

MOBOTIX HUB – Guide des certificats

V2.04

Table des matières

	1	DROITS D'AUTEUR, MARQUES DE COMMERCE ET CLAUSE DE NON-RESPONSABILITÉ
	2	À PROPOS DE CE GUIDE
	3	QUAND AVEZ-VOUS BESOIN D'INSTALLER DES CERTIFICATS ?
	4	INTRODUCTION AUX CERTIFICATS
	4.1	CERTIFICAT DISTRIBUTION
	5	VUE D'ENSEMBLE DES SCÉNARIOS ET DES PROCÉDURES UTILISÉS AVEC CERTIFICATS 10
	5.1 5.2 5.3 5.4 5.5 5.6 5.7	SERVEUR MOBILE MOBOTIX HUB.10SERVEUR DE GESTION ET SERVEUR D'ENREGISTREMENT MOBOTIX HUB.10CERTIFICAT D'AUTORITÉ DE CERTIFICATION D'UN TIERS OU D'UN ORGANISME COMMERCIAL11DOMAINE11GROUPE DE TRAVAIL11SERVEUR D'ÉVÉNEMENTS MOBOTIX HUB11CLIENT11
	6	QUELS CLIENTS ONT BESOIN DE CERTIFICATS ?
	7	CONFIGURATEUR DE SERVEUR (EXPLIQUÉ) 15
	7.1 7.2 7.3 7.4	Certificat de serveur 16 Serveur d'événements et add-ons 17 Certificat de diffusion multimédia en continu 17 Certificat de diffusion multimédia mobile 17
	8	SCRIPTS POWERSHELL
	9	CRÉATION ET DISTRIBUTION MANUELLES DE CERTIFICATS 19
	9.1 9.2	IMPORTANT À SAVOIR :
	10	INSTALLER LES CERTIFICATS SUR LES CLIENTS
	11	CRÉER UN CERTIFICAT SSL
Mx_GL_	MX_H XPro	IUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 2/131Guide des certificats - Milestone XProtect® VMSGuide des certificates - VMSGuide des certificates - Milestone XProtect® VMSGuide des certificates - Milestone XProtect

MOBOTIX HUB – Guide des certificats - Error! Use the Home tab to apply

12	IMPORTER UN CERTIFICAT SSL	32
12.1	GÉRER LES CLÉS PRIVÉES	38
13	CRÉATION D'UN CERTIFICAT SSL POUR LE SERVEUR DE GESTION DE BASCULEMENT	40
14	INSTALLER CERTIFICATS POUR LA COMMUNICATION AVEC LE SERVEUR MOBILE	42
14.1	AJOUTER UNE AUTORITÉ DE CERTIFICATION CERTIFICAT VERS LE SERVEUR	42
14.2	TÉLÉCHARGEZ LE FICHIER .REQ POUR RECEVOIR UN CERTIFICAT SIGNÉ EN RETOUR	51
14.3	ACTIVER LE CHIFFREMENT SUR LE SERVEUR MOBILE	54
15 LA C	INSTALLER DES CERTIFICATS D'AUTORITÉ DE CERTIFICATION TIERS OU COMMERCIAUX COMMUNICATION AVEC LE SERVEUR DE GESTION OU LE SERVEUR D'ENREGISTREMENT	POUR 56
15.1	AJOUTER UN CERTIFICAT D'AUTORITÉ DE CERTIFICATION AU SERVEUR	56
15.2	TÉLÉCHARGEZ LE FICHIER .REQ POUR RECEVOIR UN CERTIFICAT SIGNÉ EN RETOUR	65
15.3	ACTIVER LE CHIFFREMENT VERS ET DEPUIS LE SERVEUR DE GESTION	68
15.3.	.1 CONDITIONS PRÉALABLES:	68
15.3.	.2 Pour installer AD CS :	70
15.4	INSTALLER DES CERTIFICATS DANS UN DOMAINE POUR LA COMMUNICATION AVEC LE SERVEUR DE GESTI	ON OU LE
SERVE	EUR D'ENREGISTREMENT	81
15.4.	.1 AJOUTER UN CERTIFICAT D'AUTORITÉ DE CERTIFICATION AU SERVEUR	82
15.4.	.2 TÉLÉCHARGEZ LE FICHIER .REQ POUR RECEVOIR UN CERTIFICAT SIGNÉ EN RETOUR	91
15.5	INSTALLER LE CERTIFICAT MANUELLEMENT	94
15.5.	.1 ACTIVER LE CHIFFREMENT DU SERVEUR POUR LES SERVEURS DE GESTION ET LES SERVEURS	
D'ENF	REGISTREMENT	97
16 СОМ	INSTALLER CERTIFICATS DANS UN ENVIRONNEMENT DE GROUPE DE TRAVAIL POUR IMUNICATION AVEC LE SERVEUR DE GESTION OU LE SERVEUR D'ENREGISTREMENT.	LA 99
16.1	AJOUTER UN CERTIFICAT D'AUTORITÉ DE CERTIFICATION AU SERVEUR	99
16.1.	.1 TÉLÉCHARGEZ LE FICHIER .REQ POUR RECEVOIR UN CERTIFICAT SIGNÉ EN RETOUR	107
16.1.	.2 ÉMETTRE DES CERTIFICATS MANUELLEMENT	111
16.1.	.3 ACTIVER LE CHIFFREMENT DU SERVEUR POUR LES SERVEURS DE GESTION ET LES SERVEURS	
D'ENF	REGISTREMENT	117
16.2	INSTALLER DES CERTIFICATS POUR LA COMMUNICATION AVEC L'EVÈNEMENT SERVEUR	118
16.3	ACTIVER CHIFFREMENT DU SERVEUR D'ÉVÉNEMENTS MOBOTIX HUB	118
16.3.	.1 CONDITIONS PRÉALABLES:	118
16.3.	.2 IMPORTER DES CERTIFICATS CLIENTS	120
1.	TÉLÉCHARGER LA CHAÎNE DE CERTIFICATS DE L'AUTORITÉ DE CERTIFICATION	121
16.4	AFFICHER I 'ÉTAT DU CHIFFREMENT POUR I ES CLIENTS	

MX_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 3/ 131Guide des certificats - Milestone XProtect® VMSGuide des certificates des certificates - Milestone XProtect® VMSGuide des certificates - Milestone XProtect® XProtect[®] VMS

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

Droits d'auteur © 2025 MOBOTIX AG

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'apporter des modifications 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 HUB.

2 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 ordinateurs clients qui font confiance aux certificats sont moins vulnérables aux attaques.

3 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

4 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 construites avec MIP SDK 2018 R3 ou version antérieure qui accèdent 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- En cas de doute, Demandez à votre fournisseur qui a fourni l'intégration

4.1 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 pour sécuriser la communication avec le serveur de gestion.



❶ Un certificat d'autorité de certification agit en tant que tiers de confiance, approuvé à la fois par le sujet/propriétaire (serveur de gestion) et par la partie qui vérifie le certificat (serveurs d'enregistrement) 🕑 Le certificat de l'autorité de certification doit être approuvé sur tous les serveurs d'enregistrement. De cette façon, les serveurs d'enregistrement peuvent vérifier la validité des certificats émis par l'autorité de certification Le certificat CA est utilisé pour établir une connexion sécurisée entre le serveur de gestion et les serveurs d'enregistrement

🕑 Le certificat de l'autorité de certification doit être installé sur l'ordinateur sur lequel le serveur de gestion s'exécute

Conditions requises pour le certificat de serveur de gestion privé :

- Attribué au serveur de gestion afin que le nom d'hôte du serveur de gestion 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 le serveur de gestion lui-même, en approuvant le certificat de l'autorité de certification utilisé pour émettre le certificat du serveur de gestion
- Approuvé sur tous les serveurs d'enregistrement connectés au serveur de gestion, en approuvant le certificat de l'autorité de certification utilisé pour émettre le certificat du serveur de gestion

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 8/ 131Guide des certificats - Milestone XProtect® VMSGuide des certificates - Milestone XProtect® VMSGuide des cer XProtect[®] VMS



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

5 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 :

5.1 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.

5.3 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:

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

5.4 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

5.5 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

5.7 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

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 ? 6

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.

Third Party CA/ Domain	Self Signed CA / Domain
Third Party CA/ Non-Domain	Self Signed CA/ Non-Domain

No Public Key Distribution Needed

Public Key Distribution Needed

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 13/ 131Guide des certificats - Milestone XProtect® VMSGuide des c XProtect® VMS

MOBOTIX HUB - Guide des certificats - Quels clients ont besoin de certificats ?

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.

7 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

MOBOTIX HUB - Guide des certificats - Configurateur de serveur (expliqué)

Milestone Server Configurator		7	
Encryption	Encryption		
Registering servers	It is recommended to secure communication with encryptic	n, <u>Learn m</u>	ore
Language selection	Server certificate Applies to: management server, recording server, failover server, data collector		
	Encryption: On	0	
	DocCert1	2	Details
	Certificate issued by mit-MJT-DC-CA, DC=mit, DC=local. Expires 4/27/2022		
	Mobile streaming media certificate Applies to mobile and web clients that retrieve data streams from the server	mobile	
	Encryption: On		
	DocCert1	*	Details
	Certificate issued by mjt-MJT-DC-CA, DC =mjt, DC=local. Expires 4/27/2022		
			Apply

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.

Certificat de serveur 7.1

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 •

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 16/ 131Guide des certificats - Milestone XProtect® VMSGuide des certificates XProtect[®] VMS

^{7,2} 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.

73 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.

74 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.

8 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.

9 Création et distribution manuelles de certificats

9.1 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).
- 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.

9.2 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.

1	CreateCACertificate.ps1 - Notepad	
ile Edit Format View Help		
Run this script once, to create Private certificate for signing ica_certificate = New-SelfSignedC KeyUsage CertSign, CRLSign, Digi Thumbprint of private certifica tet-Content -Path "\$PSScriptRoot\ Public CA certificate to trust ixport-Certificate -Cert "Cert:\C	a certificate that can sign multiple recording server certificates other certificates (in certificate store) ertificate -CertStoreLocation cert:\CurrentUser\My -DnsName 'VMS Certificate talSignature -FriendlyName 'VMS CA Certificate' te used for signing other certificates ca_thumbprint.txt" -Value \$ca_certificate.Thumbprint (Third-Party Root Certification Authorities) urrentUser\My\\$(\$ca_certificate.Thumbprint)" -FilePath "\$PSScriptRoot\root-r	e Authority' -KeyusageProperty All ` authority-public.cer"
		3
		Lo 9 Col 120

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.

			Cert				
File Open <u>n</u> ew window	•	Open Windows PowerShell	Open +	Select all			
Open command prompt	+	Open Windows PowerShell as <u>a</u> dministrator	Properties History Open	Select			
Open Windows Powe <u>r</u> Shell							
			Date modified	Туре	Size		
Delete mistory			04-02-2019 11:31	File folder			
			04-02-2019 11:31	File folder			
Teib			04-02-2019 11:31	File folder			
¥			04-02-2019 11:31	File folder			
Liose			04-02-2019 11:31	File folder			
			04-02-2019 11:31	File folder			
Second and a second		i CreateCACertificate.ps1	31-01-2019 15:01	Windows PowerShell Script		1 KB	
🖳 This PC							

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

🛃 Admin	istrator: Windows Pov	werShell				×
PS C:\Cert	:ificates> .\CreateCACertificate.ps1					^
Direct	tory: C:\Certifi	cates				
lode	LastW	riteTime	Length	Name		
				and a second		

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



10 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.



Voir Importer les certificats clients à la page 129 pour une procédure alternative à Installation de certificats sur les clients.

8. Copiez le root-authority-public.cer à partir de l'ordinateur sur lequel vous avez créé le certificat d'autorité de certification (c :\Certificats\root-authority-public.cer) à 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 nécessitent le certificat, voir Introduction aux certificats à la page 5.



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

Certificate Import Wizard Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
Stars Location	
Store Location	
<u>Current User</u> <u>Éacal Machine</u>	
To continue, click Next.	

- 10. Dans l'**Assistant Importation** de certificat, choisissez d'installer le certificat dans le magasin de l'**ordinateur local** et cliquez sur **Suivant**.
- 11. Sélectionnez cette option pour localiser manuellement le magasin dans lequel le certificat sera installé.

Certificate Store			
Certificate stores are	system areas where cert	ficates are kept.	
Windows can automat the certificate. O A <u>u</u> tomatically s Place all certific	cally select a certificate : lect the certificate store ites in the following store	store, or you can spec based on the type of	ify a location for certificate
Certificate stor	25		Browse

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



13. 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.

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 24/ 131Guide des certificats - Milestone XProtect® VMSGuide des certificates XProtect[®] VMS

Completing th	e Certificate Import Wizard
The certificate will be in	mported after you click Finish.
You have specified the	following settings:
Certificate Store Sele Content	ected by User Trusted Root Certification Authorities Certificate

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



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



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

New Ctrl+N		1
Save Ctrl+S	Name	Actions
Save As	There are no items to show in this view.	Console Root
Add/Remove Snap-in Ctrl+M	1	More Actions
Options		
Recent File		
Exit		

17. Sélectionnez le composant logiciel enfichable Certificats et cliquez sur Ajouter.

inap-in	Vendor	^	Console Root	Edit Extensions
ActiveX Control	Microsoft Cor			Eendre
Component Services	Microsoft Cor			(Mpristp)
Device Manager	Microsoft Cor Microsoft Cor	ſ	Add >	There Ban-
Event Viewer	Microsoft Cor	-		
Group Policy Object	Microsoft Cor			
Internet Informatio	Microsoft Cor Microsoft Cor			
IP Security Monitor	Microsoft Cor			Advanced
scription:				

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

Certificates snap-in	×
This snap-in will always manage certificates for:	
<u>My</u> user account <u>Service account</u>	
Computer account	

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

ect Computer	
Select the computer you want this snap-in to manage.	
This snap-in will always manage:	
Ocal computer: (the computer this console is running on)	
O Another computer:	Byzane
only applies if you save the console.	
only applies if you save the console.	
only applies if you save the console.	

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

ailable <u>s</u> nap-ins:			Selected snap-ins:		
nap-in	Vendor	^	Console Root	Edit Extens	ions
ActiveX Control	Microsoft Cor		Certificates (Local Computer)	Lend.	8
Authorization Manager	Microsoft Cor				-
Certificates	Microsoft Cor			_	
Component Services	Microsoft Cor			Inforts i	to.
Computer Managem	Microsoft Cor				
Device Manager	Microsoft Cor		5	under D	
Disk Management	Microsoft and				
Event Viewer	Microsoft Cor				
Folder	Microsoft Cor				
Group Policy Object	Microsoft Cor				
Internet Informatio	Microsoft Cor				
Internet Informatio	Microsoft Cor				
IP Security Monitor	Microsoft Cor	v		Advance	ed
scription:					
Cortificator man in alle	we you to browse	the	of the certificate stores for yourself a service	or a computer	-

21. Vérifiez que le certificat est répertorié dans la vue centrale des autorités de certification racine approuvées

sous-arbre.

© MOBOTIX AG www.mobotix.com

WDBOTTA AG WWW.FINODOTIX.com Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 28/131Guide des certificats - Milestone XProtect® VMSGuide des certificates - Milesto XProtect[®] VMS

Eile Action View Favorites Window He	lp				- B
File Action View Favgrites Window He Image: State of the sta	Ip Issued To 10.5,14.40 10.5,6,101 AddTrust External CA Root Baltimore CyberTrust Root CKMS Cass 3 Public Primary Certificat Copyright (c) 1997 Microsoft C DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert High Assurance EV Ro DigiCert Bight Bight Assurance EV Ro DigiCert Bight	Issued By 10.5.14.40 10.5.6.101 AddTrust External CA Root Baltimore CyberTrust Root CKMS Class 3 Public Primary Certificatio Copyright (c) 1997 Microsoft Corp. DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert High Assurance EV Root DST Root CA X3 Equifax Secure Certificate Authority GeoTrust Global CA GlobalSign GlobalSign GlobalSign	Exp * 20: 20: 20: 20: 20: 20: 20: 20:	Actions Certificates More Actions	
Smart Card Trusted Roots Trusted Devices Web Hosting Windows Live ID Token Issuer	Go Dady Class 2 Certification Go Dady Class 2 Certification GTE CyberTrust Global Root Hotspot 2.0 Trust Root CA - 03 Microsoft Root Authonity Microsoft Root Certificate Auth Microsoft Root Certificate Auth Microsoft Root Certificate Auth Microsoft Root Certificate Auth Starfield Class 2 Certification A Starfield Class 2 Certification A Starfield Services Root Certificat Symantec Enterprise Mobile Ro C	Go Daddy Class 2 Certification Au GTE CyberTrust Global Root Hotspot 2.0 Trust Root CA - 03 Microsoft Authenticode(tm) Root Microsoft Root Certificate Authori Microsoft Root Certificate Authori Microsoft Root Certificate Authori Microsoft Root Certificate Authori Starfield Class 2 Certification Auth Starfield Services Root Certificate Symantec Enterprise Mobile Root	202 203 204 204 204 204 204 204 205 205 205 205 205 205 205 205 205 205		

22. 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.

11 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).

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

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'annexe B à la fin de ce guide vous propose un script de création de certificats de serveur.

1. 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.

2. 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.

- 3. Dans l'Explorateur de fichiers, accédez à C :\Certificates et sélectionnez le fichier CreateServerCertificate.ps1.
- 4. Dans le menu Fichier, sélectionnez Ouvrir Windows PowerShell, puis Ouvrir Windows PowerShell en tant qu'administrateur.

Open <u>n</u> ew window	*	Open Windows F	PowerShell	☐ Open •	E Select all		
Open command <u>p</u> rompt	÷	Open Windows F	owerShell as administrator	Properties + History Open	Select		
Open Windows Powe <u>r</u> Sh	ell 🕨						
D				Date modified	Туре	Size	
				04-02-2019 11:	31 File folder		
and a second sec				04-02-2019 11:	31 File folder		
Пеір				04-02-2019 11:	31 File folder		
a second				04-02-2019 11:	31 File folder		
Close				04-02-2019 11:	53 File folder		
				04-02-2019 11:	31 File folder		
6. J.			ReateCACertificate.ps1	31-01-2019 15:	01 Windows PowerS	hell Script	1 K
🜉 This PC			CreateServerCertificate.ps1	25-01-2019 15:	31 Windows PowerS	hell Script	3.K

- 5. Dans PowerShell, à l'invite, entrez .\CreateServerCertificate.ps1 et appuyez sur Entrée.
- 6. 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.

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 30/ 131Guide des certificats - Milestone XProtect® VMSGuide des c XProtect® VMS



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**.



7. 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**.

8. 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.

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

12 Importer un certificat SSL

1

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

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

- 10. 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.
- 11. Sur l'ordinateur de service serveur, démarrez Gérer les certificats de l'ordinateur.
- 12. Cliquez sur **Personnel**, cliquez avec le bouton droit de la souris sur **Certificats** et sélectionnez **Toutes les tâches** > **importer**.



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

4	Certificate Import Wizard	
	Welcome to the Certificate Import Wizard	
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
	Store Location	
	Local Machine	
	To continue, dick Next.	
	QNext Canc	el

14. Accédez au fichier de certificat et cliquez sur Suivant.

Specify the file you want to import.	
File name:	
C: Users gis Documents My Receive	ed Files WMS-REC-01.pb
Note: More than one certificate can	be stored in a single file in the following formats:
Personal Information Exchange- P	KCS #12 (.PFX,.P12)
Cryptographic Message Syntax St	tandard-PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Sto	ore (.SST)

15. 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**.

1	Private key protection
	To maintain security, the private key was protected with a password.
	Type the password for the private key.
	Password:

	Display Password
	Import options:
	Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
	Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
	✓ Include all extended properties.

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

Certificate S	itore		2014	
Certific	ate stores are syst	tem areas where (certificates are kept	t,
Window	us can automatical	ly select a certific:	ate store, or you ca	n specify a location fr
the cer	tificate.	ly select a cer unca	ste store, or you ca	in specify a location in
0	Automatically selec	t the certificate st	tore based on the t	/pe of certificate
	Place all certificates	s in the following s	store	
ę	Certificate store:			
	Personal			Browse

17. Vérifiez les informations et cliquez sur Terminer pour importer le certificat.
| You have specified the following settings:
Certificate Store Selected by User Personal |
|---|
| Certificate Store Selected by User Personal |
| Content PFX
File Name C;\Users\gis\Desktop\VMS-REC-01.pfx |
| |

Le certificat importé apparaît dans la liste.

• 🔿 🚈 🔟 🖬 🖌 🖬 👘		
 Certificates - Local Computer Personal Certificates Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Trusted People Client Authentication Issuers Homegroup Machine Certificates MSIEHistoryJournal OfcEdge OfficeScan SSL Agent 	Issued To	Issued By Iocalhost VMS Certificate Authority VMS Certificate Authority

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

12.1 Gérer les clés privées.

Open
Request Certificate with New Key
Renew Certificate with New Key
Manage Private Keys
Advanced Operations
Export

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

roup or user names:		
SYSTEM		
Administrators (Administrator	5)	_
	Add	Remove
ermissions for NETWORK ERVICE	Allow	Deny
Full control		
Read	Ð	
Special permissions		
	ed settings,	Advanced
or special permissions or advance		Auvancou

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

13 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.

- 3. Dans l'annexe C de ce guide, copiez le script de création des certificats de serveur de gestion de basculement.
- 4. 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.

- 5. 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.
- 6. Dans l'Explorateur de fichiers, accédez à C :\Certificates et sélectionnez le fichier CreateFailoverCertificate.ps1.
- 7. Dans le menu Fichier, sélectionnez Ouvrir Windows Powershell, puis Ouvrir Windows PowerShell en tant qu'administrateur.

File						
Open <u>n</u> ew window	*	Open Windows PowerShell	Dpen •	Select all		
Open command <u>p</u> rompt	*	Open Windows PowerShell as administrator	Properties + Upen	Select:		
Open Windows Powe <u>r</u> Shell						
D			Date modified	Туре	Size	
	'		04-02-2019 11:	31 File folder		
the last			04-02-2019 11:	31 File folder		
Деір			04-02-2019 11:	31 File folder		
			04-02-2019 11:	31 File folder		
Liose			04-02-2019 11:	53 File folder		
			04-02-2019 11:	31 File folder		
6. J.		🧟 CreateCACertificate.ps1	31-01-2019 15:	01 Windows PowerShell Scrip	b.	1
🜉 This PC		CreateServerCertificate.p	os1 25-01-2019 15:	31 Windows PowerShell Scrip	t	3
- Deskton						

- 8. Dans PowerShell, entrez .\CreateFailoverCertificate.ps1 à l'invite et appuyez sur Entrée.
- 9. Spécifiez les noms de domaine complets et les noms d'hôte de l'ordinateur principal et de l'ordinateur secondaire, séparés par une virgule.

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 40/ 131Guide des certificats - Milestone XProtect® VMSGuide des c XProtect® VMS

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

- 10. Appuyez sur Entrée.
- 11. Spécifiez l'adresse IP virtuelle du cluster de basculement. Appuyez sur **Entrée**.
- 12. 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.

14 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



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

données.



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

14.1 Ajouter un certificat d'autorité de certification au serveur

Ajoutez le certificat d'autorité de certification au serveur mobile en procédant comme suit Sur l'ordinateur qui héberge le serveur mobile, ouvrez la console de gestion Microsoft.



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

	Type the na	ame of a progr	am, folder, docur	ment, or Internet
	resource, an	nd Windows w	vill open it for you	1.
<u>)</u> pen:	mmd			,

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



Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 42/ 131Guide des certificats - Milestone XProtect® VMSGuide des c XProtect® VMS

MOBOTIX HUB – Guide des certificats - Installer des certificats pour la communication

Open Ctrl+O	I NOT	A
Save Ctrl+S	Name There are no items to show in this view	Actions Console Root
Save As		More Actions
Options Ctri+M		
Recent File		
Exit		

- 2. Sélectionnez le composant logiciel enfichable Certificats et cliquez sur Ajouter.
- 3. Cliquez sur OK.

Snap-in Vendor Console Root Edit Extension ActiveX Control Microsoft Cor Certificates - Current User Remove Certificate Templates Microsoft Cor Certificates - Current User Remove Certificates Microsoft Cor Add > Certificates Microsoft Cor Add > Component Services Microsoft Cor Add > Computer Managem Microsoft Cor Add > Device Manager Microsoft Cor Add > Enterprise PKI Microsoft Cor Add > Enterprise PKI Microsoft Cor Add > Folder Microsoft Cor Add >				Selected snap-ins;	
ActiveX Control Microsoft Cor Authorization Manager Microsoft Cor Certificates Microsoft Cor Certificates Microsoft Cor Certification Authority Microsoft Cor Component Services Microsoft Cor Computer Manager Microsoft Cor Device Manager Microsoft Cor Disk Management Microsoft Cor Enterprise PKI Microsoft Cor Folder Microsoft Cor	Snap-in	Vendor	^	Console Root	Edit Extensions.
Authorization Manager Microsoft Cor Certificate Templates Microsoft Cor Certificates Microsoft Cor Certification Authority Microsoft Cor Component Services Microsoft Cor Computer Managem Microsoft Cor Device Manager Microsoft Cor Disk Management Microsoft Cor Enterprise PKI Microsoft Cor Event Viewer Microsoft Cor Folder Microsoft Cor	ActiveX Control	Microsoft Cor		Certificates - Current Us	Remove
Image: Certificate Templates Microsoft Cor Image: Certificates Microsoft Cor Image: Certification Authority Microsoft Cor Image: Certification Authority Microsoft Cor Image: Component Services Microsoft Cor Image: Computer Managem Microsoft Cor Image: Certification Computer Management Microsoft Cor Image: Certification Cert	Authorization Manager	Microsoft Cor			Traction Fragment
Certificates Microsoft Cor Certification Authority Microsoft Cor Component Services Microsoft Cor Computer Managem Microsoft Cor Device Manager Microsoft Cor Disk Management Microsoft Cor Enterprise PKI Microsoft Cor Event Viewer Microsoft Cor Folder Microsoft Cor	Rertificate Templates	Microsoft Cor			
Image: Certification Authority Microsoft Cor Component Services Microsoft Cor Computer Managem Microsoft Cor Device Manager Microsoft Cor Disk Management Microsoft Cor Enterprise PKI Microsoft Cor Event Viewer Microsoft Cor Folder Microsoft Cor	Certificates	Microsoft Cor			10000
Component Services Microsoft Cor Computer Managem Microsoft Cor Device Manager Microsoft Cor Disk Management Microsoft Cor Enterprise PKI Microsoft Cor Event Viewer Microsoft Cor Folder Microsoft Cor	Certification Authority	Microsoft Cor			Marine Concer
Computer Managerian Microsoft Conner Device Managerian Microsoft Conner Disk Management Microsoft Conner Enterprise PKI Microsoft Conner Event Viewer Microsoft Conner Folder Microsoft Conner	Computer Manadem	Microsoft Cor	Add :	>	
Disk Management Microsoft and Enterprise PKI Microsoft Cor Event Viewer Microsoft Cor Folder Microsoft Cor	Device Manager	Microsoft Cor			
Enterprise PKI Microsoft Cor Event Viewer Microsoft Cor Folder Microsoft Cor	Disk Management	Microsoft and			
Event Viewer Microsoft Cor Folder Microsoft Cor	Enterprise PKI	Microsoft Cor			
Folder Microsoft Cor	Event Viewer	Microsoft Cor			
Provide Different Manual Con	Folder	Microsoft Cor			
Group Policy Object Microsoft Cor	Group Policy Object	Microsoft Cor	~		Advanced
Description:	Description:				
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.	The Certificates snap-in all	ows you to browse	the contents	of the certificate stores for yourself, a	service, or a computer.

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 43/ 131Guide des certificats - Milestone XProtect® VMSGuide des certificates - Milestone XProtect® VMSGuide des ce

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.

🔌 🙋 📷 🗎 🖌 🐼 📾 🖬				
Console Root Certificates - Current User	Object T	Type ficates		
Find Certificates				
En All Tasks	>	Find Certificates		
Ac View	*	Request New Certificate Import		
Th New Taskpad View		Advanced Operations	×	Create Custom Request
Tru Refresh				Enroll On Behalf Of Manage Enrollment Policies
Sn Help				

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

- 🗆 X

Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by you	Add New
Custom Request	
Proceed without enrollment policy	
	Next Cance
	- Here Conce

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

Custom request		
Chose an option fron	the list below and configure the certificate option	is as required.
Template:	(No template) CNG key	
	Suppress default extensions	
Request format:	○ <u>P</u> KCS #10	
	● <u>C</u> MC	
Note: Key archival is	not available for certificates based on a custom cer	rtificate request, even when
option is specified in	the certificate template.	

- Suivant.
- 8. Développez le champ d'affichage des détails de la demande personnalisée, puis cliquez sur Propriétés.
- 9. Dans l' onglet Général, remplissez les champs Nom convivial et Description avec le nom de domaine enregistré auprès de l'autorité de certification.



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

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 45/ 131Guide des certificats - Milestone XProtect® VMSGuide des c XProtect[®] VMS

MOBOTIX HUB – Guide des certificats - Installer des certificats pour la communication

ertificat	e Propen					
General	Subject	Extensions	Private Key	Signature		
A friend	lly name	and descript	tion will make	e it easier to iden	tify and use a certi	ficate.
Friendly	name:					
TestLak	Domain	.com				
Descript	tion:					
TestLat	Domain	.com				
				OK	Cancel	Apply

10. 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 :

ertificat	e Propert	ties				×
General	Subject	Extensions	Private Key	Signature		
The sub can ent can be	oject of a er inform used in a	certificate is lation about certificate.	the user or c the types of :	omputer to w subject name	hich the certif and alternativ	icate is issued. You e name values that
Subject	of certifi	cate				
The use	r or com	puter that is	receiving the	certificate		
Subject	name:		2 T - 1			
Туре:					CN=Test fo	or Docs
Count	ry		0	Add	OEMJT L	ab
Value:			×	Remove	L=Maple G S=MN C=USA	rove
Alternat	tive name	e;	4			
Туре:						
Direct	ory name		-			
Value:				Add >		
			10	Remove		
-						
				OK	Cano	tel Apply

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

and the second second					2
General Subject Extensions	Private Key	Signature			
The following are the certific	ate extension	s for this cer	rtificate type.		^
Key usage				^	
The key usage extension des	scribes the pu	rpose of a c	ertificate.		
Available options:			Selected options:	-	
CRL signing Data encipherment			Digital signature Key certificate signing		
Encipher only Key agreement	Ac	id >	Key encipherment		
Non repudiation	< Re	emove			
☑ Make these key usages cr	itical			_	
Extended Key Usage (applic	ation policies)		*	i
Extended Key Usage (applic Basic constraints	ation policies)		* *	~

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

Ì

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

MOBOTIX HUB – Guide des certificats - Installer des certificats pour la communication

ertificate P	roperti	ies					×
Seneral Su	bject	Extensions	Private Key	Signature			
Cryptogra	aphic S	Service Prov	ider				۲
Key optio	ons						*
Set the key	y lengt	h and expo	rt options for	the private k	ey.		
Key size:	2048				~		
Make p	rivate	key exportal	ble				
Allowp	orivate	key to be an	chived				
Strong	nrivate	key protec	tion				
	private	ney protec	lion				
Select Ha	ch Ala	orithm					
Select Has	sh Alac	orithm to be	used for the	request			
Hash Algo	prithm:	cha756				0	
-		51102.30			_		
Select Sig	inature	Format					~
Select Sig	mature	Format					

- 14. À moins que l'autorité de certification n'exige une signature, l'étape suivante consiste à cliquer sur **OK**.
- 15. Une fois que toutes les propriétés du certificat ont été définies, cliquez sur **Suivant** dans l'Assistant **Inscription de certificat**.

Certificate Enroll	ment
--------------------	------

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

Key usage:	Digital signature Key certificate signing	
Application polic	Key encipherment ies:	
Validity period (d	lays):	
		Properties

16. 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.

MOBOTIX HUB - Guide des certificats - Installer des certificats pour la communication

quez sur Terminer.	
	- L
Certificate Enrollment	
Where do you want to save the offline request?	
If you want to save a copy of your certificate request or want to p to your hard disk or removable media. Enter the location and nan click Finish.	rocess the request later, save the reques ne of your certificate request, and then
File Name:	200000000000000000000000000000000000000
C:\Users\Administrator\Desktop\CSR6.1.21	Browse
Ella fannati	
File format:	
Base 64	
 Base 64 Binary 	

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

14.2 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.

© MOBOTIX AG www.mobotix.com

Ì

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 51/131Guide des certificats - Milestone XProtect® VMSGuide des c XProtect[®] VMS

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.

CSR6.1.21 - Notepad

X

File Edit Format View Help

----BEGIN NEW CERTIFICATE REQUEST-----

MIIGBAYJKoZIhvcNAQcCoIIF9TCCBfECAQMxDzANBglghkgBZQMEAgEFADCCBEoG CCsGAQUFBwwcoIIEPASCBDgwggQ0MGQwYgIBAgYKKwYBBAGCNwoKATFRME8CAQAw AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QLTBBMDAwNDY3DB1JUC0wQTAw MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRVhFMIIDxqCCA8ICAQEwgg07MIICowIB ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAgMAk10MRQwEgYDVQQHDAtNYXBsZSBH cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UECgwDTUpUMRYwFAYDVQQDDA1U ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7G1/ 5z1YrUGOo4dW1/b3o35rpcQQbyOUE0K1NWjaIy4YrRPM9HjhKReThbcSnxddj6eR Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ//Zi08bEPobLv8YnWieNDuw lkaJWWRx3mbl/Yz0f1bwZrKFT3nkrXYOFYmZOR19W0J+Iin0BtziwiC8DHt+bxST nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9gC47RP9yMjyuuEtpdR9ERoR qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs18zBATRXkk/kRI+Po6cXNJp Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEAYI3DQIDMQ4WDDEwLjAuMTc3 NiMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/wQEAwICpDAdBgNVHQ4EFgQU vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCNxUUMTYwNAIBBQwLSVAtMEEw MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b3IMB01NQy5FWEUwZgYKKwYB BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMAbwBmAHQAdwBh AHIAZQAgAEsAZQB5ACAAUwB0AG8AcgBhAGcAZQAgAFAAcgBvAHYAaQBkAGUAcgMB ADANBgkqhkiG9w0BAQsFAAOCAQEAqtKb5HCh2a1BD2QcKdFuhVQbNxg+G5wcVkZt 7bXdwVuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJCcxRZeTKPBFnHG0SeaYupUrG cX4ySsKR1xGSuOhsfIVa/5NXiIYgYxMh1z3nt2CDw+RNqAp/1gLV2cLsui01y5ib 088po4/b9eiXV7A1DWFy7ecw/7Z20a07Sa00aRbwzGJ8He1IiVEjfyAt7KLoufAg LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbcOxzVkPCQbiHOwSxDG1kqYHZ8Xru665Q6 0L7QgBXCc7tcecDieqbYmp50LJPpqEQDQiYjzg57j3eYIFNYYjAAMAAxggGLMIIB hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJYIZIAWUDBAIBBQCgSjAXBgkq hkiG9w0BC0MxCgYIKwYBB0UHDAIwLwYJKoZIhvcNAQkEMSIEICk1SKp5MUjMa+vr DU1UXU+V05r1F8bNdM0mDgYfmjCiMA0GCSqGSIb3DQEBAQUABIIBAEjqqe4GSGE4 oZQj0vbWrAP0Ab2u8epFm7ZIMZzsJSzR0z98m+R+1R2mCoqWC0SSafybJ701Jh1y A3eqzDYxAu9p9drJft317sGAERE/i1D3BFvKZZQH0sz0JNRwDp3qByHHzVCULUEI JSOpYvI1s3S23ZYEedQLp35Xy87378zLLGLpgGKTK4teav1IitUJwVCKikL47uyF uOY4XLagwI1WWALsPF1+5ZcVNZMvsgzsbuMEXvjBkFKyhMv49oisgFcLJ1AoMtWn 7Mbq8K6ckbKkVpuvmWThkVTp1W3hIS/i/J0X7c2unA25LxAC/P/LyWhPt/Vk/oqf 06jNaHC/zBQ=

-----END NEW CERTIFICATE REQUEST-----

Windows (CRLF Ln 1, Col 1 100%

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.

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 52/131Guide des certificats - Milestone XProtect® VMSGuide des certificates - Milestone XProtect® VMSGuide des cer XProtect® VMS

MOBOTIX HUB – Guide des certificats - Installer des certificats pour la communication

File Home S	nloads hare View			-	□ × * 0
< - ·↑↓,	This PC > Down	loads	v Ö	Search Downloads	Q
Desktop	^ Name	~	Date modif	ied Type	Size
 Documents Downloads Music Pictures Videos Local Disk (C:) 	🙀 certnew	Open Install Certificate ☐ Edit with Notepad++ ☆ Share Open with	E 110011	2:23 PM Security Cer	tificate
- Network	~ <	Give access to Restore previous versio	> ns		, s
1 item 1 item selecte	ed 1.11 KB	Send to	>		

X

- 3. Acceptez l'avertissement de sécurité s'il apparaît.
- 4. Sélectionnez cette option pour installer le certificat pour l'ordinateur local et cliquez sur **Suivant**.

Welcome to the (ertificate Import Wizard	
This wizard helps you copy lists from your disk to a ceri	ertificates, certificate trust lists, and certificate revo ficate store.	cation
A certificate, which is issued and contains information us connections. A certificate s	by a certification authority, is a confirmation of your ad to protect data or to establish secure network ore is the system area where certificates are kept.	identity
Store Location		
O Current User		
Local Machine		
To continue, click Next.		

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

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 53/ 131Guide des certificats - Milestone XProtect® VMSGuide des certificates XProtect[®] VMS

MOBOTIX HUB - Guide des certificats - Installer des certificats pour la communication

🗧 🔄 Certificate Import Wizard	*
Certificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location fo	
Automatically select the certificate store based on the type of certificate Place all certificates in the following store. Certificate store: Browse	Select Certificate Store × Select the certificate store you want to use.
Next	Show physical stores OK Cancel Cancel

6. Terminez l'assistant d'installation du certificat.

14.3 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.

MOBOTIX HUB – Guide des certificats - Installer des certificats pour la communication

Server Configurator		-		×
Encryption	Encryption			
Registering servers	It is recommended to secure communication with encryption. Le	arn m	iore	
anguage selection	Server certificate Applies to: management server, recording server, failover server, data collector			
	Encryption: On	0		
	-		Details	
	Camilicate inneed by MS-Organization-P2P-Accent [2027], https://di/2021.			
	Mobile streaming media certificate Applies to mobile and web clients that retrieve data streams from the mob server	ile		
	Encryption: On	9		
	No		Details	
	Certificate issued by Expires 5/3/2121			
			Apply	

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.

15 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.



Ì

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

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

15.1 Ajouter un certificat d'autorité de certification au serveur

Ajoutez le certificat de l'autorité de certification au serveur en procédant comme suit. Sur l'ordinateur qui héberge le serveur MOBOTIX HUB, ouvrez la console de gestion Microsoft.



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

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

😅 Run		×
e	Type the name of a program, folder, do resource, and Windows will open it for	cument, or Internet you.
Open:	mmd	Ý
	OK Cancel	<u>B</u> rowse

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 56/ 131Guide des certificats - Milestone XProtect® VMSGuide des c XProtect[®] VMS

MOBOTIX HUB – Guide des certificats - Installer des certificats d'autorité de

Save Ctrl+S Save As There are no items to show in this view. Add/Remove Snap-in Ctrl+M Options Recent File Exit Exit	
Add/Remove Snap-in Ctrl+M Options Recent File Exit	
Options Recent File Exit	
Recent File Exit	
Exit	

- 2. Sélectionnez le composant logiciel enfichable Certificats et cliquez sur Ajouter.
- 3. Cliquez sur **OK**.

	Mandan	~	Console Root	Edit Extensions
парни	vendor		Certificates - Current Use	Edit Externationation
ActiveX Control	Microsoft Cor			Remove
Authorization Manager	Microsoft Cor			
	Microsoft Cor			A housed by
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor	Internet		Talana Crean
Computer Managem	Microsoft Cor	Add >		
Device Manager	Microsoft Cor			
Disk Management	Microsoft and			
Enterprise PKI	Microsoft Cor			
Event Viewer	Microsoft Cor			
Folder	Microsoft Cor			
Group Policy Object	Microsoft Cor	*		Advanced
scription				
ha Carlificatas sans in alle	we you to browee	the contents of th	a contificate ateras for valuealf a	version or a computer
Group Policy Object	Microsoft Cor	*		Advanced

© MOBOTIX AG www

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 57/131Guide des certificats - Milestone XProtect® VMSGuide des certificates - Milestone XProtect® VMSGuide des cer XProtect[®] VMS

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.
- 6. Cliquez sur Suivant.

X П

Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by you	Add New
Custom Request	
Proceed without enrollment policy	
	Next Cance

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

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 58/ 131Guide des certificats - Milestone XProtect® VMSGuide des c XProtect[®] VMS

MOBOTIX HUB – Guide des certificats - Installer des certificats d'autorité de

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

X

Certificate Enrollment

Custom request

Chose an option from the list below and configure the certificate options as required.

Template:	(No template) CNG key
	Suppress default extensions
Request format:	O <u>P</u> KCS #10
	● <u>C</u> MC
Note: Key archival is option is specified in	not available for certificates based on a custom certificate request, even when this the certificate template.
	<u>N</u> ext Cancel
Le format de l incorrect, l'auto signature de co	a demande dépend de l'autorité de certification. Si le format choisi est orité de certification émettra une erreur lors de l'envoi de la demande de ertificat (CSR). Vérifiez auprès de l'autorité de certification pour vous

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

Subject Extensions Private N	ey signature		
A friendly name and description will m	hake it easier to ide	ntify and use a cert	ificate.
Friendly name:			
TestLabDomain.com			
Description:			
TestLabDomain.com			

- 10. Dans l'**onglet Objet**, entrez les paramètres requis par l'autorité de certification spécifique.
- 11. 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 :

ertificat	e Propert	ties			>
General	Subject	Extensions	Private Key	Signature	
The sub can ent can be	oject of a er inform used in a	certificate is ation about certificate.	the user or c the types of	omputer to w subject name	which the certificate is issued. You and alternative name values that
Subject	of certifi	cate			
The use	er or com	puter that is	receiving the	certificate	
Subject	name:				The second s
Туре:					CN=Test for Docs
Count	ny	4		Add:	OU=MJT Lab
Value:			×	Remove	L=Maple Grove S=MN C=USA
Alterna	tive name	2:			
Туре:					1
Direct	ory name	-	-		
Value:				Add >-	
) <	Remiave	
_					
				OK	Cancel Apply

 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.

Certificat	te Propert	ties					
General	Subject	Extensions	Private Key	Signature			
The fol	lowing an	e the certific	ate extension	is for this cer	tificate t	ype.	1
Key u	sage						
The ke	y usage e	extension des	cribes the pu	irpose of a ce	ertificate		_
Availa	ble option	15:			Select	ed options:	
CRL si Data e	gning ncipherm	nent	1		Digita Key c	al signature ertificate signi	ng
Decip	her only		-		Key e	ncipherment	
Encipł	ner only		A	dd >	1		
Key ac	reement		-				
⊠ Mal	ke these k	ey usages cr	itical				
Exten	ded Key U	lsage (applic	ation policie	s)			*
Basic	constrain	ts					¥

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

S

14. 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

MOBOTIX HUB – Guide des certificats - Installer des certificats d'autorité de

Leftificate P	ropert	ies				×
General S	ubject	Extensions	Private Key	Signature		
Cryptog	raphic	Service Prov	ider			۷
Key optio	ons					*
Set the ke	ey lengt	th and expo	rt options for	the private key.		
Key size:	2048			*	L	
Make p	orivate	key exportal	ble			
Allow	private	key to be an	chived			
Strong	private	e key protec	tion			
Select Ha	ash Alg	orithm				*
Select Ha	sh Algo	orithm to be	used for this	request		
Hash Alg	orithm	sha256			~	
Select Sig	gnature	e Format				~
Select Sig	gnature	e Format				v
Select Sig	gnature	e Format				v
Select Sig	gnature	e Format				¥

- 15. À moins que l'autorité de certification n'exige une signature, l'étape suivante consiste à cliquer sur **OK**.
- 16. Une fois toutes les propriétés du certificat définies, cliquez sur **Suivant** dans l'Assistant **Inscription de certificat**.

to use the options d then click Next.	s already selected for this template, or click Details to o	customize the certifi
m request	i) STATUS: Available	Detai
llowing options	describe the uses and validity period that apply to this	type of certificate:
ey usage:	Digital signature	
	Key certificate signing	
pplication policies	s:	
alidity period (day	rs):	
		Propertie
	m request ollowing options o ey usage: pplication policies alidity period (day	im request STATUS: Available billowing options describe the uses and validity period that apply to this ey usage: Digital signature Key certificate signing Key encipherment pplication policies: alidity period (days):

- 17. 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.
- 18. Cliquez sur **Terminer**.

Where do you want to save the offline request?	
f you want to save a copy of your certificate request or want to o your hard disk or removable media. Enter the location and n :lick Finish.	o process the request later, save the reque name of your certificate request, and then
ile Name:	Denter
CAUSERS (Administrator Desktop (CSN0, 1,21	Browse,,
-ile format:	
Base 64 Binary	
Base 64 Binary	

Finish

Cancel

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

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



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.

0

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 65/ 131Guide des certificats - Milestone XProtect® VMSGuide des c XProtect[®] VMS

CSR6.1.21 - Notepad

- 🗆 X

File Edit Format View Help -----BEGIN NEW CERTIFICATE REQUEST-----MIIGBAYJKoZIhvcNAQcCoIIF9TCCBfECAQMxDzANBg1ghkgBZQMEAgEFADCCBEoG CCsGAQUFBwwCoIIEPASCBDgwggQ0MGQwYgIBAgYKKwYBBAGCNwoKATFRME8CAQAw AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QLTBBMDAwNDY3DB1JUC0wQTAw MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRVhFMIIDxqCCA8ICA0Ewgg07MIICowIB ADBpM0wwCgYDV00GEwNVU0ExCzAJBgNVBAgMAk10MR0wEgYDV00HDAtNYXBsZSBH cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UECgwDTUpUMRYwFAYDVQQDDA1U ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7G1/ 5z1YrUG0o4dW1/b3o35rpcQQbyOUE0K1NWjaIy4YrRPM9HjhKReThbcSnxddj6eR Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ//Zi08bEPobLv8YnWieNDuw lkaJWWRx3mb1/Yz0f1bwZrKFT3nkrXY0FYmZ0R19W0J+Iin0BtziwiC8DHt+bxST nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9gC47RP9yMjyuuEtpdR9ERoR qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs18zBATRXkk/kRI+Po6cXNJp Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEAYI3DQIDMQ4WDDEwLjAuMTc3 NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/wQEAwICpDAdBgNVHQ4EFgQU vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCNxUUMTYwNAIBBQwLSVAtMEEw MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b3IMB01NQy5FWEUwZgYKKwYB BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMAbwBmAHQAdwBh AHIAZQAgAEsAZQB5ACAAUwB0AG8AcgBhAGcAZQAgAFAAcgBvAHYAaQBkAGUAcgMB ADANBgkqhkiG9w0BAQsFAAOCAQEAqtKb5HCh2a1BD2QcKdFuhVQbNxg+G5wcVkZt 7bXdwVuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJCcxRZeTKPBFnHG0SeaYupUrG cX4ySsKR1xGSuOhsfIVa/5NXiIYgYxMhlz3nt2CDw+RNqAp/1gLV2cLsui01y5ib 088po4/b9eiXV7A1DWFy7ecw/7Z20a07Sa00aRbwzGJ8He1IiVEjfyAt7KLoufAg LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbcOxzVkPCQbiHOwSxDG1kqYHZ8Xru665Q6 0L7QgBXCc7tcecDieqbYmp50LJPpqEQDQiYjzg57j3eYIFNYYjAAMAAxggGLMIIB hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJYIZIAWUDBAIBBQCgSjAXBgkq hkiG9w0BCQMxCgYIKwYBBQUHDAIwLwYJKoZIhvcNAQkEMSIEICk1SKp5MUjMa+vr DU1UXU+V05r1F8bNdM0mDgYfmjCiMA0GCSqGSIb3DQEBAQUABIIBAEjqqe4GSGE4 oZQj0vbWrAP0Ab2u8epFm7ZIMZzsJSzR0z98m+R+1R2mCoqWC0SSafybJ701Jh1y A3eqzDYxAu9p9drJft317sGAERE/i1D3BFvKZZQH0sz0JNRwDp3qByHHzVCULUEI JSOpYvI1s3S23ZYEedQLp35Xy87378zLLGLpgGKTK4teav1IitUJwVCKikL47uyF uOY4XLagwI1WWALsPF1+5ZcVNZMvsgzsbuMEXvjBkFKyhMv49oisgFcLJ1AoMtWn 7Mbg8K6ckbKkVpuvmWThkVTp1W3hIS/i/J0X7c2unA25LxAC/P/LyWhPt/Vk/ogf 06jNaHC/zBQ= -----END NEW CERTIFICATE REQUEST-----

81

Windows (CRLF Ln 1, Col 1 100%

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**.

MOBOTIX HUB – Guide des certificats - Installer des certificats d'autorité de

↓ ↓ ↓ ↓ Down File Home S	nloads hare View				□ × ○
< - · · · + .	This PC > Down	loads	võ Sei	arch Downloads	P
E Desktop	^ Name	~	Date modified	Туре	Size
 Documents Downloads Music Pictures Videos Local Disk (C:) 	Certnew	Open Install Certificate Edit with Notepad++ Share Open with	E/1/0011 12:23	PM Security Cert	ificate
Network	v e	Give access to Restore previous versi	> ons		, ×
1 item 1 item select	ed 1.11 KB	Send to	>		

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

🔮 Certificate Import Wizard

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

Welcome to the Certif	ficate Import Wizard
his wizard helps you copy certifica sts from your disk to a certificate	ates, certificate trust lists, and certificate revocation store.
A certificate, which is issued by a c and contains information used to p connections. A certificate store is t	ertification authority, is a confirmation of your identity rotect data or to establish secure network the system area where certificates are kept.
Store Location	
O Current User	
Local Machine	
To continue, click Next.	

X

© MOBOTIX AG www.mobotix.com Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 67/131Guide des certificats - Milestone XProtect® VMSGuide des cMifconBtoTIX XProtect® VMS

MOBOTIX HUB - Guide des certificats - Installer des certificats d'autorité de

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

Certificate Store	
Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location fo the certificate. Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Browse	Select Certificate Store Select the certificate store you want to use.
	Show physical stores

6. Terminez l'assistant d'installation du certificat.

15.3 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.

15.3.1 Conditions préalables:

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

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.

1

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 68/ 131Guide des certificats - Milestone XProtect® VMSGuide des c XProtect[®] VMS

Escalier:

- 7. 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
- 1. Dans le configurateur de serveur, sous Certificat de serveur, activez le cryptage.
- 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.
- 3. 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.
- 4. Sélectionnez **Détails** pour afficher les informations du Magasin de certificats Windows concernant le certificat sélectionné.

MOBOTIX HUB – Guide des certificats - Installer des certificats d'autorité de

incryption	Encryption		
egistering servers	It is recommended to secure communication with encryption. Learn more		
Language selection	Server certificate Applies to: management server, recording server, failover server, collector, api gateway, log server	data	
	Encryption: Off		
	Select certificate	~	
	No certificate selected		
	Streaming media certificate Applies to clients and servers that retrieve data streams from the recording server		
	Encryption: Off		
	Select certificate	~	
	No certificate salected		
	Mobile streaming media certificate Applies to mobile and web clients that retrieve data streams from server	the mobile	
	Encryption: Off		
	Select certificate	~	
	No certificate selected		
	No certificate selected		A

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)

15.3.2 Pour installer AD CS :

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

🔚 Server Manager		– 🗆 X
Server l	Manager • Dashboard	
🔛 Dashboard	WELCOME TO SERVER MANAGER	Remove Roles and Features Add Servers
Local Server All Servers File and Storage Services	1 Configure th	Create Server Group Dis local server Server Manager Properties
- The and storage services	QUICK START	

- 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.

	Select one or more roles to install on the	he selected server.	
-1 atten type	Roles	Description	
WWE LEIGTLON	Active Directory Certificate Ser	Active Directory Cer	tificate Services
	Ad Ad Ad Ad Ad Ad Certificate Services Di Fa The following tools are in have to be installed on th Ho Ho Ni Ni Ni Remote Server Adm Active Direct [Tools] Ce Re Re Re Vi Wi Wi Wi Ni Ni Ni Ni Ni Ni Ni Ni Ni N	are required for Active Directory required to manage this feature, but do not the same server. ministration Tools tion Tools tory Certificate Services Tools ertification Authority Management Tools	you to issue is used in a
		contract data sector and	Cancel

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 71/131Guide des certificats - Milestone XProtect® VMSGuide des certificates XProtect[®] VMS

MOBOTIX HUB – Guide des certificats - Installer des certificats d'autorité de

- 6. Cliquez sur **Suivant**.
- 7. Dans **Fonctionnalités**, cliquez sur **Suivant**. Toutes les fonctionnalités requises sont sélectionnées pour l'installation.
- 8. Dans AD CS, lisez la description des services certifiés Active Directory, puis cliquez sur Suivant.
- 9. 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.

Select Tole Sel V	Select the role services to install for Artive Directory Cer	IP-0A00049
Installation Type Server Selection Server Roles Features AD CS Role Services	Role services Certification Authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Certification Authority Web Enrollment Network Device Enrollment Service Online Responder	Description Network Device Enrollment Service makes it possible to issue and manage certificates for routers and other network devices that do not have network accounts.
Web Server Role (IIS) Role Services Confirmation		

- 10. Cliquez sur **Suivant**.
- 11. Dans Confirmation, sélectionnez Redémarrer automatiquement le serveur de destination si nécessaire, puis cliquez sur Installer.
- 12. Une fois l'installation terminée, cliquez sur le **bouton Fermer**.
- 13. Sélectionnez l'indicateur de notification dans l'application Gestionnaire de serveur.



- 14. Un message pour commencer la configuration post-déploiement est répertorié sous l' **indicateur de notification**.
- 15. Cliquez sur le lien pour commencer la configuration des services installés.



- 16. L'Assistant de configuration des services de certificats Active Directory démarre.
- 17. 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.
- 18. Entrez les informations de compte requises et cliquez sur Suivant.

AD CS Configuration		-	+		×
Credentials		DESTI	NAT	ION SER P-0A000	VER)450
Credentials Role Services	Specify credentials to configure role service To install the following role services you must belong to the loca	'S al Administrators g	proup	0:	
	Certification Authority Web Enrollment Online Responder To install the following role services you must belong to the Enter	erprīse Admīns gro	oup:		
	 Enterprise certification authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Network Device Enrollment Service 				
	Credentials: IP-0A000450\Administrator	Change			
	More about AD CS Server Roles				
	More about AD CS Server Roles < Previous Next >	Configure		Cance	el

- 19. Dans Services de rôle, sélectionnez les services suivants :
 - Autorité de certification
 - Inscription Web de l'autorité de certification
- 20. Cliquez sur Suivant.

ole Services		DESTINA	IP-0A000	45
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation	Select Role Services to configure			
	More about AD CS Server Roles			

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

Setup Type	DESTINATION SERVE
Credentials Role Services	Specify the setup type of the CA
Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation	 Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates. Enterprise CA Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies. Standalone CA Standalone CAs can be members or a workgroup or domain, Standalone CAs do not require AI DS and can be used without a network connection (offline).
	More about Setup Type

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

СА Туре	DESTINATION SERVER
Credentials Role Services Setup Type CA Type	Specify the type of the CA When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own cellscienced certificate A subordinate CA receiver a cartificate from the CA above it in the PKI
Private Key	hierarchy.
Cryptography	Root CA
CA Name	Root CAs are the first and may be the only CAs configured in a PKI hierarchy.
Validity Period	() Subardinata CA
Certificate Database Confirmation	Subordinate CA Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.
	More about CA Type

23. n Clé privée, sélectionnez l'option de création d'une clé privée, puis cliquez sur Suivant.

	DECTINATION CEDUC
Private Key	IP-0A000450
Credentials Role Services	Specify the type of the private key
Setup Type	to generate and issue certificates to clients, a certification authority (CA) must have a private key.
Private Key	 Create a new private key Use this option if you do not have a private key or want to create a new private key.
Cryptography CA Name Validity Period Certificate Database Confirmation	 Use existing private key Use this option to ensure continuity with previously issued certificates when reinstalling a CA. Select a certificate and use its associated private key Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key. Select an existing private key on this computer Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.
	More about Private Key

24. 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**.

Cryptography fo	or CA		DESTINATIO	ON SERVER
Credentials Role Services Setup Type	Specify the cryptographic options Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider	y	Key length:	
Private Key	Select the hash algorithm for signing certificates issued by	this CA:		
CA Name Validity Period Certificate Database Confirmation	SHA256 SHA384 SHA512 SHA1 MD5	accessed b	by the CA,	
	More about Cryptography			

25. 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 ».

CA Name	DESTINATION SERVER IP-0A000450
Credentials Role Services	Specify the name of the CA
Setup Type CA Type Private Key	Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.
Cryptography CA Name	IP-0A000450-CA
Validity Period Certificate Database Confirmation	Distinguished name suffix: Preview of distinguished name:
	CN=IP-0A000450-CA
	More shout CA Name
	More about CA Name

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

📥 AD CS Configuration							e		×
Validity Period						1	DESTINA	TION SER	VER)450
Credentials Role Services Setup Type	Spec Select t	ify the validit	y period	l ficate gener	ated for this c	ertification au	thority (C	:A):	
СА Туре	5	Years	*						
Private Key	CA exp	iration Date: 4/27/2	2026 3:27:00	PM					
Cryptography	The val	idity period config	ured for this	CA certifica	ate should exc	eed the validi	ity period	for the	
CA Name	certifica	ates it will issue.							
Validity Period									
Certificate Database									
Confirmation									
	More a	bout Validity Period	d						
		- Values de dece							
			<	Previous	Next >	Cont	figure	Cance	el

27. 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

- 28. Cliquez sur Suivant.
- 29. Dans Confirmation, passez en revue les options de configuration sélectionnées et cliquez sur Configurer pour commencer le processus de configuration.
- 30. Une fois la configuration terminée, cliquez sur Fermer.
- 31. Lorsque vous êtes invité à configurer des services de rôle supplémentaires, cliquez sur Non.
- 32. Redémarrez le serveur local pour vous assurer qu'il est prêt à servir de serveur de certificats Active Directory.

15.4 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.

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 81/131Guide des certificats - Milestone XProtect® VMSGuide des c XProtect[®] VMS

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

15.4.1 Ajouter un certificat d'autorité de certification au serveur

Ì

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.

a Kun			-
ð	Type the name of a progr resource, and Windows w	am, folder, docum ill open it for you.	nent, or Internet
Open:	mmd		~
-F -111	-		

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

File	Action View Favorites V	Vindow trl+N	Help	- U A
	Open C	trl+0	Name	Actions
	Save C	Ctrl+S	There are no items to show in this view.	Console Root
	Save C Save As Ct Options Recent File Exit	tri+S	There are no items to show in this view.	Console Root Actions

composant logiciel enfichable....

3. Sélectionnez le composant logiciel enfichable Certificats, puis cliquez sur Ajouter des certificats, puis

allable snap-ins:		-	Selected snap-ins:	
Snap-in	Vendor	^	Console Root	Edit Extensions
ActiveX Control	Microsoft Cor		Certificates (Local Comput	ar) Jacobia
Authorization Manager	Microsoft Cor		and the second sec	and a second sec
Certificates	Microsoft Cor			
Component Services	Microsoft Cor			(d) s mill
Computer Managem	Microsoft Cor		-	
Device Manager	Microsoft Cor	T	Add >	THERE DEVIC
Disk Management	Microsoft and	L		
Event Viewer	Microsoft Cor			
Folder	Microsoft Cor			
Group Policy Object	Microsoft Cor			
Internet Informatio	Microsoft Cor			
IP Security Monitor	Microsoft Cor			
IP Security Policy M	Microsoft Cor	4		Advanced
	*** ***	-		
scription:			and the second	the second second second

Compte d'ordinateur.

ertificates snap-in	×
This snap-in will always manage certificates for:	
O My user account	
O Service account	
Computer account	

- Dans Sélectionner un ordinateur, sélectionnez Ordinateur local. 4.
- 5. Sélectionnez Terminer, puis OK.

Select the computer you want this snap-i	in to manage.	
This snap-in will always manage:		
Local computer: (the computer this	is console is running on)	
O Another computer:	Browne	8
only applies if you save the consol	ie.	

WODOTIA AG WWW.MODOUX.com
Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 85/ 131Guide des certificats - Milestone XProtect® VMSGuide des certificates - Mileston XProtect[®] VMS

- 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.

8. Cliquez sur Suivant.

Ì

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

÷	×

Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by you	Add New
Custom Request	
Proceed without enrollment policy	
	Next Cancel
7 🔤 Remote Desitop	
Smart Card Trusted Roots SMAC	
imit Trusted Root Certification Authorities	
> ill Web Hosting Windowe Live ID Token Issuer	
V VIIIdows Live ID Token Issuer	
WindowsServerUpdateServices	
WindowsServerUpdateServices	
S 🖻 WindowsServerUpdateServices	

Suivant.

© MOBULIX AG WWW.mobotix.com Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 86/ 131Guide des certificats - Milestone XProtect® VMSGuide des certificates - Milest 10. Développez le champ d'affichage des **détails** de la demande personnalisée, puis cliquez sur **Propriétés**.

Chose an option from the list below and configure the certificate options as required. Template: (No template) CNG key Suppress default extensions Request format: PKCS #10 OMC Note: Key archival is not available for certificates based on a custom certificate request, option is specified in the certificate template.	even w	
Chose an option from the list below and configure the certificate options as required. Template: (No template) CNG key Suppress default extensions Request format: PKCS #10 © CMC Note: Key archival is not available for certificates based on a custom certificate request, option is specified in the certificate template.	even w	
Template: (No template) CNG key Suppress default extensions Request format: PKCS #10 O EMC Note: Key archival is not available for certificates based on a custom certificate request, option is specified in the certificate template.	evenw	
□ Suppress default extensions Request format: ○ PKCS #10 ④ CMC Note: Key archival is not available for certificates based on a custom certificate request, option is specified in the certificate template.	even w	
Request format: <u>PKCS</u> #10 <u>CMC</u> Note: Key archival is not available for certificates based on a custom certificate request, option is specified in the certificate template.	even w	
OMC Note: Key archival is not available for certificates based on a custom certificate request, option is specified in the certificate template.	even w	
Note: Key archival is not available for certificates based on a custom certificate request, option is specified in the certificate template.	even w	
		nen tr
N	ext	C
	-	

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

	-			and the second		
Seneral	Subject	Extensions	Private Key	Signature		
A friend	ly name	and descript	tion will make	e it easier to ide	ntify and use	a certificate.
Friendly	name:	_				
TestLab	Domain	.com				
Descript	ion:					
TestLab	Domain	.com				

12. 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.

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.

General	Subject	Extensions	Private Key	Signature				
The foll	owing are	e the certific	ate extension	s for this ce	rtificate	type.		^
Key us	age						v	
Extend	led Key U	sage (applic	ation policie	5)			^	
An app certific certific Availab	ate can b ates issue ates option	oolicy (called e used. Selected by this ter	i enhanced k ct the applica nplate.	ey usage in tion policy	Window required Selec	rs 2000) d I for valid	efines how a signatures of ons:	
Code S Secure Time S Micros IP secu IP secu IP secu	igning Email tamping toft Trust toft Time trity end s trity tunn trity user	List Signii Stamping system el termina	< R	dd > emove	¢	ш	2	
Mak	e the Exte	ended Key U	sage critical					~

- 14. Sous l' onglet Clé privée, développez le menu Options de clé .
- 15. Définissez la taille de la clé sur 2048 et sélectionnez l'option permettant d'exporter la clé privée. Cliquez sur **OK**.

Certificate P	propert	ies				×
General S	ubject	Extensions	Private Key	Signature		
Cryptog	raphic !	Service Prov	ider			۷
Key optio	ons					*
Set the ke	ey lengt	th and expo	rt options for	the private key.		
Key size:	2048			~	2	
Make p	private	key exportal	ble		_	
Allow	private	key to be an	chived			
Strong	private	e kev protec	tion			
	P 0.1-2-	- 1997 (B.1999)				
Select Ha	ash Alo	orithm				
Select Ha	sh Algo	orithm to be	used for this	request		
Hash Alg	orithm	sha256			~	
Select Sig	gnature	e Format				*
						0
				OK	Cancel	Apply

- 16. Une fois que toutes les propriétés du certificat ont été définies, cliquez sur **Suivant** dans l'Assistant **Inscription de certificat**.
- 17. 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.
- 18. Cliquez sur **Terminer**.

Certificate Enrollment	
Where do you want to save the offline request?	
If you want to save a copy of your certificate request or want to pro- to your hard disk or removable media. Enter the location and name click Finish.	cess the request later, save the reques of your certificate request, and then
File Name: C:\Users\Administrator\Desktop\CSR6.1.21	Browse
File format:	Business

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

Ì

15.4.2 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.

107Test1 - Notepad	- 🗆 X
File Edit Format View Help	
BEGIN NEW CERTIFICATE F	REQUEST
IIIF2AYJKoZIhvcNAQcCoIIFyTCO	CBcUCAQMxDzANBg1ghkgBZQMEAgEFADCCBB4G
CsGAQUFBwwCoIIEEASCBAwwggQ1	IMGYwZAIBAgYKKwYBBAGCNwoKATFTMFECAQAw
wIBATFHMEUGCSsGAQQBgjcVFDE4	4MDYCAQUMDENsdXN0ZXIxVEVNUAwaQ0xVU1RF
jFURU1QXEFkbWluaXN0cmF0b3IN	MB01NQy5FWEUwgg0YoIID1AIBATCCA40wggJ1
gEAMBcxFTATBgNVBAMMDENsdXN	0ZXIxVEVNUDCCASIwDQYJKoZIhvcNAQEBBQAD
gEPADCCAQoCggEBAKVp0982yi0	5tcnypaTujsFBe9jwOyRp+c5N00xf8OcN0Dyg
VMVTSU9s9rTMWmUDzP+zLumOmC6	6gCWIo5RgiT+dLjOvq+Z6AUWC1H+WVUsaVbJc
ktV8ut805gi46dkQ4MD71btX6mr	njjUB294Xwf8yUVP1Be0dkfqjUVnn6EAYzHdS
czK1yUZmY576IBwf6LZMujXbNDD	D5ZXzdhG3pggarNdzHvg0RIJvro4IJ0rM6EsJ
N2d0SZms4Utj21DekFde3BsENvo	cvk0/PHZk8b8Bww050+ya3tk7jDbvw0a1VXE9
qL+Zy4pEP1jKnTwM1IyPmsXyw7g	gx6CrTw8ntqECAwEAAaCCAS8wHAYKKwYBBAGC
W@CAzEOFgwxMC4wLjE0MzkzLjIv	wRQYJKwYBBAGCNxUUMTgwNgIBBQwMQ2x1c3R1
jFURU1QDBpDTFVTVEVSMVRFTVB	cQWRtaW5pc3RyYXRvcgwHTU1DLkVYRTBgBgkq
kiG9w0BCQ4xUzBRMBMGA1UdJQQM	MMAoGCCsGAQUFBwMBMBsGCSsGAQQBgjcVCgQO
1AwwCgYIKwYBBQUHAwEwHQYDVR00	OBBYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG
isGAQQBgjcNAgIxWDBWAgEAHk44	ATQBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0
AHcAYQByAGUAIABLAGUAeQAgAFM4	AdABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1
AHIDAQAwDQYJKoZIhvcNAQELBQAI	DggEBAFGoQLCtyiv0XG0T0U4MS9VnUS0sQUnN
)APtDKNDGskV/dq6rqgpYEKiQfW2	ZeSndEOzxieJtES/1I5hmVUm51TIVydzE8iyW
(jUze/+WIiZifGFnkMKYwrzKgx7d	qIr' Undo t
n3dWazix8dSVOQIRZ3Lr7yXg9ii	F49 j
EX7yVZFyEAs/6uoApcKXc2KPgBP8	8aHé Cut 9
[p4XCYYiuyw/+iHqyNca2fvIIm8	Hpb(Copy 3
zCCAYcCAQOAFOBsTd6/Hpi6c18	n5HI Paste
wYJKoZIhvcNAQkDMQoGCCsGAQUF	FBWI Delete
)Y6dr8BzietMf5QwmoRNzq8MRGS(QINI Delete v
-q/316NKKLzg/ROhm16Xj7tL4Id2	Select All
LWR7EktvnBLYuBQVPGYb+gwd8EfE	Bh9l C
+52/i0E2HZpsBrS1d1+u89F0Pi+	+W/r Right to left Reading order J
1117K+ce+EDoHhXkbSD+fHYFbUqa	Show Unicode control characters
2PmPVkUJGJEUMwfo8rb4xb9taP6y F8XTFWMOJCPMvkW2	Insert Unicode control character
END NEW CERTIFICATE REC	QUE: Open IME
END NEW CERTIFICATE REC	QUE: Open IME Reconversion

- 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.

S Microsoft Active Directory Certii × +	0	-	Ц	×
← → C ▲ Not secure 10.0.4.103/certsrv/	\$		Updat	ie :)
Vicrosoft Active Directory Certificate Services - IP-0A000467-CA				Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see <u>Active Directory Certificate Services</u> <u>Documentation</u>.

Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>

- 4. Cliquez sur le lien Demander un certificat.
- 5. Cliquez sur le lien de demande de certificat avancé.

0	Micr	osoft A	ctive [Directory Certi	×	+				
4	÷	C		Not secure	10.0	0.4.103	/cert	srv/ce	ertrqus	asp.
Micr	rosof	t Active	e Dire	ctory Certifica	te Se	rvices	– IP	0A00	0467-0	CA .
Req	uest	t a Ce	ertifi	cate	_					_
Sele	ect th	ie cer	tifica	ite type:						
V	Veb I	Brows	ser C	ertificate						
F	-Mai	I Prot	ectio	on Certificat	e					

Or, submit an advanced certificate request.

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.

Microsoft Active	Directory Certificate S	ervices - CLUSTER2TE	MP-CA	Home
ubmit a Cer	tificate Request o	r Renewal Request		
o submit a sa enewal reque	aved request to the st generated by ar	CA, paste a base-64 external source (suc	I-encoded CMC or PKCS #10 o ch as a Web server) in the Save	certificate request or PKCS #7 ed Request box.
ase-64-encodec ertificate request CMC or KCS #10 or KCS #7):	1WR7EktvnBLYuBQ r+52710E2H2psBrs nI17k+ce+EDoHhX 2EmPVkUJGJEUMwfc TSXTFWMOJCPMykW END NEW CE	VPGYD+gwd8EfBh9K9Qqt Sldl+u89F0Pi+W/a8/Y\ dSD+fHYFbUqaTYUfg04 SEb4xb9taP6ycUZwieI HIFICATE REQUEST	rd5fMu: 77BhAl: hu5Pg6: .rNWw31	
dditional Attrib	utes:			
Attributes	4	\$ 2		

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.

15.5 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.
- 4. Sélectionnez cette option pour installer le certificat de l'utilisateur actuel et cliquez sur Suivant.

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

X

Cadifica	And I start and a	+ Mr.	4
Certifica	te impo	int wizar	a

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Ourrent User	
O Local Machine	

To continue, click Next.

	Next	Cancel
--	------	--------

Certificate Store		
Certificate stores are system areas where certificates are	kept.	
	S	
Windows can automatically select a certificate store, or yo the certificate.	u can specify a location for	
O Automatically select the certificate store based on the	ne type of certificate	Select Certificate Store
Place all certificates in the following store		Coloct the contificate stars you want to use
Certificate store:		Select the certificate store you want to use.
	Browse	Personal
		Trusted Root Certification Authorities
		Enterprise Trust
		Certificates
		Show physical stores
		OK Cano

- 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.

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

File Action View Favorites Window	/ Help			
🧇 🔿 🙍 🚮 🔏 🐴 🗙 🗟 🔒 🚺				
Console Root	Issued To	~	Issued By	Expiration
Certificates (Local Computer) Personal Coefficienter	Cluster17	Open	CLUSTER2TEMP-CA	10/26/202
 Certificates Trusted Root Certification Authoritie 		All Tasks	Open	
 Enterprise Trust Intermediate Certification Authoritie Trusted Publishers 		Cut Copy	Request Certificate with N Renew Certificate with Ne	lew Key w Key
Untrusted Certificates		Delete	Manage Private Keys	
Certificates		Properties	Advanced Operations	>
Trusted People		Help	Export	

- 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.
- 9. 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

15.5.1 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.

- 10. Sur un ordinateur sur lequel un serveur de gestion ou un serveur d'enregistrement est installé, ouvrez le configurateur de serveur à partir 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
- 11. Dans le configurateur de serveur, sous Certificat de serveur, activez le cryptage.
- 12. 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.
- 13. 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.
- 14. 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.

Server Configurator		-		>
Encryption	Encryption			
Registering servers	It is recommended to secure communication with encryption	on. <u>Learn n</u>	nore	
anguage selection	Server certificate Applies to: management server, recording server, failover server, data collector	a		
	Encryption: On			
	Sectors.	ý.	Details	
	Carolicate issued by MS-Grgaostation-P29-Actess [2021], Espires 5/8/2021			
	Streaming media certificate Applies to clients and servers that retrieve data streams from the rec server	ording		
	Encryption: On			
	And the second s	*	Details	
	Certificate Instellity MS-Organizations #29-Access (2023), Instead 5/07/2023			
		1.1	America	
			Apply	

15. 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

16 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 ressemble à la fois aux scénarios de domaine et d'autorité de certification commerciale.

16.1 Ajouter un certificat d'autorité de certification au serveur

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

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

😅 Run	×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	mmd
	OK Cancel <u>B</u> rowse

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

MOBOTIX HUB – Guide des certificats - Installer des certificats dans un environnement

Open Ctrl+O	Name	Actions	
Save Ctrl+S	There are no items to show in this view.	Console Root	
Add/Remove Span-in Ctrl+M		More Actions	l.
Options			
Recent File			
Exit			

- 18. Sélectionnez le composant logiciel enfichable Certificats et cliquez sur Ajouter.
- 19. Cliquez sur **OK**.

nap-in	Vendor	^	Console Root	Edit Extensions
ActiveX Control	Microsoft Cor		Certificates (Local Computer)	
Authorization Manager	Microsoft Cor			Remove
Certificates	Microsoft Cor	Ξ		
Component Services	Microsoft Cor			MoveLip
Computer Managem	Microsoft Cor			
Device Manager	Microsoft Cor		4HA	Move Down
Euset Visuer	Microsoft and		100	
Eolder	Microsoft Cor			
Group Policy Object	Microsoft Cor			
Internet Informatio	Microsoft Cor			
Internet Informatio	Microsoft Cor			
IP Security Monitor	Microsoft Cor			
IP Security Policy M	Microsoft Cor	~		Advanced
a minitiani				
zscripuois:		-		

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 100/131Guide des certificats - Milestone XProtect® VMSGuide des XProtect® VMSGUIDE ACCEST A XProtect[®] VMS

20. 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.

🔿 🙋 💼 📋 🙆 🗟 🛅			
Console Root Q Certificates - Current User	Object T	Type ficates	
Find Certificates			
> 🤷 En 🛛 All Tasks > 🚰 Int	>	Find Certificates	
Ac View	>	Request New Certificate Import	
📔 Ur Th New Taskpad View		Advanced Operations	Create Custom Request
Try Refresh Cli Cce Export List,			Enroll On Behalf Of Manage Enrollment Policies
Sn Help			

- 21. Cliquez sur Suivant dans l'Assistant Inscription de certificat et sélectionnez Continuer sans stratégie d'inscription.
- 22. Cliquez sur Suivant.
- 23. Sélectionnez le modèle de clé CNG (sans modèle) et le format de demande CMC, puis cliquez sur

X

Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by you	Add New
Custom Request	
Proceed without enrollment policy	
	Next Cancel
	INCAL CALLE

Suiv

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 101/131Guide des certificats - Milestone XProtect® VMSGuide des Milestone XProtect® VMSGuide des Certificates - Mi XProtect[®] VMS

MOBOTIX HUB – Guide des certificats - Installer des certificats dans un environnement

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

Certificate Information		
Click Next to use the options already request, and then click Next.	selected for this template, or click Details to cu	istomize the certifica
Custom request	i) STATUS: Available	Details
The following options describe	the uses and validity period that apply to this ty	ype of certificate:
Key usage: Application policies:		
Validity period (days):		
		Properties
		-

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

MOBOTIX HUB – Guide des certificats - Installer des certificats dans un environnement

General Subject Extensions	Private Kev	Signature		
A friendly name and descrip	otion will make	e it easier to identif	y and use a certif	ficate.
TestI abDomain.com				_
Description:				
TestLabDomain.com				

- 26. Dans l' **onglet Objet**, entrez les paramètres requis pour le nom de l'objet.
- 27. Dans le champ **Nom d'objet Type**, entrez dans **Nom commun** le nom d'hôte de l'ordinateur sur lequel le certificat sera installé.

General	Subject	Extensions	Private Key	Signature	
The sub can ent can be Subject The use	oject of a er inform used in a of certifi er or com	certificate is ation about certificate. cate puter that is	the user or c the types of s receiving the	omputer to w subject name certificate	hich the certificate is issued. You and alternative name values that
Subject	name:		T I		CN=MJT-12A
Comm	non name			< bbA	
Value:				Remove	
Alternat	tive name	8	-1		
Direct	ory name		a		
Value:				4dd ≥	
-			E	Remove	

28. 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.

MOBOTIX HUB – Guide des certificats - Installer des certificats dans un environnement

General	Subject	Extensions	Private Key	Signature					
The foll	owing an	e the certific	ate extension	s for this cer	tificate ty	pe.			^
Key us	age							¥	
Extend	led Key U	sage (applic	ation policies	5)				^	
An app certific certific Availab	lication p ate can b ates issue ble option	oolicy (called e used. Selected by this ter is:	d enhanced k ct the applica mplate.	ey usage in V tion policy n	Vindows equired for Selector	2000) d or valid ed opti	lefines hov signatures	v a s of	
Code S Secure Time S Micros Micros IP secu IP secu IP secu	igning Email tamping toft Trust toft Time urity end s urity tunn urity user	List Signi Stamping system el termina	A R	dd> emove	C	H	nacetion	2	
Mak	e the Exte	ended Key U	sage critical		121				v

- 29. Sous l' onglet Clé privée, développez le menu Options de clé .
- 30. Définissez la taille de la clé sur 2048 et sélectionnez l'option permettant d'exporter la clé privée. Cliquez sur **OK**.

MOBOTIX HUB – Guide des certificats - Installer des certificats dans un environnement

Certificate F	propert	ies				>
General S	ubject	Extensions	Private Key	Signature		
Cryptog	raphic	Service Prov	ider			۷
Key opti	ons					*
Set the ke	ey leng	th and expo	rt options for	the private key.		
Key size:	2048			~		
Make	private	key exporta	ble			
Allow	private	key to be an	chived			
Strong	private	e kev protec	tion			
		a service a				
Select H	ash Alo	orithm				*
Select Ha	sh Alg	orithm to be	used for this	request		
Hash Alg	orithm	sha256			~	
Select Si	gnatur	e Format				*
				OK	Cancel	Apply

- **31.** Une fois que toutes les propriétés du certificat ont été définies, cliquez sur **Suivant** dans l' **onglet Inscription au certificat**
- 32. sorcier.
- 33. 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.
- 34. Cliquez sur **Terminer**.

adificate Encollement	
eruncate enroiment	
Where do you want to save the offline request	?
If you want to save a copy of your certificate request or want to your hard disk or removable media. Enter the location and click Finish.	to process the request later, save the requ name of your certificate request, and the
File Name:	(purrough and a second se
Cillicard Administrator Deckton CCR6 1 21	Description
C:\Users\Administrator\Desktop\CSR6.1.21	Browse
C:\Users\Administrator\Desktop\CSR6.1.21 File format:	Browse
C:\Users\Administrator\Desktop\CSR6.1.21 File format: Base 64 Binary	Browse
C:\Users\Administrator\Desktop\CSR6.1.21 File format: Base 64 Binary	Browse
C:\Users\Administrator\Desktop\CSR6.1.21 File format: Base 64 Binary	Browse
C:\Users\Administrator\Desktop\CSR6.1.21 File format:	Browse

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

Ì

16.1.1 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.

File Edit Format View Help	
BEGIN NEW CERTIFICATE REQU	JEST
IIIF2AYJKoZIhvcNAQcCoIIFyTCCBcU	JCAQMxDzANBg1ghkgBZQMEAgEFADCCBB4G
CcsGAQUFBwwCoIIEEASCBAwwggQIMGY	/wZAIBAgYKKwYBBAGCNwoKATFTMFECAQAw
AwIBATFHMEUGCSsGAQQBgjcVFDE4MDY	CAQUMDENsdXN0ZXIxVEVNUAwaQ0xVU1RF
JjFURU1QXEFkbWluaXN0cmF0b3IMB01	NQy5FWEUwggOYoIID1AIBATCCA40wggJ1
AgEAMBcxFTATBgNVBAMMDENsdXN0ZXI	<pre>CxVEVNUDCCASIwDQYJKoZIhvcNAQEBBQAD</pre>
ggEPADCCAQoCggEBAKVp0982yi05tcn	nypaTujsFBe9jwOyRp+c5N00xf8OcN0Dyg
dVMVTSU9s9rTMWmUDzP+zLumOmC6gCW	WIo5RgiT+dLjOvq+Z6AUWC1H+WVUsaVbJc
ZktV8ut805gi46dkQ4MD71btX6mnjjU	JB294Xwf8yUVP1Be0dkfqjUVnn6EAYzHdS
zczK1yUZmY576IBwf6LZMujXbNDD5ZX	(zdhG3pggarNdzHvg0RIJvro4IJ0rM6EsJ
JN2d0SZms4Utj21DekFde3BsENvcvk0)/PHZk8b8Bww050+ya3tk7jDbvw0a1VXE9
pqL+Zy4pEP1jKnTwM1IyPmsXyw7gx6C	CrTw8ntgECAwEAAaCCAS8wHAYKKwYBBAGC
W@CAzEOFgwxMC4wLjE0MzkzLjIwRQY	/JKwYBBAGCNxUUMTgwNgIBBQwMQ2x1c3R1
jFURU1QDBpDTFVTVEVSMVRFTVBcQWR	RtaW5pc3RyYXRvcgwHTU1DLkVYRTBgBgkq
kiG9w0BCQ4xUzBRMBMGA1UdJQQMMAo	bGCCsGAQUFBwMBMBsGCSsGAQQBgjcVCgQ0
NWWCBATKMABRÓDHWMEMHÓADAKOOBRA	/EFOBsTd6/Hpi6c18h5HHq88hWc911MGYG
HAWWCgYIKWYBBQUHAWEWHQYDVR0OBBY LisGAQQBgjcNAgIxWDBWAgEAHk4ATQB	/EFOBsTd6/Hpi6c18h5HHq88hWc911MGYG 8pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0
AWWCgYIKWYBBQUHAWEWHQYDVR0OBBY isGAQQBgjcNAgIxWDBWAgEAHk4ATQB HCAYQByAGUAIABLAGUAeQAgAFMAdAB	/EFOBsTd6/Hpi6c18h5HHq88hWc911MGYG 8pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 8vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1
MAWWCgYIKWYBBQUHAWEWHQYDVR0OBBY CisGAQQBgjcNAgIxWDBWAgEAHk4ATQB AHcAYQByAGUAIABLAGUAeQAgAFMAdAB AHIDAQAWDQYJKoZIhvcNAQELBQADggE	/EFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN
AAWWCgYIKWYBBQUHAWEWHQYDVR0OBBY CisGAQQBgjcNAgIxWDBWAgEAHk4ATQB AHCAYQByAGUAIABLAGUAeQAgAFMAdAB AHIDAQAwDQYJKoZIhvcNAQELBQADggE DAPtDKNDGskV/dq6rqgpYEKiQfWZeSn	/EFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW
AAWWCgYIKWYBBQUHAWEWHQYDVR0OBBY CisGAQQBgjcNAgIxWDBWAgEAHk4ATQE AHcAYQByAGUAIABLAGUAeQAgAFMAdAB AHIDAQAWDQYJKoZIhvcNAQELBQADggE DAPtDKNDGskV/dq6rqgpYEKiQfWZeSn KjUze/+WIiZifGFnkMKYwrzKgx7qIr	/EFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo
AAWWCgYIKWYBBQUHAWEWHQYDVR00BBY LisGAQQBgjcNAgIxWDBWAgEAHk4ATQE AHCAYQByAGUAIABLAGUAeQAgAFMAdAB AHIDAQAWDQYJKoZIhvcNAQELBQADggE DAPtDKNDGskV/dq6rqgpYEKiQfWZeSn (jUze/+WIiZifGFnkMKYwrzKgx7qIr I3dWazix8dSVOQIRZ3Lr7yXg9iiF49	/EFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo
AGWCGYIKWYBBQUHAWEWHQYDVR00BBY isGAQQBgjcNAgIxWDBWAgEAHk4ATQE HCAYQByAGUAIABLAGUAeQAgAFMAdAB HIDAQAwDQYJKoZIhvcNAQELBQADggE APtDKNDGskV/dq6rqgpYEKiQfWZeSn (jUze/+WIiZifGFnkMKYwrzKgx7qIr I3dWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe	/EFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN hdEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo
AWWCgYIKWYBBQOHAWEWHQYDVR00BBY isGAQQBgjcNAgIxWDBWAgEAHk4ATQE HcAYQByAGUAIABLAGUAeQAgAFMAdAB HIDAQAWDQYJKoZIhvcNAQELBQADggE APtDKNDGskV/dq6rqgpYEKiQfWZeSn jUze/+WIiZifGFnkMKYwrzKgx7qIr 3dWazix8dSV0QIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0	<pre>/EFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy</pre>
AGACYTERSTEINSTEINSTEINSTEINSTEINSTEINSTEINSTEIN	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN hdEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy Paste
TARWCgYIKWYBBQUHAWEWHQYDVR00BBY LisGAQQBgjcNAgIxWDBWAgEAHk4ATQE AHCAYQByAGUAIABLAGUAeQAgAFMAdAB AHIDAQAwDQYJKoZIhvcNAQELBQADggE DAPtDKNDGskV/dq6rqgpYEKiQfWZeSn (jUze/+WIiZifGFnkMKYwrzKgx7qIr 13dWazix8dSV0QIRZ3Lr7yXg9iiF49- X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 L2CCAYcCAQOAF0BsTd6/Hpi6c18h5H WYJKoZIhvcNAQkDMQoGCCsGAQUFBw	<pre>/EFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN hdEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy Paste Delete</pre>
AWWCgYIKWYBBQUHAWEWHQYDVR00BBY isGAQQBgjcNAgIxWDBWAgEAHk4ATQE HCAYQByAGUAIABLAGUAeQAgAFMAdAE HIDAQAwDQYJKoZIhvcNAQELBQADggE OAPtDKNDGskV/dq6rqgpYEKiQfWZeSn (jUze/+WIiZifGFnkMKYwrzKgx7qIr) OdWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe P4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAFOBsTd6/Hpi6c18h5H WYJKoZIhvcNAQkDMQoGCCsGAQUFBw WY6dr8BzietMf5QwmoRNzq8MRGSQiN1	/EFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy Paste Delete
AWWCgYIKWYBBQUHAWEWHQYDVR00BBY isGAQQBgjcNAgIxWDBWAgEAHk4ATQE AHCAYQByAGUAIABLAGUAeQAgAFMAdAE AHIDAQAwDQYJKoZIhvcNAQELBQADggE OAPtDKNDGskV/dq6rqgpYEKiQfWZeSn (jUze/+WIiZifGFnkMKYwrzKgx7qIr I3dWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe P4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAFOBsTd6/Hpi6c18h5H WYJKoZIhvcNAQkDMQoGCCsGAQUFBw OY6dr8BzietMf5QwmoRNzq8MRGSQiN1 -q73I6NKKLzg7ROhm16Xj7tL4Id2iV	/EFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN hdEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy Paste Delete Select All
AWWCgYIKWYBBQUHAWEWHQYDVR00BBY isGAQQBgjcNAgIxWDBWAgEAHk4ATQE HCAYQByAGUAIABLAGUAeQAgAFMAdAE HIDAQAwDQYJKoZIhvcNAQELBQADggE APtDKNDGskV/dq6rqgpYEKiQfWZeSn (jUze/+WIIZifGFnkMKYwrzKgx7qIr) 3dWazix8dSV0QIRZ3Lr7yXg9iiF49- X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQ0AF0BsTd6/Hpi6c18h5H wYJKoZIhvcNAQkDMQoGCCsGAQUFBw Y6dr8BzietMf5QwmoRNzq8MRGSQiNI q73I6NKKLzg7ROhm16Xj7tL4Id2iVL WR7EktvnBLYuBQVPGYb+gwd8EfBh9H	VEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN hdEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy Paste Delete Select All Biskt to left Pasadian and a
AWWCgYIKWYBBQUHAWEWHQYDVR00BBY isGAQQBgjcNAgIxWDBWAgEAHk4ATQE HCAYQByAGUAIABLAGUAeQAgAFMAdAE HIDAQAwDQYJKoZIhvcNAQELBQADggE OAPtDKNDGskV/dq6rqgpYEKiQfWZeSn (jUze/+WIiZifGFnkMKYwrzKgx7qIr) O3dWazix8dSV0QIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe P4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAF0BsTd6/Hpi6c18h5H WYJKoZIhvcNAQkDMQoGCCsGAQUFBw OY6dr8BzietMf5QwmoRNzq8MRGSQiN1 -q73I6NKKLzg7R0hm16Xj7tL4Id2iVU WR7EktvnBLYuBQVPGYb+gwd8EfBh9U +5Z7i0E2HZpsBrS1d1+u89F0Pi+W/a	<pre>/EFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/115hmVUm51TIVydzE8iyW Undo Cut Copy Paste Delete Select All Right to left Reading order</pre>
AWWCgYIKWYBBQUHAWEWHQYDVR00BBY isGAQQBgjcNAgIxWDBWAgEAHk4ATQE HCAYQByAGUAIABLAGUAeQAgAFMAdAE HIDAQAwDQYJKoZIhvcNAQELBQADggE APtDKNDGskV/dq6rqgpYEKiQfWZeSn (jUze/+WIiZifGFnkMKYwrzKgx7qIr) 3dWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAFOBsTd6/Hpi6c18h5H wYJKoZIhvcNAQkDMQoGCCsGAQUFBw Y6dr8BzietMf5QwmoRNzq8MRGSQiN1 q73I6NKKLzg7ROhm16Xj7tL4Id2iVL WR7EktvnBLYuBQVPGYb+gwd8EfBh9L +5Z7i0E2HZpsBrS1d1+u89F0Pi+W/a Ii7k+ce+EDoHhXkbSD+fHYFbUqaTYL	CEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN hdEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy Paste Delete Select All Right to left Reading order Show Unicode control characters
AWWCgYIKWYBBQUHAWEWHQYDVR00BBY isGAQQBgjcNAgIxWDBWAgEAHk4ATQE HCAYQByAGUAIABLAGUAeQAgAFMAdAB HIDAQAwDQYJKoZIhvcNAQELBQADggE APtDKNDGskV/dq6rqgpYEKiQfWZeSr (jUze/+WIIZifGFnkMKYwrzKgx7qIr) BdWazix8dSV0QIRZ3Lr7yXg9iiF49- X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQ0AF0BsTd6/Hpi6c18h5H WYJKoZIhvcNAQkDMQoGCCsGAQUFBw)Y6dr8BzietMf5QwmoRNzq8MRGSQiN Q73I6NKKLzg7ROhm16Xj7tL4Id2iV WR7EktvnBLYuBQVPGYb+gwd8EfBh9 +5Z7i0E2HZpsBrSld1+u89F0Pi+W/A Di7k+ce+EDoHhXkbSD+fHYFbUqaTV PmPVkUJGJEUMwf08rb4xb9taP6ycU	VEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQATABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN bdEOzxieJtES/115hmVUm51TIVydzE8iyW Undo Cut Copy Paste Delete Select All Right to left Reading order Show Unicode control characters Insert Unicode control character
Address of the second s	ZEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQATABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 BAFGoQLCtyiv0XG0T0U4MS9VnUS0sQUnN bdE0zxieJtES/115hmVUm51TIVydzE8iyW Undo Cut Copy Paste Delete Select All Right to left Reading order Show Unicode control characters Insert Unicode control character
Adding TKWYBBQUHAWEWHQYDVR00BBY CisGAQQBgjcNAgIxWDBWAgEAHk4ATQE AHcAYQByAGUAIABLAGUAeQAgAFMAdAE AHIDAQAwDQYJKoZIhvcNAQELBQADggE DAPtDKNDGskV/dq6rqgpYEKiQfWZeSr (jUze/+WIiZifGFnkMKYwrzKgx7qIr) 13dWazix8dSVOQIRZ3Lr7yXg9iiF49 EX7yVZFyEAs/6uoApcKXc2KPgBP8aHe P4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 EZCAYcCAQOAFOBsTd6/Hpi6c18h5H WJKoZIhvcNAQkDMQoGCCsGAQUFBw DY6dr8BzietMf5QwmoRNzq8MRGSQiN1 -q73I6NKKLzg7ROhm16Xj7tL4Id2iVU UWR7EktvnBLYuBQVPGYb+gwd8EfBh9U +5Z7i0E2HZpsBrSld1+u89F0Pi+W/a 1i7k+ce+EDoHhXkbSD+fHYFbUqaTYU PmPVkUJGJEUMwfo8rb4xb9taP6ycUI 8XTFWM0JCPMykW2	ZEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 BAFGoQLCtyiv0XG0T0U4MS9VnUS0sQUnN bdE0zxieJtES/115hmVUm51TIVydzE8iyW Undo Cut Paste Delete Select All Right to left Reading order Show Unicode control characters Insert Unicode control character Open IME

- 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.

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 108/131Guide des certificats - Milestone XProtect® VMSGuide des Milestone XProtect® VMSGuide des Certificates_VAS XProtect[®] VMS
MOBOTIX HUB – Guide des certificats - Installer des certificats dans un environnement

S Microsoft Active Directory Certi × +	0	-	Ц	^
← → C ▲ Not secure 10.0.4.103/certsrv/	\$		Updat	e :)
Microsoft Active Directory Certificate Services – IP-0A000467-CA			1	lome

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see <u>Active Directory Certificate Services</u> <u>Documentation</u>.

Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>

- 4. Cliquez sur le lien Demander un certificat.
- 5. Cliquez sur le lien de demande de certificat avancé.



Web Browser Certificate E-Mail Protection Certificate

Or, submit an advanced certificate request.

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

MOBOTIX HUB – Guide des certificats - Installer des certificats dans un environnement

A Shttp://102.158.50.108/centro Q = C Stature A Advin Directory	- D ×
Microsoft Active Directory *	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
licrosoft Active Directory Certificate Services — CLUSTER2TEMP-CA	Home
dvanced Certificate Request	
he policy of the CA determines the types of certificates you can request. Click one of	the following options to:
Create and submit a request to this CA.	
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or using a base-64-encoded PKCS #7 file.	submit a renewal request by

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.

Microsoft Active	Directory Certificate Services - CLUSTER2TEMP-CA	Home
Submit a Cer	tificate Request or Renewal Request	
o submit a sa enewal reque	aved request to the CA, paste a base-64-encoded CMC or PKCS #10 co st generated by an external source (such as a Web server) in the Save	ertificate request or PKCS #7 d Request box.
Sase-64-encodec ertificate reques CMC or VKCS #10 or VKCS #7):	IWR7EktvnBLYuBQVPGYb+gwd3EfBh9K9Qqvd5fMu: r+527i0E2H2psBrSldl+uB9F0Pi+W/aB/YV7BhAl; nll7k+ce+EDOHhXkbSD+fHYFbUqaTYUfgU4uSPq6; 2FmFVkUJGJEUMwfoSrb4xb9taP6ycU2wieLrNWw31 T8XTFWMOJCPMykW2 END NEW CERTIFICATE REQUEST	
dditional Attrib	outes:	
Attributes		

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 •

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 110/ 131Guide des certificats - Milestone XProtect® VMSGuide des Milestone XProtect® VMSGuide des Certificates - M XProtect[®] VMS

MOBOTIX HUB - Guide des certificats - Installer des certificats dans un environnement

0	Micr	osoft A	Active !	Directory Certif	×	+	0	+		×
÷	7	C	A	Not secure	10.0	0.4.103/certsrv/certfnsh.asp	☆	4	Update	• • •
Mice	rosol	t Activ	e Dire	ctory Certificat	e Ser	rvices - IP-0A000467-CA			Į	lome

Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

Your Request Id is 6.

Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with this web browser within 10 days to retrieve your certificate

16.1.2 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.
- 4. 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**.
- 5. Ouvrez un navigateur et rendez-vous sur le site Internal CA IIS situé à l'adresse [ip.ad.dr.ess/certsrv].

🛅 Console Root	Request ID	Binary Request	Request Statu	s Code	Actions
 Certification Authonity (Local) IP-0A000467-CA Revoked Certificates Issued Certificates Pending Requests Failed Requests 	5	All Ta Refree Help	sks ≯ sh	View At Export E Issue Deny	tributes/Extensions Binary Data

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

MOBOTIX HUB - Guide des certificats - Installer des certificats dans un environnement

0	Micr	osoft A	ctive !	Directory Certif	×	+	0	-		×
4	÷	C		Not secure	10.0	0.4.103/certsrv/	4	8	Updat	e ()
Micr	rosot	t Activ	e Dire	ctory Certificat	e Se	rvices - IP-0A000467-CA			1	Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see <u>Active Directory</u> <u>Certificate Services Documentation</u>.

Select a task:

Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

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

0	Microsoft A	uctive D	irectory Certif	×	+			0	-		×
4	⇒ C	A	Not secure	10.0	0.4.103/certs	srv/certckpn	n.asp	☆	4	Upda	te :)
Micr	rosoft Activ	e Direc	tory Certificat	te Ser	rvices - IP-	0A000467-C	A				Home
Viev	v the Sta	tus of	f a Pendin	g Ce	ertificate F	Request	-				
Sele	ect the cer	tificat	e request y		want to vie						

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

MOBOTIX HUB – Guide des certificats - Installer des certificats dans un environnement

Microsoft Act	ive Directory Certificate Services – CLUSTER2TEMP-CA	
Certificate	Issued	
The certifica	te you requested was issued to you.	
	• DER encoded or OBase 64 encoded	
	ownload certificate	
Ľ		

le menu contextuel.

↓ ↓ ↓ ↓ ↓ File Home SI ← ↓ ↓ ↓	nloads hare View This PC > Downloa	ds		
Ouick access	Name	A.	Date modified	Туре
Desktop Downloads	* Certnew	Open Install Certificate Scan with Windows Defender Open with	10/26/2021 2:22 PM	PKCS #7 Certificates

- 9. Acceptez l'avertissement de sécurité s'il apparaît.
- 10. Sélectionnez cette option pour installer le certificat de l'utilisateur actuel et cliquez sur Suivant.

X

Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identit and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
Current User O Local Machine
To continue, click Next.

- Choisissez l'emplacement d'un magasin. Sélectionnez Placer tous les certificats dans le magasin suivant, puis cliquez sur le bouton Parcourir pour ouvrir la fenêtre Sélectionner le magasin de certificats. Accédez au magasin de certificats personnel et cliquez sur OK.
- 12. Cliquez sur Suivant.

MOBOTIX HUB – Guide des certificats - Installer des certificats dans un environnement

Certificate Store	
Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a locat the certificate.	tion for
O Automatically select the certificate store based on the type of certificate	select Certificate Store
Place all certificates in the following store	Colort the cartificate stars you want to use
Certificate store:	Select the certificate store you want to use.
Brows	se Personal
	Trusted Root Certification Authorities
	Intermediate Certification Authorities
	Trusted Publishers
	<
	Show physical stores
	OK Cancel
	Ort

- 13. Terminez l'assistant d'importation de certificat.
- 14. Accédez au composant logiciel enfichable Certificats Microsoft Management Console (MMC).

15. 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.



- 16. 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.
- 17. Assurez-vous que l'utilisateur dispose des autorisations Contrôle total et Lecture activées.

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

CREATOR OWNER		
INETWORK SERVICE		
Administrators (CLUSTER1	TEMP\Administrator	e)
	A <u>d</u> d	Remove
missions for NETWORK RVICE	Allow	Deny
ull control		
Read		
Special permissions		

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 116/131Guide des certificats - Milestone XProtect® VMSGuide des Miles Bio TIX XProtect[®] VMS

16.1.3 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** à partir 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.
- 5. 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.

Server Configurator		-		×
Incryption	Encryption			
egistering servers	It is recommended to secure communication with encryptio	n. <u>Learn r</u>	nore	
Language selection	Server certificate Applies to: management server, recording server, failover server, data collector			
	Encryption: On	0		
	Concession in the local division of the loca	4	Detail	s
	Camplicate issued by MS-Organization-928-Actess (2021), Expires 3/8/2021			
	Streaming media certificate Applies to clients and servers that retrieve data streams from the reco server	ording		
	Encryption: On			
	And the second sec	÷	Detail	ş
	Certificate instead by MS-Degarization 8(#-Access (2021), hyperes 5(0/2021-			
			Apply	
		_		

6. 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

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 117/131Guide des certificats - Milestone XProtect® VMSGuide des Miles BsOTIX XProtect[®] VMS

16.2 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



Ì

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.

d'événements et tous les composants de connexion.

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

16.3 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

16.3.1 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.

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 118/131Guide des certificats - Milestone XProtect® VMSGuide des XProtect® XProtect[®] VMS

Escalier:

- 7. 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
- 8. Dans le configurateur de serveur, sous Serveur d'événements et modules complémentaires, activez le chiffrement.
- 9. 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.
- 10. Sélectionnez un certificat pour chiffrer la communication entre le serveur d'événements et les modules complémentaires associés.
- 11. Sélectionnez Détails pour afficher les informations du Magasin de certificats Windows concernant le certificat sélectionné.



12. 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.

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_FR.docx • 04.03.2025 • Page 119/131Guide des certificats - Milestone XProtect® VMSGuide des XProtect® XProtect[®] VMS

16.3.2 Importer des certificats clients

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

 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:

Microsoft Active Directory Certif × +	0	-		×
← → C A Not secure 10.0.4,103/certsrv/		\$	-	ŧ
Microsoft Active Directory Certificate Services – IP-0A000467-CA			H	ome
Welcome				

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see <u>Active Directory Certificate Services</u> <u>Documentation</u>.

Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>

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

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

Microsoft Active Directory Certif × +	• - □ ×
← → C ▲ Not secure 10.0.4.103/certsrv/certcarc.asp	☆ ≛ :
Microsoft Active Directory Certificate Services - IP-0A000467-CA	Home
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, install this	CA certificate.
To download a CA certificate, certificate chain, or CRL, select the cert	rtificate and encoding method.
CA certificate:	
Current [IP-0A000467-CA] ~	
Encoding method:	
● DER ○ Base 64	
Install CA certificate	
Download CA certificate	
Download CA certificate chain	
Download latest base CRL	

- 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.

↓ ↓ ↓ Downloads File Home Share View				÷	□ X ~ 0
←	Downloads	v 0	Search D	ownloads	p
Desktop 🔷 Name	~	Date mo	dified	Туре	Size
🗄 Documents 🗔 🕞	rtnew,p7b	5/11/202	1 1:31 PM	PKCS #7 Certi	ficates
	Open				
💧 Music	Install Certificate				
Pictures	Edit with Notepad++				
Videos	🖻 Share				
Local Disk (C:)	Open with				
	Give access to	>			
Network	Restore previous version	15			,
1 item 1 item selected 832 bytes	Send to	>		_	
	Cut				
	Сору				
	Create shortcut				
	Delete				
	Rename				
	Properties				

- 6. L'assistant d'importation de certificats est lancé.
- 7. Cliquez sur Suivant.

Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identit and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept,
To continue, dick Next.

8. 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**.

Cliquez sur **Suivant**.

9. Accédez au magasin de certificats Third-Party Root Certification Authorities et cliquez sur OK.

Certificate Store		
Certificate sto	es are system areas where cer	rtificates are kept.
Windows can a the certificate.	utomatically select a certificate	e store, or you can specify a location for
() Automa	cally select the certificate stor	e based on the type of certificate
Place all	certificates in the following sto	re
Certifica	te store:	
		Browse

elect the certificate store you want to use.	
Intermediate Certification Authorities Trusted Publishers Untrusted Certificates	* tificates are kept.
Third-Party Root Certification Authorities Trusted People Client Authentication Issuers	e based on the type of certificate
Show physical stores	re Browse
L	Drowsett

10. 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.

16.4 Afficher l'état du chiffrement pour les clients

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

- 1. Ouvrez le client de gestion.
- Dans le volet de navigation du site, sélectionnez Serveurs > Serveurs d'enregistrement. Cela ouvre une liste de serveurs d'enregistrement.

Next

Cancel

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.

Recording server information	
Name:	
Recording server 1	
Description:	
Covers sector 1	15
	1996-
Host name:	
Local web server address:	
https://	
Web server address:	
https://www.recordingserver1.dk:89/	
Time zone:	
(UTC+01:00) Brussels, Copenhagen, Madrid, Paris	

16.4.1 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 :

- 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.

Guide des certificats | MOBOTIX

ia ues	
Failover server information	
Name:	
Failover recording server 1	
Description:	
Failover for Recording server 1	*
	2
Host name:	
Jocal	
Local web server address:	
https:// local:7563/	
Web server address:	
https://www.failoverrecordingserver1:89/	
UDP port: 8844	
Database location:	
C:\MediaDatabase	
Enable this failover server	

Annexe A | Création d'un script de certificat

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)

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 »

Annexe B | Créer un script de certificat SSL de

```
# 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'

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

Annexe C | Création d'un script de certificat

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 »

 $\#\,\text{Le\,seul}\,\text{objectif}\,\text{requis}\,\text{du}\,\text{sertificat}\,\text{est}\,\text{\ensuremath{\text{\circ}}}\,\text{l'authentification}\,\text{du}\,\text{serveur}\,\text{\ensuremath{\text{\circ}}}\,$

 $serverAuthentication = '2.5.29.37 = \{critique\} \{texte\} 1.3.6.1.5.5.7.3.1'$

Maintenant - créez le certificat du serveur de gestion

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



EN_03/25

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

MOBOTIX est une marque commerciale de MOBOTIX AG déposée dans l'Union européenne, aux États-Unis et dans d'autres pays. Sujet à changement sans préavis. MOBOTIX n'assume aucune responsabilité pour les erreurs ou omissions techniques ou éditoriales contenues dans le présent document. Tous droits réservés. © MOBOTIX AG 2025