



Markvision Enterprise

Guide de l'utilisateur

Avis d'édition

Avril 2012

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 COMMERCIALITE 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 contacter l'assistance technique de Lexmark, consultez la page support.lexmark.com.

Pour des informations sur les consommables et les téléchargements, visitez le site www.lexmark.com.

Si vous ne disposez pas d'un accès à Internet, vous pouvez contacter Lexmark par courrier, à l'adresse suivante :

Lexmark International, Inc.
Bldg 004-2/CSC
740 New Circle Road NW
Lexington, KY 40550
USA

© 2012 Lexmark International, Inc.

Tous droits réservés.

Marques commerciales

Lexmark, Lexmark accompagné du logo en forme de diamant et MarkVision sont des marques de Lexmark International, Inc. déposées aux Etats-Unis et/ou dans d'autres pays.

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.

Avis relatifs à l'accord de licence

Tous les avis relatifs à l'accord de licence correspondant à ce produit peuvent être consultés à partir du répertoire racine du CD du logiciel d'installation.

Contenu

- Avis d'édition.....2**
- Aperçu.....7**
 - Qu'est-ce que MarkVision Enterprise ?.....7
- Mise en route.....8**
 - Déclaration de support.....8
 - Configuration requise8
 - Serveurs de base de données pris en charge.....8
 - Installation de MarkVision.....8
 - Mise à niveau vers la dernière version de MarkVision.....9
 - Sauvegarde et restauration de la base de données Firebird.....9
 - Accès à MarkVision.....10
 - Migration de MarkVision Professional vers MarkVision Enterprise.....11
 - Utilisation de MarkVision.....12
 - Présentation de l'écran d'accueil.....14
 - Présentation des ports et protocoles.....15
- Gestion des actifs.....18**
 - Découverte de périphériques.....18
 - Création d'un profil de recherche.....18
 - Modification ou suppression d'un profil de recherche.....20
 - Importation de périphériques à partir d'un fichier.....20
 - Gestion des périphériques.....21
 - Définition de l'état du cycle de vie du périphérique.....21
 - Audit d'un périphérique.....22
 - Affichage des propriétés d'un périphérique23
- Localisation et organisation des périphériques du système.....24**
 - Recherche de périphériques système.....24
 - Travailler avec des signets.....27
 - Création de signets27
 - Accès aux signets27
 - Suppression de signets27
 - Utilisation de catégories et de mots-clés.....27
 - Ajout, modification ou suppression de catégories28
 - Ajout, modification ou suppression de mots clés.....28

Attribution de mots clés à un périphérique.....	28
Suppression d'un mot clé attribué sur un périphérique.....	29
Gestion des polices.....	30
Création d'une police.....	30
Création d'une nouvelle stratégie.....	30
Création d'une stratégie à partir d'un périphérique.....	31
Comprendre la police de sécurité.....	31
Présentation des périphériques sécurisés.....	31
Présentation des paramètres des stratégies de sécurité.....	33
Création d'une police de sécurité.....	34
Modification des informations d'authentification de communication d'un périphériques restreint.....	39
Modification ou suppression d'une stratégie.....	40
Attribution d'une stratégie.....	41
Contrôle de la conformité à une stratégie.....	41
Mise en œuvre d'une stratégie.....	41
Suppression d'une stratégie.....	42
Gestion du Service Desk.....	43
Travailler avec des polices.....	43
Vérification de la conformité du périphérique aux stratégies.....	43
Mise en œuvre des stratégies.....	43
Travailler avec un périphérique.....	43
Vérification de l'état d'un périphérique.....	43
Affichage d'un périphérique à distance.....	44
Affichage de la page Web incorporée.....	44
Gestion des évènements de périphériques.....	45
Création d'une destination.....	45
Modification ou suppression d'une destination.....	46
Création d'un événement.....	46
Modification ou suppression d'un événement.....	46
Attribution d'un événement à un périphérique.....	47
Suppression d'un événement sur un périphérique.....	47
Affichage des détails d'un événement.....	47
Réaliser d'autre tâches d'administration.....	48
Téléchargement de fichiers génériques.....	48
Configuration des paramètres de courrier électronique.....	48
Configuration des paramètres système.....	49

Ajout, modification ou suppression d'un utilisateur dans le système.....	49
Activation de l'authentification de serveur LDAP.....	50
Génération de rapports.....	55
Planification de tâches.....	56
Affichage du journal système.....	57
Foire aux questions.....	58
Dépannage.....	59
L'utilisateur a oublié son mot de passe.....	59
L'application ne détecte aucun périphérique réseau.....	59
Vérifiez les connexions de l'imprimante.	59
Assurez-vous que le serveur d'impression interne est correctement installé et activé.	59
Assurez-vous que le nom du périphérique dans l'application est le même que le nom défini dans le serveur d'impression.	60
Vérifiez que le serveur d'impression communique bien avec le réseau.....	60
Les informations relatives au périphérique sont incorrectes.....	60
Glossaire des termes de sécurité.....	61
Index.....	62

Aperçu

Qu'est-ce que MarkVision Enterprise ?

Markvision™ Enterprise (MVE) est un utilitaire de gestion de périphériques avec interface Web, destiné aux services informatiques. MVE fonctionne en mode client-serveur. Le serveur détecte les périphériques et établit une communication avec eux sur le réseau, puis il fournit des informations les concernant au client. Le client affiche les informations sur les périphériques et fournit une interface utilisateur pour gérer ces derniers. Chaque serveur MarkVision peut gérer des milliers de périphériques en même temps.

Les fonctions de sécurité intégrées à MVE empêchent les tentatives d'accès non autorisé à l'application. Seuls les utilisateurs autorisés peuvent utiliser le client pour accéder aux options de gestion.

MarkVision vous permet de surveiller et de gérer tout votre parc d'impression, composé d'imprimantes et de serveurs d'impression. Dans *ITIL (Information Technology Infrastructure Library)*, les imprimantes et serveurs d'impression sont appelés *Configuration Items* (éléments de configuration ou CI). Dans ce document, les CI, imprimantes ou serveurs d'impression sont également appelés périphériques.

Mise en route

Déclaration de support

Pour obtenir la liste complète des systèmes d'exploitation et des navigateurs Web pris en charge, consultez les *Notes de publication*.

Configuration requise

RAM

- Requise : 1 Go
- Recommandée : 2 Go+

Vitesse du processeur

- Requise : 1 processeur physique à 2 GHz ou plus (Hyper-Threaded/Dual Core)
- Recommandée : 1+ processeur physique à 3+ GHz (Hyper-Threaded/Dual Core+)

Espace disque de l'ordinateur

- Au moins 60 Go d'espace disponible

Résolution de l'écran

- Au moins 1024 × 768 pixels (clients MVE uniquement)

Serveurs de base de données pris en charge

- Firebird
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

Remarques :

- L'application prend uniquement en charge les versions 32 bits et est fournie avec une base de données Firebird préconfigurée.
- Le serveur de base de données sur laquelle le MVE est installée doit comporter une seule *carte d'interface réseau*(NIC).

Installation de MarkVision

MarkVision permet d'utiliser soit Firebird soit Microsoft SQL Server comme base de données principale.

Si vous utilisez Microsoft SQL Server, procédez comme suit avant d'installer MarkVision :

- Activez l'authentification en mode mixte et l'exécution automatique.
- Configurez les bibliothèques réseau pour utiliser un port statique et des sockets TCP/IP.

- Créez un compte utilisateur que MarkVision utilisera pour créer le schéma de base de données et les connexions de base de données nécessaires.
- Créez les bases de données suivantes :
 - FRAMEWORK
 - MONITOR
 - QUARTZ

Remarque : Le compte utilisateur que vous avez créé doit être propriétaire de ces bases de données, ou du moins avoir les droits nécessaires pour créer un schéma et effectuer des opérations *DML* (Data Manipulation Language).

- 1 Décompressez les fichiers d'installation dans un dossier dont le chemin ne contient *pas* d'espace.
- 2 Lancez le fichier **setup.exe**, puis suivez les instructions à l'écran.

Mise à niveau vers la dernière version de MarkVision

Seule la mise à niveau de la toute dernière version est possible.

- 1 Sauvegardez votre base de données.

Remarques :


- Si vous utilisez une base de données Firebird, reportez-vous à la section « Sauvegarde de la base de données Firebird », page 9 pour de plus amples informations.
- Si vous utilisez un serveur MS SQL, contactez votre administrateur MS SQL.

- 2 Dézippez les fichiers d'installation à un emplacement temporaire, puis vérifiez que le chemin d'accès ne contient *aucun* espace.
- 3 Lancez **setup.exe**, puis suivez les instructions qui s'affichent sur l'écran de l'ordinateur.

Sauvegarde et restauration de la base de données Firebird

Sauvegarde de la base de données Firebird

Remarque : Si vous utilisez un serveur MS SQL comme base de données, contactez votre administrateur MS SQL.

- 1 Arrêtez le service Markvision Enterprise.
 - a Cliquez sur  ou sur **Démarrer > Paramètres**.
 - b Sélectionnez **Panneau de configuration**, puis cliquez éventuellement sur **Système et sécurité**.
 - c Cliquez deux fois sur **Outils d'administration**.
 - d Si nécessaire, double-cliquez sur le fichier **Services de composants**.
 - e Cliquez deux fois sur **Services**.
 - f Dans le volet Services, sélectionnez **Markvision Enterprise** et cliquez sur **Arrêter**.
- 2 Recherchez le dossier dans lequel Markvision Enterprise est installé, puis naviguez jusqu'à firebird\data.
Par exemple, `C:\Program Files\Lexmark\Markvision Enterprise\firebird\data`

- 3 Copiez les bases de données suivantes dans un référentiel sûr.
 - FRAMEWORK.FDB
 - MONITOR.FDB
 - QUARTZ.FDB
- 4 Redémarrez le service Markvision Enterprise.
 - a Répétez les étapes 1a à 1e.
 - b Dans le volet Services, sélectionnez **Markvision Enterprise** et cliquez sur **Redémarrer**.

Restauration de base de données Firebird

- 1 Assurez-vous d'avoir terminé le processus de sauvegarde de la base de données Firebird.
- 2 Arrêtez le service Markvision Enterprise.

Pour de plus amples informations, reportez-vous à la section étape 1 de « Sauvegarde de la base de données Firebird », page 9.
- 3 Recherchez le dossier dans lequel Markvision Enterprise est installé, puis naviguez jusqu'à firebird\data.

Par exemple, **C:\Program Files\Lexmark\Markvision Enterprise\firebird\data**
- 4 Remplacez les bases de données suivantes par les bases de données enregistrées lors de l'exécution du processus de sauvegarde.
 - FRAMEWORK.FDB
 - MONITOR.FDB
 - QUARTZ.FDB
- 5 Redémarrez le service Markvision Enterprise.

Pour de plus amples informations, reportez-vous à la section étape 4 de « Sauvegarde de la base de données Firebird », page 9.

Accès à MarkVision

- 1 Ouvrez un navigateur Web, puis tapez **http://SERVEUR_MVE:9788/mve/** dans le champ URL.

Remarque : Remplacez **SERVEUR_MVE** par le nom d'hôte ou l'adresse IP de la machine sur laquelle s'exécute MarkVision.
- 2 Dans le champ Utilisateur, tapez **admin**.
- 3 Dans le champ Mot de passe, tapez **Administrator1**, puis cliquez sur **Connexion**.

Remarque : Pour changer votre mot de passe, cliquez sur **Modifier le mot de passe** dans le coin supérieur droit de l'écran d'accueil.


Si Markvision est inactif pendant plus de 30 minutes, il se déconnecte automatiquement. Vous devez vous reconnecter pour accéder à MarkVision.

Migration de MarkVision Professional vers MarkVision Enterprise

Remarque : MarkVision Enterprise (MVE) prend uniquement en charge la migration des données depuis MarkVision Professional (MVP) version 11.2.1.

Exportation des données de MVP

Via la page Web MVP Server

- 1 Ouvrez un navigateur Web et tapez `http://SERVEUR_MVP:9180/~MvServer` dans la barre d'adresse.
Remarque : Remplacez `SERVEUR_MVP` par l'adresse IP ou le nom d'hôte du serveur MVP.
- 2 Dans la page Web du serveur MarkVision, cliquez sur **Data Dir** (répertoire de données).
- 3 Entrez vos nom d'utilisateur et mot de passe si vous y êtes invité.
- 4 Dans la page Download Data Directory (répertoire de téléchargement des données), cliquez sur  pour télécharger vos données MVP sous forme de fichier ZIP.
- 5 Enregistrez le fichier ZIP.

Via le système de fichiers

- 1 Sur le système où s'exécute le serveur MVP, naviguez jusqu'au dossier d'installation du serveur MVP.
- 2 Comprimez le dossier Data sous forme de fichier ZIP.

Importation des données dans MVE

- 1 Connectez-vous à MarkVision Enterprise.
- 2 Dans la boîte de dialogue « Importer des données de MarkVision Professional », cliquez sur **Oui**, puis cliquez sur **Parcourir**.

Remarques :

- Si vous cliquez sur **Oui**, la boîte de dialogue ne s'affichera pas la prochaine fois que vous vous connectez à MVE.
- Si vous cliquez sur **Non** et ne souhaitez pas que cette boîte de dialogue apparaisse de nouveau, sélectionnez **Ne plus afficher ce message**.

- 3 Naviguez jusqu'à l'emplacement contenant votre fichier ZIP, sélectionnez-le, puis cliquez sur **Ouvrir**.
- 4 Dans la zone Données à importer, sélectionnez le type de données que vous souhaitez importer.

Données	Détails
Utilisateurs	<ul style="list-style-type: none"> • Dans MarkVision Professional, les utilisateurs se voient attribuer des droits fonction par fonction. • Dans MarkVision Enterprise, les utilisateurs se voient affecter des rôles correspondant à différentes fonctions. • Les utilisateurs importés depuis MVP reçoivent automatiquement tous les rôles, sauf ROLE_ADMIN. • Si le mot de passe d'un utilisateur MVP ne satisfait pas les critères de mot de passe MVE, la chaîne Administrator1 est ajoutée après son mot de passe actuel.

Données	Détails
Périphériques	<ul style="list-style-type: none"> • MVE n'importe de MVP que les informations de base sur les périphériques telles que les noms de modèle, numéros de série, adresses MAC et adresses IP. • Si une imprimante existe déjà dans MVE, cette imprimante est ignorée lors de l'importation. • Lors de l'importation, MVE ignore également les imprimantes connectées à des adaptateurs réseau externes (ENA), puisque MVE ne prend pas en charge les ENA. • Les périphériques importés prennent automatiquement l'état du cycle de vie Géré (Normal). • MVP gère les imprimantes et les serveurs d'imprimante. MVE gère seulement les imprimantes. Deux entrées dans MVP donnent donc une seule entrée dans MVE.
Profils de recherche	<ul style="list-style-type: none"> • Lorsque les profils MVP sont importés dans le système MVE, seuls sont importés les détails suivants : <ul style="list-style-type: none"> – Nom de communauté SNMP – Nouvelles tentatives – Délai dépassé – Exclure adresse – Inclure adresse • Dans MVP, chaque entrée Inclure/Exclure contient un ensemble de noms de communauté lecture/écriture SNMP. Un profil contenant plusieurs entrées Inclure/Exclure peut aussi contenir plusieurs ensembles de noms de communauté lecture/écriture. Dans MVE, l'ensemble de noms de communauté lecture/écriture appartient au profil lui-même. Chaque profil contient un seul ensemble de noms de communauté lecture/écriture. Ainsi, un profil de recherche dans MVP (contenant plusieurs ensembles de noms de communauté lecture/écriture) est décomposé en autant de profils de recherche lors de l'importation dans MVE (chaque profil contenant un ensemble de noms de communauté lecture/écriture). Le nombre de profils dans MVE est égal au nombre d'ensembles de noms de communauté lecture/écriture uniques dans le profil MVP d'origine. • Pour le paramètre Délai dépassé, MVE convertit le délai MVP en millisecondes en multipliant la valeur MVP (en secondes) par 1000. • L'option Gérer automatiquement est définie sur Faux lors de l'importation.

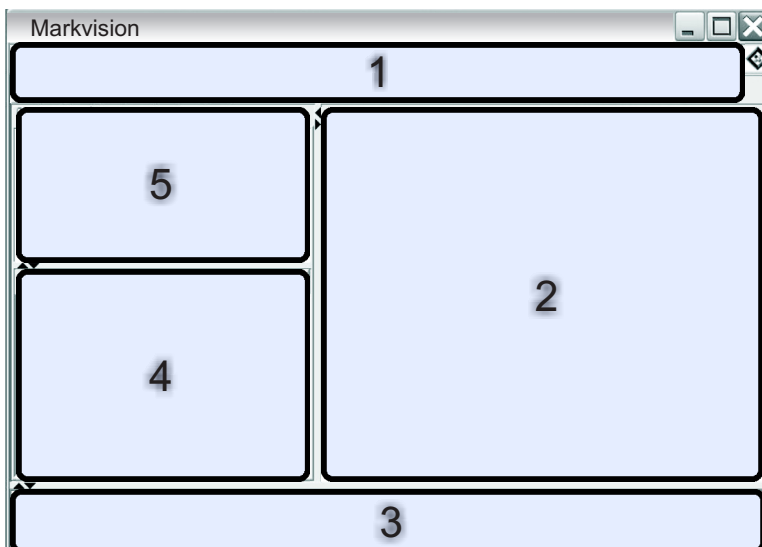
5 Cliquez sur **Importer**.

Utilisation de MarkVision

Les fonctions disponibles dans MarkVision sont réparties entre quatre zones de service. Une telle organisation facilite l'utilisation, chaque vue de l'interface n'affichant que les fonctions nécessaires à la tâche en question. Chaque zone de service est accessible par le biais d'un onglet dans l'écran d'accueil et correspond à une étape du cycle de vie utile dans la bibliothèque ITIL (Information Technology Infrastructure Library) version 3. La méthodologie ITIL est reconnue mondialement comme somme des meilleures pratiques pour la gestion des ressources informatiques au sein d'une organisation.

Utilisez cet onglet	Pour
Actifs	<p>Rechercher, identifier, cataloguer, organiser et suivre les actifs physiques (imprimantes et périphériques multi-fonctions) qui composent votre parc d'impression. Cet onglet permet de recueillir et mettre à jour les informations concernant différents aspects du parc : modèles, fonctions, options installées, cycle de vie.</p> <p>Dans ITIL, cela correspond à la zone « Service Transition ».</p> <p>Si la gestion des actifs informatiques fait partie de vos responsabilités, reportez-vous à « Gestion des actifs », page 18.</p>
Stratégies	<p>Définir et gérer la configuration logicielle du parc d'impression. Cet onglet permet d'attribuer une stratégie qui spécifie les paramètres de configuration propres à chaque modèle. Vous pouvez vérifier que le parc d'impression est conforme aux stratégies et mettre ces stratégies en œuvre si nécessaire.</p> <p>Dans ITIL, cela correspond à la zone « Service Transition ».</p> <p>Si l'administration et la maintenance des outils de gestion de la configuration font partie de vos responsabilités, reportez-vous à « Gestion des polices », page 30.</p>
Service Desk	<p>Interagir directement avec un périphérique particulier du parc. Cet onglet permet de gérer le périphérique à distance, de contrôler la conformité et de mettre en œuvre des stratégies, ainsi que de personnaliser les paramètres de configuration via le serveur Web intégré au périphérique.</p> <p>Dans ITIL, cela correspond à la zone « Service Operation ».</p> <p>Si la gestion ou l'administration des services d'assistance informatique aux utilisateurs fait partie de vos responsabilités, reportez-vous à « Gestion du Service Desk », page 43.</p>
Gestionnaire des événements	<p>Créer un événement automatisé lorsqu'un périphérique envoie une alerte au réseau. Vous pouvez envoyer un e-mail ou effectuer d'autres actions scriptées pour informer les personnes désignées.</p> <p>Dans ITIL, cela correspond à la zone « Service Operation ».</p> <p>Si la gestion des problèmes ou la réponse aux incidents fait partie de vos responsabilités, reportez-vous à « Gestion des événements de périphériques », page 45.</p>

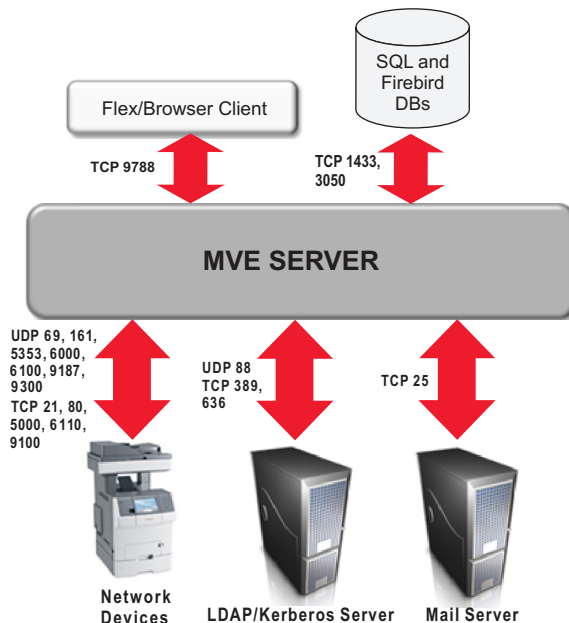
Présentation de l'écran d'accueil



Utilisez cette section		Pour
1	En-tête	Accéder aux quatre onglets de service et effectuer d'autres tâches administratives.
2	Résultats de la recherche	Afficher la liste complète paginée des périphériques correspondant au signet ou à la recherche actuellement sélectionnés.
3	Informations sur les tâches	Afficher le statut de l'activité la plus récente.
4	Récapitulatif des résultats de la recherche	Afficher un récapitulatif catégorisé du signet ou de la recherche actuellement sélectionnés.
5	Signets ou Recherche avancée	Gérer et sélectionner des signets et affiner les requêtes de recherche.

Présentation des ports et protocoles

MarkVision utilise différents ports et protocoles pour différents types de communication réseau, comme illustré dans le diagramme ci-dessous.



Remarque : Les ports sont bidirectionnels et doivent être ouverts ou actifs pour que MarkVision puisse fonctionner correctement. Vérifiez que les ports de tous les périphériques sont réglés sur sur **Activé**, selon le périphérique **Sécurisé et non sécurisé** ou sur **Activé**, selon le périphérique.

Communication du serveur vers le périphérique

Voici les ports et protocoles utilisés pour la communication entre le serveur MarkVision et les périphériques réseau.

Protocole	Serveur MarkVision	Périphérique	Utilisé pour
NPAP <i>Network Printer Alliance Protocol</i>	Port (UDP) <i>User Datagram Protocol</i> éphémère	UDP 9300	Communication avec les imprimantes réseau Lexmark
XMLNT <i>XML Network Transport</i> (référentiel d'objets)	Ports UDP et TCP <i>Transmission Control Protocol</i> éphémères	UDP 6000 TCP 5000	Communication avec les imprimantes réseau Lexmark
LST <i>Lexmark Secure Transport</i>	UDP 6100 Port TCP éphémère (signaux de reconnaissance)	UDP 6100 TCP 6110 (signaux de reconnaissance)	Communication cryptée avec les imprimantes réseau Lexmark
mDNS <i>Multicast Domain Name System</i>	Port UDP éphémère	UDP 5353	Détection de certaines imprimantes réseau Lexmark et détermination des fonctions de sécurité des périphériques

Protocole	Serveur MarkVision	Périphérique	Utilisé pour
SNMP <i>protocole SNMP (Simple Network Management Protocol)</i>	Port UDP éphémère	UDP 161	Détection des imprimantes réseau de Lexmark et d'autres marques et communication avec celles-ci
FTP <i>File Transfer Protocol</i>	Port TCP éphémère	TCP 21	Téléchargements de fichiers génériques
TFTP <i>Trivial File Transfer Protocol</i>	Port UDP éphémère	UDP 69	Mises à jour du microcode et téléchargements de fichiers génériques
HTTP <i>Hypertext Transfer Protocol</i>	Port TCP éphémère	TCP 80	Téléchargements de fichiers génériques
Port d'impression brute	Port TCP éphémère	TCP 9100	Téléchargements de fichiers génériques

Communication des périphériques vers le serveur

Il s'agit du port et du protocole utilisés pour la communication entre les périphériques réseau et le serveur MarkVision.

Protocole	Périphérique	Serveur MarkVision	Utilisé pour
NPAP	UDP 9300	UDP 9187	Génération et réception d'alertes

Communication du serveur vers les bases de données

Il s'agit des ports et protocoles utilisés pour la communication entre le serveur MarkVision et les bases de données.

Serveur MarkVision	Base de données	Utilisé pour
Port TCP éphémère	TCP 1433 (SQL Server) Port par défaut, configurable par l'utilisateur.	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

Il s'agit du port et du protocole utilisés pour la communication entre le client flex/navigateur et le serveur MarkVision.

Protocole	Client flex/navigateur	Serveur MarkVision
AMF <i>ActionScript Message Format</i>	Port TCP	TCP 9788

Messagerie et alertes

Il s'agit du port et du protocole utilisés pour la communication entre le serveur MarkVision et un serveur de messagerie électronique.

Protocole	Serveur MarkVision	Serveur SMTP	Utilisé pour
SMTP <i>Simple Mail Transfer Protocol</i>	Port TCP éphémère	TCP 25 Port par défaut, configurable par l'utilisateur.	Fournit la fonction de courrier électronique permettant de recevoir des alertes des périphériques

Communication du serveur MarkVision vers le serveur LDAP

Il s'agit des ports et protocoles utilisés pour les communications visant à l'identification des utilisateurs et des groupes.

Protocole	Serveur MarkVision	Serveur LDAP	Utilisé pour
LDAP <i>Lightweight Directory Access Protocol</i>	Port TCP éphémère	TCP 389, ou le port que le serveur LDAP est configuré pour écouter	Authentification des utilisateurs MarkVision Enterprise par un serveur LDAP
LDAPS <i>Secure Lightweight Directory Access Protocol</i>	Port TCP éphémère	<i>Transport Layer Security (TLS)</i> , ou le port que le serveur LDAP est configuré pour écouter Utilisé pour les connexions cryptées TLS.	Authentification des utilisateurs MarkVision Enterprise par un serveur LDAP via un canal sécurisé qui utilise TLS.
Kerberos	Port UDP éphémère	UDP 88 Il s'agit du port par défaut pour le service d'authentification Kerberos.	Authentification Kerberos

Gestion des actifs

Découverte de périphériques

L'application permet de rechercher des périphériques sur le réseau. Lorsque des périphériques sont détectés, les informations d'identification correspondantes sont enregistrées sur le système. Utilisez les signets ou les recherches pour afficher les périphériques dans la zone des résultats de recherche.

Les périphériques détectés prennent par défaut l'état **Nouveau** et ne sont pas gérés par le système. Avant de pouvoir effectuer une opération sur un périphérique, vous devez le définir sur l'état **Géré**. Pour plus d'informations, reportez-vous à la section « Gestion des périphériques », page 21.

Il y a deux manières d'ajouter des périphériques au système :


- **Utilisation d'un profil de recherche** : permet de détecter les périphériques du réseau selon des paramètres personnalisés.
- **Importation de périphériques depuis un fichier** : vous importez des périphériques à partir d'un *fichier de valeurs séparées par des virgules (CSV)*.

Remarque : Vous ne pouvez utiliser qu'une de ces deux méthodes. Ajouter des périphériques au système en utilisant les deux procédures entraînerait des périphériques en double.

Après l'ajout d'un périphérique au système, exécutez immédiatement un audit du périphérique. L'exécution d'un audit fournit des informations supplémentaires sur le périphérique, celles-ci étant nécessaires à l'exécution correcte de certaines tâches. Pour plus d'informations sur l'audit d'un périphérique, reportez-vous à la section « Audit d'un périphérique », page 22.

Remarque : Remarque : Cela s'applique *uniquement* aux périphériques non restreints. Pour les périphériques restreints, affectez d'abord une stratégie de sécurité, puis mettez-la en œuvre sur les périphériques restreints avant de procéder à l'audit. Sinon, l'audit échouera et les périphériques restreints prendront l'état **Géré (Manquant)**. Pour plus d'informations sur les périphériques restreints, reportez-vous à la section « Présentation des périphériques sécurisés », page 31.

Création d'un profil de recherche

- 1 Si nécessaire, cliquez sur **Profils de recherche** dans l'onglet Ressources pour afficher la section Profils de recherche.
- 2 Cliquez sur **+**, puis tapez le nom du nouveau profil de recherche.
- 3 Dans l'onglet Adresses, sélectionnez **Inclure** ou **Exclure**.
- 4 Pour importer d'un fichier la liste des éléments à inclure ou exclure, procédez comme suit :
 - a Cliquez sur .
 - b Naviguez jusqu'au dossier contenant le fichier.
 - c Sélectionnez le fichier puis cliquez sur **Ouvrir**.

Remarque : Le fichier peut contenir n'importe quelle séquence susceptible d'être saisie dans le champ de texte au-dessus de Adresse/Plage. Pour afficher des exemples de séquence valide, passez la souris par-dessus le champ de texte.

5 A côté de **+**, tapez l'adresse IP, le nom d'hôte DNS complet, les sous-réseaux avec caractères génériques, ou encore les plages d'adresses désirées, puis cliquez sur **+**.

Remarques :

- Vous ne pouvez taper qu'une entrée à la fois. Pour afficher des exemples d'entrée valide, passez la souris par-dessus le champ de texte situé au-dessus de Adresse/Plage.
- Lorsque vous tapez des plages d'adresses, n'utilisez *pas* de caractères génériques.
- Pour supprimer une entrée, sélectionnez-la, puis cliquez sur **—**.

6 Cliquez sur l'onglet **SNMP**, puis sélectionnez **Version 1,2c** ou **Version 3**.

Remarque : Si vous ne connaissez pas avec certitude la version de SNMP que vous utilisez, contactez le technicien de support système.

7 Si vous avez sélectionné **Version 1,2c** dans étape 6, définissez le profil de confidentialité à partir de la zone Noms de communauté.

Si vous avez sélectionné **Version 3**, définissez le profil de sécurité à partir de la zone Sécurité.

Remarque : Si vous n'êtes pas certain de la manière dont il faut configurer le profil de sécurité SNMP Version 3, contactez le technicien de support système.

8 Cliquez sur l'onglet **Général**, puis dans la zone Performances, procédez comme suit :

- Dans le champ Délai, spécifiez la durée (en millisecondes) d'attente de la réponse des périphériques.
- Dans le champ Tentatives, spécifiez le nombre de tentatives de communication avec un périphérique qui sont exécutées avant que le système abandonne cette tâche.

9 Spécifiez si vous souhaitez inclure les périphériques sécurisés dans la recherche.

Remarques :

- En l'absence de périphérique sécurisé, laissez cette option *désactivée*. Dans le cas contraire, les résultats seront affectés et la détection des périphériques prendra beaucoup plus de temps.
- Lorsqu'un périphérique est sécurisé, une et/ou l'autre conditions ci-dessous s'appliquent : (a) les ports de communication sont désactivés et (b) une authentification est nécessaire pour obtenir des informations du périphérique.

10 Spécifiez si le profil de recherche doit automatiquement gérer les périphériques détectés.



Remarque : Si vous activez cette option, tous les périphériques détectés prennent automatiquement l'état de cycle de vie **Géré**.

11 Cliquez sur **Enregistrer >Fermer**.

Remarques :

- Si vous cliquez sur **►**, le profil de recherche est exécuté, mais il n'est *pas* enregistré.
- Un nouveau profil de recherche recueille juste assez d'informations pour permettre l'identification fiable d'un périphérique. Pour récupérer les informations complètes sur un périphérique, définissez l'état du périphérique sur **Géré**, puis pratiquez son audit.
- Pour vous assurer que les informations du périphérique sont à jour, vous pouvez planifier une recherche à intervalle régulier. Pour plus d'informations, reportez-vous à la section « Planification de tâches », page 56.

Modification ou suppression d'un profil de recherche

- 1 Si nécessaire, cliquez sur **Profils de recherche** dans l'onglet Ressources pour afficher la section Profils de recherche.
- 2 Sélectionnez un profil, puis cliquez sur  pour apporter des modification ou sur  pour supprimer le profil de recherche.
- 3 Suivez les instructions à l'écran.

Importation de périphériques à partir d'un fichier

Vous pouvez importer des périphériques depuis un fichier de valeurs séparées par des virgules (CSV).

Remarque : MarkVision vous permet ainsi de préparer un déploiement en ajoutant les périphériques au système *avant* même qu'ils soient disponibles sur le réseau.

- 1 Dans l'onglet Ressources, cliquez sur **Importer**, puis sur **Parcourir**.
- 2 Naviguez jusqu'au dossier contenant le fichier CSV.
Remarque : Vérifiez qu'il y a bien un périphérique par ligne dans le fichier CSV.
- 3 Sélectionnez le fichier CSV, puis cliquez sur **Ouvrir**.
- 4 Dans la section Colonnes possibles, sélectionnez les colonnes à mettre en correspondance avec les valeurs du fichier CSV.
- 5 Si vous communiquez avec le périphérique à l'aide du protocole SNMP V3, vous *devez* sélectionner les colonnes suivantes :

- **Utilisateur lecture/écriture SNMP V3**
- **Mot de passe lecture/écriture SNMP V3**
- **Niveau d'authentification minimal SNMP V3**
- **Hachage d'authentification SNMP V3**
- **Algorithme autorisé SNMP V3**

Remarque : Dans le fichier CSV que vous avez sélectionné dans étape 3, assurez-vous que les paramètres suivants contiennent une des valeurs spécifiées à leur suite :

- Niveau d'authentification minimal
 - **NO_AUTHENTICATION_NO_PRIVACY**
 - **AUTHENTICATION_NO_PRIVACY**
 - **AUTHENTICATION_PRIVACY**
- Hachage d'authentification
 - **MD5**
 - **SHA1**
- Algorithme autorisé
 - **DES**
 - **AES_128**

- AES_192
- AES_256

Remarque : Si votre fichier CSV ne contient pas les valeurs exactes spécifiées, MVE ne peut pas découvrir le périphérique.

- 6 Cliquez sur **Ajouter** pour faire passer les colonnes sélectionnées dans la liste des colonnes du fichier CSV.
 - Si vous souhaitez que le système ignore une colonne du fichier CSV, sélectionnez **Ignorer**. Répétez la procédure pour chaque colonne du fichier CSV qui n'apparaît pas encore dans la section Colonnes possibles.
 - Pour changer l'ordre des colonnes à mettre en correspondance avec le fichier CSV, sélectionnez une colonne dans la liste des colonnes du fichier CSV, puis utilisez les flèches pour déplacer les en-têtes vers le haut ou vers le bas.
- 7 Spécifiez si la première ligne du fichier CSV contient un en-tête.
- 8 Spécifiez si les périphériques importés doivent automatiquement prendre l'état de cycle de vie **Géré**.
- 9 Cliquez sur **OK**.

Gestion des périphériques

Un périphérique peut se voir attribuer trois états de cycle de vie :

- **Géré** : le périphérique est inclus dans toutes les activités effectuées au sein du système.
 - **Géré (Normal)** : le périphérique est dans son état régulier.
 - **Géré (Modifié)** : les propriétés physiques du périphérique ont été modifiées depuis le dernier audit. A la prochaine communication du système avec le périphérique, s'il n'y a pas d'autre changement dans les propriétés physiques, l'état redevient Géré (Normal).
 - **Géré (Manquant)** : le système ne parvient pas à communiquer avec le périphérique. A la prochaine tentative, si le système parvient à communiquer avec le périphérique et qu'il n'y a pas de changement dans les propriétés physiques, l'état devient Géré (Trouvé).
 - **Géré (Trouvé)** : le périphérique, précédemment manquant, est à même de communiquer avec le système lors de la dernière tentative. A la prochaine tentative, si le système parvient à communiquer avec le périphérique et qu'il n'y a pas de changement dans les propriétés physiques, l'état devient Géré (Normal).
- **Non géré** : le périphérique est exclu de toutes les activités effectuées au sein du système.
- **Retiré** : le périphérique était précédemment dans l'état Géré mais a maintenant été retiré du réseau. Le système conserve les informations du périphérique mais ne s'attend pas à détecter de nouveau le périphérique sur le réseau. Si le périphérique réapparaît sur le réseau, le système le traitera comme un nouveau périphérique.

Définition de l'état du cycle de vie du périphérique

Avant de pouvoir effectuer une opération sur un périphérique, vous devez le définir sur l'état **Géré**.

- 1 Dans l'onglet Actifs, sélectionnez **Nouvelles imprimantes** dans le menu déroulant Signets et recherches.
- 2 Cochez la case en regard de l'adresse IP du périphérique.

Remarque : Vous pouvez sélectionner plusieurs périphériques, voire tous.

- 3 Dans le menu déroulant Définir l'état sur, sélectionnez **Géré**, puis cliquez sur **Oui**.

Audit d'un périphérique

La fonction d'audit permet de recueillir les informations de n'importe quels périphériques gérés sur le réseau, puis de stocker ces informations dans le système. Un audit régulier permet d'assurer que les informations du système sont à jour.


1 Dans la zone des résultats de recherche, cochez la case en regard de l'adresse IP d'un périphérique.

Remarques :

- Si vous ne connaissez pas l'adresse IP, recherchez le périphérique dans les colonnes Nom du système ou Nom d'hôte.
- Pour auditer plusieurs périphériques, cochez la case en regard de l'adresse IP de ceux-ci.
- Pour auditer tous les périphériques, cochez la case en regard de l'en-tête « Adresse IP ».

2 Cliquez sur **Auditer**.

L'état de l'audit s'affiche dans la zone d'informations sur les tâches.

3 Lorsque l'audit est terminé, cliquez sur  dans l'en-tête.

Les résultats du dernier audit sont affichés dans la boîte de dialogue Journal.

Une fois les périphériques audités, le système peut les faire passer à l'état **Géré (Modifié)** dans les cas suivants :

- Des modifications ont été apportées à certaines valeurs d'identification de ces périphériques ou à certaines de leurs fonctionnalités :
 - Identifiant de l'imprimante
 - Nom d'hôte
 - Nom du contact
 - Emplacement du contact
 - Adresse IP
 - Taille de la mémoire
 - Nom de l'option de copie
 - Recto verso
- Ajouts ou retraits des options matérielles suivantes du périphérique :
 - Fournitures
 - Options d'entrée
 - Options de sortie
 - Ports
- Ajouts ou suppressions des fonctions ou applications suivantes du périphérique :
 - Polices
 - Applications eSF

Remarque : Vous pouvez planifier l'exécution d'un audit à une heure donnée ou à intervalle fixe. Pour plus d'informations, reportez-vous à la section « Planification de tâches », page 56.

Affichage des propriétés d'un périphérique

Pour voir la liste complète des informations relatives au périphérique, vous devez avoir préalablement exécuté un audit du périphérique.

- 1 Dans l'onglet Actifs, sélectionnez **Imprimantes gérées** dans le menu déroulant Signets et recherches.
- 2 Dans la section Toutes les imprimantes, sélectionnez l'adresse IP du périphérique.

Remarque : Si vous ne connaissez pas l'adresse IP, recherchez le périphérique dans la colonne Nom du système.

- 3 Dans la boîte de dialogue Propriétés de l'actif :

Cliquez sur	Pour afficher
Identification	Les informations d'identification réseau du périphérique.
Dates	La liste des événements du périphérique. Sont notamment indiquées la date d'ajout dans le système, la date de détection et la date du dernier audit.
Microcode	Niveaux du microcode du périphérique.
Possibilités	Fonctions offertes par le périphérique.
Ports	Ports disponibles sur le périphérique.
Fournitures	Niveaux et détails des fournitures dans le périphérique.
Cartouches de polices	Informations sur les cartouches de polices installées.
Options	Informations sur les options du périphérique, comme le disque dur et l'espace libre sur ce disque.
Options d'alimentation	Paramètres des tiroirs papier disponibles et autres entrées du périphérique.
Options de sortie	Paramètres des tiroirs de sortie papier disponibles.
Applications eSF	Informations sur les applications <i>Embedded Solutions Framework</i> (eSF) installées sur le périphérique, telles que numéro de version et l'état.
Statistiques du périphérique	Valeurs spécifiques pour chacune des propriétés du périphérique.
Détails des modifications	Informations sur les modifications apportées sur le périphérique. Remarque : Cela s'applique <i>uniquement</i> aux périphériques définis dans l'état Géré (Modifié) .

Localisation et organisation des périphériques du système.

Recherche de périphériques système

Utilisation des signets par défaut

Les signets montrent une recherche de périphérique enregistrée. Lors de la sélection d'un signet, les périphériques repris correspondent aux critères de la recherche.

Les signets par défaut sont basés sur l'état du cycle de vie du périphérique.

- 1 Sélectionnez les Signets et les Recherches depuis le menu-déroulant

Sélectionner	A
Imprimantes gérées	Recherche de périphériques actifs dans le système. Remarque : Les périphériques qui apparaissent lors de la sélection du signet peuvent être dans l'un des états suivant: <ul style="list-style-type: none"> • Géré (Normal) • Géré (Modifié) • Géré (Manquant) • Géré (Trouvé)
Imprimantes Gérées (Normales)	Recherche de périphériques actifs dans le système avec des propriétés spécifiques restées les mêmes depuis le dernier audit.
Imprimantes Gérées (Modifiées)	Recherche de périphériques actifs dans le système avec des propriétés spécifiques restées les mêmes depuis le dernier audit.
Imprimantes Gérées (Manquantes)	Recherche de périphériques pour lesquels le système n'a pas été capable de communiquer.
Imprimantes Gérées (Trouvées)	Recherche de périphériques rapportés comme manquant lors de la recherche précédente mais qui ont été trouvés maintenant.
Nouvelles imprimantes	Recherche de périphériques ajoutés récemment au système.
Imprimantes non-gérées	Recherche de périphériques qui ont été exclus des activités exécutées par le système.
Imprimantes hors-service	Recherche de périphériques qui ne sont plus actifs dans le système.

- 2 Sélectionnez un critère pour restreindre rapidement et facilement les résultats produits par vos recherches favorites.

Utiliser la Recherche avancée.

La possibilité de recherche avancée, vous permet de réaliser rapidement des recherches complexes basée sur un ou plusieurs paramètres.

- 1 Sélectionnez la **Recherche avancée** à partir des Signets et des Recherches du menu-déroulant
- 2 Sélectionnez soit un ou tous les critères

3 Pour ajouter un critère de recherche, cliquer sur **+**.

Pour grouper des critères de recherche ensemble, cliquer sur **[+]**, et cliquer ensuite sur **+** pour ajouter un critère individuel.

Remarque : Si vous groupez des critères de recherche, le système traite tous les critères groupés ensemble comme s'ils ne faisaient qu'un.

4 Sélectionnez un paramètre du menu-déroulant Paramètre.

Sélectionner	A
Numéro d'inventaire	Recherche de périphériques qui ont un numéro d'inventaire
Capacité Couleur	Recherche de périphériques selon la possibilité d'imprimer en couleur
Localisation de contact	Recherche de périphériques qui se situe à un endroit spécifique
Nom du contact	Recherche de périphériques qui ont un nom de contact spécifique
Capacité de copie	Recherche de périphériques selon leur capacité de copie
Capacité Duplex	Recherche de périphériques qui peuvent réaliser des impressions recto-verso
capacité ESF	Recherche de périphériques qui peuvent gérer l'application Embedded Solutions Framework (eSF)
Application eSF (Nom)	Recherche de périphériques par le nom spécifique de l'application eSF installée
Application eSF (Etat)	Recherche de périphériques selon l'état de l'application eSF installée
Application eSF (Version)	Recherche de périphériques selon la version de l'application eSF installée.
Version du Firmware	Recherche de périphériques en fonction de la version de leur firmware.
Firmware AIO	Recherche de périphériques selon la valeur AIO de leur firmware
Firmware:Base	Recherche de périphériques selon la version de base de leur firmware
Firmware:Moteur	Recherche de périphériques selon le moteur de leur firmware.
Firmware:Fax	Recherche de périphériques selon la valeur fax de leur firmware
Firmware:Font	Recherche de périphériques selon la valeur font de leur firmware.
Firmware:Kernel	Recherche de périphériques selon la valeur du kernel de leur firmware.
Firmware:Chargeur	Recherche de périphériques selon la valeur du chargeur de leur firmware.
Firmware:Réseau	Recherche de périphériques selon la valeur réseau de leur firmware.
Firmware:Pilote Réseau	Recherche de périphériques selon la valeur du pilote réseau de leur firmware.
Firmware:Panneau	Recherche de périphériques selon la version du panneau de leur firmware.
Firmware:Scanner	Recherche de périphériques selon la version du scanner de leur firmware.
Nom de l'Hôte	Recherche de périphériques par leur nom d'hôte.
Adresse IP	<p>Recherche de périphériques par leur adresse IP.</p> <p>Remarque : Vous pouvez utiliser une astérisque (*) comme caractère passe partout à la place des trois derniers octets de l'adresse IP pour trouver toutes les adresses IP qui correspondent. Si une astérisque est utilisée dans un octet, les autres octets restants doivent être également des astérisques</p> <ul style="list-style-type: none"> • Voici quelques exemples valident 157.184.32.*, 157.184.*.*, et 157.*.*.*. • Voici un <i>exemple non-valide</i>: 157.184.*.10.
mot clé	Recherche de périphériques selon leurs mots-clés assignés, si ils en ont

Sélectionner	A
Compteur de page	Recherche de périphériques selon la valeur de leur compteur à vie de pages.
Adresse MAC	Recherche de périphériques par leur adresse MAC.
Compteur de maintenance	Recherche de périphériques selon la valeur de leur compteur de maintenance.
Fabricant	Recherche de périphériques selon le moteur de leur fabricant.
Capacité MFP	Recherche de périphériques qui peuvent réaliser des impressions multifonction (MFP).
Technologie de marquage	Recherche de périphériques en fonction de la technologie de marquage qu'ils supportent
Modèle	Recherche de périphériques par leur nom de modèle.
Etats Imprimante	Recherche de périphériques selon leurs statuts (par exemple: Pret, Bourrage papier, Bac 1 Manquant).
Capacité de profil	Recherche de périphériques selon leurs capacités de profils supportés.
Capacité à recevoir des fax	Recherche de périphériques qui peuvent recevoir des fax
Capacité de scanner vers e-mail	Recherche de périphériques qui peuvent réaliser une tâche de scan vers courriel.
Capacité de scanner vers fax	Recherche de périphériques qui peuvent réaliser une tâche de scan vers fax.
Capacité de scanner vers réseau	Recherche de périphériques qui peuvent réaliser une tâche de scan vers réseau.
Numéro de série	Recherche de périphériques selon leurs numéros de série.
État	Recherche de périphériques selon leurs statuts dans la base de données.
Etat de l'alimentation	Recherche de périphériques selon l'état d'alimentation.
Nom du système	Recherche de périphériques selon leur nom.

5 Sélectionnez un opérateur selon le menu déroulant Opération

Sélectionner	A
Contient	Recherche de périphériques avec un paramètre qui contient une valeur spécifique
Ne contient pas	Recherche de périphériques avec un paramètre qui ne contient pas une valeur spécifique
N'est pas égal à	Recherche de périphériques avec un paramètre qui n'est pas égal à une valeur spécifique
Fini par	Recherche de périphériques avec un paramètre qui ne finit pas par une valeur spécifique
Egal	Recherche de périphériques avec un paramètre qui est égal à une valeur spécifique
Début par	Recherche de périphériques avec un paramètre qui commence par une valeur spécifique

6 Entrez la valeur du paramètre dans le champ Valeur ou dans le menu déroulant

Remarque : Si vous voulez supprimer le critère, cliquez sur **X**.

7 Cliquez sur **OK** pour commencer la recherche.

Les périphériques repris dans les résultats de recherche apparaissent dans cette zone.


8 Sélectionnez un critère pour restreindre rapidement et facilement les résultats produits par vos recherches favorites.

Travailler avec des signets

Les signets montrent une recherche de périphérique enregistrée

Quand un périphérique est ajouté au système et correspond aux critères spécifiés pour un signet, le périphérique est inclu dans les résultats de recherche lorsque le signet est sélectionné.

Création de signets

- 1 Dans le menu déroulant Signets et recherches, sélectionnez le signet correspondant au groupe de périphériques à partir duquel vous souhaitez lancer votre recherche.
Pour affiner la recherche, cliquez sur **Recherche avancée**.
- 2 Si nécessaire, dans le récapitulatif des résultats de la recherche, cliquez sur les sous-catégories disponibles pour affiner encore votre recherche.
- 3 Lorsque le périphérique ou groupe de périphériques souhaité apparaît dans la fenêtre de recherche, cliquez sur  .
- 4 Entrez un nom pour le signet, puis cliquez sur **OK**.

Accès aux signets

- 1 Dans le menu déroulant Signets et recherches, sélectionnez le signet à afficher.
- 2 Si nécessaire, dans le récapitulatif des résultats de la recherche, cliquez sur les sous-catégories disponibles pour affiner encore votre recherche.

Suppression de signets

- 1 Dans le menu déroulant Signets et recherches, sélectionnez **Gérer les signets**.
- 2 Sélectionnez le ou les signets à supprimer, puis cliquez sur **—**.
- 3 Cliquez sur **Oui**, puis sur **Fermer**.

Utilisation de catégories et de mots-clés


Les mots clés permettent d'attribuer aux périphériques des étiquettes personnalisées, ce qui permet de retrouver et d'organiser plus facilement les périphériques au sein du système. Vous pouvez grouper les mots clés en catégories, puis attribuer plusieurs mots clés de différentes catégories à un même périphérique.

Avant de créer un mot clé, vous devez créer la catégorie à laquelle il appartient.

Par exemple, vous pourriez créer une catégorie appelée **Emplacement**, puis créer des mots clés à l'intérieur de cette catégorie. Cette catégorie Emplacement pourrait ainsi contenir des mots clés tels que **Bâtiment 1**, **Bâtiment 2**, etc. ou des intitulés plus spécifiques, selon les besoins de votre entreprise.

Après avoir créé les catégories et les mots clés, vous pouvez attribuer les mots clés à plusieurs périphériques. Vous pouvez rechercher des périphériques d'après les mots clés qui leur sont associés, puis mémoriser les résultats de cette recherche sous la forme d'un signet pour utilisation ultérieure.

Ajout, modification ou suppression de catégories


- 1 Si nécessaire, dans l'onglet Actifs, cliquez sur **Mots clés** pour afficher la section Mots clés.
- 2 Dans le volet Catégorie, cliquez sur **+** pour ajouter, sur  pour modifier ou sur **—** pour supprimer une catégorie.

Remarque : La suppression d'une catégorie entraîne également la suppression de ses mots clés et les supprimera de tous les périphériques auxquels ils sont associés.

- 3 Suivez les instructions à l'écran.

Ajout, modification ou suppression de mots clés

- 1 Si nécessaire, dans l'onglet Actifs, cliquez sur **Mots clés** pour afficher la section Mots clés.
- 2 Dans le volet Mots clés, effectuez l'une des opérations suivantes :

- Pour ajouter un mot clé :
 - a Dans le volet Catégorie, sélectionnez la catégorie à laquelle appartient le mot clé.
 - b Dans le volet Mots clés, cliquez sur **+**.
 - c Tapez le nom du nouveau mot clé, puis appuyez sur **Entrée**.
- Pour modifier un mot clé :
 - a Sélectionnez un mot clé, puis cliquez sur .
 - b Modifiez l'intitulé, puis appuyez sur **Entrée**.
- Pour supprimer un mot clé :
 - a Sélectionnez un mot clé, puis cliquez sur **—**.
 - b Cliquez sur **Oui**.

Remarque : La suppression d'un mot clé entraîne également sa suppression de tous les périphériques auxquels il est associé.


Attribution de mots clés à un périphérique

- 1 Si nécessaire, dans l'onglet Actifs, cliquez sur **Mots clés** pour afficher la section Mots clés, puis sélectionnez un mot clé.

Remarque : Pour sélectionner plusieurs mots clés, utilisez **Maj + clic** ou **Ctrl + clic**.

- 2 Cochez l'adresse IP du périphérique auquel vous souhaitez attribuer le mot clé.

Remarque : Vous pouvez sélectionner plusieurs périphériques, voire tous.


- 3 Cliquez sur .

- 4 Dans la zone des informations sur les tâches, vérifiez que la tâche est terminée.

- 5 Pour vérifier que le mot clé a bien été attribué au périphérique, consultez les propriétés du périphérique en sélectionnant son adresse IP.

Dans la section Propriété d'identification, la nouvelle valeur du mot clé pour le périphérique apparaît.

Suppression d'un mot clé attribué sur un périphérique

- 1 Dans l'onglet Actifs, cochez la case en regard de l'adresse IP du périphérique duquel vous souhaitez supprimer un mot clé.
- 2 Si nécessaire cliquez sur **Mots clés** pour afficher la section Mots clés.
- 3 Sélectionnez un mot clé, puis cliquez sur  .
- 4 Sélectionnez le mot clé à supprimer, puis cliquez sur **OK**.
Remarque : Pour sélectionner plusieurs mots clés, utilisez **Maj + clic** ou **Ctrl + clic**.
- 5 Dans la zone des informations sur les tâches, vérifiez que la tâche est terminée.
- 6 Pour vérifier que le mot clé a bien été supprimé du périphérique, procédez comme suit :
 - a Sélectionnez l'adresse IP du périphérique.
 - b Dans la section Propriété d'identification, vérifiez que le mot clé n'apparaît plus.

Gestion des polices

Une stratégie est un ensemble d'informations de configuration qui peut être attribué à un périphérique ou à un groupe de périphériques de même modèle. Pour vérifier que les informations de configuration pour un périphérique ou groupe de périphériques correspondent bien à la stratégie en question, vous effectuez un contrôle de conformité. Si le contrôle de conformité indique que le périphérique n'est pas conforme à la stratégie, vous pouvez mettre en œuvre la stratégie sur le périphérique ou groupe de périphériques.

Vous créez des stratégies selon différents types fonctionnels prédéfinis :

- Copie
- Courrier électronique/FTP
- Télécopie
- Lecteur flash
- Microcode
- Général
- Réseau
- Papier
- Impression
- Sécurité

Remarque : Pour plus d'informations sur la mise en œuvre de la stratégie de sécurité, reportez-vous à la section « Comprendre la police de sécurité », page 31.

Chaque type de stratégie contient des paramètres exclusifs qui garantissent que l'attribution de plusieurs types de stratégies à un périphérique ne donnera lieu à aucun conflit de paramètres.

Création d'une police

Création d'une nouvelle stratégie

- 1 Si nécessaire, cliquez sur **Stratégies de périphérique** dans l'onglet Stratégies pour afficher la section correspondante.
- 2 Cliquez sur **+**, puis tapez le nom de la nouvelle stratégie.
Remarque : Les noms de stratégie doivent être uniques pour chaque modèle de périphérique. Veillez à ne pas entrer un nom déjà utilisé dans la base de données.
- 3 Dans la liste Modèles pris en charge, sélectionnez un périphérique.
- 4 Dans le menu déroulant Type, sélectionnez un type de stratégie, puis cliquez sur **OK**.
- 5 Dans la boîte de dialogue Nouvelle stratégie, cochez l'option **Nom du paramètre**.
Tous les paramètres sont automatiquement sélectionnés, ce qui vous permet de les personnaliser un à un.
- 6 Décochez les paramètres que vous souhaitez *exclure* des contrôles de conformité ou des tâches de mise en œuvre de la stratégie.
- 7 Sélectionnez une valeur pour chaque paramètre à inclure dans les contrôles de conformité et les tâches de mise en œuvre de la stratégie.
- 8 Cliquez sur **Enregistrer**.

Création d'une stratégie à partir d'un périphérique

1 Dans l'onglet Stratégies, cochez la case en regard de l'adresse IP du périphérique.


2 Cliquez sur **Stratégies de périphérique** pour afficher la section du même nom, puis cliquez sur .

3 Dans le champ Nom, tapez le nom de la nouvelle stratégie.

4 Sélectionnez le type de stratégie, puis cliquez sur **OK**.

Remarque : Vous pouvez sélectionner plusieurs types de stratégie, voire tous.

5 Modifiez les paramètres de la nouvelle stratégie si nécessaire.

a Dans la section Stratégies de périphérique, sélectionnez le nom de la nouvelle stratégie, puis cliquez sur .

b Sélectionnez une valeur pour chaque paramètre à inclure dans les contrôles de conformité et les tâches de mise en œuvre de la stratégie.

c Décochez les paramètres que vous souhaitez *exclure* des contrôles de conformité ou des tâches de mise en œuvre de la stratégie.

d Cliquez sur **Enregistrer**.

6 Vérifiez que les paramètres de la nouvelle stratégie contiennent des valeurs correctes.

Si la stratégie est affichée en rouge et que le nom est précédé d'un point d'exclamation, vous ne pouvez l'attribuer à un périphérique. Un ou plusieurs paramètres de la stratégie contiennent des valeurs non valides ; la stratégie ne peut donc être mise en œuvre telle quelle.

Procédez comme suit pour rendre la stratégie applicable à un périphérique :

a Sélectionnez la stratégie, puis cliquez sur .

b Entrez une valeur valide pour les paramètres, puis cliquez sur **Enregistrer**.

c Si un message d'avertissement apparaît, notez les paramètres dont les valeurs ne sont pas valides.

d Cliquez sur **Non**, puis entrez une valeur valide pour chacun des paramètres signalés.

e Cliquez sur **Enregistrer**.

f Si nécessaire, répétez les étapes étape c à étape e jusqu'à ce que l'avertissement ne s'affiche plus.

Comprendre la police de sécurité

Markvision peut configurer l'installation de périphériques Lexmark sécurisés, en ce compris les paramètres de sécurité de différentes fonctions de périphériques ou la communication à distance.

Lors de l'utilisation de la police de sécurité, assurez-vous que vous utilisez *uniquement* Markvision pour gérer les paramètres de sécurité de vos périphériques. Si vous utilisez d'autres systèmes parallèlement à Markvision, cela peut entraîner un comportement inattendu.

La police de sécurité peut être assignée à un sous-groupe de périphériques spécifiques. Pour voir la liste complète des périphériques pris en charge, reportez-vous aux *Notes de publication*.

Présentation des périphériques sécurisés

Il peut exister différentes configurations d'un périphérique sécurisé. Cependant, Markvision ne prend actuellement en charge que les périphériques *totalelement non restreints* ou *totalelement restreints*.

Configurations de périphériques à l'accès totalement restreint ou non restreint

		Totalement non restreints	Totalement restreints
Paramètres du périphérique	<i>Contrôle d'accès à la fonction de gestion à distance (RM FAC) ou mot de passe avancé</i> Remarque : Pour connaître la liste des périphériques qui prennent en charge RM FAC, reportez-vous à la section « Imprimantes Lexmark prenant en charge la stratégie de sécurité » des <i>Notes de publication</i> .	Aucune sécurité et aucun mot de passe	Le RM FAC est configuré à l'aide d'un modèle de sécurité ou d'un mot de passe
	Ports pertinents	Les ports suivants sont ouverts : <ul style="list-style-type: none"> • UDP 161 (SNMP) • UDP 9300/9301/9302 (NPAP) 	Fermé
	Ports de sécurité	Les ports suivants sont ouverts : <ul style="list-style-type: none"> • UDP 5353 (mDNS) • TCP 6110 • TCP/UDP 6100 (LST) 	Les ports suivants sont ouverts : <ul style="list-style-type: none"> • UDP 5353 (mDNS) • TCP 6110 • TCP/UDP 6100 (LST)

		Totalement non restreints	Totalement restreints
Paramètres MarkVision	Profil de recherche	Vérifiez que l'option Inclure les imprimantes sécurisées dans la recherche est désélectionnée.	Vérifiez que l'option Inclure les imprimantes sécurisées dans la recherche est sélectionnée.
	Des canaux sécurisés sont-ils utilisés pour la communication entre MarkVision et les périphériques réseau ?	Non Remarques : <ul style="list-style-type: none"> Ce type de configuration est recommandé, à moins que vous soyez particulièrement soucieux de la sécurité de votre communication réseau. Une exception toutefois lorsque certains paramètres peuvent être lus/écrits <i>uniquement</i> au moyen de canaux sécurisés. 	Oui
	Comment puis-je déterminer la configuration de sécurité des périphériques de mon réseau ?	Dans la grille de données principale de Markvision, une icône représentant un verrou <i>ouvert</i> apparaît en regard de l'adresse IP d'un périphérique totalement non restreint.	Dans la grille de données principale de Markvision, une icône représentant un verrou <i>fermé</i> apparaît en regard de l'adresse IP d'un périphérique totalement restreint. Remarque : Si Markvision ne connaît pas les informations d'authentification de communication du périphérique, l'icône représentant un verrou fermé est barrée en rouge. Cela signifie que Markvision est actuellement incapable de communiquer avec le périphérique au-delà de cette recherche minimale.
	Comment puis-je rechercher les périphériques possédant ce type de configuration ?	<ol style="list-style-type: none"> Dans la zone « Signets et Recherche avancée », sélectionnez Toutes les imprimantes. Dans la zone Récapitulatif des résultats de la recherche, accédez à la catégorie Communications, puis sélectionnez Non sécurisées. 	<ol style="list-style-type: none"> Dans la zone « Signets et Recherche avancée », sélectionnez Toutes les imprimantes. Dans la zone Récapitulatif des résultats de la recherche, accédez à la catégorie Communications, puis sélectionnez Sécurisées.

Remarques :

- Si le périphérique ou le profil de recherche ne correspondent à aucun de ces scénarios, le comportement risque d'être inattendu ou non défini.
- Vérifiez que l'état du périphérique est correct et que le profil de recherche est bien configuré *avant* de rechercher le périphérique. Si vous modifiez l'un ou l'autre paramètre après l'exécution du profil de recherche, cela risque d'entraîner un comportement inattendu ou non défini.

Présentation des paramètres des stratégies de sécurité

Utilisez la stratégie de sécurité pour personnaliser les paramètres de sécurité d'un périphérique réseau.

Pour que Markvision exécute efficacement les fonctions de gestion à distance sur un périphérique réseau, veillez à ce que la stratégie de sécurité applique les paramètres suivants :

- Dans la section Paramètres généraux de la stratégie de sécurité, les paramètres d'accès aux ports suivants sont réglés sur **Activé** ou sur **Sécurisé et non sécurisé**:
 - Accès au port : mDNS (UDP 5353)
 - Accès au port : TCP/UDP (6110/6100)
- Dans la section Contrôles d'accès (si disponible sur périphérique mobile), les paramètres Modifications du paramètre de l'adaptateur réseau NPA et Mises à jour du microcode sont définis sur **Aucune sécurité**.
- Les sections suivantes (si disponible sur périphérique mobile) sont en lecture seule et ne peuvent pas être modifiées :
 - Contrôles d'accès
 - Modèles de sécurité

Remarque : Il sera peut-être nécessaire de spécifier les informations d'authentification pour les blocs fonctionnels situés sous la colonne Configuration authentification.

 - Paramètres divers

Remarque : Dans la section Contrôles d'accès (si disponible sur périphérique mobile), modèles de sécurité et les paramètres divers ne sont pas disponibles pour tous les modèles de périphériques. Pour plus d'informations, reportez-vous à la section « Imprimantes Lexmark prenant en charge la stratégie de sécurité » des *Notes de publication*.

Utilisation de blocs fonctionnels à partir d'une application eSF

Si vous souhaitez utiliser le bloc fonctionnel à partir d'une application Embedded Solutions Framework (eSF) pour la stratégie de sécurité, veillez d'abord à installer manuellement l'application eSF sur tous les périphériques affectés. Markvision ne procède *pas* à l'installation de l'application si une stratégie de sécurité est en vigueur.

Remarque : Seuls les paramètres internes disponibles pour l'ensemble des applications eSF seront clonés, contrôlés pour leur conformité ou appliqués au moyen de la stratégie de sécurité.

Création d'une police de sécurité

Pour créer une police de sécurité, copiez une police existante d'un périphérique principal pré-configuré.

Clonage d'une stratégie de sécurité afin de restreindre des périphériques

Etape 1. Configurez un périphérique à restreindre à l'aide de son serveur Web incorporé.

Lorsque vous avez configuré un périphérique à restreindre, utilisez-le comme périphérique maître à cloner pour une stratégie de sécurité.

- 1 Réglez le contrôle d'accès sur un modèle de sécurité existant dans le cas où le modèle du périphérique prend en charge la gestion du contrôle d'accès à distance. Réglez le contrôle d'accès sur un modèle de sécurité existant dans le cas où le modèle du périphérique ne prend pas en charge la gestion du contrôle d'accès à distance, ensuite configurez un mot de passe avancé. Effectuez une des opérations suivantes :

Remarque : Pour voir la liste des périphériques qui prennent en charge la gestion du contrôle d'accès à distance, reportez-vous à la section « Imprimantes Lexmark prenant en charge la stratégie de sécurité » des *Notes de publication*.

Configuration de la gestion du contrôle d'accès à distance

- a Depuis MarkVision, cliquez sur **Centre de services**.
- b Recherchez le périphérique à configurer, puis sélectionnez son adresse IP.
- c Cliquez sur **Page Web incorporée > Paramètres > Sécurité > Configuration de la sécurité**.
- d Dans la section Configuration avancée de la sécurité, cliquez sur **Contrôles d'accès**.
- e Accédez à Gestion à distance, puis sélectionnez un modèle de sécurité dans le menu déroulant.
Remarque : Le modèle de sécurité doit spécifier l'authentification uniquement.
- f Cliquez sur **Soumettre**.

Configuration d'un mot de passe avancé

- a Depuis MarkVision, cliquez sur **Centre de services**.
- b Recherchez le périphérique à configurer, puis sélectionnez son adresse IP.
- c Cliquez sur **Page Web incorporée > Configuration > Sécurité**.
- d Cliquez sur **Créer/Modifier mot de passe** ou **Créer mot de passe**.
- e Si nécessaire, cliquez sur **Créer un mot de passe avancé**, et saisissez-le.
- f Confirmez le mot de passe en le saisissant de nouveau dans le champ suivant puis cliquez sur **Soumettre**.

2 Vérifiez que les ports pertinents sont fermés et que les ports de sécurité sont ouverts.

Remarque : Si nécessaire, vous pouvez sélectionner **Mode sécurisé**, puis passer à étape 3.


- a Dans Embedded Web Server, cliquez sur **Paramètres** ou **Configuration**, puis cliquez sur **Sécurité > Accès au port TCP/IP**.
- b Recherchez les ports importants suivants et désélectionnez les cases à cocher à côté de ces derniers, le cas échéant ou sélectionnez **Désactivé** dans le menu déroulant.
 - **UDP 161 (SNMP)**
 - **UDP 9300/9301/9302 (NPAP)**
- c Recherchez les ports de sécurité et assurez-vous de sélectionner les cases à cocher à côté de ces derniers ou sélectionnez **Sécurisé et non sécurisé** dans le menu déroulant.
 - **UDP 5353 (mDNS)**
 - **TCP 6110**
 - **TCP/UDP 6100 (LST)**
- d Cliquez sur **Soumettre**.

3 Configurez d'autres paramètres de sécurité.

- a Depuis le serveur Web incorporé, cliquez sur **Paramètres** ou **Configuration**, ensuite cliquez sur **Sécurité**.
- b Apportez d'autres modifications aux paramètres de sécurité, le cas échéant.
- c Une fois les autres modifications apportées, cliquez sur **Paramètres** ou **Configuration**, puis cliquez sur **Sécurité > Afficher le résumé de sécurité** (si disponible sur le modèle de périphérique).
- d Vérifiez que vos modifications se reflètent dans la page de résumé.


Remarque : Ce n'est pas nécessaire d'utiliser le serveur Web incorporé pour limiter le périphérique maître dans le cas où vous utilisez un mot de passe avancé au lieu de la gestion du contrôle d'accès à distance. Vous pouvez utiliser MarkVision pour créer une politique de sécurité à partir de n'importe quel périphérique, puis configurer le mot de passe avancé et les paramètres du port au sein des paramètres généraux de la politique.

Etape 2. Vérifiez que Markvision reconnaît votre périphérique maître restreint.


- 1 Créez un profil de recherche. Pour plus d'informations sur la création d'un profil de recherche, reportez-vous à la section « Création d'un profil de recherche », page 18.
- 2 Dans la boîte de dialogue « Profil de recherche – Ajouter », assurez-vous que l'option **Inclure les imprimantes sécurisées dans la recherche** est sélectionnée.
- 3 Pour exécuter le profil de recherche, cliquez sur .

Remarque : A ce stade, le périphérique est « partiellement détecté ». Cela signifie que Markvision a détecté le périphérique avec des informations limitées, mais ne pourra pas exécuter des options supplémentaires avec le périphérique, telles que la conformité d'une stratégie, la mise en œuvre d'une stratégie et l'audit. Pour acquérir ses informations complètes, vous devez fournir les informations d'authentification de communication du périphérique.

Etape 3. Lancez le processus de clonage.

- 1 Depuis MarkVision, cliquez sur **Stratégies**.
- 2 Recherchez votre périphérique maître restreint, puis cochez la case en regard de son adresse IP.
- 3 Le cas échéant, cliquez sur **Stratégies de périphérique**, puis sur .
- 4 Dans le champ Nom, tapez le nom de la nouvelle stratégie de sécurité.
- 5 Assurez-vous que le type de stratégie de sécurité est sélectionné.
- 6 Entrez les informations nécessaires à l'authentification auprès du périphérique, puis cliquez sur **OK**.

Remarque : Utilisez les informations d'authentification du modèle de sécurité que vous avez défini dans le contrôle d'accès de gestion à distance ou utilisez un mot de passe avancé que vous avez configuré.

- 7 Attendez la fin du processus de clonage.
Si la stratégie est affichée en rouge, cela signifie qu'il manque certaines informations d'authentification et qu'elle ne peut donc pas être attribuée à un périphérique dans son état actuel. Pour rendre la stratégie applicable à un périphérique, entrez les informations d'authentification correctes du périphérique.
- 8 Modifiez les paramètres de la nouvelle stratégie de sécurité et vérifiez qu'ils contiennent des valeurs correctes.
 - a Dans la section Stratégies de périphérique, sélectionnez le nom de la stratégie, puis cliquez sur .
 - b Sélectionnez une valeur pour chaque paramètre à inclure dans les contrôles de conformité et les tâches de mise en œuvre de la stratégie.
 - c Décochez les paramètres que vous souhaitez *exclure* des contrôles de conformité ou des tâches de mise en œuvre de la stratégie.
 - d Saisissez le mot de passe de sécurité, puis cliquez sur **Enregistrer**.

Remarque : Pour plus d'informations sur les paramètres valides d'une stratégie de sécurité, reportez-vous à la section « Présentation des paramètres des stratégies de sécurité », page 33.

- 9 Affectez la stratégie de sécurité à des périphériques non restreints du même modèle que le périphérique maître restreint.

Pour plus d'informations sur l'affectation d'une stratégie à plusieurs périphériques, reportez-vous à la section « Attribution d'une stratégie », page 41.

10 Appliquez la stratégie de sécurité aux périphériques sélectionnés.

Pour plus d'informations sur la mise en œuvre d'une stratégie, reportez-vous à la section « Mise en œuvre d'une stratégie », page 41.

11 Relancez la détection des périphériques.

Les périphériques sont à présent restreints. En outre, Markvision connaît à présent les informations d'authentification de communication du périphérique et peut les utiliser pour exécuter des tâches dans les zones de service Actifs et Stratégies.

Clonage d'une stratégie de sécurité afin d'annuler la restriction de périphériques

Etape 1. Configurez un périphérique comme non restreint à l'aide de son serveur Web incorporé.

Lorsque vous avez configuré un périphérique comme non restreint, utilisez-le comme périphérique maître à cloner pour une stratégie de sécurité.

- 1 Réglez le contrôle d'accès sur **Aucune sécurité** dans le cas où le modèle du périphérique prend en charge la gestion du contrôle d'accès à distance. Supprimez le mot de passe avancé dans le cas où le périphérique ne prend pas en charge la gestion du contrôle d'accès à distance. Effectuez une des opérations suivantes :

Remarque : Pour voir la liste des périphériques qui prennent en charge la gestion du contrôle d'accès à distance, reportez-vous à la section « Imprimantes Lexmark prenant en charge la stratégie de sécurité » des *Notes de publication*.

Configuration de la gestion du contrôle d'accès à distance

- a Depuis MarkVision, cliquez sur **Centre de services**.
- b Recherchez le périphérique à configurer, puis sélectionnez son adresse IP.
- c Cliquez sur **Page Web incorporée > Paramètres > Sécurité > Configuration de la sécurité**.
- d Dans la section Configuration avancée de la sécurité, cliquez sur **Contrôles d'accès**.
- e Accédez à **Gestion à distance**, puis sélectionnez **Aucune sécurité** dans le menu déroulant.
- f Cliquez sur **Soumettre**.

Suppression du mot de passe avancé

- a Depuis MarkVision, cliquez sur **Centre de services**.
- b Recherchez le périphérique à configurer, puis sélectionnez son adresse IP.
- c Cliquez sur **Page Web incorporée > Configuration > Sécurité**.
- d Cliquez sur **Créer/Modifier mot de passe** ou **Créer mot de passe**.
- e Le cas échéant, cliquez sur **Créer un mot de passe avancé**.
- f Videz les champs réservés au mot de passe, puis cliquez sur **Soumettre**.

- 2 Vérifiez que les ports pertinents et les ports de sécurité sont ouverts.

- a Dans Embedded Web Server, cliquez sur **Paramètres** ou **Configuration**, puis cliquez sur **Sécurité > Accès au port TCP/IP**.
- b Recherchez les ports suivants et assurez-vous qu'ils sont sélectionnés ou réglés sur **Sécurisé et non sécurisé**.

Ports pertinents

- **UDP 161 (SNMP)**
- **UDP 9300/9301/9302 (NPAP)**

Ports de sécurité

- **UDP 5353 (mDNS)**
- **TCP 6110**
- **TCP/UDP 6100 (LST)**

c Cliquez sur **Envoyer**.

3 Configurez d'autres paramètres de sécurité.

a Depuis le serveur Web incorporé, cliquez sur **Paramètres** ou **Configuration**, ensuite cliquez sur **Sécurité**.

b Apportez d'autres modifications aux paramètres de sécurité, le cas échéant.

c Une fois les autres modifications apportées, cliquez sur **Paramètres** ou **Configuration**, puis cliquez sur **Sécurité > Afficher le résumé de sécurité** (si disponible sur le modèle de périphérique).


d Vérifiez que vos modifications se reflètent dans la page de résumé.

Remarque : Ce n'est pas nécessaire d'utiliser le serveur Web incorporé pour autoriser l'accès à un périphérique maître dans le cas où vous utilisez un mot de passe avancé au lieu de la gestion du contrôle d'accès à distance. Vous pouvez utiliser MarkVision pour créer une politique de sécurité à partir de n'importe quel périphérique, puis configurer le mot de passe avancé et les paramètres du port dans les paramètres généraux de la politique.

Etape 2. Vérifiez que Markvision reconnaît votre périphérique maître non restreint.

1 Créez un profil de recherche. Pour plus d'informations sur la création d'un profil de recherche, reportez-vous à la section « Création d'un profil de recherche », page 18.

2 Dans la « boîte de dialogue Profil de recherche – Ajouter », vérifiez que l'option **Inclure les imprimantes sécurisées dans la recherche** n'est pas sélectionnée.

3 Pour exécuter le profil de recherche, cliquez sur .

Etape 3. Lancez le processus de clonage.

1 Depuis MarkVision, cliquez sur **Stratégies**.

2 Recherchez votre périphérique maître non restreint, puis cochez la case en regard de son adresse IP.

3 Le cas échéant, cliquez sur **Stratégies de périphérique**, puis sur .

4 Dans le champ Nom, tapez le nom de la nouvelle stratégie de sécurité.

5 Assurez-vous que le type de stratégie de sécurité est sélectionné.


6 Entrez les informations nécessaires à l'authentification auprès du périphérique, puis cliquez sur **OK**.

Remarque : Utilisez les informations d'authentification du modèle de sécurité que vous avez défini dans le contrôle d'accès de gestion à distance ou utilisez un mot de passe avancé que vous avez configuré.

7 Attendez la fin du processus de clonage.

Si la stratégie est affichée en rouge, cela signifie qu'il manque certaines informations d'authentification et qu'elle ne peut donc pas être attribuée à un périphérique dans son état actuel. Pour rendre la stratégie applicable à un périphérique, entrez les informations d'authentification correctes du périphérique.

8 Modifiez les paramètres de la nouvelle stratégie de sécurité et vérifiez ensuite qu'ils contiennent des valeurs correctes.

- a** Dans la section Stratégies de périphérique, sélectionnez le nom de la stratégie, puis cliquez sur .
- b** Sélectionnez une valeur pour chaque paramètre à inclure dans les contrôles de conformité et les tâches de mise en œuvre de la stratégie.
- c** Décochez les paramètres que vous souhaitez *exclure* des contrôles de conformité ou des tâches de mise en œuvre de la stratégie.
- d** Cliquez sur **Enregistrer**.

Remarque : Pour plus d'informations sur les paramètres valides d'une stratégie de sécurité, reportez-vous à la section « Présentation des paramètres des stratégies de sécurité », page 33.

9 Affectez la stratégie de sécurité à des périphériques non restreints du même modèle que le périphérique maître non restreint.

Remarques :

- Pour plus d'informations sur l'affectation d'une stratégie à plusieurs périphériques, reportez-vous à la section « Attribution d'une stratégie », page 41.
- Si l'un des périphériques sélectionnés est restreint, il devient non restreint après la mise en œuvre de la stratégie.

10 Appliquez la stratégie de sécurité aux périphériques sélectionnés.

Pour plus d'informations sur la mise en œuvre d'une stratégie, reportez-vous à la section « Mise en œuvre d'une stratégie », page 41.

11 Relancez la détection des périphériques.

Les périphériques sont à présent non restreints et peuvent être utilisés par l'ensemble des zones de service.

Modification des informations d'authentification de communication d'un périphériques restreint

Les *informations d'authentification de communication* sont nécessaires pour s'authentifier auprès d'un périphérique réseau à l'aide de LST (Lexmark Secure Transport). Il peut s'agir d'une combinaison des éléments suivants : nom d'utilisateur, zone, mot de passe et *numéro d'identification personnel* (PIN).


Remarque : Quelques modèles de périphériques prennent uniquement en charge des mots de passe. Pour plus d'informations, reportez-vous à la section « Imprimantes Lexmark prenant en charge la stratégie de sécurité » des *Notes de publication*.

Il existe deux types de blocs fonctionnels d'informations d'authentification de communication :


- **Autorité finale** : le bloc fonctionnel est l'autorité finale en matière d'authentification ou d'autorisation au moyen d'informations d'identification. Les mots de passe et codes PIN constituent quelques exemples.
- **Autorité de connexion directe** : le bloc fonctionnel transmet les informations d'identification à une autorité externe pour authentification ou autorisation. Citons comme exemples d'autorité externe le protocole *LDAP (Lightweight Directory Access Protocol)* et Kerberos.

Modification des informations d'authentification d'un bloc fonctionnel d'autorité finale


Remarque : Les options de sécurité des contrôles d'accès et modèles de sécurité ne sont pas disponibles pour tous les modèles de périphériques. Pour plus d'informations, reportez-vous à la section « Imprimantes Lexmark prenant en charge la stratégie de sécurité » des *Notes de publication*.

- 1 Si nécessaire, cliquez sur **Stratégies de périphérique** dans l'onglet Stratégies pour afficher la section correspondante.
- 2 Sélectionnez la stratégie de sécurité restreinte souhaitée et cliquez sur  > **Contrôles d'accès**.
- 3 Recherchez **Gestion à distance**, puis notez sa valeur.
- 4 Cliquez sur **Modèles de sécurité**.
- 5 Dans la colonne Configuration authentification, sélectionnez le bloc fonctionnel situé à côté de la valeur notée à l'étape étape 3.
- 6 Dans le champ Mot de passe, saisissez le nouveau mot de passe.
- 7 Confirmez le mot de passe en le saisissant de nouveau dans le champ suivant puis cliquez sur **Enregistrer**.
- 8 Appliquez la stratégie de sécurité restreinte aux périphériques qui lui sont affectés.
Une fois la tâche de mise en œuvre terminée, les informations d'authentification de communication du périphérique sont mises à jour.

Modification des informations d'authentification d'un bloc fonctionnel d'autorité de connexion directe

- 1 Apportez les modifications aux informations d'authentification à partir de l'autorité externe que vous utilisez.
- 2 Dans la page Web MarkVision, cliquez sur **Stratégies > Stratégies de périphérique** pour afficher la section correspondante.
- 3 Sélectionnez la stratégie de sécurité restreinte souhaitée et cliquez sur  > **Informations d'authentification du périphérique**.
- 4 Dans la section Informations d'authentification du périphérique, placez les valeurs actuelles par celles saisies dans l'autorité externe.
- 5 Cliquez sur **Enregistrer**.
- 6 Appliquez la stratégie de sécurité restreinte aux périphériques qui lui sont affectés.
Une fois la tâche de mise en œuvre terminée, Markvision peut à nouveau communiquer avec les périphériques.

Modification ou suppression d'une stratégie

- 1 Si nécessaire, cliquez sur **Stratégies de périphérique** dans l'onglet Stratégies pour afficher la section correspondante.
- 2 Sélectionnez une stratégie, puis effectuez l'une des opérations suivantes :
 - Pour modifier la stratégie, cliquez sur  .
 - a Dans le champ Nom de la stratégie, tapez le nouveau nom de la stratégie, si applicable.
 - b Sélectionnez une valeur pour chaque paramètre à inclure dans les contrôles de conformité et les tâches de mise en œuvre de la stratégie.

- c Décochez les paramètres que vous souhaitez *exclure* des contrôles de conformité ou des tâches de mise en œuvre de la stratégie.
- d Cliquez sur **Enregistrer**.
- Pour supprimer la stratégie, cliquez sur —, puis cliquez sur **Oui**.

Attribution d'une stratégie


- 1 Si nécessaire, cliquez sur **Stratégies de périphérique** dans l'onglet Stratégies pour afficher la section correspondante.
- 2 Sélectionnez une stratégie.

Remarques :

- Pour sélectionner plusieurs stratégies, utilisez **Maj + clic** ou **Ctrl + clic**.
- Vous pouvez attribuer plusieurs types de stratégies à un même périphérique. En revanche, vous ne pouvez utiliser qu'une seule stratégie de chaque type de stratégie.

- 3 Cochez l'adresse IP du périphérique auquel vous souhaitez attribuer la stratégie.

Remarque : Vous pouvez sélectionner plusieurs périphériques, voire tous.

- 4 Cliquez sur 

Dans la colonne Type de stratégie, un point d'interrogation s'affiche en regard du périphérique sélectionné.

Ce point d'interrogation indique que la conformité du périphérique à la stratégie attribuée n'a pas encore été vérifiée.

Contrôle de la conformité à une stratégie

- 1 Dans l'onglet Stratégies, cochez la case en regard de l'adresse IP du périphérique.

Remarque : Vous pouvez sélectionner plusieurs périphériques, voire tous.

- 2 Cliquez sur **Conformité**.

- 3 Sélectionnez un type de stratégie dans la boîte de dialogue Stratégies de contrôle de la conformité, puis cliquez sur **OK**.

- 4 Dans la colonne Type de stratégie, vérifiez si un point d'interrogation est affiché en regard du périphérique sélectionné.

- 5 Si un point d'interrogation ou un X est affiché, cliquez sur  pour afficher les détails.


Remarque : Vous pouvez planifier l'exécution d'un contrôle de conformité à une heure donnée ou à intervalle fixe. Pour plus d'informations, voir « Planification de tâches », page 56.

Mise en œuvre d'une stratégie

- 1 Dans l'onglet Stratégies, cochez la case en regard de l'adresse IP du périphérique.


Remarque : Vous pouvez sélectionner plusieurs périphériques, voire tous.

- 2 Cliquez sur **Imposer**.

- 3 Sélectionnez un type de stratégie dans la boîte de dialogue Mettre en œuvre les stratégies, puis cliquez sur **OK**.
- 4 Cliquez sur  pour vérifier que la mise en œuvre de la stratégie est effective.

Remarque : Vous pouvez planifier l'exécution d'une tâche de mise en œuvre de la stratégie à une heure donnée ou à intervalle fixe. Pour plus d'informations, voir « Planification de tâches », page 56.

Suppression d'une stratégie

- 1 Dans l'onglet Stratégies, cochez la case en regard de l'adresse IP du périphérique.
- 2 Si nécessaire, cliquez sur **Stratégies de périphérique** pour afficher la section du même nom, puis cliquez sur .
- 3 Sélectionnez une stratégie dans la boîte de dialogue Supprimer la stratégie, puis cliquez sur **OK**.


Remarque : Vous pouvez aussi sélectionner plusieurs stratégies.

Gestion du Service Desk


Travailler avec des polices

Avant de tenter de résoudre un problème sur un périphérique, assurez-vous d'abord est en conformité avec la police qui lui est associée.

Vérification de la conformité du périphérique aux stratégies

- 1 Cochez la case en regard de l'adresse IP du périphérique dans l'onglet Service Desk.
Remarque : vous pouvez également sélectionner plusieurs ou l'intégralité des périphériques.
- 2 Cliquez sur **Conformité**.
- 3 Sélectionnez un type de stratégie dans la boîte de dialogue Stratégies de contrôle de la conformité, puis cliquez sur **OK**.
- 4 Patientez jusqu'à ce que la tâche soit terminée dans la zone des informations relatives à la tâche.
- 5 Cliquez sur  pour afficher les résultats de la vérification de la conformité.




Mise en œuvre des stratégies

- 1 Cochez la case en regard de l'adresse IP du périphérique dans l'onglet Service Desk.
Remarque : vous pouvez également sélectionner plusieurs ou l'intégralité des périphériques.
- 2 Cliquez sur **Appliquer**.
- 3 Sélectionnez un type de stratégie dans la boîte de dialogue Mettre en œuvre les stratégies, puis cliquez sur **OK**.
- 4 Patientez jusqu'à ce que la tâche soit terminée dans la zone des informations relatives à la tâche.
- 5 Cliquez sur  pour vérifier que la mise en œuvre de la stratégie est effective.

Travailler avec un périphérique

Vérification de l'état d'un périphérique

- 1 Recherchez un périphérique sous Signets ou Recherche avancée.
Remarque : Vous pouvez affiner la liste des périphériques renvoyés à l'aide des catégories dans le récapitulatif des résultats de la recherche.
- 2 Cochez la case en regard de l'adresse IP du périphérique, puis cliquez sur **Récupérer l'état actuel**.
- 3 Dans les colonnes Etat de l'imprimante et Etat des fournitures, notez l'icône affichée à côté du périphérique.

Icône	Etat
	OK : le périphérique est prêt et les fournitures sont suffisantes.
	Avertissement : le périphérique fonctionne, mais les fournitures s'amenuisent ou exigeront bientôt votre attention.
	Erreur : le périphérique ou les fournitures exigent votre attention immédiate.

- 4 Cliquez sur **Utiliser le périphérique** pour afficher les détails de l'état du périphérique.

Affichage d'un périphérique à distance

Remarque : Cette fonction est uniquement disponible avec les périphériques qui prennent en charge l'affichage à distance.

- 1 Cochez la case en regard de l'adresse IP du périphérique dans l'onglet Service Desk.
- 2 Cliquez sur **Utiliser le périphérique**.
La boîte de dialogue qui s'ouvre affiche les détails du périphérique ainsi qu'une image du périphérique.
- 3 Cliquez sur **Panneau de commandes à distance** > **Cliquez ici pour continuer**.
La nouvelle boîte de dialogue qui s'ouvre affiche à distance une vue dynamique du panneau de commandes du périphérique dans son état actuel.
- 4 Reportez-vous aux touches du clavier correspondant à chacun des boutons de commande (en commençant par le coin inférieur gauche).

Remarque : L'emplacement des touches du clavier peut varier selon le modèle du périphérique.

Affichage de la page Web incorporée

Remarque : Cette fonction est uniquement disponible avec les périphériques qui prennent en charge l'affichage à distance de la page Web incorporée.

- 1 Cochez la case en regard de l'adresse IP du périphérique dans l'onglet Service Desk.
- 2 Cliquez sur **Utiliser le périphérique**.
La boîte de dialogue qui s'ouvre affiche les détails du périphérique ainsi qu'une image du périphérique.
- 3 Cliquez sur **Page Web incorporée**.

Remarque : Dans la partie inférieure de la boîte de dialogue, vous pouvez également sélectionner la langue à utiliser.

Gestion des évènements de périphériques

Le gestionnaire d'évènements vous permet de monitorer et de gérer pro-activement votre parc d'impression. Déterminez une destination pour vous notifier à vous-même ou à d'autres utilisateurs spécifiques quand un évènement particulier survient. Créer un évènement automatique quand un périphérique envoie une alerte réseau.

Création d'une destination




Une destination est une action prédéfinie qui exécute une commande spécifique lorsqu'un évènement particulier affectant un groupe de périphériques se produit. Une destination peut être une notification par courrier électronique ou une invite de ligne de commande s'affichant lorsque l'action en question est requise.

- 1 Si nécessaire, cliquez sur **Destinations** dans l'onglet Gestionnaire des évènements pour afficher la section Destinations.
- 2 Cliquez sur **+**, puis saisissez un nom unique pour la destination.
- 3 Effectuez l'une des opérations suivantes :
 - Sélectionnez **Commande**, puis cliquez sur **Suivant**.
 - a Saisissez le nom d'une commande d'exécution dans la zone Chemin d'accès de commande.
 - b Ajoutez un ou plusieurs mots clés dans la zone Paramètres de commande en sélectionnant un mot clé dans la liste Espaces réservés, puis cliquez sur **►**.
 - Sélectionnez **Email**, puis cliquez sur **Suivant**.
 - a Vérifiez que les paramètres de messagerie sont correctement configurés dans la boîte de dialogue Configuration du système.
Pour plus d'informations, reportez-vous à la section « Configuration des paramètres de courrier électronique », page 48.
 - b Entrez les valeurs dans les champs appropriés :
 - **De** : saisissez l'adresse électronique de l'expéditeur.
 - **A** : saisissez l'adresse électronique du destinataire.
 - **CC** : saisissez l'adresse électronique d'autres destinataires qui recevront une copie du message.
 - **Objet** : saisissez l'objet, le cas échéant.
 - **Corps** : saisissez le message électronique par défaut.

Remarque : vous pouvez utiliser les *espaces réservés* disponibles pour les inclure dans l'objet du message à partir de la colonne Espaces réservés. Vous pouvez également utiliser les espaces réservés dans le corps du message. Les espaces réservés sont des éléments variables qui, lorsqu'ils sont utilisés, sont remplacés par la valeur correspondante.


- 4 Cliquez sur **Terminer**.

Modification ou suppression d'une destination

- 1 Si nécessaire, cliquez sur **Destinations** dans l'onglet Gestionnaire des événements pour afficher les destinations actives.
- 2 Sélectionnez une destination, puis effectuez l'une des opérations suivantes :
 - Pour modifier la destination, cliquez sur  .
 - a Modifiez le nom de la destination, le cas échéant, puis cliquez sur **Suivant**.
 - b Si nécessaire, modifiez le nom de la commande d'exécution dans la zone Chemin d'accès de commande.
 - c Pour supprimer un mot clé de la zone Paramètres de commande, cliquez deux fois sur celui-ci, puis appuyez sur **Supprimer**.
 - d Pour ajouter un ou plusieurs mots clés à la zone Paramètres de commande, sélectionnez un mot clé dans la liste Espaces réservés, puis cliquez sur  .
 - Pour supprimer une destination, cliquez sur  , puis sur **Oui**.


Attention — Dommages potentiels : lors de la suppression d'une destination, les événements associés sont également supprimés.
- 3 Cliquez sur **Terminer**.


Création d'un événement

- 1 Si nécessaire, cliquez sur **Evénements** dans l'onglet Gestionnaire des événements pour afficher la section Evénements.
- 2 Cliquez sur  , puis saisissez un nom unique pour l'événement ainsi que sa description.
- 3 Sélectionnez une alerte dans la section Alertes, puis cliquez sur **Suivant**.


Remarque : vous pouvez sélectionner plusieurs ou l'intégralité des alertes.
- 4 Sélectionnez une destination, puis effectuez l'une des opérations suivantes :
 - Pour déclencher un événement lors de l'activation de l'alerte, sélectionnez **Actif(ve) uniquement**.
 - Pour déclencher un événement lors de l'activation et de la suppression de l'alerte, sélectionnez **Actif(ve) et Effacé(e)**.
- 5 Cliquez sur **Terminer**.

Modification ou suppression d'un événement


- 1 Si nécessaire, cliquez sur **Evénements** dans l'onglet Gestionnaire des événements pour afficher les événements actifs.
- 2 Sélectionnez un événement, puis effectuez l'une des opérations suivantes :
 - Pour modifier l'événement, cliquez sur  .
 - a Modifiez le nom et la description de l'événement, le cas échéant.
 - b Ajoutez des alertes supplémentaires en les sélectionnant ou supprimez une alerte en décochant la case correspondante dans la section Alertes.
 - c Cliquez sur **Suivant**.

- d Ajoutez des destinations supplémentaires en les sélectionnant ou supprimez une destination en décochant la case correspondante dans la section Destinations.
- e Sélectionnez un déclencheur de destination, puis cliquez sur **Terminer**.
- Pour supprimer l'événement, cliquez sur , puis sur **Oui**.

Attribution d'un événement à un périphérique

- 1 Cochez la case en regard de l'adresse IP du périphérique dans l'onglet Gestionnaire des événements.
- 2 Si nécessaire, cliquez sur **Événements** pour afficher les événements actifs.
- 3 Sélectionnez un événement, puis cliquez sur .

Suppression d'un événement sur un périphérique

- 1 Cochez la case en regard de l'adresse IP du périphérique dans l'onglet Gestionnaire des événements.
- 2 Si nécessaire, cliquez sur **Événements** pour afficher les événements actifs.
- 3 Sélectionnez un événement, puis cliquez sur .


Affichage des détails d'un événement

- 1 Dans l'onglet Gestionnaire des événements, sélectionnez un périphérique sous Signets ou Recherche avancée.
Remarque : Vous pouvez affiner la liste des périphériques renvoyés à l'aide des catégories dans le récapitulatif des résultats de la recherche.
- 2 Dans la zone des résultats de recherche, cochez la case en regard de l'adresse IP d'un périphérique.
Remarque : Si vous ne connaissez pas l'adresse IP, recherchez le périphérique dans la colonne Nom du système.
- 3 Cliquez sur **Propriétés**.
La boîte de dialogue qui s'ouvre indique les conditions actuellement actives et les détails d'événement associés au périphérique.

Réaliser d'autres tâches d'administration.

Téléchargement de fichiers génériques

L'application permet de télécharger différents fichiers à partir du serveur MarkVision vers un ou plusieurs périphériques du réseau. Vous pouvez ainsi distribuer instantanément différents types de fichier, tels les fichiers *UCF (Universal Configuration Files)*, vers n'importe quels périphériques gérés par l'application.

- 1 Dans l'en-tête, cliquez sur .
- 2 Dans le menu déroulant Inclure les imprimantes, sélectionnez un groupe de périphériques ou un signet disponible.
- 3 Cliquez sur **Parcourir**, puis naviguez jusqu'au dossier contenant le fichier.
- 4 Sélectionnez le fichier à télécharger, puis cliquez sur **Ouvrir**.
- 5 Dans le menu déroulant Destination, sélectionnez l'une des options suivantes :
 - **Configuration (HTTP)** : permet de télécharger un fichier UCF d'imprimante.
 - **Configuration (FTP)** : permet de télécharger un fichier UCF réseau.
 - **Mise à jour du microcode** : permet de télécharger une mise à jour du microcode des périphériques.
 - **Imprimer (FTP)** : permet de télécharger un fichier imprimable par FTP.
 - **Imprimer (socket brut)** : permet de télécharger un fichier imprimable depuis l'ordinateur.
- 6 Cliquez sur **Télécharger**.


Remarques :

- La tâche « Téléchargement de fichier générique » n'est pas disponible lorsque l'option Verrouillage de l'imprimante est activée.
- Vous pouvez planifier l'exécution d'une tâche de téléchargement de fichier générique à une heure donnée ou à intervalle fixe. Pour plus d'informations, reportez-vous à la section « Planification de tâches », page 56.

Configuration des paramètres de courrier électronique


Remarques :

- Pour que MarkVision puisse envoyer des e-mails de notification des alertes et des messages d'erreur, vous devez configurer les paramètres SMTP (Simple Mail Transfer Protocol).
- Si vous activez la configuration SMTP maintenant, puis la désactivez ultérieurement, MarkVision ne pourra plus envoyer des e-mails de notification des alertes et des messages d'erreur.


- 1 Dans l'en-tête, cliquez sur l'onglet  > **Courrier électronique**.
- 2 Activez la case à cocher **Activer la configuration SMTP**, puis entrez des valeurs dans les champs appropriés :
 - **Serveur de messagerie SMTP** : entrez les informations relatives au serveur de messagerie électronique.
 - **Port** : entrez le numéro de port du serveur de messagerie SMTP.
 - **De** : entrez l'adresse électronique de l'expéditeur.

- 3 Si les utilisateurs doivent se connecter pour pouvoir envoyer l'e-mail, cochez l'option **Connexion requise**.
 - a Tapez le nom d'utilisateur et le mot de passe.
 - b Confirmez le mot de passe en le saisissant de nouveau.
- 4 Cliquez sur **Appliquer** > **Fermer**.

Configuration des paramètres système

- 1 Dans l'en-tête, cliquez sur l'onglet  > **Général**.
- 2 Dans la section Source du nom d'hôte, sélectionnez la source à partir de laquelle le système doit acquérir le nom d'hôte pour un périphérique, puis cliquez sur **Appliquer**.
- 3 Dans la section Gestionnaire des événements, spécifiez la fréquence à laquelle le système doit interroger les périphériques pour récupérer les alertes, puis cliquez sur **Appliquer**.

Ajout, modification ou suppression d'un utilisateur dans le système

- 1 Dans l'en-tête, cliquez sur l'onglet  > **Utilisateur**.
- 2 Effectuez l'une des opérations suivantes :
 - Pour ajouter un utilisateur, cliquez sur **+**.
 - a Entrez les informations nécessaires.
 - b Dans la section Rôles, sélectionnez le rôle du nouvel utilisateur, puis cliquez sur **OK**.

Un utilisateur peut se voir affecter un ou plusieurs rôles parmi les suivants :

- **Administrateur** : l'utilisateur peut accéder aux fonctions et tâches de tous les onglets. Seuls les utilisateurs titulaires de ce rôle disposent des droits administratifs, nécessaires par exemple pour ajouter des utilisateurs au système ou configurer les paramètres du système.
- **Actifs** : l'utilisateur a seulement accès aux fonctions et tâches de l'onglet Actifs.
- **Gestionnaire des événements** : l'utilisateur a seulement accès aux fonctions et tâches de l'onglet Gestionnaire des événements.
- **Stratégies** : l'utilisateur a seulement accès aux fonctions et tâches de l'onglet Stratégies.
- **Service Desk** : l'utilisateur a seulement accès aux fonctions et tâches de l'onglet Service Desk.

- Sélectionnez un utilisateur, puis cliquez sur  pour le modifier ou sur **—** pour le supprimer.

- 3 Suivez les instructions à l'écran.

Remarque : Au bout de trois tentatives de connexion incorrectes, le compte utilisateur est désactivé ; il ne peut être réactivé que par un administrateur. S'il s'agit de l'unique utilisateur du système disposant de droits d'administrateur, le compte est simplement suspendu pendant environ cinq minutes.

Activation de l'authentification de serveur LDAP


LDAP (*Lightweight Directory Access Protocol*) est un protocole évolutif multi-plateforme reposant sur des normes qui s'exécute directement sur TCP/IP et permet d'accéder à des bases de données spéciales appelées *Annuaire*s.

Les administrateurs de Markvision peuvent utiliser le serveur LDAP de l'entreprise pour authentifier les identifiants utilisateur et les mots de passe. Il n'est donc plus nécessaire de créer des identifiants et mots de passe distincts pour Markvision.

Markvision tente d'abord d'effectuer l'authentification par rapport aux identifiants utilisateurs valides présents dans le système. Si Markvision ne parvient pas à authentifier l'utilisateur à la première tentative, il tente une authentification par rapport aux utilisateurs enregistrés sur le serveur LDAP. Toutefois, si un utilisateur dispose du même nom à la fois pour le serveur Markvision interne et le serveur d'annuaire LDAP externe, Markvision utilisera alors les informations d'identification stockées dans son serveur interne. Ce qui signifie que l'utilisateur doit utiliser le mot de passe de Markvision et *non* le mot de passe LDAP.

Pour cela, le serveur LDAP doit contenir des groupes d'utilisateurs correspondant aux rôles définis à la section « Ajout, modification ou suppression d'un utilisateur dans le système », page 49.

Étape 1 : configurer les paramètres d'authentification

1 Dans l'en-tête, cliquez sur l'onglet  >LDAP.

2 Tapez les valeurs dans les champs appropriés de la section Informations d'authentification.

- **Serveur** : tapez l'adresse IP ou le nom d'hôte du serveur d'annuaire LDAP sur lequel sera exécutée l'authentification.

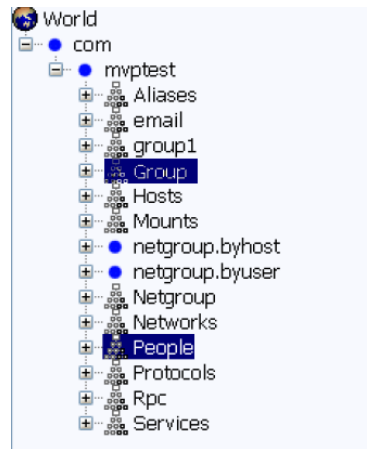
Si vous souhaitez utiliser une communication cryptée entre le serveur MVE et le serveur d'annuaire LDAP, procédez alors comme suit :

- a Utilisez le *nom de domaine complet* (FQDN, Fully Qualified Domain Name) de l'hôte du serveur.
- b Accédez au fichier de l'hôte du réseau puis créez une entrée pour associer le nom de l'hôte du serveur à son adresse IP.

Remarques :

- Sous UNIX/Linux, le fichier de l'hôte du réseau se trouve généralement dans `/etc/hosts`.
 - Sous Windows, le fichier de l'hôte du réseau se trouve généralement dans `%SystemRoot%\system32\drivers\etc`.
 - Avec le protocole TLS (*Transport Layer Security*), il est nécessaire que le nom de l'hôte du serveur corresponde au nom « émis vers » l'hôte spécifié dans le certificat TLS.
- **Port** : entrez le numéro du port qui sera utilisé par l'ordinateur local pour communiquer avec le serveur de communauté LDAP.
Le port LDAP par défaut est 389.

- **Nom unique de la racine** : saisissez le nom unique du nœud racine. Dans la hiérarchie du serveur LDAP, il devrait s'agir de l'ancêtre direct du nœud utilisateur et du nœud de groupe. Dans cet exemple, vous saisissez `dc=mvptest, dc=com` dans le champ Nom unique de la racine.

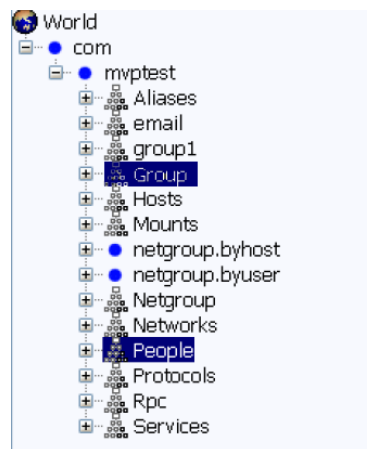


Remarque : Lors de la spécification du nom unique de la racine, assurez-vous que seuls `dc` et `o` font partie de l'expression du nom unique de la racine. Si `ou` ou `cn` représente l'ancêtre commun au nœud utilisateur et au nœud de groupe, utilisez alors `ou` ou `cn` dans les expressions de la base de recherche d'utilisateurs ou dans la base de recherche de groupes.

- 3 Si vous souhaitez que Markvision recherche les *utilisateurs* imbriqués sur le serveur LDAP, sélectionnez alors **Activer la recherche d'utilisateurs imbriqués**.

Pour préciser davantage la recherche, tapez les valeurs dans les champs appropriés.

- **Base de recherche d'utilisateurs** : spécifiez le nœud du serveur LDAP qui contient l'objet utilisateur. Il s'agit également du nœud qui contient le nom unique de la racine ; tous les nœuds Utilisateur y sont répertoriés. Dans cet exemple, vous saisissez `ou=utilisateurs` dans le champ Base de recherche d'utilisateurs.

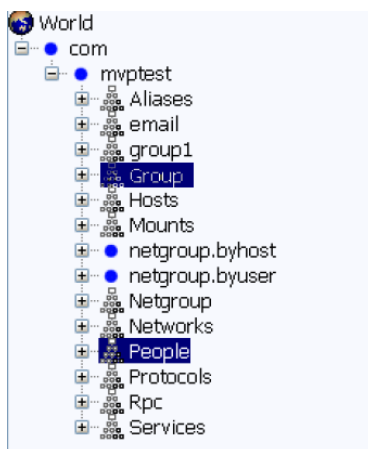


Si les utilisateurs se trouvent sur plusieurs niveaux hiérarchiques d'annuaires sur le serveur LDAP, procédez alors comme suit :

- a Déterminez chaque hiérarchie en amont commune à tous les emplacements possibles du nœud Utilisateur.
- b Incluez la configuration dans le champ Base de recherche d'utilisateurs.

Remarque : Sinon, vous pouvez également sélectionner **Activer la recherche d'utilisateurs imbriqués** puis laisser le champ Base de recherche d'utilisateurs vierge. De cette manière, Markvision recherche les utilisateurs dans l'arborescence complète du serveur LDAP en commençant par la base/le nom unique de la racine.

- **Filtre de recherche d'utilisateurs** : saisissez le paramètre d'après lequel rechercher un objet utilisateur sur le serveur LDAP. Dans cet exemple, vous saisissez `(uid={0})` dans le champ Filtre de recherche d'utilisateurs.



La fonction Filtre de recherche d'utilisateurs peut s'adapter à plusieurs conditions et expressions complexes, comme indiqué dans le tableau suivant.

Si vous souhaitez que l'utilisateur se connecte à l'aide du	Saisissez-le ensuite dans le champ Filtre de recherche d'utilisateurs
Nom commun	<code>(CN={0})</code>
Nom de connexion	<code>(sAMAccountName={0})</code>
Numéro de téléphone	<code>(telephoneNumber={0})</code>
Nom de connexion ou nom commun	<code>((sAMAccountName={0})(CN={0}))</code>

Remarques :

- Ces expressions s'appliquent *uniquement* au serveur LDAP Windows Active Directory.
- Pour le Filtre de recherche d'utilisateurs, le seul modèle valide est `{0}`, ce qui signifie que MVE recherchera le nom de connexion de l'utilisateur MVE.

4 Si vous souhaitez que Markvision recherche les *groupes* imbriqués sur le serveur LDAP, sélectionnez alors **Activer la recherche de groupes imbriqués**.

Pour préciser davantage la recherche, tapez les valeurs dans les champs appropriés.

- **Base de recherche de groupes** : tapez le nœud du serveur de communauté LDAP qui contient les groupes d'utilisateurs correspondant aux rôles Markvision. Il s'agit également du nœud qui contient le nom unique de la racine ; tous les nœuds Groupe (Rôle) y sont répertoriés.

Dans cet exemple, vous saisissez **ou=groupe** dans le champ Base de recherche de groupes.

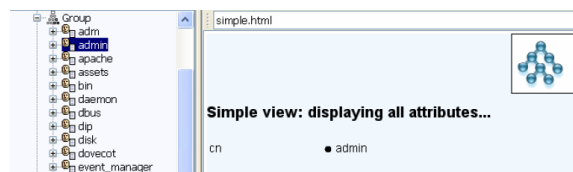


Remarque : Une Base de recherche comprend plusieurs attributs séparés par des virgules, tels que cn (nom commun), ou (unité organisationnelle), o (organisation), c (pays) et dc (domaine).

- **Filtre de recherche de groupes :** saisissez le paramètre d'après lequel rechercher un utilisateur dans un groupe correspondant à un rôle Markvision.

Remarque : Vous pouvez utiliser les modèles **{0}** et **{1}**, cela dépend de la configuration de schéma de votre serveur LDAP principal. Si vous utilisez **{0}**, MVE recherchera le nom unique de l'utilisateur LDAP. Le nom unique de l'utilisateur est récupéré en interne, pendant le processus d'authentification de l'utilisateur. Si vous utilisez **{1}**, MVE recherchera le nom de connexion de l'utilisateur MVE.

- **Attribut de rôle de groupe :** saisissez l'attribut contenant le nom complet du groupe (rôle). Dans cet exemple, vous saisissez **cn** dans le champ Attribut de rôle de groupe.



Remarque : Sélectionner **Activer la recherche d'utilisateurs imbriqués** et **Activer le recherche de groupes imbriqués** permet de spécifier la profondeur du serveur LDAP. Par défaut, la Recherche d'utilisateurs LDAP et la Recherche de groupes LDAP ont lieu au maximum à un niveau en dessous de la Base de recherche d'utilisateurs et de la Base de recherche de groupes spécifiées. Par conséquent, la Recherche imbriquée (sous-arborescence) est utilisée pour indiquer qu'il faut rechercher toutes les entrées de tous les niveaux imbriqués figurant en dessous de la Base de recherche d'utilisateurs et de la Base de recherche de groupes spécifiées. Ces Bases sont incluses.

Étape 2. Configurer les paramètres de liaison

Cette section permet de déterminer le protocole que le serveur MVE utilisera pour communiquer avec le serveur d'annuaires LDAP externe.

- 1 Cliquez sur **Informations de liaison**.

Remarques :

- Par défaut, si aucune configuration LDAP n'est stockée sous Markvision, la Liaison LDAP anonyme est automatiquement sélectionnée. Cela signifie que, pour utiliser le système de recherche du serveur LDAP, le serveur MVE ne produit pas son identité ou ses informations d'identification pour le serveur LDAP. Le suivi de la session de recherche LDAP s'effectuera exclusivement via une communication non cryptée.
- Le LDAP Windows Active Directory ne prend *pas* en charge l'option Liaison anonyme.

2 Si vous souhaitez que le serveur MVE produise son identité pour le serveur LDAP afin de pouvoir utiliser le système de recherche du serveur LDAP, configurez l'option Liaison simple.

a Sélectionnez **Liaison simple**.

b Dans le champ Nom unique de liaison, saisissez le nom unique de la liaison.

c Saisissez le mot de passe de liaison puis confirmez le mot de passe en le saisissant une nouvelle fois.

Remarques :

- Le Mot de passe de liaison dépend des paramètres de l'Utilisateur de la liaison du serveur d'annuaires LDAP. Si l'Utilisateur de la liaison est défini comme étant **Non vide** sur le serveur LDAP, un Mot de passe de liaison est requis. Si l'Utilisateur de la liaison est défini comme étant **Vide** sur le serveur LDAP, aucun Mot de passe de liaison n'est requis. Pour obtenir des informations sur les paramètres de l'Utilisateur de la liaison du serveur LDAP, contactez votre administrateur LDAP.
- L'option Liaison simple utilise une communication non cryptée entre le serveur MVE et le serveur LDAP.

3 Si vous souhaitez utiliser une communication cryptée entre le serveur MVE et le serveur d'annuaires LDAP, sélectionnez **TLS** (Transport Layer Security) ou **Kerberos V5 (Active Directory Windows)**.

Si vous avez sélectionné **TLS**, le serveur MVE devra entièrement s'authentifier sur le serveur d'annuaires LDAP en utilisant l'identité (Nom unique de liaison) et les informations d'identification (Mot de passe de liaison) du serveur MVE.

a Dans le champ Nom unique de liaison, saisissez le nom unique de la liaison.

b Saisissez le mot de passe de liaison puis confirmez le mot de passe en le saisissant une nouvelle fois.

Remarque : Le Mot de passe de liaison est requis.

Pour les certificats auto-signés, l'empreinte TLS doit être accessible au référentiel de la *Machine virtuelle Java* (JVM) nommé **cacerts** pour l'ensemble du système. Ce référentiel se situe dans le dossier [racine.mve]/jre/lib/security où [racine.mve] désigne le dossier d'installation de Markvision.

Si vous avez sélectionné **Kerberos V5 (Windows Active Directory)**, effectuez les opérations suivantes :

a Dans le champ Nom d'utilisateur du centre de distribution de clés, saisissez le nom du Centre de distribution de clés (KDC).

b Saisissez le mot de passe de centre de distribution de clés puis confirmez le mot de passe en le saisissant une nouvelle fois.

c Cliquez sur **Parcourir**, puis naviguez vers le dossier contenant le fichier *krb5.conf*.

Remarques :

- Pour plus d'informations sur le fichier de configuration Kerberos, consultez la documentation concernant votre protocole de sécurité Kerberos.
- Le protocole de sécurité Kerberos est *uniquement* pris en charge sous les versions de Windows Active Directory prenant en charge GSS-API.

d Sélectionnez le fichier puis cliquez sur **Ouvrir**.

Étape 3. Configurer les paramètres de mappage de rôle

- 1 Cliquez sur **Mappage de rôle**.
- 2 Tapez les valeurs dans les champs appropriés.
 - **Administrateur** : saisissez le rôle existant sous LDAP qui disposera de droits Administrateur sous MVE.
 - **Ressources** : entrez le rôle existant sous LDAP qui gèrera le module Ressources sous MVE.
 - **Stratégies** : entrez le rôle existant sous LDAP qui gèrera le module Stratégies sous MVE.
 - **Service Desk** : entrez le rôle existant sous LDAP qui gèrera le module Service Desk sous MVE.
 - **Gestionnaire des événements** : entrez le rôle existant sous LDAP qui gèrera le module Gestionnaire des événements.

Remarques :

- MVE associera automatiquement le groupe LDAP (Rôle) spécifié au rôle MVE qui lui correspond.
 - Vous pouvez attribuer un groupe LDAP à plusieurs rôles MVE et vous pouvez également taper plusieurs groupes LDAP dans un champ Rôle MVE.
 - Lorsque vous tapez plusieurs groupes LDAP dans les champs de rôle, séparez les groupes par un trait vertical (|). Si, par exemple, vous souhaitez inclure les groupes **admin** et **assets** pour le rôle Admin, tapez **admin | assets** dans le champ Admin.
- 3 Si vous choisissez de ne *pas* utiliser certains des rôles MVE, vous devez laisser les champs correspondants vides.


Remarque : Ceci s'applique à tous les autres rôles *sauf* au rôle Administrateur.
 - 4 Pour valider votre configuration, cliquez sur **Tester**.
 - 5 Tapez vos nom d'utilisateur et mot de passe LDAP, puis cliquez sur **Tester la connexion**.

La boîte de dialogue Résultats de la configuration LDAP de test s'affiche. En cas d'erreur, procédez comme suit :

- a Vérifiez les informations de la boîte de dialogue pour déterminer la cause des erreurs.
- b Mettez à jour les entrées des onglets Informations d'authentification, Informations de liaison et Mappage de rôle.
- c Répétez l'étape 4 à l'étape 5 jusqu'à ce que la boîte de dialogue Résultats de la configuration LDAP de test n'indique plus aucune erreur.

- 6 Cliquez sur **Appliquer > Fermer**.

Génération de rapports


- 1 Dans l'en-tête, cliquez sur .
- 2 Dans le menu déroulant Inclure les imprimantes, sélectionnez un groupe de périphériques d'après vos recherches précédentes mémorisées dans des signets.
- 3 Dans le menu déroulant Type de rapport, sélectionnez le type de données à afficher.

Sélectionner	Pour afficher
Etat du cycle de vie – Récapitulatif	Rapport récapitulatif des états du cycle de vie des périphériques.
Fabricant de l'imprimante – Récapitulatif	Rapport récapitulatif des fabricants de périphériques.
Modèle d'imprimante – Récapitulatif	Rapport récapitulatif des noms et numéros de modèle d'imprimante.


Sélectionner	Pour afficher
Fonctionnalités de l'imprimante	Feuille de calcul indiquant les fonctionnalités des périphériques.
Fonctionnalités de l'imprimante – Récapitulatif	Rapport récapitulatif des fonctionnalités des périphériques.
Etat du cycle de vie	Feuille de calcul indiquant les états du cycle de vie des périphériques.
Historique du nombre de pages	Feuille de calcul indiquant le nombre de pages traitées par les périphériques.
Compteur de maintenance	Feuille de calcul indiquant le compteur de maintenance des périphériques.
Versions du microcode	Feuille de calcul indiquant la version du microcode des périphériques.
Solutions eSF	Feuille de calcul indiquant les différentes solutions eSF (Embedded Server Framework) installées sur les périphériques.
Statistiques : Travaux par pages imprimées	Feuille de calcul indiquant le nombre de travaux exécutés par les périphériques.
Statistiques : Travaux par nombre de faces de support	Feuille de calcul indiquant le nombre de feuillets pour les tâches d'impression, de télécopie et de copie exécutées par les périphériques.
Statistiques : Travaux par utilisation du scanner	Feuille de calcul indiquant le nombre de travaux de numérisation exécutés par les périphériques.
Statistiques : Travaux par utilisation du télécopieur	Feuille de calcul indiquant le nombre de travaux de télécopie exécutés par les périphériques.
Statistiques : Travaux par informations sur les fournitures	Feuille de calcul indiquant des informations importantes sur chaque article de fourniture dans les périphériques.

- 4 Dans le menu déroulant Format du rapport, sélectionnez **PDF** ou **CSV**.
- 5 Si vous sélectionnez PDF, vous pouvez personnaliser le titre du rapport dans le champ Titre.
- 6 Si applicable, sélectionnez un groupe dans le menu déroulant Groupe.
- 7 Cliquez sur **Générer**.

Planification de tâches

- 1 Dans l'en-tête, cliquez sur .
- 2 Dans le menu déroulant Ajouter, effectuez l'une des opérations suivantes :
 - Sélectionnez **Audit**, puis sélectionnez un groupe de périphériques.
 - Sélectionnez **Recherche**, puis sélectionnez un profil de recherche.
 - Sélectionnez **Conformité**, puis sélectionnez un groupe de périphériques et un type de stratégie.
 - Sélectionnez **Mise en œuvre**, puis sélectionnez un groupe de périphériques et un type de stratégie.
 - Sélectionnez **Téléchargement de fichier générique**, puis sélectionnez un groupe de périphériques, un fichier et une destination. Seuls les utilisateurs possédant le rôle d'administrateur peuvent utiliser cette option.
- 3 Cliquez sur **Suivant**.
- 4 Dans le champ Nom, tapez le nom du nouvel événement programmé.
- 5 Sélectionnez les paramètres de votre choix, puis cliquez sur **Terminer**.

Affichage du journal système

1 Dans l'en-tête, cliquez sur .

Par défaut, la dernière activité dans la base de données apparaît en premier.

2 Pour afficher les activités par catégorie, procédez comme suit :

a Cliquez sur **Filtrer**.

b Dans la section Période, sélectionnez les dates de début et de fin.

c Dans le champ Identifiant(s), saisissez les numéros d'identification de tâche.

Remarque : Ce champ est facultatif.

d Dans la section Nom de la tâche, décochez la tâche que vous ne souhaitez pas inclure dans le fichier journal.

e Dans la section Catégories, décochez la catégorie que vous ne souhaitez pas inclure dans le fichier journal.

f Cliquez sur **OK**.

3 Cliquez sur **Préparation de l'exportation > Finaliser l'exportation**.

4 Dans le menu déroulant d'enregistrement, naviguez jusqu'au dossier dans lequel vous souhaitez enregistrer le fichier.

5 Dans le champ Nom du fichier, tapez le nom du fichier, puis cliquez sur **Enregistrer**.

6 Naviguez jusqu'au dossier dans lequel le fichier journal est enregistré, puis ouvrez-le pour afficher le journal système.

Foire aux questions

Quels sont les périphériques pris en charge par l'application ?

Pour obtenir la liste exhaustive des périphériques pris en charge, consultez les notes de version.

Comment changer mon mot de passe ?

Dans l'en-tête, cliquez sur **Modifier le mot de passe**, puis suivez les instructions qui s'affichent à l'écran.

Je ne peux pas sélectionner plusieurs périphériques dans la liste Modèles pris en charge de la boîte de dialogue Créer une stratégie. Pourquoi ?

Les paramètres de configuration et les commandes varient selon les modèles. Il arrive donc qu'une commande qui fonctionne sur un modèle ne fonctionne pas sur un autre. Afin d'éviter les dysfonctionnements, les stratégies sont limitées à un modèle à la fois.

Le meilleur moyen d'éviter de créer une stratégie inefficace est de créer une nouvelle stratégie, puis de l'attribuer à plusieurs périphériques.

Mes signets sont-ils accessibles par d'autres utilisateurs ?

Oui. Les signets sont globaux. Ils peuvent être affichés et gérés par tous les utilisateurs.

Où puis-je trouver les fichiers journaux ?

Naviguez jusqu'à ce répertoire pour rechercher les fichiers journaux suivants du programme d'installation : %TEMP%\

- *mve-*.log*
- **.isf*

Naviguez jusqu'à ce répertoire pour rechercher les fichiers journaux d'application :



<REP_INSTALL>\tomcat\logs, où <REP_INSTALL> est le dossier d'installation de Markvision.

Les fichiers contenus dans ce répertoire possédant le format **.log* sont les fichiers journaux d'application.

Dépannage

L'utilisateur a oublié son mot de passe

Pour réinitialiser le mot de passe d'un utilisateur, vous devez disposer de droits d'administrateur.

- 1 Dans l'en-tête, cliquez sur .
- 2 Dans l'onglet Utilisateur, sélectionnez un utilisateur, puis cliquez sur .
- 3 Changez le mot de passe.
- 4 Cliquez sur **OK**, puis sur **Fermer**.
- 5 Demandez à l'utilisateur de se connecter de nouveau.

L'application ne détecte aucun périphérique réseau

VÉRIFIEZ LES CONNEXIONS DE L'IMPRIMANTE.

- Vérifiez que le cordon d'alimentation est solidement branché sur l'imprimante et dans une prise de courant correctement mise à la terre.
- Assurez-vous que l'imprimante est allumée.
- Vérifiez que les autres appareils électriques branchés sur cette source d'alimentation électrique fonctionnent.
- Assurez-vous que le câble LAN est branché sur le serveur d'impression et sur le réseau local.
- Assurez-vous que le câble LAN fonctionne correctement.
- Redémarrez l'imprimante et le serveur d'impression.

ASSUREZ-VOUS QUE LE SERVEUR D'IMPRESSION INTERNE EST CORRECTEMENT INSTALLÉ ET ACTIVÉ.

- Imprimez une page de configuration pour l'imprimante. Le serveur d'impression apparaît dans la liste des pièces jointes de la page de configuration.
- Assurez-vous que le protocole TCP/IP du serveur d'impression est activé. Le protocole doit être activé pour que le serveur d'impression et l'application fonctionnent. Dans le panneau de configuration de l'imprimante, vérifiez que le protocole est actif.
- Reportez-vous à la documentation de votre serveur d'impression.

ASSUREZ-VOUS QUE LE NOM DU PÉRIPHÉRIQUE DANS L'APPLICATION EST LE MÊME QUE LE NOM DÉFINI DANS LE SERVEUR D'IMPRESSION.

- 1 Vérifiez le nom du périphérique défini dans l'application.

Dans la zone des résultats de recherche, recherchez l'adresse IP de l'imprimante.

Le nom du périphérique apparaît à côté de son adresse IP. Il s'agit du périphérique dans l'application et *non* du nom du périphérique sur le serveur d'impression.

- 2 Vérifiez le nom de périphérique défini sur le serveur d'impression. Pour plus d'informations, consultez la documentation du serveur d'impression.

VÉRIFIEZ QUE LE SERVEUR D'IMPRESSION COMMUNIQUE BIEN AVEC LE RÉSEAU.

- 1 Envoyez une requête Ping au serveur d'impression.
- 2 Si le ping fonctionne, vérifiez l'adresse IP, le masque de réseau ainsi que la passerelle du serveur d'impression pour vous assurer que ces paramètres sont corrects.
- 3 Eteignez l'imprimante et envoyez un nouveau ping afin de rechercher d'éventuels doublons d'adresses IP. Si le ping ne fonctionne pas, imprimez une page de configuration et vérifiez que la fonction IP est activée.
- 4 Si tel est le cas, vérifiez l'adresse IP, le masque de réseau ainsi que la passerelle pour vous assurer que ces paramètres sont corrects.
- 5 Assurez-vous que les ponts et les routeurs fonctionnent correctement et sont bien configurés.
- 6 Vérifiez que l'ensemble des connexions physiques entre le serveur d'impression, l'imprimante et le réseau fonctionnent.

Les informations relatives au périphérique sont incorrectes

Si les informations affichées par l'application au sujet d'un périphérique semblent incorrectes, effectuez un audit du périphérique.

Glossaire des termes de sécurité

Authentification	Une méthode pour identifier de façon sûre un utilisateur
Autorisation	Une méthode pour spécifier quelles fonctions sont disponibles à un utilisateur spécifique, par exemple qu'est-ce que l'utilisateur est autorisé à faire.
Construire des blocs	Les outils d'authentification et d'autorisation utilisés dans le Embedded Web Server. Ils comprennent : mot de passe, code PIN, comptes internes, LDAP, LDAP +GSSAPI, Kerberos 5 et NTLM.
Contrôles d'accès	Des paramètres qui contrôlent soit des menus, des fonctions et des valeurs individuellement, et à qui Aussi connu comme la Fonction de contrôle d'accès de certains périphériques.
Groupe	Un ensemble d'utilisateurs qui partagent les mêmes caractéristiques.
Modèle de sécurité	Un profil créé et sauvegardé dans le Embedded Web Server, utilisé conjointement avec les Contrôles d'accès pour gérer les fonctions de périphériques.

Index

A

- activation du serveur
- d'authentification LDAP 50
- affichage des détails d'un événement 47
- affichage des propriétés du périphérique 23
- ajouter un utilisateur 49
- alertes 2
- analyse de l'écran de démarrage 14
- analyse des ports 15
- analyse des protocoles 15
- aperçu 7
- assigner des mots-clés à un périphérique 28
- assigner un événement à un périphérique 47
- assigner une police 41
- auditer un périphérique 22

B

- base de données Firebird
 - restauration 10
 - sauvegarde 9

C

- catégories
 - ajout 28
 - édition 28
 - suppression 28
 - utilisation 27
- changement de mot de passe 58
- configuration des paramètres du système 49
- configuration système requise
 - Espace sur le disque dur 8
 - RAM 8
 - Résolution de l'écran 8
 - vitesse du processeur 8
- configurations système
 - configuration 49
- création d'un événement 46
- création d'un police d'un périphérique 31
- création d'un signet 27
- création d'une nouvelle police 30
- Créer un profil de recherche 18

D

- découverte de périphériques 18
- découverte de profil
 - création 18
 - édition 20
 - suppression 20
- Démarrer
 - écran d'accueil 14
- Dépannage
 - incapable de trouver un périphérique réseau 59
- Information sur le périphérique incorrecte 60
- réinitialisation du mot de passe utilisateur 59
- destination
 - création 45
 - édition 46
 - suppression 46

E

- écran d'accueil
 - compréhension 14
- édition d'un événement 46
- édition d'un profil de recherche 20
- édition d'un utilisateur 49
- édition d'une destination 46
- édition d'une police 40
- espace réservé 45
- Etat de l'alimentation 43
- état du cycle de vie du périphérique
 - Configuration 21
 - Géré 21
 - Géré (Manquant) 21
 - Géré (Modifié) 21
 - Géré (Normal) 21
 - Géré (Trouvé) 21
 - Hors service 21
 - Non-géré 21
- états du périphérique
 - vérification 43
- Etats Imprimante 43
- événement
 - affichage des détails 47
 - création 46
 - édition 46
 - suppression 46

- suppression d'un périphérique 47

F

- fichier de journal d'application
 - localisation 58
- fichier journal
 - localisation 58
- fichier journal d'installation
 - localisation 58
- fichiers
 - téléchargement 48
- forçage d'une police 41
- forçage de polices 43

G

- génération de rapports 55

I

- importation de périphériques depuis un fichier 20
- incapable de trouver un périphérique réseau 59
- Information sur le périphérique incorrecte 60

J

- journal système
 - affichage 57

L

- liste de modèles compatibles 58

M

- Markvision
 - accéder 10
 - installation 8
 - utilisation 12
- Markvision Enterprise
 - définition 7
 - mise à jour de la dernière version 9
- MarkVision Professional
 - migration vers Markvision Enterprise 11
- menu de gestion d'événement
 - utilisation 12

menu Général
 utilisation 49

menu polices
 utilisation 12

menu service desk
 en cours d'utilisation 12

migration de Markvision
 Professional vers Markvision
 Enterprise 11

mise à niveau de Markvision avec la
 dernière version disponible 9

mot de passe utilisateur oublié 59

mot de passe, utilisateur
 réinitialisation 59

mots-clés
 ajout 28
 assigner à un périphérique 28
 édition 28
 suppression 28
 suppression d'un périphérique 29
 utilisation 27

MVE
 migré de 11

MVP
 importé dans Markvision
 Enterprise 11
 migration vers Markvision
 Enterprise 11

N

noms de système
 vérification 59

O

onglets ressources
 utilisation 12

P

page web intégrée
 visionnage 44

périphérique
 affichage des détails d'un
 événement 47
 assignation d'un événement 47
 assignation de mots-clés 28
 audit 22
 importation depuis un fichier 20
 suppression d'un événement 47
 suppression d'un mot-clé
 assigné 29
 vérification des statuts 43

visionner à distance 44
 visionner les propriétés 23

périphérique, alertes
 réception 49

périphérique, nom de l'hôte
 acquisition 49

périphériques
 découverte 18
 recherche de 24

périphériques pris en charge 58

police
 assigné 41
 création 30
 créer à partir d'un
 périphérique 31
 édition 40
 forcer 41
 suppression 40, 42
 types 30
 vérification de la conformité 41

polices
 forcer 43
 géré 30
 vérification de la conformité du
 périphérique 43

ports
 compréhension 15

propriétés, périphérique
 visionnage 23

protocoles
 compréhension 15

R

RAM 8

rapports
 génération 55

Réception d'alertes d'un
 périphérique 49

recherche avancée 24

recherche de périphériques 24

réinitialisation du mot de passe
 utilisateur 59

restauration d'une base de données
 Firebird 10

S

sauvegarder une base de données
 Firebird 9

Serveur LDAP
 activation de l'authentification 50

serveurs de base de données
 supporté 8

serveurs de base de données pris
 en charge 8

signet par défaut, utilisant 24

signets
 accéder 27
 création 27
 suppression 27

suppression d'un événement 46

suppression d'un événement d'un
 périphérique 47

suppression d'un mot-clé assigné
 d'un périphérique 29

suppression d'un profil de
 recherche 20

suppression d'un signet 27

suppression d'un utilisateur 49

suppression d'une destination 46

suppression d'une police 40, 42

T

tâches
 organiser 56

tâches planifiées 56

téléchargement de fichiers
 génériques 48

U

utilisateur
 ajout 49
 édition 49
 suppression 49

utilisation des catégories 27

utilisation des mots-clés 27

V

vérification de l'état du
 périphérique 43

vérification de la conformité avec la
 police 41

vérification de la conformité du
 périphérique avec les polices 43

Visionnage d'un périphérique à
 distance 44

Visionnage d'une page web
 intégrée 44

Visionnage du journal système 57

vitesse du processeur 8

Z

Zone Aperçu Résultats de
Recherche 14

zone d'information de Tâche 14

zone Header 14

zone Résultats de Recherche 14

zone signet et recherche

avancée 14