Guide de l’utilisateur

Policy Manager pour Intellex®

Version 1.2

Numéro d’article 8200-0566-04 A0

Remarque

Les informations dans le présent manuel étaient actuelles au moment de leur publication. Le fabricant se réserve le droit de revoir et améliorer ses produits. Pour cette raison, toutes les caractéristiques sont soumises à des modifications sans préavis.

Copyright

American Dynamics
6795 Flanders Drive
San Diego, CA 92121-2903 États-Unis

Service clients

Merci d'utiliser les produits d'American Dynamics. Nous assurons le support de nos produits au travers d'un réseau international de distributeurs. Le distributeur chez lequel vous avez acquis ce produit est votre point de contact si vous avez besoin de services ou de support. Nos distributeurs sont habilités pour offrir la meilleure qualité de service et de support à nos clients. Les distributeurs devraient contacter American Dynamics au (800) 507-6268 ou au +1 (561) 912-6259 ou sur le Web à www.americandynamics.net.

Marques commerciales

Intellex® est une marque déposée de Sensormatic Electronics Corporation. IntelleCord™ et Smart Search™ sont des marques déposées de Sensormatic Electronics Corporation. Windows® est une marque déposée de Microsoft Corporation. PS/2® est une marque déposée de International Business Machines Corporation. Sony® est une marque déposée de Sony Corporation.

Des noms de marque commerciale sont utilisés au travers de ce manuel. Plutôt que de placer un symbole à chaque occurrence, les noms de marque commerciale sont indiqués par des majuscules initiales. L'inclusion ou l'exclusion du symbole ne constitue pas un jugement sur la validité ou le statut légal du terme.

Avertissements

AVERTISSEMENT : POUR ÉVITER LES DÉCHARGES ÉLECTRIQUES, N'ENLEVEZ JAMAIS LE COUVERCLE. AUCUN COMPOSANT RÉPARABLE PAR L'UTILISATEUR NE SE TROUVE À L'INTÉRIEUR DE CE BOÎTIER. CONFIEZ TOUTES LES RÉPARATIONS À DES PROFESSIONNELS QUALIFIÉS.
N'EXPOSEZ JAMAIS CET APPAREIL À LA PLUIE OU À DE L'HUMIDITÉ.
N'INSTALLEZ JAMAIS CE PRODUIT DANS DES ZONES DANGEREUSES OÙ DES PRODUITS COMBUSTIBLES OU EXPLOSIFS SONT UTILISÉS OU ENTREPOSÉS.

Le symbole de la foudre/pointe de flèche dans un triangle indique qu'il y a danger de décharges électriques au sein du boîtier du produit.

Attention : Il y a risque d'explosions si la batterie est mal remplacée.

Ne la remplacez qu'avec le même type ou son équivalant, recommandé par le fabricant de la batterie. Éliminez les anciennes batteries conformément aux instructions du fabricant.

VORSICHT: ZUR VERMEIDUNG EINES STROMSCHLAGES DARF DAS GEHÄUSE NICHT ENTFERNT WERDEN. ES ENTHÄLT KEINE VOM BENUTZER ZU WARTENDEN TEILE. ÜBERLASSEN SIE DIE WARTUNG NUR QUALIFIZIERTEM FACHPERSONAL.

Attention : Es besteht die Gefahr einer Explosion, wenn die Batterie nicht ordnungsgemäß ausgetauscht wird.

N205

AVERTISSEMENT : CET ÉQUIPEMENT EST UN PRODUIT LASER DE CATÉGORIE 1 CONTENANT UNE DIODE LASER DE CATÉGORIE 1 ET IL EST CONFORME AUX STANDARDS DE PERFORMANCE DE RADIATION DE LA FDA, 21 CFR SOUS-CHAPITRE J ET DE LA CANADIAN RADIATION EMITTING DEVICES ACT, REDR C1370.

Montage en rack

Consultez auprès du fournisseur de votre rack à propos des moyens de montage en rack appropriés, en tenant compte du poids de ce produit.

Consultez auprès du fabricant de votre rack à propos du matériel adéquat et de la procédure pour monter ce produit en toute sécurité.

Évitez les charges inégales ou les instabilités mécaniques lorsque vous montez des unités dans un rack.

Assurez-vous que les unités soient installées de façon à permettre un débit d'air suffisant pour permettre le fonctionnement en toute sécurité.

La température maximale pour les unités montées en rack est de 40 °C.

Évitez les charges inégales ou les instabilités mécaniques lorsque vous montez des unités dans un rack.

Consultez l'étiquette du produit à propos des exigences en alimentation électrique pour assurer qu'aucune surcharge ou intensité excessive ne puisse survenir.

La mise à la terre doit être fiable et indépendante d'autres connexions.

AVERTISSEMENT : CET ÉQUIPEMENT A ÉTÉ TESTÉ ET TROUVÉ CONFORME AUX LIMITES POUR UN DISPOSITIF NUMÉRIQUE DE CLASSE A, CONFORME À LA SECTION 15 DES DIRECTIVES FCC. CES LIMITES ONT POUR OBJECTIF D'OFFRIR UNE PROTECTION RAISONNABLE CONTRE DES INTERFÉRENCES NOCIVES LORSQUE L'ÉQUIPEMENT EST UTILISÉ DANS UN ENVIRONNEMENT COMMERCIAL. CET ÉQUIPEMENT GÉNÈRE, UTILISE ET PEUT IRRADIER DE L'ÉNERGIE DE FRÉQUENCES RADIO ET PEUT, S'IL N'EST PAS INSTALLÉ ET UTILISÉ SELON LE MANUEL D'INSTRUCTIONS, PROVOQUER DES INTERFÉRENCES AUX COMMUNICATIONS RADIOPHONIQUES. L'UTILISATION DE CET ÉQUIPEMENT DANS DES ZONES RÉSIDENTIELLES PROVOQUERA PROBABLEMENT DES INTERFÉRENCES NOCIVES ET DANS CE CAS, L'UTILISATEUR DEVRA ÉLIMINER LES INTERFÉRENCES À SES FRAIS.

Des changements ou des modifications non-autorisées expressément par l'organisme responsable de la conformité, pourraient annuler l'autorité de l'utilisateur pour utiliser l'équipement.

REMARQUE : Ce produit a été vérifié par la FCC sous des conditions de test comprenant l'utilisation de câbles E/S et des connecteurs blindés entre les composants du système. Pour être conforme aux directives FCC, l'utilisateur doit utiliser des câbles et des connecteurs blindés pour tous les câbles, à l'exception des câbles d'alimentation et les câbles d'alarmes.

This digital apparatus does not exceed the Class A limits for radio noise emissions as set out in the Radio Interference Regulations (ICES-003) of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables de la Classe A prescrites dans le Réglement (ICES-003) sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.

Informations de licence

LISEZ LE PRÉSENT ACCORD DE LICENCE AVANT D'OUVRIR L'EMBALLAGE DU DISQUE, D'INSTALLER LE LOGICIEL OU D'UTILISER VOTRE SYSTÈME.

LE PRÉSENT ACCORD DE LICENCE DÉFINIT VOS DROITS ET OBLIGATIONS. EN ROMPANT LE SCEAU DE CET EMBALLAGE, INSTALLANT LE LOGICIEL OU UTILISANT VOTRE SYSTÈME, VOUS VOUS DÉCLAREZ D'ACCORD AVEC TOUS LES TERMES ET CONDITIONS DU PRÉSENT ACCORD. SI VOUS N'ÊTES PAS D'ACCORD AVEC TOUS LES TERMES ET CONDITIONS DU PRÉSENT ACCORD, VOUS POUVEZ, AVANT 30 JOURS, RETOURNEZ CET EMBALLAGE, TOUTES LES DOCUMENTATIONS ET TOUS LES MATÉRIAUX D'ACCOMPAGNEMENT AU POINT D'ACQUISITION AFIN D'OBTENIR UN REMBOURSEMENT.

LICENCE DE LOGICIEL

Le logiciel inclut l'API Intellex, les programmes modulaires et les codes source fournis en tant qu'exemples, le manuel API Intellex et toute documentation électronique ; elle vous est attribuée en installant le logiciel sur le disque dur d'un ordinateur. Le logiciel est fourni sous licence, il n'est pas vendu.

ATTRIBUTION DE LICENCE

L'acquisition du logiciel API Intellex constitue un accord de licence entre Sensormatic et vous. Cet accord de licence vous autorise, à vous et uniquement à vous, d'utiliser le logiciel. En acquérant l'accord de licence API Intellex, vous pouvez utiliser le logiciel API et les programmes modulaires d'accompagnement avec leurs codes source. Cet accord de licence ne vous attribue pas le droit de revendre ni de distribuer l'API ou les programmes modulaires et leurs codes source ni de copies supplémentaires à une autre entité. La licence pour le logiciel n'est valable que s'il est utilisé avec l'équipement Intellex. Il n'y a pas de restrictions pour initialiser un programme de licence interne à votre organisation concernant les produits logiciels que vous développez en utilisant l'API ; cependant, aucun programme logiciel que vous développez en utilisant l'API Intellex ou les programmes modulaires ne peuvent être vendus ni distribués par vous ou par d'autres entités en tant que produits accessoires à la ligne de produits Intellex sans avoir obtenu l'autorisation de Sensormatic.

AUTRES DROITS ET LIMITATIONS

- Une copie de démo du logiciel est considérée acquise et est couverte par le présent accord de licence.
- Le bon de commande est votre preuve de licence pour exercer les droits définis ici et vous devez le conserver.
- Vous ne pouvez pas décompiler, désassembler ou pratiquer l'ingénierie inverse sur aucun des exécutables ; y compris, sans toutefois s'y limiter, les fichiers de librairie, pour lesquels vous n'avez pas obtenu le code source. Les programmes modulaires sont exclus de cette restriction et vous pouvez les recompiler, ré-assembler ou modifier tout composant du code source qui vous a été fourni.
- Vous ne pouvez pas émettre de sous-licences, louer ou donner en leasing le logiciel ; ni transférer de manière permanente le logiciel à des tiers en leur donnant le support original comprenant le paquet de logiciels et la licence.
- Sensormatic se réserve le droit de résilier immédiatement le présent accord si vous ne respectez pas les termes et conditions du présent accord. Dans un tel cas, vous devez détruire tous les logiciels API Intellex sur et/ou chargé à partir du CD-ROM acquis, tous les logiciels API téléchargés du web ou envoyés sur des supports « patch », tous les programmes modulaires que vous avez modifiés et tous les logiciel que vous avez développé en utilisant l'API Intellex.
- Le logiciel peut contenir des logiciels de tiers qui sont porteurs d'une licence spéciale ; un Accord de Licence d'Utilisateur Final (EULA). Lisez et conservez toute la documentation de licence qui pourrait être incluse avec le logiciel. La conformité avec les termes d'éventuels tiers EULA est requise en tant que condition du présent accord.

La non-conformité avec ces restrictions entraînera la résiliation immédiate de la présente licence et permettra à Sensormatic, l'utilisation d'autres moyens légaux.

COPYRIGHT

Le logiciel est un produit propriétaire de Sensormatic et il est protégé par les lois sur le copyright des États-Unis et internationales.

MISES À NIVEAU

Si le logiciel est une mise à niveau d'une autre version du logiciel ou une mise à niveau d'un composant du paquet de logiciels pour lequel vous avez une licence, vous ne pouvez utiliser ou transférer le logiciel que selon les spécifications du présent accord.

GARANTIE LIMITÉE

Sensormatic garantit que le support sur lequel ce logiciel est enregistré et la documentation qui l'accompagne est libre de défaut matériel et de main-d'oeuvre pour une période de 90 jours à compter de la date de livraison au premier utilisateur. En outre, Sensormatic garantit que lors de la même période, le logiciel fourni sur le support d'enregistrement sous la présente licence aura des performances comme décrites dans la documentation pour l'utilisateur fournie avec le produit s'il est utilisé avec le matériel et l'environnement de développement spécifié.

RECOURS DES CLIENTS

La seule responsabilité de Sensormatic et votre unique recours sous cette garantie sera, selon l'option choisie par Sensormatic, de a) essayer de corriger les erreurs logicielles par des actions que nous croyons appropriées pour résoudre le problème, b) remplacer gratuitement le support d'enregistrement, le logiciel ou la documentation par des équivalents fonctionnels comme applicable ou c) rembourser le montant de la licence et résilier le présent accord. Tout élément de remplacement restera sous garantie pendant la période restante de la garantie originale. Aucun recours n'est prévu pour des dysfonctionnements de la disquette ou du logiciel si un tel dysfonctionnement est le résultat d'un accident, d'une mauvaise utilisation, d'une altération ou d'une application erronée. Les services ou l'assistance sous garantie seront fournis au point d'acquisition original.

AUCUNE AUTRE GARANTIE

La présente garantie remplace toute autre garantie, expresse ou implicite, y compris et sans s'y limiter la garantie impliquée de sa qualité marchande ou l'adéquation à un besoin ou à un usage particulier. Aucune information ni aucun conseil oral ou écrit donné par Sensormatic, ses représentants, distributeurs ou revendeurs ne constituera une garantie additionnelle et vous ne pourrez pas vous appuyer sur de telles informations ou de tels conseils.

AUCUNE RESPONSABILITÉ POUR DES DOMMAGES DE CONSÉQUENCE

En aucun cas Sensormatic ne sera responsable pour des dommages directs, indirects ou de conséquence provenant de l'utilisation ou de l'incapacité d'utilisation du logiciel ou de la documentation. Cette limitation sera applicable même si Sensormatic ou un représentant autorisé avaient été informés à propos de la possibilité de tels dommages. En outre, Sensormatic ne garantit pas que l'utilisation du logiciel sera sans aucune interruption ou totalement libre d'erreurs.

Cette garantie limitée vous attribue des droits légaux spécifiques. Vous pourriez avoir d'autres droits, selon votre pays de résidence. Certains états ne permettent pas de limitations sur les dommages indirects ou de conséquence concernant la période de garantie impliquée, la limitation ou l'exclusion mentionnée pourrait donc ne pas vous concerner.

GÉNÉRALITÉS

Si une des provisions de l'accord était prouvée illégal, invalide ou non-applicable pour une raison ou une autre, cette provision sera retirée du présent accord, ce qui n'influencera d'aucune manière la validité et l'applicabilité des provisions restantes. Cet accord est soumis aux lois de l'état de Floride, États-Unis.

Vous devez conserver une preuve du montant payé pour la licence, y compris le numéro de modèle, le numéro de série et la date de payement et présenter cette preuve lorsque vous avez besoin de services ou d'assistance couverts par la présente garantie.

DROITS RESTREINTS DU GOUVERNEMENT DES ÉTATS-UNIS

Le logiciel et sa documentation sont fournis avec des DROITS LIMITÉS. L'utilisation, la duplication ou la publication par le gouvernement des Etats Unis est limitée par les restrictions exprimées dans le sous-paragraphe (c)(1)(ii) de la clausule des Droits sur les données techniques et logiciels d'ordinateur sous DFARS 252.227-7013 ou les sous-paragraphes (c)(1) et (2) de Logiciels commerciaux d'ordinateurs - Droits limités sous 48 CFR 52.227-19, selon ce qui est applicable. Le fabricant est Sensormatic Electronics Corporation, 6600 Congress Ave., Boca Raton, FL 33487, États-Unis.

Informations importantes

Avant de continuer, veuillez lire et appliquer toutes les instructions et avertissements contenus dans ce manuel. Conservez ce manuel avec la facture de vente originale en tant que référence future et, si nécessaire, le service de garantie.

Lorsque vous déballez votre unité Intellex, vérifiez s'il y a des éléments manquants ou endommagés. S'il y a des éléments manquants ou s'il y a des dommages évidents, N'INSTALLEZ NI UTILISEZ CE PRODUIT. Contactez Sensormatic ou votre distributeur pour de l'assistance.

Pour vos archives

Renseignez les informations d'acquisition de produit suivantes : L'usine vous demandera ces informations lorsque vous la contactez pour du support technique. Ces informations sont également très utiles en cas de perte ou de vol.

Date d'acquisition :

Numéro de série :

Clé de licence

Le logiciel Intellex 4.0 est protégé des utilisations non-autorisées par une clé logicielle de licence. Cette clé correspond au matériel électronique de votre système avec la version logicielle autorisée et le niveau des fonctions de votre logiciel pour permettre le fonctionnement correct de votre système. Toute modification à l'adaptateur réseau dans votre unité, suppression ou modification du fichier de licence ou remplacement du disque système, affectera le fonctionnement normal et exigera l'installation d'un nouveau fichier de licence. Veuillez contacter votre représentant Sensormatic autorisé pour de plus amples informations.

Table des matières

Policy Manager

Caractéristiques 2
Vue de Intellex Management Suite 3

Icônes

Ce que signifient les images des icônes et leurs vues 5

Travailler avec des politiques par le biais de Politiques globales du site

Gérer la sécurité avancée d'Intellex par le biais des Paramètres de sécurité

Les éléments d'Intellex sécurisables fonctionnant en mode Sécurité avancée 9
Menu Instruments 10
Ajouter un instrument 10
Supprimer un instrument 11
Associer un instrument à un site différent 11
Éditer les paramètres de sécurité d'un Intellex 12
Ajouter ou Retirer des utilisateurs ou groupes d'utilisateurs 13
Propager (copier) les paramètres de sécurité d'un Intellex à un autre 16

Travailler avec des zones

Menu Zones de sécurité 17
La zone des instruments non attribués 17
Création d'une nouvelle zone (regrouper des instruments avec des propriétés de sécurité communes) 18
Supprimer une zone 18
La vue Zone unique 18
Le menu Zone unique 19
Déplacer une unité Intellex vers une zone de sécurité 20
Remplacer un Intellex 20

Travailler avec le Gestionnaire de licences

Licence corporative Network Client 24

Travailler avec la Visualisation d’événements

Ajouter le Snap-in Visualisation d’événements 26

Annexe A : Concepts de sécurité pour Policy Manager 29

Questions de base 29
Authentification 30
Qui êtes vous et êtes-vous qui vous prétendez être ? 30
La session Windows 30
Politiques et permissions de site 31
Autorisation 31
À quoi voulez-vous accéder ? 31
Que voulez-vous en faire une fois que vous l’avez obtenu ? 32
Descripteurs de sécurité 32
Utilisateurs, groupes et héritages 33
Trois formes de permissions d’accès 34
Accès implicite 34
Accès explicite 34
Refus explicite 34

Annexe B : Forum aux questions 35

Que signifie propagation ? 35
Que signifie héritage ? 35
Que se passe-t-il lorsque je propage vers un unique instrument ou groupe d’instruments ? 36
Que sont des instruments par défaut ? 36
Quelle est la différence entre un instrument actif et un instrument inactif ? 36

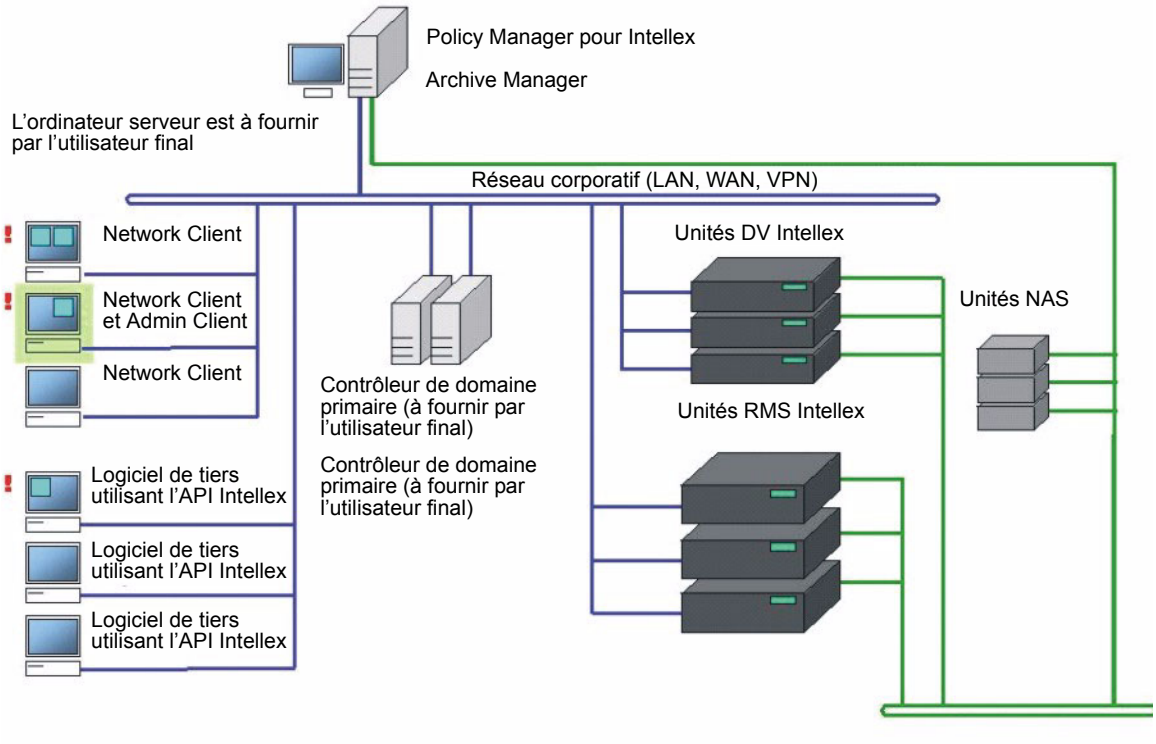
Annexe C : Liste des fonctionnalités sécurisables 37

Index 41

Policy Manager

Intellex® Policy Manager (PM) v1.2 est un produit logiciel installé sur un serveur. Il réside sur le même réseau que les unité Intellex, les postes Network Client et/ou les autres applications à distance basées API et assure la sécurité avancée du réseau vidéo. En implémentant la sécurité avancée, les clients peuvent :

- Arriver à un niveau plus élevé et plus sévère de sécurité en ce qui concerne l'accès à et l'utilisation des ressources et fonctions d'Intellex.
- Profiter d'un niveau de sécurité Microsoft pour leurs informations vidéo.
- Administrer centralement un contrôle de sécurité sur plusieurs unités Intellex.



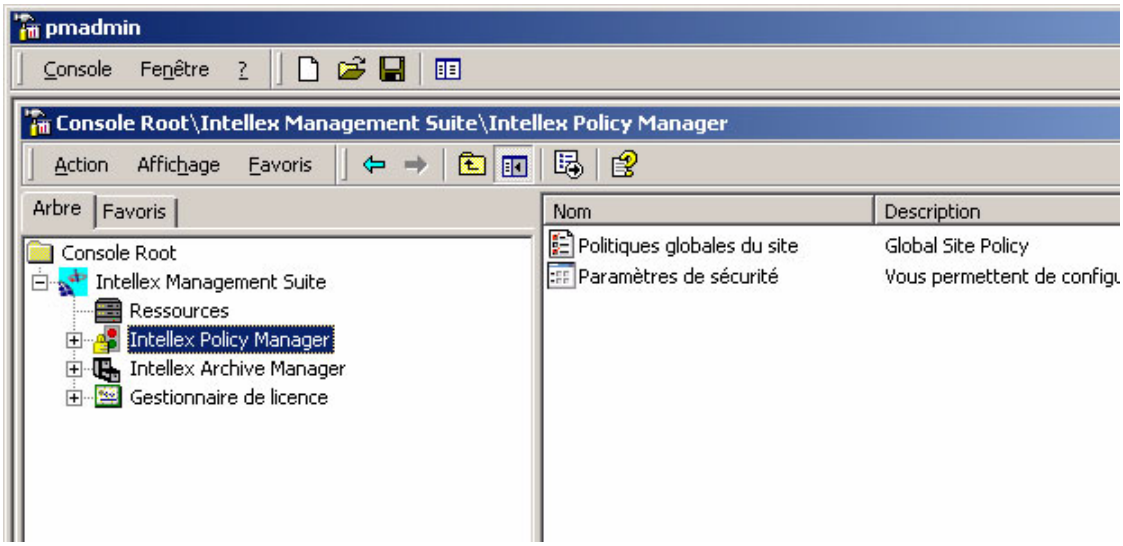
Caractéristiques

- Le client d'administration pour Policy Manager s'intègre dans la console de gestion Microsoft (Microsoft Management Console - MMC) de façon que l'administration de la sécurité Intellex sera égale à l'administration d'autres applications réseau.
- En outre d'assurer une granularité plus élevée à la sécurisation indépendante des caractéristiques et fonctions d'Intellex, Policy Manager s'intègre à la sécurité de Microsoft Windows. Cela permet aux utilisateurs d'apprendre facilement comment naviguer dans l'IGU et d'administrer la sécurité ou d'ajouter des groupes d'Intellex et des groupes d'utilisateurs, puisque Policy Manager hérite le maximum possible d'éléments de l'IGU. En conséquence, Policy Manager peut assurer la sécurité avancée pour Intellex.
- Par le biais de Policy Manager, les administrateurs IT peuvent intégrer des systèmes vidéo Intellex dans leur réseau existant, sans avoir à compromettre aucune politique de sécurité de réseau qu'ils avaient mis en place. Policy Manager s'intègre dans la console MS Windows et hérite des protocoles de sécurité que l'organisation utilisait déjà. Par conséquence, les administrateurs IT ne sont pas obligés d'introduire de nouveaux protocoles de mise en réseau rien que pour de la vidéo. Même si les organisations continuent à exécuter la vidéo sur un réseau LAN privé séparé de leur LAN/WAN corporatif, la sécurité avancée de Policy Manager élimine les soucis de l'administrateur IT concernant les brèches de sécurité dans le réseau corporatif causées par le trafic au travers du réseau vidéo passant par les systèmes IT partagés (murailles coupe-feu, routeurs, etc.).
- Policy Manager permet à l'administrateur de sécurité d'administrer les accès locaux et à distance sur plusieurs unités Intellex de manière centralisée.
- Les administrateurs de sécurité peuvent attribuer différents niveaux d'accès à différents utilisateurs des fonctions et ressources d'Intellex, outrepassant ce que peuvent offrir les concepts de sécurité classiques.
- Policy Manager permet la gestion de ressources et la détection d'erreurs pour les unités Intellex en réseau. Le serveur détecte quelles unités deviennent disponibles ou non et apporte les entrées appropriées au journal système.
- Vous pouvez surveiller l'état et les rapports d'erreur par le biais de journaux d'événements du système. Policy Manager crée et maintient son propre journal d'événements, intégré dans le mécanisme existant de journaux, fourni par le système d'exploitation. Tous les accès d'administration ainsi que la disponibilité des instruments sont mis en journal. En outre, les violations d'accès sont détectées et publiées dans le journal d'événements. Utiliser la visualisation d'événements de Microsoft pour visualiser les journaux localement ou à distance.

Remarque

Les illustrations dans le présent manuel s'appliquent à une application sous Windows 2000. Votre écran pourrait avoir un aspect différent.

Vue de Intellex Management Suite



L'arborescence des répertoires est composée de 4 écrans principaux :

Ressources	Cet écran montre le groupe d'instruments de tous les types et états.
Intellex Policy Manager	Cet écran forme l'outil de gestion de la sécurité avancée.
Intellex Archive Manager	Cet écran forme l'outil pour archiver et récupérer des données de stockage connecté au réseau. Archive Manager n'est disponible que si cette icône est présente.
Gestionnaire de licence	Cet écran vous permet de surveiller et de mettre à jour les informations de licence actuelles.

Icônes

Ce que signifient les images des icônes et leurs vues

Image	Vue
	Cette icône représente la Intellex Management Suite.
	Cette icône représente les ressources.
	Cette icône représente le programme Policy Manager.
	Cette icône représente les politiques appliquées globalement par Policy Manager sur chaque instrument et utilisateur de votre site.
	Cette icône représente les paramètres de sécurité que vous pouvez appliquer sélectivement aux instruments et zones de votre site.
	Cette icône représente tous les instruments Intellex sécurisés dans votre système.
	Cette icône représente un unique instrument Intellex opérationnel sous sécurité avancé.
	Cette icône représente un instrument Intellex sécurisé (en mode sécurité avancé) qui n’est pas opérationnel.
	Cet icône représente une ressource non sécurisée (pas en mode sécurité avancée) en fonctionnement.
	Cet icône représente une unité Intellex non sécurisée (pas en mode sécurité avancée) qui n'est pas en fonctionnement.
	Cette icône représente les zones de sécurité qui vous permettent d’organiser des instruments Intellex dans des unités de sécurité gérées séparément.
	Cette icône représente une unique zone de sécurité contenant un groupe d’instruments partageant des paramètres de sécurité communs.
	Cette icône représente la licence d’un module spécifique, tel que Policy Manager ou Archive Manager.
	Cette icône représente un groupe de gestion de licence.

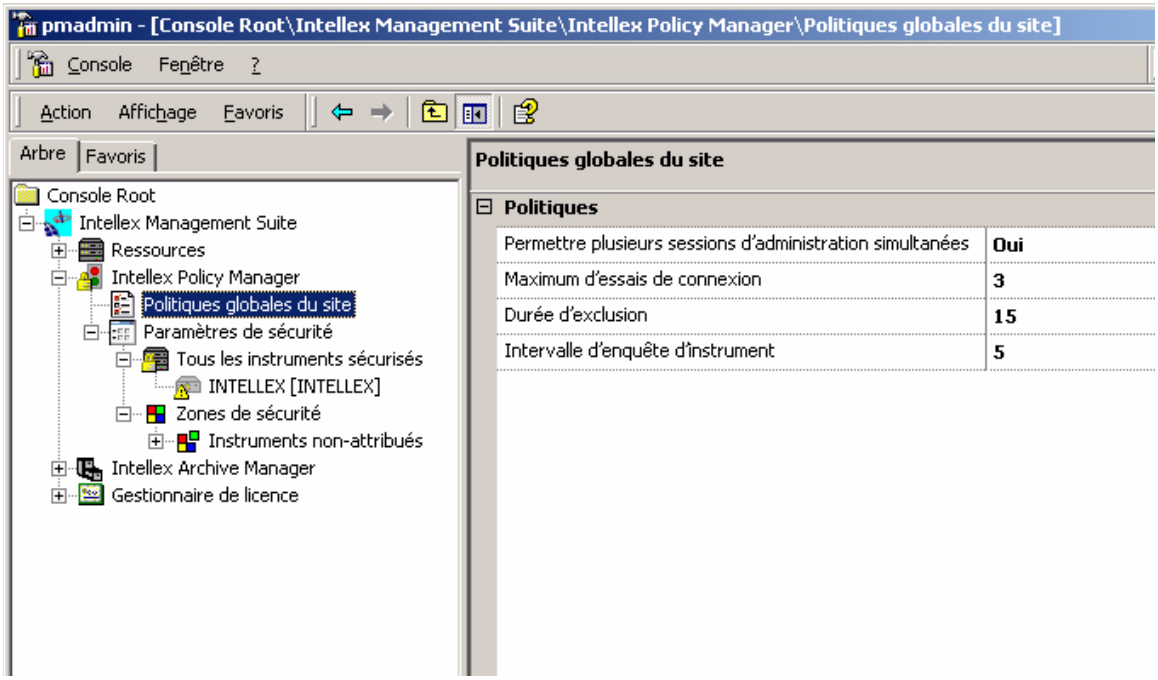
Remarque

Cette fenêtre offre des vues optionnelles des objets. Les visualisations sont Grandes icônes, Petites icônes, Liste ou Détails.

Travailler avec des politiques par le biais de Politiques globales du site

Le nœud Global Site Policies dans Policy Manager fournit les stratégies que le système de sécurité applique au site sur une base globale. L'illustration ci-dessous montre comment les informations sont affichées dans le volet de droite lorsque vous sélectionnez Politiques globales du site.

1. Sélectionnez Politiques globales du site pour afficher le volet de droite. Le volet est divisé en deux colonnes ; les politiques à la gauche et leurs propriétés à la droite.
2. Éditez les Politiques globales du site directement dans la colonne de droite.

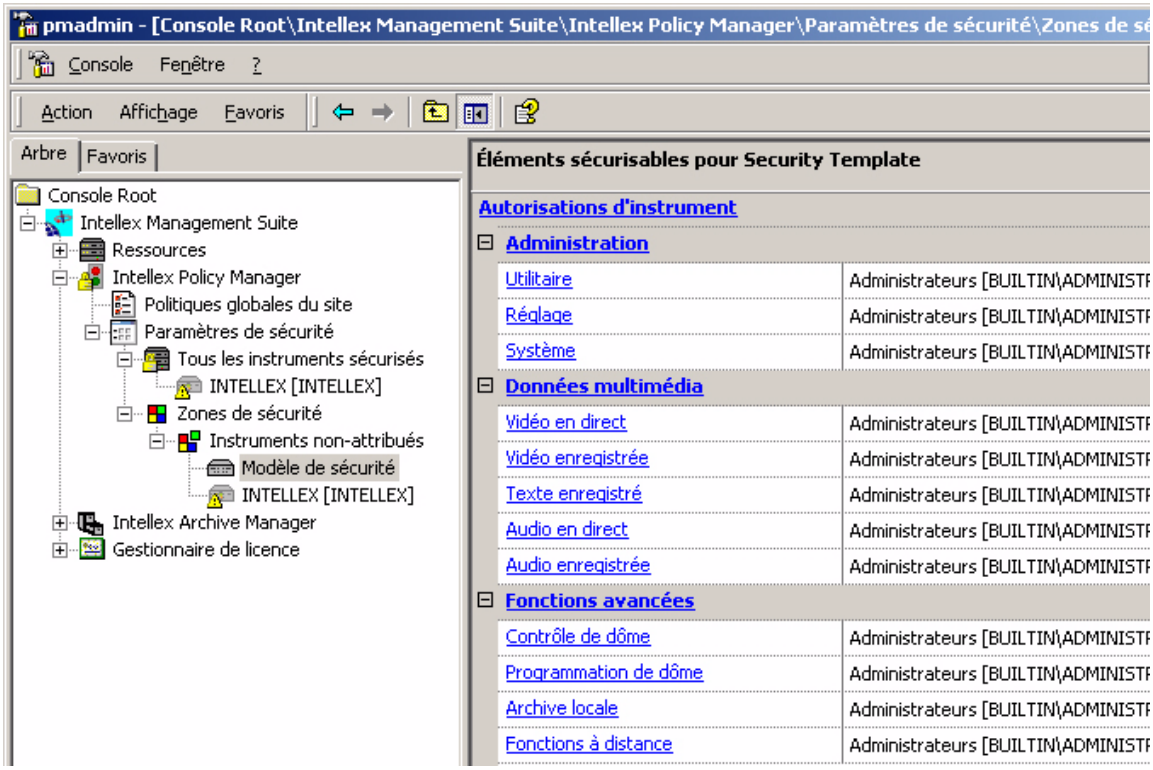


Action :	Description :
Sélectionnez la case dans la colonne à la droite de Permettre plusieurs sessions d'administration simultanées.	Une case de sélection Oui/Non est affichée. Sélectionnez Oui pour permettre que plusieurs administrateurs puissent accéder et contrôler simultanément ce site. Sélectionnez Non pour n'autoriser qu'une seule session d'administration pour accéder et contrôler ce site. Oui est sélectionné par défaut.
Sélectionnez la case dans la colonne à la droite de Maximum d'essais de connexion.	Affiche une valeur numérique avec un minimum et un maximum prédéfinis. Insérez le nombre d'essais de connexion consécutifs permis par le système avant l'exclusion de l'utilisateur pendant une période prolongée. Un message vous indiquera si des valeurs sont hors limites. La valeur par défaut est 3.
Sélectionnez la case dans la colonne à la droite de Durée d'exclusion.	Affiche une valeur numérique en minutes avec un minimum et un maximum prédéfinis. Insérez le nombre de minutes que l'utilisateur doit attendre avant de pouvoir se connecter au système une fois que le maximum d'essais de connexion avait été atteint. Un message vous indiquera si des valeurs sont hors limites. Le système n'accepte pas des valeurs inférieures à une minute. La durée maximale est illimitée. La valeur par défaut est de quinze minutes.
Sélectionnez la case dans la colonne à la droite de Intervalle d'enquête d'instrument.	Affiche une valeur numérique en minutes avec un minimum et un maximum prédéfinis. L'intervalle d'enquête d'instrument est le temps, en minutes, entre les enquêtes d'instruments actifs consécutives. Les instruments sont vérifiés régulièrement pour assurer qu'ils sont toujours actifs et disponibles pour utilisation. Insérez le nombre de minutes, entre les envois d'enquêtes d'instruments. Un message vous indiquera si des valeurs sont hors limites. Le système n'accepte pas des valeurs inférieures à une minute. L'intervalle maximale est illimitée. L'expérience démontre qu'une intervalle d'enquête de cinq minutes (par défaut) est suffisant. Remarque : Des intervalles plus courtes résultent dans un trafic réseau plus intense, pouvant réduire la vitesse de réponse.

Gérer la sécurité avancée d'Intellex par le biais des Paramètres de sécurité

Les éléments d'Intellex sécurisables fonctionnant en mode Sécurité avancée

L'illustration ci-dessous montre le module Tous les instruments sécurisées de Policy Manager, qui contient tous les instruments actuellement enregistrés auprès du site Policy Manager, indépendamment de leurs attributions de zone respectives. L'arborescence à gauche montre tous les instruments. Sélectionner un instrument spécifique affiche l'environnement de sécurité pour cet instrument dans le volet de droite. L'annexe 2 contient une liste complète des fonctions sécurisables pour la version 3.2 d'Intellex. Le volet de droite est divisé en deux colonnes. La première colonne montre les propriétés des éléments pouvant être sécurisés pour une unité Intellex. La seconde colonne montre les utilisateurs/groupes attribués à chacun des éléments pouvant être sécurisés. La section inférieure du volet droit donne une explication plus détaillée de l'élément que vous sélectionnez.



Au démarrage, chaque Intellex (instrument) notifie Policy Manager qu'il est disponible pour être utilisé. Si le serveur ne reconnaît pas l'instrument, il rejette l'appel. Si c'est le cas, l'unité Intellex exécute un enregistrement initial auprès du serveur. Si l'enregistrement réussit, Policy Manager ajoute l'unité Intellex dans sa base de données interne. En outre, l'instrument est ajouté au conteneur Tous les instruments sécurisés et à la zone des instruments non-attribués. À la fin du processus d'enregistrement, les paramètres de sécurité pour l'instrument par défaut du site ont été appliqués au nouvel instrument. Si l'instrument est correctement enregistré auprès de Policy Manager, une notification est envoyée à toutes les consoles d'administration actuellement actives et un événement est ajouté au journal d'activité de PM.

Remarque

Si la liste des utilisateurs et des groupes n'est que partiellement visible, positionnez la souris sur la liste d'un élément ; une fenêtre d'aide apparaîtra, affichant le contenu complet de cette liste.

Action :	Description :
Sélectionnez un élément souligné dans la page des propriétés.	Lance l'éditeur de sécurité pour éditer l'objet sécurisable spécifique.
Cliquez sur l'icône +/-.	Étend/réduit la liste des propriétés.

Menu Instruments

Sélectionnez Action dans le menu principal ou cliquez du bouton droit sur un Intellex spécifique de l'arborescence pour afficher le menu Instruments, comme illustré ci-dessous.

Le menu Instruments permet les actions suivantes :	
Propager paramètres...	Applique les propriétés de sécurité d'un Intellex à un ou plusieurs autres unités Intellex. La sélection de cet élément affiche le dialogue Propager paramètres qui sert à attribuer des unités Intellex.
Définir description...	Change la description d'une zone existante. La sélection de cet élément affiche le dialogue Définir description qui sert à définir la description d'une zone.
Attribuer à la zone...	Ajoute un Intellex à un groupe d'Intellexes. Cette option n'est disponible que pour des instruments réels, pas pour les instruments par défaut. La sélection de cet élément affiche le dialogue Attribuer instrument.
Couper	Rend disponible l'action Coller. Cette action n'est disponible que pour des instruments réels. La sélection de cet élément grise l'icône de l'instrument et le rend disponible pour être collé dans une zone d'instruments.
Supprimer	Supprimer cet instrument. L'élément Supprimer n'est disponible que si un instrument est actuellement listé comme non-disponible. La suppression d'un instrument le retire de la liste des instruments enregistrés de Policy Manager.

Ajouter un instrument

Lorsque l'administrateur installe des unités Intellex sur le domaine et les configure pour la sécurité avancée, ils s'enregistrent automatiquement auprès du site Policy Manager selon les informations fournies par l'administrateur. Les unités Intellex ne peuvent être ajoutées manuellement.

Supprimer un instrument

Remarque

Vous ne pouvez supprimer que des instruments inactifs.

1. Ouvrez le client d'administration de Policy Manager et cliquez du bouton droit sur l'instrument que vous souhaitez supprimer.
2. Sélectionnez Supprimer et ensuite Oui. Ceci retire l'instrument du site ainsi que de la zone (si applicable) à laquelle il était attribué.

Associer un instrument à un site différent

Dans certains cas, vous pourriez avoir à associer un instrument à un autre site, par exemple :

- Vous avez établi un nouveau site pour contrôler des instruments attribués à un site différent.
- Vous avez déplacé un instrument d'un emplacement physique à un autre et devez l'associer à un site différent.

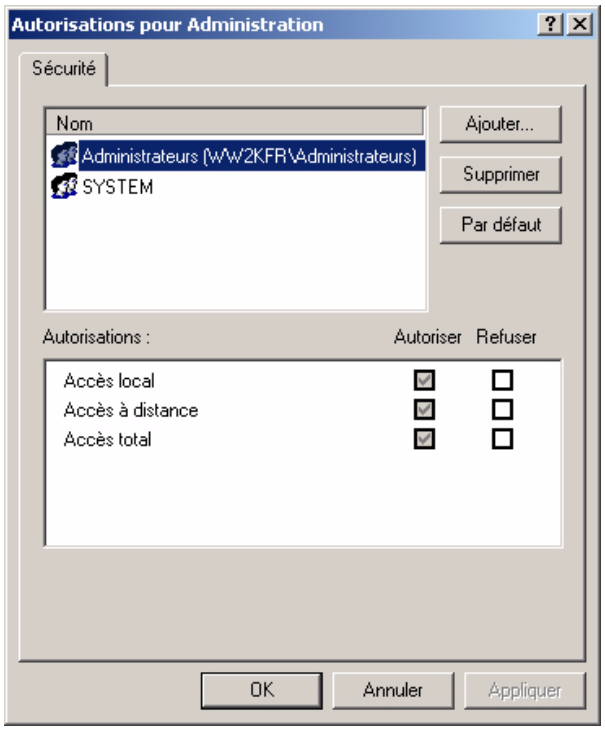
Remarque

Vous devez avoir des privilèges administratifs sur l'instrument que vous souhaitez associer.

1. Si l'application Intellex.exe est lancée sur l'instrument, quittez l'application pour retourner au bureau.
2. Ouvrez les services composants MMC, situés dans Panneau de configuration \Outils administratifs\ Services composants.
3. Sous Services de composant, naviguez à l'application PolicyManagerRemoteServices, cliquez du bouton droit et sélectionnez Propriétés. Le dialogue Propriétés de l'application apparaît.
4. Naviguez à la page Activation.
5. Sélectionnez le champ Nom du serveur distant : et saisissez le nom du serveur du nouveau site.
6. Cliquez sur OK.
7. Ouvrez le Policy Manager client administration (client d'administration de Policy Manager) de l'ancien site et supprimez l'instrument (voir Supprimer un instrument).
8. Redémarrez l'application Intellex.exe sur l'instrument. Cela démarrera l'enregistrement de l'instrument auprès du nouveau site. Souvenez-vous que, lors de l'enregistrement, l'instrument reçoit une copie des paramètres de sécurité pour l'instrument par défaut du site pour le nouveau site.
9. Ouvrez le client d'administration de Policy Manager du nouveau site et apportez les modifications nécessaires à l'instrument (l'attribuer à une zone, changer l'environnement de sécurité, etc.).

Éditer les paramètres de sécurité d'un Intellex

Pour éviter la sécurité d'un des éléments sécurisables dans la liste de droite, placez la souris sur l'élément (le curseur devient un pointeur) et cliquez. La fenêtre Éditeur de contrôle d'accès de Windows apparaît. Si vous avez sélectionné un objet « conteneur » (les objets de la liste avec une petite case devant le nom), comme « Données multimédia » ou « Administration », vous obtiendrez un éditeur générique, comme celui illustré ci-dessous.



Les permissions que vous pouvez attribuer ici sont :

Accès local	Vous attribuez à l'utilisateur ou au groupe la permission d'accès à l'instrument que sur l'instrument même. Cela signifie que tout accès distant via API ou Network Client est explicitement refusé (reportez-vous au chapitre Concepts de sécurité pour Policy Manager plus loin pour de plus amples informations à propos des types d'accès).
Accès à distance	Vous n'attribuez à l'utilisateur ou au groupe que la permission d'accéder à l'instrument par le biais des applications distantes (des applications quelconques utilisant API ou Network Client).
Accès total	Vous attribuez à l'utilisateur ou au groupe la permission d'accès à l'instrument à la fois sur l'instrument même et à distance. En outre, choisir Accès total attribue automatiquement toutes les permissions spécifiques à toutes les fonctions ou groupes de fonctions dans ce conteneur et tous les conteneurs ou objets directement sous-jacents de ce conteneur (reportez-vous au chapitre à propos des Utilisateurs, Groupes et Héritages plus loin).

Ajouter des utilisateurs ou groupes d'utilisateurs à un conteneur est une méthode rapide pour qu'un administrateur établisse une environnement de sécurité générique pour un instrument. Ceci car les utilisateurs et les groupes ajoutés au niveau du conteneur sont « hérités » par toutes les fonctions dans ce conteneur. Par exemple, si vous ajoutez un utilisateur nommé J Smith au conteneur « Données multimédia » et lui attribuez l'accès total, J Smith pourra tout voir, indépendamment de s'il se trouve directement devant l'instrument (accès local) ou s'il accède à distance aux données par le biais de Network Client ou l'API.

Lorsqu’un utilisateur ou un groupe d’utilisateurs est ajouté à un conteneur et ensuite passé en héritage aux objets enfants de ce conteneur (par exemple Données multimédia à Vidéo en direct), les permissions sur l’objet enfant sont attribuées comme suit :

- Si vous n’avez pas sélectionné l’option Accès total, des permissions par défaut spécifiques sont attribuées. Cela est différent d’objet en objet. Le tableau dans la section Liste de fonctions sécurisables donne un aperçu des paramètres par défaut actuels pour les différents objets de sécurité.
- Si vous avez sélectionné l’option Accès total, toutes les permissions spécifiques pour chaque objet enfant sont attribuées.
- Si vous avez sélectionné une fonction spécifique, telle que Vidéo en direct, un éditeur contenant les éléments spécifiques pour cette fonction apparaîtra. Tous les utilisateurs et groupes d’utilisateurs ajoutés à la fonction ne sont valides que pour cette fonction.

L’avantage principal de l’application de paramètres à des conteneurs plutôt que des fonctions spécifiques, est que avec une seule entrée, vous pouvez définir des permissions d’accès pour une liste entière d’éléments ou pour tout l’Intellex.

Ajouter ou Retirer des utilisateurs ou groupes d’utilisateurs

Dès que l’éditeur de contrôle d’accès est affiché, vous pouvez attribuer ou refuser l’accès à des utilisateurs ou groupes d’utilisateurs. Ces utilisateurs et groupes d’utilisateurs sont les mêmes que ceux définis pour votre réseau corporatif.

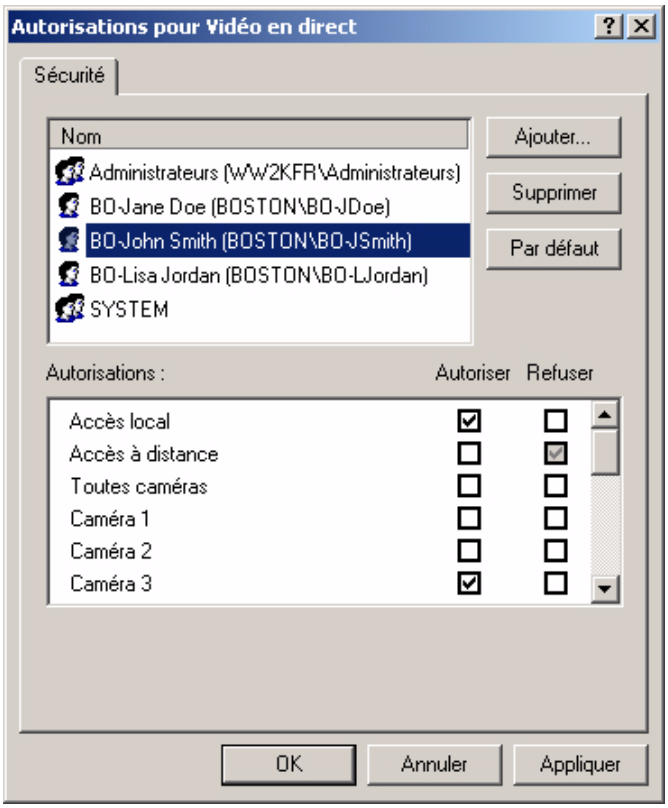
1 Pour ajouter un utilisateur ou un groupe, cliquez sur le bouton Ajouter... et le dialogue Sélectionner utilisateurs ou groupes apparaît.

La liste déroulante à la droite de Regarder dans : vous permet de naviguer à tout domaine reconnu par votre entreprise corporative. Ensuite, vous pouvez sélectionner un utilisateur ou un groupe d’utilisateurs à ajouter.

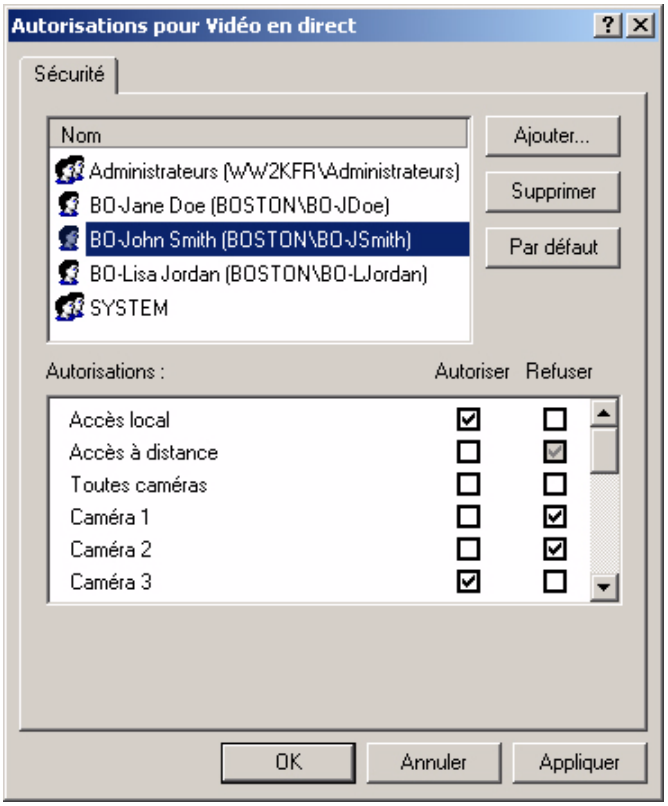
2 Sélectionnez le groupe, cliquez sur Ajouter et ensuite sur OK.

Dans l’exemple ci-dessous, si vous souhaitez refuser l’accès aux caméras 1 et 2, vous pouvez ce faire de deux manières :

3 Décochez les cases à la droite des caméras 1 et 2 dans la colonne Permettre, comme illustré ci-dessous, pour indiquer que vous n'attribuez pas au groupe l'accès EXPLICITE à ces caméras.



4 Alternativement, vous pouvez cocher les cases à la droite des caméras 1 et 2 dans la colonne Deny (Refuser), comme illustré ci-dessous, pour refuser explicitement l'accès à ces caméras.



Remarque

Décocher simplement les cases dans la colonne Permettre pourrait ne pas empêcher un individu ou un groupe de visualiser de la vidéo en direct sur ces caméras. C'est parce que un individu (ou un groupe) pourrait avoir hérité la permission de visualiser de la vidéo sur ces caméras par le biais d'un autre groupe. Pour être totalement certain qu'un individu ou un groupe se verra refuser l'accès (la permission) à une fonction, vous devez cocher la case dans la colonne Refuser.

Si vous allez retirer un utilisateur ou un groupe d'utilisateurs que vous avez ajouté préalablement, veuillez remarquer que :

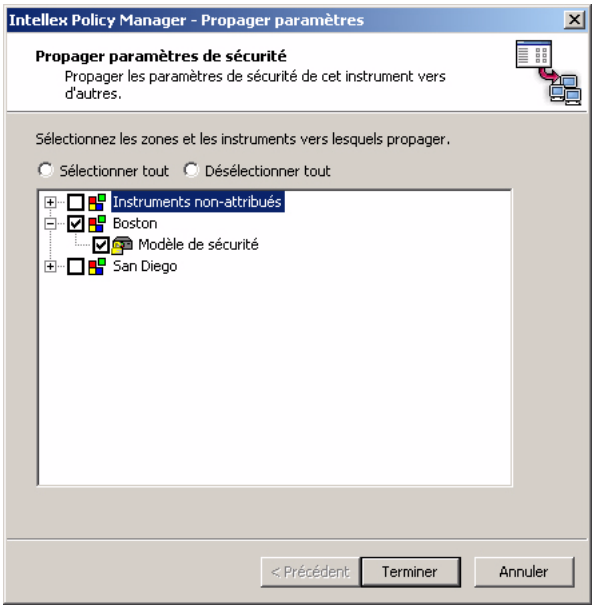
- Si l'utilisateur ou le groupe d'utilisateurs que vous avez ajouté est listé en tant qu'hérité, ce qui signifie que l'utilisateur ou le groupe d'utilisateur avait été ajouté à un niveau plus élevé que celui de l'objet actuel, vous ne pourrez pas ce faire.
- Si l'utilisateur ou le groupe d'utilisateurs n'est pas listé en tant qu'hérité, vous pourrez le retirer.

Remarque

Si vous retirez un utilisateur ou un groupe d'utilisateurs ayant été hérité, il est non seulement retiré de l'objet actuel, mais également de tous les objets enfants directement sous-jacents. Par exemple, si vous avez ajouté un utilisateur appelé J Smith à Données multimédia et l'avez retiré ensuite, il est également retiré de Vidéo en direct, Vidéo enregistrée, etc. jusqu'au dernier élément enfant, Audio enregistrée.

Propager (copier) les paramètres de sécurité d'un Intellex à un autre

L'illustration montre le dialogue Propager paramètres de sécurité, qui vous permet de copier les paramètres d'un instrument vers un ou plusieurs autres instruments.



Une arborescence de répertoires contient une liste de zones et d'instruments membres. La case à cocher à la gauche d'un nom indique si un élément reçoit ou non les nouveaux paramètres. La case à cocher en face du nom de la zone même indique l'état actuel de la zone. Déterminez (ou calculez) l'état de la zone en appliquant les règles suivantes :

1. Si aucun instrument n'est coché, l'état de la zone est néant et aucune coche n'apparaît dans la case. ☐
2. Si au moins un, mais pas tous les membres de la zone sont cochés, l'état de la zone est partial et un coche apparaît dans la case grisée. ☑
3. Si tous les membres de la zone sont cochés, l'état de la zone est complet et un coche apparaît dans la case blanche. ☑

Action :	Description :
Cliquez sur une icône +/-.	Étend/réduit la zone d'instruments.
Cliquez dans une case de sélection de zone.	Si cochée ou partiellement cochée (grisée), tous les membres de la zone sont désélectionnés ainsi que la zone même. Si décochée, tous les membres de la zone sont sélectionnés ainsi que la zone même.
Cliquez dans une case de sélection d'instrument.	Si elle était cochée, l'instrument est désélectionné et l'état de la zone est recalculé (voir plus haut). Si elle n'était pas cochée, l'instrument est sélectionné et l'état de la zone est recalculé (voir plus haut).
Cliquez sur le bouton Terminar.	Accepte les changements.
Cliquez sur le bouton Annuler.	Abandonne les changements.
Cliquez sur le bouton Aide.	Appelle l'aide contextuelle à propos du changement de description.

Travailler avec des zones

Le deuxième élément sous Policy Manager est Zones de sécurité. Les zones de sécurité permettent à l'administrateur d'organiser des instruments dans des unités de sécurité gérées séparément. Chaque zone contient un instrument par défaut qui représente les paramètres de sécurité appliqués à toutes les zones membre.

En créant des zones et en les attribuant des instruments, l'administrateur implémente une topologie corporative ou de site que Policy Manager maintiendra automatiquement.

Le volet de droite affiche une de plusieurs visualisations, selon le mode de visualisation de MMC. Les visualisations Grandes icônes, Petites icônes, Liste ou Détails sont affichées. La visualisation Détails indique le nom de groupe et une description.

Action :	Description :
Cliquez sur l'icône + / - de l'arborescence.	Étend/réduit la visualisation de l'arborescence.
Double-cliquez sur une icône de zone dans le volet de droite.	L'arborescence est étendue pour afficher la zone sélectionnée. Le volet de droite affiche tous les instruments attribués à la zone.
Cliquez sur une zone dans l'arborescence des objets.	Le volet de droite affiche tous les instruments attribués à la zone.

Menu Zones de sécurité

Sélectionnez Action dans le menu principal ou cliquez du bouton droit sur un objet de zone de sécurité dans le menu Zones de sécurité.

Le menu contient une combinaison d'éléments de menu MMC et d'éléments spécifiques au conteneur des Zones de sécurité.

La zone des instruments non attribués

La zone des instruments non-attribués est une zone par défaut, livrée avec le logiciel. Elle ne peut être supprimée. L'instrument dans cette zone est considéré comme l'instrument par défaut du site. Cet instrument peut être visualisé en tant que modèle de sécurité pour tous les instruments du site. Tous les instruments fraîchement enregistrés sont d'abord attribués à cette zone et héritent ces paramètres de sécurité par défaut.

Création d'une nouvelle zone (regrouper des instruments avec des propriétés de sécurité communes)

1. Dans le client d'administration, naviguez au nœud Zones de sécurité dans le volet gauche, cliquez du bouton droit et sélectionnez Nouvelle zone. L'assistant Nouvelle zone apparaît.
2. Saisissez les informations requises et cliquez sur Terminer. La nouvelle zone apparaît dans la liste des zones de sécurité disponibles.

   Vous pouvez maintenant attribuer des instruments et changer les paramètres par défaut pour l'instrument par défaut de cette zone. L'ajout d'une nouvelle zone déclenche l'envoi par le serveur d'une signalisation d'événement à tous les clients actuellement actifs.

Remarque

Les nouvelles zones reçoivent automatiquement un instrument de zone par défaut qui est une copie de l'instrument par défaut actuel du site. En changeant les paramètres pour l'instrument par défaut de la zone et en propageant ensuite ces paramètres aux membres de la zone, l'administrateur peut configurer et maintenir un environnement de sécurité uniforme autour de plusieurs instruments individuels en même temps.

Supprimer une zone

En supprimant une zone, tous les instruments attribués à cette zone sont retournés à la zone des instruments non-attribués. Peuvent être ré-attribué à une zone différente à tout moment. Aucun instruments n'est supprimé, à l'exception de l'instrument par défaut de la zone qui n'est plus nécessaire.

1. Dans le client d'administration, naviguez à la zone de sécurité que vous souhaitez supprimer dans le volet gauche, cliquez du bouton droit et ensuite sur Supprimer.

   Si la zone contient des instruments, le programme vous demande si vous souhaitez appliquer les paramètres de sécurité pour l'instrument par défaut de la zone pour chaque instrument lorsqu'il est déplacé à la zone des instruments non-attribués.
2. Cliquez sur Oui pour hériter les paramètres ou sur Non maintenir les paramètres. Ceci termine le processus. Cliquez sur annuler si vous souhaitez annuler la suppression.

La vue Zone unique

La vue Zone unique montre les instruments qui sont membres de cette zone. Chaque zone contient également un instrument par défaut comme mentionné ci-dessus. Vous pouvez propager les paramètres de sécurité pour l'instrument par défaut vers des ou tous les instruments dans la zone.

Le vue d'une zone est similaire à la vue du nœud « Tous les instruments sécurisés ». Le volet de droite affiche une de plusieurs visualisations, selon le mode de visualisation de MMC. Les visualisations Grandes icônes, Petites icônes, Liste ou Détails sont disponibles. La visualisation Détails indique le nom de l'instrument, une description et la version logicielle de l'instrument.

Action :	Description :
Cliquez sur l'icône + / - de l'arborescence.	Étend/réduit la visualisation de l'arborescence.
Double-cliquez sur une icône de zone dans le volet de droite.	Le volet de droite affiche les instruments attribués à cette zone.
Sélectionnez un instrument dans cette zone.	Le volet de droite affiche les paramètres de sécurité pour cet instrument.

Le menu Zone unique

1 Sélectionnez Action dans le menu principal ou cliquez du bouton droit sur une zone spécifique de l'arborescence des objets pour afficher le menu Zones.

Le menu contient une combinaison d'éléments de menu MMC et d'éléments spécifiques du groupe d'instruments. Les éléments spécifiques à l'instrument sont :

- Définir description...
- Coller
- Supprimer
- Renommer

Remarque

L'option Coller n'est disponible que lorsqu'un instrument ou une zone avait été préalablement coupé.

Action :	Description :
Définir description...	Affiche le dialogue Définir description.
Sélectionne Coller	Cet élément n'est disponible que lorsqu'un instrument avait été préalablement coupé. Coller un instrument déplace l'instrument de la zone source à la zone de collage (de destination). L'opération de Coller n'est admise que lorsque l'instrument provient d'une zone différente. L'utilisateur est invité à indiquer si les paramètres de sécurité par défaut de la zone cible doivent être propagés au nouveau membre de zone. En outre, l'utilisateur peut choisir d'annuler complètement l'opération.
Sélectionnez Supprimer	Supprime la zone d'instruments. Tous les instruments sont retirés de la zone et placés dans le conteneur des « Instruments non-attribués ». L'utilisateur est invité à indiquer si les paramètres de sécurité par défaut de site (représentés par l'instrument par défaut du site) doivent être propagés à tous les instruments déplacés. Une réponse négative (NON) permet aux instruments individuels de retenir leurs paramètres de sécurité spécifiques. En outre, l'utilisateur peut choisir d'annuler complètement l'opération.
Sélectionnez Renommer	Écrase le nom de la zone.
Liste d'exportation...	Vous permet d'enregistrer les informations dans un fichier.

Le dialogue Définir description vous permet de changer la description d'une zone existante. La longueur de la description est illimitée ; cependant, elle ne peut contenir que des caractères alphanumériques. Une boîte d'édition vous permet de modifier la description.

Déplacer une unité Intellex vers une zone de sécurité

Le dialogue Assign Instrument (Attribuer instrument) vous permet d'attribuer un instrument à zone.

Une liste de sélection contient les zones dans lesquelles vous pouvez déplacer l'instrument. La liste ne montre pas la zone à laquelle est attribué actuellement l'instrument.

Action :	Description :
Sélectionnez une zone dans la liste de sélection.	Sélectionne la zone en tant que destination pour l'instrument. Une seule zone peut être sélectionnée.
Sélectionnez la case « Hériter paramètres par défaut de la zone de destination ».	La sélection de la case est une indication que le nouveau membre (l'instrument déplacé dans la zone) doit hériter les paramètres de sécurité par défaut comme représentés par l'instrument par défaut de la zone. En ne cochant pas la case, l'instrument sera déplacé à la zone, mais les paramètres de sécurité par défaut de la zone ne seront pas appliqués à l'instrument pendant le déplacement.
Cliquez sur Terminar.	Accepte les changements.
Cliquez sur Annuler.	Abandonne les changements.
Cliquez sur Aide.	Appelle l'aide contextuelle à propos du changement de description.

Vous pouvez également glisser/coller pour déplacer un instrument d'une zone à une autre. Si vous choisissez cette méthode, un dialogue apparaît, vous demandant si voulez que les paramètres de sécurité par défaut de la zone soient appliqués au nouvel instrument.

Action :	Description :
Cliquez sur Oui.	Fait le déplacement et applique les paramètres par défaut au nouveau membre.
Cliquez sur Non.	Fait le déplacement, mais n'applique pas les paramètres par défaut au nouveau membre.
Cliquez sur Annuler.	Annule le déplacement. L'instrument reste attribué à la zone dont l'instrument est actuellement membre.

Remplacer un Intellex

Une variété de scénarios peut vous mener à remplacer un instrument déjà enregistré sur votre site. Par exemple :

- Vous avez déplacé l'instrument vers un autre emplacement et avez acquis un remplacement plus récent pour l'emplacement original.
- Vous avez remplacé l'instrument à cause d'un dysfonctionnement matériel.

Pour installer le nouvel instrument, vous devez donner l'identité de l'instrument que vous allez remplacer. Supposons que vous avez ajouté le nouvel instrument au domaine en utilisant le nom de l'ancien instrument.

1. Installez les pilotes de Policy Manager sur le nouvel instrument selon la procédure standard.
2. Démarrez l'instrument et laissez-le s'enregistrer auprès de Policy Manager.
3. Les noms des instruments sont les mêmes, mais les clés d'identification primaires et secondaires (l'adresse MAC et l'ID unique générée par l'instrument) sont différentes. Policy Manager le considère comme un nouvel instrument, enregistre ses informations et notifie tous les clients administratifs actuellement actifs qu'un nouvel instrument vient d'être enregistré.

4 Ouvrez le client d'administration et naviguez à la collection Tous les instruments sécurisés.

5 Deux entrées avec le même nom apparaissent. Un est actif (le nouvel instrument que vous venez d'installer) et l'autre inactif (l'instrument remplacé).

6 Propagez les paramètres de sécurité de l'ancien instrument (inactif) vers le nouvel instrument.

7 Si l'ancien instrument était attribué à une zone, déplacez le nouvel instrument à la même zone.

Remarque

Assurez-vous de ne pas propager les paramètres de sécurité par défaut de la zone au nouvel instrument ; vous avez déjà copié les paramètres de l'ancien instrument.

8 Supprimez l'ancien instrument.

Action :	Description :
Changez le texte dans le contrôle d'édition.	Met à jour la description.
Cliquez sur OK.	Accepte les changements.
Cliquez sur Annuler.	Abandonne les changements.
Cliquez sur Aide.	Appelle l'aide contextuelle à propos du changement de description.
Changez le texte dans le contrôle d'édition.	Met à jour la description.

Vous pouvez saisir le nom de groupe et la description dans les deux boîtes d'édition.

Action :	Description :
Changez le texte dans le contrôle d'édition du nom de groupe.	Met à jour le nom de groupe.
Changez le texte dans le contrôle d'édition de description.	Met à jour la description.
Cliquez sur le bouton OK.	Accepte les changements.
Cliquez sur le bouton Annuler.	Abandonne les changements.
Cliquez sur le bouton Aide.	Appelle l'aide contextuelle à propos du changement de description.

Travailler avec le Gestionnaire de licences

Le troisième module sous Policy Manager pour Intellex est le Gestionnaire de licence. Sous le nœud Gestionnaire de licences, un ou deux sous-nœuds apparaissent. Si vous n'avez installé que Policy Manager, le sous-nœud Policy Manager est disponible. Si vous avez également installé Archive Manager, le sous-nœud Archive Manager est également disponible.

Une clé USB matérielle avec numéro de série est incluse et requise pour lancer Policy Manager. Une ID de produit (PID) est lié au numéro de série de la clé matérielle. Dès que vous recevez le produit, installez le logiciel et installez ensuite la clé matérielle sur le port USB de l'ordinateur serveur. Après avoir terminé l'installation, l'utilisateur final ou l'installateur doit démarrer l'application du client d'administration, entrer le module Gestionnaire de licence et mettre à jour la PID pour que Policy Manager commence à sécuriser le nombre d'unités Intellex sur le réseau correspondant à la licence acquise.

Cette PID saisie dans le module d'administration Gestionnaire de licence contrôle le nombre d'unités Intellex autorisé pouvant fonctionner simultanément sous sécurité avancée. Dès que l'administrateur saisit la PID, Policy Manager utilise la quantité imbriquée dans la PID pour identifier le nombre d'unités Intellex autorisé pouvant fonctionner sous sécurité avancée.

En outre, la PID contient des informations à propos de la licence corporative de Network Client (NC) si vous avez acquis cette fonctonnalité. Elle vous permet de distribuer une unique copie de Network Client à un nombre illimité d'utilisateurs (sièges) de votre organisation.

Remarque

Policy Manager peut démarrer sans la clé matérielle. Installez le logiciel Policy Manager sans la clé matérielle. Insérez la clé matérielle soit avant, soit après le démarrage du serveur de Policy Manager.

- PMAdmin peut démarrer sans la clé matérielle et les permissions d'accès de tous les utilisateurs peuvent être définies.
- Pour que puisse se connecter à Policy Manager, une clé matérielle spécifique à PM est requise. La clé accompagnant le CD permet la connexion d'un Intellex, mais aucune licence de Network Client n'est incluse.
- Pour permettre que plusieurs Intellexes se connectent simultanément, l'utilisateur doit obtenir une PID auprès de American Dynamics.
- L'accès concurrent d'Intellex est basé sur le principe premier arrivé, premier servi.
- Pour autoriser les licence NC, l'utilisateur doit obtenir une PID auprès de American Dynamics.
- Le client peut demander une PID combinant le nombre de licences de site NC et Intellex concurrents.
- Des licences pour l'utilisation concurrente d'Intellexes peuvent être acquises en paquets de 10, 25 et illimité (avec ou sans licence de site de Network Client). Le nombre représente le total et n'inclut pas le supplémentaire au-dessus du libre. Si vous avez déjà une PID, vous devriez l'envoyer à American Dynamics pour acquérir une mise à niveau.

Licence corporative Network Client

Le PID accompagnant le logiciel Policy Manager détermine la présence ou l'absence d'une licence corporative NC.

Le PID est inscrite sur le boîtier et contient :

- Type de produit (Policy Manager)
- Version
- S/N (numéro de série unique) - Le S/N est directement lié au numéro de série imbriqué dans la clé matérielle et pas au serveur hôte du logiciel Policy Manager
- Fonctions (huit bits marche/arrêt individuellement sélectionnés)
- Somme de vérification d'intégrité

Une licence corporative permet aux clients corporatifs de :

- Acheter une copie de NC
- L'installer sur le nombre de nœuds requis
- Utiliser la même ID de produit (NCCPID) pour chaque installation
- Désactiver automatiquement la vérification de PID double sur Intellex

Pour mettre à jour :

1. Sélectionnez Gestionnaire de licence.
2. Cliquez sur Mise à niveau.
3. Saisissez le PID, ce qui mettra à niveau la clé matérielle pour attribuer la licence corporative NC.

Travailler avec la Visualisation d’événements

Policy Manager crée un journal d’événements personnalisé que l’administrateur peut consulter à tout moment en utilisant l’outil de visualisation d’événements du système d’exploitation. Les journaux d’événements ont l’aspect suivant :

Application	Journaux d’erreurs d’application
Policy Manager	Journaux d’erreurs de journal personnalisé
Sécurité	Journaux d’audit de sécurité
Système	Journaux d’erreurs système

Policy Manager ajoute des entrées à son propre journal d’événement personnalisé sous les quatre catégories suivantes :

Information

Élaboration de routine sur l’action prise. Fournit également des informations générales et utiles aux administrateurs (par exemple, une nouvelle session d’administration démarre sur le serveur).

Avertissement

Signale que l’action prise ou que les données saisies peuvent provoquer une erreur. Indique également que l’attention de l’administrateur est requise pour s’occuper d’une situation erronée. Un événement d’avertissement est généré lorsque la licence du site est échue ou si la clé matérielle rapporte que toutes les licences sont utilisées.

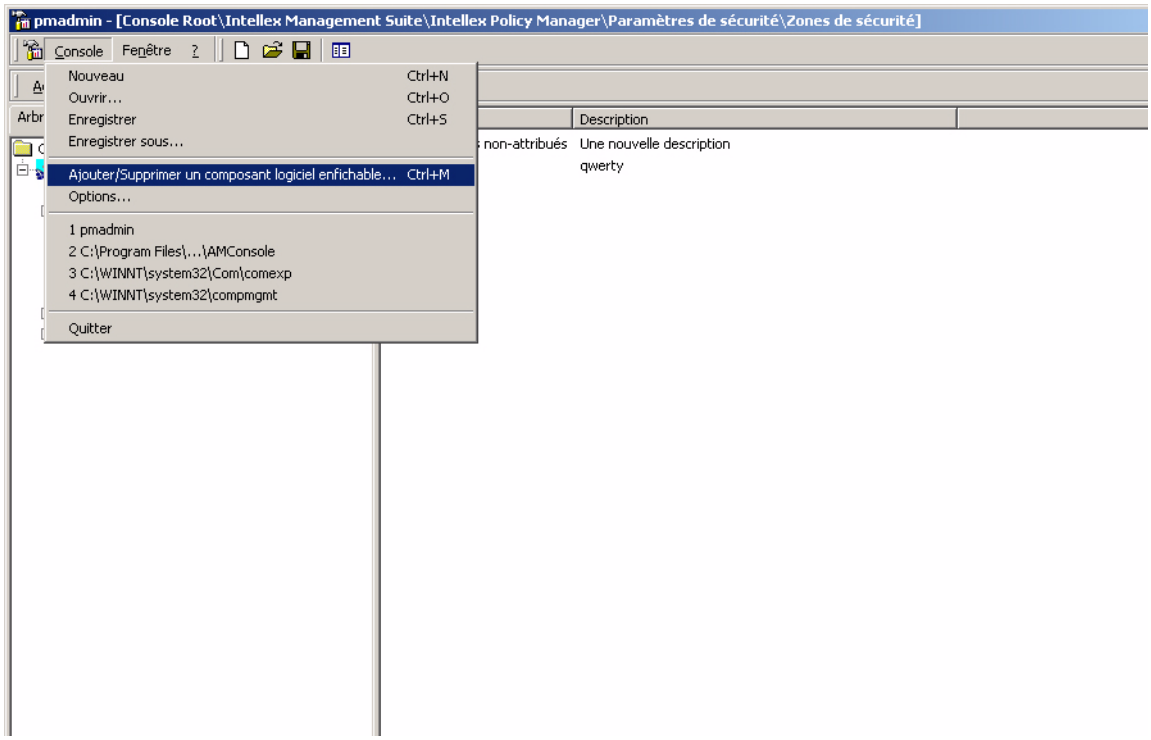
Erreur

Signale que l’action prise ou que les données saisies ont provoqués une erreur critique (fatale). Indique également la détection d’un état anormal (par exemple, un instrument enregistré est devenu indisponible) pendant le fonctionnement du serveur.

Audit d’erreurs

Avertissement qu’un utilisateur inconnu a essayé d’accéder au système. Cet événement est également généré si un utilisateur reconnu essaye d’accéder à une fonction à laquelle il n’a pas le droit.

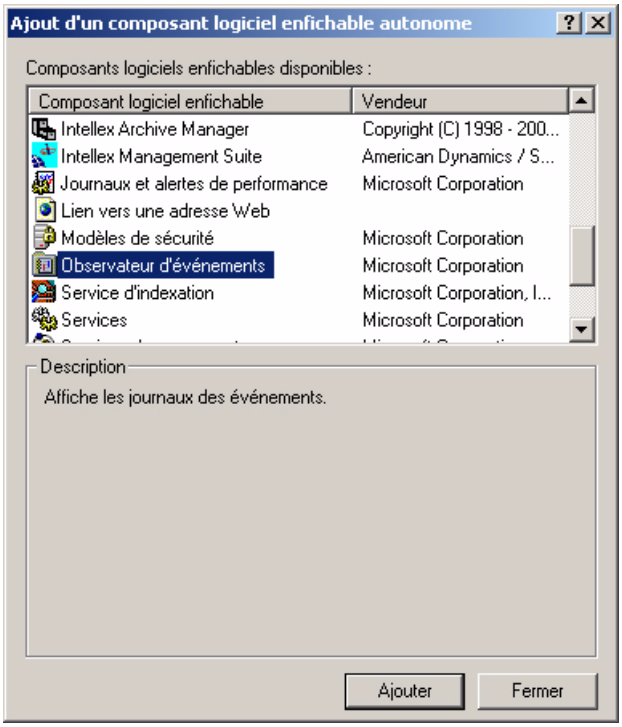
Ajouter le Snap-in Visualisation d'événements



Pour ajouter le Snap-in Visualisation d'événements à l'application console MMC configurée lors de l'installation :

1. Sélectionnez Console - Ajouter/Supprimer un composant logiciel enfichable...
2. Sélectionnez Ajouter...

Le dialogue Ajouter d'un composant logiciel enfichable autonome apparaît, comme illustré ci-dessous.



1 Sélectionnez Observateur d’événements et cliquez sur Ajouter.

2 Alternativement, vous pouvez double-cliquer sur l’élément de la liste Visualisation d’événements.

Le dialogue Sélectionner un ordinateur apparaît.

Remarque

Assurez-vous de sélection de : ordinateur où le serveur de Policy Manager est lancé.
Si nécessaire, recherchez l’ordinateur correct par le biais du bouton Parcourir.

1 Dans le dialogue Sélectionner ordinateur, cliquez sur Terminer.

2 Dans le dialogue Ajouter d’un composant logiciel enfichable autonome, cliquez sur Fermer.

3 Cliquez sur OK.

Annexe A : Concepts de sécurité pour Policy Manager

Policy Manager intègre votre installation de sécurité physique dans votre environnement de sécurité de réseau existant. La sécurité physique et de réseau sont des branches de spécialisation complexes employant des équipes de professionnels dévoués avec des connaissances spécifiques concernant leur spécialité. En utilisant Policy Manager, les deux groupes collaborent pour fournir un réseau de sécurité intégrée à leurs environnements de travail respectifs. Une grande diversité en littérature et documentations techniques, couvrant des sujets de base à avancés, prennent en charge les deux branches. Reportez-vous à cette littérature supplémentaire pour améliorer vos connaissances.

Puisque ce produit est utilisé en combinaison avec la ligne Intellex d'enregistreurs vidéo numériques, votre source principale d'informations à propos de sécurité physique est le manuel de l'utilisateur et les documents accompagnant votre système. Là, vous trouverez des informations à propos de chacune des fonctions sécurisables listées dans le tableau des fonctions de l'annexe 2.

Policy Manager est totalement intégré avec le système d'exploitation Windows 2000. Par conséquent, vous pouvez personnaliser la sécurité du système pour les adapter à vos exigences de mise en réseau corporatif. La configuration par défaut de Policy Manager fournit une sécurité appropriée pour la majorité des applications. Mais si vous avez des exigences spéciales, les paramètres par défaut pourraient être inadéquats. Si c'est la cas, vous avez besoin d'une installation personnalisée. Les installations personnalisées ne font pas l'objet de ce manuel. Si vous allez faire une installation personnalisée, nous recommandons vivement de demander conseil auprès de votre service IS et qu'un membre de l'équipe IS vous assiste lors du processus physique d'installation. En outre, vous ou le professionnel IS doivent posséder un connaissance de travail avec la sécurité Windows, les applications distribuées par COM+, leurs paramètres, comment ils sont déployés et les paramètres de sécurité DCOM.

Questions de base

Pour créer un environnement sécurisé, répondez à ces trois questions au-delà de tout doute raisonnable :

1. Qui êtes vous et êtes-vous qui vous prétendez être ?
2. À quoi voulez-vous accéder ?
3. Que voulez-vous en faire une fois que vous l'avez obtenu ?

Dans le monde de la sécurité des réseau, la réponse à la première question est appelé « authentification ». Les réponses aux réponses deux et trois sont appelées « autorisation ».

Authentification

Qui êtes vous et êtes-vous qui vous prétendez être ?

Répondre de façon fiable à cette question est le domaine exclusif de l'authentification. Cette question nous confronte à chaque fois que nous nous connectons à nos réseaux respectifs. Afin d'accéder aux éléments partagés du réseau, aux ressources globales et même à nos courriels, nous devons nous authentifier.

La sécurité de réseau est similaire à la sécurité d'accès physique à de nombreux sites de travail. Tout comme les badges d'entrée qui identifient les employés auprès du système de contrôle, les légitimations réseau (nom d'utilisateur, mot de passe et autorité d'authentification) identifient positivement les individus dans le réseau corporatif. Le stockage et l'accès à ces légitimations est centralisé, de façon que nous puissions les utiliser à partir de tout ordinateur ayant accès à l'autorité d'authentification (généralement, un contrôleur de domaine).

L'autorité d'authentification est un concept clé. L'autorité, généralement un contrôleur de domaine spécifique au sein de l'entreprise, prend en charge les requêtes d'authentification du réseau. Par conséquence, l'ordinateur demandeur doit être à la fois physiquement connecté à ce domaine et reconnu par celui-ci.

Si les légitimations sont valides, c.-à-d., elles présentent les informations requises pour que l'autorité d'authentification reconnaisse une personne unique (J. Smith, par exemple), l'identité réseau de cette personne a été établie et il ou elle a été authentifié.

Policy Manager utilise l'authentification à deux endroits :

Pour toutes les communications entre clients (tant le client d'administration que les instruments Intellex) et le serveur, COM+ et le sous-système DCOM sous-jacent authentifient la session interactive actuelle sur la machine client et appliquent ensuite le résultat pour autoriser l'utilisateur en base de ses attributions de rôle.

Pour toutes les communications entre un poste de travail Network Client et un instrument Intellex individuel, une authentification explicite est utilisée à l'instrument, en base des légitimations encodées que lui envoye l'application client. Ce processus d'authentification invite à la création d'une session Windows sur l'instrument. L'autorisation est donnée en utilisant des vérifications d'accès explicites pour chaque fonction requise par le client.

La session Windows

Lorsque les légitimations d'un utilisateur ont été correctement traitées, une session Windows est créée pour l'utilisateur sur l'ordinateur hôte. Les règles sont représentées par un ensemble de politiques et de permissions que Policy Manager maintient pour la totalité du site, ainsi que pour chaque instrument individuel. L'application des règles pour chaque utilisateur est appelée l'autorisation.

Politiques et permissions de site

Policy Manager applique des règles à la fois générales et spécifiques. Les règles générales sont des politiques de site qui seront appliquées à tous les utilisateurs qui accèdent au système, indépendamment de quel instrument elles visent. Les permissions sont spécifiques à l'instrument et forment le noyau de la sécurité avancée d'Intellex. Chaque instrument surveille et applique le même ensemble de permissions, telles que Vidéo en direct. Par exemple, à la fois Intellex1 et Intellex2 surveilleront l'accès à la vidéo en direct sur caméra 13, même si la caméra 13 pourrait ne pas exister. Ensemble, ces permissions forment l'environnement de sécurité qui contrôle et protège l'unité.

Bien que tous les instruments prennent en charge et appliquent le même ensemble de permissions, celles-ci sont données ou refusées par instrument et par utilisateur. Par exemple, si J Smith est un utilisateur authentifié, il peut être autorisé à regarder de la vidéo en direct sur Intellex1, mais pas sur Intellex2.

Consultez votre manuel de l'utilisateur d'Intellex pour une explication plus approfondie de chaque permission ou fonction.

Autorisation

En général, les utilisateurs souhaitent accéder à des unités et fonctions Intellex spécifiques. En tant qu'administrateur, vous (ou une autre personne) pourriez souhaiter accéder aux données stockées sur le serveur qui décrit votre site. En outre d'y accéder, vous souhaitez modifier les données. Par conséquence, tant l'accès aux instruments individuels que l'accès au serveur doit être contrôlé.

Vous contrôlez l'accès au serveur en utilisant les rôles prédéfinis pour l'application serveur expliquée plus haut. Si l'accès à un serveur spécifique est restreint (comme pour créer de nouvelles zones), l'utilisateur émettant la requête doit être un membre du rôle ayant accès à cette fonction. Dans notre exemple, l'utilisateur doit être enregistré en tant que membre du rôle « Administrateur de site ».

L'accès aux instruments est contrôlé par le biais de « l'environnement de sécurité » qui s'applique à cet instrument (reportez-vous au chapitre « Instruments et leurs environnements de sécurité »). Cela signifie que le client a été authentifié et une session Windows valide a été créée sur l'instrument cible.

À quoi voulez-vous accéder ?

Pour retourner à notre exemple, J Smith, qui possède un badge d'accès, nous savons que les informations (légitimations) stockées sur le badge sont suffisantes pour que le système de contrôle d'accès reconnaisse (authentifie) J Smith. J Smith souhaite utiliser ses légitimations pour avoir accès à la porte arrière.

Puisque J Smith a utilisé le lecteur de badges de la porte arrière, le système la considère (la porte arrière) comme étant l'objet cible actuel (J Smith souhaite entrer et vérifier ses courriels). Désormais, le système dispose de deux pièces d'information : il sait qui est J Smith et il sait que J Smith souhaite avoir accès (par la porte arrière).

Que voulez-vous en faire une fois que vous l'avez obtenu ?

Dans cet exemple, il est clair ce que veut faire J Smith avec la porte arrière, puisqu'il ne peut que l'ouvrir. Le système a donc répondu avec succès aux trois questions :

- Qui êtes vous et êtes-vous qui vous prétendez être ? (J Smith, OUI)
- À quoi voulez-vous accéder ? (La porte arrière)
- Que voulez-vous en faire une fois que vous l'avez obtenu ? (Ouvrez le)

Mais le système a besoin de plus d'informations pour déterminer si J Smith peut entrer à l'immeuble. Il doit consulter une base de données pour consulter une liste d'utilisateurs valides qui ont l'autorisation d'accéder à la porte arrière (peut-être J Smith ne peut entrer à l'immeuble que par l'entrée des employés). Dans la sécurité de réseau, cette base de données peut être la base de données SAM locale ou un serveur de Répertoire actif.

En supposant qu'il y a une base de données et qu'il y a une entrée de porte arrière, le système de contrôle d'accès peut traduire nos trois questions générales en une seul requête spécifique :

J Smith peut-il ouvrir la porte arrière ?

Désormais, le requête peut être complètement traitée et J Smith peut soit se mettre au travail soit rester dehors.

Descripteurs de sécurité

Dans la sécurité de Windows, la base de données mentionnée est appelée « descripteur de sécurité ». Un descripteur de sécurité de Windows représente l'environnement de sécurité pour un unique objet ou groupe d'objets pouvant être sécurisés (par exemple, un fichier ou tous les fichiers). Il contient des permissions spécifiques et pertinentes à cet objet (lecture et écriture pour un fichier) ainsi que certaines permissions générales pertinentes à tous les objets. Il contient également une liste d'utilisateurs ou de groupes qui reçoivent ou non l'accès, ainsi que quelles permissions s'appliquent à l'accès (par exemple, J Smith a la permission de lecture mais pas d'écriture).

Si J Smith utilisait son ordinateur pour accéder à un fichier spécifique sur un serveur, la sécurité Windows rassemble les informations nécessaires pour répondre à nos questions générales et exécute ensuite la même traduction. Dans ce cas, la question devient :

J Smith peut-il accéder au fichier Forcasts.xls sur MyFileServer ?

D'abord, le système authentifie J Smith. Si cela réussi, il récupère le descripteur de sécurité du fichier auquel J Smith souhaite accéder (Forcasts.xls) et vérifie si :

- Il possède l'accès spécifique, dans quel cas son descripteur unique apparaîtra dans le descripteur de sécurité

  Ou

- Il a hérité l'accès en base de son appartenance à un groupe.

S'il a la permission, il obtiendra le fichier.

Policy Manager et la écurité avancée d'Intellex utilisent les mêmes mécanismes. En outre de certaines informations spécifiques à l'instrument, telles que le nom de l'unité, l'adresse MAC, etc., l'environnement de sécurité de l'instrument contient une liste de descripteurs de sécurité qu'il rend disponible au système d'exploitation. Ensuite, le système d'exploitation utilise ces informations, en combinaison avec les informations dont il dispose à propos de la session d'utilisateur dont émane la requête, pour déterminer si un utilisateur ou un groupe d'utilisateurs ont la permission qu'ils demandent.

Supposons que J Smith souhaite visualiser la vidéo en direct sur la caméra 13. Nos trois questions fondamentales sont :

- Qui êtes vous et êtes-vous qui vous prétendez être ? (J Smith, OUI)
- À quoi voulez-vous accéder ? (Caméra 13)
- Que voulez-vous en faire une fois que vous l'avez obtenu ? (Visualiser de la vidéo en direct)

La sécurité avancée d'Intellex charge d'abord le descripteur de sécurité pour la vidéo en direct de l'environnement de sécurité. Ensuite, en utilisant l'information de la session de connexion créée pour JSmith lors de l'authentification, le système d'exploitation est interrogé :

J Smith a-t-il accès à de la vidéo en direct sur la caméra 13 ?

Le système traite cette requête comme si J Smith demandait le fichier dans l'exemple précédent, mais maintenant, le descripteur de sécurité est spécialement créé et maintenu par Intellex. Comme avant, s'il a la permission, il peut visualiser la vidéo en direct sur la caméra 13.

Utilisateurs, groupes et héritages

Policy Manager utilise des utilisateurs et des groupes du votre réseau corporatif existant. Il n'est pas nécessaire de maintenir une liste séparée en outre de celle de votre environnement de réseau normal. Par conséquence, le client d'administration n'a aucun mécanisme qui vous permet d'ajouter de nouveaux utilisateurs ou groupes ; ils sont déjà présents.

Pour qu'un utilisateur ou un groupe d'utilisateurs ait accès aux instruments, le domaine dans lequel est installé Policy Manager doit reconnaître cet utilisateur ou ce groupe. Si vous avez besoin d'utilisateurs ou de groupes supplémentaires, vous ou votre administrateur de réseau doivent les ajouter à l'entreprise.

Vous ne pouvez authentifier que des utilisateurs. Les groupes sont des utilisateurs partageant des permissions communes. Par exemple, si J Smith est un membre du groupe Marketing et que le groupe Marketing possède la permission totale sur le fichier « Forcasts.xls » sur un serveur de fichiers, alors J Smith aura la permission totale sur ce fichier, bien que J Smith n'ait pas reçu la permission explicite d'accès sur ce fichier. En d'autres mots, les permissions d'accès d'un utilisateur sont en réalité la somme de toutes les permissions qu'il a explicitement reçues, plus les permissions attribuées à chacun des groupes auquel appartient cet utilisateur.

Ce principe s'applique également à la sécurité avancée d'Intellex. En nous appuyant sur l'exemple précédent, si le groupe Boston à accès à de la vidéo en direct sur les caméras 1 à 16 sur Intellex1, J Smith pourra également visualiser ces caméras, même s'il n'apparaît pas dans la liste des utilisateurs et des groupes ayant reçus l'accès à ces caméras.

Les exemples précédents illustrent le concept centralisé de la sécurité réseau : l'héritage. Dans le scénario précédent, J Smith avait hérité les permissions attribuées au groupe Boston. En outre, J Smith n'hérite pas seulement les permissions attribuées aux groupes auxquels il appartient, mais également les refus explicites. Donc, si l'accès à de la vidéo en direct sur caméra 3 avait été explicitement refusé à Boston, J Smith ne pourra pas visualiser la caméra 3. Les refus sont prioritaires sur les permissions, donc, même si J Smith avait accès (soit explicitement, soit indirectement par héritage) à de la vidéo en direct sur caméra 3, il ne pourra pas la visualiser.

Trois formes de permissions d’accès

Il y a trois formes de base de permissions d’accès qu’un administrateur peut attribuer à un utilisateur ou un groupe d’utilisateurs :

- Accès implicite
- Accès explicite
- Refus explicite

Accès implicite

Virtuellement synonyme avec l’accès hérité. Si J Smith est un membre du groupe Boston et que ce groupe à accès à Forcasts.xls, alors J Smith aura accès à Forcasts.xls. Lorsque l’administrateur doit résoudre des problèmes d’accès, ce type d’accès est le plus difficile à reconnaître puisqu’il n’y a pas d’entrée pour J Smith dans le descripteur de sécurité et son nom n’apparaît donc pas dans l’éditeur de contrôle d’accès pour de descripteur.

Accès explicite

L’administrateur peut explicitement attribuer l’accès à un objet à un utilisateur ou un groupe d’utilisateurs. Supposons qu’il y a un second fichier, Forcasts2.xls auquel Boston n’a pas accès. L’administrateur peut explicitement attribuer l’accès à J Smith en l’ajoutant à la liste d’utilisateurs ou de groupes d’utilisateurs dans le descripteur de sécurité des fichiers. L’administrateur attribue l’accès par le biais de l’éditeur de contrôle d’accès, en ajoutant J Smith au descripteur de sécurité du fichier et en cochant ensuite la case avec l’intitulé Permettre. Ultérieurement, le nom de J Smith apparaîtra à chaque fois que lui ou une autre personne, édite le descripteur de sécurité.

Refus explicite

L’administrateur peut explicitement refuser l’accès à un objet à un utilisateur ou un groupe d’utilisateurs. Supposons que le patron du groupe Boston décide que J Smith ne peut plus visualiser le fichier Forcasts.xls. J Smith a hérité l’accès à ce fichier (c.-à-d. il n’apparaît pas dans le descripteur de sécurité de ce fichier). La seule manière d’annuler un accès implicite (hérité) est le refus explicite d’accès pour un utilisateur ou groupe d’utilisateurs spécifiques. Le refus explicite est prioritaire sur toute autre forme de permission d’accès. Utilisation de l’éditeur de contrôle d’accès, en ajoutant J Smith au descripteur de sécurité du fichier et en cochant ensuite la case avec l’intitulé Refus.

Annexe B : Forum aux questions

Que signifie propagation ?

Le dialogue Propager paramètres vous permet de copier les paramètres de sécurité d'un instrument vers un ou plusieurs autres instruments. Uniquement les paramètres de sécurité seront copiés ; le nom de l'instrument et la description restent inchangés.

Que signifie héritage ?

Si vous allez éditer les paramètres de sécurité pour un instrument et sélectionnez un objet « conteneur » (les objets de la liste avec une petite case devant le nom), comme « Données multimédia » ou « Administration », vous obtiendrez un éditeur générique. Puisqu'un conteneur n'a pas d'éléments spécifiques, vous ne pouvez attribuer qu'un accès local ou distant à la fonction. Cependant, les utilisateurs et les groupes ajoutés au niveau du conteneur sont « hérités » par toutes les fonctions dans ce conteneur (c.-à-d., tous les objets enfants pour lesquels le parent direct est le conteneur).

Par exemple, si vous ajoutez un utilisateur nommé J Smith au conteneur « Données multimédia » et lui attribuez l'accès total, J Smith pourra tout vois, indépendamment de s'il se trouve directement devant l'instrument (accès local) ou s'il accède à distance aux données par le biais de Network Client ou l'API. Cela se passe car la permission d'accès pour tous les flux de données (c.-à-d., toutes les sous-fonctions dans Données multimédia) sont « accès permis » les permissions de J Smith ont été automatiquement hérités du conteneur parent à tous les objets enfant. En outre, l'accès attribué à chaque enfant est déterminé par un ensemble spécial de règles appliquées par le serveur. Ces règles sont différentes pour chaque objet (fonction) enfant (pour les flux multimédia, l'accès est autorisé pour tous les 16 flux, pour Administration\Utilitaire, l'accès est autorisé pour Générer les alarmes, Effacer les alarmes verrouillées et Effacer CD-RW. Aucune autre fonction n'est autorisée).

L'héritage est un puissant outil qui permet d'attribuer rapidement des permissions par défaut à plusieurs utilisateurs ou groupes.

Que se passe-t-il lorsque je propage vers un unique instrument ou groupe d'instruments ?

La propagation des paramètres de sécurité d'un instrument à un ou plusieurs instruments copie les paramètres de l'instrument source (celui où vous avez sélectionné Propager dans le menu) vers les instruments désignés en tant qu'instruments cible dans le dialogue Policy Manager - Propager paramètres.

Par exemple, en changeant les paramètres pour un instrument par défaut et en propageant ensuite ces paramètres à d'autres instruments ou zones, l'administrateur peut configurer et maintenir un environnement de sécurité uniforme autour de plusieurs instruments individuels en même temps. Vous pouvez propager les paramètres de sécurité pour l'instrument par défaut vers des ou tous les instruments dans la même zone ou dans des zones non-connexes. Vous pouvez également propager les paramètres vers des instruments en-dehors de la zone où se trouve l'instrument source. Le vue d'une zone est similaire à la vue du nœud « Tous les instruments sécurisés » (le nœud « Tous les instruments sécurisés » est une autre zone).

Lorsqu'un instrument s'enregistre la première fois auprès de Policy Manager, il reçoit une copie des paramètres de sécurité actuels pour l'instrument par défaut du site. Dans un sens, les paramètres pour l'instrument par défaut du site ont été automatiquement propagés au nouvel instrument.

La propagation NE MODIFIE PAS le nom ou la description des instruments ciblés.

Que sont des instruments par défaut ?

Les instruments par défaut sont en réalité des modèles de sécurité que les administrateurs peuvent utiliser en tant qu'aide pour maintenir un environnement de sécurité uniforme sur le site entier ou pour différentes zones de sécurité au sein du site.

Par exemple, chaque zone contient un instrument par défaut qui représente les paramètres de sécurité appliqués à tous les instruments des zones membre (vous pouvez outrepasser ce comportement par défaut).

Un instrument par défaut spécial est l'instrument par défaut du site dans la zone des « Instruments non-attribués ». Ce modèle est utilisé à chaque fois qu'un nouvel instrument s'enregistre auprès de Policy Manager et doit donc représenter l'environnement de sécurité de base pour le site entier.

Quelle est la différence entre un instrument actif et un instrument inactif ?

Un instrument actif est un instrument prêt à utiliser, c'est à dire, il enregistre de la vidéo et peut recevoir des commandes de recherche et d'autres fonctions à partir d'un client local ou distant.

Un instrument inactif est un instrument qui ne répond pas aux requêtes émanant du serveur. Ceci ne signifie pas nécessairement qu'actuellement l'instrument n'enregistre pas de la vidéo ; il pourrait y avoir un problème de réseau qui empêche les communications entre le serveur et le client. C'est cependant une situation que l'administrateur doit investiguer.

Les instruments sont vérifiés régulièrement pour assurer qu'ils sont toujours actifs et disponibles pour utilisation. Lorsqu'un instrument actif ne répond pas à cette enquête ou qu'il répond par un code d'erreur, l'instrument est considéré inactif. À ce moment, une notification est envoyée à toutes les sessions d'administration actuellement actives et un événement est ajouté aux journaux d'activité.

Annexe C : Liste des fonctionnalités sécurisables

Remarque

Il s'agit de liste des fonctions sécurisables, actuellement prises en charge par la version 3.2 d'Intellex. Consultez le Guide d'installation et de configuration d'Intellex pour une explication plus approfondie de chaque fonction.

Catégorie	Fonction	Éléments	Valeur par défaut
Instrument	Toutes les fonctions sont concernées	Ceci est le niveau supérieur d'un instrument. Les utilisateurs ou les groupes avec l'accès refusé ou autorisé donneront en héritage ces paramètres à toutes les fonctions. Lorsque des paramètres sont hérités d'un conteneur vers ses enfants, seules les valeurs par défaut spécifiques pour chaque enfant (fonction) seront définies.	
Administration	Utilitaires	Générer les alarmes - permet la génération manuelle des alarmes à des fins de test.	X
		Effacer les alarmes verrouillées - permet d'effacer les messages d'alarme des volets en mode Alarme verrouillée.	X
		Effacer CD-RW - permet d'effacer des données sur le support CD-RW inséré.	
		Visualiser les rapports d'activité - permet de visualiser le journal d'activité interne.	
	Réglage	Configurer le mode d'enregistrement - permet de basculer entre le mode linéaire et circulaire et de programmer le seuil d'avertissement linéaire.	
		Régler les alarmes - permet de changer les noms et les paramètres des alarmes.	X
		Régler le planning d'archivage - permet de personnaliser des plannings d'archivage.	

Catégorie	Fonction	Éléments	Valeur par défaut
		Installer caméras - permet de changer les noms et les paramètres des caméras.	
		Installer caméras cachées - permet de changer les paramètres des caméras cachées et de visualiser des caméras configurées en tant que cachées.	
		Régler le planning - permet d'apporter des modifications au planning d'enregistrement.	X
		Régler l'affichage - permet d'apporter des modifications aux paramètres d'affichage en direct/moniteur d'appel.	
		Régler la sécurité - permet de créer et de changer les paramètres de sécurité.	
		Configurer texte - permet d'apporter des modifications aux paramètres du flux de texte.	
		Régler audio - permet d'apporter des modifications aux paramètres audio.	
		Notification par courrier électronique - permet la notification d'événements système sur l'Intellex, notamment les alarmes, etc.	
	Système	Mettre à niveau ou modifier la licence - permet la mise à niveau de la licence	
		Commencer l'enregistrement - permet de reprendre l'enregistrement après son arrêt.	
		Arrêter le système - permet d'arrêter le système.	X
		Sortir aux permissions système - permet de sortir au système d'exploitation.	

Catégorie	Fonction	Éléments	Valeur par défaut
		Accès aux paramètres de stockage du système - permet d'apporter des modifications aux paramètres du volume de stockage.	
		Accès aux paramètres du serveur - permet d'apporter des modifications aux adresses de port.	
		Accès aux paramètres de date et heure - permet de modifier la date et l'heure du système.	
Données multimédia	Vidéo en direct	Caméras 1-16 - permet de visualiser de la vidéo en direct sur les caméras sélectionnées.	Tous
	Recorded Video Vidéo enregistrée	Caméras 1-16 - permet de reproduire/rechercher de la vidéo enregistrée sur les caméras sélectionnées.	Tous
	Texte enregistré	Flux de texte 1-16 - permet de reproduire/rechercher des textes enregistrés sur des flux de texte sélectionnés.	Tous
	Audio en direct	Flux de données audio 1 - permet d'écouter de l'audio en direct sur le flux audio 1.	Tous
	Audio enregistrée	Flux de données audio 1 - permet de reproduire de l'audio enregistré sur le flux 1.	Tous
Avancée	Contrôle de dôme	Caméras 1-16 - permet le contrôle de dôme pour la caméra sélectionnée.	Tous
	Programmation de dôme	Caméras 1-16 - permet d'accéder à la programmation de dôme pour les caméras spécifiées.	
	Local Archive Archive locale	Activer l'archivage - permet d'accéder au menu d'archivage.	X
	Fonctions à distance : Sous-permissions	Télécharger rapport d'alarmes : Permission de télécharger le journal des alarmes de cet instrument.	

Catégorie	Fonction	Éléments	Valeur par défaut
		Télécharger un rapport d'activité : Permission de télécharger le journal des activités de cet instrument	
		Télécharger l'état système : Permission de récupérer les informations d'état du système de cet instrument.	
		Accès à distance aux paramètres d'enregistrement : Permission d'accéder à distance aux paramètres d'enregistrement pour cet instrument (spécifique API).	
		Générer les alarmes à distance : Permission de générer des alarmes à distance sur cet instrument (spécifique API).	

Index

A

Ajouter un instrument 10
Attribuer à la zone 10
Attribution de licence v

C

Caractéristiques 2
Clé de licence vi
Couper 10

D

Définir description 10
Durée d'exclusion 8

F

fonctions sécurisables pour la version 3.2 d'Intellex 9

G

Garantie v
Gérer la sécurité avancée d'Intellex par le biais des Paramètres de sécurité 9
Gestionnaire de licence 3

I

Icônes et leurs vues 5
Informations de licence v
Intellex Archive Manager 3
Intellex Policy Manager 3
Intervalle d'enquête d'instrument 8

J

journaux d'événements système 2

L

Licence
  Attribution v
  Logiciel v
License
  Mise à niveau v

M

Maximum d'essais de connexion 8
Mise à niveau de licence v
Module Tous les instruments sécurisés 9

P

Permettre plusieurs sessions d'administration simultanées 8
Policy Manager (PM) v1.1 pour Intellex® DVMS 1
Propager paramètres 10

R

Ressources 3

S

sécurité avancée 1
Supprimer 10

T

Travailler avec des politiques par le biais de Politiques globales du site 7