme suit.

1. Sur un ordinateur sur lequel un serveur de gestion ou un serveur d'enregistrement est installé, ouvrez le **configurateur de serveur**

   De:

   - Le menu Démarrer de Windows

   ou

   - Le gestionnaire de serveur, en cliquant avec le bouton droit de la souris sur l'icône du gestionnaire de serveur dans la barre des tâches de l'ordinateur

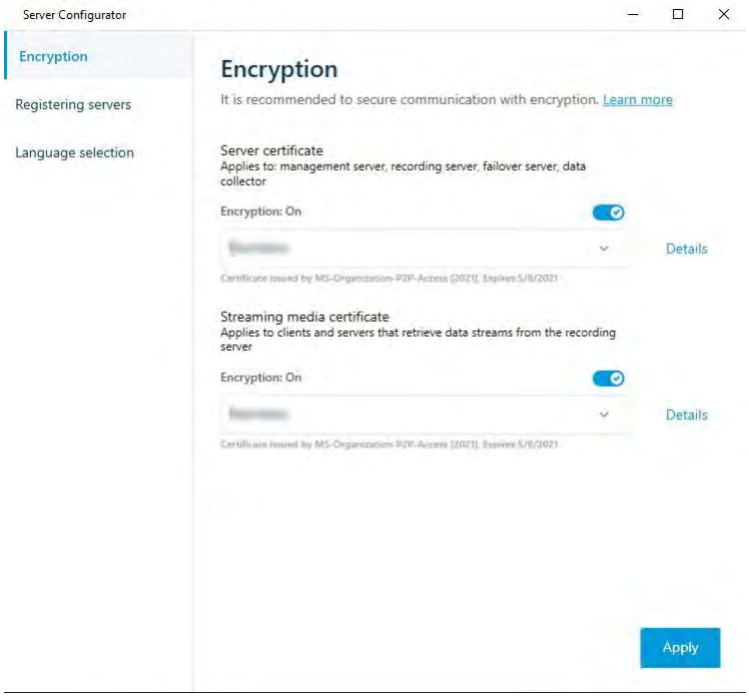
2. Dans le **configurateur de serveur**, sous **Certificat de serveur**, activez **le cryptage**.

3. Cliquez sur **Sélectionner un certificat** pour ouvrir une liste avec les noms d'objet uniques des certificats qui ont une clé privée et qui sont installés sur l'ordinateur local dans le magasin de certificats Windows.

4. Sélectionnez un certificat pour chiffrer la communication entre le serveur d'enregistrement, le serveur de gestion, le serveur de basculement et le serveur de collecte de données.

   Sélectionnez **Détails** pour afficher les informations du Magasin de certificats Windows concernant le certificat sélectionné.

   L'utilisateur du service Recording Server a accès à la clé privée. Il est nécessaire que ce certificat soit approuvé sur tous les clients.



5. Cliquez sur **Appliquer**.

> Lorsque vous appliquez des certificats, le serveur d'enregistrement est arrêté et redémarré. L'arrêt du service de serveur d'enregistrement signifie que vous ne pouvez pas enregistrer et visionner des vidéos en direct pendant que vous vérifiez ou modifiez la configuration de base du serveur d'enregistrement.

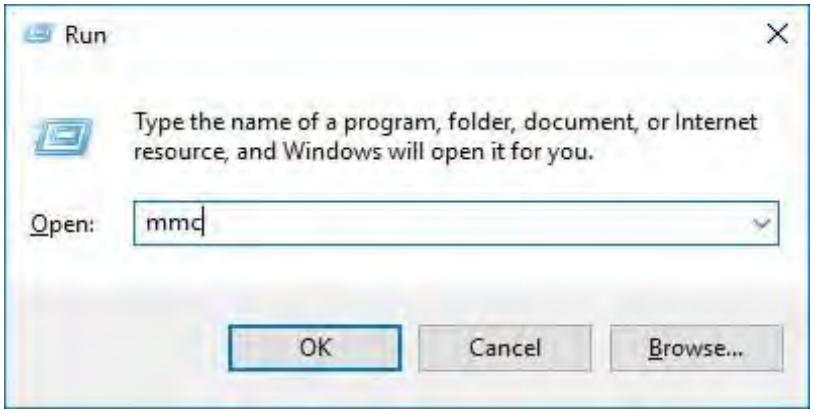
Installer des certificats dans un environnement de groupe de travail pour la communication avec le serveur de gestion ou le serveur d'enregistrement

Lorsque vous utilisez un environnement de groupe de travail, il est supposé qu'il n'existe pas d'infrastructure d'autorité de certification. Pour distribuer des certificats, il est nécessaire de créer une infrastructure d'autorité de certification. Il est également nécessaire de distribuer les clés de certificat aux postes de travail clients. À l'exception de ces exigences, le processus de demande et d'installation d'un certificat sur un serveur est similaire à celui des scénarios de domaine et d'autorité de certification commerciale.

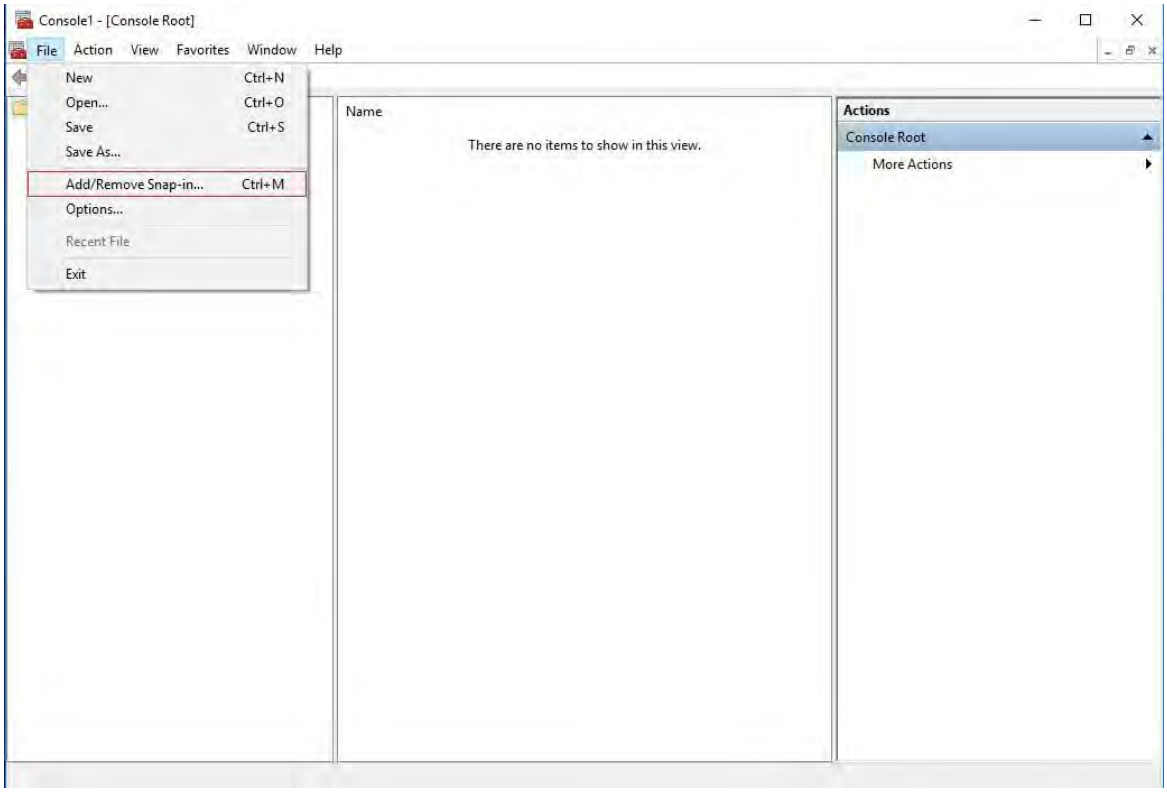
Ajouter un certificat d'autorité de certification au serveur

Ajoutez le certificat de l'autorité de certification au serveur en procédant comme suit.

1. Sur l'ordinateur qui héberge le serveur MOBOTIX HUB, ouvrez la console de gestion Microsoft.

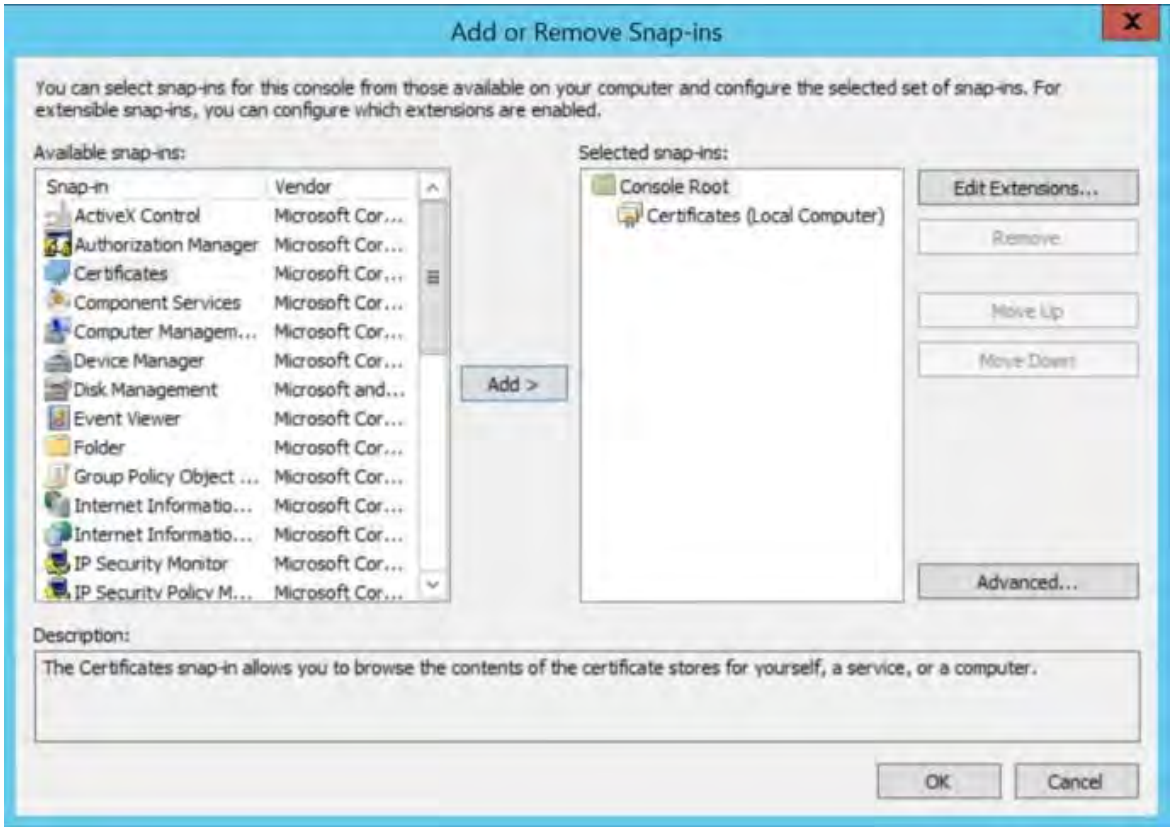


2. Dans Microsoft Management Console, dans le menu Fichier, sélectionnez **Ajouter/Supprimer un composant logiciel enfichable...**.

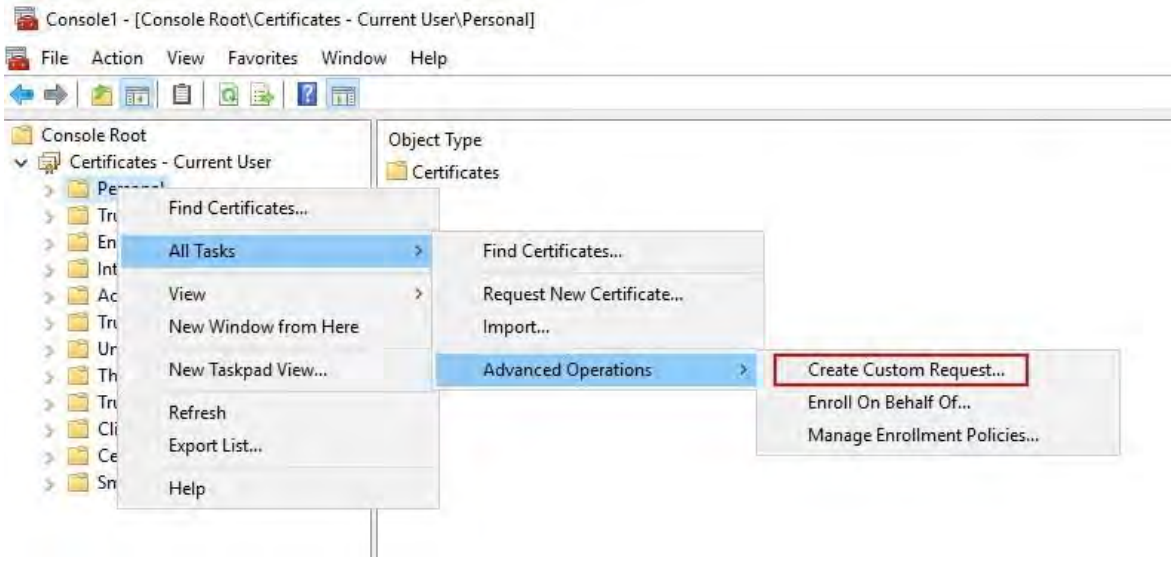


3. Sélectionnez le composant logiciel enfichable Certificats et cliquez sur **Ajouter**.

   Cliquez sur **OK**.

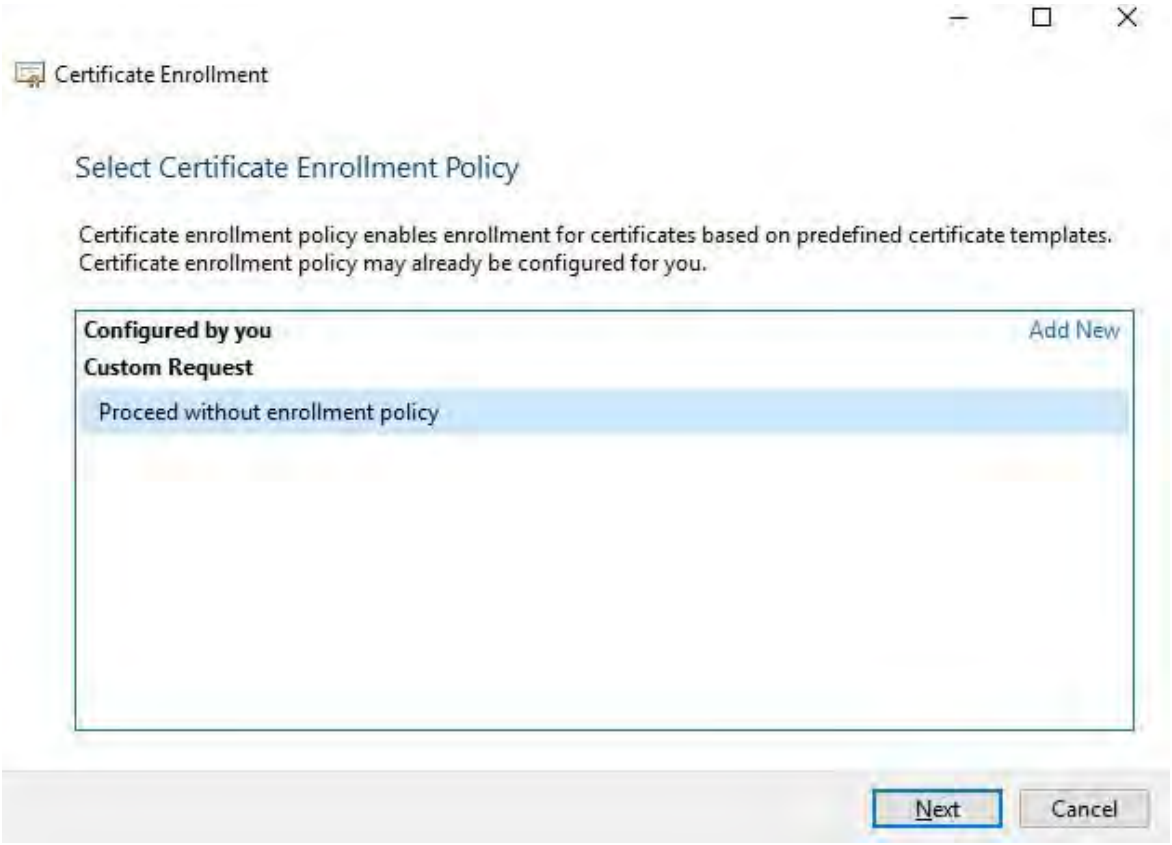


4. Développez l'objet Certificates. Cliquez avec le bouton droit de la souris sur le **dossier Personnel** et sélectionnez **Toutes les tâches** > **Opérations avancées** > **Créer une demande personnalisée**.

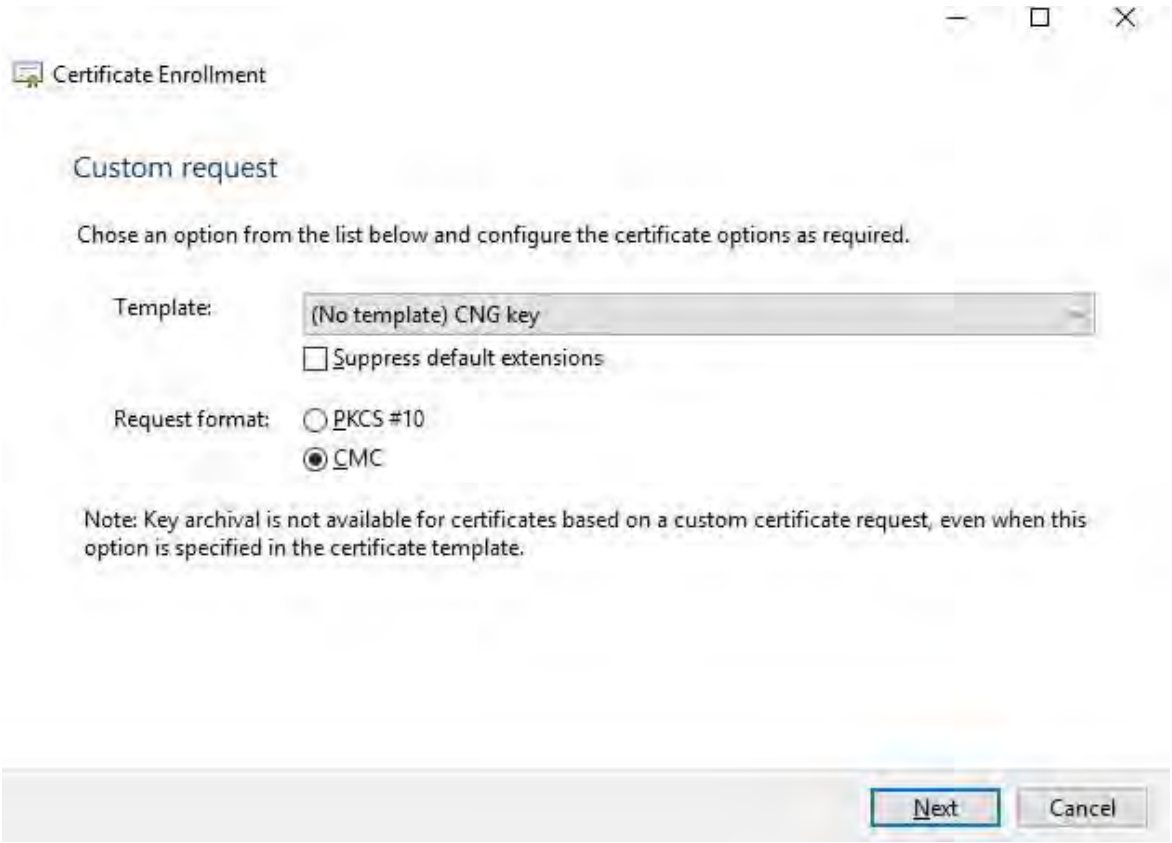


5. Cliquez sur **Suivant** dans l' Assistant **Inscription de certificat** et sélectionnez **Continuer sans stratégie d'inscription**.

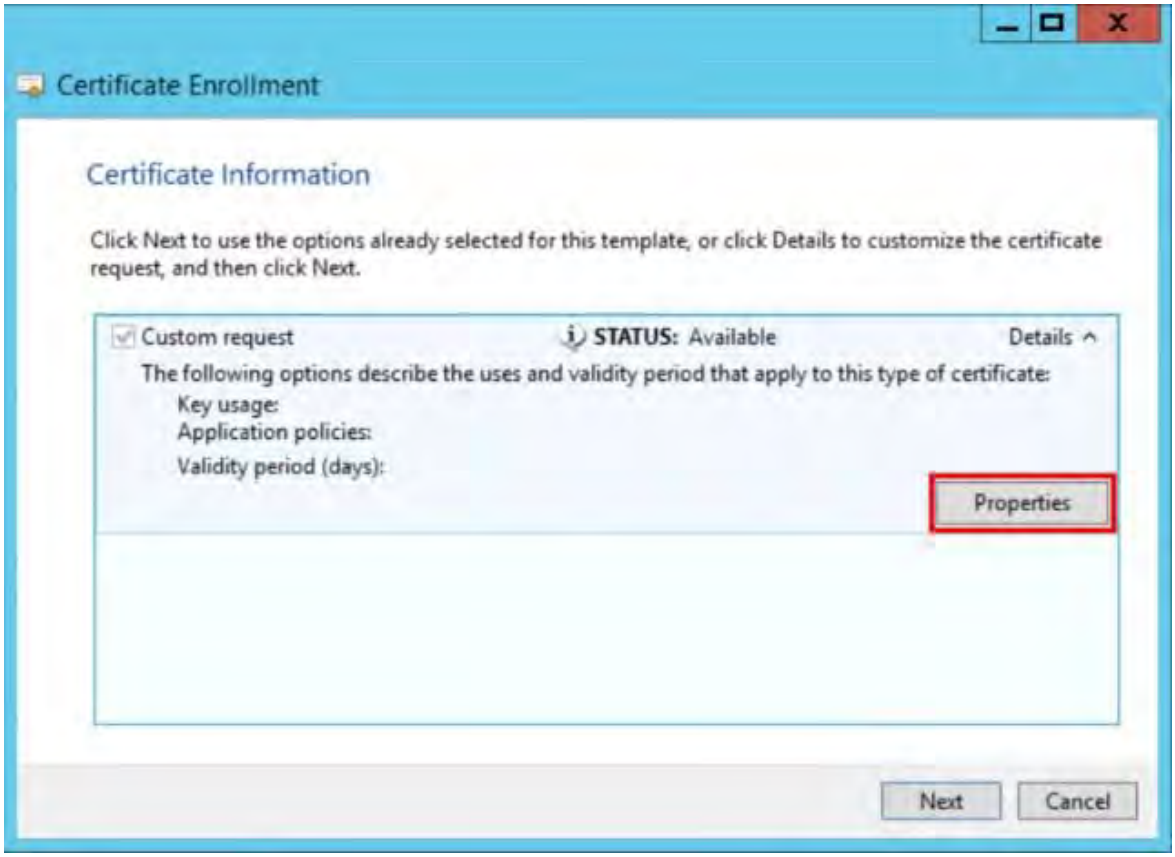
   Cliquez sur **Suivant**.



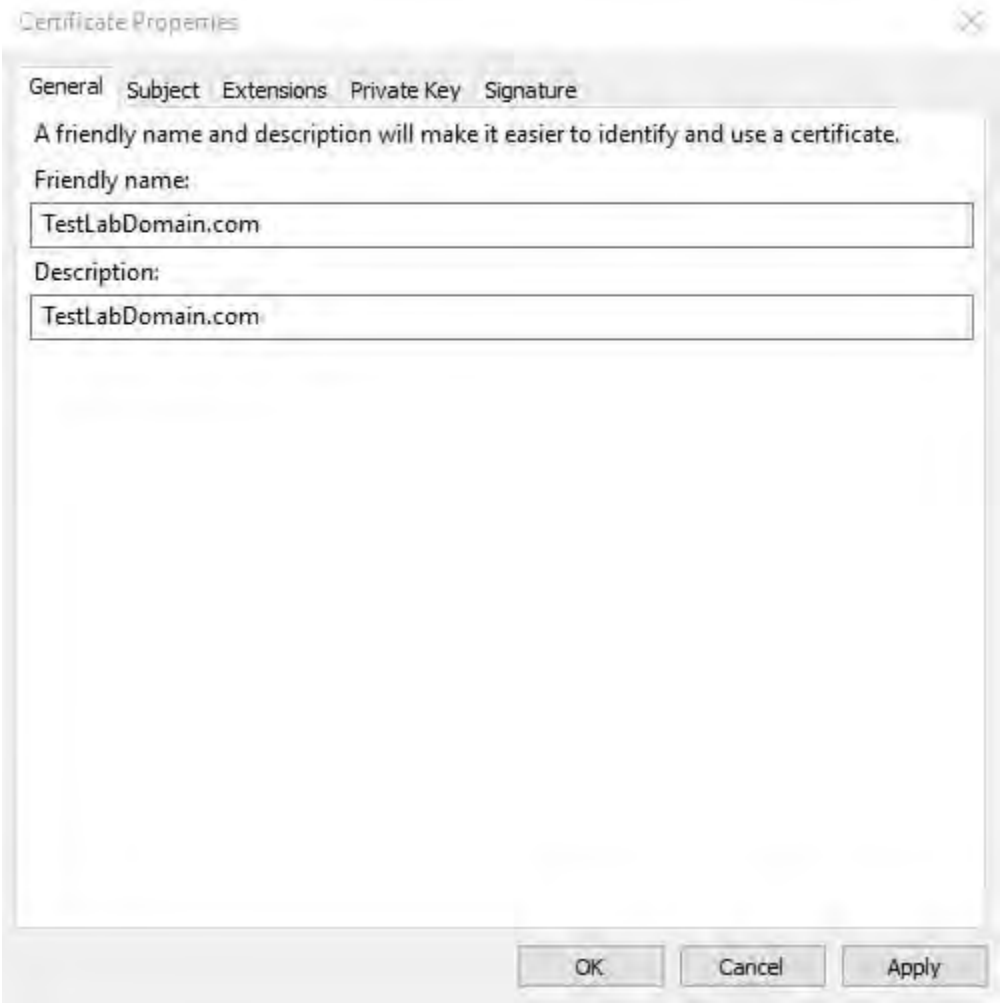
6. Sélectionnez le **modèle de clé CNG (sans modèle)** et le format de demande **CMC**, puis cliquez sur **Suivant**.



7. Développez le champ d'affichage des **détails** de la demande personnalisée, puis cliquez sur **Propriétés**.



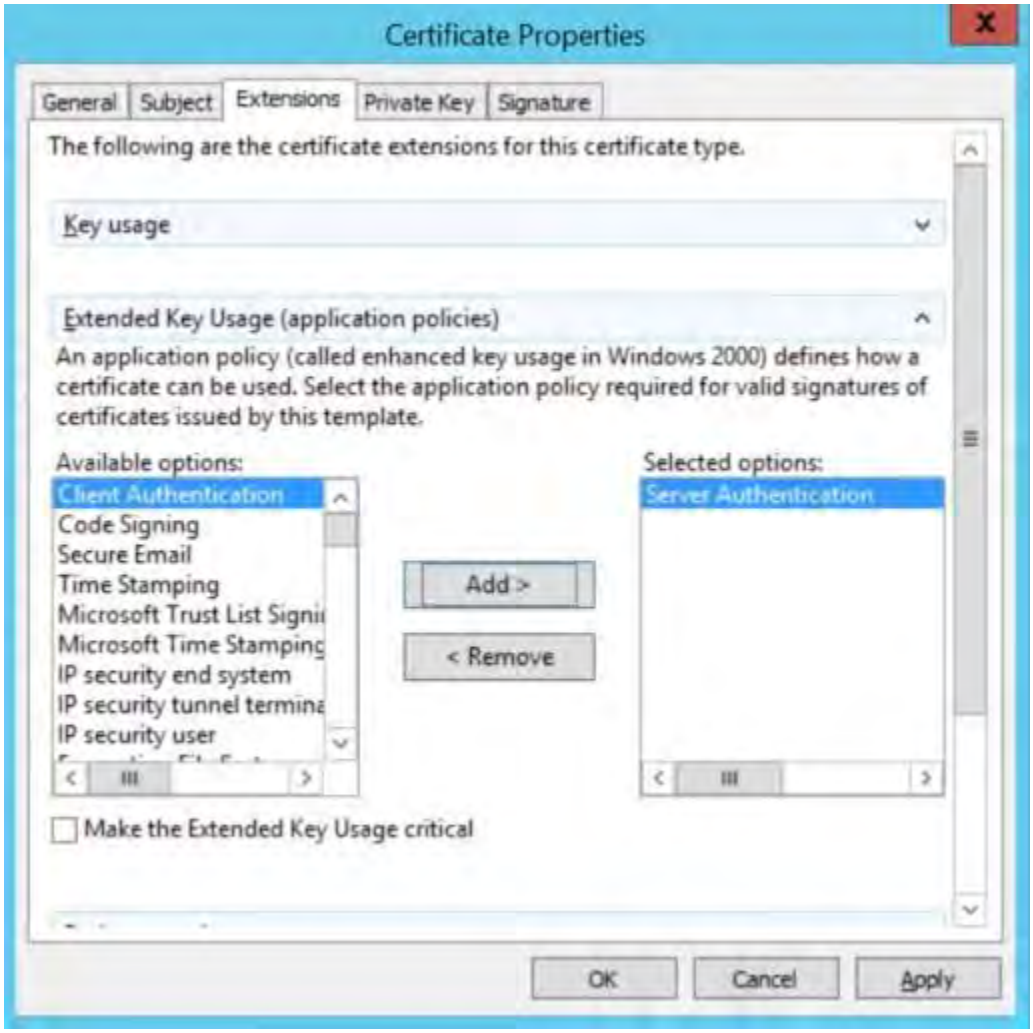
8. Sous l' **onglet Général**, renseignez les champs **Nom convivial** et **Description** avec le nom de domaine, le nom de l'ordinateur ou l'organisation.



9. Dans l' **onglet Objet**, entrez les paramètres requis pour le nom de l'objet.

   Dans le champ **Nom d'objet Type**, entrez dans **Nom commun** le nom d'hôte de l'ordinateur sur lequel le certificat sera installé.

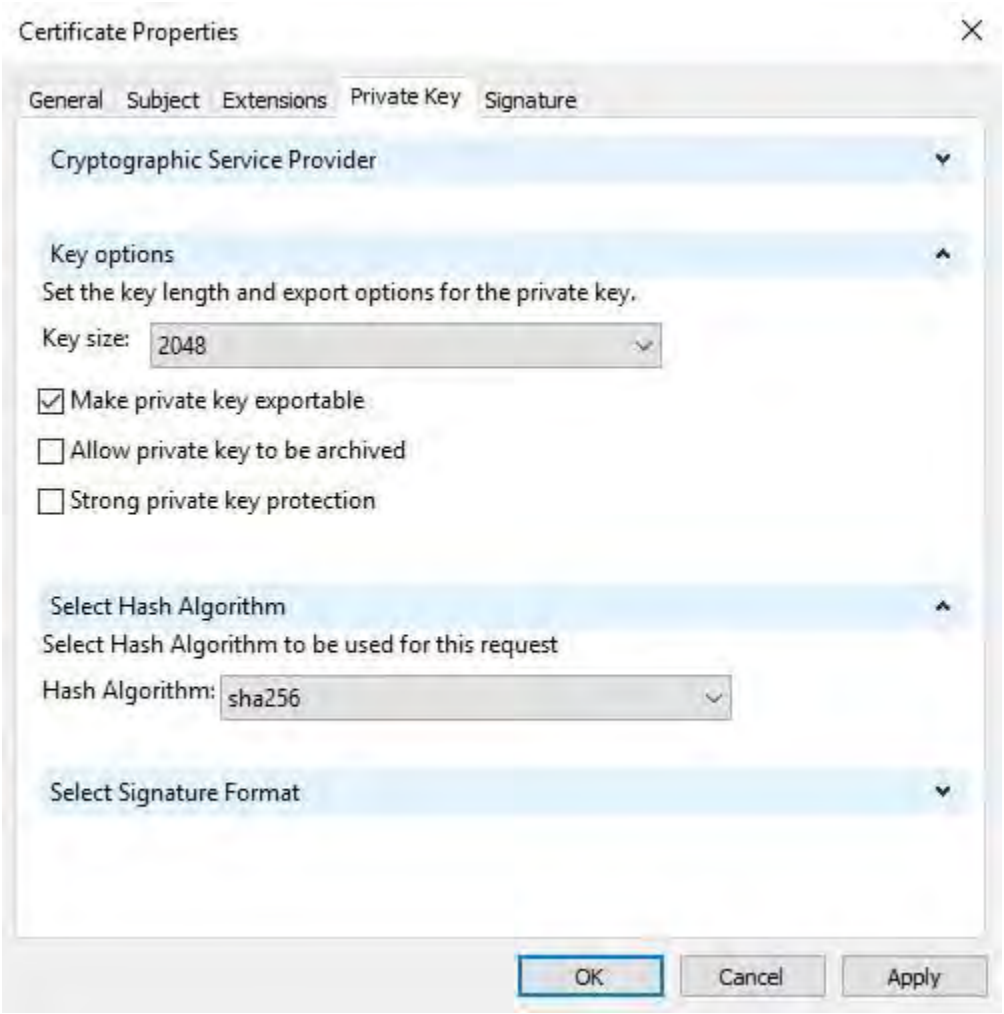
10. Dans l' **onglet Extensions**, développez le menu **Utilisation étendue des clés (stratégies d'application).** Ajoutez l'**authentification du serveur** dans la liste des options disponibles.



11. Sous l' **onglet Clé privée**, développez le menu Options de clé .

    Définissez la taille de la clé sur 2048 et sélectionnez l'option permettant d'exporter la clé privée.

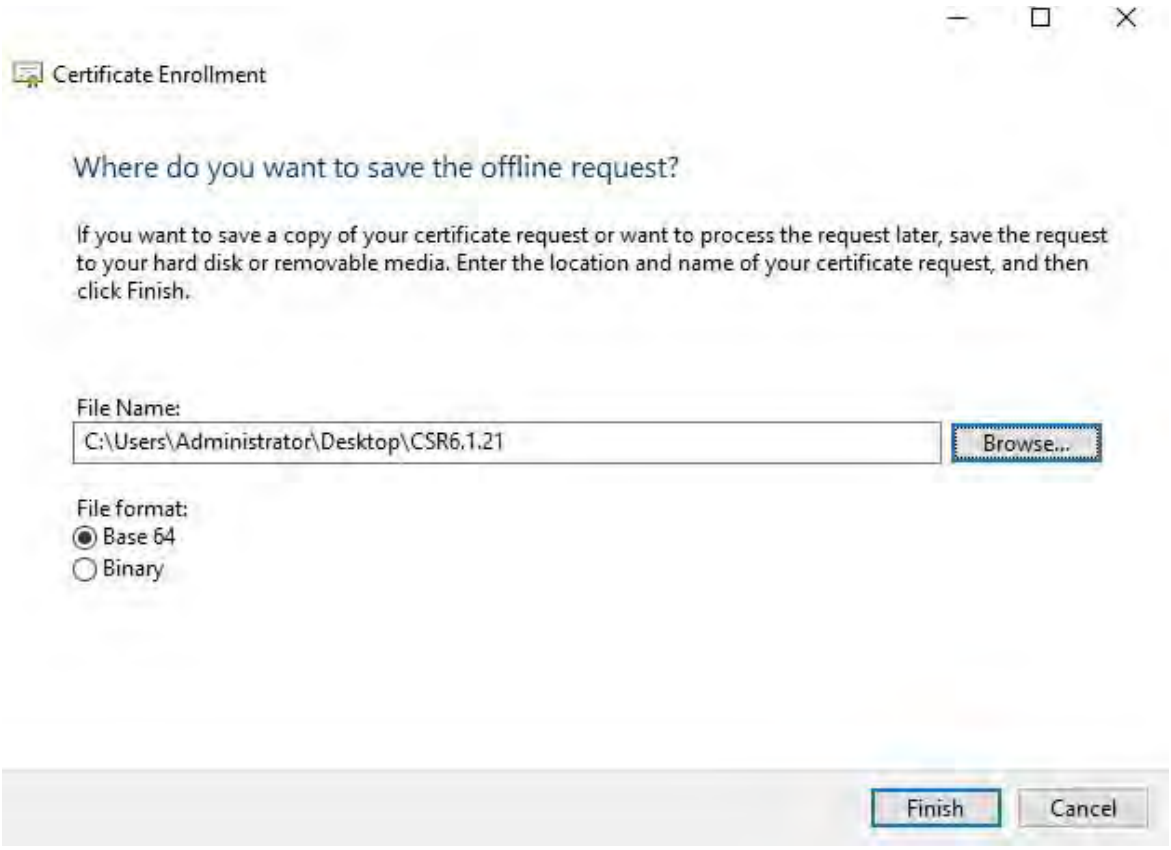
    Cliquez sur **OK**.



12. Une fois que toutes les propriétés du certificat ont été définies, cliquez sur **Suivant** dans l' **onglet Inscription au certificat**
    sorcier.

13. Sélectionnez un emplacement pour enregistrer la demande de certificat et un format. Naviguez jusqu'à cet emplacement et spécifiez un nom pour le fichier .req. Le format par défaut est la base 64.

14. Cliquez sur **Terminer**.



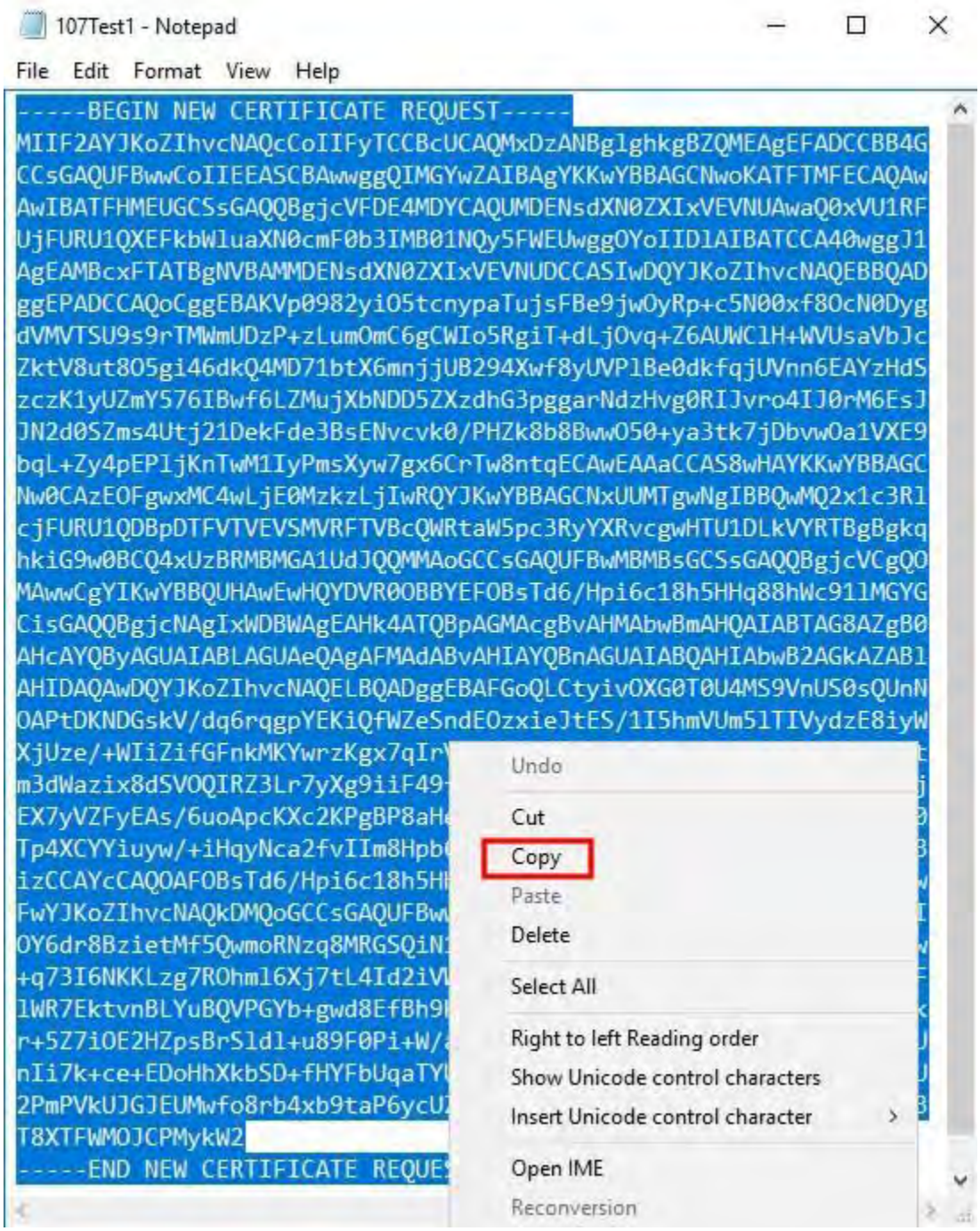
Un fichier .req est généré, que vous devez utiliser pour demander un certificat signé.

Téléchargez le fichier .req pour recevoir un certificat signé en retour

Vous devez copier l'intégralité du texte du fichier .req, y compris les lignes de début et de fin, et coller le texte dans l' autorité de certification interne des services de certificats Active Directory au sein du réseau. Voir Installer les services de certificats Active Directory à la page 74.

À moins que votre domaine n'ait récemment installé les services de certificats Active Directory ou qu'il n' ait été installé uniquement à cet effet, vous devrez soumettre cette demande en suivant une procédure distincte configurée par votre équipe d'administration de domaine. Veuillez confirmer ce processus avec eux avant de continuer.

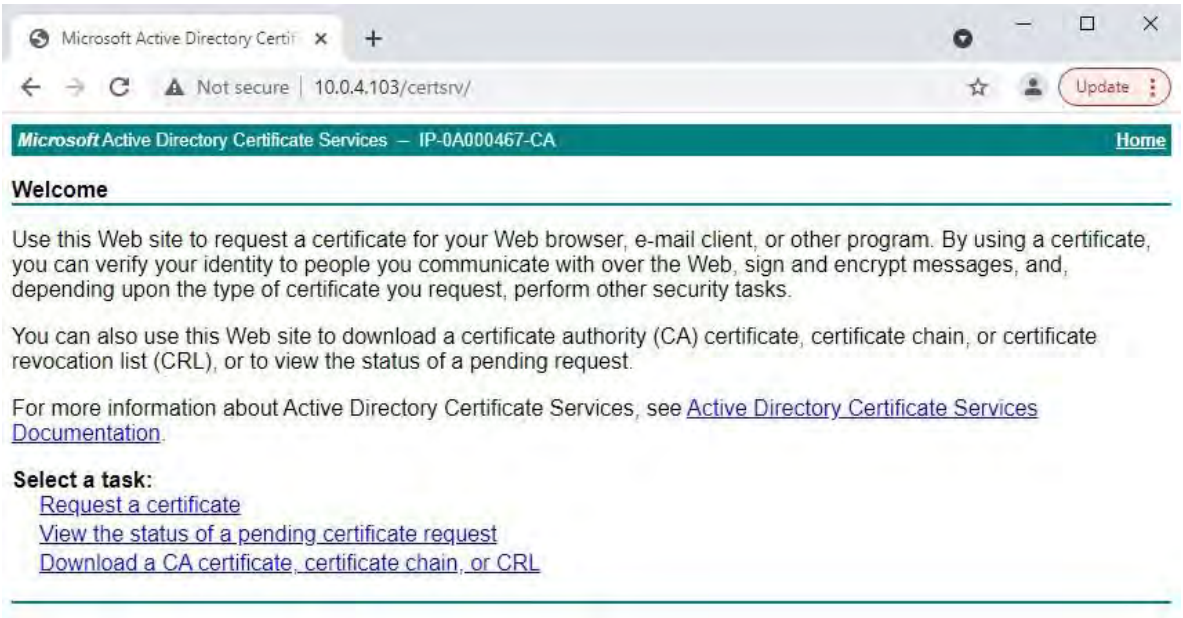
1. Naviguez jusqu'à l'emplacement du fichier .req et ouvrez-le dans le Bloc-notes.



2. Copiez l'intégralité du contenu du fichier. Cela inclut les lignes pointillées marquant le début et la fin de la demande de certificat.

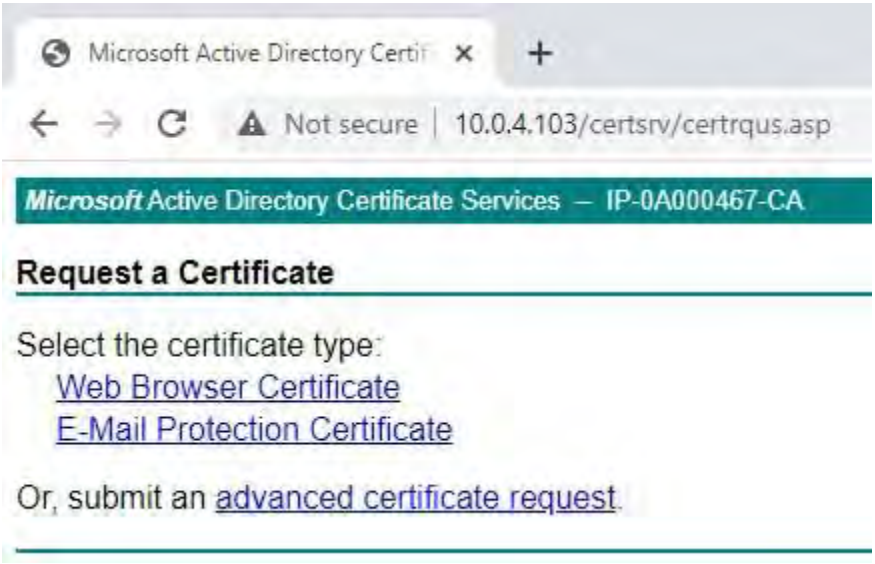
3. Ouvrez un navigateur Web et entrez l'adresse de l'autorité de certification interne, qui doit se trouver à l'adresse suivante : [ip.ad.dr.ess/certsrv].

   Où ip.ad.dr.ess est l'adresse IP ou le nom DNS du serveur hôte AD CS du réseau interne.

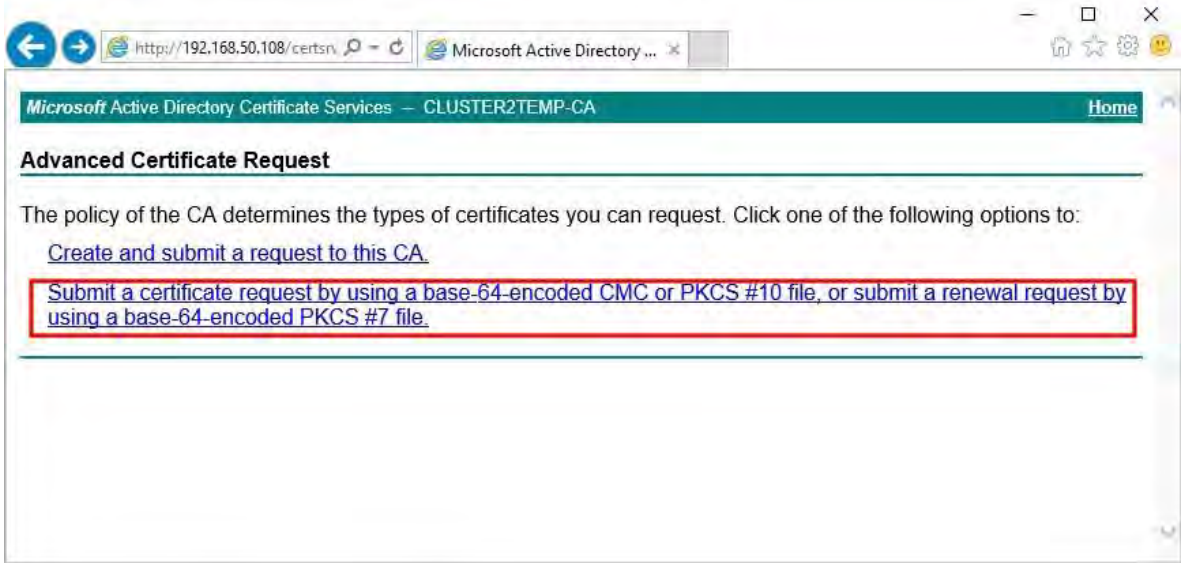


4. Cliquez sur le **lien Demander un certificat**.

5. Cliquez sur le lien de demande de **certificat avancé** .

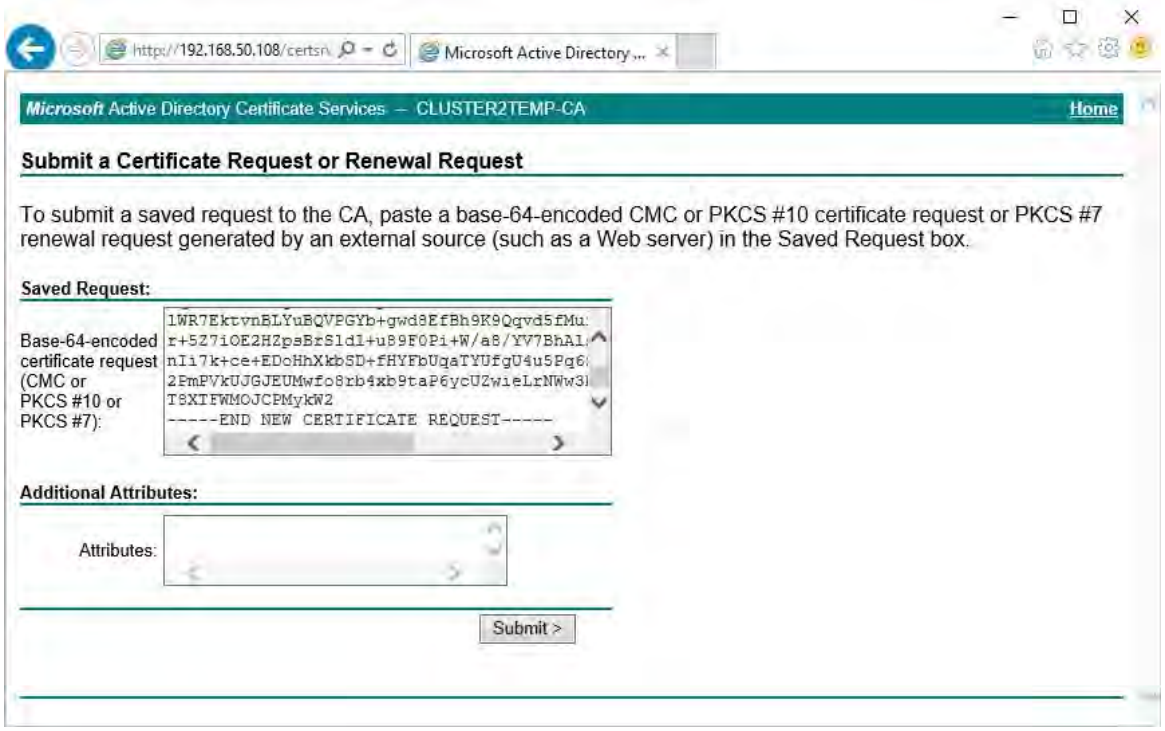


6. Choisissez d'envoyer une demande de certificat à l'aide d'un fichier CMC encodé en base 64.



7. Collez le contenu du fichier .req dans le formulaire. S'il est nécessaire de sélectionner un modèle de certificat, sélectionnez

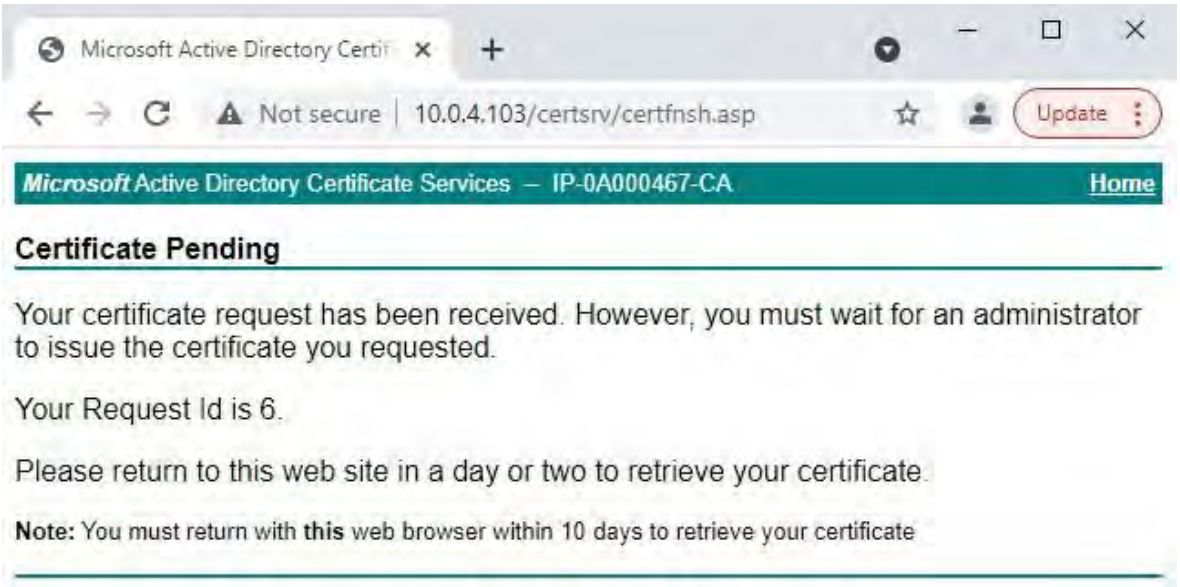
   Serveur Web dans la liste Modèle de certificat.



8. Cliquez sur **Soumettre**.

   Le site affiche un message indiquant que le certificat sera émis dans quelques jours.

   - Les serveurs d'autorité de certification internes peuvent être utilisés pour émettre manuellement des certificats
   - Notez la date et l'heure auxquelles la demande de certificat a été soumise

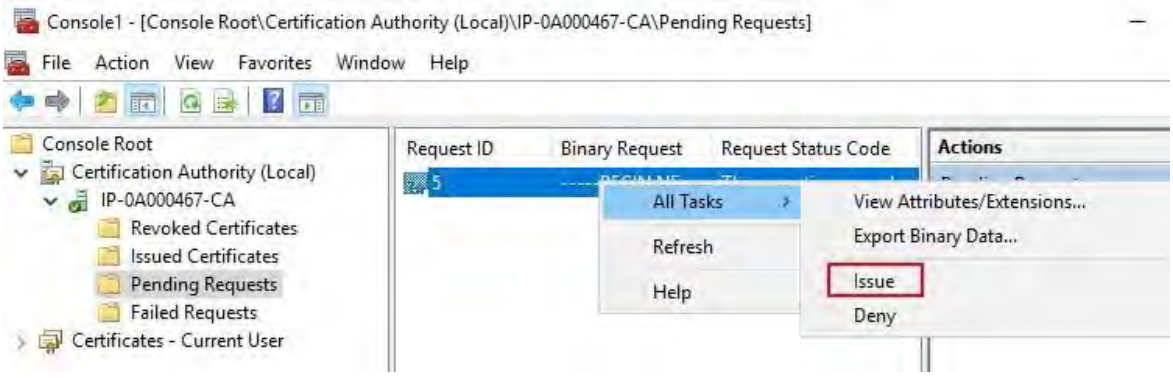


Émettre des certificats manuellement

Vous pouvez émettre des certificats manuellement à partir de l'ordinateur qui héberge les services de certificats Active Directory (AD CS).

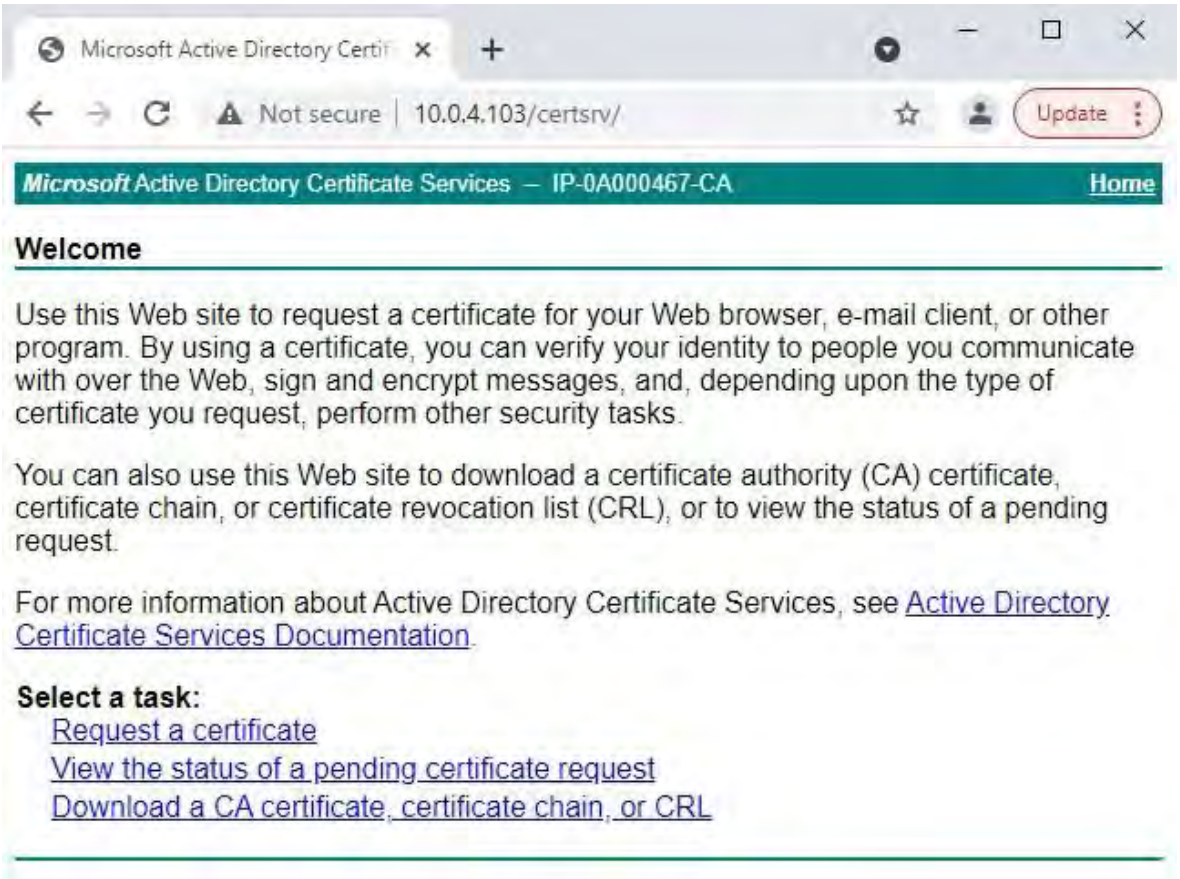
1. Ouvrez la console de gestion Microsoft (MMC).
2. Accédez au **composant logiciel enfichable Autorité de** certification.
3. Développez l' objet **Autorité de certification**.

   Dans le dossier **Demandes en attente**, cliquez avec le bouton droit de la souris sur l'ID de demande correspondant et, dans la **liste Toutes les tâches**, sélectionnez **Problème**.

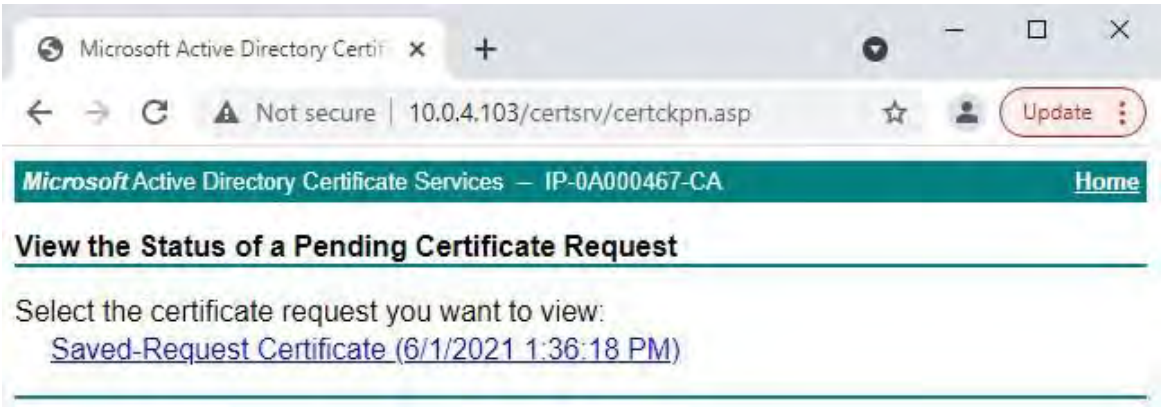


4. Ouvrez un navigateur et rendez-vous sur le site Internal CA IIS situé à l'adresse [ip.ad.dr.ess/certsrv].

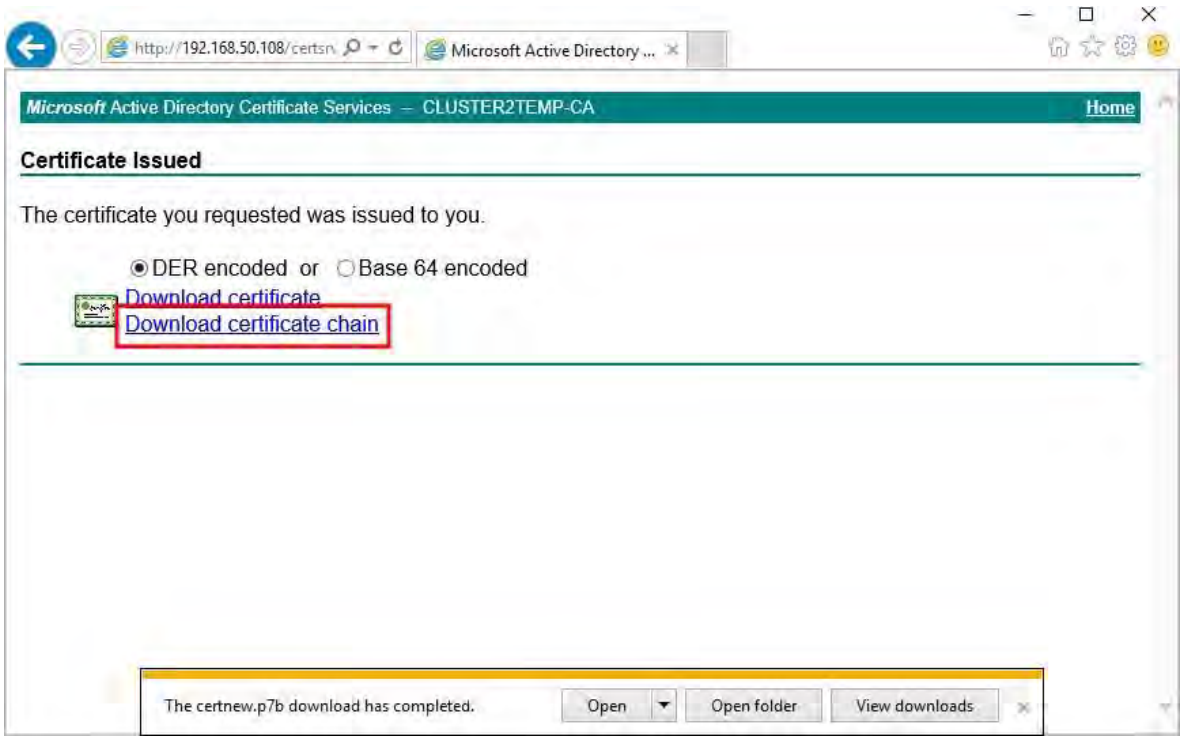
   Cliquez sur le lien **Afficher l'état d'une demande de certificat en attente**.



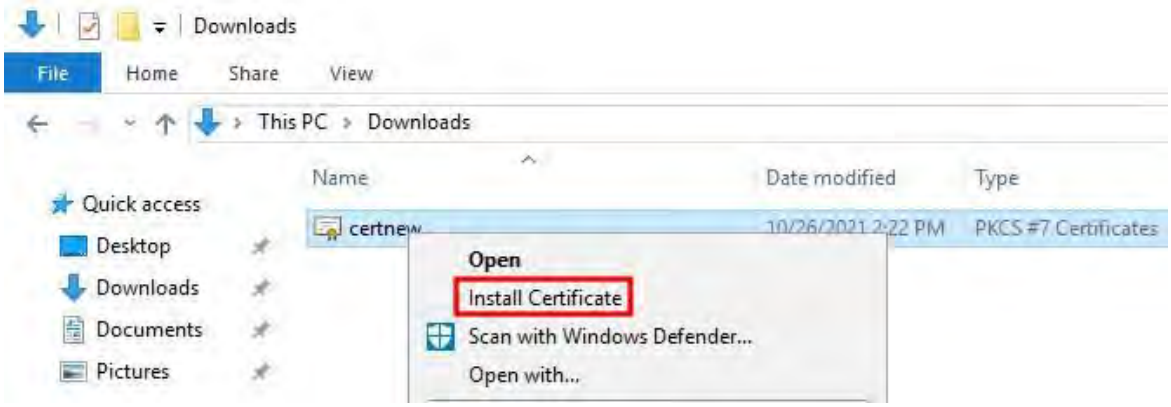
5. Si le certificat a été émis, un lien sera disponible sur la page résultante qui contient la date de la demande de certificat.



6. Sélectionnez **DER encodé** et téléchargez la chaîne de certificats.



7. Accédez au dossier téléchargements, cliquez avec le bouton droit sur le certificat, puis sélectionnez **Installer le certificat** dans le menu contextuel.



8. Acceptez l'avertissement de sécurité s'il apparaît.

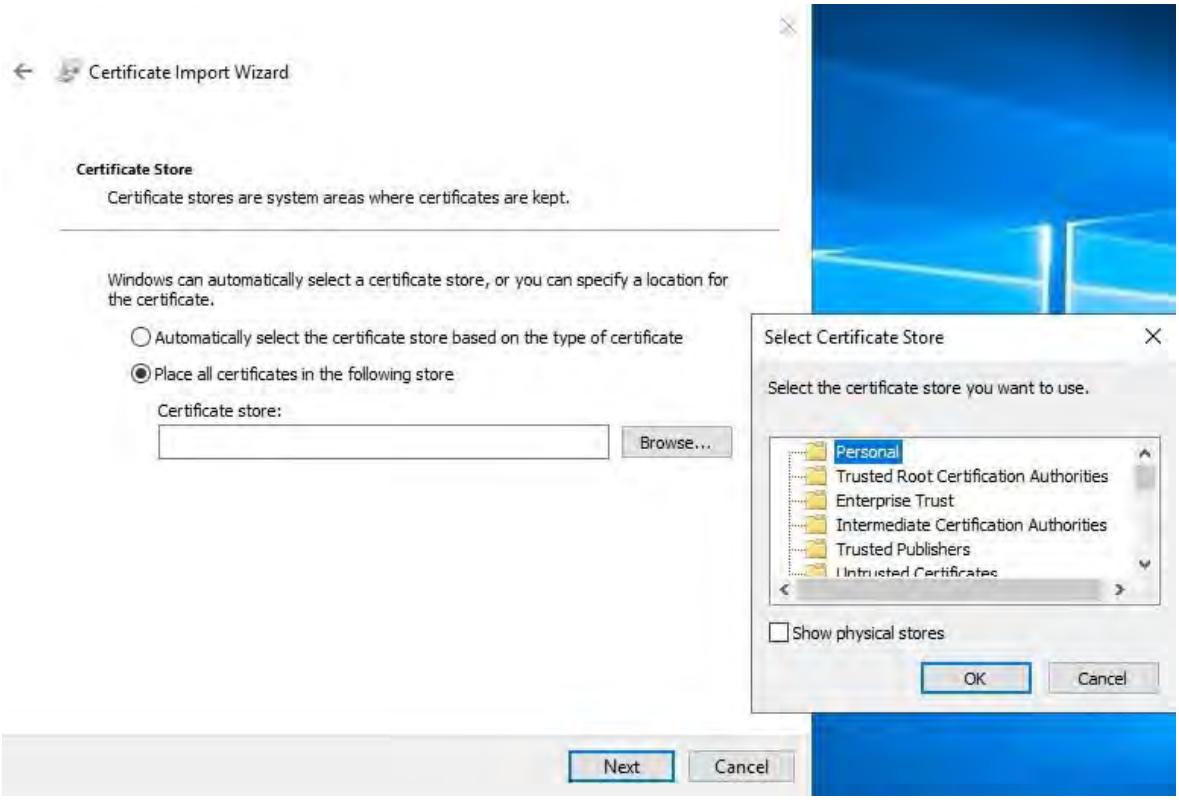
   Sélectionnez cette option pour installer le certificat de l'utilisateur actuel et cliquez sur **Suivant**.

9. Choisissez l'emplacement d'un magasin. Sélectionnez **Placer tous les certificats dans le magasin suivant**, puis cliquez sur l'icône **Parcourir**

   pour ouvrir la fenêtre **Sélectionner le magasin de certificats**.

   Accédez au magasin de certificats **personnel** et cliquez sur **OK**.

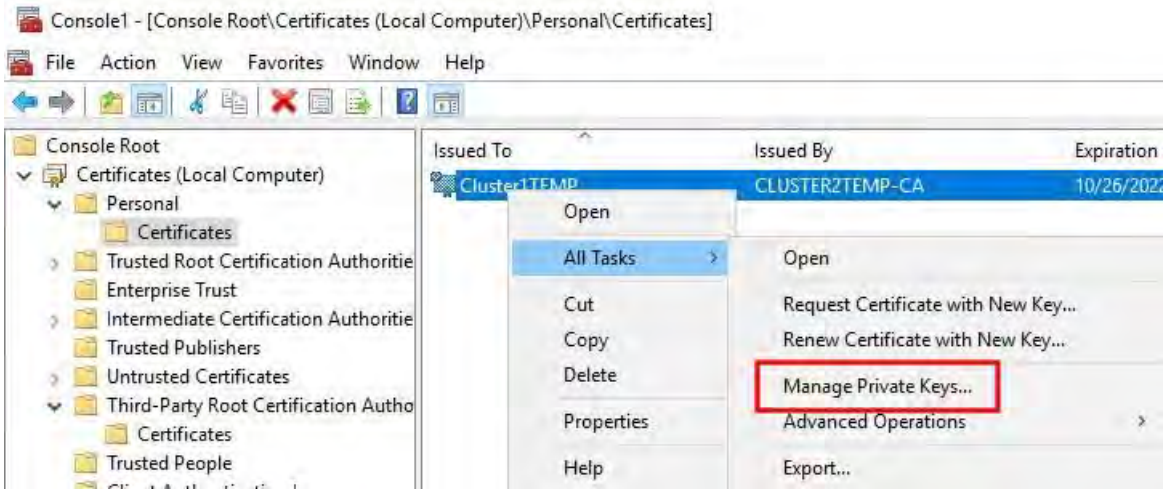
   Cliquez sur **Suivant**.



10. Terminez l' **assistant d'importation de certificat**.

11. Accédez au composant logiciel enfichable Certificats Microsoft Management Console (MMC).

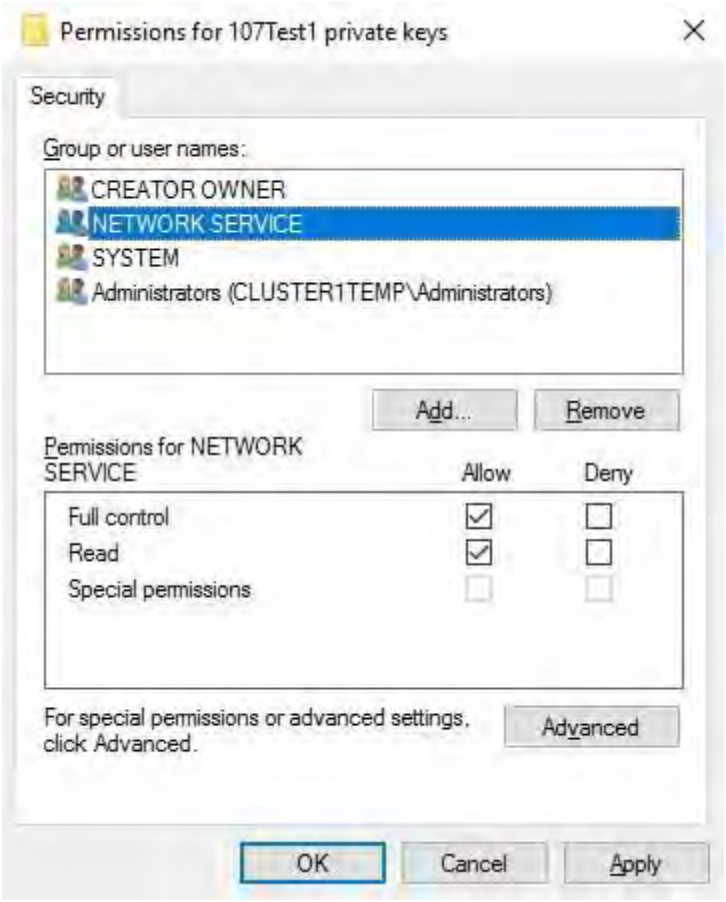
12. Dans la console, accédez au magasin personnel où le certificat est installé. Cliquez avec le bouton droit de la souris sur le certificat et sélectionnez **Toutes les tâches** > **Gérer les clés privées**.



13. Ajoutez le compte qui exécute le logiciel MOBOTIX HUB Management Server, Recording Server ou Mobile Server à la liste des utilisateurs autorisés à utiliser le certificat.

    Assurez-vous que l'utilisateur dispose des autorisations Contrôle total et Lecture activées.

    Par défaut, le logiciel MOBOTIX HUB utilise le compte NETWORK SERVICE.



Activer le chiffrement du serveur pour les serveurs de gestion et les serveurs d'enregistrement

Une fois le certificat installé avec les propriétés et les autorisations appropriées, procédez comme suit.

1. Sur un ordinateur sur lequel un serveur de gestion ou un serveur d'enregistrement est installé, ouvrez le **configurateur de serveur**

   De:

   - Le menu Démarrer de Windows

   ou

   - Le gestionnaire de serveur, en cliquant avec le bouton droit de la souris sur l'icône du gestionnaire de serveur dans la barre des tâches de l'ordinateur

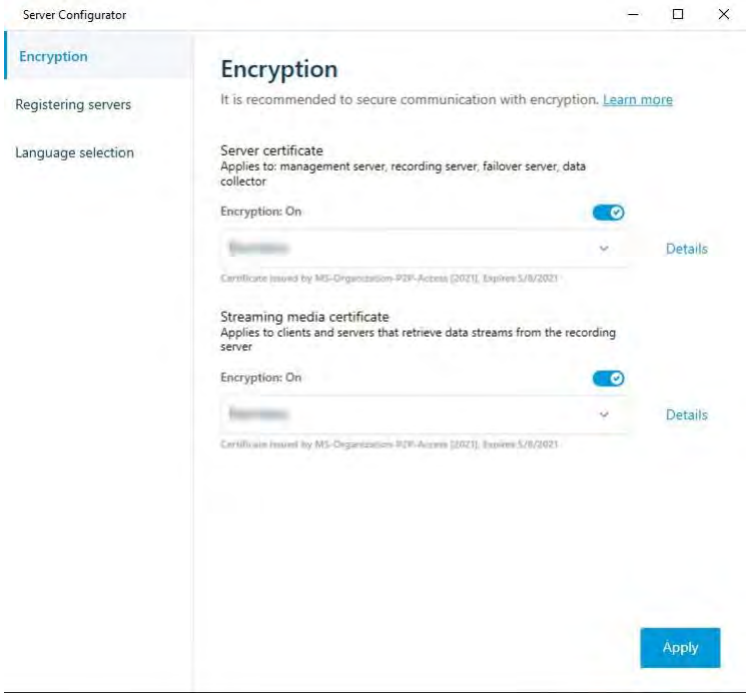
2. Dans le **configurateur de serveur**, sous **Certificat de serveur**, activez **le cryptage**.

3. Cliquez sur **Sélectionner un certificat** pour ouvrir une liste avec les noms d'objet uniques des certificats qui ont une clé privée et qui sont installés sur l'ordinateur local dans le magasin de certificats Windows.

4. Sélectionnez un certificat pour chiffrer la communication entre le serveur d'enregistrement, le serveur de gestion, le serveur de basculement et le serveur de collecte de données.

   Sélectionnez **Détails** pour afficher les informations du Magasin de certificats Windows concernant le certificat sélectionné.

   L'utilisateur du service Recording Server a accès à la clé privée. Il est nécessaire que ce certificat soit approuvé sur tous les clients.



5. Cliquez sur **Appliquer**.

> ⚠ Lorsque vous appliquez des certificats, le serveur d'enregistrement est arrêté et redémarré. L'arrêt du service de serveur d'enregistrement signifie que vous ne pouvez pas enregistrer et visionner des vidéos en direct pendant que vous vérifiez ou modifiez la configuration de base du serveur d'enregistrement.

Installer des certificats pour la communication avec le serveur d'événements

Vous pouvez chiffrer la connexion bidirectionnelle entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements, y compris le serveur LPR. Lorsque vous activez le chiffrement sur le serveur d'événements, il s'applique aux connexions de tous les composants qui se connectent au serveur d'événements. Avant d'activer le chiffrement, vous devez installer des certificats de sécurité sur le serveur d'événements et tous les composants de connexion.

> Lorsque la communication du serveur d'événements est chiffrée, cela s'applique à toutes les communications avec ce serveur d'événements. C'est-à-dire qu'un seul mode est pris en charge à la fois, http ou https, mais pas en même temps.

Le chiffrement s'applique à tous les services hébergés dans le serveur d'événements, y compris Transact, Maps, GisMap et Intercommunication.

> Avant d'activer le chiffrement dans Event Server, tous les clients (Desk Client et Management Client) et le plug-in MOBOTIX HUB LPR doivent être mis à jour vers au moins la version 2022 R1.
> HTTPS n'est pris en charge que si chaque composant est mis à jour vers au moins la version 2022 R1.

La création des certificats est identique à celle décrite dans ces sections, en fonction de l'environnement de certificat :

- Installez des certificats d'autorité de certification tiers ou commerciaux pour la communication avec le serveur de gestion ou le serveur d'enregistrement à la page 57
- Installez des certificats dans un domaine pour la communication avec le Serveur de gestion ou le Serveur d'enregistrement à la page 86
- Installez les certificats dans un environnement de groupe de travail pour la communication avec le serveur de gestion ou le serveur d'enregistrement à la page 104

Activer le chiffrement du serveur d'événements MOBOTIX HUB

Une fois le certificat installé, vous pouvez l'activer pour qu'il soit utilisé avec toutes les communications avec le serveur d'événements.

> Une fois que tous les clients ont été mis à jour vers au moins la version 2022 R1, vous pouvez activer le chiffrement sur le serveur d'événements.

Vous pouvez chiffrer la connexion bidirectionnelle entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements, y compris le serveur LPR.

> Lorsque vous configurez le chiffrement pour un groupe de serveurs, il doit être activé à l'aide d'un certificat appartenant au même certificat d'autorité de certification ou, si le chiffrement est désactivé, il doit être désactivé sur tous les ordinateurs du groupe de serveurs.

Conditions préalables:

- Un certificat d'authentification de serveur est approuvé sur l'ordinateur qui héberge le

serveur d'événements Tout d'abord, activez le chiffrement sur le serveur d'événements.

Escalier:

1. Sur un ordinateur sur lequel un serveur d'événements est installé, ouvrez le **configurateur de serveur** à partir de :

   - Le menu Démarrer de Windows

   ou

   - Le serveur d'événements en cliquant avec le bouton droit de la souris sur l'icône Serveur d'événements dans la barre des tâches de l'ordinateur

2. Dans le **configurateur de serveur**, sous **Serveur d'événements et modules complémentaires**, activez **le chiffrement**.

3. Cliquez sur **Sélectionner un certificat** pour ouvrir une liste avec les noms d'objet uniques des certificats qui ont une clé privée et qui sont installés sur l'ordinateur local dans le magasin de certificats Windows.

4. Sélectionnez un certificat pour chiffrer la communication entre le serveur d'événements et les modules complémentaires associés.

Sélectionnez **Détails** pour afficher les informations du Magasin de certificats Windows concernant le certificat sélectionné.

5. Cliquez sur **Appliquer**.

Pour terminer l'activation du cryptage, l'étape suivante consiste à mettre à jour les paramètres de cryptage sur chaque serveur LPR add-on associé .

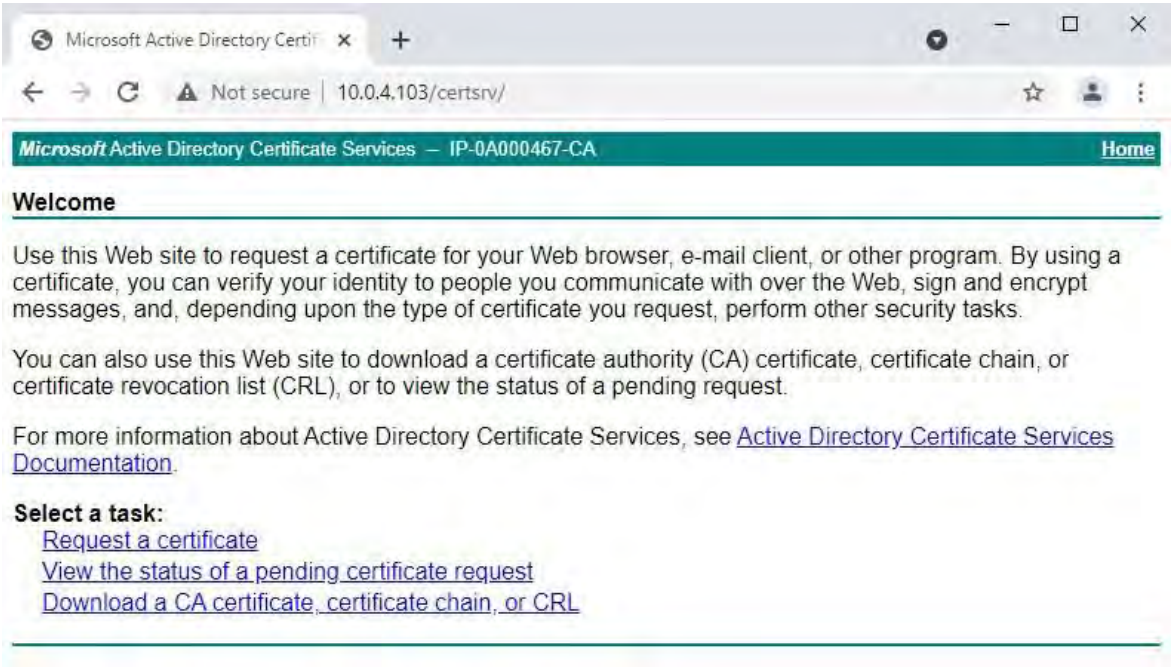
Importer des certificats clients

Cette section décrit comment importer des certificats client sur un poste de travail ou un périphérique client.

1. Après avoir importé un certificat d'autorité de certification sur le serveur de gestion ou le serveur d'enregistrement, vous pouvez y accéder à partir de n' importe quel poste de travail ou serveur du réseau en vous rendant à l'adresse suivante :

   - http://localhost/certsrv/

   Cependant, l'adresse du serveur qui détient le certificat (clé privée) prendra la place de « localhost ». Par exemple:

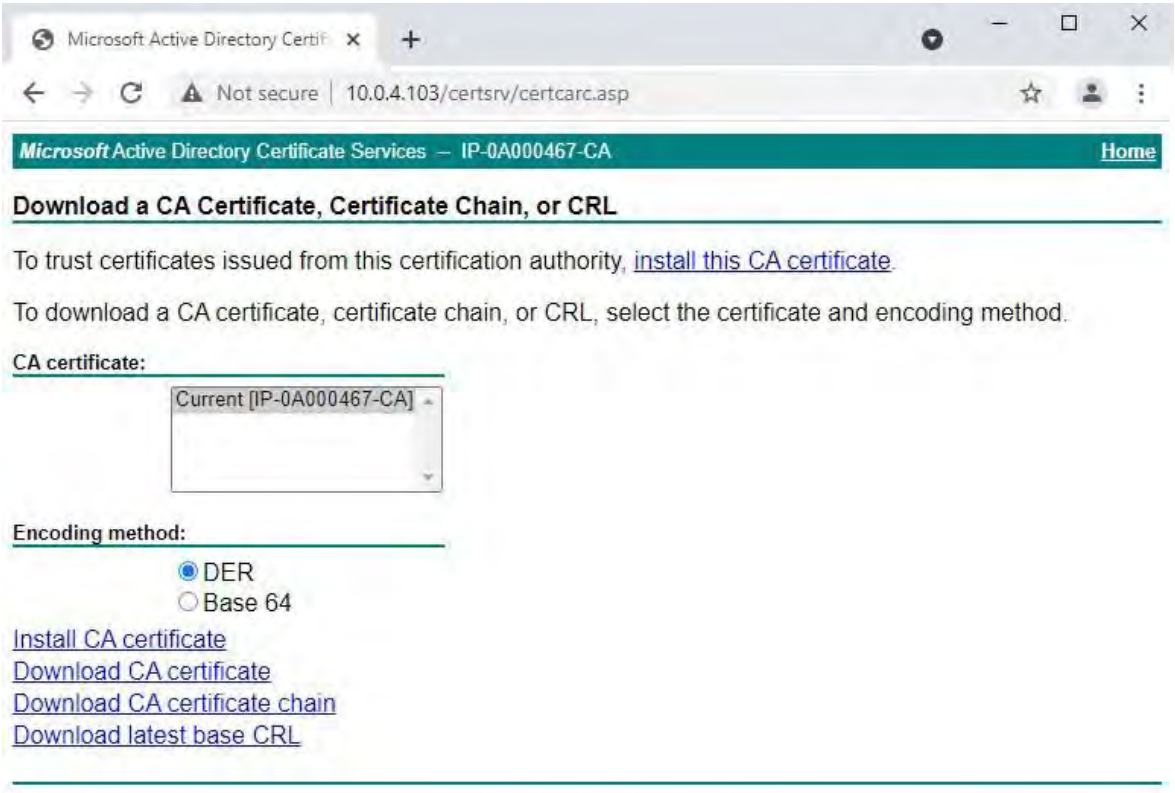


   Ce serveur Web est hébergé sur le serveur hôte AD CS (Active Directory Certificate Services) qui contient le certificat de l'autorité de certification.

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

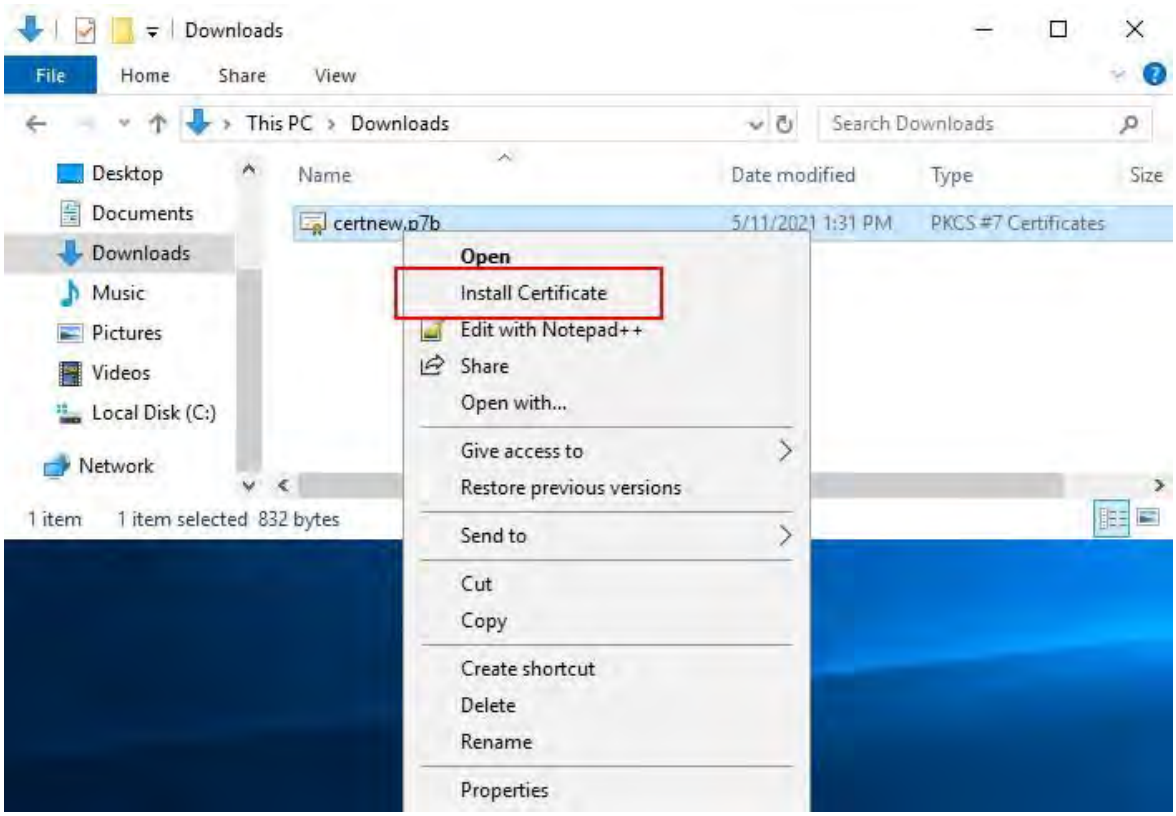
3. Dans le champ Certificat de **l'autorité de certification** , sélectionnez le certificat de l'autorité de certification à utiliser avec le système MOBOTIX HUB, puis cliquez sur

   Télécharger la chaîne de certificats de l'autorité de certification.



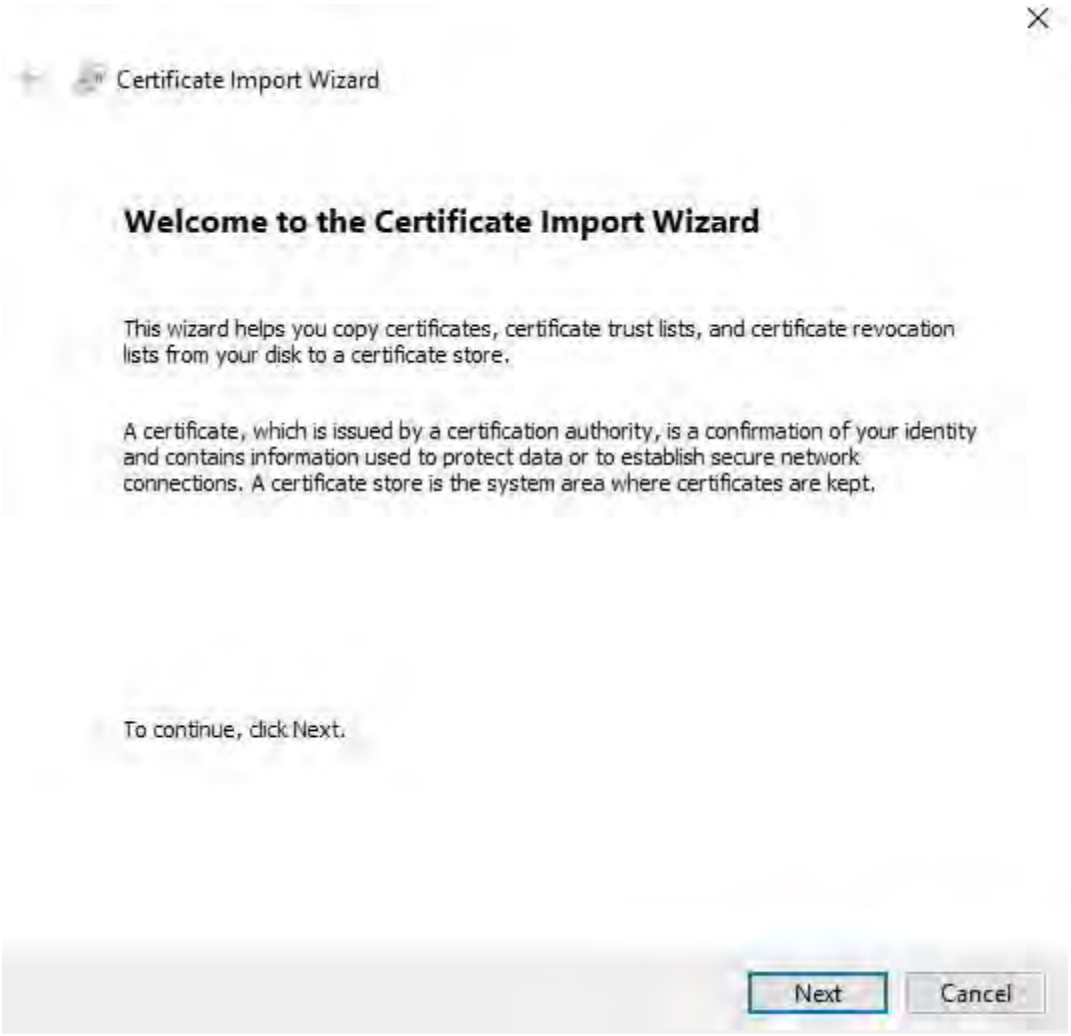
4. Sélectionnez **DER encodé** et téléchargez la chaîne de certificats.

5. Accédez au dossier téléchargements, cliquez avec le bouton droit sur le certificat, puis sélectionnez **Installer le certificat** dans le menu contextuel.



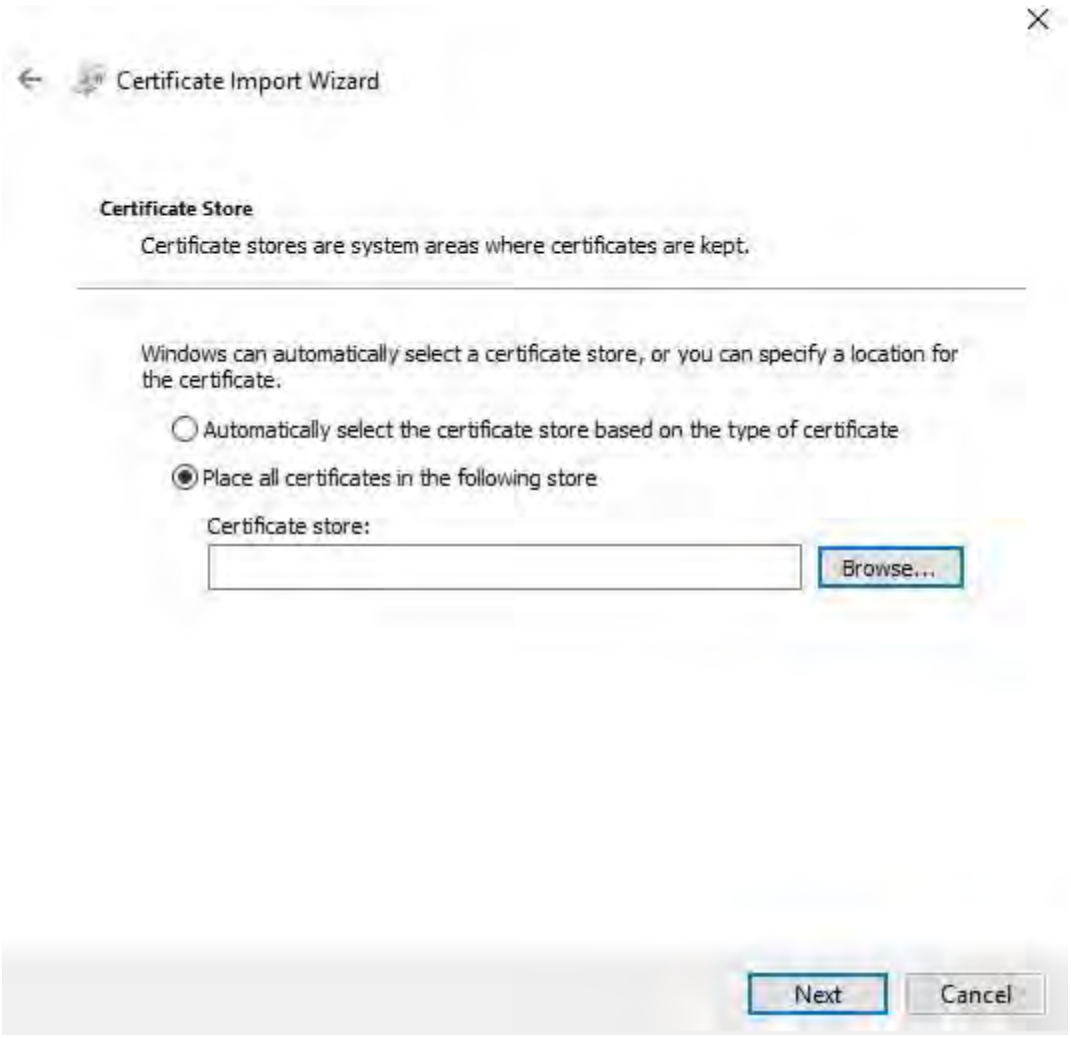
6. L'**assistant d'importation de certificats** est lancé.

   Cliquez sur **Suivant**.

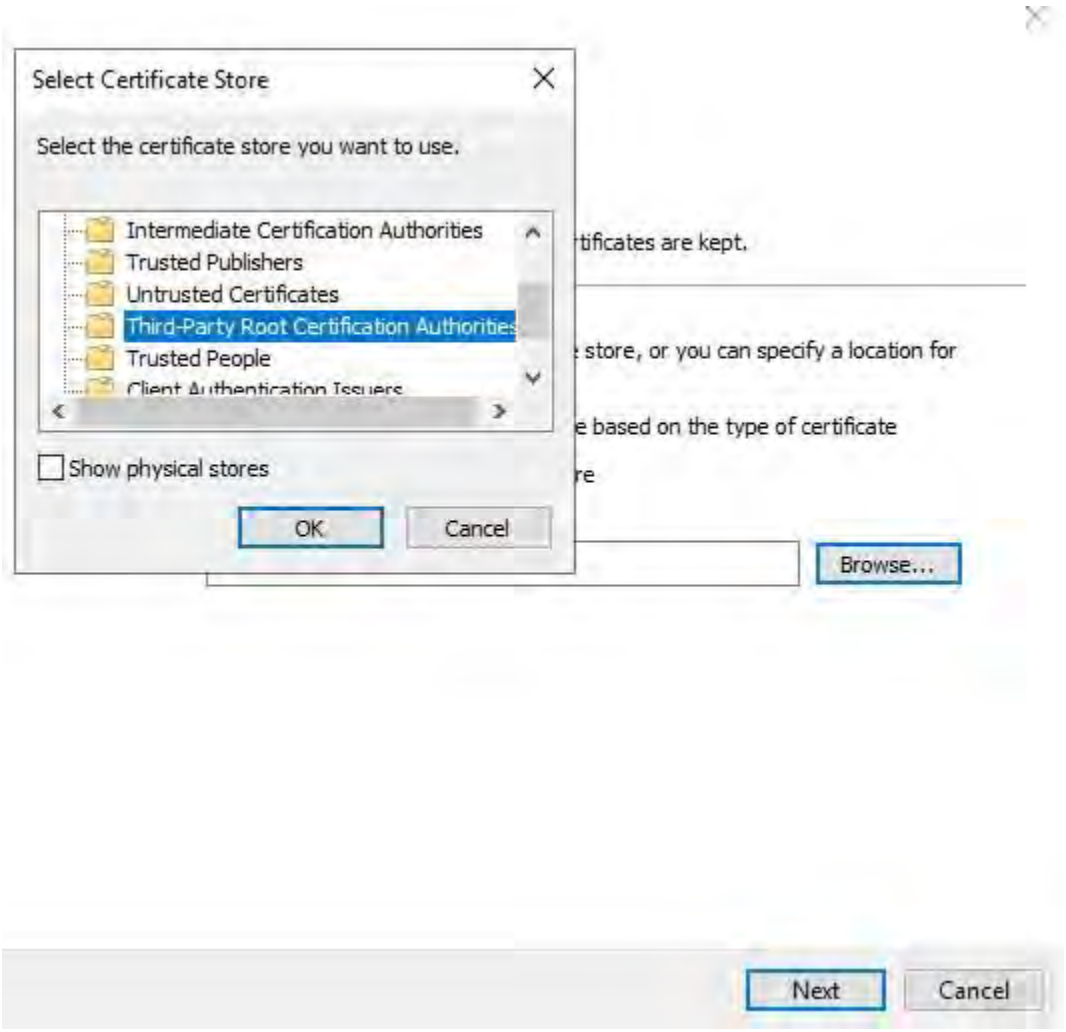


7. Choisissez l'emplacement d'un magasin. Sélectionnez **Placer tous les certificats dans le magasin suivant**, puis cliquez sur l'icône **Parcourir**

   pour ouvrir la fenêtre **Sélectionner le magasin de certificats**.



8. Accédez au magasin de **certificats Third-Party Root Certification Authorities** et cliquez sur **OK.** Cliquez sur **Suivant**.



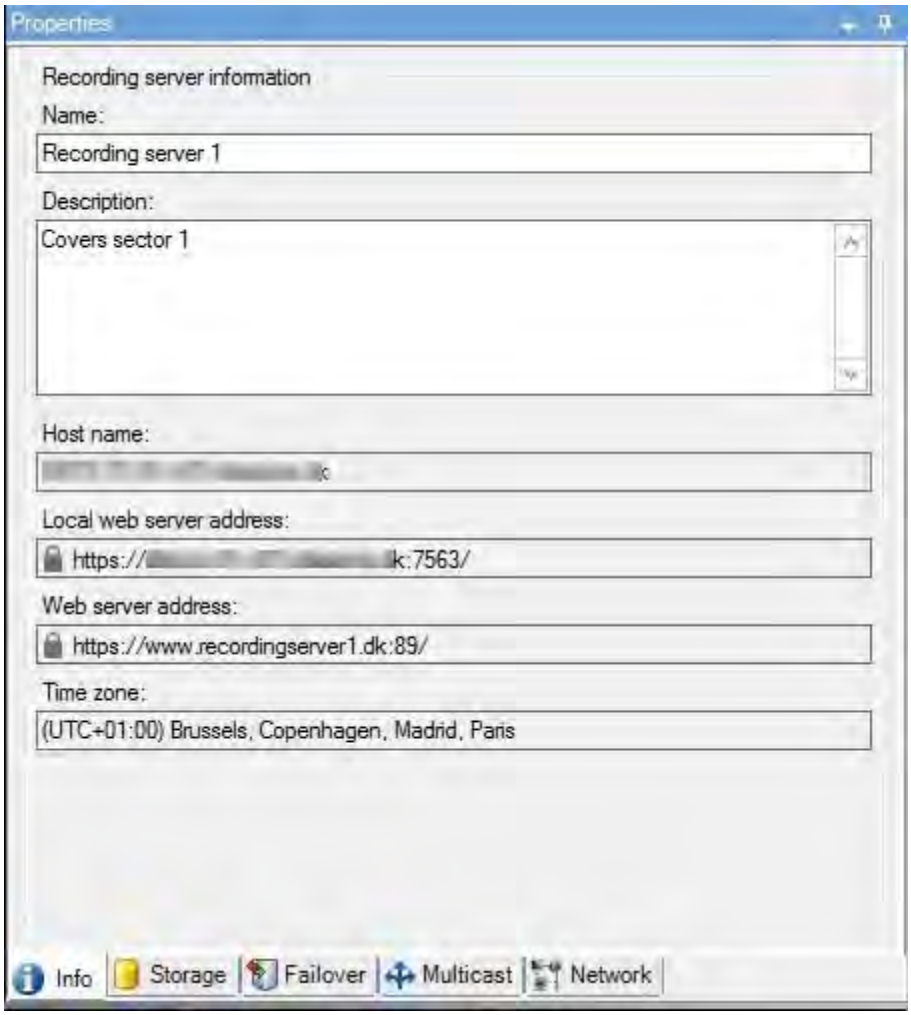
9. Terminez l' **assistant d'importation de certificat**.

Le poste de travail a maintenant importé les composants de certificat nécessaires pour établir des communications sécurisées avec le serveur de gestion ou le serveur d'enregistrement.

Afficher l'état du chiffrement pour les clients

Pour vérifier si votre serveur d'enregistrement crypte les connexions :

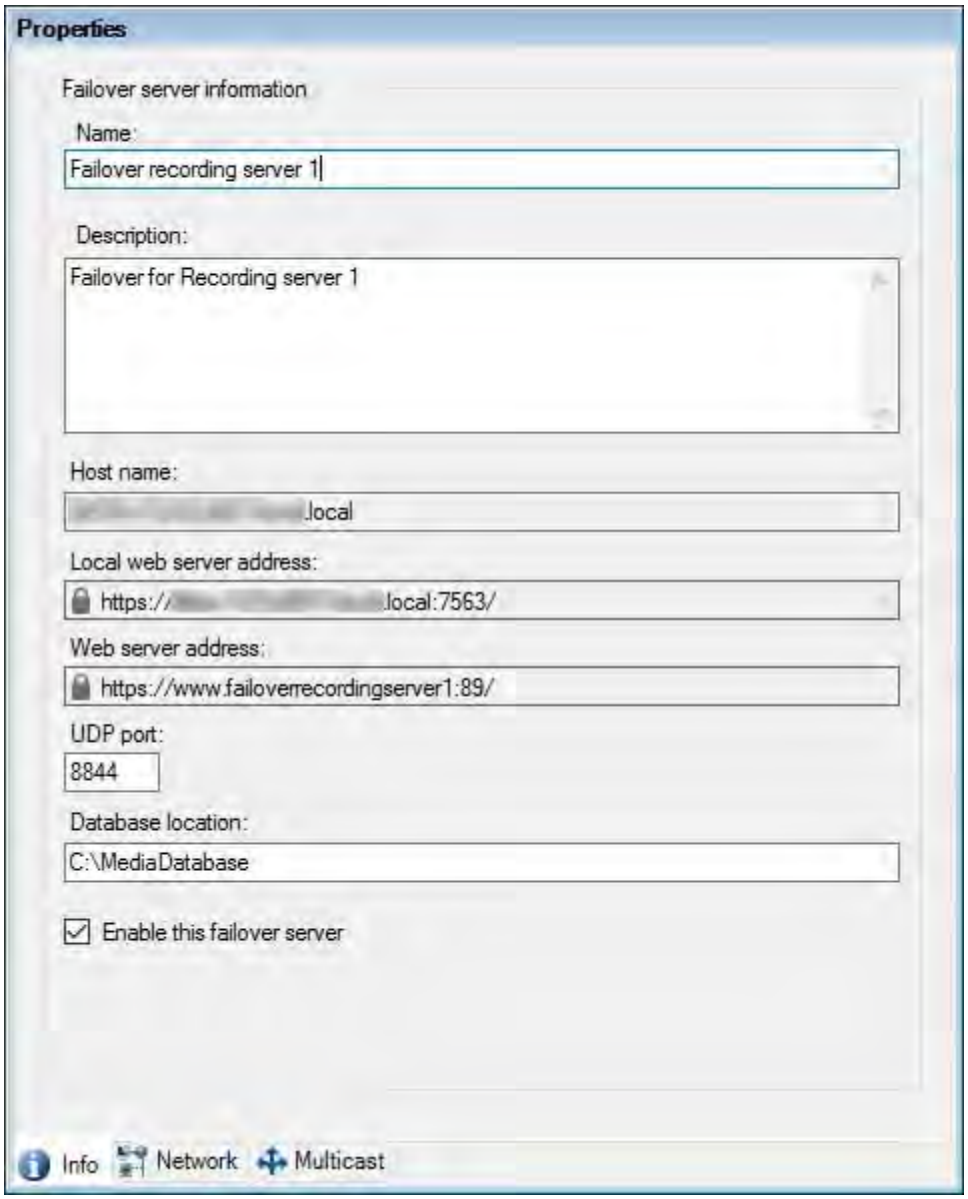
1. Ouvrez le client de gestion.
2. Dans le volet **de navigation du site**, sélectionnez **Serveurs** > **Serveurs d'enregistrement**. Cela ouvre une liste de serveurs d'enregistrement.
3. Dans le volet **Vue d'ensemble**, sélectionnez le serveur d'enregistrement approprié et accédez à l' **onglet Infos**.
   Si le chiffrement est activé pour les clients et les serveurs qui récupèrent des flux de données à partir du serveur d'enregistrement, une icône de cadenas apparaît devant l'adresse du serveur Web local et l'adresse facultative du serveur Web.



Afficher l'état du chiffrement sur un serveur d'enregistrement de basculement

Pour vérifier si votre serveur d'enregistrement de basculement utilise le chiffrement, procédez comme suit :

1. Dans le volet **de navigation du site**, sélectionnez **Serveurs** > **Serveurs de basculement**. Cela ouvre une liste de serveurs d'enregistrement de basculement.
2. Dans le volet **Vue d'ensemble**, sélectionnez le serveur d'enregistrement approprié et accédez à l' **onglet Infos**. Si le chiffrement est activé pour les clients et les serveurs qui récupèrent des flux de données à partir du serveur d'enregistrement, une icône de cadenas apparaît devant l'adresse du serveur Web local et l'adresse facultative du serveur Web.



```
# Exécutez ce script une fois, pour créer un certificat capable de signer plusieurs certificats SSL de serveur

# Certificat privé pour la signature d'autres certificats (dans le magasin de certificats)
$ca_certificate = New-SelfSignedCertificate -CertStoreLocation cert :\CurrentUser\My -DnsName 'Autorité de certification VMS' -KeyusageProperty All '
                                                                                    -KeyUsage CertSign, CRLSign, DigitalSignature -FriendlyName 'Certificat VMS CA' '
                                                                                    -TextExtension @(« 2.5.29.19={critique}{text}ca=VRAI »)

# Empreinte du certificat privé utilisée pour signer d'autres certificats
set-content -chemin « $PSScriptRoot\ca_thumbprint.txt » -valeur $ca_certificat. Empreinte

# Certificat d'autorité de certification publique à confiance (Third-Party Root Certification Authoritys)
export-certificate -cert "cert :\CurrentUser\My\$($ca_certificate. empreinte) » -filepath « $PSScriptRoot\root-authority-public.cer »
```

```
# Exécutez ce script une fois pour chaque serveur pour lequel un certificat SSL est nécessaire.
# Le certificat doit être exécuté sur l'ordinateur unique où se trouve le certificat de l'autorité de certification. # Le certificat SSL du serveur
créé doit ensuite être déplacé vers le serveur et importé dans le magasin de certificats #.
# Après avoir importé le certificat, autorisez l'accès à la clé privée du certificat pour # le(s) utilisateur(s) du service des services qui
doivent utiliser le certificat.

# Charger le certificat de l'autorité de certification à partir du magasin (l'empreinte doit être dans ca_thumbprint.txt)
$ca_thumbprint = get-content -chemin « $PSScriptRoot\ca_thumbprint.txt »
$ca_certificate = (Get-ChildItem -Path cert :\CurrentUser\My\$ca_thumbprint)

# Demander à l'utilisateur les noms DNS à inclure dans le certificat
$dnsNames = Read-Host 'Noms DNS pour le certificat SSL du serveur (délimités par un espace - la 1ère entrée fait également l'objet du certificat)'
$dnsNamesArray = @($dnsNames -Split ' ' | foreach { $_. trim() } | où { $_ })

if ($dnsNamesArray.Length -eq 0) {
        Write-Host -ForegroundColor Rouge 'Au moins un nom dns doit être spécifié' exit
}
$subjectName = $dnsNamesArray[0]
$dnsEntries = ($dnsNamesArray | foreach { « DNS=$_ » }) -Join '&'

# Autoriser éventuellement l'utilisateur à saisir une liste d'adresses IP à mettre dans le certificat
$ipAddresses = Read-Host 'Adresses IP pour le certificat SSL du serveur (déliées par l'espace)'
$ipAddressesArray = @($ipAddresses -Split ' ' | foreach { $_. trim() } | où { $_ }) if ($ipAddressesArray.Length -gt 0) {
        $ipEntries = ($ipAddressesArray | foreach { « IPAddress=$_ » }) -Join '&'
        $dnsEntries = « $dnsEntries&$ipEntries »
}

# Construire la chaîne finale d'entrées dns (par exemple « 2.5.29.17={text}DNS=myhost&DNS=myhost.domain.com&IPAddress=10.0.0.103 »)
$dnsEntries = « 2.5.29.17={texte}$dnsEntries »

# Le seul objectif requis du sertificat est « l'authentification du serveur »
$serverAuthentication = '2.5.29.37={critique}{texte}1.3.6.1.5.5.7.3.1'

# Maintenant - créez le certificat SSL du serveur
$certificate = New-SelfSignedCertificate -CertStoreLocation Cert :\CurrentUser\My -Subject $subjectName -Signer $ca_Certificate '
                                                        -friendlyName 'Certificat SSL VMS' -TextExtension @($dnsEntries, $serverAuthentication)

# Exporter le certificat sur le disque - protéger avec un mot de passe
$password = Read-Host -AsSecureString « Mot de passe du certificat SSL du serveur »
export-pfxCertificate -cert "cert :\CurrentUser\My\$($certificate. empreinte) » -filepath « $PSScriptRoot\$subjectName.pfx » -mot de passe $password

# Supprimer le certificat SSL du serveur du magasin de certificats local
$certificate | Supprimer-Article
```

```
# Exécutez ce script une fois pour chaque serveur de gestion pour lequel un certificat est nécessaire.
# Le certificat doit être exécuté sur l'ordinateur unique où se trouve le certificat de l'autorité de certification. # Le certificat créé doit ensuite
être déplacé vers les serveurs de gestion et
# importé dans le magasin de certificats qui s'y trouve.

# Charger le certificat de l'autorité de certification à partir du magasin (l'empreinte doit être dans ca_thumbprint.txt)
$ca_thumbprint = get-content -chemin « $PSScriptRoot\ca_thumbprint.txt »
$ca_certificate = (Get-ChildItem –Path cert :\CurrentUser\My\$ca_thumbprint)

# Demander à l'utilisateur les noms DNS à inclure dans le certificat
$dnsNames = Read-Host 'Noms DNS pour le certificat du serveur de gestion (délimités par des virgules - la 1ère entrée fait également l'objet du certificat)'
$dnsNamesArray = @($dnsNames -Split ',' | foreach { $_. trim() } | où { $_ })

si ($dnsNamesArray. Longueur -eq 0) {
        Write-Host -ForegroundColor Rouge 'Au moins un nom dns doit être spécifié' exit
}

$dnsEntries = ($dnsNamesArray | foreach { « DNS=$_ » }) -Join '&'

# Autoriser éventuellement l'utilisateur à saisir une liste d'adresses IP à mettre dans le certificat
$ipAddresses = Read-Host 'Adresses IP pour le certificat du serveur de gestion (délimitées par des virgules)'
$ipAddressesArray = @($ipAddresses -Split ',' | foreach { $_. trim() } | où { $_ }) if ($ipAddressesArray. Longueur -gt 0) {
        $ipEntries = ($ipAddressesArray | foreach { « IPAddress=$_ » }) -Join '&'
        $dnsEntries = « $dnsEntries&$ipEntries »
}
$subjectName = $ipAddressesArray[0]

# Construire la chaîne finale d'entrées dns (par exemple « 2.5.29.17={text}DNS=myhost&DNS=myhost.domain.com&IPAddress=10.0.0.103 »)
$dnsEntries = « 2.5.29.17={texte}$dnsEntries »

# Le seul objectif requis du sertificat est « l'authentification du serveur »
$serverAuthentication = '2.5.29.37={critique}{texte}1.3.6.1.5.5.7.3.1'

# Maintenant - créez le certificat du serveur de gestion
$certificate = New-SelfSignedCertificate -CertStoreLocation Cert :\CurrentUser\My -Subject $subjectName -Signer $ca_Certificate '
                                                        -friendlyName 'Certificat du serveur VMS' -TextExtension @($dnsEntries, $serverAuthentication)

# Exporter le certificat sur le disque - protéger avec un mot de passe
$password = Read-Host -AsSecureString « Mot de passe du certificat du serveur de gestion »
export-pfxCertificate -cert "cert :\CurrentUser\My\$($certificate. empreinte) » -filepath « $PSScriptRoot\$subjectName.pfx » -mot de passe $password

# Supprimer le certificat du serveur de gestion du magasin de certificats local
$certificate | Supprimer-Article
```

MOBOTIX

BeyondHumanVision

FR_02/25

MOBOTIX AG • Kaiserstrasse • D-67722 Langmeil • Tél. : +49 6302 9816-103 • sales@mobotix.com • www.mobotix.com