



Markvision Enterprise

Version 4.0

Guide de l'administrateur

Novembre 2020

www.lexmark.com

Contenus

Historique des modifications.....	7
Aperçu.....	10
Comprendre Markvision Enterprise.....	10
Mise en route.....	11
Meilleures pratiques.....	11
Configuration requise.....	13
Langues prises en charge.....	14
Modèles d'imprimante pris en charge.....	14
Configuration de la base de données.....	17
Configuration d'une exécution en tant qu'utilisateur.....	18
Installation de MVE.....	19
Installation silencieuse de MVE.....	20
Accès à MVE.....	22
Modification de la langue.....	22
Modification de votre mot de passe.....	22
Maintenance de l'application.....	24
Mise à niveau vers MVE 4.0.....	24
Sauvegarde et restauration de la base de données.....	25
Mise à jour des paramètres du programme d'installation après l'installation.....	27
Configuration de l'accès utilisateur.....	28
Aperçu.....	28
Présentation des rôles utilisateur.....	28
Gestion des utilisateurs.....	29
Activation de l'authentification de serveur LDAP.....	30
Installation de certificats de serveur LDAP.....	32
Détection des imprimantes.....	33
Création d'un profil de recherche.....	33
Gestion des profils de recherche.....	35
Exemple de scénario : Détection des imprimantes.....	36

Affichage des imprimantes.....37

Affichage de la liste des imprimantes.....	37
Affichage des informations de l'imprimante.....	40
Exportation des données de l'imprimante.....	41
Gestion des vues.....	41
Modification de la vue Liste des imprimantes.....	43
Filtrage des imprimantes via la barre de recherche.....	43
Gestion des mots clés.....	44
Utilisation des recherches enregistrées.....	44
Présentation des états du cycle de vie de l'imprimante	44
Exécution d'une recherche enregistrée	46
Création d'une recherche enregistrée	46
Présentation des paramètres de règles de recherche	47
Gestion des recherches enregistrées	49
Exemple de scénario : Surveillance des niveaux de toner de votre parc.....	50

Sécurisation des communications avec l'imprimante..... 52

Présentation des états de sécurité de l'imprimante.....	52
Sécurisation des imprimantes à l'aide des configurations par défaut.....	53
Présentation des autorisations et des contrôles d'accès aux fonctions.....	55
Configuration de la sécurité d'une imprimante.....	56
Sécurisation des communications avec les imprimantes de votre parc.....	57
Autres méthodes de sécurisation de vos imprimantes.....	57

Gestion des imprimantes.....59

Redémarrage de l'imprimante.....	59
Affichage de l'Embedded Web Server de l'imprimante.....	59
Audit d'imprimantes.....	59
Mise à jour de l'état de l'imprimante.....	59
Réglage de l'état de l'imprimante.....	60
Attribution de configurations à des imprimantes.....	60
Annulation de l'attribution de configurations.....	60
Mise en œuvre de configurations.....	60
Vérification de la conformité d'une imprimante avec une configuration.....	61
Déploiement de fichiers sur des imprimantes.....	61
Mise à jour du microcode de l'imprimante.....	62
Désinstallation d'applications présentes sur les imprimantes.....	63

Attribution d'événements à des imprimantes.....	63
Attribution de mots-clés aux imprimantes.....	64
Saisie des informations d'identification pour les imprimantes sécurisées.....	64
Configuration manuelle des certificats d'imprimante.....	65
Suppression d'imprimantes.....	65

Gestion des configurations..... 67

Aperçu.....	67
Création d'une configuration.....	67
Exemple de scénario : Déploiement d'une configuration sur des imprimantes.....	69
Création d'une configuration à partir d'une imprimante.....	69
Exemple de scénario : clonage d'une configuration.....	70
Création d'un composant de sécurité avancée à partir d'une imprimante.....	70
Génération d'une version imprimable des paramètres de configuration.....	71
Présentation des paramètres de variable.....	71
Configuration des autorisations d'impression couleur.....	71
Création d'un package d'applications.....	72
Importation ou exportation d'une configuration.....	73
Importation de fichiers vers la bibliothèque de ressources.....	73

Gestion des certificats.....74

Configuration de MVE pour gérer automatiquement les certificats.....	74
Présentation de la fonction de gestion automatisée des certificats	74
Configuration de MVE pour la gestion automatisée des certificats	75
Gestion des certificats à l'aide de l'autorité de certification Microsoft.....	76
Configuration du serveur CA racine.....	76
Configuration de la CA d'entreprise Microsoft avec NDES.....	77
Configuration du serveur CA subordonné	78
Configuration des paramètres du point de distribution de la certification et de l'accès aux informations d'autorité	80
Configuration de l'accessibilité CRL.....	81
Configuration du serveur NDES	81
Configuration de NDES pour MVE.....	82
Gestion des certificats à l'aide de l'autorité de certification OpenXPki.....	84
Configuration de l'autorité de certification OpenXPki	84
Configuration manuelle de l'autorité de certification OpenXPki.....	87
Génération des informations CRL.....	92
Configuration de l'accessibilité CRL.....	93
Activation du service SCEP.....	94
Activation du certificat du signataire pour le compte de (agent d'inscription)	94

Activation de l'approbation automatique des demandes de certificat dans l'autorité de certification OpenXPki.....	95
Création d'un deuxième domaine.....	95
Définition du numéro de port par défaut pour l'autorité de certification OpenXPki.....	98
Désactivation de Mot de passe de challenge sur l'autorité de certification OpenXPki.....	99
Ajout de l'Eku d'authentification client dans les certificats	99
obtention de l'objet de certificat complet lors d'une demande via SCEP.....	99
Révocation des certificats et configuration de l'accessibilité CRL	100

Gestion des alertes d'imprimante.....102

Aperçu.....	102
Création d'une action.....	102
Compréhension des espaces réservés d'action.....	103
Gestion des actions.....	104
Création d'un événement.....	104
Présentation des alertes d'imprimante.....	105
Gestion des événements.....	109

Affichage de l'état et de l'historique d'une tâche..... 110

Aperçu.....	110
Affichage de l'état de la tâche.....	110
Arrêt des tâches.....	110
Affichage des journaux.....	110
Effacement des journaux.....	110
Exporter les journaux.....	111

Planification de tâches.....112

Création d'une programmation.....	112
Gestion des tâches planifiées.....	113

Autres tâches administratives..... 114

Configuration des paramètres généraux.....	114
Configuration des paramètres de courrier électronique.....	114
Ajout d'un avertissement de connexion.....	114
Signature du certificat MVE.....	115
Suppression des références et des informations utilisateur.....	115

Questions fréquemment posées..... 118

FAQ Markvision Enterprise.....	118
--------------------------------	-----

Dépannage.....	121
L'utilisateur a oublié son mot de passe.....	121
L'utilisateur administrateur a oublié son mot de passe.....	121
La page ne charge pas.....	122
Impossible de détecter une imprimante réseau.....	122
Informations d'imprimante incorrectes.....	122
MVE ne reconnaît pas une imprimante comme imprimante sécurisée.....	123
L'application de configurations avec plusieurs applications échoue à la première tentative, mais réussit lors des tentatives suivantes.....	123
Echec de l'application des configurations avec un certificat d'imprimante.....	124
Autorité de certification OpenXPKI.....	124
Annexe.....	127
Avis.....	131
Glossaire.....	133
Index.....	134

Historique des modifications

Novembre 2020

- Mise à jour des informations sur les éléments suivants :
 - Modèles d'imprimante pris en charge
 - Bases de données prises en charge
- Ajout d'informations sur les éléments suivants :
 - Gestion et déploiement des configurations
 - Sauvegarde et restauration de la base de données
 - Gestion des certificats à l'aide de l'autorité de certification OpenXPki et Microsoft
- Ajout de prise en charge pour les éléments suivants :
 - Gestion et déploiement de configurations dans un groupe de modèles d'imprimante
 - Création de noms de base de données personnalisés

Février 2020

- Mise à jour des informations sur les éléments suivants :
 - Modèles d'imprimante pris en charge
 - Serveurs pris en charge
 - Bases de données prises en charge
 - Chemin de mise à niveau Markvision™ Enterprise (MVE) valide
- Ajout d'informations sur les éléments suivants :
 - Instructions relatives aux meilleures pratiques
 - Instructions relatives à la gestion des certificats automatisés
 - Composants de sécurité avancée par défaut et leurs paramètres
 - Autres méthodes de sécurisation des imprimantes
 - Exemples de scénarios

Juin 2019

- Mise à jour des informations sur les éléments suivants :
 - Notes de bas de page ajoutées aux modèles d'imprimante exigeant des certificats
 - Attribution de droits dbo lors de la configuration de la base de données
 - Chemin de mise à niveau valide lors de la mise à niveau vers la version 3.4
 - Fichiers nécessaires lors de la sauvegarde et de la restauration de la base de données
 - Paramètres d'authentification du serveur LDAP
 - L'état de validité du certificat, les dates et le fuseau horaire sont ajoutés aux paramètres de la règle de recherche
 - Configuration des autorisations et des contrôles d'accès aux fonctions dans les paramètres de sécurité de l'imprimante
 - Sélection d'un fichier de microcode à partir de la bibliothèque de ressources lors de la mise à jour du microcode de l'imprimante

- Sélection de la date de début, de l'heure de début et de pause et des jours de la semaine pour la mise à jour du microcode de l'imprimante
- Gestion des configurations
- Ajout d'informations sur les éléments suivants :
 - Présentation des états de sécurité de l'imprimante
 - Configuration des composants de sécurité avancée
 - Création d'un composant de sécurité avancée à partir d'une imprimante
 - Génération d'une version imprimable des paramètres de configuration
 - Téléchargement d'une autorité de certification pour le parc d'imprimantes
 - Suppression des références et des informations utilisateur
 - Présentation des autorisations et des contrôles d'accès aux fonctions
 - Etapes de dépannage lors de l'application des configurations avec plusieurs échecs d'applications
 - Etapes de dépannage lorsque l'utilisateur Admin a oublié son mot de passe

Août 2018

- Mise à jour des informations sur les éléments suivants :
 - Modèles d'imprimante pris en charge
 - Configuration de la base de données
 - Mise à niveau vers MVE 3.3
 - Questions fréquemment posées
 - Création d'une action
 - Création d'une programmation
- Ajout d'informations sur les éléments suivants :
 - Configuration d'une exécution en tant que compte d'utilisateur de domaine
 - Exportation de journaux
 - Etapes de dépannage lorsque MVE ne reconnaît pas les imprimantes sécurisées

Juillet 2018

- Mise à jour des informations sur la mise à niveau vers MVE 3.2.

Avril 2018

- Mise à jour des informations sur les éléments suivants :
 - Modèles d'imprimante pris en charge
 - Configuration de la base de données
 - Sauvegarde et restauration des fichiers de bases de données
 - URL d'accès à MVE
 - Présentation des paramètres de variable
- Ajout d'informations sur les éléments suivants :
 - Configuration des certificats d'imprimante
 - Arrêt des tâches
 - Mise à jour du microcode de l'imprimante

Septembre 2017

- Mise à jour des informations sur les éléments suivants :
 - Configuration requise
 - Communication entre MVE et les modèles d'imprimantes LexmarkTM Forms 2580, 2581, 2590 et 2591
 - Suppression manuelle des bases de données Microsoft SQL Server
 - Sauvegarde et restauration des fichiers de bases de données
 - Paramètres de sécurité requis pour les contrôles d'accès aux fonctions lors du déploiement du microcode et des fichiers de solution sur des imprimantes
 - Prise en charge des licences lors du déploiement d'applications
 - Alertes d'imprimante et actions qui leur sont associées
 - Récupération automatique de l'état de l'imprimante
 - Attribution des événements et des mots clés

Juin 2017

- Version initiale du document pour MVE 3.0.

Aperçu

Comprendre Markvision Enterprise

Markvision Enterprise (MVE) est un utilitaire de gestion d'imprimantes avec interface Web, destiné aux services informatiques.

Grâce à MVE, vous pouvez gérer efficacement un grand parc d'imprimantes dans un environnement d'entreprise en effectuant les opérations suivantes :

- Recherche, organisation et suivi d'un ensemble d'imprimantes. Vous pouvez auditer une imprimante pour collecter ces données, par exemple état, paramètres et consommables.
- Création de configurations et attributions de ces dernières à des imprimantes.
- Déploiement du microcode, des certificats d'imprimante, de l'autorité de certification (CA) et des applications sur les imprimantes.
- Surveillance des événements et des alertes d'imprimante.

Ce document fournit des informations sur la configuration, l'utilisation et le dépannage de l'application.

Ce document est destiné aux administrateurs.

Mise en route

Meilleures pratiques

Cette rubrique décrit les étapes d'utilisation de MVE recommandées afin de gérer efficacement votre parc.

1 Installez MVE dans votre environnement.

- a** Créez un serveur à l'aide de l'environnement Windows Server le plus récent.

Contenu associé :

[Configuration requise pour le serveur Web](#)

- b** Créez un compte d'utilisateur de domaine ne disposant pas d'un accès administrateur.

Contenu associé :

[Configuration d'une exécution en tant qu'utilisateur](#)

- c** Créez une base de données Microsoft SQL Server, configurez le chiffrement, puis octroyez au nouveau compte d'utilisateur l'accès aux bases de données.

Contenu associé :

- [Configuration requise pour la base de données](#)
- [Configuration de la base de données](#)

- d** Installez MVE à l'aide du compte d'utilisateur de domaine et du serveur SQL avec authentification Windows.

Contenu associé :

[Installation de MVE](#)

2 Configurez MVE, puis détectez et organisez votre parc.

- a** Signez le certificat du serveur.

Contenu associé :

- [Signature du certificat MVE](#)
- [Configuration de MVE pour gérer automatiquement les certificats](#)

- b** Configurez les paramètres LDAP.

Contenu associé :

- [Activation de l'authentification de serveur LDAP](#)
- [Installation des certificats LDAP](#)

- c** Connectez-vous au serveur de messagerie.

Contenu associé :

[Configuration des paramètres de courrier électronique](#)

- d** Détectez votre parc.

Contenu associé :

[Détection des imprimantes](#)

- e** Planifiez les audits et les mises à jour d'état.

Contenu associé :

- [Audit d'imprimantes](#)
- [Mise à jour de l'état de l'imprimante](#)

- f** Configurez les paramètres de base, tels que les noms de contact, les emplacements, les identifications de propriété et les fuseaux horaires.
- g** Organisez votre parc. Utilisez des mots-clés, tels que les emplacements, pour classer les imprimantes.

Contenu associé :

- [Attribution de mots-clés aux imprimantes](#)
- [Création d'une recherche enregistrée](#)

3 Sécurisez votre parc.

- a** Sécurisez l'accès à l'imprimante à l'aide des composants de sécurité avancée par défaut.

Contenu associé :

- [Sécurisation des imprimantes à l'aide des configurations par défaut](#)
- [Présentation des autorisations et des contrôles d'accès aux fonctions](#)
- [Autres méthodes de sécurisation de vos imprimantes](#)

- b** Créez une configuration sécurisée qui inclut des certificats.

Contenu associé :

- [Création d'une configuration](#)
- [Importation de fichiers vers la bibliothèque de ressources](#)

- c** Appliquez la configuration à votre parc actuel.

Contenu associé :

- [Attribution de configurations à des imprimantes](#)
- [Mise en œuvre de configurations](#)

- d** Planifiez des mises en œuvre et des contrôles de conformité.

Contenu associé :

[Création d'une programmation](#)

- e** Ajoutez des configurations aux profils de détection pour sécuriser les nouvelles imprimantes.

Contenu associé :

[Création d'un profil de recherche](#)

- f** Signez les certificats d'imprimante.

Contenu associé :

[Signature du certificat MVE](#)

4 Actualisez votre microcode.

Contenu associé :

[Mise à jour du microcode de l'imprimante](#)

5 Installez et configurez les applications.

Contenu associé :

- [Création d'une configuration](#)
- [Importation de fichiers vers la bibliothèque de ressources](#)

6 Surveillez votre parc.

Contenu associé :

[Création d'une recherche enregistrée](#)

Configuration requise

MVE est installé en tant que serveur Web et est accessible à partir d'un navigateur Web sur n'importe quel ordinateur du réseau. MVE utilise également une base de données pour stocker des informations sur le parc d'imprimantes. La liste suivante répertorie la configuration requise pour le serveur Web, la base de données et le système de l'utilisateur :

Configuration requise pour le serveur Web

Processeur	Processeur double cœur d'au moins 2 GHz utilisant la technologie Hyper-Threading (HTT)
Mémoire vive	Au moins 4 Go
Disque dur	Au moins 60 Go

Remarque : MVE, Lexmark Document Distributor (LDD) et l'Utilitaire de déploiement des périphériques ne peuvent pas être exécutés sur le même serveur.

Serveurs pris en charge

- Windows Server 2019
- Windows Server 2016 Edition Standard
- Windows Server 2012 Edition Standard
- Windows Server 2012 R2

Remarque : MVE prend uniquement en charge la version 64 bits des systèmes d'exploitation.

Configuration requise pour la base de données

Bases de données prises en charge

- Firebird® base de données (intégrée)
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012

Remarque : La taille minimale recommandée pour les bases de données est de 60 Go, afin d'attribuer 20 Mo pour FRAMEWORK et 4,5 Mo pour MONITOR et QUARTZ. Pour plus d'informations, reportez-vous à la section « [Configuration de la base de données](#) » à la page 17.

Configuration requise pour l'utilisateur

Navigateurs Web pris en charge

- Microsoft Edge
- Internet Explorer 11 ou version ultérieure
- Mozilla Firefox (dernière version)
- Google Chrome™ (dernière version)
- Apple Safari (dernière version)

Résolution de l'écran

Au moins 1 280 x 768 pixels

Langues prises en charge

- Portugais brésilien
- Anglais
- Français
- Allemand
- Italien
- Chinois simplifié
- Espagnol

Modèles d'imprimante pris en charge

- Dell 3330dn¹, 3333dn¹, 3335dn¹
- Dell 5230dn¹, 5350dn¹, 5530dn¹, 5535dn¹
- Dell B2360dn, B3460dn, B3465dn
- Dell B5460dn, B5465dnf, S5830dn
- Dell S2830dn
- Dell S5840cdn
- Lexmark 4600, 6500
- Lexmark B2236
- Lexmark B2338², B2442², B2546², B2650², B2865¹
- Lexmark B3440, B3442
- Lexmark C2132
- Lexmark C2240², C2325², C2425², C2535²
- Lexmark C3224
- Lexmark C3326
- Lexmark C3426
- Lexmark C4150², C6160², C9235²
- Lexmark C520¹, C522¹, C524¹, C530¹, C532¹, C534¹, C540³, C543³, C544³, C546³
- Lexmark C734¹, C736¹, C746, C748

- Lexmark C770¹, C772¹, C780¹, C782¹, C792
- Lexmark C920¹, C925¹, C935¹, C950
- Lexmark CS310, CS410, CS510
- Lexmark CS317, CS417, CS517
- Lexmark CS331
- Lexmark CS421², CS521², CS622²
- Lexmark CS431
- Lexmark CS720², CS725²
- Lexmark CS727², CS728², CX727²
- Lexmark CS820², CS827²
- Lexmark CS921², CS923², CS927²
- Lexmark CX310, CX410, CX510
- Lexmark CX317, CX417, CX517
- Lexmark CX331
- Lexmark CX421², CX522², CX622², CX625²
- Lexmark CX431
- Lexmark CX725
- Lexmark CX820², CX825², CX827², CX860²
- Lexmark CX920², CX921², CX922², CX923², CX924², CX927²
- Lexmark E250¹, E260³, E352¹, E360³, E450¹, E460¹, E462¹
- Imprimante Lexmark Forms 2580⁴, 2581⁴, 2590⁴, 2591⁴
- Lexmark M1140, M1145, M3150
- Lexmark M1242², M1246², M3250², M5255², M5265², M5270²
- Lexmark M5155, M5163, M5170
- Lexmark M5255², M5265², M5270²
- Lexmark MB2236
- Lexmark MB2338², MB2442², MB2546², MB2650², MB2770²
- Lexmark MB3442
- Lexmark MC2325², MC2425², MC2535², MC2640²
- Lexmark MC3224
- Lexmark MC3326
- Lexmark MC3426
- Lexmark MS310, MS312, MS315, MS410, MS415, MS510, MS610
- Lexmark MS317, MS417, MS517
- Lexmark MS321², MS421², MS521², MS621², MS622²
- Lexmark MS331, MS431
- Lexmark MS617, MS817, MS818
- Lexmark MS710, MS711, MS810, MS811, MS812
- Lexmark MS725², MS821², MS822², MS823², MS824², MS825², MS826²
- Lexmark MS911
- Lexmark MX310, MX410, MX510, MX511, MX610, MX611

- Lexmark MX317, MX417, MX517
- Lexmark MX321², MX421², MX521², MX522², MX622²
- Lexmark MX331, MX431
- Lexmark MX617, MX717, MX718
- Lexmark MX6500
- Lexmark MX710, MX711, MX810, MX811, MX812
- Lexmark MX721², MX722², MX725², MX822², MX824², MX826²
- Lexmark MX910, MX911, MX912
- Lexmark T640¹, T642¹, T644¹, T650¹, T652¹, T654¹, T656¹
- Lexmark W840¹, W850¹
- Lexmark X264³, X363³, X364³, X463¹, X464¹, X466¹
- Lexmark X543³, X544³, X546³, X548
- Lexmark X642¹, X644¹, X646¹, X651¹, X652¹, X654¹, X656¹, X658¹
- Lexmark X734¹, X736¹, X738¹, X746, X748, X792
- Lexmark X850¹, X852¹, X854¹, X860¹, X862¹, X864¹
- Lexmark X925, X940¹, X945¹, X950, X952, X954
- Lexmark XC2130, XC2132
- Lexmark XC2235², XC2240², XC4240²
- Lexmark XC4140², XC4150², XC6152², XC8155², XC8160²
- Lexmark XC9225², XC9235², XC9245², XC9255², XC9265²
- Lexmark XM1135, XM1140, XM1145, XM3150
- Lexmark XM1242², XM1246², XM3250²
- Lexmark XM5163, XM5170, XM5263, XM5270
- Lexmark XM5365², XM5370²
- Lexmark XM7155, XM7163, XM7170, XM7263, XM7270
- Lexmark XM7355², MX7365², MX7370²
- Lexmark XM9145, XM9155, XM9165
- Pantum CM7105DN
- Pantum CM7000
- Pantum CP2300DN
- Pantum CP2500
- Pantum CP2500DN Plus
- Pantum M7600
- Pantum M7650DN
- Pantum P4000
- Pantum P4200DN
- Pantum P5000
- Pantum P5500DN
- Source Technologies ST9530¹
- Source Technologies ST9620¹, ST9630¹
- Source Technologies ST9712, ST9715, ST9717, ST9720, ST9722, ST9730

- Source Technologies ST9815², ST9818², ST9820², ST9821², ST9822², ST9830²
- Toshiba e-Studio 305CP
- Toshiba e-Studio 388CP²
- Toshiba e-Studio 305CS, 306CS
- Toshiba e-Studio 338CS², 388CS², 389CS², 479CS²
- Toshiba e-Studio 385P, 470P
- Toshiba e-Studio 385S, 425S
- Toshiba e-Studio 408P², 478P²
- Toshiba e-Studio 408S², 448S², 478S²
- Toshiba e-Studio 409P², 409S²
- Toshiba e-Studio 520P, 525P
- Toshiba e-Studio 528P²

¹ Une mise à jour du certificat d'imprimante est requise. Dans cette version, la mise à jour de la sécurité et des performances de la plate-forme Java supprime la prise en charge de certains algorithmes de signature de certificat, comme MD5 et SHA1. Cette modification empêche le fonctionnement de MVE avec certaines imprimantes. Pour plus d'informations, consultez la [documentation d'aide](#).

² La prise en charge de SNMPv3 doit être activée sur l'imprimante.

³ Si un mot de passe de sécurité avancé est défini sur l'imprimante, MVE ne peut pas la prendre en charge.

⁴ MVE ne peut pas communiquer avec les modèles d'imprimante Lexmark Forms 2580, 2581, 2590 ou 2591 dont l'état est Non prêt. La communication fonctionne uniquement lorsque MVE a déjà communiqué avec l'imprimante lorsque son état était Prêt. L'état de l'imprimante peut être Non prêt s'il existe des erreurs ou des avertissements, par exemple en cas de consommables épuisés. Pour modifier l'état, résolvez l'erreur ou l'avertissement, puis appuyez sur **Prêt**.

Configuration de la base de données

Vous pouvez utiliser Firebird ou Microsoft SQL Server comme base de données principale. Le tableau suivant peut vous aider à décider quelle base de données utiliser.

	Firebird	Microsoft SQL Server
Installation du serveur	Doit être installé sur le même serveur que MVE.	Peut être exécuté à partir de n'importe quel serveur.
Communication	Verrouillé sur localhost uniquement.	Communique via un port statique ou une instance nommée dynamique. La communication SSL/TLS avec un serveur Microsoft SQL sécurisé est prise en charge.
Performances	Affiche des problèmes de performances avec les grands parcs.	Affiche les meilleures performances pour les grands parcs.
Taille de la base de données	Les tailles par défaut des bases de données sont de 6 Mo pour FRAMEWORK et de 1 Mo pour MONITOR et QUARTZ. La table FRAMEWORK passe à une capacité de 1 Ko pour chaque enregistrement d'imprimante ajouté.	Les tailles par défaut des bases de données sont de 20 Mo pour FRAMEWORK et de 4,5 Mo pour MONITOR et QUARTZ. La table FRAMEWORK passe à une capacité de 1 Ko pour chaque enregistrement d'imprimante ajouté.

	Firebird	Microsoft SQL Server
Configuration	Configuré automatiquement pendant l'installation.	Nécessite une configuration pré-installation.

Si vous utilisez Firebird, le programme d'installation de MVE installe et configure Firebird sans qu'aucune autre configuration ne soit requise.

Si vous utilisez Microsoft SQL Server, effectuez les opérations suivantes avant d'installer MVE :

- Autorisez l'application à s'exécuter automatiquement.
- Configurez les bibliothèques réseau de sorte qu'elles utilisent des sockets TCP/IP.
- Créez les bases de données suivantes :

Remarque : Les noms de base de données par défaut sont les suivants. Vous pouvez également fournir des noms de base de données personnalisés.

- FRAMEWORK
- MONITOR
- QUARTZ

- Si vous utilisez une instance nommée, configurez le service Microsoft SQL Server Browser pour que celui-ci démarre automatiquement. Dans le cas contraire, configurez un port statique sur les sockets TCP/IP.
- Créez un compte d'utilisateur disposant des droits de propriétaire de base de données (dbowner) pour les trois bases de données que MVE utilise pour se connecter à et configurer la base de données. Si l'utilisateur détient un compte Microsoft SQL Server, activez les modes d'authentification Microsoft SQL Server et Windows sur Microsoft SQL Server.

Remarque : La désinstallation d'une instance de MVE configurée pour l'utilisation de Microsoft SQL Server n'entraîne pas la suppression des tables et des bases de données qui ont été créées. Après la désinstallation, vous devez supprimer manuellement les bases de données FRAMEWORK, MONITOR et QUARTZ.

- Attribuez les droits dbo à l'utilisateur de la base de données, puis définissez le schéma dbo comme le schéma par défaut.

Configuration d'une exécution en tant qu'utilisateur

Pendant l'installation, vous pouvez spécifier MVE pour qu'il s'exécute en tant que compte système local ou en tant que compte d'utilisateur de domaine. L'exécution de MVE en tant que compte d'utilisateur de domaine offre une installation plus sécurisée. Le compte d'utilisateur de domaine dispose de privilèges limités par rapport à un compte système local.

	Exécuter en tant que compte d'utilisateur de domaine	Exécuter en tant que système local
Autorisations de système local	• Classez tous les accès en fonction de ce qui suit : – \$MVE_INSTALL/tomcat/logs – \$MVE_INSTALL/tomcat/temp – \$MVE_INSTALL/tomcat/work – \$MVE_INSTALL/apps/library – \$MVE_INSTALL/apps/dm-mve/picture – \$MVE_INSTALL/./mve_truststore* – \$MVE_INSTALL/jre/lib/security/cacerts – \$MVE_INSTALL/apps/dm-mve/WEB-INF/ldap – \$MVE_INSTALL/apps/dm-mve/download Où \$MVE_INSTALL est le répertoire d'installation. • Privilèges Windows : LOGON_AS_A_SERVICE	Autorisations d'administrateur
Authentification de connexion à la base de données	• Authentification Windows avec Microsoft SQL Server • Authentification SQL	Authentification SQL
Configuration	Un utilisateur de domaine doit être configuré avant l'installation.	Configuré automatiquement pendant l'installation

Si vous avez configuré MVE en tant que compte d'utilisateur de domaine d'exécution, alors créez l'utilisateur sur le même domaine que le serveur MVE.

Installation de MVE

- 1 Téléchargez le fichier exécutable dans un chemin ne contenant aucun espace.
- 2 Exécutez le fichier en tant qu'administrateur et suivez les instructions qui s'affichent sur l'écran de l'ordinateur.

Remarques :

- Les mots de passe sont hachés et stockés en toute sécurité. Assurez-vous de bien retenir vos mots de passe, ou de les stocker dans un emplacement sécurisé car ils ne peuvent pas être déchiffrés une fois stockés.
- Si vous vous connectez à Microsoft SQL Server via l'authentification Windows, aucune vérification de connexion n'a lieu pendant l'installation. Vérifiez que l'utilisateur désigné pour exécuter le service Windows MVE possède un compte correspondant dans l'instance Microsoft SQL Server. L'utilisateur désigné doit disposer des droits de propriétaire de base de données (dbowner) pour les bases de données FRAMEWORK, MONITOR et QUARTZ.

Installation silencieuse de MVE

Paramètres de base de données pour une installation silencieuse

Paramètre	Description	Valeur
<code>--help</code>	Affiche la liste des options valides.	
<code>--version</code>	Affiche les informations sur le produit.	
<code>--unattendedmodeui <unattendedmodeui></code>	L'interface utilisateur pour le mode automatique.	Par défaut : sans Autorisé : • sans • minimum • minimalWithDialogs
<code>--optionfile <optionfile></code>	Le fichier des options d'installation.	Par défaut :
<code>--debuglevel <debuglevel></code>	Le niveau de verbosité des informations de débogage.	Par défaut : 2 Autorisé : • 0 • 1 • 2 • 3 • 4
<code>--mode <mode></code>	Le mode d'installation.	Par défaut : win32 Autorisé : • win32 • automatique
<code>--debugtrace <debugtrace></code>	Le nom du fichier de débogage.	Par défaut :
<code>--installer-language <installer-language></code>	La sélection de la langue.	Par défaut : fr Autorisé : • fr • es • de • fr • it • pt_BR • zh_CN
<code>--encryptionKey <encryptionKey></code>	La clé de cryptage.	Clé de cryptage : Par défaut :
<code>--prefix <prefix></code>	Le répertoire d'installation.	Par défaut : C:\Program Files
<code>--mveLexmark_runas <mveLexmark_runas></code>	Les options de l'exécution en tant qu'utilisateur.	Par défaut : LOCAL_SYSTEM Autorisé : • LOCAL_SYSTEM • SPECIFIC_USER

Paramètre	Description	Valeur
<code>--serviceRunAsUsername <serviceRunAsUsername></code>	Le nom de l'exécution en tant qu'utilisateur.	Nom d'utilisateur : Par défaut :
<code>--serviceRunAsPassword <serviceRunAsPassword></code>	Le mot de passe de l'exécution en tant qu'utilisateur.	Mot de passe : Par défaut :
<code>--mveLexmark_database <mveLexmark_database></code>	Le type de base de données.	Par défaut : Autorisé : • FIREBIRD • SQL_SERVER
<code>--firebirdUsername <firebirdUsername></code>	Le nom d'utilisateur de la base de données Firebird.	Nom d'utilisateur : Par défaut :
<code>--firebirdPassword <firebirdPassword></code>	Le mot de passe de la base de données Firebird.	Mot de passe : Par défaut :
<code>--firebirdFWDbName <firebirdFWDbName></code>	Le nom de la base de données Firebird pour FRAMEWORK.	Noms de bases de données : Par défaut : FRAMEWORK
<code>--firebirdMNDbName <firebirdMNDbName></code>	Le nom de la base de données Firebird pour MONITOR.	Par défaut : MONITOR
<code>--firebirdQZDbName <firebirdQZDbName></code>	Le nom de la base de données Firebird pour QUARTZ.	Par défaut : QUARTZ
<code>--databaseIPAddress <databaseIPAddress></code>	L'adresse IP ou le nom de l'hôte de la base de données.	Adresse IP ou nom d'hôte : Par défaut :
<code>--databasePort <databasePort></code>	Le numéro de port de la base de données.	Numéro du port : Par défaut :
<code>--instanceName <instanceName></code>	Le nom de l'instance.	Nom de l'instance : Par défaut :
<code>--instanceIdentifier <instanceIdentifier></code>	L'instance.	Par défaut : databasePort Autorisé : • databasePort • instanceName
<code>--databaseUsername <databaseUsername></code>	Le nom d'utilisateur de la base de données.	Nom d'utilisateur : Par défaut :
<code>--databasePassword <databasePassword></code>	Le mot de passe de la base de données.	Mot de passe : Par défaut :
<code>--sqlServerAuthenticationMethod <sqlServerAuthenticationMethod></code>	La méthode d'authentification Microsoft SQL Server.	Par défaut : sqlServerDbAuthentication Autorisé : • sqlServerDbAuthentication • sqlServerWindowsAuthentication
<code>--fWDbName <fWDbName></code>	Le nom de la base de données pour FRAMEWORK.	Noms de bases de données : Par défaut : FRAMEWORK

Paramètre	Description	Valeur
<code>--mNdbName <mNdbName></code>	Le nom de la base de données pour MONITOR.	Par défaut : MONITOR
<code>--qZdbName <qZdbName></code>	Le nom de la base de données pour QUARTZ.	Par défaut : QUARTZ
<code>--mveAdminUsername <mveAdminUsername></code>	Le nom d'utilisateur de l'administrateur.	Nom d'utilisateur : Par défaut : admin
<code>--mveAdminPassword <mveAdminPassword></code>	Le mot de passe administrateur.	Mot de passe : Par défaut :

Accès à MVE

Pour accéder à MVE, utilisez les informations de connexion que vous avez créées pendant l'installation. Vous pouvez également configurer d'autres méthodes de connexion, comme LDAP, Kerberos ou d'autres comptes locaux. Pour plus d'informations, reportez-vous à la section [« Configuration de l'accès utilisateur » à la page 28](#).

- 1 Ouvrez un navigateur Web et saisissez **`https://SERVEUR_MVE/mve/`**, où **SERVEUR_MVE** est le nom d'hôte ou l'adresse IP du serveur hébergeant MVE.
- 2 Le cas échéant, acceptez la clause de non-responsabilité.
- 3 Saisissez vos informations d'authentification.
- 4 Cliquez sur **Se connecter**.

Remarques :

- Après la connexion, assurez-vous de modifier le mot de passe administrateur par défaut qui a été utilisé pendant l'installation. Pour plus d'informations, reportez-vous à la section [« Modification de votre mot de passe » à la page 22](#).
- Si MVE est inactif pendant plus de 30 minutes, l'utilisateur est automatiquement déconnecté.

Modification de la langue

- 1 Ouvrez un navigateur Web et saisissez **`https://SERVEUR_MVE/mve/`**, où **SERVEUR_MVE** est le nom d'hôte ou l'adresse IP du serveur hébergeant MVE.
- 2 Le cas échéant, acceptez la clause de non-responsabilité.
- 3 Dans le coin supérieur droit de la page, sélectionnez la langue.

Modification de votre mot de passe

- 1 Ouvrez un navigateur Web et saisissez **`https://SERVEUR_MVE/mve/`**, où **SERVEUR_MVE** est le nom d'hôte ou l'adresse IP du serveur hébergeant MVE.
- 2 Le cas échéant, acceptez la clause de non-responsabilité.
- 3 Saisissez vos informations d'authentification.

- 4 Cliquez sur **Se connecter**.
- 5 Dans le coin supérieur droit de la page, cliquez sur votre nom d'utilisateur, puis sur **Modifier le mot de passe**.
- 6 Changez le mot de passe.

Maintenance de l'application

Mise à niveau vers MVE 4.0

Avant de commencer la mise à niveau, effectuez les opérations suivantes :

- Sauvegardez les fichiers de base de données et d'application. Pour plus d'informations, reportez-vous à la section [« Sauvegarde et restauration de la base de données » à la page 25](#).
- Si nécessaire, indiquez des noms de base de données personnalisés.

Si vous effectuez la mise à niveau depuis la version 1.x, effectuez d'abord la mise à niveau vers la version 2.0, puis vers la version 3.3 avant de pouvoir mettre à niveau vers la version 4.0. Le processus de migration des stratégies est exécuté uniquement lors de la mise à niveau vers MVE 2.0.

Ordre de mise à niveau valide	3.3 vers 4.0
Ordre de mise à niveau non valide	1.6.x vers 4.0 2.0 vers 4.0

- 1 Sauvegardez vos fichiers de base de données et d'application. Toute mise à niveau ou désinstallation crée un risque de perte de données irrémédiable. Vous pouvez utiliser les fichiers de sauvegarde pour restaurer l'état précédent de l'application en cas d'échec de la mise à niveau.

Avertissement—Danger potentiel : Lorsque vous mettez à niveau MVE, la base de données est modifiée. Ne restaurez pas la sauvegarde d'une base de données créée à partir d'une version précédente.

Remarque : Pour plus d'informations, reportez-vous à la section [« Sauvegarde et restauration de la base de données » à la page 25](#).

- 2 Téléchargez le fichier exécutable vers un emplacement temporaire.
- 3 Exécutez le programme d'installation en tant qu'administrateur et suivez les instructions qui s'affichent sur l'écran de l'ordinateur.

Remarques :

- Lorsque vous effectuez la mise à niveau vers MVE 2.0, les stratégies associées aux imprimantes migrent dans une configuration unique pour chaque modèle d'imprimante. Par exemple, si des stratégies de télécopie, de copie, de papier et d'impression sont associées à une imprimante X792, elles seront consolidées dans une configuration X792. Ce processus ne s'applique qu'aux stratégies associées à des imprimantes. MVE génère un fichier journal qui confirme que les stratégies ont effectivement migré dans une configuration. Pour plus d'informations, reportez-vous à la section [« Où puis-je trouver les fichiers journaux ? » à la page 118](#).
- Une fois la mise à niveau terminée, assurez-vous de vider le cache du navigateur avant d'accéder de nouveau à l'application.
- Lorsque vous mettez à niveau MVE vers la version 3.5 ou ultérieure, les composants de sécurité avancée sont exclus des configurations dans lesquelles ils se trouvent. Si un ou plusieurs composants de sécurité avancée sont identiques, ils sont combinés en un seul composant. Le composant de sécurité avancée créé est automatiquement ajouté à la bibliothèque de composants de sécurité avancée.

Sauvegarde et restauration de la base de données

Remarque : Il existe un risque de perte de données lors de l'exécution des procédures de sauvegarde et de restauration. Assurez-vous d'effectuer les étapes correctement.

Sauvegarde des fichiers de base de données et d'application

Nous vous recommandons de sauvegarder régulièrement votre base de données.

- 1 Arrêtez les services Firebird et Markvision Enterprise.
 - a Ouvrez la boîte de dialogue Exécuter, puis saisissez **services.msc**.
 - b Cliquez avec le bouton droit de la souris sur **Firebird Guardian - DefaultInstance**, puis cliquez sur **Arrêter**.
 - c Cliquez avec le bouton droit de la souris sur **Markvision Enterprise**, puis cliquez sur **Arrêter**.
- 2 Accédez au dossier dans lequel Markvision Enterprise est installé.
Par exemple, **C:\Program Files**
- 3 Sauvegardez les fichiers d'application et de base de données.

Sauvegarde des fichiers d'application

Copiez les fichiers suivants dans un référentiel sûr :

- Lexmark\mve_encryption.jceks
- Lexmark\mve_truststore.p12
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\encryption.properties
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\platform.properties
- Lexmark\Markvision Enterprise\apps\library
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\encryption.properties
- Lexmark\Markvision Enterprise\jre\lib\security\cacerts
- Lexmark\Markvision Enterprise\tomcat\conf\server.xml

Remarque : Assurez-vous que ces fichiers sont correctement stockés. Sans les clés de cryptage du fichier mve_encryption.jceks, les données stockées dans un format crypté dans la base de données et sur le système de fichiers ne peuvent pas être récupérées.

Sauvegarde des fichiers de la base de données

Effectuez l'une des opérations suivantes :

Remarque : Les fichiers suivants utilisent les noms de base de données par défaut. Ces instructions s'appliquent également aux noms de base de données personnalisés.

- Si vous utilisez une base de données Firebird, copiez les fichiers suivants dans un référentiel sécurisé. Sauvegardez régulièrement ces fichiers pour éviter toute perte de données.
 - Lexmark\Markvision Enterprise\firebird\security2.fdb

Si vous utilisez des noms de base de données personnalisés, mettez à jour les éléments suivants :

- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\application.yml
- Lexmark\Markvision Enterprise\firebird\aliases.conf
- Lexmark\Markvision Enterprise\firebird\data\QUARTZ.FDB
- Lexmark\Markvision Enterprise\firebird\data\MONITOR.FDB
- Lexmark\Markvision Enterprise\firebird\data\FRAMEWORK.FDB
- Si vous utilisez Microsoft SQL Server, créez une sauvegarde pour FRAMEWORK, MONITOR et QUARTZ. Pour plus d'informations, contactez votre administrateur Microsoft SQL Server.

4 Redémarrez les services Firebird et Markvision Enterprise.

- a** Ouvrez la boîte de dialogue Exécuter, puis saisissez **services.msc**.
- b** Cliquez avec le bouton droit de la souris sur **Firebird Guardian - DefaultInstance**, puis cliquez sur **Redémarrer**.
- c** Cliquez avec le bouton droit de la souris sur **Markvision Enterprise**, puis cliquez sur **Redémarrer**.

Restauration des fichiers de base de données et d'application

Avertissement—Danger potentiel : Lorsque vous mettez à niveau MVE, la base de données peut être modifiée. Ne restaurez pas la sauvegarde d'une base de données créée à partir d'une version précédente.

1 Arrêtez le service Markvision Enterprise.

Pour plus d'informations, reportez-vous à la section [étape 1](#) de « [Sauvegarde des fichiers de base de données et d'application](#) » à la page 25.

2 Accédez au dossier dans lequel Markvision Enterprise est installé.

Par exemple, **C:\Program Files**

3 Restaurez les fichiers d'application.

Remplacez les fichiers suivants par les fichiers que vous avez enregistrés durant le processus de sauvegarde :

- Lexmark\mve_encryption.jceks
- Lexmark\mve_truststore.p12
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\encryption.properties
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\platform.properties
- Lexmark\Markvision Enterprise\apps\library
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\encryption.properties
- Lexmark\Markvision Enterprise\jre\lib\security\cacerts
- Lexmark\Markvision Enterprise\tomcat\conf\server.xml

Remarque : Vous pouvez restaurer une sauvegarde de base de données sur une nouvelle installation MVE uniquement si la version de ladite installation est la même.

4 Restaurez les fichiers de base de données.

Effectuez l'une des opérations suivantes :

- Si vous utilisez une base de données Firebird, alors remplacez les fichiers suivants que vous avez enregistrés pendant le processus de sauvegarde :

Remarque : Les fichiers suivants utilisent les noms de base de données par défaut. Cette instruction s'applique également aux noms de base de données personnalisés.

- Lexmark\Markvision Enterprise\firebird\security2.fdb

Si vous utilisez des noms de base de données personnalisés, les fichiers suivants sont également restaurés :

- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\application.yml
- Lexmark\Markvision Enterprise\firebird\aliases.conf
- Lexmark\Markvision Enterprise\firebird\data\QUARTZ.FDB
- Lexmark\Markvision Enterprise\firebird\data\MONITOR.FDB
- Lexmark\Markvision Enterprise\firebird\data\FRAMEWORK.FDB
- Si vous utilisez Microsoft SQL Server, contactez votre administrateur Microsoft SQL Server.

5 Redémarrez le service Markvision Enterprise.

Pour plus d'informations, reportez-vous à la section [étape 4](#) de « [Sauvegarde des fichiers de base de données et d'application](#) » à la page 25.

Mise à jour des paramètres du programme d'installation après l'installation

L'utilitaire de mot de passe Markvision Enterprise vous permet de mettre à jour les paramètres de Microsoft SQL Server qui ont été configurés lors de l'installation, mais durant laquelle la réinstallation de MVE n'a pas été effectuée. L'utilitaire vous permet également de mettre à jour les informations d'identification du compte de domaine relatives à l'exécution en tant qu'utilisateur, telles que le nom et le mot de passe d'utilisateur. Vous pouvez également utiliser cet utilitaire pour créer un autre utilisateur administrateur si vous avez oublié vos informations d'identification d'utilisateur administrateur précédentes.

1 Accédez au dossier dans lequel Markvision Enterprise est installé.

Par exemple, **C:\Program Files**

2 Lancez le fichier **mvepwdutility-windows.exe** dans le répertoire Lexmark\Markvision Enterprise\.

3 Sélectionnez une langue, puis cliquez sur **OK > Suivant**.

4 Suivez les instructions qui s'affichent sur l'écran de l'ordinateur.

Configuration de l'accès utilisateur

Aperçu

MVE vous permet d'ajouter des utilisateurs internes directement au serveur MVE ou d'utiliser les comptes utilisateur enregistrés sur un serveur LDAP. Pour plus d'informations sur l'ajout d'utilisateurs externes, reportez-vous à la section « [Gestion des utilisateurs](#) » à la page 29. Pour plus d'informations sur l'utilisation de comptes utilisateur, reportez-vous à la section « [Activation de l'authentification de serveur LDAP](#) » à la page 30.

Lors de l'ajout d'utilisateurs, les rôles doivent être attribués. Pour plus d'informations, reportez-vous à la section « [Présentation des rôles utilisateur](#) » à la page 28.

Lors de l'authentification, le système vérifie les informations d'identification des utilisateurs internes présents dans le serveur MVE. Si MVE ne parvient pas à authentifier l'utilisateur, il tente son authentification sur le serveur LDAP. Si le nom d'utilisateur existe dans le serveur MVE et le serveur LDAP, le mot de passe présent sur le serveur MVE est utilisé.

Présentation des rôles utilisateur

Il est possible d'attribuer les utilisateurs MVE à un ou plusieurs rôles. Selon le rôle, les utilisateurs peuvent effectuer les tâches suivantes :

- **Administrateur** : accès aux tâches de tous les menus et exécution de celles-ci. Un administrateur dispose également de droits administratifs, par exemple l'ajout d'utilisateurs au système ou la configuration des paramètres du système. Seuls les utilisateurs bénéficiant d'un rôle Admin peuvent arrêter n'importe quelle tâche en cours, quel que soit le type d'utilisateur l'ayant lancée.
- **Imprimantes**
 - gestion des profils de recherche,
 - réglage des états d'imprimante,
 - réalisation d'audits,
 - gestion des catégories et des mots clés,
 - programmation d'audits, exportation de données et détection d'imprimantes.
- **Configurations**
 - gestion des configurations, notamment l'importation et l'exportation des fichiers de configuration,
 - téléchargement de fichiers vers la bibliothèque de ressources,
 - attribution de configurations aux imprimantes et leur mise en œuvre,
 - programmation d'un contrôle de conformité et de mises en œuvre de configurations.
 - Déployer des fichiers sur les imprimantes.
 - Mettre à jour le micrologiciel de l'imprimante.
 - Générer les demandes de signature de certificat d'imprimante.
 - Télécharger les demandes de signature de certificat d'imprimante.
- **Gestionnaire des événements**
 - gestion des actions et des événements,
 - attribution d'événements aux imprimantes,
 - test d'actions.

- **Service Desk**

- mise à jour de l'état de l'imprimante,
- redémarrage des imprimantes,
- exécution d'un contrôle de conformité,
- mise en œuvre de configurations sur les imprimantes.

Remarques :

- Tous les utilisateurs MVE peuvent afficher la page des informations de l'imprimante, ainsi que gérer les recherches enregistrées et les affichages.
- Pour plus d'informations sur l'attribution des rôles utilisateur, voir la section « [Gestion des utilisateurs](#) » à la page 29.

Gestion des utilisateurs

- 1 Dans le coin supérieur droit de la page, cliquez sur .
- 2 Cliquez sur **Utilisateur**, puis effectuez l'une des opérations suivantes :

Ajout d'un utilisateur

- a Cliquez sur **Créer**.
- b Saisissez le nom d'utilisateur, l'ID utilisateur et le mot de passe.
- c Sélectionnez les rôles.

Remarque : Pour plus d'informations, reportez-vous à la section « [Présentation des rôles utilisateur](#) » à la page 28.

- d Cliquez sur **Créer un utilisateur**.

Modifier un utilisateur

- a Sélectionnez un ID utilisateur.
- b Configurez les paramètres.
- c Cliquez sur **Enregistrer les modifications**.

Suppression d'utilisateurs

- a Sélectionnez un ou plusieurs utilisateurs.
- b Cliquez sur **Supprimer**, puis confirmez la suppression.

Remarque : Un compte utilisateur est bloqué après trois tentatives de connexion échouées. Seul un utilisateur administrateur peut réactiver le compte utilisateur. Si l'utilisateur administrateur est bloqué, le système le réactive automatiquement au bout de cinq minutes.

Activation de l'authentification de serveur LDAP

Le LDAP est un protocole extensible de plate-forme croisée basé sur des normes, qui s'exécute directement sur TCP/IP. Il est utilisé pour accéder à des bases de données spécialisées, appelées répertoires.

Pour éviter de gérer plusieurs ensembles d'informations d'identification utilisateur, vous pouvez utiliser le serveur LDAP de l'entreprise pour authentifier les ID et mots de passe des utilisateurs.

Pour cela, le serveur LDAP doit contenir des groupes d'utilisateurs correspondant aux rôles d'utilisateur requis. Pour plus d'informations, reportez-vous à la section [« Présentation des rôles utilisateur » à la page 28](#).

- 1 Dans le coin supérieur droit de la page, cliquez sur .
- 2 Cliquez sur **LDAP**, puis sélectionnez **Activer l'authentification LDAP**.
- 3 Dans le champ Nom d'hôte du serveur LDAP, saisissez l'adresse IP ou le nom de l'hôte du serveur LDAP sur lequel l'authentification est effectuée.

Remarque : Si vous souhaitez utiliser la communication chiffrée entre le serveur MVE et le serveur LDAP, utilisez le nom de domaine complet (FQDN).
- 4 Indiquez le numéro de port selon le protocole de chiffrement sélectionné.
- 5 Sélectionnez le protocole de chiffrement.
 - **Aucun**
 - **TLS** : protocole de sécurité commun utilisant le chiffrement des données et l'authentification par certificat pour protéger la communication entre un serveur et un client. Si cette option est sélectionnée, une commande START_TLS est envoyée au serveur LDAP une fois la connexion établie. Utilisez ce paramètre si vous souhaitez une communication sécurisée sur le port 389.
 - **SSL/TLS** : protocole de sécurité utilisant la cryptographie de clé publique pour authentifier les communications entre un serveur et un client. Utilisez cette option si vous souhaitez une communication sécurisée à partir du début de la liaison LDAP. Cette option est généralement utilisée pour le port 636 ou d'autres ports LDAP sécurisés.
- 6 Sélectionnez le type de liaison.
 - **Anonyme** : cette option est sélectionnée par défaut. Le serveur MVE ne produit pas ses informations d'identification ou d'identité pour le serveur LDAP afin que ce dernier utilise ses fonctionnalités de recherche. Cette option est dépréciée dans presque toutes les mises en œuvre LDAP et ne doit jamais être utilisée.
 - **Simple** : le serveur MVE produit les informations d'identification spécifiées pour le serveur LDAP afin que ce dernier utilise ses fonctionnalités de recherche.
 - a Saisissez le nom d'utilisateur de la liaison.
 - b Saisissez le mot de passe de liaison, puis confirmez-le en le saisissant une nouvelle fois.
 - **Kerberos** : pour configurer les paramètres, procédez comme suit :
 - a Saisissez le nom d'utilisateur de la liaison.
 - b Saisissez le mot de passe de liaison, puis confirmez-le en le saisissant une nouvelle fois.
 - c Cliquez sur **Sélectionner un fichier**, puis localisez le fichier krb5.conf.
 - **SPNEGO** : pour configurer les paramètres, procédez comme suit :
 - a Saisissez le nom principal de service.
 - b Cliquez sur **Sélectionner un fichier**, puis localisez le fichier krb5.conf.
 - c Cliquez sur **Sélectionner un fichier**, puis localisez le fichier keytab Kerberos.

Cette option est utilisée uniquement pour configurer le mécanisme de négociation GSSAPI simple et protégé (SPNEGO) afin de prendre en charge la fonctionnalité d'authentification unique.

7 Dans la section Options avancées, configurez les éléments suivants :

- **Base de recherche** : nom unique (DN) du nœud racine. Dans la hiérarchie du serveur de communauté LDAP, ce nœud doit être l'ancêtre du nœud d'utilisateur et du nœud de groupe. Par exemple, **dc=mvptest,dc=com**.

Remarque : Lorsque vous spécifiez le nom unique de la racine, assurez-vous que seuls **dc** et **o** font partie du nom unique de la racine. Si **ou** ou **cn** est l'ancêtre des nœuds d'utilisateur et de groupe, utilisez **ou** ou **cn** dans les bases de recherche des utilisateurs et des groupes.

- **Base de recherche d'utilisateurs** : nœud du serveur de communauté LDAP dans lequel l'objet utilisateur existe. Ce nœud se trouve sous le nom unique de la racine, où tous les nœuds des utilisateurs sont répertoriés. Par exemple, **ou=people**.
- **Filtre de recherche d'utilisateurs** : paramètre de localisation d'un objet utilisateur dans le serveur de communauté LDAP. Par exemple, **(uid={0})**.

Exemples de conditions multiples et d'expressions complexes autorisées

Connexion avec	Dans le champ Filtre de recherche d'utilisateurs, saisissez
Nom commun	(CN={0})
Nom de connexion	(sAMAccountName={0})
Nom principal de l'utilisateur	(userPrincipalName={0})
Numéro de téléphone	(telephoneNumber={0})
Nom de connexion ou nom commun	((sAMAccountName={0}) (CN={0}))

Remarque : Le seul modèle valide est **{0}**, ce qui signifie que MVE recherche le nom de connexion de l'utilisateur MVE.

- **Rechercher un objet dans la base d'utilisateurs et l'ensemble de la sous-arborescence** : le système recherche tous les nœuds sous la base de recherche des utilisateurs.
- **Base de recherche de groupes** : nœud du serveur de communauté LDAP qui contient les groupes d'utilisateurs correspondant aux rôles MVE. Ce nœud se trouve sous le nom unique de la racine, où tous les nœuds de groupe sont répertoriés. Par exemple, **ou=group**.
- **Filtre de recherche de groupes** : paramètre de localisation permettant de rechercher un utilisateur dans un groupe correspondant à un rôle dans MVE.

Remarque : Seuls les modèles **{0}** et **{1}** peuvent être utilisés. Si **{0}** est utilisé, MVE recherche le nom unique de l'utilisateur LDAP. Si **{1}** est utilisé, MVE recherche le nom de connexion de l'utilisateur MVE.

- **Attribut de rôle de groupe** : saisissez l'attribut LDAP pour le nom complet du groupe. Un attribut LDAP a une signification spécifique et définit une correspondance entre l'attribut et un nom de champ. Par exemple, l'attribut LDAP **cn** est associé au champ Nom complet. L'attribut LDAP **commonname** est également associé au champ Nom complet. En général, cet attribut doit conserver la valeur par défaut **cn**.
- **Rechercher un objet dans la base d'utilisateurs et l'ensemble de la sous-arborescence** : le système recherche tous les nœuds sous la base de recherche des groupes.

8 Dans la section Mappage des rôles des groupes LDAP vers MVE, saisissez les noms des groupes LDAP correspondant aux rôles MVE.

Remarques :

- Pour plus d'informations, reportez-vous à la section [« Présentation des rôles utilisateur » à la page 28](#).
- Vous pouvez attribuer un groupe LDAP à plusieurs rôles MVE. Vous pouvez également saisir plusieurs groupes LDAP dans un champ de rôle, en utilisant la barre verticale (|) pour séparer plusieurs groupes. Par exemple, pour inclure les groupes **admin** et **assets** pour le rôle Admin, saisissez **admin|assets** dans le champ du rôle Groupes LDAP pour l'administrateur.
- Si vous souhaitez utiliser uniquement le rôle Admin et non les autres rôles MVE, laissez les champs vides.

9 Cliquez sur **Enregistrer les modifications**.

Installation de certificats de serveur LDAP

Pour établir une communication chiffrée entre le serveur MVE et le serveur LDAP, MVE doit approuver le certificat du serveur LDAP. Dans l'architecture MVE, lorsque MVE procède à l'authentification au moyen d'un serveur LDAP, MVE est le client et le serveur LDAP est le pair.

- 1** Dans le coin supérieur droit de la page, cliquez sur .
- 2** Cliquez sur **LDAP**, puis configurez les paramètres LDAP. Pour plus d'informations, reportez-vous à la section [« Activation de l'authentification de serveur LDAP » à la page 30](#).
- 3** Cliquez sur **Tester LDAP**.
- 4** Saisissez un nom et un mot de passe d'utilisateur LDAP valides, puis cliquez sur **Démarrer le test**.
- 5** Analysez le certificat pour confirmer sa validité, puis acceptez-le.

Détection des imprimantes

Création d'un profil de recherche

Utilisez un profil de recherche pour rechercher des imprimantes sur votre réseau et les ajouter au système. Dans un profil de recherche, vous pouvez inclure ou exclure une liste ou une plage d'adresses IP ou de noms d'hôte en effectuant l'une ou l'autre des actions suivantes :

- Ajout d'entrées une par une
- Importation d'entrées à l'aide d'un fichier TXT ou CSV

Vous pouvez également attribuer et appliquer automatiquement une configuration à un modèle d'imprimante compatible. Une configuration peut contenir des paramètres d'imprimante, des applications, des licences, le microcode et les certificats d'autorité de certification qui peuvent être déployés sur les imprimantes.

- 1 Dans le menu Imprimantes, cliquez sur **Profils de recherche > Créer**.
- 2 Dans la section Général, saisissez un nom unique et une description pour le profil de recherche, puis configurez les options suivantes :
 - **Délai** : durée d'attente par le système d'une réponse de l'imprimante.
 - **Nouvelles tentatives** : nombre de tentatives effectuées par le système pour communiquer avec une imprimante.
 - **Gérer automatiquement les imprimantes détectées** : l'état des imprimantes nouvellement détectées est automatiquement défini sur Géré et l'état Nouveau est omis lors de la détection.
- 3 Dans la section Adresses, effectuez l'une des procédures suivantes :

Ajouter des adresses

- a** Sélectionnez **Inclure** ou **Exclure**.
- b** Saisissez l'adresse IP, le nom de l'hôte, le sous-réseau ou la plage d'adresses IP.

Addresses

10.194.25.70-77

+ Add

Delete

Import

Include

Exclude

10.20.15.*10.20.*, 10.20.15.3-10.20.15.45, myprinter.domain.com, 2001:db8:0:0:0:0:2:1,

	Include/Exclude
☐ 10.195.7.203	Include
☐ 10.195.0.208	Include

N'ajoutez qu'une seule entrée à la fois. Utilisez les formats suivants pour les adresses :

- **10.195.10.1** (adresse IPv4 unique)
- **monimprimante.exemple.com** (nom d'hôte unique)
- **10.195.10.3-10.195.10.255** (plage d'adresses IPv4)
- **10.195.*.*** (caractères génériques)
- **10.195.10.1/22** (notation CIDR [IPv4 Classless Inter-Domain Routing])
- **2001:db8:0:0:0:0:2:1** (adresse IPv6 complète)
- **2001:db8::2:1** (adresse IPv6 réduite)

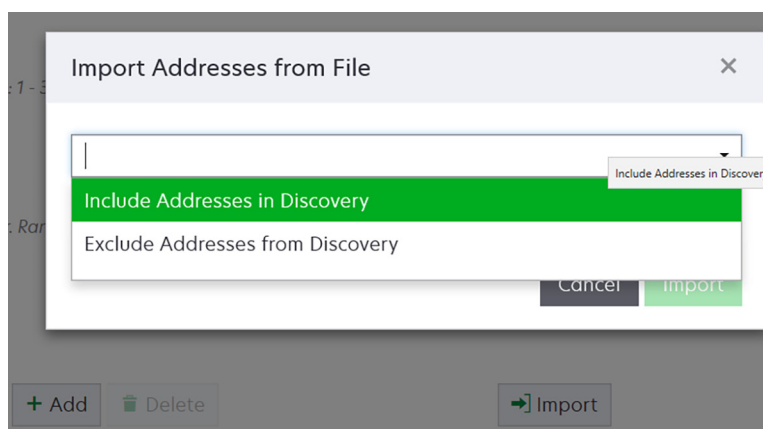
Remarque : Si des profils de recherche distincts sont créés pour les adresses IPv6 et IPv4 de la même imprimante, la dernière adresse détectée s'affiche. Par exemple, si une imprimante est détectée via IPv6, puis de nouveau via IPv4, seule l'adresse IPv4 s'affiche dans la liste des imprimantes.

c Cliquez sur **Ajouter**.

Importer les adresses

a Cliquez sur **Importer**.

b Choisissez si vous souhaitez inclure ou exclure des adresses IP au cours de la détection.



c Accédez au fichier texte qui contient une liste d'adresses. Chaque entrée d'adresse doit figurer sur une ligne distincte.

Exemple de fichier texte

```
10.195.10.1
myprinter.example.com
10.195.10.3-10.195.10.255
10.195.*.*
10.195.10.1/22
2001:db8:0:0:0:0:2:1
2001:db8::2:1
```

d Cliquez sur **Importer**.

4 Dans la section SNMP, sélectionnez **Version 1.2c** ou **Version 3**, puis définissez les autorisations d'accès.

Remarque : Pour détecter des imprimantes à l'aide de SNMP version 3, créez un nom d'utilisateur et un mot de passe dans l'instance d'Embedded Web Server sur l'imprimante, puis redémarrez l'imprimante. Si aucune connexion ne peut être établie, relancez la détection des imprimantes. Pour plus d'informations, reportez-vous au *Guide de l'administrateur Embedded Web Server - Sécurité* pour votre imprimante.

5 Le cas échéant, dans la section Saisir les informations d'identification, sélectionnez la méthode d'authentification que les imprimantes utilisent, puis saisissez les informations d'identification.

Remarque : Cette fonction vous permet d'établir une communication avec les imprimantes sécurisées pendant la détection. Les informations d'identification correctes doivent être fournies pour effectuer des tâches sur les imprimantes sécurisées, telles que l'audit, la mise à jour de l'état ou la mise à jour du microcode.

6 Si nécessaire, dans la section Attribuer des configurations, associez une configuration à un modèle d'imprimante. Pour plus d'informations sur la création d'une configuration, reportez-vous à la section [« Création d'une configuration » à la page 67](#).

7 Cliquez sur **Enregistrer le profil** ou **Enregistrer et exécuter le profil**.

Remarque : Il est possible de programmer une détection pour qu'elle s'exécute à intervalle régulier. Pour plus d'informations, reportez-vous à la section « [Création d'une programmation](#) » à la page 112.

Gestion des profils de recherche

1 Dans le menu Imprimantes, cliquez sur **Profils de recherche**.

2 Effectuez l'une des opérations suivantes :

Modifier un profil

- a** Sélectionnez un profil, puis cliquez sur **Modifier**.
- b** Configurez les paramètres.
- c** Cliquez sur **Enregistrer le profil** ou **Enregistrer et exécuter le profil**.

Copier un profil

- a** Sélectionnez un profil, puis cliquez sur **Copier**.
- b** Configurez les paramètres.
- c** Ajoutez les adresses IP. Pour plus d'informations, reportez-vous à la section « [Ajouter des adresses](#) » à la page 33.
- d** Cliquez sur **Enregistrer le profil** ou **Enregistrer et exécuter le profil**.

Supprimer un profil

- a** Sélectionnez un ou plusieurs profils.
- b** Cliquez sur **Supprimer**, puis confirmez la suppression.

Exécuter un profil

- a** Sélectionnez un ou plusieurs profils.
- b** Cliquez sur **Exécuter**. Vérifiez l'état de la détection dans le menu Tâches.

Exemple de scénario : Détection des imprimantes

La société ABC est une grande entreprise de fabrication occupant un bâtiment de neuf étages. La société vient d'acheter 30 nouvelles imprimantes Lexmark, réparties sur les neuf étages. En tant que membre du personnel informatique, vous devez ajouter ces nouvelles imprimantes à MVE. Les imprimantes sont déjà connectées au réseau, mais vous ne connaissez pas toutes les adresses IP.

Vous souhaitez sécuriser les nouvelles imprimantes suivantes du service Comptabilité.

10.194.55.60

10.194.56.77

10.194.55.71

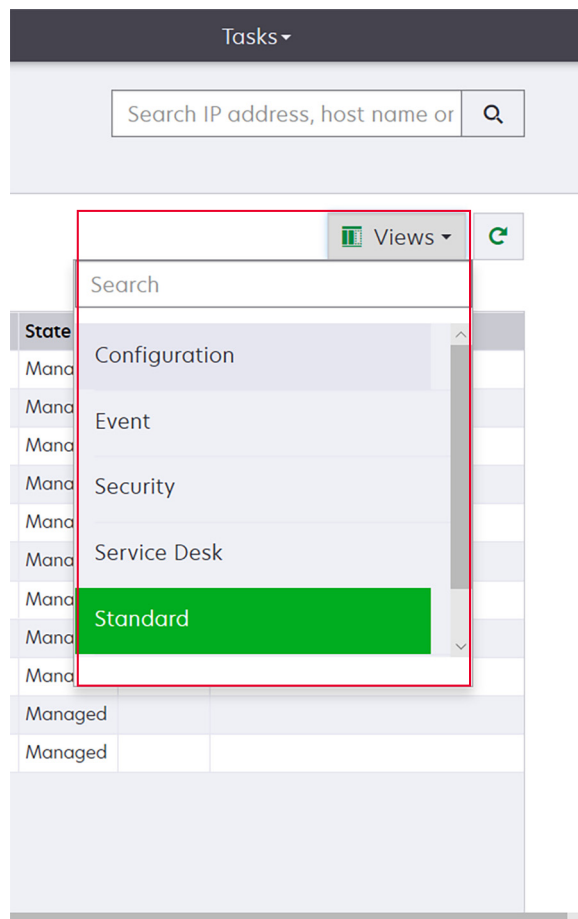
10.194.63.27

10.194.63.10

Exemple de mise en œuvre

- 1** Créez un profil de détection pour les imprimantes du service Comptabilité.
- 2** Ajoutez les cinq adresses IP.
- 3** Créez une configuration qui sécurise les imprimantes spécifiées.
- 4** Incluez les configurations dans le profil de détection.
- 5** Enregistrez et exécutez le profil.
- 6** Créez un autre profil de détection pour les autres imprimantes.
- 7** Incluez les adresses IP à l'aide d'un caractère générique. Utilisez le suivant : **10.194.*.***
- 8** Excluez les adresses IP des cinq imprimantes du service Comptabilité.
- 9** Enregistrez, puis exécutez le profil.

- Modifiez la vue Listes des imprimantes. Pour plus d'informations, reportez-vous à la section « [Modification de la vue Liste des imprimantes](#) » à la page 43.



Remarque : Si vous utilisez la zone de recherche, la recherche porte sur toutes les imprimantes du système. Les filtres sélectionnés et les recherches enregistrées sont ignorés. Si vous exécutez une recherche enregistrée, les critères indiqués dans celle-ci sont utilisés. Les filtres sélectionnés et l'adresse IP ou le nom d'hôte saisi dans le champ de recherche sont ignorés. Vous pouvez également utiliser les filtres pour affiner les résultats de la recherche actuelle.

- Utilisez les filtres.

The screenshot shows the 'All Printers' interface. On the left, there are filter sections: 'Keywords' (No keywords (4)), 'Subnets' (157184.205.* (4), 10.195.7.* (3), 10.194.29.* (1), 10.195.0.* (1), 10.195.6.* (1)), 'Supply Status Severity' (Unknown supply status (4)), 'Printer Status Severity' (Unknown printer status (4)), 'Configuration Conform...' (Clear), and 'Model Names' (Clear). On the right, there are buttons for 'Printer', 'Configure', 'Assign', and 'Security'. Below these, it says '4 total items' and shows a table of printers.

IP Address	Model	Contact Name
157184.205.135	Lexmark B2236dw	
157184.205.186	Lexmark CX922de	
157184.205.212	Lexmark CX725	
157184.205.250	Lexmark MX611dhe	

- Exécutez une recherche enregistrée. Pour plus d'informations, reportez-vous à la section « [Exécution d'une recherche enregistrée](#) » à la page 46.

The screenshot shows the 'All Printers' interface with the 'Run Saved Search' dropdown menu open. The menu lists various search categories: All Printers, Managed (Changed) Printers, Managed Printers, Managed (Found) Printers, Managed (Missing) Printers, Managed (Normal) Printers, New Printers, Retired Printers, Unmanaged Printers, and C2lite. The background shows the same printer list as the previous screenshot.

- Pour trier les imprimantes, cliquez sur un en-tête de colonne dans le tableau de la liste des imprimantes. Les imprimantes sont triées en fonction de l'en-tête de colonne sélectionné.

- Pour afficher plus d'informations sur les imprimantes, redimensionnez les colonnes. Placez votre curseur sur la bordure verticale de l'en-tête de la colonne, puis faites glisser la bordure vers la gauche ou vers la droite.

Affichage des informations de l'imprimante

Pour voir la liste complète des informations, vérifiez qu'un audit de l'imprimante est effectué. Pour plus d'informations, reportez-vous à la section « [Audit d'imprimantes](#) » à la page 59.

1 Dans le menu Imprimantes, cliquez sur **Listes des imprimantes**.

2 Cliquez sur l'adresse IP de l'imprimante.

3 Consultez les informations suivantes :

- **Etat** : état de l'imprimante.
- **Fournitures** : détails et pourcentage restant des fournitures.
- **Identification** : informations d'identification réseau de l'imprimante.

Remarque : Les informations du fuseau horaire sont disponibles uniquement sur certains modèles d'imprimante.

- **Dates** : date d'ajout de l'imprimante au système, date de détection et date de la dernière vérification.
- **Microcode** : propriétés et niveaux de code du microcode de l'imprimante.
- **Fonctionnalité** : fonctions de l'imprimante.
- **Options mémoire** : taille du disque dur et espace libre sur la ou les cartes flash utilisateur.
- **Options d'entrée** : paramètres des bacs disponibles.
- **Options de sortie** : paramètres des réceptacles disponibles.
- **Applications eSF** : informations sur les applications Embedded Solutions Framework (eSF) installées sur l'imprimante.
- **Statistiques imprimante** : valeurs spécifiques à chacune des propriétés de l'imprimante.
- **Détails des modifications** : informations sur les modifications apportées à l'imprimante.

Remarque : Ces informations s'appliquent uniquement aux imprimantes dont l'état est Géré (Modifié). Pour plus d'informations, reportez-vous à la section « [Présentation des états du cycle de vie de l'imprimante](#) » à la page 44.

- **Informations d'identification de l'imprimante** : informations d'identification utilisées dans la configuration attribuée à l'imprimante.
- **Certificat de l'imprimante par défaut** : propriétés du certificat de l'imprimante.

Remarques :

- Cette information est disponible uniquement sur certains modèles d'imprimante.
- L'état de validité Va bientôt expirer indique que le certificat expire dans 30 jours.
- **Propriétés de la configuration** : propriétés de la configuration attribuée à l'imprimante.
- **Alertes actives** : alertes de l'imprimante en attente d'effacement.
- **Événements attribués** : événements attribués à l'imprimante.

Exportation des données de l'imprimante

MVE vous permet d'exporter les informations de l'imprimante qui sont disponibles dans l'affichage actuel.

- 1 Sur le menu Imprimantes, cliquez sur **Liste des imprimantes**.
- 2 Sélectionnez une ou plusieurs imprimantes.
- 3 Cliquez sur **Imprimante** > **Exporter des données**.

Remarques :

- Les données exportées sont enregistrées dans un fichier CSV.
- Il est possible de programmer l'exportation des données pour qu'elle s'exécute à intervalle régulier. Pour plus d'informations, reportez-vous à la section [« Création d'une programmation » à la page 112](#).

Gestion des vues

Les vues vous permettent de personnaliser les informations qui s'affichent dans la page Listes des imprimantes.

- 1 Dans le menu Imprimantes, cliquez sur **Vues**.
- 2 Effectuez l'une des opérations suivantes :

Créer une vue

- a Cliquez sur **Créer**.
- b Saisissez un nom unique pour la vue, ainsi que sa description.
- c Dans la section Afficher les colonnes, dans le menu Colonne 1, sélectionnez la colonne des identificateurs.

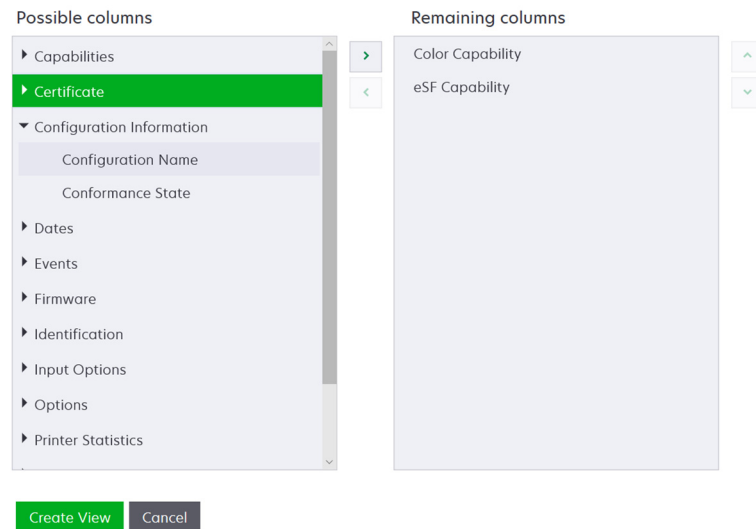
View Columns

Select the information you want to view for each printer.

Column 1

IP Address
Host Name
System Name
Serial Number

- d** Dans la section Colonnes possibles, développez une catégorie, sélectionnez les informations que vous souhaitez afficher sous forme de colonne, puis cliquez sur >.



- **Fonctionnalités** : indique si les fonctions sélectionnées sont prises en charge sur l'imprimante.
- **Certificat** : affiche la date de création du certificat d'imprimante, l'état de l'inscription, la date d'expiration, la date de renouvellement, le numéro de révision, l'objet du certificat, la validité et l'état de la signature.
- **Informations de configuration** : affiche les informations de l'imprimante relatives à la configuration, comme la conformité, le nom de la configuration et l'état.
- **Dates** : affiche la dernière vérification, le dernier contrôle de conformité, la dernière détection et la date de l'ajout de l'imprimante au système.
- **Événements** : affiche les informations relatives aux événements de l'imprimante.
- **Microcode** : affiche les informations relatives au microcode, comme sa version.
- **Identification** : affiche des informations sur l'imprimante, comme l'adresse IP, le nom de l'hôte et le numéro de série.
- **Options d'entrée** : affiche des informations sur les options d'entrée, comme le format du bac d'alimentation et le type de support.
- **Options** : affiche des informations sur les options de l'imprimante, comme le disque dur et le lecteur flash.
- **Statistiques imprimante** : affiche des informations sur l'utilisation de l'imprimante, comme le nombre de pages imprimées ou numérisées et le nombre total de travaux de télécopie envoyés.
- **Solutions** : affiche les applications eSF installées sur l'imprimante et leurs numéros de version.
- **Etat** : affiche l'état de l'imprimante et des fournitures.
- **Fournitures** : affiche les informations liées aux fournitures.

- e** Cliquez sur **Créer une vue**.

Modifier une vue

- Sélectionnez une vue.
- Cliquez sur **Modifier**, puis modifiez les paramètres.
- Cliquez sur **Enregistrer les modifications**.

Copier une vue

- a Sélectionnez une vue.
- b Cliquez sur **Copier**, puis configurez les paramètres.
- c Cliquez sur **Créer une vue**.

Supprimer des vues

- a Sélectionnez une ou plusieurs vues.
- b Cliquez sur **Supprimer**, puis confirmez la suppression.

Définir une vue par défaut

- a Sélectionnez une vue.
- b Cliquez sur **Définir par défaut**.

Les vues suivantes sont générées par le système et ne peuvent être ni modifiées, ni supprimées :

- Configuration
- Liste d'imprimantes
- Événement
- Sécurité
- Service Desk
- Standard

Modification de la vue Liste des imprimantes

Pour plus d'informations, reportez-vous à la section « [Gestion des vues](#) » à la page 41.

- 1 Dans le menu Imprimantes, cliquez sur **Liste des imprimantes**.
- 2 Cliquez sur **Vues**, puis sélectionnez une vue.

Filtrage des imprimantes via la barre de recherche

Notez les informations suivantes lorsque vous utilisez la barre de recherche pour rechercher des imprimantes.

- Pour rechercher une adresse IP, assurez-vous de saisir l'adresse ou la plage IP complète.

Par exemple :

- 10.195.10.1
- 10.195.10.3-10.195.10.255
- 10.195.*.*
- 2001:db8:0:0:0:0:2:1

- Si la chaîne de recherche ne correspond pas à une adresse IP complète, les imprimantes sont recherchées en fonction de leur nom d'hôte, de système ou de leur numéro de série.
- Le trait de soulignement (_) peut être utilisé comme caractère générique.

Gestion des mots clés

Les mots clés permettent de créer des étiquettes personnalisées et de les attribuer aux imprimantes.

1 Dans le menu Imprimantes, cliquez sur **Mots clés**.

2 Effectuez l'une des opérations suivantes :

- Ajoutez, modifiez ou supprimez une catégorie.

Remarque : Les catégories regroupent les mots clés entre eux.

- Ajoutez, modifiez ou supprimez un mot clé.

Pour plus d'informations sur l'attribution de mots clés aux imprimantes, voir la section [« Attribution de mots-clés aux imprimantes » à la page 64](#).

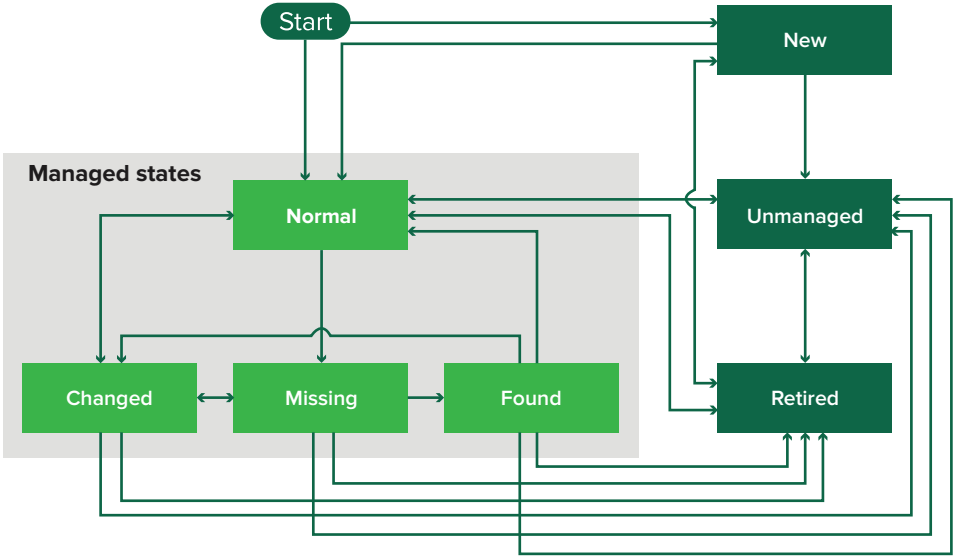
Utilisation des recherches enregistrées

Présentation des états du cycle de vie de l'imprimante

Les recherches enregistrées générées par le système affichent les états du cycle de vie suivants pour les imprimantes :

- **Toutes les imprimantes** : toutes les imprimantes du système.
- **Imprimantes gérées** : les états des imprimantes affichées peuvent être les suivants :
 - Géré (Normal)
 - Géré (Modifié)
 - Géré (Manquant)
 - Géré (Trouvé)
- **Imprimantes gérées (Modifiées)** : imprimantes du système dont les propriétés suivantes ont été modifiées à la dernière vérification :
 - Identifiant de l'imprimante
 - Nom de l'hôte
 - Nom du contact
 - Emplacement du contact
 - Taille de la mémoire
 - Recto verso
 - Fournitures (sauf niveaux)
 - Options d'entrée
 - Options de sortie
 - Applications eSF
 - Certificat de l'imprimante par défaut
- **Imprimantes gérées (Trouvées)** : imprimantes qui ont été signalées comme manquantes, mais qui ont été trouvées depuis.
- **Imprimantes gérées (Manquantes)** : imprimantes avec lesquelles le système n'a pas pu communiquer.
- **Imprimantes gérées (Normales)** : imprimantes du système dont les propriétés sont restées les mêmes depuis la dernière vérification.

- **Nouvelles imprimantes** : imprimantes récemment détectées et non définies automatiquement sur l'état Géré.
- **Imprimantes retirées** : imprimantes qui ne sont plus actives dans le système.
- **Imprimantes non gérées** : imprimantes manuellement exclues des opérations exécutées par le système.



Etat d'origine	Etat résultant	Transition
Démarrer	Normal	Déecté. ¹
Démarrer	Nouveau	Déecté. ²
Toute	Normal, Non géré ou Retiré	Manuel (Manquant ne devient pas Normal).
Retiré	Normal	Déecté. ¹
Retiré	Nouveau	Déecté. ²
Normal, Manquant ou Trouvé	Modifié	Nouvelle adresse lors de la détection.
Normal	Modifié	Les propriétés d'audit ne correspondent pas à celles présentes dans la base de données.
Normal, Modifié ou Trouvé	Manquant	Introuvable à l'audit ou la mise à jour.
Modifié	Normal	Les propriétés d'audit correspondent à celles présentes dans la base de données.
Manquant	Trouvé	Déectée à l'audit ou la mise à jour.
Trouvé	Normal	Déectée à l'audit ou la mise à jour.

¹ Le paramètre Gérer automatiquement les imprimantes déctées est activé dans le profil de recherche.

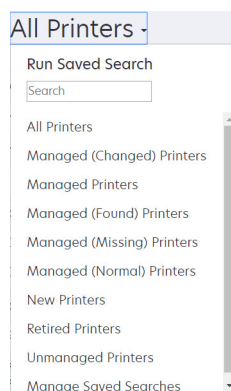
² Le paramètre Gérer automatiquement les imprimantes déctées est désactivé dans le profil de recherche.

Exécution d'une recherche enregistrée

Une recherche enregistrée est un ensemble enregistré de paramètres qui renvoie les dernières informations d'imprimante correspondant aux paramètres.

Vous pouvez créer et exécuter une recherche enregistrée personnalisée ou exécuter les recherches enregistrées par défaut générées par le système. Les recherches enregistrées générées par le système affichent les états du cycle de vie des imprimantes. Pour plus d'informations, reportez-vous à la section [« Présentation des états du cycle de vie de l'imprimante » à la page 44](#).

- 1 Dans le menu Imprimantes, cliquez sur **Listes des imprimantes**.
- 2 Dans le menu déroulant, sélectionnez une recherche enregistrée.



Création d'une recherche enregistrée

Utilisation des filtres

- 1 Dans le menu Imprimantes, cliquez sur **Listes des imprimantes**.
- 2 A gauche de la page, sélectionnez les filtres.
Remarque : les filtres sélectionnés sont répertoriés au-dessus de l'en-tête des résultats de recherche.
- 3 Cliquez sur **Enregistrer**, puis saisissez un nom unique pour la recherche enregistrée ainsi que sa description.
- 4 Cliquez sur **Créer une recherche enregistrée**.

Utilisation de la page Recherche enregistrée

- 1 Dans le menu Imprimantes, cliquez sur **Recherches enregistrées > Créer**.
- 2 Dans la section Général, saisissez un nom unique pour la recherche enregistrée ainsi que sa description.
- 3 Dans la section Règles et groupes de règles du menu Correspondance, indiquez si les résultats de recherche doivent correspondre à toutes les règles ou uniquement à certaines de ces règles.
- 4 Effectuez l'une des opérations suivantes :

Ajouter une règle

- a Cliquez sur **Ajouter une règle**.
- b Spécifiez le paramètre, l'opération et la valeur de la règle de recherche. Pour plus d'informations, reportez-vous à la section « [Présentation des paramètres de règles de recherche](#) » à la page 47.

Ajouter un groupe de règles

Un groupe de règles contient une combinaison de règles. Si **N'IMPORTE quel(le) règle ou groupe de règles** est activé dans le menu Correspondance, le système recherche les imprimantes satisfaisant toutes les règles dans le groupe de règles. Si **TOUTES les règles et TOUS les groupes de règles** est activé dans le menu Correspondance, le système recherche les imprimantes satisfaisant au moins une règle dans le groupe de règles.

- a Cliquez sur **Ajouter un groupe de règles**.
- b Spécifiez le paramètre, l'opération et la valeur de la règle de recherche. Pour plus d'informations, reportez-vous à la section « [Présentation des paramètres de règles de recherche](#) » à la page 47.
- c Pour ajouter une autre règle, cliquez sur **Ajouter une règle**.

- 5 Cliquez sur **Créer une recherche enregistrée** ou **Créer et exécuter une recherche enregistrée**.

Présentation des paramètres de règles de recherche

Recherchez des imprimantes à l'aide d'un ou plusieurs des paramètres suivants :

Paramètre	Description
Identification de propriété	Valeur du paramètre d'identification de propriété sur l'imprimante.
Date de création du certificat	Date à laquelle le certificat a été créé.
Etat de l'inscription du certificat	Etat de l'inscription du certificat.
Date d'expiration du certificat	Date à laquelle le certificat expire.

Paramètre	Description
Date de renouvellement du certificat	Date à laquelle le certificat est renouvelé.
Numéro de révision du certificat	Numéro de révision du certificat.
Etat de signature du certificat	Etat du certificat.
Etat de validité du certificat	Validité du certificat. Remarque : Un état Va bientôt expirer indique que le certificat expire dans 30 jours.
Fonction de couleur	L'imprimante imprime en couleur ou en noir et blanc.
Configuration	Nom de la configuration attribuée à l'imprimante.
Conformité de la configuration	Etat de conformité de l'imprimante par rapport à la configuration attribuée.
Emplacement du contact	Valeur du paramètre d'emplacement du contact sur l'imprimante.
Nom du contact	Valeur du paramètre de nom du contact sur l'imprimante.
Copie	L'imprimante prend en charge la fonction de copie.
Date : Ajouté au système	Date d'ajout de l'imprimante au système.
Date : Dernier audit	Date du dernier audit de l'imprimante.
Date : Dernière vérification de conformité	Date de la dernière vérification de conformité de la configuration de l'imprimante.
Date : Dernière détection	Date de la dernière détection de l'imprimante.
Chiffrement du disque	L'imprimante est configurée pour le chiffrement du disque dur.
Effacement du disque	L'imprimante est configurée pour l'effacement du disque.
Recto verso	L'imprimante prend en charge l'impression recto verso.
Fonction eSF	L'imprimante prend en charge la gestion des applications eSF.
Informations eSF	Informations relatives à l'application eSF installée sur l'imprimante, comme le nom, l'état et la version.
Nom de l'événement	Nom des événements attribués.
Nom du télécopieur	Valeur du paramètre de nom du télécopieur sur l'imprimante.
N° de télécopieur	Valeur du paramètre du numéro de télécopie sur l'imprimante.
Réception de télécopie	L'imprimante prend en charge la réception des télécopies.
Informations sur le microcode	Informations sur le microcode installé sur l'imprimante. • Nom : nom du microcode. Par exemple, Base ou Noyau. • Version : version du microcode de l'imprimante.
Nom d'hôte	Nom de l'hôte de l'imprimante.
Adresse IP	Adresse IP de l'imprimante. Remarque : Vous pouvez utiliser un astérisque à la place des trois derniers octets pour rechercher plusieurs entrées. Par exemple : 123.123.123.* , 123.123.*.* , 123.*.*.* , 2001:db8::2:1 et 2001:db8:0:0:0:0:2:1 .
Mot clé	Mots clés attribués.
Historique du nombre de pages	Nombre total de pages de l'imprimante.
Adresse MAC	Adresse MAC de l'imprimante.

Paramètre	Description
Compteur de maintenance	Valeur du compteur de maintenance de l'imprimante.
Fabricant	Nom du fabricant de l'imprimante.
Technologie de marquage	Technologie de marquage prise en charge par l'imprimante.
Fonction MFP	L'imprimante est un produit multifonction (MFP).
Modèle	Nom du modèle d'imprimante.
Numéro de série modulaire	Le numéro de série modulaire.
Etat de l'imprimante	Etat de l'imprimante. Par exemple : Prêt, Bourrage papier, Tiroir 1 manquant .
Gravité de l'état de l'imprimante	Valeur de l'état de gravité le plus important de l'imprimante. Par exemple, Inconnu, Prêt, Avertissement ou Erreur .
Profil	L'imprimante prend en charge les profils.
Numériser vers un email	L'imprimante prend en charge la numérisation vers un courrier électronique.
Numériser vers télécopie	L'imprimante prend en charge la numérisation vers une télécopie.
Numériser vers le réseau	L'imprimante prend en charge la numérisation vers le réseau.
Etat de la communication sécurisée	Etat de sécurité ou d'authentification de l'imprimante.
Numéro de série	Numéro de série de l'imprimante.
Etat	Etat actuel de l'imprimante dans la base de données.
Etat des consommables	Etat des consommables de l'imprimante.
Gravité de l'état des consommables	Valeur de l'état de gravité le plus important des consommables de l'imprimante. Par exemple, Inconnu, OK, Avertissement ou Erreur .
Nom du système	Nom du système de l'imprimante.
Fuseau horaire	Fuseau horaire de la région dans laquelle l'imprimante se trouve.
TLI	Valeur du paramètre TLI sur l'imprimante.

Utilisez les opérateurs suivants lorsque vous recherchez des imprimantes :

- **Correspond exactement à** : un paramètre est égal à une valeur spécifiée.
- **N'est pas** : un paramètre n'est pas égal à une valeur spécifiée.
- **Contient** : un paramètre contient une valeur spécifiée.
- **Ne contient pas** : un paramètre ne contient pas une valeur spécifiée.
- **Commence par** : un paramètre commence par une valeur spécifiée.
- **Se termine par** : un paramètre se termine par une valeur spécifiée.

Remarque : Pour rechercher les imprimantes dont les paramètres possèdent des valeurs vides, utilisez **_EMPTY_OR_NULL_**. Par exemple, pour rechercher les imprimantes dont le champ Valeur pour Nom du télécopieur est vide, saisissez **_EMPTY_OR_NULL_**.

Gestion des recherches enregistrées

1 Dans le menu Imprimantes, cliquez sur **Recherches enregistrées**.

2 Effectuez l'une des opérations suivantes :

Modifier une recherche enregistrée

- a Sélectionnez une recherche enregistrée, puis cliquez sur **Modifier**.

Remarque : Les recherches enregistrées générées par le système ne peuvent pas être modifiées. Pour plus d'informations, reportez-vous à la section « [Présentation des états du cycle de vie de l'imprimante](#) » à la page 44.

- b Configurez les paramètres.
- c Cliquez sur **Enregistrer les modifications** ou **Enregistrer et Exécuter**.

Copier une recherche enregistrée

- a Sélectionnez une recherche enregistrée, puis cliquez sur **Copier**.
- b Configurez les paramètres.
- c Cliquez sur **Créer une recherche enregistrée** ou **Créer et exécuter une recherche enregistrée**.

Supprimer des recherches enregistrées

- a Sélectionnez une ou plusieurs recherches enregistrées.

Remarque : Les recherches enregistrées générées par le système ne peuvent pas être supprimées. Pour plus d'informations, reportez-vous à la section « [Présentation des états du cycle de vie de l'imprimante](#) » à la page 44.

- b Cliquez sur **Supprimer**, puis confirmez la suppression.

Exemple de scénario : Surveillance des niveaux de toner de votre parc

En tant que membre du personnel informatique de la société ABC, vous devez organiser le parc d'imprimantes pour le surveiller facilement. Vous souhaitez surveiller l'utilisation du toner des imprimantes pour déterminer si les fournitures doivent être remplacées.

Exemple de mise en œuvre

- 1 Créez une recherche enregistrée qui récupère les imprimantes dont les fournitures présentent des erreurs ou des avertissements.

Exemple de règle pour votre recherche enregistrée

Paramètre : **Gravité de l'état des fournitures**

Opération : **N'est pas**

Valeur : **Fournitures OK**

- 2 Créez une vue qui indique l'état, la capacité et le niveau des fournitures de chaque imprimante.

Exemple de colonnes à afficher dans la vue Fournitures

Etat des fournitures

Capacité de la cartouche noir

Niveau de la cartouche noir

Capacité de la cartouche cyan

Niveau de la cartouche cyan

Capacité de la cartouche magenta

Niveau de la cartouche magenta

Capacité de la cartouche jaune

Niveau de la cartouche jaune

- 3** Exécutez la recherche enregistrée lors de l'utilisation de la vue.

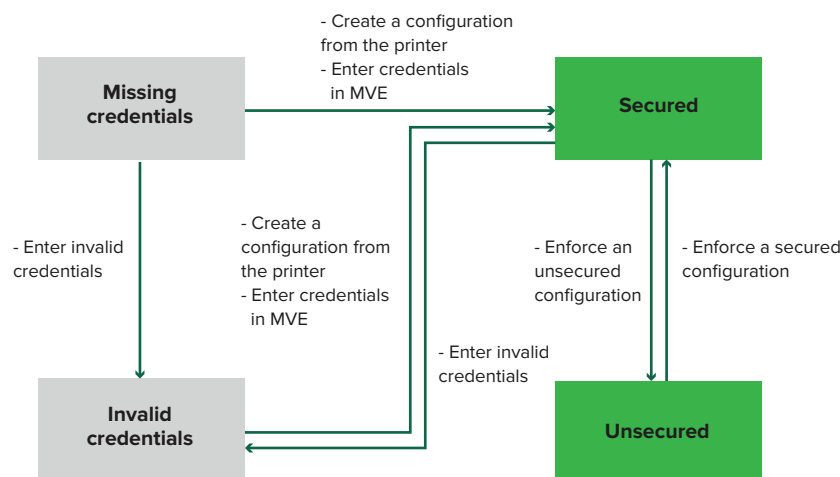
Remarque : Les informations affichées dans la vue Listes des imprimantes sont basées sur le dernier audit. Effectuez un audit et une mise à jour de l'état pour obtenir l'état actuel de l'imprimante.

Sécurisation des communications avec l'imprimante

Présentation des états de sécurité de l'imprimante

Pendant la détection, l'imprimante peut se trouver dans l'un des états de sécurité suivants :

- **Non sécurisé** : MVE ne nécessite pas d'informations d'identification pour communiquer avec le périphérique.
- **Sécurisé** : MVE a besoin d'informations d'identification sécurisées et celles-ci ont été fournies.
- **Informations d'authentification manquantes** : MVE nécessite des informations d'identification, mais elles n'ont pas été fournies.
- **Informations d'authentification non valides** : MVE nécessite des informations d'identification, mais celles fournies sont incorrectes.



Une imprimante est dans l'état Informations d'authentification non valides lorsque les informations d'identification ne sont pas valides pendant la détection, l'audit, la mise à jour de l'état, le contrôle de conformité ou l'application de la configuration.

L'imprimante se trouve dans un état Non sécurisé uniquement lorsqu'elle ne nécessite pas d'informations d'identification durant la détection.

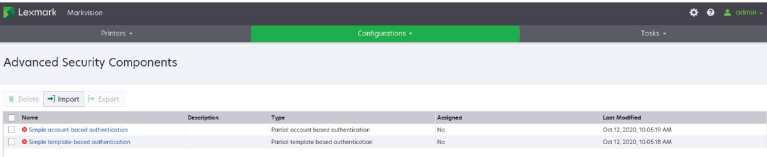
Pour modifier l'état de Non sécurisé à Sécurisé, appliquez une configuration sécurisée.

Pour modifier l'état d'une imprimante Informations d'authentification manquantes ou Informations d'authentification non valides, saisissez les informations d'identification dans MVE manuellement ou créez un fichier de configuration à partir de l'imprimante.

Sécurisation des imprimantes à l'aide des configurations par défaut

Certains modèles d'imprimante ne nécessitent pas d'utilisateur administrateur par défaut. L'utilisateur invité dispose d'un accès ouvert et n'est pas connecté. Cette configuration permet à l'utilisateur d'accéder à toutes les autorisations et à tous les contrôles d'accès de l'imprimante. MVE gère ce risque par le biais de configurations par défaut. Après une nouvelle installation, deux composants de sécurité avancée sont automatiquement créés. Chaque composant contient les paramètres de sécurité par défaut et un compte d'administrateur local préconfiguré. Vous pouvez utiliser ces composants de sécurité lorsque vous créez une configuration, puis déployer et appliquer la configuration aux nouvelles imprimantes.

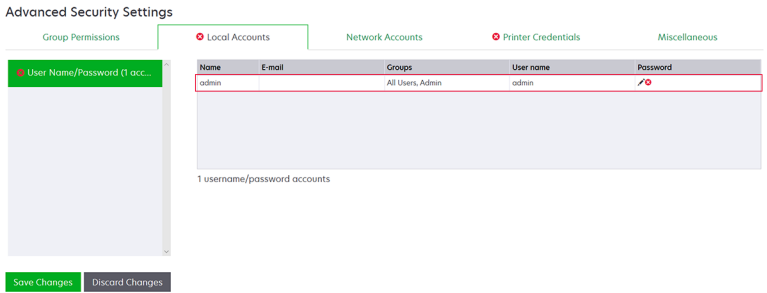
Dans le menu Configurations, cliquez sur **Tous les composants de sécurité avancée**.



Name	Description	Type	Assigned	Last Modified
Simple account based authentication	Simple account based authentication	Simple account based authentication	No	Oct 12, 2020, 10:05:19 AM
Simple template based authentication	Simple template based authentication	Simple template based authentication	No	Oct 12, 2020, 10:05:19 AM

Authentification simple basée sur un compte

Ce composant de sécurité contient un Compte local Nom d'utilisateur/Mot de passe appelé **admin**.



Advanced Security Settings

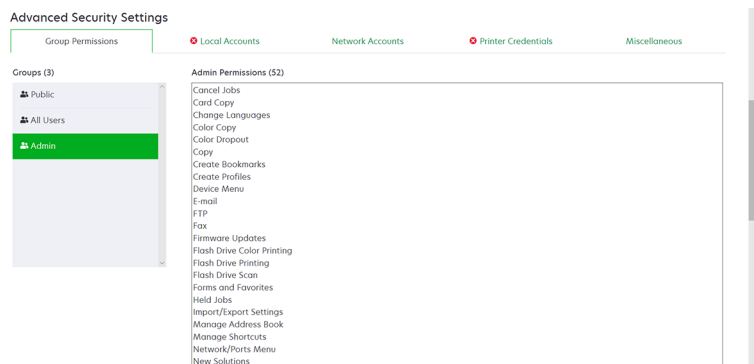
Group Permissions Local Accounts Network Accounts Printer Credentials Miscellaneous

Name	E-mail	Groups	User name	Password
admin		All Users, Admin	admin	admin

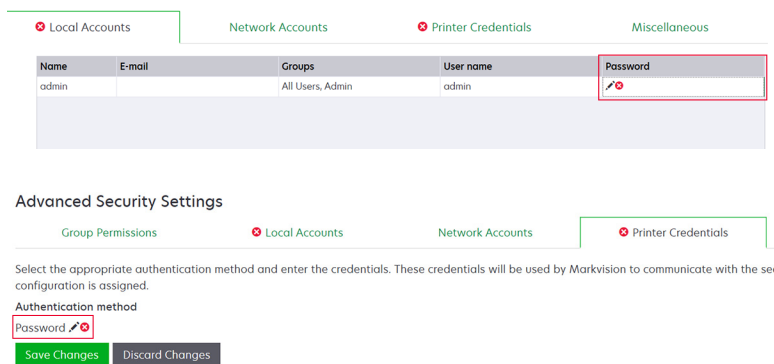
1 username/password accounts

Save Changes Discard Changes

Le compte **admin** est membre du groupe Admin, dont les autorisations incluent des contrôles d'accès aux fonctions et des autorisations de sécurisation de l'imprimante et de restriction de l'accès public. Pour plus d'informations, reportez-vous à la section « [Présentation des autorisations et des contrôles d'accès aux fonctions](#) » à la page 55.

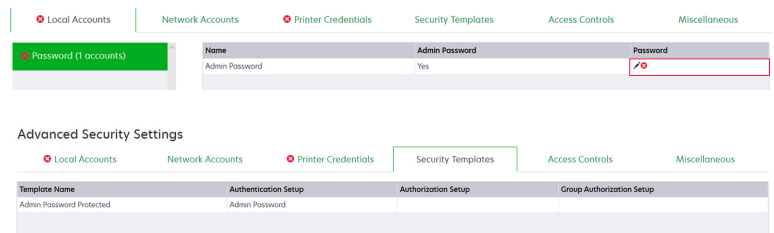


Avant d'ajouter ce composant à une configuration, assurez-vous de définir le mot de passe **admin** et les informations d'identification de l'imprimante.



Authentification simple basée sur un modèle

Ce composant de sécurité contient un modèle de sécurité appelé Protégé par mot de passe Admin qui est configuré avec un Mot de passe compte local.



Ce modèle de sécurité est appliqué aux contrôles d'accès suivants :

- Mises à jour du microcode
- Gestion à distance
- Menu Sécurité à distance

Les contrôles d'accès restants sont définis sur **Pas de sécurité**. Cependant, vous pouvez toujours configurer les autres menus d'administration de l'imprimante de sorte qu'ils utilisent le modèle de sécurité, pour une protection accrue. Pour plus d'informations sur les contrôles d'accès, reportez-vous à la section « [Présentation des autorisations et des contrôles d'accès aux fonctions](#) » à la page 55.

Avant d'ajouter ce composant à une configuration, assurez-vous de définir le mot de passe et les informations d'identification de l'imprimante.

The top screenshot shows the 'Advanced Security Settings' window with the 'Local Accounts' tab selected. It displays a table with one account named 'Admin Password' and a password field. The bottom screenshot shows the 'Advanced Security Settings' window with the 'Printer Credentials' tab selected. It prompts the user to select an authentication method and enter credentials, with 'Password' selected.

Présentation des autorisations et des contrôles d'accès aux fonctions

Les imprimantes peuvent être configurées pour restreindre l'accès public à des menus administrateur et à des fonctionnalités de gestion des périphériques. Dans les modèles d'imprimante plus récents, les autorisations nécessaires pour accéder aux fonctions de l'imprimante peuvent être sécurisées grâce à différents types de méthodes d'authentification. Dans les anciens modèles d'imprimante, un modèle de sécurité peut être appliqué à un contrôle d'accès aux fonctions (FAC).

Pour communiquer avec ces imprimantes sécurisées et les gérer, MVE nécessite certaines autorisations ou FAC, selon le modèle d'imprimante.

Le tableau suivant présente les fonctions de gestion de l'imprimante pouvant être gérées dans MVE et les autorisations ou FAC nécessaires.

Notez que MVE nécessite l'authentification lorsque la gestion à distance est sécurisée. Si d'autres menus administrateur et des autorisations de gestion des périphériques ou FAC sont sécurisés, la gestion à distance doit également être sécurisée. Dans le cas contraire, MVE ne peut pas exécuter les fonctions.

Ces autorisations et contrôles d'accès aux fonctions sont prédéfinis dans MVE en tant que composants de sécurité avancée par défaut et peuvent facilement être utilisés dans une configuration. Pour plus d'informations, reportez-vous à la section « [Sécurisation des imprimantes à l'aide des configurations par défaut](#) » à la page 53.

Si vous n'utilisez pas les composants de sécurité avancée par défaut, assurez-vous que ces autorisations et contrôles d'accès aux fonctions sont configurés manuellement dans l'imprimante. Pour plus d'informations, reportez-vous à la section « [Configuration de la sécurité d'une imprimante](#) » à la page 56.

Autorisations ou FAC	Description
Gestion à distance	Possibilité de lire et d'écrire les paramètres à distance. Si aucune autre autorisation ou FAC répertorié dans ce tableau n'est sécurisé, la gestion à distance doit également être sécurisée.
Mises à jour du microcode	Possibilité de mettre à jour le microcode avec n'importe quelle méthode.

Autorisations ou FAC	Description
Configuration des applications	Possibilité d'installer ou de supprimer des applications de l'imprimante et d'envoyer des fichiers de paramètres d'application vers l'imprimante.
Importer / Exporter tous les paramètres ou sur Importation/exportation du fichier de configuration	Possibilité d'envoyer des fichiers de configuration vers l'imprimante.
Menu Sécurité ou sur Menu Sécurité à distance	Possibilité de gérer des méthodes de connexion et de configurer les options de sécurité de l'imprimante.

Pour sécuriser les modèles d'imprimante plus récents dans MVE, désactivez l'accès public pour la gestion à distance et les autorisations du menu Sécurité. Pour les anciens modèles d'imprimante, appliquez un modèle de sécurité au FAC de la gestion à distance.

Configuration de la sécurité d'une imprimante

- 1 Dans le menu Imprimantes, cliquez sur **Listes des imprimantes**.
- 2 Cliquez sur l'adresse IP de l'imprimante, puis sur **Ouvrir Embedded Web Server**.
- 3 Cliquez sur **Paramètres** ou sur **Configuration**.
- 4 Selon votre modèle d'imprimante, effectuez l'une des opérations suivantes :
 - Cliquez sur **Sécurité > Méthodes de connexion**, puis procédez comme suit :

Pour les modèles d'imprimante plus récents

- a Dans la section Sécurité, créez une méthode de connexion.
 - b Cliquez sur **Gérer les groupes/les autorisations** ou **Gestion des autorisations** en regard de la méthode de connexion.
 - c Développez **Menus administrateur**, puis sélectionnez **Menu Sécurité**.
 - d Développez **Gestion des périphériques**, puis sélectionnez les autorisations suivantes :
 - **Gestion à distance**
 - **Mises à jour du microcode**
 - **Configuration des applications**
 - **Importer / Exporter tous les paramètres**
 - e Cliquez sur **Enregistrer**.
 - f Dans la section Public, cliquez sur **Gestion des autorisations**.
 - g Développez **Menus administrateur**, puis décochez **Menu Sécurité**.
 - h Développez **Gestion des périphériques**, puis décochez **Gestion à distance**.
 - i Cliquez sur **Enregistrer**.
- Cliquez sur **Sécurité > Configuration de la sécurité** ou **Modifier la configuration de sécurité**, puis effectuez les opérations suivantes :

Pour les anciens modèles d'imprimante

- a Dans la section Configuration de sécurité avancée, créez un bloc fonctionnel et un modèle de sécurité.
- b Cliquez sur **Contrôles d'accès**, puis développez **Menus administrateur**.
- c Dans le menu Menu Sécurité à distance, sélectionnez le modèle de sécurité.
- d Développez **Gestion**, puis sélectionnez le modèle de sécurité pour les contrôles d'accès aux fonctions suivants :
 - Configuration des applications
 - Gestion à distance
 - Mises à jour du microcode
 - Importation/exportation du fichier de configuration
- e Cliquez sur **Envoyer**.

Sécurisation des communications avec les imprimantes de votre parc

- 1 Détectez une imprimante sécurisée. Pour plus d'informations, reportez-vous à la section [« Détection des imprimantes » à la page 33](#).

Remarques :

- Une imprimante est sécurisée lorsque l'icône  apparaît en regard de celle-ci. Pour plus d'informations sur la sécurisation d'une imprimante, reportez-vous [au document d'aide](#).
- Pour plus d'informations sur les états de sécurité de l'imprimante, reportez-vous à la section [« Présentation des états de sécurité de l'imprimante » à la page 52](#).

- 2 Créez une configuration à partir d'une imprimante. Pour plus d'informations, reportez-vous à la section [« Création d'une configuration à partir d'une imprimante » à la page 69](#).
- 3 Attribuez la configuration à votre parc. Pour plus d'informations, reportez-vous à la section [« Attribution de configurations à des imprimantes » à la page 60](#).
- 4 Mettez en œuvre la configuration. Pour plus d'informations, reportez-vous à la section [« Mise en œuvre de configurations » à la page 60](#). Un symbole représentant un cadenas s'affiche en regard de l'imprimante sécurisée.

Autres méthodes de sécurisation de vos imprimantes

Pour plus d'informations sur la configuration des paramètres de sécurité de l'imprimante, reportez-vous au *Guide de l'administrateur d'Embedded Web Server* pour votre imprimante.

Vérifiez les paramètres suivants sur vos imprimantes :

- Le chiffrement du disque est activé.
- Les ports suivants sont restreints :
 - TCP 79 (Finger)
 - TCP 21 (FTP)
 - UDP 69 (TFTP)
 - TCP 5001 (IPDS)

- TCP 9600 (IPDS)
- TCP 10000 (Telnet)
- La liste de chiffrement par défaut est la chaîne de chiffrement OWASP 'B'.

Gestion des imprimantes

Redémarrage de l'imprimante

- 1 Sur le menu Imprimantes, cliquez sur **Liste des imprimantes**.
- 2 Cliquez sur l'adresse IP de l'imprimante.
- 3 Cliquez sur **Redémarrer l'imprimante**.

Affichage de l'Embedded Web Server de l'imprimante

L'Embedded Web Server est un logiciel intégré à l'imprimante comprenant un panneau de commandes utilisé pour configurer l'appareil à partir de n'importe quel navigateur Web.

- 1 Dans le menu Imprimantes, cliquez sur **Liste des imprimantes**.
- 2 Cliquez sur l'adresse IP de l'imprimante.
- 3 Cliquez sur **Ouvrir l'Embedded Web Server**.

Audit d'imprimantes

La fonction d'audit permet de recueillir les informations de n'importe quelle imprimante du réseau dont l'état est Géré, puis de stocker ces informations dans le système. Un audit régulier permet d'assurer que les informations du système sont à jour.

- 1 Dans le menu Imprimantes, cliquez sur **Liste des imprimantes**.
- 2 Sélectionnez une ou plusieurs imprimantes.
- 3 Cliquez sur **Imprimante > Audit**.

Remarque : Il est possible de programmer un audit pour qu'il s'exécute à intervalle régulier. Pour plus d'informations, reportez-vous à la section [« Création d'une programmation » à la page 112](#).

Mise à jour de l'état de l'imprimante

La fonction Mettre à jour l'état permet de mettre à jour l'état de l'imprimante et les informations sur les fournitures. Pour vous assurer que l'état de l'imprimante et les informations sur les fournitures sont à jour, actualisez régulièrement l'état.

- 1 Dans le menu Imprimantes, cliquez sur **Listes des imprimantes**.
- 2 Sélectionnez une ou plusieurs imprimantes.
- 3 Cliquez sur **Imprimante > Mettre à jour l'état**.

Remarque : Il est possible de programmer une mise à jour d'état pour qu'elle s'exécute à intervalle régulier. Pour plus d'informations, reportez-vous à la section [« Création d'une programmation » à la page 112](#).

Réglage de l'état de l'imprimante

Pour plus d'informations sur les états d'imprimante, reportez-vous à la section « [Présentation des états du cycle de vie de l'imprimante](#) » à la page 44.

- 1 Dans le menu Imprimantes, cliquez sur **Liste des imprimantes**.
- 2 Sélectionnez une ou plusieurs imprimantes.
- 3 Cliquez sur **Imprimante**, puis sélectionnez l'une des options suivantes :
 - **Définir l'état sur géré** : l'imprimante est incluse dans toutes les activités effectuées au sein du système.
 - **Définir l'état sur non géré** : l'imprimante est exclue de toutes les activités effectuées au sein du système.
 - **Définir l'état sur retiré** : l'imprimante est supprimée du réseau. Le système conserve les informations de l'imprimante mais ne s'attend pas à la détecter de nouveau sur le réseau.

Attribution de configurations à des imprimantes

Avant de commencer, assurez-vous que la configuration de l'imprimante a été créée. L'attribution d'une configuration à une imprimante permet au système d'exécuter des contrôles de conformité et des mises en œuvre. Pour plus d'informations, reportez-vous à la section « [Création d'une configuration](#) » à la page 67.

- 1 Dans le menu Imprimantes, cliquez sur **Listes des imprimantes**.
- 2 Sélectionnez une ou plusieurs imprimantes.
- 3 Cliquez sur **Configurer > Attribuer les configurations**.
- 4 Dans la section Configuration, sélectionnez une configuration.

Remarque : Si le système est défini sur **Utiliser Markvision pour gérer les certificats de périphérique**, sélectionnez **Approuver les périphériques sélectionnés**. Cette confirmation permet à l'utilisateur de vérifier que les imprimantes sont des périphériques réels et non falsifiés.
- 5 Cliquez sur **Attribuer les configurations**.

Annulation de l'attribution de configurations

- 1 Dans le menu Imprimantes, cliquez sur **Liste des imprimantes**.
- 2 Sélectionnez une ou plusieurs imprimantes.
- 3 Cliquez sur **Configurer > Annuler l'attribution des configurations**.
- 4 Cliquez sur **Annuler l'attribution des configurations**.

Mise en œuvre de configurations

MVE exécute un contrôle de conformité pour l'imprimante. Si certains paramètres ne sont pas conformes, MVE les modifie sur l'imprimante. MVE effectue ensuite un contrôle de conformité final. Il est possible que les mises à jour nécessitant le redémarrage de l'imprimante, comme les mises à jour du micrologiciel, requièrent l'exécution d'une seconde mise en œuvre.

Avant de commencer, assurez-vous qu'une configuration est attribuée à l'imprimante. Pour plus d'informations, reportez-vous à la section [« Attribution de configurations à des imprimantes » à la page 60](#).

- 1 Dans le menu Imprimantes, cliquez sur **Liste des imprimantes**.
- 2 Sélectionnez une ou plusieurs imprimantes.
- 3 Cliquez sur **Configurer > Mettre en œuvre des configurations**.

Remarques :

- Si l'imprimante indique une erreur, certains paramètres peuvent ne pas être mis à jour.
- Pour que MVE puisse déployer le micrologiciel et les fichiers de solution sur une imprimante, le contrôle d'accès de la fonction Mises à jour du micrologiciel doit être défini sur **Pas de sécurité**. Si une option de sécurité a été appliquée, le contrôle d'accès de la fonction Mises à jour du micrologiciel doit utiliser le même modèle de sécurité que le contrôle d'accès de la fonction Gestion à distance. Pour plus d'informations, reportez-vous à la section [« Déploiement de fichiers sur des imprimantes » à la page 61](#).
- Il est possible de programmer une mise en œuvre pour qu'elle s'exécute à intervalle régulier. Pour plus d'informations, reportez-vous à la section [« Création d'une programmation » à la page 112](#).

Vérification de la conformité d'une imprimante avec une configuration

Lors d'un contrôle de conformité, MVE vérifie les paramètres d'imprimante et s'ils correspondent à la configuration attribuée. MVE n'apporte aucune modification à l'imprimante pendant cette opération.

Avant de commencer, assurez-vous qu'une configuration est attribuée à l'imprimante. Pour plus d'informations, reportez-vous à la section [« Attribution de configurations à des imprimantes » à la page 60](#).

- 1 Dans le menu Imprimantes, cliquez sur **Liste des imprimantes**.
- 2 Sélectionnez une ou plusieurs imprimantes.
- 3 Cliquez sur **Configurer > Vérifier la conformité**.

Remarques :

- vous pouvez consulter les résultats dans la page d'état de la tâche.
- Il est possible de programmer une vérification de la conformité pour qu'elle s'exécute à intervalle régulier. Pour plus d'informations, reportez-vous à la section [« Création d'une programmation » à la page 112](#).

Déploiement de fichiers sur des imprimantes

Vous pouvez déployer les fichiers suivants sur l'imprimante :

- **Certificats CA** : fichiers **.cer** ou **.pem** qui sont ajoutés au magasin de certificats de l'imprimante.
- **Bundle de configuration** : fichiers **.zip** exportés à partir d'une imprimante prise en charge ou obtenus directement auprès de Lexmark.
- **Mise à jour du micrologiciel** : fichier **.fls** flashé sur l'imprimante.

- **Fichier générique** : n'importe quel fichier que vous souhaitez envoyer à l'imprimante.
 - **Socket brut** : envoyé sur le port 9100. L'imprimante le traite comme les autres données d'impression.
 - **FTP** : fichier envoyé par FTP. Cette méthode de déploiement n'est pas prise en charge sur les imprimantes sécurisées.
- **Certificat de l'imprimante** : certificat signé installé sur l'imprimante en tant que certificat par défaut.
- **Fichier de configuration Universel (UCF)** : fichier de configuration exporté à partir d'une imprimante.
 - **Service Web** : le service Web HTTPS est utilisé lorsque le modèle d'imprimante le prend en charge. Dans le cas contraire, l'imprimante utilise le service Web HTTP.
 - **FTP** : fichier envoyé par FTP. Cette méthode de déploiement n'est pas prise en charge sur les imprimantes sécurisées.

- 1 Dans le menu Imprimantes, cliquez sur **Liste des imprimantes**.
- 2 Sélectionnez une ou plusieurs imprimantes.
- 3 Cliquez sur **Configurer > Déployer un fichier sur des imprimantes**.
- 4 Cliquez sur **Sélectionner un fichier**, puis localisez le fichier.
- 5 Sélectionnez un type de fichier, puis une méthode de déploiement.
- 6 Cliquez sur **Déployer le fichier**.

Remarques :

- Pour que MVE puisse déployer le micrologiciel et les fichiers de solution sur une imprimante, le contrôle d'accès de la fonction Mises à jour du micrologiciel doit être défini sur **Pas de sécurité**. Si une option de sécurité a été appliquée, le contrôle d'accès de la fonction Mises à jour du micrologiciel doit utiliser le même modèle de sécurité que le contrôle d'accès de la fonction Gestion à distance.
- Il est possible de programmer un déploiement de fichier pour qu'il s'exécute à intervalle régulier. Pour plus d'informations, reportez-vous à la section [« Création d'une programmation » à la page 112](#).

Mise à jour du microcode de l'imprimante

- 1 Dans le menu Imprimantes, cliquez sur **Listes des imprimantes**.
- 2 Sélectionnez une ou plusieurs imprimantes.
- 3 Cliquez sur **Configurer > Mettre à jour le microcode sur les imprimantes**.
- 4 Sélectionnez un fichier de microcode dans la bibliothèque de ressources, ou cliquez sur **Choisir un fichier**, puis accédez au fichier de microcode.

Remarque : Pour plus d'informations sur l'ajout de fichiers de microcode à la bibliothèque, reportez-vous à la section [« Importation de fichiers vers la bibliothèque de ressources » à la page 73](#).

- 5 Le cas échéant, pour planifier la mise à jour, sélectionnez **Définir la fenêtre de mise à jour**, puis sélectionnez l'heure de début, l'heure de pause et les jours de la semaine.

Remarque : Le microcode est envoyé aux imprimantes entre l'heure de début et l'heure de pause. La tâche est suspendue à l'heure de pause, puis reprend à l'heure de début suivante jusqu'à ce qu'elle se termine.

- 6 Cliquez sur **Mettre à jour le microcode**.

Remarque : Pour que MVE puisse mettre à jour le microcode de l'imprimante, le contrôle d'accès à la fonction Mises à jour du microcode doit être défini sur **Pas de sécurité**. Si une option de sécurité a été appliquée, le contrôle d'accès à la fonction Mises à jour du microcode doit utiliser le même modèle de sécurité que le contrôle d'accès à la fonction Gestion à distance. Dans ce cas, MVE doit gérer l'imprimante en toute sécurité. Pour plus d'informations, reportez-vous à la section [« Sécurisation des communications avec l'imprimante » à la page 52](#).

Désinstallation d'applications présentes sur les imprimantes

MVE peut uniquement désinstaller les applications qui ont été ajoutées au système. Pour plus d'informations sur le téléchargement d'applications sur le système, voir [« Importation de fichiers vers la bibliothèque de ressources » à la page 73](#).

- 1 Dans le menu Imprimantes, cliquez sur **Liste des imprimantes**.
- 2 Sélectionnez une ou plusieurs imprimantes.
- 3 Cliquez sur **Configurer > Désinstaller des applications des imprimantes**.
- 4 Sélectionnez les applications.
- 5 Cliquez sur **Désinstaller les applications**.

Attribution d'événements à des imprimantes

L'attribution d'événements à des imprimantes permet à MVE d'effectuer l'action associée dès que l'une des alertes associées est déclenchée sur l'imprimante attribuée. Pour plus d'informations sur la création d'événements, reportez-vous à [« Gestion des alertes d'imprimante » à la page 102](#).

Remarque : Les événements peuvent être uniquement attribués aux imprimantes non sécurisées.

- 1 Dans le menu Imprimantes, cliquez sur **Liste des imprimantes**.
- 2 Sélectionnez une ou plusieurs imprimantes.
- 3 Cliquez sur **Attribuer > Événements**.
- 4 Sélectionnez un ou plusieurs événements.

Remarque : Si l'événement a déjà été attribué à certaines des imprimantes sélectionnées, un tiret s'affiche dans la case à cocher. Si vous conservez le tiret, l'événement n'est pas modifié. Si vous cochez la case, l'événement sera attribué à toutes les imprimantes sélectionnées. Si vous décochez la case, l'événement sera désattribué des imprimantes auxquelles il était attribué.

- 5 Cliquez sur **Attribuer les événements**.

Attribution de mots-clés aux imprimantes

L'attribution de mots-clés aux imprimantes vous permet d'organiser les imprimantes. Pour plus d'informations sur la création de mots-clés, reportez-vous à [« Gestion des mots clés » à la page 44](#).

- 1 Dans le menu Imprimantes, cliquez sur **Liste des imprimantes**.
- 2 Sélectionnez une ou plusieurs imprimantes.
- 3 Cliquez sur **Attribuer > Mots clés**.
- 4 Si nécessaire, dans le menu Affichage, sélectionnez une catégorie.
- 5 Sélectionnez un ou plusieurs mots-clés.

Remarque : Les mots-clés sont répertoriés en fonction d'une catégorie. Si un mot-clé a déjà été attribué à certaines des imprimantes sélectionnées, un tiret s'affiche dans la case à cocher. Si vous laissez le tiret, le mot-clé ne sera ni attribué, ni désattribué aux imprimantes sélectionnées. Si vous cochez la case, le mot-clé sera attribué à toutes les imprimantes sélectionnées. Si vous décochez la case, le mot-clé sera désattribué des imprimantes auxquelles il était attribué.

- 6 Cliquez sur **Attribuer les mots clés**.

Saisie des informations d'identification pour les imprimantes sécurisées

Les imprimantes sécurisées peuvent être détectées et enregistrées. Pour communiquer avec ces imprimantes, vous pouvez soit appliquer une configuration, soit saisir les informations d'identification directement dans MVE.

Remarque : Une imprimante est sécurisée lorsque l'icône  apparaît en regard de celle-ci.

Pour saisir les informations d'identification, procédez comme suit :

- 1 Dans le menu Imprimantes, cliquez sur **Listes des imprimantes**.
- 2 Sélectionnez une ou plusieurs imprimantes sécurisées.
- 3 Cliquez sur **Sécurité > Saisir les informations d'identification**.
- 4 Sélectionnez la méthode d'authentification, puis saisissez les informations d'identification.
- 5 Cliquez sur **Saisir les informations d'identification**.

Remarque : Les imprimantes enregistrées qui sont sécurisées, mais qui ne disposent pas d'informations d'identification appropriées dans MVE, sont marquées comme Informations d'authentification manquantes sous le filtre Communications. Une fois les informations d'identification correctes saisies, les imprimantes sont marquées comme Sécurisées.

Configuration manuelle des certificats d'imprimante

Lorsqu'il n'utilise pas la fonction de gestion automatisée des certificats, MVE peut simplifier le processus de signature du certificat d'imprimante par défaut dans un parc d'imprimantes. MVE rassemble les demandes de signature de certificat depuis le parc, puis déploie les certificats signés sur les imprimantes adéquates.

En tant qu'administrateur système, effectuez les opérations suivantes :

- 1 Générez les demandes de signature de certificat d'imprimante.
 - a Dans le menu Imprimantes, cliquez sur **Listes des imprimantes**.
 - b Sélectionnez une ou plusieurs imprimantes.
 - c Cliquez sur **Sécurité > Générer les demandes de signature de certificat d'imprimante**.

Remarque : Ce processus autorise la présence d'une seule demande de signature de certificat d'imprimante sur le serveur à la fois. Si une autre demande est générée, la demande précédente est remplacée. Veillez à bien télécharger la demande existante avant d'en générer une nouvelle.
- 2 Attendez la fin de la tâche, puis téléchargez les demandes de signature de certificat d'imprimante.
 - a Dans le menu Imprimantes, cliquez sur **Listes des imprimantes**.
 - b Cliquez sur **Sécurité > Télécharger les demandes de signature de certificat d'imprimante**.
- 3 Utilisez une autorité de certification approuvée pour signer les demandes de signature de certificat.
- 4 Enregistrez les certificats signés dans un fichier ZIP.

Remarque : Tous les certificats signés doivent être enregistrés dans l'emplacement racine du fichier ZIP. Dans le cas contraire, MVE ne peut pas analyser le fichier.
- 5 Dans le menu Imprimantes, cliquez sur **Listes des imprimantes**.
- 6 Sélectionnez une ou plusieurs imprimantes.
- 7 Cliquez sur **Configurer > Déployer un fichier sur des imprimantes**.
- 8 Cliquez sur **Sélectionner un fichier**, puis localisez le fichier ZIP.
- 9 Dans le menu Type de fichier, sélectionnez **Certificats d'imprimante**.
- 10 Cliquez sur **Déployer le fichier**.

Suppression d'imprimantes

- 1 Dans le menu Imprimantes, cliquez sur **Listes des imprimantes**.
- 2 Sélectionnez une ou plusieurs imprimantes.
- 3 Cliquez sur **Imprimante**.
- 4 Si nécessaire, pour supprimer le certificat d'imprimante, sélectionnez **Supprimer le(s) certificat(s) par défaut du périphérique**.

Remarque : La suppression d'une imprimante de MVE supprime uniquement le certificat de MVE et n'affecte pas le serveur CA.

5 Effectuez l'une des opérations suivantes :

- Pour conserver les informations de l'imprimante, cliquez sur **Retirer l'imprimante**.
- Pour supprimer l'imprimante du système, cliquez sur **Supprimer l'imprimante**.

Gestion des configurations

Aperçu

MVE utilise des configurations pour gérer les imprimantes de votre parc.

Une configuration est un ensemble de paramètres pouvant être attribués et appliqués à une imprimante ou à un groupe de modèles d'imprimante. Dans une configuration, vous pouvez modifier les paramètres d'imprimante et déployer des applications, des licences, des microcodes et des certificats d'imprimante.

Vous pouvez créer une configuration composée des éléments suivants :

- Paramètres de base de l'imprimante
- Paramètres de sécurité avancés
- Autorisations d'impression couleur

Remarque : Ce paramètre est uniquement disponible dans les configurations des imprimantes couleur prises en charge.

- Microcode de l'imprimante
- Applications
- Certificats d'autorité de certification

A l'aide des configurations, vous pouvez effectuer les opérations suivantes pour gérer les imprimantes :

- Attribuez une configuration aux imprimantes.
- Appliquez la configuration aux imprimantes. Les paramètres spécifiés dans la configuration sont appliqués aux imprimantes ; le microcode, les applications et les certificats d'autorité de certification sont installés.
- Vérifiez si les imprimantes sont conformes à une configuration. Si une imprimante n'est pas conforme, la configuration peut être appliquée à l'imprimante.

Remarque : L'application de la configuration et la vérification de la conformité peuvent être programmées pour s'exécuter à intervalle régulier.

- Si l'imprimante prend en charge les paramètres de configuration, mais que les valeurs ne sont pas prises en charge, l'imprimante s'affiche alors comme non conforme.

Création d'une configuration

Une configuration est un ensemble de paramètres pouvant être attribués et appliqués à une imprimante ou à un groupe de modèles d'imprimante. Dans une configuration, vous pouvez modifier les paramètres d'imprimante et déployer des applications, des licences, des microcodes et des certificats CA vers les imprimantes.

- 1 Dans le menu Configurations, cliquez sur **Toutes les configurations > Créer**.
- 2 Saisissez un nom unique pour la configuration, ainsi que sa description.

3 Essayez une ou plusieurs des solutions suivantes :

- Dans l'onglet Base, dans la liste Paramètre, sélectionnez un ou plusieurs paramètres, puis définissez-en les valeurs. Si la valeur est un paramètre de variable, entourez l'en-tête de `{ }`. Par exemple, `{Contact_Name}`. Pour utiliser un fichier de paramètres de variables, sélectionnez le fichier dans le menu Utiliser le fichier de données des paramètres de variables, ou importez le fichier. Pour plus d'informations, reportez-vous à la section [« Présentation des paramètres de variable » à la page 71](#).

Settings

Basic Advanced Security Color Print Permissions Firmware Apps Certificates

Use variable setting data file

None Import

☐ Show only included settings Show settings for All models

View All settings Filter by setting name

Setting	Category	Value
☐ E-mail: Blank Page Removal	E-mail/FTP	Do not remove
☐ "Copy from" Size	Copy	Letter
☐ (Assign Type/Bin) Bond Bin	Paper	Disabled

- Sous l'onglet Sécurité avancée, sélectionnez un composant de sécurité avancée.

Remarques :

- Pour créer un composant de sécurité avancée, reportez-vous à la section [« Création d'un composant de sécurité avancée à partir d'une imprimante » à la page 70](#).
- Vous pouvez gérer les paramètres de sécurité avancée uniquement lors de la création d'une configuration à partir d'une imprimante sélectionnée. Pour plus d'informations, reportez-vous à la section [« Création d'une configuration à partir d'une imprimante » à la page 69](#).
- Dans l'onglet Autorisations d'impression couleur, configurez les paramètres. Pour plus d'informations, reportez-vous à la section [« Configuration des autorisations d'impression couleur » à la page 71](#).

Remarque : Ce paramètre est uniquement disponible dans les configurations des imprimantes couleur prises en charge.

- Sélectionnez un fichier de microcode dans l'onglet Microcode. Pour importer un fichier de microcode, reportez-vous à la section [« Importation de fichiers vers la bibliothèque de ressources » à la page 73](#).

- Sélectionnez une ou plusieurs applications à déployer dans l'onglet Applications. Pour plus d'informations, reportez-vous à la section [« Création d'un package d'applications » à la page 72](#).

Remarque : MVE ne prend pas en charge le déploiement d'applications dotées de licences d'essai. Vous pouvez déployer uniquement les applications gratuites ou celles dotées de licences de production.

- Dans l'onglet Certificats, sélectionnez un ou plusieurs certificats à déployer. Pour importer un fichier de certificat, reportez-vous à la section [« Importation de fichiers vers la bibliothèque de ressources » à la page 73](#).

Remarque : Sélectionnez **Utiliser Markvision pour gérer les certificats de périphérique** afin que MVE puisse évaluer les certificats manquants, non valides, révoqués et expirés, puis remplacez-les automatiquement. Pour plus d'informations, reportez-vous à la section [« Configuration de MVE pour la gestion automatisée des certificats » à la page 75](#).

4 Cliquez sur **Créer une configuration**.

Exemple de scénario : Déploiement d'une configuration sur des imprimantes

La société ABC possède plus de 50 imprimantes Lexmark MX710. En tant que membre du personnel informatique, vous devez définir le format de papier du tiroir sur **Lettre**.

Remarque : Vous pouvez également déployer une configuration sur un groupe de modèles d'imprimante.

Exemple de mise en œuvre

- 1 Créez une configuration pour l'imprimante Lexmark MX710.
- 2 Dans l'onglet Base, définissez Format de papier du tiroir sur **Lettre**.
- 3 Filtrez la vue Listes des imprimantes ou utilisez une recherche enregistrée affichant les imprimantes Lexmark MX710.
- 4 Attribuez, puis appliquez la configuration aux imprimantes.

Création d'une configuration à partir d'une imprimante

Les composants suivants ne sont pas inclus :

- Microcode de l'imprimante
- Applications
- Certificats

Pour ajouter le microcode, des applications et des certificats, modifiez la configuration dans MVE.

- 1 Dans le menu Imprimantes, cliquez sur **Listes des imprimantes**.
- 2 Sélectionnez l'imprimante, puis cliquez sur **Configurer > Créer une configuration à partir de l'imprimante**.
- 3 Si nécessaire, sélectionnez **Inclure les paramètres de sécurité avancée** pour créer un composant de sécurité avancée à partir de l'imprimante sélectionnée.
- 4 Si l'imprimante est sécurisée, sélectionnez la méthode d'authentification, puis saisissez les informations d'identification.

- 5 Saisissez un nom unique pour la configuration et sa description, puis cliquez sur **Créer la configuration**.
- 6 Dans le menu Configurations, cliquez sur **Toutes les configurations**.
- 7 Sélectionnez la configuration, puis cliquez sur **Modifier**.
- 8 Si nécessaire, modifiez les paramètres.
- 9 Cliquez sur **Enregistrer les modifications**.

Exemple de scénario : clonage d'une configuration

Quinze imprimantes Lexmark MX812 ont été ajoutées au système après la détection. En tant que membre du personnel informatique, vous devez appliquer les paramètres des imprimantes existantes aux nouvelles imprimantes détectées.

Remarque : Vous pouvez également cloner une configuration à partir d'une imprimante, puis appliquer la configuration à un groupe de modèles d'imprimante.

Exemple de mise en œuvre

- 1 Sélectionnez une imprimante Lexmark MX812 dans la liste des imprimantes existantes.
- 2 Créez une configuration à partir de l'imprimante.
Remarque : Pour sécuriser les imprimantes, incluez les paramètres de sécurité avancée.
- 3 Attribuez, puis appliquez la configuration aux nouvelles imprimantes détectées.

Création d'un composant de sécurité avancée à partir d'une imprimante

Créez un composant de sécurité avancée à partir d'une imprimante pour gérer les paramètres de sécurité avancée. MVE lit tous les paramètres de cette imprimante, puis crée un composant qui les inclut. Le composant peut être associé à plusieurs configurations pour les modèles d'imprimante présentant la même structure de sécurité.

- 1 Dans le menu Imprimantes, cliquez sur **Listes des imprimantes**.
- 2 Sélectionnez l'imprimante, puis cliquez sur **Configurer > Créer un composant de sécurité avancée à partir de l'imprimante**.
- 3 Saisissez un nom unique pour le composant, ainsi que sa description.
- 4 Si l'imprimante est sécurisée, sélectionnez la méthode d'authentification, puis saisissez les informations d'identification.
- 5 Cliquez sur **Créer un composant**.

Remarque : Lorsque vous créez et appliquez une configuration avec un composant de sécurité avancée contenant des comptes locaux, ces derniers sont ajoutés aux imprimantes. Tous les comptes locaux existants préconfigurés dans l'imprimante sont conservés.

Génération d'une version imprimable des paramètres de configuration

- 1 Modifiez une configuration ou un composant de sécurité avancée.
- 2 Cliquez sur **Version imprimable**.

Présentation des paramètres de variable

Les paramètres de variable vous permettent de gérer les paramètres qui sont uniques à chaque imprimante comme le nom d'hôte ou l'identification de propriété, sur l'ensemble de votre parc. Lorsque vous créez une configuration ou que vous la modifiez, vous pouvez l'associer à un fichier CSV de votre choix.

Exemple de format CSV :

```
IP_ADDRESS,Contact_Name,Address,Disp_Info
1.2.3.4,John Doe,1600 Penn. Ave., Blue
4.3.2.1,Jane Doe,1601 Penn. Ave., Red
2.3.6.5,"Joe, Jane and Douglas",1601 Penn. Ave.,Yellow
2.3.6.7,"Joe, Jane and Douglas",1600 Penn. Ave.,He is 6'7" tall
```

Sur la ligne d'en-tête du fichier de variables, la première colonne est un jeton unique d'identification de l'imprimante. Celui-ci doit correspondre à l'une des valeurs suivantes :

- **HOSTNAME**
- **IP_ADDRESS**
- **SYSTEM_NAME**
- **SERIAL_NUMBER**

Chacune des colonnes qui suivent dans la ligne d'en-tête du fichier de variables est un jeton de remplacement défini par l'utilisateur. Ce jeton doit être référencé dans la configuration au format \${HEADER}. Dans les lignes suivantes, il est remplacé par les valeurs lorsque la configuration est appliquée. Vérifiez que les jetons ne contiennent aucun espace.

Lorsque vous créez ou modifiez une configuration, vous pouvez importer le fichier CSV qui contient les paramètres de variable. Pour plus d'informations, reportez-vous à la section « [Création d'une configuration](#) » à la page 67.

Configuration des autorisations d'impression couleur

MVE vous permet de limiter les impressions couleur pour les ordinateurs hôtes et pour certains utilisateurs.

Remarque : Ce paramètre est uniquement disponible dans les configurations des imprimantes couleur prises en charge.

- 1 Dans le menu Configurations, cliquez sur **Toutes les configurations**.
- 2 Créez ou modifiez une configuration.
- 3 Dans l'onglet Autorisations d'impression couleur, effectuez l'une des opérations suivantes :

Configurer les autorisations d'impression couleur pour les ordinateurs hôtes

- a Dans le menu Affichage, sélectionnez **Ordinateurs hôtes**, puis **Inclure des autorisations d'impression couleur pour les ordinateurs hôtes**.
- b Cliquez sur **Ajouter**, puis saisissez le nom de l'ordinateur hôte.
- c Pour permettre à l'ordinateur hôte d'imprimer en couleur, sélectionnez **Autoriser l'impression couleur**.
- d Pour permettre aux utilisateurs qui se connectent à l'ordinateur hôte d'imprimer en couleur, sélectionnez **Remplacer l'autorisation de l'utilisateur**.
- e Cliquez sur **Enregistrer et ajouter** ou **Enregistrer**.

Configurer les autorisations d'impression couleur pour les utilisateurs

- a Dans le menu Affichage, sélectionnez **Utilisateurs**, puis **Inclure des autorisations d'impression couleur pour les utilisateurs**.
- b Cliquez sur **Ajouter**, puis saisissez le nom de l'utilisateur.
- c Sélectionnez **Autoriser l'impression couleur**.
- d Cliquez sur **Enregistrer et ajouter** ou **Enregistrer**.

Création d'un package d'applications

- 1 Exportez la vue Liste des imprimantes à partir de MVE à l'aide de la fonction Exporter les données.
 - a Dans le menu Imprimantes, cliquez sur **Vues**.
 - b Sélectionnez la **Liste des imprimantes**, puis cliquez sur **Exporter les données**.
 - c Sélectionnez une recherche enregistrée.
 - d Dans le menu «Sélectionnez le type de fichier pour l'exportation des données», sélectionnez **CSV**.
 - e Cliquez sur **Exporter les données**.

- 2 Accédez au Créateur de package.

Remarque : Si vous avez besoin d'accéder au Créateur de package, contactez votre représentant Lexmark.

- a Connectez-vous au Créateur de package à l'adresse cdp.lexmark.com/package-builder.
- b Importez la liste des imprimantes, puis cliquez sur **Suivant**.
- c Saisissez la description du package, puis indiquez votre adresse e-mail.
- d Dans le menu Produit, sélectionnez les applications dans le menu Produits, puis ajoutez des licences si nécessaire.
- e Cliquez sur **Suivant** > **Terminer**. Le lien de téléchargement du package vous est envoyé par e-mail.

- 3 Téléchargez le package.

Remarques :

- MVE ne prend pas en charge le déploiement d'applications dotées de licences d'essai. Vous pouvez déployer uniquement les applications gratuites ou celles dotées de licences de production. Pour obtenir les codes d'activation, contactez votre représentant Lexmark.

- Pour ajouter des applications à une configuration, importez le package d'applications dans la bibliothèque de ressources. Pour plus d'informations, reportez-vous à la section « [Importation de fichiers vers la bibliothèque de ressources](#) » à la page 73.

Importation ou exportation d'une configuration

Avant de commencer l'importation d'un fichier de configuration, vérifiez que la version du MVE à partir duquel il est exporté est la même.

- 1 Dans le menu Configurations, cliquez sur **Toutes les configurations**.
- 2 Effectuez l'une des opérations suivantes :
 - Pour importer un fichier de configuration, cliquez sur **Importer**, naviguez jusqu'au fichier de configuration, puis cliquez sur **Importer**.
 - Pour exporter un fichier de configuration, sélectionnez une configuration, puis cliquez sur **Exporter**.

Remarque : Lorsque vous exportez une configuration, les mots de passe sont exclus. Après l'importation, ajoutez-les manuellement.

Importation de fichiers vers la bibliothèque de ressources

La bibliothèque de ressources est un ensemble de fichiers de microcode, de certificats CA et de packages d'applications importés dans MVE. Ces fichiers peuvent être associés à une ou plusieurs configurations.

- 1 Dans le menu Configurations, cliquez sur **Bibliothèque de ressources**.
- 2 Cliquez sur **Importer > Sélectionner un fichier**, puis localisez le fichier.

Remarque : Seuls des fichiers de microcode (.fls), des packs d'application ou de configuration (.zip), des certificats CA (.pem) et des fichiers de configuration universelle peuvent être importés.

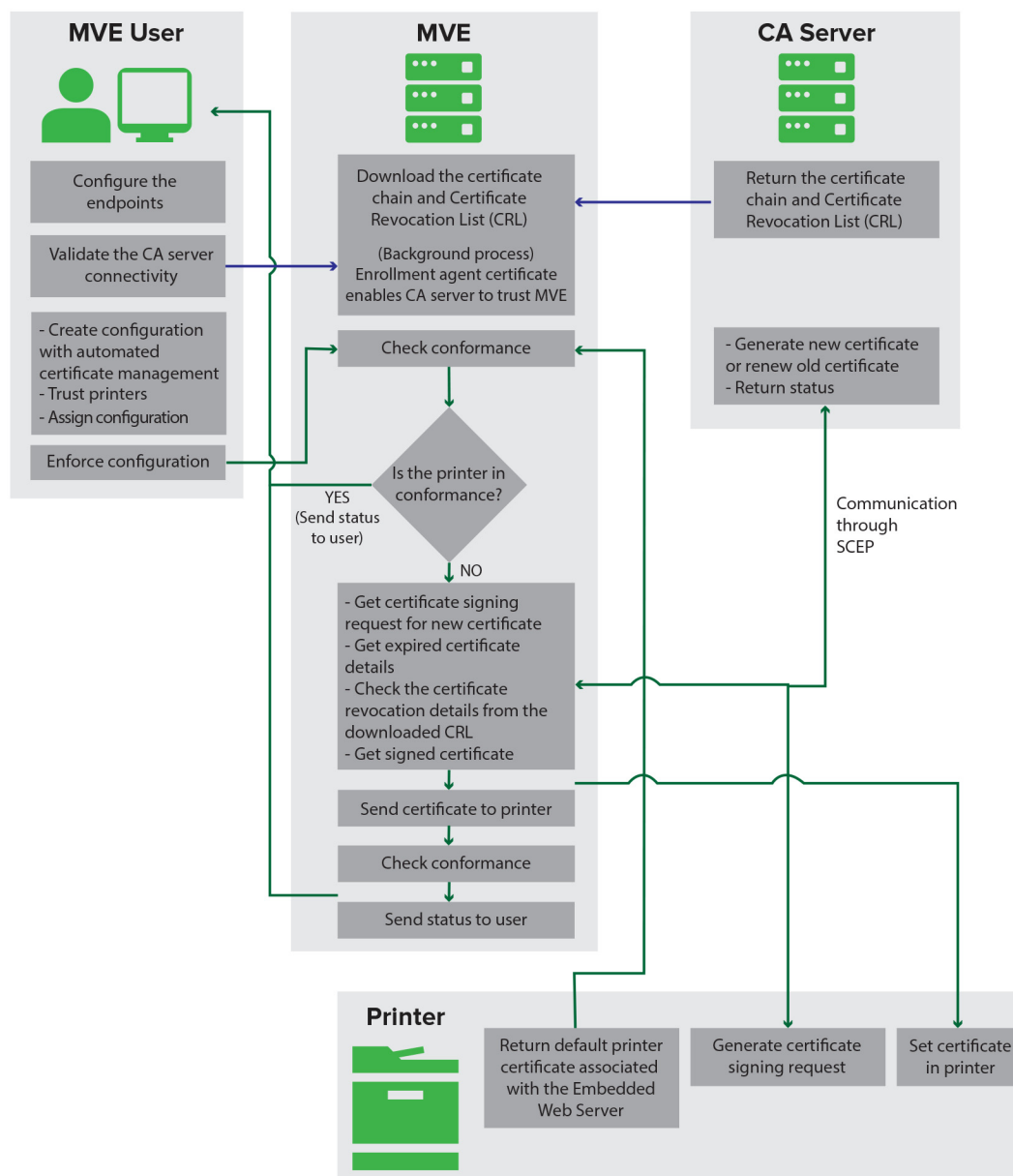
- 3 Cliquez sur **Importer ressource**.

Gestion des certificats

Configuration de MVE pour gérer automatiquement les certificats

Présentation de la fonction de gestion automatisée des certificats

Vous pouvez configurer MVE de sorte que les certificats d'imprimante soient gérés automatiquement, puis installés sur les imprimantes en appliquant la configuration. Le schéma suivant décrit le processus de bout en bout relatif à la fonction de gestion automatisée des certificats.



Les points de terminaison de l'autorité de certification, tels que le serveur CA et l'adresse du serveur, doivent être définis dans MVE.

Les serveurs CA pris en charge sont les suivants :

- **Autorité de certification OpenXPki** : pour plus d'informations, reportez-vous à [« Gestion des certificats à l'aide de l'autorité de certification OpenXPki » à la page 84](#).
- **CA d'entreprise Microsoft** : pour plus d'informations, reportez-vous à [« Gestion des certificats à l'aide de l'autorité de certification Microsoft » à la page 76](#).

La connexion entre MVE et les serveurs CA doit être validée. Pendant la validation, MVE communique avec le serveur CA pour télécharger la chaîne de certificats et la liste de révocation des certificats (CRL). Le certificat de l'agent d'inscription est également généré. Ce certificat permet au serveur CA d'approuver MVE.

Pour plus d'informations sur la définition des points de terminaison et la validation, reportez-vous à la section [« Configuration de MVE pour la gestion automatisée des certificats » à la page 75](#).

Une configuration définie pour **Utiliser Markvision pour gérer les certificats de périphérique** doit être attribuée et appliquée à l'imprimante.

Pour plus d'informations, reportez-vous aux rubriques suivantes :

- [« Création d'une configuration » à la page 67](#)
- [« Mise en œuvre de configurations » à la page 60](#)

Pendant l'application, MVE vérifie la conformité de l'imprimante. Le certificat d'imprimante par défaut est validé par rapport à la chaîne de certificats téléchargée à partir du serveur CA. Si l'imprimante n'est pas conforme, une demande de signature de certificat (CSR) est demandée pour l'imprimante. MVE communique avec le serveur CA via le protocole SCEP (Simple Certificate Enrollment Protocol, inscription de certificats simple). Le serveur CA génère le nouveau certificat, puis MVE l'envoie à l'imprimante.

Configuration de MVE pour la gestion automatisée des certificats

1 Dans le coin supérieur droit de la page, cliquez sur .

2 Cliquez sur **Autorité de certification > Utiliser le serveur d'autorité de certification**.

Remarque : Le bouton Utiliser le serveur d'autorité de certification s'affiche uniquement lors de la configuration initiale de l'autorité de certification ou lors de la suppression du certificat.

3 Configurez les points de terminaison du serveur.

- **Serveur CA** : serveur de l'autorité de certification (CA) qui génère les certificats d'imprimante. Vous pouvez sélectionner le CA OpenXPki ou le CA d'entreprise Microsoft.
- **Adresse du serveur CA** : l'adresse IP ou le nom de l'hôte du serveur CA. Incluez l'URL complète.
- **Mot de passe de vérification** : mot de passe requis pour confirmer l'identité de MVE sur le serveur CA. Le mot de passe de vérification n'est pas pris en charge par le CA d'entreprise Microsoft.

Remarque : En fonction du serveur CA, reportez-vous à [« Gestion des certificats à l'aide de l'autorité de certification OpenXPki » à la page 84](#) ou [« Gestion des certificats à l'aide de l'autorité de certification Microsoft » à la page 76](#).

4 Cliquez sur **Enregistrer les modifications et valider > OK**.

Remarque : La connexion entre MVE et les serveurs CA doit être validée. Pendant la validation, MVE communique avec le serveur CA pour télécharger la chaîne de certificats et la liste de révocation des certificats (CRL). Le certificat de l'agent d'inscription est également généré. Ce certificat permet au serveur CA d'approuver MVE.

5 Revenez à la page Configuration du système, puis vérifiez le certificat CA.

Remarque : Vous pouvez également télécharger ou supprimer le certificat CA.

Gestion des certificats à l'aide de l'autorité de certification Microsoft

Cette section fournit des instructions sur les points suivants :

- Configuration de l'autorité de certification (CA) d'entreprise Microsoft à l'aide du Network Device Enrollment Service (NDES) de Microsoft
- Création d'un serveur CA racine

Remarque : Le système d'exploitation Windows Server 2016 est utilisé pour toutes les configurations de ce document.

Configuration du serveur CA racine

Aperçu

Le serveur CA racine est le serveur d'autorité de certification principal de toute organisation et est le premier de l'infrastructure PKI. L'autorité de certification racine authentifie le serveur CA subordonné. Ce serveur est généralement maintenu en mode hors ligne pour empêcher toute intrusion et sécuriser la clé privée.

Pour configurer le serveur CA racine, procédez comme suit :

- 1 Vérifiez que le serveur CA racine est installé. Pour plus d'informations, reportez-vous à la section [« Installation du serveur CA racine » à la page 76](#).
- 2 Configurez les paramètres du point de distribution de la certification et de l'accès aux informations d'autorité. Pour plus d'informations, reportez-vous à la section [« Configuration des paramètres du point de distribution de la certification et de l'accès aux informations d'autorité » à la page 80](#).
- 3 Configurez l'accessibilité CRL. Pour plus d'informations, reportez-vous à la section [« Configuration de l'accessibilité CRL » à la page 81](#).

Installation du serveur CA racine

- 1 Dans Server Manager, cliquez sur **Gérer > Ajouter des rôles et des fonctionnalités**.
- 2 Cliquez sur **Rôles du serveur**, sélectionnez **Services de certificats Active Directory** et toutes ses fonctionnalités, puis cliquez sur **Suivant**.
- 3 Dans la section Services de rôle AD CS, sélectionnez **Autorité de certification**, puis cliquez sur **Suivant > Installer**.

- 4 Après l'installation, cliquez sur **Configurer les services de certificats Active Directory sur le serveur de destination**.
- 5 Dans la section Services de rôle, sélectionnez **Autorité de certification > Suivant**.
- 6 Dans la section Type de configuration, sélectionnez **Autorité de certification autonome**, puis cliquez sur **Suivant**.
- 7 Dans la section Type d'autorité de certification, sélectionnez **Autorité de certification racine**, puis cliquez sur **Suivant**.
- 8 Sélectionnez **Créer une nouvelle clé privée**, puis cliquez sur **Suivant**.
- 9 Dans le menu Sélectionner un fournisseur de cryptographie, sélectionnez **RSA#Microsoft Software Key Storage Provider**.
- 10 Dans le menu Longueur de clé, sélectionnez **4096**.
- 11 Dans la liste des algorithmes de hachage, sélectionnez **SHA512**, puis cliquez sur **Suivant**.
- 12 Dans le champ Nom commun de cette autorité de certification, saisissez le nom du serveur d'hébergement.
- 13 Dans le champ Suffixe du nom unique, saisissez le composant de domaine.

Exemple de configuration du nom de l'autorité de certification

Nom de domaine complet de la machine (FQDN - Fully Qualified Domain Name) :

test.dev.lexmark.com

Nom commun (CN) : **TEST**

Suffixe du nom unique : **DC=DEV, DC=LEXMARK, DC=COM**

- 14 Cliquez sur **Suivant**.
- 15 Spécifiez la période de validité, puis cliquez sur **Suivant**.
Remarque : En général, la période de validité est de 10 ans.
- 16 Ne modifiez rien dans la fenêtre des emplacements de la base de données.
- 17 Terminez l'installation.

Configuration de la CA d'entreprise Microsoft avec NDES

Aperçu

Dans le scénario de déploiement suivant, toutes les autorisations sont basées sur les autorisations définies sur les modèles de certificat publiés dans le contrôleur de domaine. Les demandes de certificat envoyées à l'autorité de certification sont basées sur des modèles de certificat.

Pour cette configuration, assurez-vous que vous disposez des éléments suivants :

- Une machine hébergeant l'autorité de certification subordonnée (il peut également s'agir de l'autorité de certification racine)
- Une machine hébergeant le service NDES
- Un contrôleur de domaine

Utilisateurs requis

Créez les utilisateurs suivants dans le contrôleur de domaine :

- Administrateur de service
 - Nommé **SCEPAdmin**
 - Doit être membre des groupes **administrateur local** et **administrateur d'entreprise**
 - Doit être connecté localement lorsque l'installation du rôle NDES est déclenchée
 - Dispose de l'**autorisation Inscrire** pour les modèles de certificat
 - Dispose de l'**autorisation Ajouter un modèle** sur l'autorité de certification
- Compte de service
 - Nommé **SCEPSvc**
 - Doit être membre du groupe **IIS_IUSRS** local
 - Doit être un utilisateur de domaine et dispose d'autorisations de **lecture** et d'**inscription** sur les modèles configurés
 - Dispose de l'autorisation de **demande** sur l'autorité de certification
- Administrateur du périphérique
 - Nommé **DeviceAdmin**
 - Dispose de l'**autorisation Inscrire** sur tous les modèles configurés dans le registre

Configuration du serveur CA subordonné

Aperçu

Le serveur CA subordonné est le serveur CA intermédiaire et est toujours en ligne. Il gère généralement la gestion des certificats.

Pour configurer le serveur CA subordonné, procédez comme suit :

- 1** Vérifiez que le serveur CA subordonné est installé. Pour plus d'informations, reportez-vous à la section [« Installation du serveur CA subordonné » à la page 78](#).
- 2** Configurez les paramètres du point de distribution de la certification et de l'accès aux informations d'autorité. Pour plus d'informations, reportez-vous à la section [« Configuration des paramètres du point de distribution de la certification et de l'accès aux informations d'autorité » à la page 80](#).
- 3** Configurez l'accessibilité CRL. Pour plus d'informations, reportez-vous à la section [« Configuration de l'accessibilité CRL » à la page 81](#).

Installation du serveur CA subordonné

- 1** A partir du serveur, connectez-vous en tant qu'utilisateur de domaine **SCEPAdmin**.
- 2** Dans Server Manager, cliquez sur **Gérer > Ajouter des rôles et des fonctionnalités**.
- 3** Cliquez sur **Rôles du serveur**, sélectionnez **Services de certificats Active Directory** et toutes ses fonctionnalités, puis cliquez sur **Suivant**.

- 4 Dans la section Services de rôle AD CS, sélectionnez **Autorité de certification** et **Inscription Web de l'autorité de certification**, puis cliquez sur **Suivant**.
Remarque : Vérifiez que toutes les fonctionnalités de Inscription Web de l'autorité de certification sont ajoutées.
- 5 Dans la section Services de rôle du rôle Serveur Web (IIS), conservez les paramètres par défaut.
- 6 Après l'installation, cliquez sur **Configurer les services de certificats Active Directory sur le serveur de destination**.
- 7 Dans la section Services de rôle, sélectionnez **Autorité de certification** et **Inscription Web de l'autorité de certification**, puis cliquez sur **Suivant**.
- 8 Dans la section Type de configuration, sélectionnez **Autorité de certification d'entreprise**, puis cliquez sur **Suivant**.
- 9 Dans la section Type d'autorité de certification, sélectionnez **Autorité de certification subordonnée**, puis cliquez sur **Suivant**.
- 10 Sélectionnez **Créer une nouvelle clé privée**, puis cliquez sur **Suivant**.
- 11 Dans le menu Sélectionner un fournisseur de cryptographie, sélectionnez **RSA#Microsoft Software Key Storage Provider**.
- 12 Dans le menu Longueur de clé, sélectionnez **4096**.
- 13 Dans la liste des algorithmes de hachage, sélectionnez **SHA512**, puis cliquez sur **Suivant**.
- 14 Dans le champ Nom commun de cette autorité de certification, saisissez le nom du serveur d'hébergement.
- 15 Dans le champ Suffixe du nom unique, saisissez le composant de domaine.

Exemple de configuration du nom de l'autorité de certification

Nom de domaine complet de la machine (FQDN - Fully Qualified Domain Name) :

test.dev.lexmark.com

Nom commun (CN) : **TEST**

Suffixe du nom unique : **DC=DEV, DC=LEXMARK, DC=COM**

- 16 Dans la boîte de dialogue Demande de certificat, enregistrez le fichier de demande, puis cliquez sur **Suivant**.
- 17 Ne modifiez rien dans la fenêtre des emplacements de la base de données.
- 18 Terminez l'installation.
- 19 Signez la demande de l'autorité de certification racine, puis exportez le certificat signé au format PKCS7.
- 20 A partir de l'autorité de certification subordonnée, ouvrez **Autorité de certification**.
- 21 Dans le panneau de gauche, cliquez avec le bouton droit de la souris sur l'autorité de certification, puis cliquez sur **Toutes les tâches > Installer le certificat CA**.
- 22 Sélectionnez le certificat signé, puis démarrez le service d'autorisation de certificat.

Configuration des paramètres du point de distribution de la certification et de l'accès aux informations d'autorité

Remarque : Configurez les paramètres CDP (Certification Distribution Point, point de distribution de certification) et AIA (Authority Information Access, accès aux informations de l'autorité) pour la CRL (Certificate Revocation List, liste de révocation de certification).

- 1 Dans Server Manager, cliquez sur **Outils > Autorité de certification**.
- 2 Dans le panneau de gauche, cliquez avec le bouton droit de la souris sur l'autorité de certification, puis cliquez sur **Propriétés > Extensions**.
- 3 Dans le menu Sélectionner un poste, sélectionnez **Point de distribution CRL (CDP)**.
- 4 Dans la liste de révocation des certificats, sélectionnez **C:\Windows\system32**, puis procédez comme suit :
 - a Sélectionnez **Publier les CRL à cet emplacement**.
 - b Désactivez **Publier les CRL à cet emplacement**.
- 5 Supprimez toutes les autres entrées sauf **C:\Windows\system32**.
- 6 Cliquez sur **Ajouter**.
- 7 Dans le champ Emplacement, ajoutez **http://serverIP/CertEnroll/<CAName><CRLNameSuffix><DeltaCRLAllowed>.crl**, où **serverIP** est l'adresse IP du serveur.

Remarque : Si votre serveur est accessible à l'aide du FQDN, utilisez le DNS du serveur au lieu de son adresse IP.
- 8 Cliquez sur **OK**.
- 9 Sélectionnez **Inclure dans l'extension CDP des certificats émis** pour l'entrée créée.
- 10 Dans le menu Sélectionner un poste, sélectionnez **Accès aux informations de l'autorité (AIA)**.
- 11 Supprimez toutes les autres entrées sauf **C:\Windows\system32**.
- 12 Cliquez sur **Ajouter**.
- 13 Dans le champ Emplacement, ajoutez **http://serverIP/CertEnroll/<ServerDNSName>_<CAName><CertificateName>.crt**, où **serverIP** est l'adresse IP du serveur.

Remarque : Si votre serveur est accessible à l'aide du FQDN, utilisez le DNS du serveur au lieu de son adresse IP.
- 14 Cliquez sur **OK**.
- 15 Sélectionnez **Inclure dans l'extension AIA des certificats émis** pour l'entrée créée.
- 16 Cliquez sur **Appliquer > OK**.

Remarque : Si nécessaire, redémarrez le service de certification.
- 17 Dans le volet de gauche, développez l'autorité de certification, cliquez avec le bouton droit de la souris sur **Certificats révoqués**, puis cliquez sur **Propriétés**.

- 18 Spécifiez la valeur de Intervalle de publication CRL et Intervalle de publication des CRL Delta, puis cliquez sur **Appliquer > OK**.
- 19 Dans le panneau de gauche, cliquez avec le bouton droit de la souris sur **Certificats révoqués**, cliquez sur **Toutes les tâches**, puis publiez dans la nouvelle CRL.

Configuration de l'accessibilité CRL

Remarque : Avant de commencer, assurez-vous que le gestionnaire Internet Information Services (IIS) est installé.

- 1 Dans le gestionnaire IIS, développez l'autorité de certification, puis développez **Sites**.
- 2 Cliquez avec le bouton droit de la souris sur **Site Web par défaut**, puis cliquez sur **Ajouter un répertoire virtuel**.
- 3 Dans le champ Alias, saisissez **CertEnroll**.
- 4 Dans le champ Chemin physique, saisissez **C:\Windows\System32\CertSrv\CertEnroll**.
- 5 Cliquez sur **OK**.
- 6 Cliquez avec le bouton droit de la souris sur **CertEnroll**, puis cliquez sur **Modifier les autorisations**.
- 7 Dans l'onglet Sécurité, supprimez tout accès en écriture, à l'exception du système.
- 8 Cliquez sur **OK**.

Configuration du serveur NDES

- 1 A partir du serveur, connectez-vous en tant qu'utilisateur de domaine **SCEPAdmin**.
- 2 Dans Server Manager, cliquez sur **Gérer > Ajouter des rôles et des fonctionnalités**.
- 3 Cliquez sur **Rôles du serveur**, sélectionnez **Services de certificats Active Directory** et toutes ses fonctionnalités, puis cliquez sur **Suivant**.
- 4 Dans la section Services de rôle AD CS, désactivez **Autorité de certification**.
- 5 Sélectionnez **Network Device Enrollment Service** et toutes ses fonctionnalités, puis cliquez sur **Suivant**.
- 6 Dans la section Services de rôle du rôle Serveur Web (IIS), conservez les paramètres par défaut.
- 7 Après l'installation, cliquez sur **Configurer les services de certificats Active Directory sur le serveur de destination**.
- 8 Dans la section Services de rôle, sélectionnez **Network Device Enrollment Service**, puis cliquez sur **Suivant**.
- 9 Sélectionnez le compte de service **SCEPSvc**.
- 10 Dans la section Autorité de certification pour NDES, sélectionnez **Nom de l'autorité de certification** ou **Nom de l'ordinateur**, puis cliquez sur **Suivant**.
- 11 Dans la section Informations RA, spécifiez les informations, puis cliquez sur **Suivant**.
- 12 Dans la section Cryptographie pour NDES, procédez comme suit :
 - Sélectionnez les fournisseurs de signature et de clé de cryptage appropriés.
 - Dans le menu Longueur de la clé, sélectionnez la même longueur de clé que le serveur CA.

13 Cliquez sur **Suivant**.

14 Terminez l'installation.

Vous pouvez désormais accéder au serveur NDES à partir d'un navigateur Web en tant qu'utilisateur SCEPSvc. A partir du serveur NDES, vous pouvez afficher la miniature du certificat de l'autorité de certification, le mot de passe de challenge de l'inscription et la période de validité du mot de passe de challenge.

Accès au serveur NDES

Ouvrez un navigateur Web et saisissez **http://NDESserverIP/certsrv/mscep_admin**, où **NDESserverIP** correspond à l'adresse IP du serveur NDES.

Configuration de NDES pour MVE

Remarque : Avant de commencer, assurez-vous que le serveur NDES fonctionne correctement.

Création d'un modèle de certificat

- 1** A partir de l'autorité de certification (certsrv) subordonnée, ouvrez **Autorité de certification**.
- 2** Dans le panneau de gauche, développez l'autorité de certification en cliquant avec le bouton droit de la souris sur **Modèles de certificat**, puis sur **Gérer**.
- 3** Dans Console des modèles de certificat, créez une copie de **Serveur Web**.
- 4** Dans l'onglet Général, saisissez **MVEWebServer** comme nom de modèle.
- 5** Dans l'onglet Sécurité, attribuez aux utilisateurs **SCEPAdmin** et **SCEPSvc** les autorisations appropriées.
Remarque : Pour plus d'informations, reportez-vous à la section « [Utilisateurs requis](#) » à la page 78.
- 6** Dans l'onglet Nom d'objet, sélectionnez **Envoyer la demande**.
- 7** A partir de l'autorité de certification (certsrv) subordonnée, ouvrez **Autorité de certification**.
- 8** Dans l'onglet Extensions, sélectionnez **Stratégies d'application > Modifier**.
- 9** Cliquez sur **Ajouter > Authentification client > OK**.
- 10** Dans le panneau de gauche, développez l'autorité de certification en cliquant avec le bouton droit de la souris sur **Modèles de certificat**, puis sur **Nouveau > Modèle de certificat à fournir**.
- 11** Sélectionnez les nouveaux certificats créés, puis cliquez sur **OK**.

Vous pouvez désormais accéder aux modèles à l'aide du portail d'inscription Web de l'autorité de certification.

Accès aux modèles

- 1** Ouvrez un navigateur Web et saisissez **http://CAserverIP/certsrv/certrqxt.asp**, où **CAserverIP** correspond à l'adresse IP du serveur CA.
- 2** Dans le menu Modèle de certificat, affichez les modèles.

Définition des modèles de certificat pour NDES

- 1** A partir de votre ordinateur, lancez l'éditeur de registre.
- 2** Accédez à **HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptographie > MSCEP**.

- 3** Configurez les éléments suivants, puis définissez-les sur **MVEWebServer** :
 - EncryptionTemplate
 - GeneralPurposeTemplate
 - SignatureTemplate
- 4** Donnez à l'utilisateur SCEPSvc l'autorisation complète sur MSCEP.
- 5** Dans le gestionnaire IIS, développez l'autorité de certification, puis cliquez sur **Pools d'applications**.
- 6** Dans le volet de droite, cliquez sur **Recycler** pour redémarrer le pool d'applications SCEP.
- 7** Dans le gestionnaire IIS, développez l'autorité de certification, puis **Sites > Site Web par défaut**.
- 8** Dans le panneau de droite, cliquez sur **Redémarrer**.

Désactivation de Mot de passe de challenge sur le serveur CA de Microsoft

- 1** A partir de votre ordinateur, lancez l'éditeur de registre.
- 2** Accédez à **HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptographie > MSCEP**.
- 3** Définissez EnforcePassword sur **0**.
- 4** Dans le gestionnaire IIS, développez l'autorité de certification, cliquez sur **Pools d'applications**, puis sélectionnez **SCEP**.
- 5** Dans le panneau de droite, cliquez sur **Paramètres avancés**.
- 6** Définissez Charger le profil utilisateur sur **True**, puis cliquez sur **OK**.
- 7** Dans le volet de droite, cliquez sur **Recycler** pour redémarrer le pool d'applications SCEP.
- 8** Dans le gestionnaire IIS, développez l'autorité de certification, puis **Sites > Site Web par défaut**.
- 9** Dans le panneau de droite, cliquez sur **Redémarrer**.

Lors de l'ouverture de NDES à partir du navigateur Web, vous ne pouvez désormais afficher que la miniature de l'autorité de certification.

Gestion des certificats à l'aide de l'autorité de certification OpenXPki

Cette section fournit des instructions sur la configuration de l'autorité de certification OpenXPki version 2.5.x à l'aide du protocole SCEP (Simple Certificate Enrollment Protocol).

Remarques :

- Vérifiez que vous utilisez le système d'exploitation Debian 8 Jessie.
- Pour plus d'informations sur OpenXPki, rendez-vous sur www.openxpki.org.

Configuration de l'autorité de certification OpenXPki

Installation de l'autorité de certification OpenXPki

- 1 Connectez la machine à l'aide de PuTTY ou d'un autre client.
- 2 A partir du client, exécutez la commande **sudo su** - pour accéder à l'utilisateur racine.
- 3 Saisissez le mot de passe racine.
- 4 Dans **nano /etc/apt/sources.list**, modifiez la source pour l'installation des mises à jour.
- 5 Mettez à jour le fichier. Par exemple :

```
#  
  
# deb cdrom:[Debian GNU/Linux 8.11.1 _Jessie_ - Official amd64 CD Binary-1  
20190211-02:10]/ jessie local main  
# deb cdrom:[Debian GNU/Linux 8.11.1 _Jessie_ - Official amd64 CD Binary-1  
20190211-02:10]/ jessie local main  
  
deb http://security.debian.org/ jessie/updates main  
deb-src http://security.debian.org/ jessie/updates main  
  
# jessie-updates, previously known as 'volatile'  
# A network mirror was not selected during install. The following entries  
# are provided as examples, but you should amend them as appropriate  
# for your mirror of choice.  
#  
deb http://ftp.debian.org/debian/jessie-updates main  
deb-src http://ftp.debian.org/debian/jessie-updates main  
deb http://ftp.us.debian.org/debian/jessie main
```
- 6 Enregistrez le fichier.
- 7 Exécutez les commandes suivantes :
 - **mise à jour apt-get**
 - **mise à niveau apt-get**
- 8 Mettez à jour les listes de certificats CA du serveur à l'aide de **apt-get install ca-certificates**.
- 9 Installez le paramètre local **en_US.utf8 locale** à l'aide des paramètres locaux **dpkg-reconfigure locales**.
- 10 Sélectionnez le paramètre local **en_US.UTF-8 UTF-8**, puis définissez-le comme paramètre local par défaut pour le système.

Remarque : Utilisez les touches de tabulation et la barre d'espace pour sélectionner et naviguer dans le menu.

11 Vérifiez les paramètres locaux que vous avez générés à l'aide de **locale -a**.

Exemple d'impression

```
C
C.UTF-8
en_IN
en_IN.utf8
en_US.utf8
POSIX
```

12 Copiez l'empreinte du package OpenXPki à l'aide de **nano /home/Release.key**. Dans ce cas, copiez la clé dans **/home**.

13 Saisissez **9B156AD0 F0E6A6C7 86FABE7A D8363C4E 1611A2BE 2B251336 01D1CDB4 6C24BEF3** comme valeur.

14 Exécutez la commande suivante :

```
gpg --print-md sha256 /home/Release.key
```

15 Ajoutez le package à l'aide de la commande **wget https://packages.openxpki.org/v2/debian/Release.key -O - | apt-key add -**.

16 Ajoutez le référentiel à votre liste source (jessie) à l'aide de **echo "deb http://packages.openxpki.org/v2/debian/jessie release" > /etc/apt/sources.list.d/openxpki.list**, puis **aptitude update**.

17 Installez la liaison MySQL et Perl MySQL à l'aide de **aptitude install mysql-server libdbd-mysql-perl**.

18 Installez **apache2.2-common** à l'aide de **aptitude install apache2.2-common**.

19 Dans **nano /etc/apt/sources.list**, installez le module **fastcgi** pour accélérer l'interface utilisateur.

Remarque : Nous vous recommandons d'utiliser **mod_fcgid**.

20 Ajoutez la ligne **deb http://http.us.debian.org/debian/jessie main** dans le fichier, puis enregistrez-la.

21 Exécutez les commandes suivantes :

```
mise à jour apt-get
aptitude install libapache2-mod-fcgid
```

22 Activez le module **fastcgi** à l'aide de **a2enmod fcgid**.

23 Installez le package principal OpenXPki à l'aide de **aptitude install libopenxpki-perl openxpki-cgi-session-driver openxpki-i18n**.

24 Redémarrez le serveur Apache® en utilisant le **service de redémarrage apache2**.

25 Vérifiez si l'installation est réussie à l'aide de **openxpkiadm version**.

Remarque : Si l'installation est réussie, le système affiche la version d'OpenXPki installée. Par exemple, **Version (principale) : 2.5.5**.

26 Créez la base de données vide, puis affectez l'utilisateur de la base de données à l'aide de **mysql -u root -p**.

Remarques :

- Cette commande doit être saisie dans le client. Sinon, vous ne pouvez pas saisir le mot de passe.

- Saisissez le mot de passe pour MySQL. Pour cette instance, **root** est l'utilisateur MySQL.
- **MySQL** est l'utilisateur sur lequel OpenXPki est installé.

```
CREATE DATABASE openxpki CHARSET utf8;
CREATE USER 'openxpki'@'localhost' IDENTIFIED BY 'openxpki';
GRANT ALL ON openxpki.* TO 'openxpki'@'localhost';
flush privileges;
```

Si le service MySQL n'est pas en cours d'exécution, exécutez **/etc/init.d/mysql start** pour lancer le service.

27 Saisissez **quit** pour quitter MySQL.

28 Stockez les informations d'identification utilisées dans **/etc/openxpki/config.d/system/database.yaml**.

Exemple de contenu du fichier

```
debug: 0
type: MySQL
name: openxpki
host: localhost
port: 3306
user: openxpki
passwd: openxpki
```

Remarque : Modifiez les champs **user** et **passwd** pour qu'ils correspondent au nom d'utilisateur et au mot de passe MySQL.

29 Enregistrez le fichier.

30 Pour un schéma de base de données vide, exécutez **zcat /usr/share/doc/libopenxpki-perl/examples/schema-mysql.sql.gz | \mysql -u root --password --database openxpki** à partir du fichier de schéma fourni.

31 Saisissez le mot de passe de la base de données.

configuration de l'autorité de certification OpenXPki à l'aide du script par défaut

Remarque : Le script par défaut configure uniquement le domaine par défaut, **ca-one**. Les CDP et CRL ne sont pas configurés.

- 1** Décompressez l'exemple de script pour installer le certificat à l'aide de **gunzip -k /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh.gz**.
- 2** Exécutez le script à l'aide de **bash /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh**.
- 3** Confirmez la configuration à l'aide de **openxpkiadm alias --realm ca-one**.

Exemple d'impression

```
=== functional token ===
scep (scep):
Alias      : scep-1
Identifier: YsBNZ7JYTbx89F_-Z4jn_RPFFWo
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2016-01-30 20:44:40

vault (datasafe):
Alias      : vault-1
Identifier: lZILS1l6Km5aIGS6pA7P7azAJic
```

```
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2016-01-30 20:44:40

ca-signer (certsign):
Alias      : ca-signer-1
Identifier: Sw_IY7AdoGUp28F_cFEhbtI9pE
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2018-01-29 20:44:40

=== root ca ===
current root ca:
Alias      : root-1
Identifier: fVrqJAlpotPais0Asnxa9cglXCc
NotBefore : 2015-01-30 20:44:39
NotAfter  : 2020-01-30 20:44:39

upcoming root ca:
not set
```

4 Vérifiez si l'installation est réussie à l'aide de **openxpkictl start**.

Exemple d'impression

```
Starting OpenXPki...
OpenXPki Server is running and accepting requests.
DONE.
```

5 Pour accéder au serveur OpenXPki, procédez comme suit :

- a** Depuis un navigateur Web, saisissez **http://ipaddress/openxpki/**.
- b** Connectez-vous en tant qu'**opérateur**. Le mot de passe par défaut est **openxpki**.

Remarque : La connexion Opérateur a deux comptes opérateur préconfigurés, **raop** et **raop2**.

6 Créez une demande de certificat, puis testez-la.

Configuration manuelle de l'autorité de certification OpenXPki

Aperçu

Remarque : Avant de commencer, assurez-vous de disposer de connaissances de base sur la création de certificats OpenSSL.

Pour configurer l'autorité de certification OpenXPki manuellement, créez les éléments suivants :

- 1** Certificat CA racine. Pour plus d'informations, reportez-vous à la section [« Création d'un certificat CA racine » à la page 89](#).
- 2** Certificat du signataire de l'autorité de certification, signé par l'autorité de certification racine. Pour plus d'informations, reportez-vous à la section [« Création d'un certificat de signataire » à la page 89](#).
- 3** Certificat du coffre de données, auto-signé. Pour plus d'informations, reportez-vous à la section [« Création d'un certificat de coffre » à la page 90](#).
- 4** Certificat SCEP, signé par le certificat du signataire.

Remarques :

- Lorsque vous sélectionnez le hachage de signature, utilisez SHA256 ou SHA512.
- La modification de la taille de la clé publique est facultative.

Pour cette instance, nous utilisons le répertoire **/etc/certs/openxpki_ca-one/** pour la génération de certificats. Cependant, vous pouvez utiliser n'importe quel répertoire.

Création d'un fichier de configuration OpenSSL

1 Exécutez la commande suivante :

```
nano /etc/certs/openxpki_ca-one/openssl.conf
```

Remarque : Si votre serveur est accessible à l'aide du Fully Qualified Domain Name (FQDN), utilisez le DNS du serveur au lieu de son adresse IP.

Exemple de fichier

```
# x509_extensions          = v3_ca_extensions
# x509_extensions          = v3_issuing_extensions
# x509_extensions          = v3_datavault_extensions
# x509_extensions          = v3_scep_extensions
# x509_extensions          = v3_web_extensions
# x509_extensions          = v3_ca_reqexts # not for root self-signed, only for issuing
## x509_extensions         = v3_datavault_reqexts # not required self-signed
# x509_extensions          = v3_scep_reqexts
# x509_extensions          = v3_web_reqexts

[ req ]
default_bits              = 4096
distinguished_name        = req_distinguished_name

[ req_distinguished_name ]
domainComponent           = Domain Component
commonName                = Common Name

[ v3_ca_reqexts ]
subjectKeyIdentifier       = hash
keyUsage                   = digitalSignature, keyCertSign, cRLSign

[ v3_datavault_reqexts ]
subjectKeyIdentifier       = hash
keyUsage                   = keyEncipherment
extendedKeyUsage           = emailProtection

[ v3_scep_reqexts ]
subjectKeyIdentifier       = hash

[ v3_web_reqexts ]
subjectKeyIdentifier       = hash
keyUsage                   = critical, digitalSignature, keyEncipherment
extendedKeyUsage           = serverAuth, clientAuth

[ v3_ca_extensions ]
subjectKeyIdentifier       = hash
keyUsage                   = digitalSignature, keyCertSign, cRLSign
basicConstraints           = critical,CA:TRUE
authorityKeyIdentifier     = keyid:always,issuer

[ v3_issuing_extensions ]
subjectKeyIdentifier       = hash
keyUsage                   = digitalSignature, keyCertSign, cRLSign
basicConstraints           = critical,CA:TRUE
authorityKeyIdentifier     = keyid:always,issuer:always
crlDistributionPoints       = URI:http://10.195.0.111/CertEnroll/MYOPENXPKI.crl
authorityInfoAccess         = caIssuers;URI:http://10.195.0.111/CertEnroll/MYOPENXPKI.crt

[ v3_datavault_extensions ]
subjectKeyIdentifier       = hash
keyUsage                   = keyEncipherment
extendedKeyUsage           = emailProtection
basicConstraints           = CA:FALSE
authorityKeyIdentifier     = keyid:always,issuer

[ v3_scep_extensions ]
subjectKeyIdentifier       = hash
basicConstraints           = CA:FALSE
authorityKeyIdentifier     = keyid,issuer
```



```
[ v3_web_extensions ]
subjectKeyIdentifier    = hash
keyUsage                = critical, digitalSignature, keyEncipherment
extendedKeyUsage        = serverAuth, clientAuth
basicConstraints        = critical, CA:FALSE
subjectAltName          = DNS:stloopenxpkgi.dhcp.indiadev.lexmark.com
crlDistributionPoints    = URI:http://10.195.0.111/CertEnroll/MYOPENXPKE_ISSUINGCA.crl
authorityInfoAccess     =
caIssuers;URI:http://10.195.0.111/CertEnroll/MYOPENXPKE_ISSUINGCA.crt
```

2 Modifiez l'adresse IP et le nom du certificat CA avec vos informations de configuration.

3 Enregistrez le fichier.

Création d'un fichier de mots de passe pour les clés de certificat

1 Exécutez la commande suivante :

```
nano /etc/certs/openxpkgi_ca-one/pd.pass
```

2 Saisissez votre mot de passe.

3 Enregistrez le fichier.

Création d'un certificat CA racine

Remarque : Vous pouvez créer un certificat CA racine auto-signé ou générer une demande de certificat, puis le faire signer par l'autorité de certification racine.

Exécutez les commandes suivantes :

Remarque : Remplacez la longueur de clé, l'algorithme de signature et le nom du certificat par les valeurs appropriées.

```
1 openssl genrsa -out /etc/certs/openxpkgi_ca-one/ca-root-1.key -passout  
file:/etc/certs/openxpkgi_ca-one/pd.pass 4096
```

```
2 openssl req -new -key /etc/certs/openxpkgi_ca-one/ca-root-1.key -  
subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=MYOPENXPKE_ROOTCA -  
out /etc/certs/openxpkgi_ca-one/ca-root-1.csr
```

```
3 openssl req -config /etc/certs/openxpkgi_ca-one/openssl.conf -extensions  
v3_ca_extensions -x509 -days 3560 -in /etc/certs/openxpkgi_ca-one/ca-  
root-1.csr -key /etc/certs/openxpkgi_ca-one/ca-root-1.key -  
out /etc/certs/openxpkgi_ca-one/ca-root-1.crt -sha256
```

Création d'un certificat de signataire

Remarque : Remplacez la longueur de clé, l'algorithme de signature et le nom du certificat par les valeurs appropriées.

1 Exécutez la commande suivante :

```
openssl genrsa -out /etc/certs/openxpkgi_ca-one/ca-signer-1.key -passout  
file:/etc/certs/openxpkgi_ca-one/pd.pass 4096
```

- 2 Remplacez l'objet de la demande par vos informations d'autorité de certification en utilisant **openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -reqexts v3_ca_reqexts -new -key /etc/certs/openxpki_ca-one/ca-signer-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=MYOPENXPKI_ISSUINGCA -out /etc/certs/openxpki_ca-one/ca-signer-1.csr**.
- 3 Faites signer le certificat par l'autorité de certification racine à l'aide de **openssl x509 -req -extfile /etc/certs/openxpki_ca-one/openssl.conf -extensions v3_issuing_extensions -days 3650 -in /etc/certs/openxpki_ca-one/ca-signer-1.csr -CA /etc/certs/openxpki_ca-one/ca-root-1.crt -CAkey /etc/certs/openxpki_ca-one/ca-root-1.key -CAcreateserial -out /etc/certs/openxpki_ca-one/ca-signer-1.crt -sha256**.

Création d'un certificat de coffre

Remarques :

- Le certificat du coffre est auto-signé.
- Remplacez la longueur de clé, l'algorithme de signature et le nom du certificat par les valeurs appropriées.

- 1 Exécutez la commande suivante :

```
openssl genrsa -out /etc/certs/openxpki_ca-one/vault-1.key -passout  
file:/etc/certs/openxpki_ca-one/pd.pass 4096
```

- 2 Remplacez l'objet de la demande par vos informations d'autorité de certification en utilisant **openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -reqexts v3_datavault_reqexts -new -key /etc/certs/openxpki_ca-one/vault-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/DC=STLOPENXPKI_INTERNAL/CN=MYOPENXPKI_DATAVAULT -out /etc/certs/openxpki_ca-one/vault-1.csr**.
- 3 Exécutez la commande suivante :

```
openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -extensions  
v3_datavault_extensions -x509 -days 3560 -in /etc/certs/openxpki_ca-  
one/vault-1.csr -key /etc/certs/openxpki_ca-one/vault-1.key -  
out /etc/certs/openxpki_ca-one/vault-1.crt
```

Création d'un certificat SCEP

Remarque : Le certificat SCEP est signé par le certificat du signataire.

Exécutez les commandes suivantes :

Remarque : Remplacez la longueur de clé, l'algorithme de signature et le nom du certificat par les valeurs appropriées.

- 1 `openssl genrsa -out /etc/certs/openxpki_ca-one/scep-1.key -passout file:/etc/certs/openxpki_ca-one/pd.pass 4096`
- 2 `openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -reqexts v3_scep_reqexts -new -key /etc/certs/openxpki_ca-one/scep-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=MYOPENXPKI_SCEPCA -out /etc/certs/openxpki_ca-one/scep-1.csr`
- 3 `openssl x509 -req -extfile /etc/certs/openxpki_ca-one/openssl.conf -extensions v3_scep_extensions -days 900 -in /etc/certs/openxpki_ca-one/scep-1.csr -CA /etc/certs/openxpki_ca-one/ca-signer-1.crt -CAkey /etc/certs/openxpki_ca-one/ca-signer-1.key -CAcreateserial -out /etc/certs/openxpki_ca-one/scep-1.crt -sha256`

Copie du fichier de clés et création d'un lien symbolique

- 1 Copiez les fichiers de clés dans `/etc/openxpki/ca/ca-one/`.

Remarque : Les fichiers de clés doivent être lisibles par OpenXPki.

```
cp /etc/certs/openxpki_ca-one/ca-signer-1.key /etc/openxpki/ca/ca-one/
cp /etc/certs/openxpki_ca-one/vault-1.key /etc/openxpki/ca/ca-one/
cp /etc/certs/openxpki_ca-one/scep-1.key /etc/openxpki/ca/ca-one/
```

- 2 Créez le lien symbolique.

Remarque : Les liens symboliques sont des alias utilisés par la configuration par défaut.

```
ln -s /etc/openxpki/ca/ca-one/ca-signer-1.key /etc/openxpki/ca/ca-one/ca-signer-1.pem
ln -s /etc/openxpki/ca/ca-one/scep-1.key /etc/openxpki/ca/ca-one/scep-1.pem
ln -s /etc/openxpki/ca/ca-one/vault-1.key /etc/openxpki/ca/ca-one/vault-1.pem
```

Importation des certificats

Importez le certificat racine, le certificat du signataire, le certificat du coffre et le certificat SCEP dans la base de données avec les jetons appropriés.

Exécutez les commandes suivantes :

- 1 `openxpkiadm certificate import --file /etc/certs/openxpki_ca-one/ca-root-1.crt`
- 2 `openxpkiadm certificate import --file /etc/certs/openxpki_ca-one/ca-signer-1.crt --realm ca-one --token certsign`
- 3 `openxpkiadm certificate import --file /etc/certs/openxpki_ca-one/scep-1.crt --realm ca-one --token scep`
- 4 `openxpkiadm certificate import --file /etc/certs/openxpki_ca-one/vault-1.crt --realm ca-one --token datasafe`

5 Vérifiez si l'importation est réussie à l'aide de **openxpkiadm alias --realm ca-one**.

Exemple d'impression

```
=== functional token ===
scep (scep):
Alias      : scep-1
Identifiant: YsBNZ7JYTbx89F_-Z4jn_RPFFWo
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2016-01-30 20:44:40

vault (datasafe):
Alias      : vault-1
Identifiant: lZILS1l6Km5aIGS6pA7P7azAJic
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2016-01-30 20:44:40

ca-signer (certsign):
Alias      : ca-signer-1
Identifiant: Sw_IY7AdoGUp28F_cFEhbtI9pE
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2018-01-29 20:44:40

=== root ca ===
current root ca:
Alias      : root-1
Identifiant: fVrqJAlpotPaisOAsnxa9cglXCc
NotBefore  : 2015-01-30 20:44:39
NotAfter   : 2020-01-30 20:44:39

upcoming root ca:
  not set
```

Démarrage d'OpenXPki

1 Exécutez la commande **openxpkictl start**.

Exemple d'impression

```
Starting OpenXPki...
OpenXPki Server is running and accepting requests.
DONE.
```

2 Pour accéder au serveur OpenXPki, procédez comme suit :

- a** Depuis un navigateur Web, saisissez **http://ipaddress/openxpki/**.
- b** Connectez-vous en tant qu'**opérateur**. Le mot de passe par défaut est **openxpki**.

Remarque : La connexion Opérateur a deux comptes opérateur préconfigurés, **raop** et **raop2**.

3 Créez une demande de certificat, puis testez-la.

Génération des informations CRL

Remarque : Si votre serveur est accessible à l'aide du FQDN, utilisez le DNS du serveur au lieu de son adresse IP.

1 Arrêtez le service OpenXPki à l'aide de **Openxpkictl stop**.

2 Dans **nano /etc/openxpki/config.d/realm/ca-one/publishing.yaml**, mettez à jour les éléments suivants de la section **connecteurs : cdp** :

```
class: Connector::Builtin::File::Path
LOCATION: /var/www/openxpki/CertEnroll/
```

```
file: "[% ARGS.0 %].crl"
content: "[% pem %]"
```

- a** Dans **nano /etc/openxpki/config.d/realm/ca-one/profile/default.yaml**, mettez à jour les éléments suivants :

- **crl_distribution_points** : Section


```
critical: 0
uri:
  - http://10.195.0.111/CertEnroll/[% ISSUER.CN.0 %].crl
  - ldap://localhost/[% ISSUER.DN %]
```
- **authority_info_access** : Section


```
critical: 0
ca_issuers: http://10.195.0.111/CertEnroll/MYOPENXPKI.crt
ocsp: http://ocsp.openxpki.org/
```

Modifiez l'adresse IP et le nom du certificat CA en fonction de votre serveur CA.

- b** Dans **nano /etc/openxpki/config.d/realm/ca-one/crl/default.yaml**, procédez comme suit :

- Si nécessaire, mettez à jour **nextupdate** et **renewal**.
- Ajoutez **ca_issuers** à la section suivante :


```
extensions:
  authority_info_access:
    critical: 0
    # ca_issuers and ocsp can be scalar or list
    ca_issuers: http://10.195.0.111/CertEnroll/MYOPENXPKI.crt
    #ocsp: http://ocsp.openxpki.org/
```

Modifiez l'adresse IP et le nom du certificat CA en fonction de votre serveur CA.

- 3** Démarrez le service OpenXPki à l'aide de **Openxpkictl start**.

Configuration de l'accessibilité CRL

- 1 Arrêtez le service Apache à l'aide de **service apache2 stop**.
- 2 Créez un répertoire **CertEnroll** pour crl dans le répertoire **/var/www/openxpki/**.
- 3 Définissez **openxpki** comme propriétaire de ce répertoire, puis configurez les autorisations pour permettre à Apache de lire et d'exécuter, et aux autres services de lire uniquement.

```
chown openxpki /var/www/openxpki/CertEnroll
```

```
chmod 755 /var/www/openxpki/CertEnroll
```

- 4 Ajoutez une référence au fichier de configuration alias.conf à l'aide de **nano /etc/apache2/mods-enabled/alias.conf**.

- 5 Après la section **<Directory "/usr/share/apache2/icons">**, ajoutez ce qui suit :

```
Alias /CertEnroll/ "/var/www/openxpki/CertEnroll/"
<Directory "/var/www/openxpki/CertEnroll">
  Options FollowSymlinks
  AllowOverride None
  Require all granted
</Directory>
```

- 6 Ajoutez une référence dans le fichier apache2.conf à l'aide de **nano /etc/apache2/apache2.conf**.

- 7 Ajoutez ce qui suit dans la section **Serveur HTTPD Apache2** :

```
<Directory /var/www/openxpki/CertEnroll>
  Options FollowSymlinks
```

```
    AllowOverride None
    Allow from all
</Directory>
```

8 Démarrez le service Apache à l'aide de **service apache2 start**.

Activation du service SCEP

1 Arrêtez le service OpenXPKI à l'aide de **openxpkictl stop**.

2 Installez le package openca-tools à l'aide de **aptitude install openca-tools**.

3 Démarrez le service OpenXPKI à l'aide de **openxpkictl start**.

Testez le service à l'aide de n'importe quel client, tel que certnanny avec SSCEP.

Remarque : SSCEP est un client de ligne de commande pour SCEP. Vous pouvez télécharger SSCEP depuis <https://github.com/cernnanny/sscep>.

Activation du certificat du signataire pour le compte de (agent d'inscription)

Pour les demandes de certificat automatiques, nous utilisons la fonction du certificat du signataire pour le compte de d'OpenXPKI.

1 Arrêtez le service OpenXPKI à l'aide de **openxpkictl stop**.

2 Dans **nano /etc/openxpki/config.d/realm/ca-one/scep/generic.yaml**, depuis la section **authorized_signer:**, ajoutez une règle pour le nom d'objet du certificat du signataire.

```
rule1:
    # Full DN
    subject: CN=Markvision_.*
```

Remarques :

- Dans cette règle, tout certificat CN commençant par **MarkVision_** est le certificat du signataire pour le compte de.
- Le nom de l'objet est défini dans MVE pour la génération du certificat du signataire pour le compte de.
- Vérifiez l'espace et l'indentation dans le fichier de script.
- Si le CN est modifié dans MVE, ajoutez le CN mis à jour dans OpenXPKI.
- Vous ne pouvez spécifier qu'un seul certificat en tant que signataire pour le compte de, puis spécifiez le CN complet.

3 Enregistrez le fichier.

4 Démarrez le service OpenXPKI à l'aide de **openxpkictl start**.

Activation de l'approbation automatique des demandes de certificat dans l'autorité de certification OpenXPKI

- 1 Arrêtez le service OpenXPKI à l'aide de **openxpkictl stop**.
- 2 Dans **nano /etc/openxpki/config.d/realm/ca-one/scep/generic.yaml**, mettez à jour les éléments **éligibles** : section :

Ancien contenu

```
eligible:
  initial:
    value@: connector:scep.generic.connector.initial
    args: "[% context.cert_subject_parts.CN.0 %]"
    expect:
      - Build
      - New
```

Nouveau contenu

```
eligible:
  initial:
    value: 1
    # value@: connector:scep.generic.connector.initial
    # args: "[% context.cert_subject_parts.CN.0 %]"
    # expect:
    #   - Build
    #   - New
```

Remarques :

- Vérifiez l'espace et l'indentation dans le fichier de script.
- Pour approuver les certificats manuellement, commentez la ligne **valeur : 1**, puis supprimez les commentaires des autres lignes commentées précédemment.

- 3 Enregistrez le fichier.
- 4 Démarrez le service OpenXPKI à l'aide de **openxpkictl start**.

Création d'un deuxième domaine

Dans OpenXPKI, vous pouvez configurer plusieurs structures PKI dans le même système. Les rubriques suivantes expliquent comment créer un autre domaine pour MVE nommé **ca-two**.

Copie et définition du répertoire

- 1 Copiez l'exemple d'arborescence **/etc/openxpki/config.d/realm/ca-one** dans un nouveau répertoire (**cp -avr /etc/openxpki/config.d/realm/ca-one /etc/openxpki/config.d/realm/ca-two**) dans le répertoire de domaine.
- 2 Dans **etc/openxpki/config.d/system/realms.yaml**, mettez à jour la section suivante :

Ancien contenu

```
# This is the list of realms in this PKI
# You only need to enable the realms which are visible on the server

ca-one:
  label: Verbose name of this realm
```

```
baseurl: https://pki.example.com/openxpi/

#ca-two:
#   label: Verbose name of this realm
#   baseurl: https://pki.acme.org/openxpi/
```

Nouveau contenu

```
# This is the list of realms in this PKI
# You only need to enable the realms which are visible on the server

ca-one:
  label: CA-ONE
  baseurl: https://pki.example.com/openxpi/

ca-two:
  label: CA-TWO
  baseurl: https://pki.example.com/openxpi/
```

3 Enregistrez le fichier.

Création de certificats

Les instructions suivantes indiquent comment générer le certificat du signataire, le certificat du coffre et le certificat SCEP. L'autorité de certification racine signe le certificat du signataire, puis le certificat du signataire signe le certificat SCEP. Le certificat du coffre est auto-signé.

- 1 Générez, puis signez les certificats. Pour plus d'informations, reportez-vous à la section « [Configuration manuelle de l'autorité de certification OpenXPKI](#) » à la page 87.

Remarque : Modifiez le nom commun du certificat afin que l'utilisateur puisse facilement distinguer les différents certificats des différents domaines. Vous pouvez remplacer **DC=CA-ONE** par **DC=CA-TWO**. Les fichiers de certificat sont créés dans le répertoire **/etc/certs/openxpi_ca-two/**.

- 2 Copiez les fichiers de clés dans **/etc/openxpi/ca/ca-two/**.

Remarque : Les fichiers de clés doivent être lisibles par OpenXPKI.

```
cp /etc/certs/openxpi_ca-two/ca-signer-1.key /etc/openxpi/ca/ca-two/
cp /etc/certs/openxpi_ca-two/vault-1.key /etc/openxpi/ca/ca-two/
cp /etc/certs/openxpi_ca-two/scep-1.key /etc/openxpi/ca/ca-two/
```

- 3 Créez le lien symbolique. Créez également un lien symbolique pour le certificat CA racine.

Remarque : Les liens symboliques sont des alias utilisés par la configuration par défaut.

```
ln -s /etc/openxpi/ca/ca-one/ca-root-1.crt /etc/openxpi/ca/ca-two/ca-root-1.crt
ln -s /etc/openxpi/ca/ca-two/ca-signer-1.key /etc/openxpi/ca/ca-two/ca-signer-1.pem
ln -s /etc/openxpi/ca/ca-two/scep-1.key /etc/openxpi/ca/ca-two/scep-1.pem
ln -s /etc/openxpi/ca/ca-two/vault-1.key /etc/openxpi/ca/ca-two/vault-1.pem
```

- 4 Importez le certificat du signataire, le certificat du coffre et le certificat SCEP dans la base de données avec les jetons appropriés pour **ca-two**.

```
openxpkiadm certificate import --file /etc/certs/openxpi_ca-two/ca-signer-1.crt --realm
ca-two --issuer /etc/openxpi/ca/ca-two/ca-one-1.crt --token certsign

openxpkiadm certificate import --file /etc/certs/openxpi_ca-two/scep-1.crt --realm ca-
two --token scep

openxpkiadm certificate import --file /etc/certs/openxpi_ca-two/vault-1.crt --realm ca-
two --token datasafe
```


5 Vérifiez si l'importation est réussie à l'aide de **openxpkiadm alias --realm ca-two**.

Exemple d'impression

```
=== functional token ===
scep (scep):
Alias      : scep-1
Identifiant: YsBNZ7JYTbx89F_-Z4jn_RPFFWo
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2016-01-30 20:44:40

vault (datasafe):
Alias      : vault-1
Identifiant: lZILS1l6Km5aIGS6pA7P7azAJic
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2016-01-30 20:44:40

ca-signer (certsign):
Alias      : ca-signer-1
Identifiant: Sw_IY7AdoGUp28F_cFEhbtI9pE
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2018-01-29 20:44:40

=== root ca ===
current root ca:
Alias      : root-1
Identifiant: fVrqJAlpotPaisOAsnxa9cglXcc
NotBefore  : 2015-01-30 20:44:39
NotAfter   : 2020-01-30 20:44:39

upcoming root ca:
not set
```

Dans ce cas, les informations de l'autorité de certification racine sont les mêmes pour **ca-one** et **ca-two**.

- 6** Si vous avez modifié le mot de passe de la clé de certificat lors de la création du certificat, alors mettez à jour **nano /etc/openxpki/config.d/realm/ca-two/crypto.yaml**.
- 7** Générez les CRL pour ce domaine. Pour plus d'informations, reportez-vous à la section [« Génération des informations CRL » à la page 92](#).
- 8** Publier les CRL pour ce domaine. Pour plus d'informations, reportez-vous à la section [« Configuration de l'accessibilité CRL » à la page 93](#).
- 9** Redémarrez le service OpenXPki à l'aide de **openxpkiectl restart**.

Exemple d'impression

```
Stopping OpenXPki
Stopping gracefully, 3 (sub)processes remaining...
DONE.
Starting OpenXPki...
OpenXPki Server is running and accepting requests.
DONE.
```

- 10** Pour accéder au serveur OpenXPki, procédez comme suit :

- a** Depuis un navigateur Web, saisissez **http://ipaddress/openxpki/**.
- b** Connectez-vous en tant qu'**opérateur**. Le mot de passe par défaut est **openxpki**.

Remarque : La connexion Opérateur a deux comptes opérateur préconfigurés, **raop** et **raop2**.

Configuration du point de terminaison SCEP pour plusieurs domaines

Le point de terminaison SCEP du domaine par défaut est **http://<ipaddress>/scep/scep**. Si vous disposez de plusieurs domaines, configurez un point de terminaison SCEP unique (fichier de configuration différent) pour chaque domaine. Dans les instructions suivantes, nous utilisons deux domaines PKI, **ca-one** et **ca-two**.

- 1 Copiez le fichier de configuration par défaut dans **cp /etc/openxpki/scep/default.conf /etc/openxpki/scep/ca-one.conf**.

Remarque : Nommez le fichier **ca-one.conf**.

- 2 Dans **penxpki/scep/ca-one.conf**, définissez la valeur du domaine sur **realm=ca-one**.

- 3 Créez un autre fichier de configuration dans **cp /etc/openxpki/scep/default.conf /etc/openxpki/scep/ca-two.conf**.

Remarque : Nommez le fichier **ca-two.conf**.

- 4 Dans **nano /etc/openxpki/scep/ca-two.conf**, définissez la valeur du domaine sur **realm=ca-two**.

- 5 Redémarrez le service OpenXPki à l'aide de **openxpkiectl restart**.

Les points de terminaison SCEP sont les suivants :

- **ca-one**—**http://ipaddress/scep/ca-one**
- **ca-two**—**http://ipaddress/scep/ca-two**

Si vous souhaitez faire la différence entre les informations d'identification de connexion et les modèles de certificat par défaut pour différents domaines PKI, vous aurez peut-être besoin d'une configuration avancée.

Définition du numéro de port par défaut pour l'autorité de certification OpenXPki

Par défaut, Apache écoute dans le numéro de port 80. Définissez le numéro de port par défaut de l'autorité de certification OpenXPki pour éviter les conflits.

- 1 Dans **/etc/apache2/ports.conf**, ajoutez ou modifiez un port. Par exemple, **Ecouter 8080**.
- 2 Dans **/etc/apache2/sites-enabled/000-default.conf**, ajoutez ou modifiez la section **VirtualHost** pour mapper le nouveau port. Par exemple, **<VirtualHost *:8080>**.
- 3 Redémarrez le serveur Apache à l'aide de **systemctl restart apache2**.

Pour vérifier l'état, exécutez **netstat -tlnp | grep apache**. L'URL SCEP OpenXPki est désormais **http://ipaddress:8080/scep/ca-one**, et l'URL Web est **http://ip address:8080/openxpki**.

Désactivation de Mot de passe de challenge sur l'autorité de certification OpenXPki

Par défaut, OpenXPki accepte les demandes sans vérifier le mot de passe de challenge. La demande de certificat n'est pas rejetée et l'administrateur de l'autorité de certification et l'autorité de certification déterminent s'il faut approuver ou rejeter la demande. Pour éviter tout problème de sécurité potentiel, désactivez cette fonction afin que toute demande de certificat contenant des mots de passe non valides soit immédiatement rejetée. Dans MVE, Mot de passe de challenge est requis uniquement lors de la génération du certificat d'agent d'inscription.

- 1 Dans **/etc/openxpki/config.d/realm/REALM NAME/scep/generic.yaml**, à partir de la section **Politique**, remplacez la valeur **1** de **allow_man_authen** par **0**.

Remarques :

- REALM NAME est le nom du domaine. Par exemple, **ca-one**.
- Vérifiez l'espace et l'indentation dans le fichier de script.

- 2 Redémarrez le service OpenXPki à l'aide de **openxpkictl restart**.

Ajout de l'EKU d'authentification client dans les certificats

- 1 Dans **/etc/openxpki/config.d/realm/REALM NAME/profile/I18N_OPENXPki_PROFILE_TLS_SERVER.yaml**, depuis la section **extended_key_usage**, remplacez la valeur **client_auth** par **1**.

Remarques :

- REALM NAME est le nom du domaine. Par exemple, **ca-one**.
- Vérifiez l'espace et l'indentation dans le fichier de script.

- 2 Redémarrez le service OpenXPki à l'aide de **openxpkictl restart**.

obtention de l'objet de certificat complet lors d'une demande via SCEP

Par défaut, OpenXPki lit uniquement le CN de l'objet du certificat demandeur. Les autres informations, telles que le pays, la localité et DC, sont codées en dur. Par exemple, si un objet de certificat est **C=US, ST=KY, L=Lexington, O=Lexmark, OU=ISS, CN=ET0021B7C34AEC.dhcp.dev.lexmark.com**, alors après avoir signé le certificat via SCEP, le sujet est remplacé par **DC=Test Deployment, DC= OpenXPki, CN=ET0021B7C34AEC.dhcp.dev.lexmark.com**.

Remarque : REALM NAME est le nom du domaine. Par exemple, **ca-one**.

- 1 Dans **/etc/openxpki/config.d/realm/REALM NAME/profile/I18N_OPENXPki_PROFILE_TLS_SERVER.yaml**, dans la section **Inscrire**, modifiez la valeur **dn** comme suit :

```
CN=[% CN.0 %][% IF OU %][% FOREACH entry = OU %],OU=[% entry %][% END %][% END %][% IF O
%][% FOREACH entry = O %],O=[% entry %][% END %][% END %][% IF L %],L=[% L.0 %][% END %]
[% IF ST %],ST=[% ST.0 %][% END %][% IF C %],C=[% C.0 %][% END %][% IF DC %][% FOREACH
entry = DC %],DC=[% entry %][% END %][% END %][% IF EMAIL %][% FOREACH entry = EMAIL
%],EMAIL=[% entry %][% END %][% END %]
```

- 2 Enregistrez le fichier.

3 Créez un fichier intitulé **l.yaml** dans le répertoire **/etc/openxpki/config.d/realm/REALM NAME/profile/template**.

4 Ajoutez ce qui suit :

```
id: L
label: L
description: I18N_OPENXPki_UI_PROFILE_L_DESC
preset: L
type: freetext
width: 60
placeholder: Kolkata
```

5 Enregistrez le fichier.

6 Créez un fichier intitulé **st.yaml** dans le répertoire **/etc/openxpki/config.d/realm/REALM NAME/profile/template**.

7 Ajoutez ce qui suit :

```
id: ST
label: ST
description: I18N_OPENXPki_UI_PROFILE_ST_DESC
preset: ST
type: freetext
width: 60
placeholder: WB
```

8 Enregistrez le fichier.

Remarque : OpenXPki doit posséder les deux fichiers et être lisible, inscriptible et exécutable.

9 Redémarrez le service OpenXPki à l'aide de **openxpkictl restart**.

Révocation des certificats et configuration de l'accessibilité CRL

1 Accédez au serveur OpenXPki.

a Depuis un navigateur Web, saisissez **http://ipaddress/openxpki/**.

b Connectez-vous en tant qu'**opérateur**. Le mot de passe par défaut est **openxpki**.

Remarque : La connexion Opérateur a deux comptes opérateur préconfigurés, **raop** et **raop2**.

2 Cliquez sur **Recherche de flux > Rechercher maintenant**.

3 Cliquez sur un certificat à révoquer, puis cliquez sur le lien du certificat.

4 Dans la section Action, cliquez sur **demande de révocation**.

5 Saisissez les valeurs appropriées, puis cliquez sur **Continuer > Envoyer la demande**.

6 Sur la page suivante, approuvez la demande. La révocation du certificat attend la prochaine publication de CRL.

7 Dans la section Fonctionnement PKI, cliquez sur **Emettre une liste de révocation de certificat (CRL)**.

8 Cliquez sur **Appliquer la création de listes de révocation > Continuer**.

9 Dans la section Fonctionnement PKI, cliquez sur **Publier CA/CRL**.

10 Cliquez sur **Recherche de flux > Rechercher maintenant**.

11 Cliquez sur le certificat révoqué de type **certificate_revocation_request_v2**.

12 Cliquez sur **Forcer la réactivation**.

Dans le nouveau CRL, vous trouverez le numéro de série et le motif de révocation du certificat révoqué.

Gestion des alertes d'imprimante

Aperçu

Les alertes se déclenchent lorsqu'une imprimante nécessite une intervention. Les actions vous permettent d'envoyer des courriers électroniques personnalisés ou d'exécuter des scripts lorsqu'une alerte est déclenchée. Les événements définissent les actions qui s'exécutent lorsque des alertes spécifiques sont actives. Pour recevoir les alertes d'une imprimante, créez des actions, puis associez-les à un événement. Attribuez l'événement aux imprimantes que vous voulez surveiller.

Remarque : Cette fonction n'est pas applicable aux imprimantes sécurisées.

Création d'une action

Une action est un courrier électronique de notification ou un journal d'affichage d'événements. Les actions attribuées à des événements sont déclenchées en cas d'alerte.

- 1 Dans le menu Imprimantes, cliquez sur **Événements et actions** > **Actions** > **Créer**.
- 2 Saisissez un nom unique pour l'action, ainsi que sa description.
- 3 Sélectionnez un type d'action.

E-mail

Remarque : Avant de commencer, vérifiez que les paramètres de courrier électronique sont configurés. Pour plus d'informations, reportez-vous à la section « [Configuration des paramètres de courrier électronique](#) » à la page 114.

- a Dans le menu Type, sélectionnez **E-mail**.
- b Entrez les valeurs appropriées dans les champs. Vous pouvez également utiliser les espaces réservés disponibles pour l'ensemble ou une partie de l'objet du message ou pour une partie du corps du courrier électronique. Pour plus d'informations, reportez-vous à la section « [Compréhension des espaces réservés d'action](#) » à la page 103.

Type

E-mail ▼

From (Optional)

admin@mycompany.com

To

scott.summers@mycompany.com

CC (Optional)

Subject (Optional)

alert.type ▼

Body

alert.name ▼

Create Action Cancel

c Cliquez sur **Créer une action**.

Événement du journal

a Dans le menu Type, sélectionnez **Événement du journal**.

b Saisissez les paramètres de l'événement. Vous pouvez également utiliser les espaces réservés disponibles dans le menu déroulant. Pour plus d'informations, reportez-vous à la section « [Compréhension des espaces réservés d'action](#) » à la page 103.

General

Name

New Action - 2019-12-09T14:08:02+08:00

Description (Optional)

Type

Log event

Event parameters (Optional)

`${alert.type}`

Maximum length for field is 255

Create Action Cancel

About

- alert.type
- alert.location
- alert.state
- alert.name
- configurationItem.manufacturer
- configurationItem.contactName

c Cliquez sur **Créer une action**.

Compréhension des espaces réservés d'action

Utilisez les espaces réservés disponibles dans l'objet ou le corps du courrier électronique. Les espaces réservés représentent des éléments variables qui sont remplacés par des valeurs réelles lorsqu'ils sont utilisés.

- **`${eventHandler.timestamp}`** : date et heure de traitement de l'événement par MVE. Par exemple, **14 mars 2017 1 :42:24**.
- **`${eventHandler.name}`** : nom de l'événement.
- **`${configurationItem.name}`** : nom du système de l'imprimante ayant déclenché l'alerte.
- **`${configurationItem.address}`** : adresse MAC de l'imprimante ayant déclenché l'alerte.
- **`${configurationItem.ipAddress}`** : adresse IP de l'imprimante ayant déclenché l'alerte.
- **`${configurationItem.ipHostname}`** : nom d'hôte de l'imprimante ayant déclenché l'alerte.
- **`${configurationItem.model}`** : nom du modèle de l'imprimante ayant déclenché l'alerte.
- **`${configurationItem.serialNumber}`** : numéro de série de l'imprimante ayant déclenché l'alerte.
- **`${configurationItem.propertyTag}`** : identifiant de l'imprimante ayant déclenché l'alerte.
- **`${configurationItem.contactName}`** : nom du contact de l'imprimante ayant déclenché l'alerte.
- **`${configurationItem.contactLocation}`** : emplacement du contact de l'imprimante ayant déclenché l'alerte.
- **`${configurationItem.manufacturer}`** : fabricant de l'imprimante ayant déclenché l'alerte.
- **`${alert.name}`** : nom de l'alerte déclenchée.
- **`${alert.state}`** : état de l'alerte. Elle peut être active ou effacée.

- **\${alert.location}** : emplacement au sein de l'imprimante qui a déclenché l'alerte.
- **\${alert.type}** : gravité de l'alerte déclenchée, par exemple **Avertissement** ou **Intervention requise**.

Gestion des actions

- 1 Dans le menu Imprimantes, cliquez sur **Événements et actions** > **Actions**.
- 2 Effectuez l'une des opérations suivantes :

Modifier une action

- a Sélectionnez une action, puis cliquez sur **Modifier**.
- b Configurez les paramètres.
- c Cliquez sur **Enregistrer les modifications**.

Supprimer des actions

- a Sélectionnez une ou plusieurs actions.
- b Cliquez sur **Supprimer**, puis confirmez la suppression.

Tester une action

- a Sélectionnez une action, puis cliquez sur **Tester**.
- b Pour vérifier les résultats du test, consultez les journaux des tâches.

Remarques :

- Pour plus d'informations, reportez-vous à la section « [Affichage des journaux](#) » à la page 110.
- Si vous testez une action E-mail, vérifiez si le courrier électronique a été envoyé au destinataire.

Création d'un événement

Vous pouvez contrôler les alertes dans votre parc d'impression. Créez un événement, puis définissez une action à exécuter lorsque certaines alertes sont déclenchées. Les événements ne sont pas pris en charge sur les imprimantes sécurisées.

- 1 Dans le menu Imprimantes, cliquez sur **Événements et actions** > **Événements** > **Créer**.
- 2 Saisissez un nom unique pour l'événement, ainsi que sa description.
- 3 Sélectionnez une ou plusieurs alertes dans la section Alertes. Pour plus d'informations, reportez-vous à la section « [Présentation des alertes d'imprimante](#) » à la page 105.
- 4 Dans la section Actions, sélectionnez une ou plusieurs actions à exécuter lorsque les alertes sélectionnées sont actives.

Remarque : Pour plus d'informations, reportez-vous à la section « [Création d'une action](#) » à la page 102.

- 5 Activez le système pour exécuter les actions sélectionnées lorsque les alertes sont effacées de l'imprimante.
- 6 Définissez un délai de grâce avant d'exécuter les actions sélectionnées.

Remarque : si l'alerte est effacée au cours du délai de grâce, l'action n'est pas exécutée.

- 7 Cliquez sur **Créer un événement**.

Présentation des alertes d'imprimante

Les alertes se déclenchent lorsqu'une imprimante nécessite une intervention. Les alertes suivantes peuvent être associées à un événement dans MVE :

- **Bourrage papier dans le dispositif d'alimentation automatique de documents (DAA)** : du papier est coincé dans le DAA et doit être retiré manuellement.
 - Bourrage à la sortie du scanner DAA
 - Bourrage dans le chargeur du scanner DAA
 - Bourrage du convertisseur du scanner DAA
 - Elimination du bourrage du scanner DAA
 - Papier manquant dans le scanner DAA
 - Bourrage lors du pré-repérage du scanner DAA
 - Bourrage lors du repérage du scanner DAA
 - Alerte scanner - Remplacer tous les originaux pour relancer le travail
- **Porte ou capot ouvert** : une porte de l'imprimante est ouverte et doit être fermée.
 - Vérifier la porte/le capot - Boîte à lettres
 - Porte ouverte
 - Alerte de capot
 - Capot fermé
 - Capot ouvert
 - Capot ouvert ou cartouche manquante
 - Volet recto verso ouvert
 - Capot du scanner DDA ouvert
 - Capot d'accès aux bourrages du scanner ouvert
- **Format ou type de support incorrect** : un travail est en cours d'impression et nécessite le chargement d'un certain type ou format de papier dans un bac.
 - Format d'enveloppe incorrect
 - Alimentation manuelle incorrecte
 - Support incorrect
 - Format de support incorrect
 - Charger le support
- **Mémoire saturée ou erreur** : la mémoire de l'imprimante est faible, des modifications doivent être appliquées.
 - Page complexe
 - Les fichiers seront supprimés.
 - Mémoire assemblage insuffisante
 - Mémoire défragmentation insuffisante
 - Mémoire télécopie insuffisante
 - Mémoire insuffisante
 - Mémoire insuffisante - Certains travaux suspendus pourraient être perdus
 - Mémoire insuffisante pour économiser les ressources
 - Mémoire saturée

- Mémoire PS insuffisante
- Pages trop nombreuses -Numérisation annulée
- Réduction de la résolution
- **Dysfonctionnement d'une option** : l'état d'une option de l'imprimante indique une erreur. Les options englobent les options d'entrée, les options de sortie, les cartes de police, les cartes flash utilisateur, les disques durs et les unités de finition.
 - Vérifier l'alignement/la connexion
 - Vérifier la connexion recto verso
 - Vérifier l'installation de l'unité de finition/la boîte à lettres
 - Vérifier l'alimentation
 - Option corrompue
 - Option défectueuse
 - Débranchez le périphérique
 - Alerte recto/verso
 - Tiroir recto verso manquant
 - Perte de l'adaptateur de réseau externe
 - Alerte de l'unité de finition
 - Volet de l'unité de finition ouvert/système de blocage ouvert
 - Plaque à papier de l'unité de finition ouverte
 - Périphérique recto verso incompatible
 - Périphérique d'entrée incompatible
 - Périphérique de sortie incompatible
 - Périphérique inconnu incompatible
 - Installation d'option incorrecte
 - Alerte d'entrée
 - Erreur de configuration entrée
 - Option Alerte
 - Réceptacle plein
 - Niveau maximum du réceptacle bientôt atteint
 - Erreur de configuration de sortie
 - Option Plein
 - Option Manquant
 - Mécanisme d'alimentation papier manquant
 - Imprimer les travaux sous conditions
 - Rebranchez le périphérique
 - Rebranchez le périphérique de sortie
 - Trop de périphériques d'entrée installés
 - Trop d'options installées
 - Trop de périphériques de sortie installés
 - Tiroir manquant
 - Tiroir manquant pendant la mise sous tension

- Erreur de détection du tiroir
- Entrée non étalonnée
- Option non formatée
- Option non prise en charge
- Rebranchez le périphérique d'entrée
- **Bourrage papier** : du papier est coincé dans l'imprimante et doit être retiré manuellement.
 - Bourrage papier interne
 - Alerte bourrage
 - Bourrage papier
- **Erreur de scanner** : le scanner a rencontré un problème.
 - Câble débranché à l'arrière du scanner.
 - Transport du scanner verrouillé
 - Nettoyer la vitre du scanner à plat/la bande de support
 - Scanner désactivé
 - Scanner à plat ouvert
 - Câble débranché à l'avant du scanner
 - Repérage du scanner non valide
- **Erreur de fournitures** : une fourniture de l'imprimante indique une erreur.
 - Fourniture anormale
 - Erreur de zone cartouche
 - Fourniture défectueuse
 - Unité de fusion ou rouleau antiadhérent manquant(e)
 - Cartouche de gauche non valide ou manquante
 - Cartouche de droite non valide ou manquante
 - Fourniture non valide
 - Echec de l'initialisation
 - Alerte alimentation
 - Bourrage fournitures
 - Fourniture manquante
 - Poignée d'éjection de la cartouche de toner tirée
 - Cartouche de toner mal installée
 - Fourniture non étalonnée
 - Fourniture sans licence
 - Fourniture non prise en charge
- **Fournitures ou consommable vides** : une fourniture de l'imprimante doit être remplacée.
 - Entrée vide
 - Durée de vie épuisée
 - Imprimante prête pour maintenance
 - Maintenance prévue
 - Bourrage de la fourniture

- Fourniture pleine
- Fourniture pleine ou manquante

Remarque : L'alerte envoyée par l'imprimante est de type erreur et avertissement. Si l'une de ces alertes est déclenchée, son action associée s'effectue deux fois.

- **Fournitures ou consommable faible :** le niveau d'une fourniture de l'imprimante est faible.

- 1er avertissement
- Niveau premier bas
- Niveau de l'entrée bas
- Fin durée vie
- Presque vide
- Presque bas
- Niveau de fourniture bas
- Fourniture presque pleine

- **Alerte ou condition non catégorisée**

- Echec de l'étalonnage des couleurs
- Erreur de transmission de données
- Echec CRC moteur
- Alerte externe
- Perte de la connexion au télécopieur
- Ventilateur en panne
- Hex actif
- Insérez la page recto verso et cliquez sur Reprise
- Alerte interne
- L'adaptateur de réseau interne doit être révisé
- Alerte de l'unité logique
- Hors ligne
- Hors ligne pour le message d'avertissement
- Echec de l'opération
- Alerte d'intervention de l'opérateur
- Erreur page
- Alerte du port
- Echec de la communication avec le port
- Port désactivé
- Economie énergie
- Mise hors tension
- Délai exécution PS
- Délai manuel PS
- Configuration requise
- Erreur de somme de contrôle SIMM
- Etalonnage de la fourniture
- Echec du sondage du toner

- Cause d'alerte inconnue
- Configuration inconnue
- Cause d'alerte du scanner inconnue
- Utilisateurs bloqués
- Avertissement

Gestion des événements

1 Dans le menu Imprimantes, cliquez sur **Événements et actions > Événements**.

2 Effectuez l'une des opérations suivantes :

Modifier un événement

- a** Sélectionnez un événement, puis cliquez **Modifier**.
- b** Configurez les paramètres.
- c** Cliquez sur **Enregistrer les modifications**.

Supprimer les événements

- a** Sélectionnez un ou plusieurs événements.
- b** Cliquez sur **Supprimer**, puis confirmez la suppression.

Affichage de l'état et de l'historique d'une tâche

Aperçu

Une tâche est une activité de gestion d'imprimante effectuée dans MVE, par exemple la détection d'imprimante, un audit ou la mise en œuvre de configurations. La page Etat indique l'état de toutes les tâches en cours et des tâches exécutées au cours des dernières 72 heures. Les informations relatives aux tâches en cours sont consignées dans le journal. Les tâches de plus de 72 heures peuvent uniquement être consultées sur la page Journal sous forme d'entrées de journal individuelles. Il est possible de les rechercher au moyen de leurs ID de tâche.

Affichage de l'état de la tâche

Cliquez sur **Etat** dans le menu Tâches.

Remarque : l'état de la tâche est mis à jour en temps réel.

Arrêt des tâches

- 1 Cliquez sur **Etat** dans le menu Tâches.
- 2 Dans la section Tâches en cours, sélectionnez une ou plusieurs tâches.
- 3 Cliquez sur **Arrêter**.

Affichage des journaux

- 1 Cliquez sur **Journaux** dans le menu Tâches.
- 2 Sélectionnez des catégories de tâches, des types de tâche ou une période.

Remarques :

- Utilisez le champ de recherche pour rechercher plusieurs ID de tâche. Utilisez des virgules pour séparer plusieurs ID de tâche ou un tiret pour indiquer une plage. Par exemple : **11, 23, 30-35**.
- Pour exporter les résultats de recherche, cliquez sur **Exporter au format CSV**.

Effacement des journaux

- 1 Cliquez sur **Journaux** dans le menu Tâches.
- 2 Cliquez sur **Effacer le journal**, puis sélectionnez une date.
- 3 Cliquez sur **Effacer le journal**.

Exporter les journaux

- 1 Dans le menu Tâches, cliquez sur **Journal**.
- 2 Sélectionnez des catégories de tâches, des types de tâche ou une période.
- 3 Cliquez sur **Exporter vers CSV**.

Planification de tâches

Création d'une programmation

- 1 Dans le menu Tâches, cliquez sur **Planifier > Créer**.
- 2 Dans la section Général, saisissez un nom unique pour les tâches planifiées ainsi que leurs descriptions.
- 3 Dans la section Tâches, effectuez l'une des actions suivantes :

Programmer un audit

- a Sélectionnez **Audit**.
- b Sélectionnez une recherche enregistrée.

Programmer un contrôle de conformité

- a Sélectionnez **Conformité**.
- b Sélectionnez une recherche enregistrée.

Programmer une vérification d'état de l'imprimante

- a Sélectionnez **Etat actuel**.
- b Sélectionnez une recherche enregistrée.
- c Sélectionnez une action.

Programmer un déploiement de configuration

- a Sélectionnez **Déployer un fichier**.
- b Sélectionnez une recherche enregistrée.
- c Accédez au fichier, puis sélectionnez son type.
- d Si nécessaire, sélectionnez une méthode ou un protocole de déploiement.

Programmer une recherche

- a Sélectionnez **Détection**.
- b Sélectionnez un profil de recherche.

Programmer la mise en œuvre d'une configuration

- a Sélectionnez **Mise en œuvre**.
- b Sélectionnez une recherche enregistrée.

Planifier une validation de certificat

Sélectionnez **Valider le certificat**.

Remarque : Pendant la validation, MVE communique avec le serveur CA pour télécharger la chaîne de certificats et la liste de révocation de certificats (CRL). Le certificat de l'agent d'inscription est également généré. Ce certificat permet au serveur CA d'approuver MVE.

Programmer l'exportation d'un affichage

- a Sélectionnez **Exportation d'un affichage**.
 - b Sélectionnez une recherche enregistrée.
 - c Sélectionnez un modèle d'affichage.
 - d Saisissez la liste des adresses e-mail auxquelles les fichiers exportés sont envoyés.
- 4 Dans la section Planifier, réglez la date, l'heure et la fréquence de la tâche.
- 5 Cliquez sur **Créer une tâche planifiée**.

Gestion des tâches planifiées

- 1 Dans le menu Tâches, cliquez sur **Planifier**.
- 2 Effectuez l'une des opérations suivantes :

Modifier une tâche planifiée

- a Sélectionnez une tâche, puis cliquez sur **Modifier**.
- b Configurez les paramètres.
- c Cliquez sur **Modifier la tâche planifiée**.

Remarque : Les informations de la dernière exécution sont retirées lorsqu'une tâche planifiée est modifiée.

Supprimer une tâche planifiée

- a Sélectionnez une tâche, puis cliquez sur **Supprimer**.
- b Cliquez sur **Supprimer la tâche planifiée**.

Autres tâches administratives

Configuration des paramètres généraux

- 1 Dans le coin supérieur droit de la page, cliquez sur .
- 2 Cliquez sur **Général**, puis sélectionnez une source de nom d'hôte.
 - **Imprimante** : le système utilise le nom d'hôte de l'imprimante.
 - **Recherche DNS inverse** : le système récupère le nom d'hôte dans la table DNS à l'aide de l'adresse IP.
- 3 Définissez la fréquence d'interrogation des alertes.

Remarque : Il est possible que les imprimantes perdent l'état d'interrogation d'alertes en cas de modifications (par exemple, redémarrage ou mise à jour du micrologiciel). MVE tente de récupérer l'état automatiquement lors du prochain intervalle défini dans la fréquence d'interrogation.
- 4 Cliquez sur **Enregistrer les modifications**.

Configuration des paramètres de courrier électronique

La configuration SMTP doit être activée pour que MVE puisse envoyer des fichiers d'exportation de données et des notifications d'événements par courrier électronique.

- 1 Dans le coin supérieur droit de la page, cliquez sur .
- 2 Cliquez sur **E-mail**, puis sélectionnez **Activer la configuration SMTP de l'e-mail**.
- 3 Saisissez le serveur de messagerie SMTP et le port.
- 4 Saisissez l'adresse électronique de l'expéditeur.
- 5 Si un utilisateur doit se connecter pour pouvoir envoyer un courrier électronique, sélectionnez **Connexion requise** et saisissez les informations d'authentification de l'utilisateur.
- 6 Cliquez sur **Enregistrer les modifications**.

Ajout d'un avertissement de connexion

Il est possible de configurer un avertissement de connexion qui s'affiche lorsque les utilisateurs se connectent en ouvrant une nouvelle session. Les utilisateurs doivent accepter l'avertissement avant de pouvoir accéder à MVE.

- 1 Dans le coin supérieur droit de la page, cliquez sur .
- 2 Cliquez sur **Avertissement**, puis sélectionnez **Activer l'avertissement de connexion**.
- 3 Saisissez le texte de l'avertissement.
- 4 Cliquez sur **Enregistrer les modifications**.

Signature du certificat MVE

Le protocole SSL (Secure Socket Layer) ou TLS (Transport Layer Security) est un protocole de sécurité utilisant le chiffrement des données et l'authentification par certificat pour protéger la communication entre le serveur et le client. Dans MVE, TLS est utilisé pour protéger les informations sensibles partagées entre le serveur MVE et le navigateur Web. Les informations protégées peuvent être des mots de passe d'imprimante, des stratégies de sécurité, des informations d'identification d'utilisateur MVE ou des informations d'authentification d'imprimante, comme LDAP ou Kerberos.

TLS permet au serveur MVE et au navigateur Web de chiffrer ces données avant de les envoyer et de les déchiffrer une fois reçues. SSL permet également au serveur de présenter un certificat au navigateur Web qui prouve que le serveur est bien celui qu'il prétend être. Ce certificat est auto-signé ou bien signé par le biais d'une autorité de certification tierce approuvée. Par défaut, MVE est configuré pour utiliser un certificat auto-signé.

1 Télécharger la demande de signature de certificat d'imprimante.

- a** Dans le coin supérieur droit de la page, cliquez sur .
- b** Cliquez sur **TLS > Télécharger**.
- c** Sélectionnez **Demande de signature du certificat**.

Remarque : La demande de signature du certificat inclut d'autres noms du sujet (SAN).

2 Utilisez une autorité de certification approuvée pour signer la demande de signature du certificat.

3 Installer le certificat signé par une autorité de certification.

- a** Dans le coin supérieur droit de la page, cliquez sur .
- b** Cliquez sur **TLS > Installer le certificat signé**.
- c** Téléchargez le certificat signé par une autorité de certification, puis cliquez sur **Installer le certificat**.
- d** Cliquez sur **Redémarrer le service MVE**.

Remarque : Le redémarrage du service MVE relance le système, ce qui peut rendre le serveur indisponible pendant quelques minutes. Avant de redémarrer le service, assurez-vous qu'aucune tâche n'est en cours.

Suppression des références et des informations utilisateur

MVE est conforme aux règles de protection des données du Règlement général sur la protection des données. MVE peut être configuré pour appliquer le droit à l'oubli et supprimer les informations utilisateur privées du système.

Suppression d'utilisateurs

- 1** Dans le coin supérieur droit de la page, cliquez sur .
- 2** Cliquez sur **Utilisateur**, puis sélectionnez un ou plusieurs utilisateurs.
- 3** Cliquez sur **Supprimer > Supprimer des utilisateurs**.

Suppression des références utilisateur dans LDAP

- 1 Dans le coin supérieur droit de la page, cliquez sur .
- 2 Cliquez sur **LDAP**.
- 3 Supprimez les informations relatives à l'utilisateur dans les filtres de recherche et les paramètres de liaison.

Suppression des références utilisateur dans le serveur de messagerie

- 1 Dans le coin supérieur droit de la page, cliquez sur .
- 2 Cliquez sur **Courrier électronique**.
- 3 Supprimez les informations relatives à l'utilisateur, comme les informations d'identification d'utilisateur utilisées pour l'authentification avec le serveur de messagerie.

Suppression des références utilisateur dans les journaux des tâches

Pour plus d'informations, reportez-vous à la section [« Effacement des journaux » à la page 110](#).

Suppression des références utilisateur dans une configuration

- 1 Dans le menu Configurations, cliquez sur **Toutes les configurations**.
- 2 Cliquez sur le nom de la configuration.
- 3 Dans l'onglet Base, supprimez toutes les valeurs associées à l'utilisateur des paramètres de l'imprimante, comme le nom du contact et l'emplacement du contact.

Suppression des références utilisateur dans un composant de sécurité avancée

- 1 Dans le menu Configurations, cliquez sur **Tous les composants de sécurité avancée**.
- 2 Cliquez sur le nom du composant.
- 3 Dans la section Paramètres de sécurité avancée, supprimez toutes les valeurs associées à l'utilisateur.

Suppression des références utilisateur dans les recherches enregistrées

- 1 Dans le menu Imprimantes, cliquez sur **Recherches enregistrées**.
- 2 Cliquez sur une recherche enregistrée.
- 3 Supprimez toutes les règles de recherche utilisant les valeurs liées à l'utilisateur, comme le nom et l'emplacement du contact.

Suppression des références utilisateur dans les mots clés

- 1 Dans le menu Imprimantes, cliquez sur **Listes des imprimantes**.
- 2 Supprimez l'attribution de mots clés liés à l'utilisateur dans les imprimantes.
- 3 Dans le menu Imprimantes, cliquez sur **Mots clés**.
- 4 Supprimez tous les mots clés utilisant des informations relatives à l'utilisateur.

Suppression des références utilisateur dans les événements et les actions

- 1** Dans le menu Imprimantes, cliquez sur **Événements et actions**.
- 2** Supprimez toutes les actions contenant des références de courrier électronique d'utilisateurs.

Questions fréquemment posées

FAQ Markvision Enterprise

Je ne peux pas sélectionner plusieurs imprimantes dans la liste des modèles pris en charge lorsque je crée une configuration. Pourquoi ?

Les paramètres de configuration et les commandes varient selon les modèles d'imprimantes.

Mes recherches enregistrées sont-elles accessibles par d'autres utilisateurs ?

Oui. Tous les utilisateurs peuvent accéder aux recherches enregistrées.

Où puis-je trouver les fichiers journaux ?

Vous trouverez les fichiers journaux d'installation dans le répertoire caché du MVE d'installation de l'utilisateur. Par exemple, `C:\Users\Administrator\AppData\Local\Temp\mveLexmark-install.log`.

Les fichiers journaux d'application *.log se trouvent dans le dossier `installation_dir\Lexmark\Markvision Enterprise\tomcat\logs`, où `installation_dir` est le dossier d'installation de MVE.

Quelle est la différence entre la résolution DNS inverse et du nom de l'hôte ?

Le nom de l'hôte est un nom unique attribué à une imprimante d'un réseau. Chaque nom d'hôte correspond à une adresse IP. La résolution DNS inverse permet de déterminer le nom de l'hôte et le nom de domaine désigné d'une adresse IP déterminée.

Où trouver la résolution DNS inverse dans MVE ?

Vous pouvez trouver la résolution DNS inverse dans les paramètres généraux. Pour plus d'informations, reportez-vous à la section « [Configuration des paramètres généraux](#) » à la page 114.

Comment puis-je ajouter manuellement des règles au pare-feu Windows ?

Exécutez l'invite de commande en tant qu'administrateur, puis saisissez les commandes suivantes :

```
firewall add allowedprogram
"installation_dir/Lexmark/Markvision Enterprise/tomcat/bin/tomcat9.exe"
"MarkVision Enterprise Tomcat"
firewall add portopening UDP 9187 "MarkVision Enterprise NPA UDP"
firewall add portopening UDP 6100 "MarkVision Enterprise LST UDP"
```

Où `installation_dir` représente le dossier d'installation de MVE.

Comment puis-je configurer MVE pour utiliser un autre port que le 443 ?

- 1 Arrêtez le service Markvision Enterprise.
 - a Ouvrez la boîte de dialogue Exécuter, puis saisissez **services.msc**.
 - b Cliquez avec le bouton droit de la souris sur **Markvision Enterprise**, puis cliquez sur **Arrêter**.
- 2 Ouvrez le fichier **installation_dir\Lexmark\Markvision Enterprise\tomcat\conf\server.xml**.

Où **installation_dir** représente le dossier d'installation de MVE.

- 3 Remplacez la valeur **Port du connecteur** par un autre port inutilisé.

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
sslImplementationName="org.apache.tomcat.util.net.jsse.JSSEImplementation"
SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
compression="on" compressableMimeType="text/html,text/xml,text/plain,text/css,
text/javascript,application/javascript,application/json" maxThreads="150"
maxHttpHeaderSize="16384" minSpareThreads="25" enableLookups="false"
acceptCount="100" connectionTimeout="120000" disableUploadTimeout="true"
URIEncoding="UTF-8" server="Apache" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
sslProtocol="TLS" keystoreFile="C:/Program Files/Lexmark/Markvision Enterprise/
../mve_truststore.p12" keystorePass="markvision" keyAlias="mve" keyPass="markvision"
keystoreType="PKCS12" ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA"/>
```

- 4 Remplacez la valeur **redirectPort** par le même numéro de port que celui utilisé en tant que port du connecteur.

```
<Connector port="9788" maxHttpHeaderSize="16384" maxThreads="150" minSpareThreads="25"
enableLookups="false" redirectPort="443" acceptCount="100" connectionTimeout="120000"
disableUploadTimeout="true" compression="on" compressableMimeType="text/html,text/xml,
text/plain,text/css,text/javascript,application/javascript,application/json"
URIEncoding="UTF-8" server="Apache"/>
```

- 5 Redémarrez le service Markvision Enterprise.
 - a Ouvrez la boîte de dialogue Exécuter, puis saisissez **services.msc**.
 - b Cliquez avec le bouton droit de la souris sur **Markvision Enterprise**, puis cliquez sur **Redémarrer**.
- 6 Accédez à MVE à l'aide du nouveau port.

Par exemple, ouvrez un navigateur, puis saisissez **https://MVE_SERVER:port/mve**.

Où **MVE_SERVER** est le nom de l'hôte ou l'adresse IP du serveur hébergeant MVE, et où **port** est le numéro du port de connecteur.

Comment puis-je personnaliser les chiffrements et les versions TLS utilisés par MVE ?

- 1 Arrêtez le service Markvision Enterprise.
 - a Ouvrez la boîte de dialogue Exécuter, puis saisissez **services.msc**.
 - b Cliquez avec le bouton droit de la souris sur **Markvision Enterprise**, puis cliquez sur **Arrêter**.
- 2 Ouvrez le fichier **installation_dir\Lexmark\Markvision Enterprise\tomcat\conf\server.xml**.

Où **installation_dir** représente le dossier d'installation de MVE.

3 Configurez les chiffrements et les versions TLS.

Pour plus d'informations sur la configuration, consultez les [instructions de configuration SSL/TLS Apache Tomcat](#).

Pour plus d'informations sur les protocoles et valeurs de chiffrement, consultez la [Documentation d'informations sur l'assistance SSL Apache Tomcat](#).

4 Redémarrez le service Markvision Enterprise.

- a** Ouvrez la boîte de dialogue Exécuter, puis saisissez **services.msc**.
- b** Cliquez avec le bouton droit de la souris sur **Markvision Enterprise**, puis cliquez sur **Redémarrer**.

Comment gérer les fichiers CRL lors de l'utilisation du CA d'entreprise Microsoft ?

1 Récupérez le fichier CRL sur le serveur CA.**Remarques :**

- Pour le CA d'entreprise Microsoft, le fichier CRL n'est pas automatiquement téléchargé via SCEP.
- Pour plus d'informations, reportez-vous au *Guide de configuration de l'autorité de certification Microsoft*.

2 Enregistrez le fichier CRL dans le dossier **installation_dir\Lexmark\Markvision Enterprise\apps\library\crl**. Où **installation_dir** représente le dossier d'installation de MVE.**3** Configurez l'autorité de certification dans MVE.

Dépannage

L'utilisateur a oublié son mot de passe

Réinitialisez le mot de passe utilisateur

Vous devez disposer des droits administratifs pour réinitialiser le mot de passe.

- 1 Dans le coin supérieur droit de la page, cliquez sur .
- 2 Cliquez sur **Utilisateur**, puis sélectionnez un utilisateur.
- 3 Cliquez sur **Modifier**, puis modifiez le mot de passe.
- 4 Cliquez sur **Enregistrer les modifications**.

Si vous avez oublié votre mot de passe, effectuez l'une des opérations suivantes :

- Contactez un autre utilisateur Admin pour réinitialiser votre mot de passe.
- Contactez le Centre d'assistance client de Lexmark.

L'utilisateur administrateur a oublié son mot de passe

Créer un autre utilisateur administrateur, puis supprimer l'ancien compte

Vous pouvez utiliser l'utilitaire de mot de passe Markvision Enterprise pour créer un autre utilisateur administrateur.

- 1 Accédez au dossier dans lequel Markvision Enterprise est installé.
Par exemple, **C:\Program Files**
- 2 Lancez le fichier **mvepwdutility-windows.exe** dans le répertoire Lexmark\Markvision Enterprise\.
- 3 Sélectionnez une langue, puis cliquez sur **OK > Suivant**.
- 4 Sélectionnez **Ajouter un compte d'utilisateur > Suivant**.
- 5 Saisissez les informations d'identification d'utilisateur.
- 6 Cliquez sur **Suivant**.
- 7 Accédez à MVE, puis supprimez l'utilisateur administrateur précédent.

Remarque : Pour plus d'informations, reportez-vous à la section [« Gestion des utilisateurs » à la page 29](#).

La page ne charge pas

Ce problème peut survenir si vous avez fermé le navigateur Web sans vous déconnecter.

Essayez l'une ou plusieurs des solutions suivantes :

Effacez le cache et supprimez les cookies de votre navigateur Web

Accédez à la page de connexion MVE, puis connectez-vous à l'aide de vos informations d'identification

Ouvrez un navigateur Web et saisissez **`https://MVE_SERVER/mve/login`**, où **`MVE_SERVER`** est le nom d'hôte ou l'adresse IP du serveur hébergeant MVE.

Impossible de détecter une imprimante réseau

Essayez les solutions suivantes :

Assurez-vous que l'imprimante est allumée.

Vérifiez que le cordon d'alimentation est solidement branché sur l'imprimante et sur une prise de courant correctement mise à la terre.

Vérifiez que l'imprimante est connectée au réseau.

Redémarrez l'imprimante

Assurez-vous que le protocole TCP/IP est activé sur l'imprimante

Assurez-vous que les ports utilisés par MVE sont ouverts et que SNMP et mDNS sont activés

Pour plus d'informations, reportez-vous à la section [« Présentation des ports et protocoles » à la page 127](#).

Contactez votre représentant Lexmark

Informations d'imprimante incorrectes

Effectuez un audit

Pour plus d'informations, reportez-vous à la section [« Audit d'imprimantes » à la page 59](#).

MVE ne reconnaît pas une imprimante comme imprimante sécurisée

Vérifier que l'imprimante est sécurisée

Pour plus d'informations sur la sécurisation des imprimantes, reportez-vous à *Embedded Web Server—Guide de l'administrateur de sécurité* pour votre imprimante.

Assurez-vous que mDNS est activé et n'est pas bloqué

Supprimez l'imprimante, puis relancez la détection d'imprimante

Pour plus d'informations, reportez-vous à la section [« Détection des imprimantes » à la page 33](#).

L'application de configurations avec plusieurs applications échoue à la première tentative, mais réussit lors des tentatives suivantes

Prolonger les délais

- 1 Accédez au dossier dans lequel Markvision Enterprise est installé.

Par exemple, **C:\Program Files**

- 2 Accédez au dossier Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes.

- 3 A l'aide d'un éditeur de texte, ouvrez le fichier *platform.properties*.

- 4 Modifiez la valeur **cdcl.ws.readTimeout**.

Remarque : La valeur est en millisecondes. Par exemple, 90 000 millisecondes équivalent à 90 secondes.

- 5 A l'aide d'un éditeur de texte, ouvrez le fichier *devCom.properties*.

- 6 Modifiez les valeurs **1st.responseTimeoutsRetries**.

Remarque : La valeur est en millisecondes. Par exemple, 10 000 millisecondes équivalent à 10 secondes.

Par exemple, **1st.responseTimeoutsRetries=10000 15000 20000**. La première tentative de connexion s'exécute au bout de 10 secondes, la deuxième tentative de connexion après 15 secondes et la troisième tentative au bout de 20 secondes.

- 7 Le cas échéant, lorsque vous utilisez le protocole LDAP GSSAPI, créez un fichier *parameters.properties*.

Ajoutez le paramètre suivant : **1st.negotiation.timeout=400**

Remarque : La valeur est exprimée en secondes.

- 8 Enregistrez les modifications.

Echec de l'application des configurations avec un certificat d'imprimante

Parfois, aucun nouveau certificat n'est émis pendant l'application.

Augmentez le nombre de nouvelles tentatives d'inscription

Ajoutez la clé suivante au fichier **platform.properties** :

```
enrol.maxEnrolmentRetry=10
```

Le nombre tentative doit être supérieur à cinq.

Autorité de certification OpenXPki

Echec de l'émission du certificat à l'aide du serveur CA OpenXPki

Assurez-vous que la clé « signataire pour le compte » dans MVE correspond à la clé de signataire autorisée dans le serveur CA

Par exemple :

Si la clé **ca.onBehalf.cn** est la suivante dans le fichier **platform.properties** de MVE,

```
ca.onBehalf.cn=Markvision_SQA-2012-23AB.lrdc.lexmark.ds
```

la clé **authorized_signer** doit figurer dans le fichier **generic.yaml** du serveur CA.

```
rule1:
    # Full DN
    Subject: CN=Markvision_SQA-2012-23AB.lrdc.lexmark.ds
```

Pour plus d'informations sur la configuration du serveur CA OpenXPki, reportez-vous au *Guide de configuration de l'autorité de certification OpenXPki*.

Une erreur de serveur interne s'est produite

Installez le paramètre local **en_US.utf8**

- 1 Exécutez la commande **dpkg-reconfigure locales**.
- 2 Installez les paramètres locaux **en_US.utf8** (locale -a | grep en_US).

L'invite de connexion n'apparaît pas

Lors de l'accès à **http://yourhost/openxpki/**, vous obtenez uniquement la bannière Open Source Trustcenter, sans invite de connexion.

Activez fcgid

Exécutez les commandes suivantes :

```
1 a2enmod fcgid
```

```
2 service apache2 restart
```

Un connecteur imbriqué sans erreur de classe se produit

Une **EXCEPTION : Une erreur de connecteur imbriqué sans classe (scep.scep-server-1.connector.initial)** s'affiche à la ligne 201 /usr/share/perl5/Connector/Multi.pm.

Mettez à jour scep.scep-server-1

Dans **/etc/openxpki/config.d/realm/REALM/scep/generic.yaml**, remplacez **scep.scep-server-1** par **scep.generic**.

Remarque : Remplacez **REALM** par le nom de votre domaine. Par exemple, lorsque vous utilisez le domaine par défaut, utilisez **ca-one**.

```
eligible:
  initial:
    value@: connector:scep.generic.connector.initial
```

Impossible d'approuver manuellement les certificats

Le bouton Approbation manuelle n'apparaît pas lors de l'approbation manuelle des certificats.

Mettez à jour scep.scep-server-1

Dans **/etc/openxpki/config.d/realm/REALM/scep/generic.yaml**, remplacez **scep.scep-server-1** par **scep.generic**.

Remarque : Remplacez **REALM** par le nom de votre domaine. Par exemple, lorsque vous utilisez le domaine par défaut, utilisez **ca-one**.

```
eligible:
  initial:
    value@: connector:scep.generic.connector.initial
```

Une erreur Perl se produit lors de l'approbation des demandes d'inscription

Mettez à jour scep.scep-server-1

Dans **/etc/openxpki/config.d/realm/REALM/scep/generic.yaml**, remplacez **scep.scep-server-1** par **scep.generic**.

Remarque : Remplacez **REALM** par le nom de votre domaine. Par exemple, lorsque vous utilisez le domaine par défaut, utilisez **ca-one**.

```
eligible:
  initial:
    value@: connector:scep.generic.connector.initial
```

Les jetons **ca-signer-1** et **vault-1** sont hors ligne

La page Etat du système indique que les jetons **ca-signer-1** et **vault-1** sont hors ligne.

Essayez les solutions suivantes :

Modifiez le mot de passe de la clé de certificat

Dans `/etc/openxpki/config.d/realm/ca-one/crypto.yaml`, modifiez le mot de passe de la clé de certificat.

Créez les liens symboliques corrects et copiez le fichier de clés

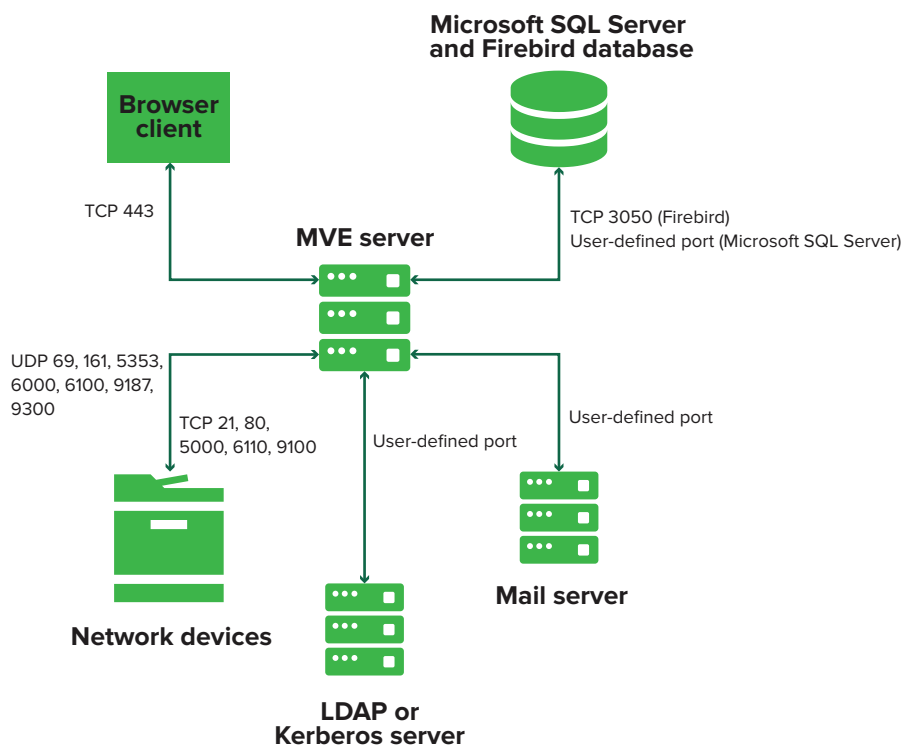
Pour plus d'informations, reportez-vous à la section « [Copie du fichier de clés et création d'un lien symbolique](#) » à la page 91.

Assurez-vous que le fichier de clés est lisible par OpenXPki

Annexe

Présentation des ports et protocoles

MVE utilise différents ports et protocoles pour différents types de communication réseau, comme illustré dans le diagramme ci-dessous :



Remarques :

- Les ports sont bidirectionnels et doivent être ouverts ou actifs pour que MVE puisse fonctionner correctement. Vérifiez que tous les ports d'imprimante sont activés.
- Certaines communications requièrent l'utilisation d'un port éphémère (gamme allouée de ports disponibles sur le serveur). Lorsqu'un client demande une session de communication temporaire, le serveur lui attribue un port dynamique. Le port n'est valide que pour une courte durée et peut redevenir disponible lorsque la session précédente expire.

Communication du serveur vers les imprimantes

Ports et protocoles utilisés pour la communication entre le serveur MVE et les imprimantes réseau

Protocole	serveur MVE	Imprimante	Utilisé pour
Network Printing Alliance Protocol (NPAP)	UDP 9187	UDP 9300	Communication avec les imprimantes réseau Lexmark.
XML Network Transport (XMLNT)	UDP 9187	UDP 6000	Communication avec certaines imprimantes réseau Lexmark.
Lexmark Secure Transport (LST)	UDP 6100 Port TCP (Transmission Control Protocol) éphémère (signaux de reconnaissance)	UDP 6100 TCP 6110 (signaux de reconnaissance)	Communication sécurisée avec certaines imprimantes réseau Lexmark.
Multicast Domain Name System (mDNS)	Port UDP (User Datagram Protocol) éphémère	UDP 5353	Détection des imprimantes réseau Lexmark et détermination des fonctions de sécurité des imprimantes. Remarque : ce port est nécessaire pour permettre à MVE de communiquer avec les imprimantes sécurisées.
Simple Network Management Protocol (SNMP)	Port UDP éphémère	UDP 161	Détection et communication avec des imprimantes réseau Lexmark et tierces.
FTP (File Transfer Protocol)	Port TCP éphémère	TCP 21 TCP 20	Déploiement de fichiers.
Hypertext Transfer Protocol (HTTP)	Port TCP éphémère	TCP 80	Déploiement de fichiers ou mise en œuvre de configurations.
		TCP 443	Déploiement de fichiers ou mise en œuvre de configurations.
Hypertext Transfer Protocol over SSL (HTTPS)	Port TCP éphémère	TCP 161 TCP 443	Déploiement de fichiers ou mise en œuvre de configurations.
RAW	Port TCP éphémère	TCP 9100	Déploiement de fichiers ou mise en œuvre de configurations.

Communication des imprimantes vers le serveur

Port et protocole utilisés pour la communication entre les imprimantes réseau et le serveur MVE

Protocole	Imprimante	serveur MVE	Utilisé pour
NPAP	UDP 9300	UDP 9187	Génération et réception d'alertes

Communication serveur vers base de données

Ports et protocoles utilisés pour la communication entre le serveur MVE et les bases de données

serveur MVE	Base de données	Utilisé pour
Port TCP éphémère	Port défini par l'utilisateur. Le port par défaut est TCP 1433.	Communication avec une base de données SQL Server.
Port TCP éphémère	TCP 3050	Communication avec une base de données Firebird.

Communication des clients vers le serveur

Port et protocole utilisés pour la communication entre le client navigateur et le serveur MVE

Protocole	Client navigateur	serveur MVE
Hypertext Transfer Protocol over SSL (HTTPS)	Port TCP	TCP 443

Communication du serveur vers le serveur de messagerie

Port et protocole utilisés pour la communication entre le serveur MVE et un serveur de messagerie électronique

Protocole	serveur MVE	Serveur SMTP	Utilisé pour
Simple Mail Transfer Protocol (SMTP)	Port TCP éphémère	Port défini par l'utilisateur. Le port par défaut est TCP 25.	Fonction de courrier électronique permettant de recevoir des alertes des imprimantes.

Communication du serveur vers le serveur LDAP

Ports et les protocoles utilisés pour la communication entre le serveur MVE et un serveur LDAP mettant en jeu les groupes d'utilisateurs et l'authentification

Protocole	serveur MVE	serveur LDAP	Utilisé pour
Lightweight Directory Access Protocol (LDAP)	Port TCP éphémère	Port défini par l'utilisateur. Le port par défaut est TCP 389.	Authentification des utilisateurs MVE via un serveur LDAP.
Lightweight Directory Access Protocol over TLS (LDAPS)	Port TCP éphémère	Port défini par l'utilisateur. Le port par défaut est TCP 636.	Authentification des utilisateurs MVE via un serveur LDAP sur TLS.
Kerberos	Port UDP éphémère	Port défini par l'utilisateur. Le port par défaut est UDP 88.	Authentification des utilisateurs MVE via Kerberos.

Activation de l'approbation automatique des demandes de certificat dans l'autorité de certification Microsoft

Par défaut, tous les serveurs CA sont en mode En attente et vous devez approuver manuellement chaque demande de certificat signée. Etant donné que cette méthode n'est pas possible pour les demandes groupées, activez l'approbation automatique des certificats signés.

- 1 Dans Server Manager, cliquez sur **Outils > Autorité de certification**.
- 2 Dans le panneau de gauche, cliquez avec le bouton droit de la souris sur l'autorité de certification, puis cliquez sur **Propriétés > Module de stratégie**.
- 3 Dans l'onglet Traitement des demandes, cliquez sur **Suivre les paramètres du modèle de certificat, le cas échéant**, puis cliquez sur **OK**.
Remarque : Si l'option **Définir l'état de la demande de certificat sur En attente** est sélectionnée, vous devez approuver manuellement le certificat.
- 4 Redémarrez le service d'autorité de certification.

Révocation des certificats

Remarque : Avant de commencer, vérifiez que le serveur d'autorité de certification est configuré pour les CRL et qu'ils sont disponibles.

- 1 Depuis le serveur d'autorité de certification, ouvrez **Autorité de certification**.
- 2 Dans le panneau de gauche, développez l'autorité de certification, puis cliquez sur **Certificats fournis**.
- 3 Cliquez avec le bouton droit de la souris sur un certificat à révoquer, puis cliquez sur **Toutes les tâches > Révoquer le certificat**.
- 4 Sélectionnez un code de motif, ainsi que la date et l'heure de la révocation, puis cliquez sur **Oui**.
- 5 Dans le panneau de gauche, cliquez avec le bouton droit de la souris sur **Certificats révoqués**, puis cliquez sur **Toutes les tâches > Publier**.

Remarque : Vérifiez que le certificat que vous avez révoqué se trouve dans Certificats révoqués.

Vous pouvez voir le numéro de série du certificat révoqué dans le fichier CRL.

Avis

Note d'édition

Novembre 2020

Le paragraphe suivant ne s'applique pas aux pays dans lesquels lesdites clauses ne sont pas conformes à la législation en vigueur : LEXMARK INTERNATIONAL, INC. FOURNIT CETTE PUBLICATION "TELLE QUELLE", SANS GARANTIE D'AUCUNE SORTE, EXPLICITE OU IMPLICITE, Y COMPRIS, MAIS SANS SE LIMITER AUX GARANTIES IMPLICITES DE COMMERCIALISABILITE OU DE CONFORMITE A UN USAGE SPECIFIQUE. Certains Etats n'admettent pas la renonciation aux garanties explicites ou implicites pour certaines transactions ; c'est pourquoi il se peut que cette déclaration ne vous concerne pas.

Cette publication peut contenir des imprécisions techniques ou des erreurs typographiques. Des modifications sont périodiquement apportées aux informations contenues dans ce document ; ces modifications seront intégrées dans les éditions ultérieures. Des améliorations ou modifications des produits ou programmes décrits dans cette publication peuvent intervenir à tout moment.

Dans la présente publication, les références à des produits, programmes ou services n'impliquent nullement la volonté du fabricant de les rendre disponibles dans tous les pays où celui-ci exerce une activité. Toute référence à un produit, programme ou service n'affirme ou n'implique nullement que seul ce produit, programme ou service puisse être utilisé. Tout produit, programme ou service équivalent par ses fonctions, n'enfreignant pas les droits de propriété intellectuelle, peut être utilisé à la place. L'évaluation et la vérification du fonctionnement en association avec d'autres produits, programmes ou services, à l'exception de ceux expressément désignés par le fabricant, se font aux seuls risques de l'utilisateur.

Pour bénéficier de l'assistance technique de Lexmark, rendez-vous sur le site <http://support.lexmark.com>.

Pour obtenir des informations sur la politique de confidentialité de Lexmark régissant l'utilisation de ce produit, consultez la page www.lexmark.com/privacy.

Pour obtenir des informations sur les fournitures et les téléchargements, rendez-vous sur le site www.lexmark.com.

© 2017 Lexmark International, Inc.

Tous droits réservés.

Marques commerciales

Lexmark, le logo Lexmark et Markvision sont des marques commerciales ou des marques déposées de Lexmark International, Inc., déposées aux Etats-Unis et/ou dans d'autres pays.

Firebird est une marque déposée de la Firebird Foundation.

Google Chrome est une marque commerciale de Google LLC.

Safari est une marque déposée d'Apple Inc.

Java est une marque déposée d'Oracle et/ou de ses filiales.

Les autres marques commerciales sont la propriété de leurs détenteurs respectifs.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

JmDNS License

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Arthur van Hoff

avh@strangeberry.com

Rick Blair

rickblair@mac.com

** JmDNS

Avis relatifs à l'accord de licence

Tous les avis relatifs à l'accord de licence peuvent être consultés à partir du dossier du programme.

Glossaire

action	Courrier électronique de notification ou opération de ligne de commande. Les actions attribuées à des événements sont déclenchées en cas d'alerte.
audit	Tâche consistant à collecter des données sur les imprimantes, concernant par exemple leurs états, leurs consommables et leurs fonctionnalités.
configuration	Un ensemble de paramètres pouvant être attribués et appliqués à une imprimante ou à un groupe de modèles d'imprimante. Dans une configuration, vous pouvez modifier les paramètres d'imprimante et déployer des applications, des licences, des microcodes et des certificats d'autorité de certification vers les imprimantes.
événement	Définit les actions qui s'exécutent lorsque des alertes spécifiques sont actives.
imprimante sécurisée	Imprimante configurée pour communiquer sur un canal chiffré et dont l'accès aux fonctions ou applications nécessite une authentification.
jeton	Identificateur qui représente les valeurs de données d'imprimante pour les paramètres de variable d'une configuration.
mot clé	Texte personnalisé attribué à des imprimantes, qui vous permet de rechercher ces imprimantes au sein du système. Lorsque vous filtrez une recherche à l'aide d'un mot clé, seules les imprimantes marquées de ce mot clé sont renvoyées.
paramètres de variable	Ensemble de paramètres d'une imprimante contenant des valeurs dynamiques qui peuvent être intégrées dans une configuration.
profil de recherche	Profil contenant un ensemble de paramètres permettant de rechercher des imprimantes sur un réseau. Il peut également contenir des configurations prédéfinies qui peuvent être automatiquement attribuées et appliquées aux imprimantes pendant la détection.

Index

A

- accès à MVE 22
- Accès aux informations de l'autorité
 - configuration 80
- accessibilité CRL
 - configuration 81, 93, 100
- action
 - espaces réservés 103
- action de courrier électronique 102
- action Événement du journal 102
- actions
 - création 102
 - gestion 104
 - modification 104
 - suppression 104
 - test 104
- activation de l'approbation automatique des demandes de certificat dans l'autorité de certification Microsoft 130
- activation de l'approbation automatique des demandes de certificat dans l'autorité de certification OpenXPKI 95
- activation de l'authentification de serveur LDAP 30
- activation des certificats de signataire pour le compte de 94
- activation du service SCEP 94
- affichage de l'aperçu de l'état et de l'historique d'une tâche 110
- affichage de l'état de la tâche 110
- affichage de l'instance d'Embedded Web Server sur l'imprimante 59
- affichage de la liste d'imprimantes 37
- affichage des informations de l'imprimante 40
- affichage des journaux 110
- AIA
 - configuration 80
- ajout d'un avertissement de connexion 114
- ajout de l'EKU d'authentification client dans les certificats 99
- alertes de l'imprimante
 - présentation 105
- annuler l'attribution de configurations 60
- aperçu
 - affichage de l'état et de l'historique d'une tâche 110
 - configuration de l'accès utilisateur 28
 - configuration du serveur CA racine 76
 - configuration du serveur CA subordonné 78
 - gestion des alertes d'imprimante 102
 - gestion des configurations 67
 - Markvision Enterprise 10
- aperçu de la gestion des configurations 67
- applications
 - désinstallation 63
- approbation automatique des demandes de certificat
 - activation dans l'autorité de certification Microsoft 130
 - activation dans l'autorité de certification OpenXPKI 95
- arrêt des tâches 110
- attribution d'événements à des imprimantes 63
- attribution d'un mot clé 64
- attribution de configurations à des imprimantes 60
- audit d'imprimantes 59
- autorisations
 - présentation 55
- autorisations d'impression
- couleur
 - configuration 71
- avertissement de connexion
 - ajout 114

B

- barre de recherche
 - filtrage des imprimantes 43
- base de données
 - configuration 17
 - configuration requise 13

- restauration 25
- sauvegarde 25
- Base de données Firebird 17
- bases de données prises en charge 13
- bibliothèque de ressources
 - importation 73

C

- CA d'entreprise Microsoft
 - configuration 118
- CA d'entreprise Microsoft avec NDES
 - configuration 77
- ca-signer-1 est hors ligne
 - dépannage 126
- CDP
 - configuration 80
- Certificat CA d'OpenXPKI
 - configuration à l'aide du script par défaut 86
 - configuration manuelle 87
 - installation 84
- certificat MVE
 - signature 115
- certificats
 - création 96
 - importation 91
 - révocation 100, 130
- certificats d'autorité de certification
 - création 89
- certificats d'imprimante
 - configuration manuelle 65
- certificats de coffre
 - création 90
- certificats de serveur LDAP
 - installation 32
- certificats du signataire
 - création 89
- certificats du signataire pour le compte de
 - activation 94
- certificats SCEP
 - création 90
- chiffrement AES256
 - configuration 118

- chiffrements
 - personnalisation 118
- clés de certificat
 - création de fichiers de mots de passe 89
- clonage de configurations
 - exemple de scénario 70
- communications avec l'imprimante
 - sécurisation 57
- composant de sécurité avancée
 - création 70
- configuration
 - conformité 61
 - création 67, 69
 - exportation 73
 - importation 73
- configuration de l'accessibilité CRL 81, 93, 100
- configuration de l'aperçu de l'accès utilisateur 28
- configuration de l'autorité de certification OpenXPki à l'aide du script par défaut 86
- configuration de la base de données 17
- configuration de la CA d'entreprise Microsoft avec NDES
 - aperçu 77
- configuration de la sécurité d'une imprimante 56
- configuration de MVE pour la gestion automatisée des certificats 75
- configuration des autorisations d'impression couleur 71
- configuration des paramètres d'accès aux informations d'autorisation 80
- configuration des paramètres de courrier électronique 114
- configuration des paramètres du point de distribution de certification 80
- configuration des paramètres généraux 114
- configuration des points de terminaison SCEP pour plusieurs domaines 98
- configuration des serveurs NDES 81

- configuration des serveurs Network Device Enrollment Service 81
- configuration manuelle de l'autorité de certification OpenXPki 87
- configuration manuelle des certificats d'imprimante 65
- configuration requise pour l'utilisateur 13
- configuration requise pour la base de données 13
- configuration requise pour le serveur Web 13
- configurations
 - annulation d'attribution 60
 - attribution 60
 - mise en œuvre 60
- configurations par défaut 53
- conformité
 - vérification 61
- connecteur imbriqué sans erreur de classe 125
- contrôles d'accès aux fonctions
 - présentation 55
- copie de fichiers de clés 91
- copie de profils de recherche 35
- copie de recherches enregistrées 49
- copie de vues 41
- copie du répertoire 95
- création d'un composant de sécurité avancée à partir d'une imprimante 70
- création d'un événement 104
- création d'un fichier de configuration OpenSSL 88
- création d'un package d'applications 72
- création d'un profil de recherche 33
- création d'une action 102
- création d'une configuration 67
- création d'une configuration à partir d'une imprimante 69
- création d'une programmation 112
- création d'une recherche enregistrée personnalisée 46
- création de certificats 96
- création de certificats d'autorité de certification racine 89

- création de certificats de coffre 90
- création de certificats du signataire 89
- création de certificats SCEP 90
- création de fichiers de mots de passe pour les clés de certificat 89
- création de liens symboliques 91
- création de modèles de certificat 82
- création de mots clés 44
- CSV
 - paramètres de variable 71

D

- définition d'une vue par défaut 41
- définition des modèles de certificat pour NDES 82
- définition des numéros de port par défaut pour l'autorité de certification OpenXPki 98
- définition du répertoire 95
- demandes de certificat dans l'autorité de certification Microsoft
 - approbation automatique 130
- demandes de certificat dans l'autorité de certification OpenXPki
 - approbation automatique 95
- démarrage d'OpenXPki 92
- dépannage
 - ca-signer-1 est hors ligne 126
 - connecteur imbriqué sans erreur de classe 125
 - échec de l'application des configurations avec un certificat d'imprimante 124
 - échec de l'émission du certificat à l'aide du serveur CA OpenXPki 124
 - erreur de serveur interne 124
 - erreur Perl 125
 - impossible d'approuver manuellement les certificats 125
 - impossible de détecter une imprimante réseau 122
 - informations d'imprimante incorrectes 122

- l'application de configurations
 - avec plusieurs applications
 - échoue à la première tentative, mais réussit lors des tentatives suivantes 123
- l'invite de connexion n'apparaît pas 125
- l'utilisateur administrateur a oublié son mot de passe 121
- la page charge de manière continue 122
- MVE ne reconnaît pas une imprimante comme imprimante sécurisée 123
- vault-1 est hors ligne 126
- déploiement de configurations
 - exemple de scénario 69
- déploiement de fichiers sur des imprimantes 61
- dernière version de MVE
 - mise à niveau 24
- désactivation du mot de passe de challenge sur l'autorité de certification OpenXPki 99
- désactivation du mot de passe de challenge sur le serveur CA Microsoft 83
- désinstallation d'applications présentes sur les imprimantes 63
- détection des imprimantes 36
- données de l'imprimante
 - exportation 41

E

- échec de l'application des configurations avec un certificat d'imprimante 124
- échec de l'émission du certificat à l'aide du serveur CA OpenXPki 124
- effacement des journaux 110
- EKU d'authentification client
 - ajout dans des certificats 99
- Embedded Web Server
 - affichage 59
- erreur de serveur interne 124
- erreur Perl 125
- espaces réservés 102
- espaces réservés d'action
 - présentation 103

- état de l'imprimante
 - configuration 60
 - mise à jour 59
- état de la tâche
 - affichage 110
- états de sécurité de l'imprimante
 - présentation 52
- états du cycle de vie de l'imprimante
 - présentation 44
- événement
 - création 104
- événements
 - attribution 63
 - gestion 109
 - modification 109
 - suppression 109
- exécution d'une recherche enregistrée 46
- exécution de profils de recherche 35
- exécution en tant qu'utilisateur
 - configuration 18
- exemple de scénario pour le déploiement de configurations 69
- exemple de scénario pour les configurations de clonage 70
- exportation CSV
 - paramètres de variable 71
- exportation de journaux 111
- exportation des données de l'imprimante 41

F

- fichier de configuration OpenSSL
 - création 88
- fichiers
 - déploiement 61
- fichiers de clés
 - copie 91
- fichiers de journal d'application
 - recherche 118
- fichiers de mots de passe pour les clés de certificat
 - création 89
- fichiers journaux
 - recherche 118
- fichiers journaux d'installation
 - recherche 118

- filtrage des imprimantes via la barre de recherche 43
- fonction de gestion automatisée des certificats 74

G

- génération des informations CRL 92
- gestion automatisée des certificats
 - configuration 75
- gestion de certificats 74
- gestion de la présentation des alertes d'imprimante 102
- gestion des actions 104
- gestion des événements 109
- gestion des mots clés 44
- gestion des profils de recherche 35
- gestion des programmations 113
- gestion des recherches enregistrées 49
- gestion des utilisateurs 29
- gestion des vues 41

H

- historique des modifications 7

I

- importation CSV
 - paramètres de variable 71
- importation de fichiers vers la bibliothèque de ressources 73
- importation des certificats 91
- importation ou exportation d'une configuration 73
- impossible d'approuver manuellement les certificats 125
- impossible de détecter une imprimante réseau 122
- imprimante
 - conformité 61
 - redémarrage 59
- imprimantes
 - audit 59
 - déploiement de fichiers 61
 - désinstallation 65
 - événements 63
 - filtrage 43
 - recherche 36
 - sécurisation 53, 57

- imprimantes sécurisées
 - authentification 64
- informations CRL
 - génération 92
- informations d'identification
 - saisie 64
- informations d'imprimante incorrectes 122
- informations sur l'imprimante
 - affichage 40
- informations utilisateur
 - désinstallation 115
- installation de certificats de serveur LDAP 32
- installation de l'autorité de certification OpenXPki 84
- installation de MVE 19
- installation des serveurs CA racine 76
- installation des serveurs CA subordonnés 78
- installation silencieuse
 - MVE 20
- installation silencieuse de MVE 20

J

- journaux
 - affichage 110
 - effacement 110
 - exportation 111

L

- l'application de configurations avec plusieurs applications échoue à la première tentative, mais réussit lors des tentatives suivantes 123
- l'invite de connexion n'apparaît pas 125
- l'utilisateur administrateur a oublié son mot de passe 121
- la page charge de manière continue 122
- langue
 - modification 22
- langues
 - prise en charge 14
- langues prises en charge 14
- liens symboliques
 - création 91

- liste d'imprimantes
 - affichage 37

M

- Markvision Enterprise
 - présentation 10
- meilleures pratiques 11
- microcode de l'imprimante
 - mise à jour 62
- Microsoft SQL Server 17
- mise à jour de l'état de l'imprimante 59
- mise à jour du microcode de l'imprimante 62
- mise à niveau vers la dernière version de MVE 24
- mise en œuvre de configurations 60
- modèles d'imprimante pris en charge 14
- modèles de certificat
 - création 82
- modèles de certificat pour NDES
 - Configuration 82
- modèles pris en charge
 - configuration 118
- modification d'actions 104
- modification de la langue 22
- modification de la vue listes des imprimantes 43
- modification de mots clés 44
- modification de profils de recherche 35
- modification de programmations 113
- modification de recherches enregistrées 49
- modification de votre mot de passe 22
- modification de vues 41
- modification des paramètres du programme d'installation après l'installation 27
- mot clé
 - attribution 64
- mot de passe
 - modification 22
 - réinitialisation 121
- Mot de passe de challenge
 - désactivation dans l'autorité de certification OpenXPki 99

- désactivation dans le serveur CA Microsoft 83

- mots clés

- création 44
 - gestion 44
 - modification 44
 - suppression 44

- MVE

- accès 22
 - installation 19

- MVE ne reconnaît pas une imprimante comme imprimante sécurisée 123

N

- navigateurs Web pris en charge 13
- numéro du port par défaut
 - paramètre pour l'autorité de certification OpenXPki 98

O

- objets de certificat complets
 - demande via SCEP 99
- obtention d'objets de certificat complets lors d'une demande via SCEP 99
- OpenXPki
 - démarrage 92

P

- package d'applications
 - création 72
- paramètres de configuration
 - version imprimable 71
- paramètres de courrier électronique
 - configuration 114
- paramètres de variable
 - présentation 71
- paramètres des règles de recherche
 - présentation 47
- paramètres du programme d'installation
 - modification 27
- paramètres généraux
 - configuration 114
- pare-feu Windows
 - ajout de règles 118

- Point de distribution de certification
 - configuration 80
- points de terminaison SCEP
 - configuration pour plusieurs domaines 98
- ports
 - configuration 118
 - présentation 127
- présentation de la configuration du serveur CA racine 76
- présentation de la configuration du serveur CA subordonné 78
- présentation des alertes d'imprimante 105
- présentation des espaces réservés d'action 103
- présentation des états du cycle de vie de l'imprimante 44
- présentation des rôles utilisateur 28
- profil de recherche
 - création 33
- profils de recherche
 - copie 35
 - exécution 35
 - gestion 35
 - modification 35
 - suppression 35
- programmation
 - création 112
- programmations
 - gestion 113
 - modification 113
 - suppression 113
- protocoles
 - présentation 127

R

- recherche enregistrée
- personnalisée
 - création 46
- recherches enregistrées
 - accès 118
 - copie 49
 - exécution 46
 - gestion 49
 - modification 49
 - suppression 49
- redémarrage de l'imprimante 59
- réglage de l'état de l'imprimante 60

- réglage de MVE comme exécution en tant qu'utilisateur 18
- règles de recherche
 - opérateurs 47
 - paramètres 47
- résolution DNS inverse 118
- résolution du nom de l'hôte
 - recherche inversée 118
- révocation des certificats 100, 130
- rôles utilisateur
 - présentation 28

S

- saisie des informations d'identification pour les imprimantes sécurisées 64
- sauvegarde et restauration de la base de données 25
- sécurisation des communications avec les imprimantes de votre parc 57
- sécurisation des imprimantes 57
- sécurisation des imprimantes à l'aide des configurations par défaut 53
- sécurité de l'imprimante
 - configuration 56
- serveur LDAP
 - activation de l'authentification 30
- serveur Web
 - configuration requise 13
- serveurs CA racine
 - installation 76
- serveurs CA subordonnés
 - installation 78
- serveurs NDES
 - configuration 81
- serveurs Network Device Enrollment Service
 - configuration 81
- serveurs pris en charge 13
- service SCEP
 - activation 94
- signature du certificat MVE 115
- Simple Certificate Enrollment Protocol
 - activation 94
- suppression d'actions 104
- suppression d'imprimantes 65

- suppression de mots clés 44
- suppression de profils de recherche 35
- suppression de programmations 113
- suppression de recherches enregistrées 49
- suppression de vues 41
- suppression des références et des informations utilisateur 115
- surveillance des imprimantes 50
- système de l'utilisateur
 - configuration requise 13
- systèmes d'exploitation pris en charge 13

T

- tâches
 - arrêt 110
- test d'actions 104

U

- utilisateurs
 - ajout 29
 - gestion 29
 - modification 29
 - suppression 29

V

- vault-1 est hors ligne
 - dépannage 126
- vérification de la conformité d'une imprimante avec une configuration 61
- versions TLS
 - personnalisation 118
- vue listes des imprimantes
 - modification 43
- vues
 - copie 41
 - gestion 41
 - modification 41
 - suppression 41