Benutzerhandbuch

Policy Manager für Intellex®

Version 1.2

Teilenummer 8200-0566-06 A0

Hinweis

Die Angaben in diesem Handbuch beziehen sich auf die Beschaffenheit des Systems zum Zeitpunkt der Veröffentlichung. Der Hersteller kann seine Produkte allerdings jederzeit ändern und verbessern. Entsprechend sind auch bei sämtlichen Spezifikationen jederzeit unangekündigte Änderungen möglich.

Copyright

American Dynamics
6795 Flanders Drive
San Diego, CA 92121-2903 U.S.A.

Kundendienst

Danke, dass Sie sich für ein Produkt von American Dynamics entschieden haben. Wir unterstützen unsere Produkte mit einem umfassenden weltweiten Händlernetz. Der Händler, von dem Sie dieses Produkt bezogen haben, ist Ihre erste Anlaufstelle, wenn Sie Unterstützung benötigen. Unsere Händler sind in der Lage, Ihnen den besten Kundendienst und die bestmögliche Unterstützung zu bieten. Händler erreichen American Dynamics unter (800) 507-6268 oder +1 561 912-6259 bzw. im Web unter www.americandynamics.net.

Markenrechtliche Hinweise

Warnhinweise

WARNUNG: UM DIE GEFAHR EINES STROMSCHLAGES MÖGLICHST AUSZUSCHLIESSEN, DARF DIESES GEHÄUSE NICHT GEÖFFNET WERDEN. ES ENTHÄLT KEINE VOM BENUTZER ZU WARTENDEN TEILE. LASSEN SIE WARTUNGS- UND KUNDENDIENSTARBEITEN VON ENTSPRECHEND GESCHULTEM FACHPERSONAL AUSFÜHREN.
SCHÜTZEN SIE DAS GERÄT VOR REGEN UND SORGEN SIE DAFÜR, DASS DAS GERÄT NICHT MIT FEUCHTIGKEIT IN BERÜHRUNG KOMMT.
DIESES PRODUKT IST NICHT IN GEFÄHRDETEN BEREICHEN ZU INSTALLIEREN, IN DENEN HOCH ENTZÜNDLICHE ODER EXPLOSIVE PRODUKTE GELAGERT ODER VERWENDET WERDEN.

DAS HOCHSPANNUNGSZEICHEN (BLITZ MIT PFEIL) IN EINEM GLEICHSEITIGEN DREIECK MACHT BENUTZER AUF DIE GEFAHR EINES STROMSCHLAGS BEIM ÖFFNEN DES GEHÄUSES AUFMERKSAM.

ACHTUNG: Wenn die Batterie unsachgemäß ersetzt wird, besteht Explosionsgefahr.

Verwenden Sie identische Batterien oder Batterien des gleichen Typs, die vom Hersteller der Batterien empfohlen werden. Entsorgen Sie leere Batterien gemäß den Herstelleranweisungen.

ACHTUNG: UM DIE GEFAHR EINES STROMSCHLAGES MÖGLICHST AUSZUSCHLIESSEN, DARF DAS GEHÄUSE NICHT GEÖFFNET WERDEN. ES ENTHÄLT KEINE VOM BENUTZER ZU WARTENDEN TEILE. ÜBERLASSEN SIE DIE WARTUNG QUALIFIZIERTEM FACHPERSONAL.

ACHTUNG: Wenn die Batterie nicht ordnungsgemäß ausgetauscht wird, besteht Explosionsgefahr.

WARNUNG: DIESES GERÄT IST EIN LASERPRODUKT DER KLASSE 1 MIT EINER LASERDIODE DER KLASSE 1 UND ERFÜLLT DIE FDA-ANFORDERUNGEN AN DAS EMISSIONSVERHALTEN GEMÄSS 21 CFR SUBCHAPTER J UND GEMÄSS DEM KANADISCHEN RADIATION EMITTING DEVICES ACT (REDR C1370).

Rack-Montage

Erkundigen Sie sich beim Lieferanten Ihres Racks nach geeigneten Befestigungen, und berücksichtigen Sie dabei in angemessener Weise das Gewicht des Produkts.

Erkundigen Sie sich beim Hersteller Ihres Racks nach geeigneter Hardware sowie danach, wie dieses Produkt sicher befestigt werden kann, ohne die Bedienung des Geräts zu beeinträchtigen.

Vermeiden Sie ungleichmäßige Belastungen und mechanische Instabilität, wenn das Gerät in einem Rack montiert wird.

Achten Sie darauf, dass die Geräte so montiert werden, dass ausreichender Luftstrom zur Kühlung gegeben ist.

Die Höchsttemperatur bei Rack-Montage beträgt 40 °C.

Vermeiden Sie ungleichmäßige Belastungen und mechanische Instabilität, wenn das Gerät in einem Rack montiert wird.

Prüfen Sie, welche die Spannungsanforderungen auf dem Typenschild genannt sind, und stellen Sie sicher, dass keine Netzüberlastungen verursacht und keine Schäden durch Spannungsspitzen hervorgerufen werden.

Sorgen dafür, dass die Erdung zuverlässig und durch keinerlei Verbindungen beeinträchtigt ist.

WARNUNG: EINE ENTSPRECHENDE PRÜFUNG HAT BESTÄTIGT, DASS DAS GERÄT DIE GRENZWERTE FÜR DIGITALGERÄTE DER KLASSE „A“ GEMÄSS DEN FCC RULES PART 15 ERFÜLLT. DIESE GRENZWERTE SOLLEN BEI NORMALEM BETRIEB DES GERÄTS IN EINER GEWERBLICHEN UMGEBUNG EINEN ANGEMESSENEN SCHUTZ GEGEN GESUNDHEITSGEFÄHRDENDE STRAHLUNG SICHERSTELLEN. DAS GERÄT ERZEUGT, NUTZT UND EMITTIERT U.U. FUNKENERGIE UND KANN DEN FUNKVERKEHR STÖREN, WENN ES NICHT GEMÄSS DER ENTSPRECHENDEN ANLEITUNG INSTALLIERT WIRD. DER BETRIEB DIESES GERÄTS IN WOHNGEBIETEN KANN STÖRSTRAHLUNGEN VERURSACHEN; WENN STÖRSTRAHLUNGEN AUFTRETEN, BEHEBT DER BENUTZER DIE URSACHE AUF EIGENE KOSTEN.

Änderungen und Modifikationen, die nicht ausdrücklich von der für die Konformität zuständigen Partei genehmigt wurden, können zum Erlöschen der Betriebserlaubnis für das Gerät führen.

HINWEIS: Dieses Produkt wurde gemäß den FCC-Bestimmungen unter Anschluss der Systemkomponenten mit abgeschirmten E-/A-Kabeln und Steckern getestet. Damit das Gerät die FCC-Bestimmungen erfüllt, müssen die Benutzer abgeschirmte Kabel und Stecker verwenden. Dies gilt nicht für Netz- und Alarmsignalkabel.

Dieses Digitalgerät hält die für Geräte der Klasse A vorgesehenen Grenzwerte für Funkstrahlungen gemäß den Radio Interference Regulations (ICES-003) des kanadischen Fernmeldeministeriums ein.

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.

Lizenzinformationen

LESEN SIE DIESE LIZENZVEREINBARUNG, BEVOR SIE DIE CD-HÜLLE ÖFFNEN, DIE SOFTWARE INSTALLIEREN UND DAS SYSTEM IN BETRIEB NEHMEN.

DIESE LIZENZVEREINBARUNG BESCHREIBT IHRE RECHTE UND VERPFLICHTUNGEN. MIT DEM AUFBRECHEN DES SIEGELS, DEM INSTALLIEREN DER SOFTWARE UND DEM EINSATZ DES SYSTEMS STIMMEN SIE SÄMTLICHEN BEDINGUNGEN DER VEREINBARUNG ZU. WENN SIE DEN BEDINGUNGEN NICHT ZUSTIMMEN, KÖNNEN SIE DAS PAKET EINSCHLIESSLICH DER DOKUMENTATION UND DER BEGLEITMATERIALIEN INNERHALB VON 30 TAGEN GEGEN RÜCKERSTATTUNG DES KAUFPREISES DORT ZURÜCKGEBEN, WO SIE DAS PRODUKT GEKAUFT HABEN.

SOFTWARE-LIZENZ

Die Software beinhaltet die Intellex API, modulare Programme und Quellcodes in Form von Beispieldaten, das Intellex API-Handbuch und die in elektronischer Form zur Verfügung gestellte Dokumentation. Sie erhalten Zugriff auf diese Komponenten, indem Sie die Software auf der Festplatte eines Rechners installieren. Die Software wird nicht veräußert, sondern nach Maßgabe einer Lizenzvereinbarung zur Verfügung gestellt.

LIZENZVEREINBARUNG

Mit dem Kauf der Intellex API-Software kommt eine Lizenzvereinbarung zwischen Sensormatic und Ihnen zustande. Gemäß dieser Lizenzvereinbarung können ausschließlich Sie diese Software verwenden. Ihre Zustimmung zur Lizenzvereinbarung betreffend die Intellex API berechtigt Sie zur Verwendung der API-Software und der begleitenden modularen Programme einschließlich des jeweiligen Quellcodes. Diese Lizenzvereinbarung berechtigt Sie jedoch nicht, die API oder die modularen Programme und die jeweiligen Quellcodes oder sonstige Kopien der API sowie von Programmen und Quellcodes an Dritte weiterzugeben oder zu veräußern. Die Software-Lizenz beschränkt sich auf den Einsatz der Software mit Intellex-Geräten. Für Software-Produkte, die Sie unter Verwendung der API entwickeln, bestehen keine Einschränkungen hinsichtlich der Einrichtung eines lizensierten Programms in Ihrem Unternehmen. Von Ihnen unter Verwendung der Intellex API oder der modularen Programme entwickelte Software-Programme können Sie jedoch ohne Genehmigung von Sensormatic nicht als Zubehörprodukte zur Intellex-Produktreihe an Dritte veräußern oder weitergeben.

SONSTIGE RECHTE UND EINSCHRÄNKUNGEN

- Der Erwerb einer Demo-Kopie der Software wird als Kauf betrachtet und unterliegt entsprechend ebenfalls dieser Lizenzvereinbarung.
- Die entsprechende Bestellung gilt als Nachweis Ihrer Lizenz zur Wahrnehmung der hiermit erteilten Rechte und ist von Ihnen aufzubewahren.
- Die ausführbaren Programme dürfen nicht dekompiliert, disassembliert oder rückentwickelt werden; dies gilt u.a. auch für die Bibliotheksdateien, deren Quellcode Sie nicht erhalten haben. Die modularen Programme werden von dieser Einschränkung ausgenommen; von den Quellcodes, die Sie von diesen Programmen erhalten haben, können Sie beliebige Bestandteile neu kompilieren, neu assemblieren und modifizieren.
- Sie können keine Unterlizenzen erteilen und Sie können die Software nicht vermieten oder im Rahmen einer Leasing-Vereinbarung überlassen; ferner sind Sie nicht berechtigt, die Software unbefristet Dritten zu überlassen, indem Sie die Originalmedien mit dem Software-Paket sowie diese Lizenz einem Dritten zukommen lassen.
- Sensormatic kann diese Vereinbarung jederzeit widerrufen, wenn Sie gegen die Bestimmungen dieser Vereinbarung verstoßen. In diesem Fall sind Sie verpflichtet, die von Ihnen gekaufte CD-ROM mit der gesamten Software und/oder die aus dem Web heruntergeladene Intellex API-Software sowie jegliche API-Software, die Sie aus dem Web heruntergeladen haben oder die Ihnen als Patch zugesendet wurde, sämtliche von Ihnen modifizierten modularen Programme und alle von Ihnen unter Verwendung der Intellex API entwickelten Software-Programme zu vernichten.
- Die Software kann Software-Komponenten von Dritten beinhalten, die gemäß einer eigenen Endbenutzer-Lizenzvereinbarung (EULA = *End User License Agreement*) überlassen wurden. Lesen Sie sämtliche Lizenzbestimmungen durch und bewahren Sie die Dokumentation der Lizenzbestimmungen auf, die Sie mit der Software erhalten haben. Die Einhaltung von Endbenutzer-Lizenzvereinbarungen (EULA) Dritter ist Bestandteil dieser Vereinbarung.

Bei Missachtung dieser Einschränkungen erlischt diese Lizenzvereinbarung, und Sensormatic ist berechtigt, geeignete juristische Schritte zu unternehmen.

COPYRIGHT

Die Software ist ein urheberrechtlich geschütztes Produkt von Sensormatic und unterliegt US-amerikanischen und internationalen Urheberrechtsbestimmungen.

UPGRADES

Wenn die Software als Upgrade einer anderen Software-Version oder als Upgrade einer Komponente eines Software-Programmpakets gekauft wurde, über das Sie eine Lizenzvereinbarung getroffen haben, können Sie die Software ausschließlich nach Maßgabe dieser Vereinbarung verwenden und übertragen.

EINGESCHRÄNKTE GARANTIE

Sensormatic garantiert, dass der Datenträger, auf dem die Software aufgezeichnet wurde, sowie die mit der Software gelieferte Dokumentation bei normalem Gebrauch über einen Zeitraum von neunzig (90) Tagen ab der Auslieferung an den Erstbenutzer keine Material- und Herstellungsfehler aufweist. Sensormatic garantiert ferner für den gleichen Zeitraum, dass sich die auf dem Datenträger gemäß dieser Lizenzvereinbarung überlassene Software weitgehend verhält, wie in den mit dem Produkt gelieferten Benutzerinformationen beschrieben, wenn das Produkt in Verbindung mit der genannten Hardware und in der genannten Entwicklungsumgebung eingesetzt wird.

ANSPRÜCHE DER KUNDEN

Die Haftung von Sensormatic sowie Ihre Ansprüche gemäß dieser Garantie beschränken sich nach Ermessen von Sensormatic auf a) den Versuch, Software-Fehler mit nach unserem Ermessen zur Behebung des jeweiligen Problems angemessenem Aufwand zu beheben, b) den kostenlosen Ersatz des Datenträgers, der Software oder der Dokumentation, wenn erforderlich, und c) die Erstattung der Lizenzgebühr unter Kündigung dieser Vereinbarung. Bei Ersatzprodukten gilt die Garantie für den noch verbleibenden Zeitraum der ursprünglichen Garantiefrist. Keinerlei Ansprüche bestehen bei CD- oder Software-Fehlern, wenn diese Fehler auf einen Unfall, Missbrauch, Änderungen oder unsachgemäßen Einsatz zurückzuführen sind. Kundendienstleistungen und Unterstützung im Rahmen der Garantie werden dort erbracht, wo das Produkt ursprünglich gekauft wurde.

KEINE SONSTIGEN GARANTIEN

Die vorstehende Garantie ersetzt alle sonstigen expliziten und impliziten Garantien einschließlich u.a. der impliziten Garantie der Marktgängigkeit und der Eignung für einen bestimmten Zweck. Mündliche und schriftliche Angaben und Hinweise von Sensormatic sowie seitens der Vertreter, Händler oder Vertriebspartner von Sensormatic begründen keinerlei sonstige Garantie, und für die Zuverlässigkeit dieser Angaben und Hinweise kann keine Gewähr übernommen werden.

KEINE HAFTUNG FÜR FOLGESCHÄDEN

Unter keinen Umständen haftet Sensormatic für Schäden einschließlich Schäden aufgrund entgangener Gewinne, Datenverlusten, beiläufiger Schäden oder Folgeschäden, die darauf zurückgeführt werden, dass Sie die Software oder die begleitende Dokumentation verwendet haben oder nicht verwenden konnten. Diese Einschränkung gilt auch dann, wenn Sensormatic oder ein befugter Vertreter von Sensormatic auf die Möglichkeit entsprechender Schäden hingewiesen wurde. Ferner übernimmt Sensormatic keine Garantie dafür, dass die Software ohne Störungen und Fehler eingesetzt werden kann.

Aufgrund dieser eingeschränkten Garantie erwerben Sie bestimmte Rechtsansprüche. Nach Maßgabe nationaler oder regionaler Rechtsvorschriften haben Sie u.U. weiter reichende Rechte. In manchen Ländern bzw. US-amerikanischen Bundesstaaten ist der Ausschluss von beiläufigen Schäden und Folgeschäden als Anspruchsgrundlage nicht zulässig; ebenso kann eine Einschränkung der Dauer einer impliziten Garantie unzulässig sein. Entsprechend sind die vorstehenden Einschränkungen u.U. nicht maßgeblich für Sie.

SALVATORISCHE BESTIMMUNG

Wenn eine Bestimmung dieser Vereinbarung rechtlich nicht zulässig, ungültig oder aus einem beliebigen Grund nicht durchsetzbar sein sollte, wird diese Bestimmung aus dieser Vereinbarung gestrichen. Dies wirkt sich jedoch nicht auf die Wirksamkeit und die Durchsetzbarkeit der übrigen Bestimmungen aus. Diese Vereinbarung unterliegt dem Recht des Staates Florida.

Bewahren Sie einen Beleg über die Entrichtung der Lizenzgebühr auf, aus dem Modellnummer, Seriennummer und Zahlungsdatum hervorgehen, und legen Sie diesen Zahlungsbeleg vor, wenn Sie Kundendienst- oder Unterstützungsleistungen gemäß dieser Garantie beanspruchen.

EINGESCHRÄNKTE RECHTE DER US-REGIERUNG

Die Software und die Dokumentation unterliegen EINGESCHRÄNKTEN RECHTEN. Nutzung, Vervielfältigung und Veröffentlichung durch die US-amerikanische Regierung unterliegen den Einschränkungen gemäß Paragraph (c)(1)(ii) der „Rights in Technical Data and Computer Software“ (DFARS 252.227-7013) bzw. gemäß Paragraph (c)(1) und (2) der „Commercial Computer Software—Restricted Rights“ (48 CFR 52.227-19). Hersteller ist die Sensormatic Electronics Corporation, 6600 Congress Ave., Boca Raton, FL 33487 USA.

Wichtiger Hinweis

Bevor Sie fortfahren, lesen Sie bitte alle Anweisungen und Warnungen in diesem Handbuch sorgfältig durch. Bewahren Sie dieses Handbuch zusammen mit dem Originalkaufbeleg zum Nachschlagen von sowie für etwaige Garantiefälle auf.

Prüfen Sie beim Auspacken Ihres Intellex-Geräts, ob Teile fehlen oder beschädigt sind. Wenn Teile fehlen oder offensichtliche Schäden festzustellen sind, INSTALLIEREN DAS PRODUKT NICHT UND NEHMEN SIE DAS PRODUKT NICHT IN BETRIEB. Wenden Sie sich dann an Sensormatic oder an Ihren Händler.

Für Ihre Unterlagen

Tragen Sie die folgenden Produktinformationen ein. Wenn Sie sich an den technischen Kundendienst wenden, werden diese Angaben im Werk benötigt. Ebenfalls hilfreich sind diese Informationen bei Verlust oder Diebstahl.

Kaufdatum:

Seriennummer:

Lizensierungsschlüssel

Die Intellex-Software der Version 4.0 ist durch einen Software-Lizenzierungsschlüssel gegen unberechtigten Zugriff geschützt. Mit diesem Schlüssel wird die elektronische Hardware des Systems mit der autorisierten Software-Version und dem Funktionsumfang der Software abgestimmt, um den ordnungsgemäßen Betrieb des Systems zu gewährleisten. Wenn Sie Änderungen an der Netzwerkkarte des Geräts vornehmen, die Lizenzdatei entfernen bzw. bearbeiten oder die Systemfestplatte austauschen, muss eine neue Lizenzdatei installiert werden. Weitere Informationen erhalten Sie ggf. von Ihrem autorisierten Sensormatic Vertreter.

Inhalt

Policy Manager

Funktionen 2
Die Administrationskonsole des Intellex-Systems 3

Symbole

Die verwendeten Symbole und ihre Bedeutung 5

Allgemeine Standort-Richtlinien verwenden

Die erweiterten Intellex-Sicherheitsfunktionen in der Kategorie Sicherheitseinstellungen definieren

Objekte, die bei Intellex-Geräten mit erweiterten Sicherheitsfunktionen geschützt werden können. 9
Menü Gerät 10
Geräte hinzufügen. 11
Geräte löschen 11
Geräte an andere Standorte binden 11
Die Sicherheitseinstellungen eines Intellex-Geräts bearbeiten 12
Benutzer und Gruppen hinzufügen und entfernen. 13
Sicherheitseinstellungen von einem Intellex-Gerät auf ein anderes übertragen (kopieren) 16

Mit Zonen arbeiten

Menü Sicherheitszonen. 17
Die Zone Nicht zugewiesene Geräte. 17
Neue Zonen erzeugen (Geräte mit gemeinsamen Sicherheitseinstellungen zusammenfassen). 17
Zonen löschen. 18
Die Zonen-Einzelansicht 18
Das Menü Zone. 19
Intellex-Geräte in eine Sicherheitsone verschieben 20
Intellex-Geräte ersetzen 20

Mit dem Lizenz-Manager arbeiten

Die Network Client-Unternehmenslizenz. 24

Mit der Ereignisanzeige arbeiten

Das Snap-in Ereignisanzeige hinzufügen 26

Anhang A: Sicherheitskonzepte für den Policy Manager 29

Grundlegende Fragen 29
Authentifizierung 30
Wer sind Sie, und sind Sie wirklich derjenige, als der Sie auftreten? 30
Die Windows-Sitzung 30
Richtlinien und Berechtigungen für Standorte 31
Authorisierung 31
Wozu möchten Sie Zugang haben? 31
Was möchten Sie mit dem Objekt anfangen, zu dem Sie Zugang erhalten haben? 32
Sicherheitsdeskriptoren 32
Benutzer, Gruppen und geerbte Berechtigungen 33
Drei Typen von Zugriffsberechtigungen 34
Impliziter Zugriff 34
Expliziter Zugriff 34
Explizite Verweigerung 34

Anhang B: Häufig gestellte Fragen (FAQ) 35

Was bedeutet der Begriff „Übertragen“? 35
Was bedeutet „vererben“? 35
Was geschieht, wenn ich Einstellungen auf ein einzelnes Gerät oder eine Gerätegruppe übertrage? 35
Was sind Standardgeräte? 36
Was ist der Unterschied zwischen einem aktiven und einem inaktiven Gerät? . . 36

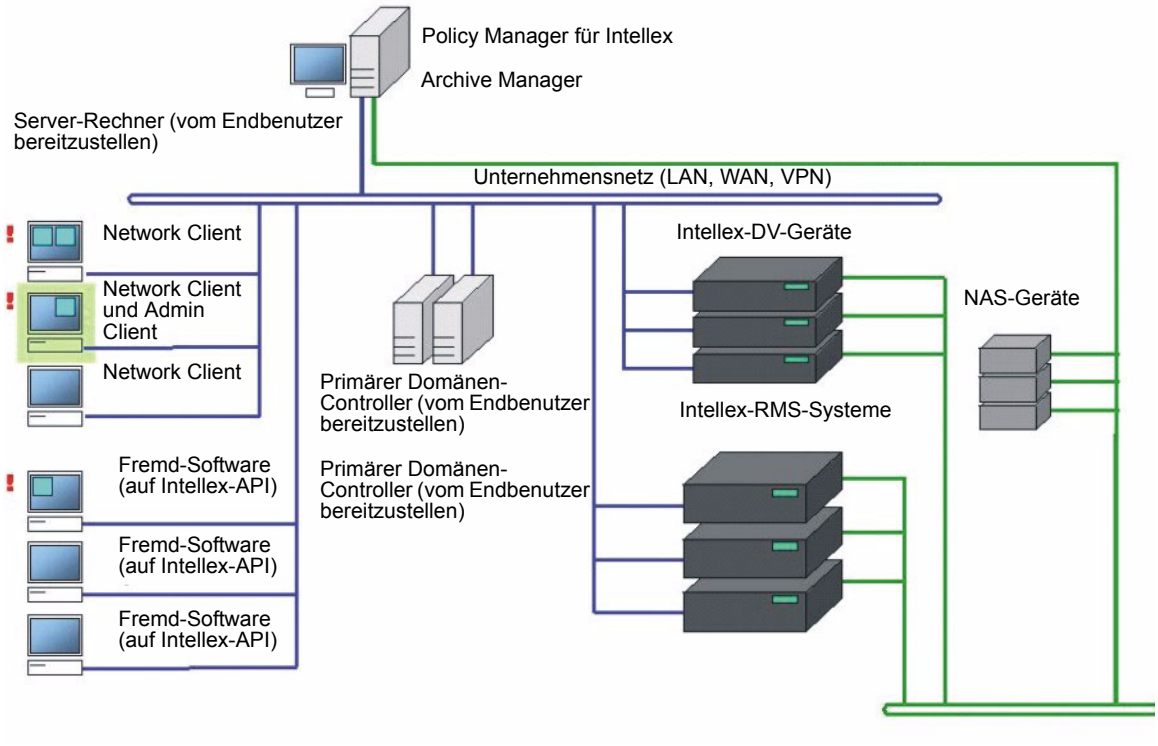
Anhang C: Menüs und Optionen, für die erweiterte Sicherheitseinstellungen aktiviert werden können 37

Index 41

Policy Manager

Der Intellex® Policy Manager V.1.2 ist ein Software-Produkt, das auf einem Server-Rechner installiert wird. Die Software wird in einem gemeinsamen Netz mit den vorhandenen Intellex-Geräten, Network Client-Workstations und/oder sonstigen API-basierten Remote-Applikationen ausgeführt und beinhaltet erweiterte Sicherheitsfunktionen für Videonetze. Die Aktivierung der erweiterten Sicherheitsfunktionen hat für die Benutzer folgende Vorteile:

- Besserer und umfassenderer Schutz vor Zugriffen auf Intellex-Ressourcen und -Funktionen und erhöhte Sicherheit bei der Nutzung von Intellex-Ressourcen und -Funktionen.
- Schutz von Videomaterial durch Microsoft-Sicherheitsfunktionen und.
- Zentrale Sicherheits-Verwaltung über mehrere Intellex-Einheiten hinweg.



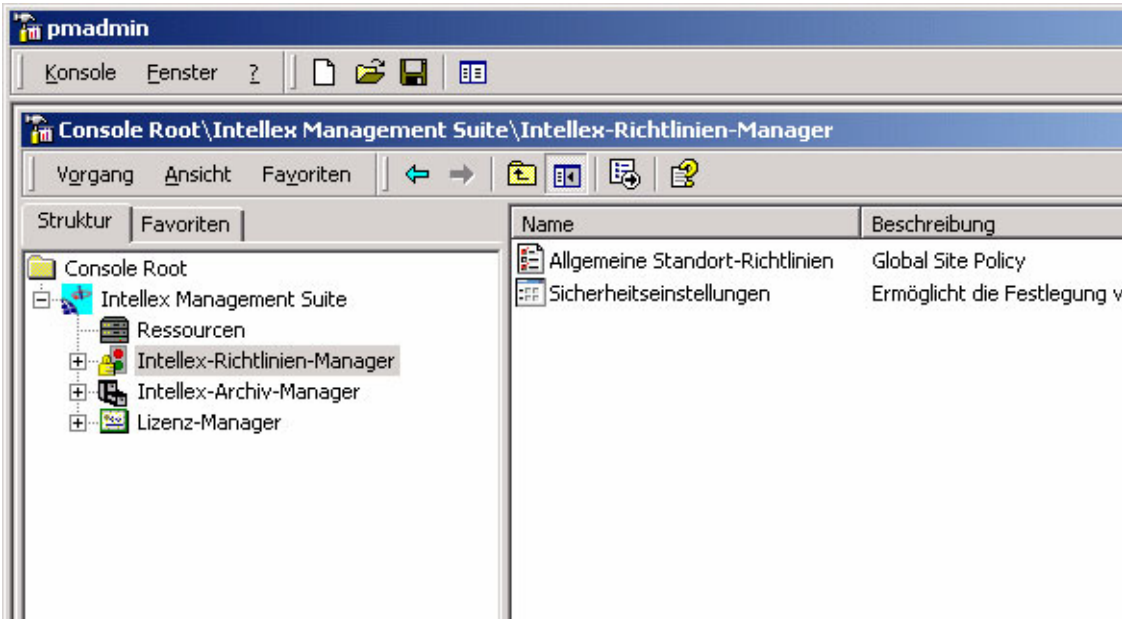
Funktionen

- Der Admin Client für den Policy Manager ist in die MMC (*Microsoft Management Console*) integriert. Daher können die Intellex-Sicherheitsfunktionen ganz ähnlich wie sonstige Netzapplikationen konfiguriert werden.
- Der Policy Manager bietet nicht nur eine größere Transparenz durch die Möglichkeit, Intellex-Attribute und Funktionen individuell zu konfigurieren, sondern fügt sich auch nahtlos in das Sicherheitskonzept von Microsoft Windows ein. Da der Policy Manager Einstellungen und Merkmale in größtmöglichem Umfang aus Windows übernimmt, finden sich die Benutzer rasch in der Benutzeroberfläche zurecht und sind mit den Sicherheitsfunktionen sowie mit den Funktionen zum Hinzufügen von Intellex-Gruppen und Benutzergruppen rasch vertraut. Auch dies trägt zu einer höheren Sicherheit beim Einsatz der Intellex-Geräte bei.
- Mit dem Policy Manager können Administratoren Intellex-Videosysteme in vorhandene Netze einbinden, ohne für ihr jeweiliges Netz definierte Sicherheitsrichtlinien zu beeinträchtigen. Der Policy Manager ist in die MS Windows-Konsole integriert und übernimmt sämtliche Sicherheitsprotokolle, die das betreffende Unternehmen bereits verwendet. Entsprechend brauchen Netzadministratoren keine zusätzlichen Netzprotokolle speziell für Videodaten mehr zu installieren. Selbst wenn Unternehmen weiterhin Videomaterial in einem privaten LAN getrennt vom jeweiligen Unternehmens-LAN/- WAN verwenden möchten, brauchen Netzadministratoren dank der erweiterten Sicherheitsfunktionen des Policy Managers nicht zu befürchten, dass die Systemsicherheit im Videonetz durch den Remote-Transfer über die gemeinsamen IT-Systeme (Firewalls, Router usw.) gefährdet wird.
- Der Policy Manager ermöglicht Sicherheitsadministratoren, Berechtigungen auf lokalen Systemen und auf Remote-Systemen zentral für mehrere Intellex-Geräte zu definieren.
- Sicherheitsadministratoren können für unterschiedliche Benutzer Berechtigungen zur Nutzung von Intellex-Funktionen und -Ressourcen auf verschiedenen Ebenen definieren; diese Möglichkeit geht über die Möglichkeiten hinaus, die das klassische Sicherheitskonzept bietet.
- Der Policy Manager ermöglicht die Ressourcenverwaltung und die Fehlererkennung bei vernetzten Intellex-Geräten. Der Server erkennt, ob Geräte zugänglich oder nicht verfügbar sind und erfasst die entsprechenden Zustände im Systemprotokoll.
- Mit Ereignisprotokollen können Sie den Systemstatus überwachen und Fehlermeldungen überprüfen. Der Policy Manager erzeugt und verwaltet ein eigenes Ereignisprotokoll, das in den vorhandenen Protokollmechanismus Ihres Betriebssystems integriert wird. Protokolliert werden sämtliche Verwaltungszugriffe und die Verfügbarkeit sämtlicher Geräte. Außerdem werden Zugriffsverletzungen erkannt und im Ereignisprotokoll erfasst. In der Microsoft-Ereignisanzeige können Sie die Protokolle wahlweise auf lokalen Systemen und auf Remote-Systemen anzeigen.

Hinweis

Die Abbildungen in diesem Handbuch wurden unter Windows 2000 erzeugt. Ihre Benutzeroberfläche sieht unter Umständen anders aus.

Die Administrationskonsole des Intellex-Systems



Im Verzeichnisbaum werden 4 Hauptkategorien dargestellt:

Ressourcen	In dieser Kategorie werden unabhängig vom Gerätetyp und vom jeweiligen Status sämtliche Gerätegruppen angezeigt.
Intellex-Policy Manager	In dieser Kategorie werden die erweiterten Sicherheitsfunktionen angezeigt.
Intellex-Archive Manager	In dieser Kategorie werden die Funktionen zum Archivieren und Abrufen von Daten aus dem verbundenen NAS-Gerät angezeigt. Der Archive Manager ist nur verfügbar, wenn dieses Icon erscheint.
Lizenz-Manager	In dieser Kategorie können Sie die aktuellen Lizenzinformationen überwachen und bearbeiten.

Die verwendeten Symbole und ihre Bedeutung

Symbol	Beschreibung
	Administrationskonsole des Intellex-Systems.
	Ressourcen.
	Policy Manager-Software.
	Richtlinien, die der Policy Manager (PM) allgemein für alle Geräte und Benutzer an Ihrem Standort definiert.
	Sicherheitsstellungen, die Sie wahlweise für alle Geräte, alle Benutzer und alle Zonen an Ihrem Standort definieren können.
	Geschützte Intellex-Geräte in Ihrem System.
	Ein einzelnes aktives Intellex-Gerät, für das die erweiterten Sicherheitsfunktionen aktiviert wurden.
	Geschütztes inaktives Intellex-Gerät (mit erweiterter Sicherheit).
	Dieses Icon repräsentiert eine funktionsfähige, ungesicherte Ressource (nicht im erweiterten Sicherheitsmodus).
	Dieses Icon repräsentiert ein nicht-funktionsfähiges Intellex-System (nicht im erweiterten Sicherheitsmodus).
	Sicherheitszonen, in denen Intellex-Geräte getrennt verwalteten Sicherheitseinheiten zugeordnet werden können.
	Eine einzelne Sicherheitszone mit einer Gruppe von Geräten, für die gemeinsam bestimmte Sicherheitseinstellungen gelten.
	Lizenz für ein bestimmtes Modul (z.B. für den Policy Manager oder den Archive Manager).
	Lizenzverwaltungsgruppe.

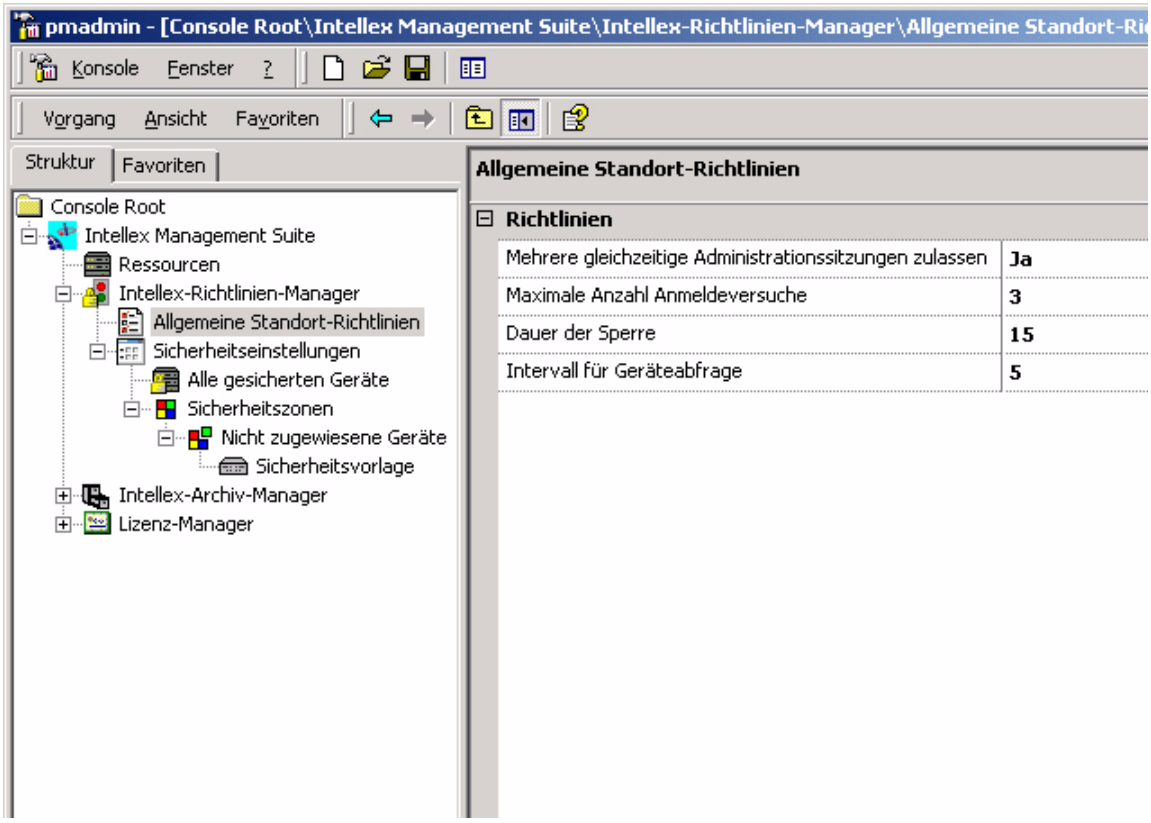
Hinweis

Außerdem können in der Windows-Oberfläche die Anzeigeformen Große Symbole, Kleine Symbole, Liste und Details ausgewählt werden.

Allgemeine Standort-Richtlinien verwenden

Wenn Sie im Policy Manager den Knoten Allgemeine Standort-Richtlinien auswählen, werden die Richtlinien angezeigt, die das Sicherheitssystem allgemein für den jeweiligen Standort definiert. In der folgenden Abbildung sehen Sie, wie die Informationen im rechten Fenster dargestellt werden, wenn Sie die Allgemeine Standort-Richtlinien wählen.

1. Wählen Sie die Option Allgemeine Standort-Richtlinien, um rechts im Bildschirm ein Fenster zu öffnen. In diesem Fenster werden in zwei Spalten links die Richtlinien und rechts die entsprechenden Eigenschaften angezeigt.
2. Die angezeigten Eigenschaften der Standort-Richtlinien können Sie in der rechten Spalte bearbeiten.

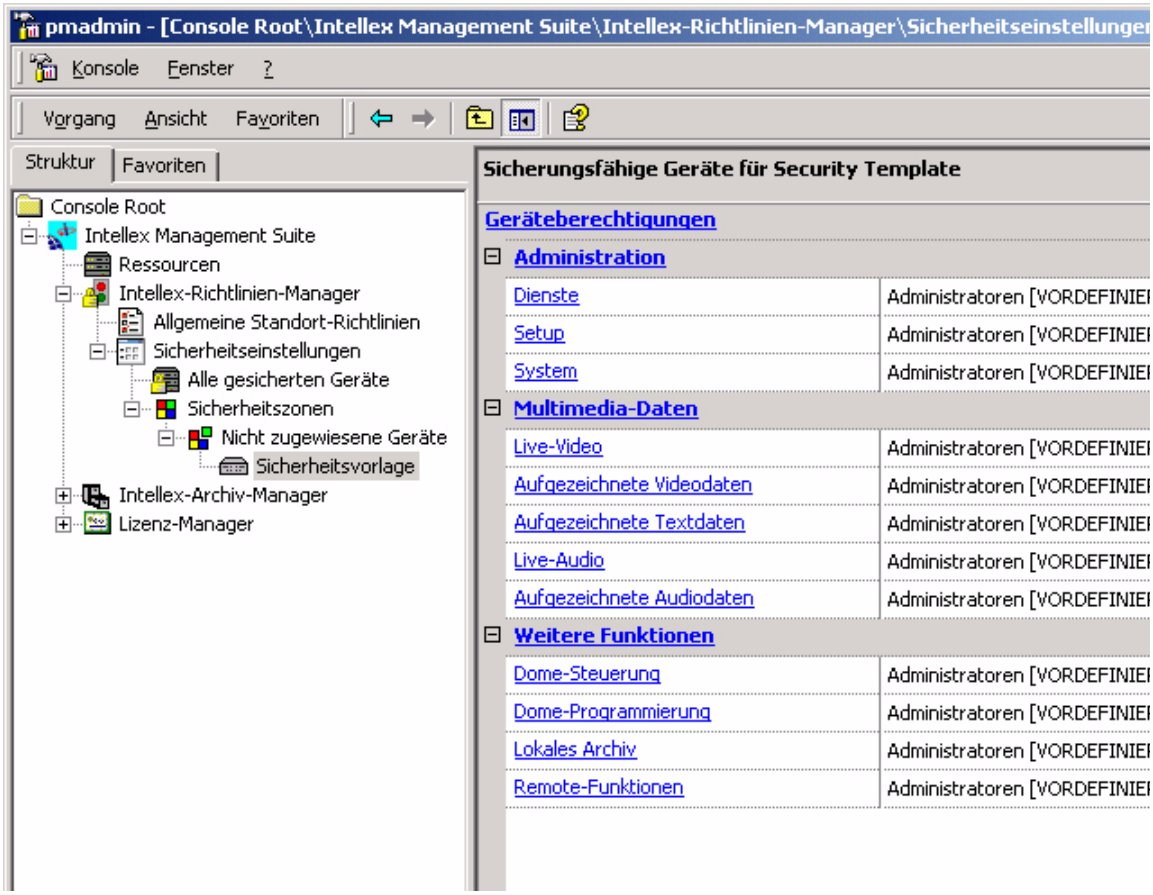


Eingabe:	Beschreibung:
Kontrollkästchen in der Spalte rechts von der Option Mehrere gleichzeitige Administrationssitzungen zulassen aktivieren.	Öffnet ein Fenster, in dem Sie die Optionen Ja und Nein auswählen können. Mit der Eingabe Ja veranlassen Sie, dass mehrere Administratoren gleichzeitig auf den betreffenden Standort zugreifen und den Standort kontrollieren können. Mit der Einstellung Nein kann nur eine Verwaltungssitzung auf den Standort zugreifen und den Standort kontrollieren. Voreinstellung ist die Einstellung Ja.
Kontrollkästchen in der Spalte rechts von der Option Maximale Anzahl Anmeldeversuche aktivieren.	Zeigt eine bestimmte Zahl aus einem verfügbaren Bereich an; definieren Sie, wie oft sich ein Benutzer nacheinander anmelden kann, bis er für eine bestimmte Zeit im System gesperrt wird. Wenn Sie den definierten Bereich überschreiten, erscheint eine entsprechende Meldung. Voreinstellung ist der Wert 3.
Kontrollkästchen in der Spalte rechts von der Option Dauer der Sperre aktivieren.	Zeigt eine Zahl in einem definierten Bereich an; definieren Sie, wie viele Minuten ein Benutzer nach der maximalen Anzahl vergeblicher Anmeldeversuche warten muss, bis er einen erneuten Anmeldeversuch unternehmen kann. Wenn Sie den definierten Bereich überschreiten, erscheint eine entsprechende Meldung. Zeiträume unter einer Minute werden nicht angenommen. Die maximale Dauer der Sperre kann beliebig definiert werden. Als Voreinstellung ist eine Dauer von 15 Minuten definiert.
Kontrollkästchen in der Spalte rechts von der Option Intervall für Geräteabfrage aktivieren.	Zeigt eine Zahl in einem definierten Bereich an; als Intervall für Geräteabfrage wird der Zeitraum in Minuten bezeichnet, der nach einer Geräteabfrage bis zur nächsten Abfrage vergeht. Die Geräte werden regelmäßig abgefragt um sicherzustellen, dass die Geräte noch aktiv und verfügbar sind. Definieren Sie, nach wie vielen Minuten jeweils eine Geräteabfrage übertragen werden soll. Wenn Sie den definierten Bereich überschreiten, erscheint eine entsprechende Meldung. Zeiträume unter einer Minute werden nicht angenommen. Das maximale Intervall kann beliebig definiert werden. Erfahrungsgemäß ist ein Abfrageintervall von fünf Minuten (Voreinstellung) ausreichend. Hinweis: Kürzere Intervalle erhöhen den Datenverkehr im Netz und können entsprechend die Reaktionszeiten beeinträchtigen.

Die erweiterten Intellex-Sicherheitsfunktionen in der Kategorie Sicherheitseinstellungen definieren

Objekte, die bei Intellex-Geräten mit erweiterten Sicherheitsfunktionen geschützt werden können

In der folgenden Abbildung sehen Sie das Modul Alle gesicherten Geräte im Policy Manager. In diesem Modul werden unabhängig von den jeweiligen Zonenzuweisungen sämtliche Geräte angezeigt, die zum betreffenden Zeitpunkt am Policy Manager-Standort registriert sind. In de Baumstruktur links im Fenster werden sämtliche Geräte dargestellt. Wenn Sie ein Gerät auswählen, wird die Sicherheitsumgebung dieses Geräts im rechten Fenster angezeigt. In Anhang 2 finden Sie eine vollständige Liste sämtlicher Objekte, die unter Intellex 3.2 mit erweiterten Sicherheitsfunktionen geschützt werden können. Das rechte Fenster enthält zwei Spalten. In der ersten Spalte sehen Sie die Eigenschaften der beim jeweiligen Intellex-Gerät geschützten Objekte. In der zweiten Spalte werden die Benutzer und Gruppen angezeigt, die den verschiedenen geschützten Objekten zugewiesen wurden. Unten im rechten Fenster werden die ausgewählten Bereiche näher beschrieben.



Beim Hochfahren teilen alle Intellex-Geräte dem Policy Manager mit, dass sie nun verfügbar sind. Wenn der Server ein Gerät nicht erkennt, wird der Aufruf dieses Geräts zurückgewiesen. In diesem Fall muss das betreffende Intellex-Gerät eine Erstregistrierung im Server vornehmen. Wenn die Registrierung erfolgreich ausgeführt wurde, fügt der Policy Manager das Intellex-Gerät zur internen Datenbank hinzu. Außerdem wird das Gerät zum Container Alle gesicherten Geräte sowie zur Zone Nicht zugewiesene Geräte hinzugefügt. Nach Abschluss des Registrierungsprozesses werden die Sicherheitseinstellungen des als Voreinstellung für den betreffenden Standort definierten Geräts für das neue Gerät übernommen. Wurde das Gerät erfolgreich im Policy Manager registriert, überträgt das System eine entsprechende Benachrichtigung an alle zum betreffenden Zeitpunkt aktiven Verwaltungskonsolen und schreibt einen Eintrag in das Ereignisprotokoll des Policy Manager.

Hinweis

Wenn die Liste der Benutzer und Gruppen nur teilweise dargestellt wird, bringen Sie den Mauszeiger auf den betreffenden Eintrag. Anschließend wird der im Hauptfenster teilweise verdeckte Inhalt in einem eigenen Fenster vollständig angezeigt.

Eingabe:	Beschreibung:
Auf der Seite mit den Eigenschaften auf eine unterstrichene Kategorie klikken.	Öffnet den Sicherheitseditor, damit um ein bestimmtes mit den erweiterten Sicherheitsfunktionen zu schützendes Objekt bearbeitet werden kann.
Auf das Pluszeichen (bzw. Minuszeichen) klicken.	Erweitert bzw. reduziert die Liste der Eigenschaften.

Menü Gerät

Wählen Sie aus dem Hauptmenü die Option Vorgang oder klicken Sie in der Baumstruktur mit der rechten Maustaste auf das gewünschte Intellex-Gerät, um das Menü Gerät zu öffnen.

	Beschreibung:
Einstellungen übertragen...	Übernimmt die Sicherheitseinstellungen eines Intellex-Geräts für eines oder mehrere sonstige Intellex-Geräte. Mit dieser Option wird das Dialogfeld Einstellungen übertragen geöffnet. In diesem Fenster können Intellex-Geräte zugewiesen werden.
Beschreibung definieren...	Ändert die Beschreibung einer vorhandenen Zone. Mit dieser Option öffnen Sie das Dialogfeld Beschreibung definieren. In diesem Dialogfeld kann die Beschreibung für eine Zone eingegeben werden.
Einer Zone zuweisen...	Fügt ein Intellex-Gerät zu einer Intellex-Gruppe hinzu. Diese Option ist nur bei „echten“ Geräten, nicht aber bei Standardgeräten verfügbar. Mit dieser Option öffnen Sie das Dialogfeld Gerät zuweisen.
Ausschneiden	Aktiviert die Funktion Einfügen; diese Funktion ist nur bei „echten“ Geräten verfügbar. Mit dieser Option deaktivieren Sie das Symbol des Geräts; das Gerät wird anschließend ausgegraut dargestellt und kann in eine andere Gerätezone eingefügt werden.
Löschen	Löscht dieses Gerät. Die Option Löschen ist nur dann verfügbar, wenn ein Gerät gerade als nicht verfügbar angezeigt wird. Mit der Funktion Löschen entfernen Sie Geräte aus der im Policy Manager verwalteten Liste registrierter Geräte.

Geräte hinzufügen

Wenn der Administrator Intellex-Geräte in einer Domäne installiert und für diese Geräte die erweiterten Sicherheitsfunktionen konfiguriert, registrieren sich diese Geräte automatisch mit den vom Administrator eingegebenen Informationen am Policy Manager-Standort. Intellex-Geräte können nicht manuell hinzugefügt werden.

Geräte löschen

Hinweis

Sie können nur inaktive Geräte löschen.

1. Öffnen Sie den Policy Manager-Admin Client. Anschließend klicken Sie mit der rechten Maustaste auf das zu löschende Gerät.
2. Klicken Sie zunächst auf Löschen und dann auf OK. Danach wird das betreffende Gerät aus dem Standort und (ggf.) aus der Zone gelöscht, der das Gerät zugewiesen wurde.

Geräte an andere Standorte binden

Unter bestimmten Umständen müssen Geräte an andere Standorte gebunden werden. Dies kann z.B. in folgenden Fällen vorkommen:

- Sie haben einen neuen Standort zur Kontrolle von Geräten eingerichtet, die einem anderen Standort zugewiesen wurden.
- Sie haben ein Gerät von einem physischen Standort entfernt und an einem anderen Standort eingerichtet und müssen dieses Gerät nun an den neuen Standort binden.

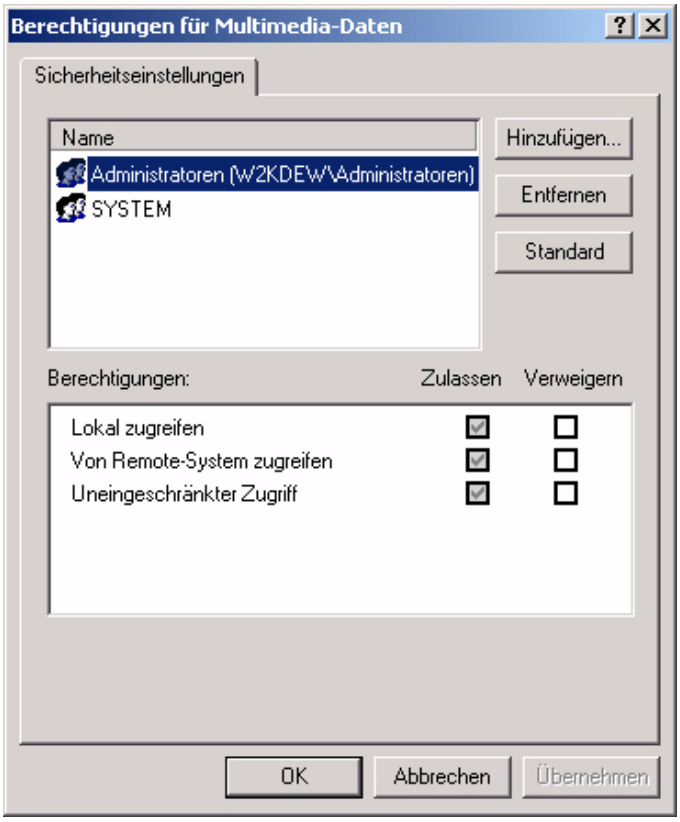
Hinweis

Sie können nur dann eine neue Bindung für ein Gerät definieren, wenn Sie die Administratorrechte für dieses Gerät besitzen.

1. Wenn die Applikation Intellex.exe auf dem Gerät ausgeführt wird, beenden Sie die Applikation und wechseln in die Desktop-Oberfläche.
2. Öffnen Sie die MMC-Komponentendienste (Systemsteuerung\Verwaltung\Komponentendienste).
3. Suchen Sie unter Komponentendienste die Applikation PolicyManagerRemoteServices, klicken Sie mit der rechten Maustaste und wählen Sie die Option Eigenschaften, um das Dialogfeld mit den Eigenschaften der Applikation anzuzeigen.
4. Öffnen Sie die Seite Aktivierung.
5. Klicken Sie auf das Feld Remote-Server und geben Sie den Servernamen des neuen Standorts ein.
6. Klicken Sie auf OK.
7. Öffnen Sie den Policy Manager-Admin Client des alten Standorts und löschen Sie das Gerät (siehe Abschnitt Geräte löschen.)
8. Starten Sie die Applikation Intellex.exe auf dem betreffenden Gerät neu, damit das Gerät sich am neuen Standort registriert. Bei der Registrierung werden die als Voreinstellung für den Standard-Standort definierten Sicherheitseinstellungen für den neuen Standort übernommen.
9. Öffnen Sie den Policy Manager administration client des neuen Standorts und nehmen Sie die nötigen Änderungen an den Einstellungen des Geräts vor. (Weisen Sie das Gerät Ihrer Zone zu, definieren Sie die gewünschte Sicherheitsumgebung usw.)

Die Sicherheitseinstellungen eines Intellex-Geräts bearbeiten

Wenn Sie die Sicherheitseinstellungen eines mit den erweiterten Sicherheitsfunktionen zu schützenden Geräts in der rechten Liste bearbeiten möchten, bringen Sie den Mauszeiger auf das betreffende Gerät. Sobald der Mauszeiger sich in einen Pfeil verwandelt, klicken Sie, um den Windows-Editor zur Eingabe der Zugriffsberechtigungen (im Folgenden auch „Zugriffseditor“ genannt) zu öffnen. Haben Sie ein Container-Objekt ausgewählt (z.B. Multmedia-Daten oder Administration) erscheint ein allgemeiner Editor (siehe folgende Abbildung). Container-Objekte erkennen Sie in der Liste am vorangestellten Kästchen.



In diesem Fenster können Sie folgende Berechtigungen definieren:

Lokal zugreifen	Sie erteilen einem Benutzer oder einer Gruppe die Berechtigung für Zugriffe auf ein Gerät ausschließlich auf Ebene des betreffenden Geräts (d.h. auf „lokaler“ Ebene). Remote-Zugriffe über die API oder über den Network Client sind also ausdrücklich ausgeschlossen. Beachten Sie in diesem Zusammenhang bitte auch die Hinweise im Abschnitt zu Sicherheitskonzepten für den Policy Manager.
Von Remote-System zugreifen	Sie erteilen dem Benutzer oder der Gruppe die Berechtigung für Zugriffe ausschließlich über Remote-Applikationen (beliebige Fremd-Software, die über die API oder über den Network Client auf Ihr Gerät zugreift).
Uneingeschränkter Zugriff	Sie erteilen dem Benutzer oder der Gruppe die Berechtigung für Zugriffe auf das Gerät sowohl von Remote-Systemen als auch vom lokalen System aus. Außerdem werden mit der Option Uneingeschränkter Zugriff automatisch sämtliche spezifischen Berechtigungen für alle Funktionen oder Funktionsgruppen im betreffenden Container sowie für sämtliche diesem Container unmittelbar untergeordneten Container und Objekte definiert.

Durch Hinzufügen von Benutzern und Gruppen zu einem Container können Administratoren rasch eine einheitliche Sicherheitsumgebung für ein Gerät einrichten. Auf Container-Ebene hinzugefügte Benutzer und Gruppen erben nämlich automatisch sämtliche in diesem Container definierten Funktionen. Wenn Sie z.B. den Benutzer JSchmitt zum Container Multimedia Data hinzufügen und für diesen Benutzer die Einstellung Uneingeschränkter Zugriff aktivieren, kann JSchmitt unabhängig davon, ob er sich direkt am Gerät befindet (lokaler Zugriff) oder über den Network Client oder die API von einem Remote-System zugreift, alle vorhandenen Informationen anzeigen.

Wird ein Benutzer oder eine Benutzergruppe zu einem Container hinzugefügt und an Kindobjekte dieses Containers „vererbt“, werden für die Kindobjekte Berechtigungen wie folgt definiert:

- Wenn Sie die Option Uneingeschränkter Zugriff nicht definiert haben, werden spezifische Berechtigungen erteilt. Welche Berechtigungen erteilt werden können, hängt vom jeweiligen Objekt ab. Die Tabelle im Abschnitt Menüs und Optionen, für die erweiterte Sicherheitseinstellungen aktiviert werden können bietet einen Überblick über die aktuellen Voreinstellungen für die verschiedenen sicherheitsrelevanten Objekte.
- Haben Sie die Einstellung Uneingeschränkter Zugriff gewählt, werden den Kindobjekten sämtliche spezifischen Berechtigungen erteilt.
- Wenn Sie eine bestimmte Funktion ausgewählt haben (z.B. Live-Video) erscheint ein Editor mit den für die jeweilige Funktion verfügbaren Einstellungen. Alle zu dieser Funktion hinzugefügten Benutzer und Gruppen sind nur in Verbindung mit dieser Funktion gültig.

Der wesentliche Vorteil beim Übernehmen von Einstellungen für Container (statt für bestimmte Funktionen) besteht darin, dass mit einem einzigen Eintrag Zugriffsberechtigungen für eine ganze Liste mit Objekten oder für ein gesamtes Intellex-Gerät definiert werden können.

Benutzer und Gruppen hinzufügen und entfernen

Sobald der Zugriffseditor geöffnet wurde, können Sie mit der Vergabe und mit dem Entzug von Berechtigungen für einzelne Benutzer und für Benutzergruppen beginnen. Diese Benutzer und Gruppen sind identisch mit den Benutzern und Gruppen, die für Ihr Unternehmensnetz definiert wurden.

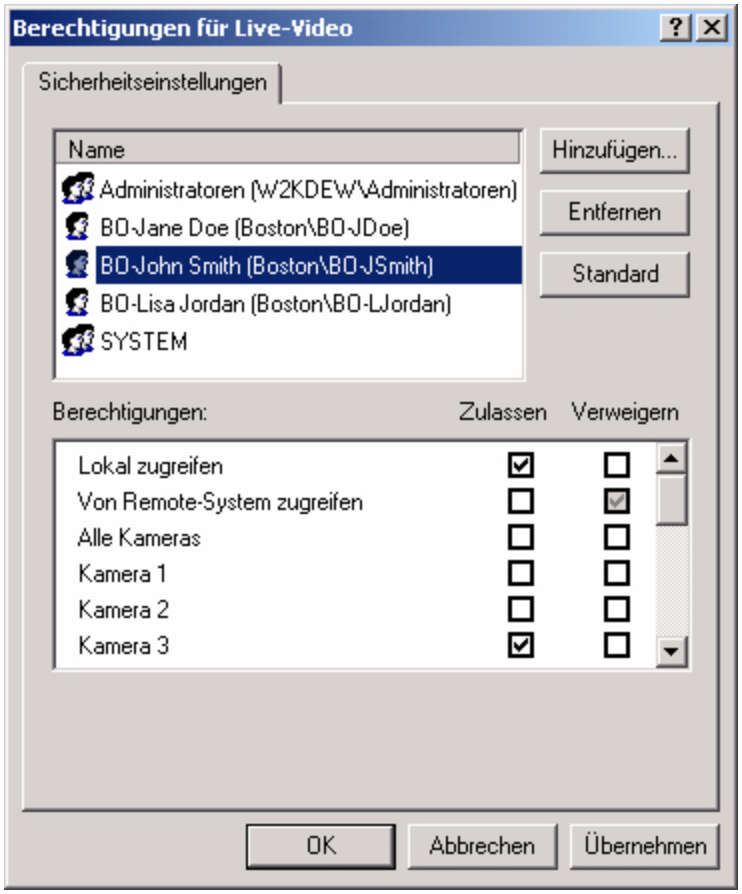
1 Wenn Sie einen Benutzer oder eine Benutzergruppe hinzufügen möchten, klicken Sie auf die Schaltfläche Hinzufügen..., um das Dialogfeld Benutzer und Gruppen auswählen zu öffnen.

Über die Dropdown-Liste hinter der Beschriftung Suchen in: können Sie auch sonstige in Ihrem Unternehmen verwendete Domänen öffnen. Anschließend können Sie einen hinzuzufügenden Benutzer oder eine hinzufügende Benutzergruppe auswählen.

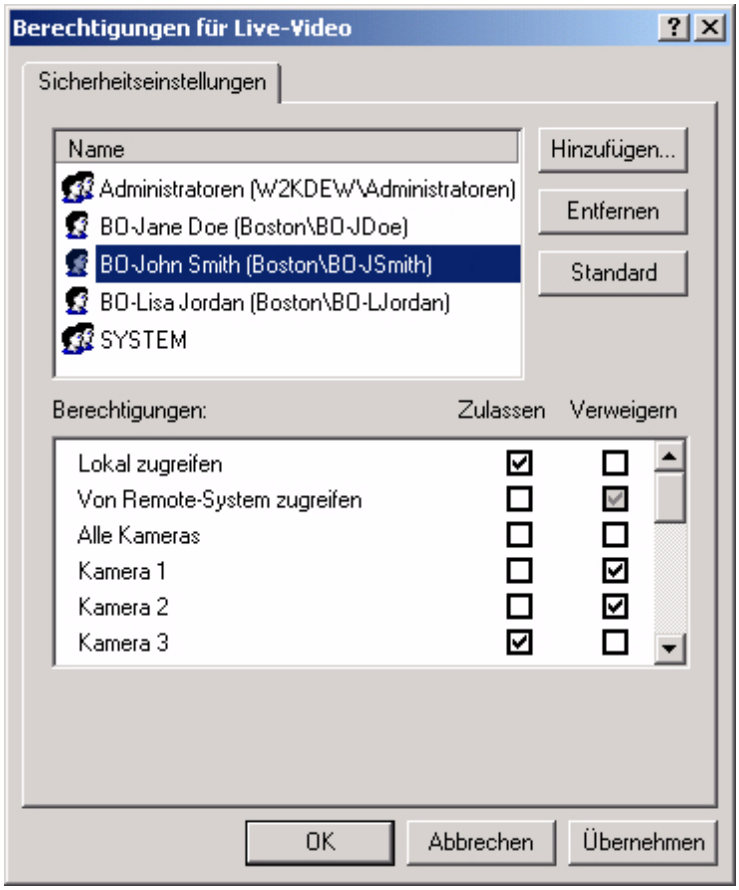
2 Wählen Sie den gewünschten Benutzer oder die gewünschte Gruppe aus. Klicken Sie zunächst auf Hinzufügen und dann auf OK.

Im folgenden Beispiel haben Sie z.B. zwei Möglichkeiten, den Zugriff auf Kamera 1 und 2 zu verweigern:

3 Sie können in der Spalte Aktivieren die Kontrollkästchen hinter Kamera 1 und Kamera 2 deaktivieren (siehe Abbildung), um zu definieren, dass Sie der Gruppe keine EXPLIZITE Berechtigung für Zugriffe auf diese Kameras erteilt haben.



4 Sie können aber auch in der Spalte Verweigern die Kontrollkästchen hinter Kamera 1 und Kamera 2 aktivieren, um den Zugriff auf diese Kameras ausdrücklich zu verwehren (siehe Abbildung).



Hinweis

Allein durch Deaktivieren der Kontrollkästchen in der Spalte Zulassen werden einzelne Benutzer oder Benutzergruppen unter Umständen jedoch nicht wirklich daran gehindert, Live-Videos dieser Kameras anzuzeigen. Einzelne Benutzer (oder Benutzergruppen) können nämlich die Berechtigung zum Anzeigen von Videomaterial von diesen Kameras über eine sonstige Gruppe geerbt haben. Wenn wirklich sichergestellt werden soll, dass einzelne Benutzer oder Benutzergruppen keinen Zugriff auf eine Funktion (keine Berechtigung für diese Funktion) besitzen, müssen Sie das Kontrollkästchen in der Spalte Verweigern aktivieren.

Beim Entfernen zuvor hinzugefügter Benutzer oder Benutzergruppen sind folgende Punkte zu beachten:

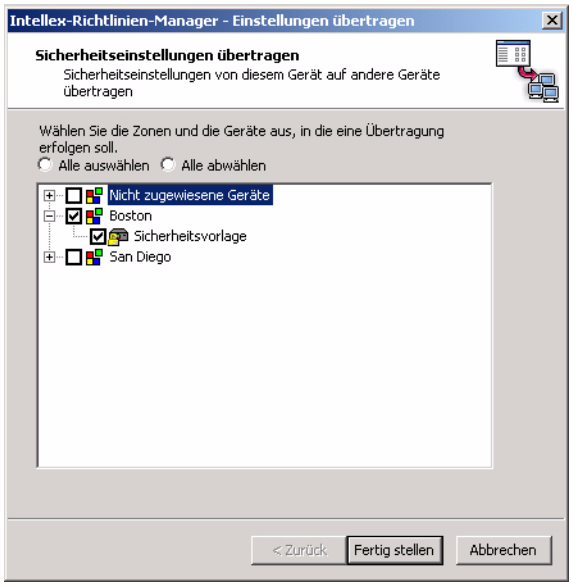
- Wenn der hinzugefügte Benutzer oder die hinzugefügte Benutzergruppe als „geerbt“ angezeigt wird (und der betreffende Benutzer bzw. die betreffende Gruppe entsprechend eine Ebene über dem aktuellen Objekt hinzugefügt wurde), kann der Löschbefehl nicht ausgeführt werden.
- Wird der hinzugefügte Benutzer oder die hinzugefügte Gruppe nicht als „geerbt“ angezeigt, können Sie den Benutzer oder die Gruppe löschen.

Hinweis

Wenn Sie einen geerbten Benutzer oder eine geerbte Benutzergruppe entfernen, wird dieser Benutzer bzw. diese Gruppe nicht nur aus dem aktuellen Objekt, sondern auch aus allen unmittelbar untergeordneten Kindobjekten entfernt. Haben Sie z.B. den Benutzer JSchmitt zum Container Multimedia Data hinzugefügt und anschließend entfernt, wird dieser Benutzer auch aus den Containern Live-Video, Aufgezeichnete Videodaten usw. bis hin zum letzten Kindobjekt Aufgezeichnete Audiodaten entfernt.

Sicherheitseinstellungen von einem Intellex-Gerät auf ein anderes übertragen (kopieren)

In dieser Abbildung sehen Sie das Dialogfeld Sicherheitseinstellungen übertragen. Über dieses Dialogfeld können Sie Geräteeinstellungen von einem Gerät auf eines oder mehrere sonstige Geräte kopieren.



In der Baumstruktur eines Verzeichnisses sehen Sie eine Liste mit Zonen und Mitgliedgeräten. An dem jeweils vorangestellten Kontrollkästchen erkennen Sie, ob für ein Objekt die neuen Einstellungen übernommen werden. Das Kontrollkästchen gegenüber dem Namen der jeweiligen Zone gibt Aufschluss über den aktuellen Zustand der Zone. Den Zustand einer Zone ermitteln (oder berechnen) Sie unter Berücksichtigung der folgenden Regeln:

1. Wenn keine Geräte aktiviert sind, ist für die Zone der Zustand Ohne definiert, und im Kontrollkästchen wird kein Häkchen angezeigt. ☐
2. Sind zwar nicht alle, aber zumindest einige Zonenmitglieder aktiviert, befindet sich die Zone im Zustand Teilweise, und das aktivierte Kontrollkästchen ist grau hinterlegt. ☑
3. Werden die Kontrollkästchen sämtlicher Zonenmitglieder aktiviert, befindet sich die Zone im Zustand Alle, und der Haken im Kontrollkästchen wird vor einem weißen Hintergrund angezeigt. ☑

Eingabe:	Beschreibung:
Auf das Pluszeichen (bzw. Minuszeichen) klicken.	Erweitert/reduziert die Gerätezone.
Auf das Kontrollkästchen einer Zone klicken.	Wenn das Kontrollkästchen aktiviert oder teilweise aktiviert (grau hinterlegt) dargestellt wird, werden sämtliche Mitglieder der Zone sowie die eigentliche Zone deaktiviert. Wird das Kontrollkästchen deaktiviert, werden sämtliche Mitglieder der Zone sowie die eigentliche Zone aktiviert.
Auf das Kontrollkästchen eines Geräts klicken.	Ist das Kontrollkästchen aktiviert, wird das Gerät deaktiviert und der Zustand der Zone neu berechnet (siehe oben). Ist das Kontrollkästchen deaktiviert, wird das Gerät aktiviert und der Zustand der Zone neu berechnet (siehe oben).
Auf Schaltfläche Fertig stellen klicken.	Bestätigt die vorgenommenen Änderungen.
Auf die Schaltfläche Abbrechen klicken.	Verwirft die vorgenommenen Änderungen.
Auf die Schaltfläche Hilfe klicken.	Öffnet die kontextsensitive Hilfe mit einer Anleitung zum Ändern von Beschreibungen.

Mit Zonen arbeiten

Das zweite Element des Policy Managers sind die Sicherheitszonen. Mit Sicherheitszonen können Administratoren Geräte als sicherheitstechnisch eigenständige Einheiten verwalten. Die Zonen enthalten jeweils ein Standardgerät mit den Sicherheitseinstellungen, die für alle als Mitglied der jeweiligen Zone definierten Geräte zu übernehmen sind.

Durch die Einrichtung von Zonen und die Zuweisung von Geräten zu diesen Zonen schaffen Administratoren eine Sicherheitstopologie für das jeweilige Unternehmen bzw. für den betreffenden Standort, die der Policy Manager anschließend automatisch überträgt.

In einem Fenster rechts im Bildschirm werden je nach gewählter MMC-Ansicht Inhalte in unterschiedlicher Form dargestellt: mit großen Symbolen, mit kleinen Symbolen, als Liste oder in einer Detailansicht. In der Detailansicht werden der jeweilige Gruppenname und eine Beschreibung angezeigt.

Eingabe:	Beschreibung:
In der Baumstruktur auf das Pluszeichen oder das Minuszeichen klicken.	Erweitert bzw. reduziert die Baumstruktur.
Im rechten Fenster auf das Symbol einer Zone doppelklicken.	Die ausgewählte Zone wird in der Baumstruktur dargestellt. Im rechten Fenster werden alle der Zone zugewiesenen Geräte angezeigt.
Klicken Sie in der Baumstruktur auf die gewünschte Zone.	Im rechten Fenster werden alle der Zone zugewiesenen Geräte angezeigt.

Menü Sicherheitszonen

Wählen Sie im Hauptmenü die Option Vorgang oder klicken Sie im Menü Sicherheitszonen mit der rechten Maustaste auf eine Sicherheitszone.

Im anschließend angezeigten Menü werden Optionen aus dem MMC-Standardmenü sowie spezifische Optionen des Containers Sicherheitszonen angezeigt.

Die Zone Nicht zugewiesene Geräte

Die Zone Nicht zugewiesene Geräte ist per Voreinstellung als Standardzone definiert und kann nicht gelöscht werden. Das Gerät in dieser Zone wird als Standardgerät des betreffenden Standorts behandelt. Dieses Gerät kann als Vorlage mit den gewünschten Sicherheitseinstellungen für alle Geräte am betreffenden Standort angenommen werden. Alle neu registrierten Geräte werden zunächst dieser Zone zugewiesen und erben diese als Voreinstellung definierten Sicherheitseinstellungen.

Neue Zonen erzeugen (Geräte mit gemeinsamen Sicherheitseinstellungen zusammenfassen)

1. Öffnen Sie im Admin Client im linken Fenster den Knoten Sicherheitszonen, klicken Sie mit der rechten Maustaste und wählen Sie die Option Neue Zone, um den Zonen-Assistenten zu öffnen.
2. Geben Sie die geforderten Informationen ein und klicken Sie auf Fertigstellen. Anschließend wird die neue Zone in der Liste der verfügbaren Sicherheitszone angezeigt.

   Sie können nun Geräte zuweisen und die Voreinstellungen des für die betreffende Zone definierten Standardgeräts ändern. Wenn Sie eine neue Zone erzeugen, veranlassen Sie, dass der Server eine entsprechende Ereignisbenachrichtigung an alle jeweils aktiven Clients überträgt.

Hinweis

In neue Zonen wird automatisch ein Standardgerät eingefügt; dieses Standardgerät besteht aus einer Kopie des aktuellen Standardgeräts im jeweiligen Bereich. Wenn Sie die für das Standardgerät der Zone definierten Einstellungen ändern und die neuen Einstellungen dann auf die übrigen Mitglieder der Zone übertragen, kann der Administrator eine einheitliche Sicherheitsumgebung unter gleichzeitiger Einbeziehung unterschiedlicher Einzelsysteme erzeugen.

Zonen löschen

Nachdem Sie eine Zone gelöscht haben, werden alle dieser Zone zugewiesenen Geräte wieder der Zone Nicht zugewiesene Geräte zugeordnet. Von dort aus können die Geräte jederzeit wieder einer bestimmten Zone zugewiesen werden. Mit Ausnahme des Standardgeräts für die betreffende Zone (das dann nicht mehr benötigt wird) werden keine Geräte gelöscht.

1. Öffnen Sie im Admin Client im linken Fenster die zu löschende Security Zone. Klicken Sie mit der rechten Maustaste und wählen Sie die Option Löschen.

   Wenn die Zone Geräte enthält, fragt die Applikation, ob die für das Standardgerät des jeweiligen Standorts definierten Sicherheitseinstellungen beim Verschieben des Standardgeräts in die Zone Nicht zugewiesene Geräte auf alle Geräte übertragen werden sollen.

2. Klicken Sie auf Ja, wenn die Einstellungen vererbt werden sollen oder klicken Sie auf Nein, um die Einstellungen beizubehalten. Damit ist der Vorgang abgeschlossen. Klicken Sie auf Abbrechen, wenn der Löschbefehl nicht ausgeführt werden soll.

Die Zonen-Einzelansicht

In der Zonen-Einzelansicht werden alle Geräte angezeigt, die als Mitglieder zur jeweiligen Zone hinzugefügt wurden. Außerdem enthalten die Zonen jeweils das oben beschriebene Standardgerät. Sie können die für dieses Standardgerät definierten Sicherheitseinstellungen auf die gewünschten Geräte in der betreffenden Zone übertragen.

Die Zonenansicht ist ähnlich aufgebaut wie die Darstellung des Knotens Alle gesicherten Geräte. In einem Fenster rechts im Bildschirm werden je nach gewählter MMC-Ansicht Inhalte in unterschiedlicher Form dargestellt: mit großen Symbolen, mit kleinen Symbolen, als Liste oder in einer Details (Detailansicht). In der Details werden der Gerätename, eine Beschreibung und die Software-Version des Geräts angezeigt.

Eingabe:	Beschreibung:
In der Baumstruktur auf das Pluszeichen oder das Minuszeichen klicken.	Erweitert bzw. reduziert die Baumstruktur.
Im rechten Fenster auf das Symbol einer Zone doppelklicken.	Im rechten Fenster werden die der Zone zugewiesenen Geräte angezeigt.
Ein Gerät in der betreffenden Zone auswählen.	Im rechten Fenster werden die für dieses Gerät definierten Sicherheitseinstellungen angezeigt.

Das Menü Zone

1 Wählen Sie im Hauptmenü die Option Vorgang, oder klicken Sie in der Baumstruktur mit der rechten Maustaste auf eine bestimmte Zone, um das Menü Zone zu öffnen.

Dieses Menü enthält Standardoptionen des MMC-Menüs sowie einige spezifische Optionen für die jeweilige Gerätegruppe. Gerätespezifisch sind die folgenden Optionen:

- Beschreibung definieren
- Einfügen
- Löschen
- Umbenennen

Hinweis

Die Option Einfügen ist nur dann verfügbar, wenn zuvor ein Gerät oder eine Zone ausgeschnitten wurde.

Eingabe:	Beschreibung:
Beschreibung definieren… klicken.	Öffnet das Dialogfeld Beschreibung definieren...
Auf Einfügen klicken.	Diese Funktion ist nur dann verfügbar, wenn zuvor ein Gerät ausgeschnitten wurde. Beim Einfügen wird ein Gerät aus der Ausgangszone in die Zielzone verschoben. Die Option Einfügen kann nur dann verwendet werden, wenn das einzufügende Gerät aus einer anderen Zone stammt. Vor dem Einfügen fragt das System, ob die Standard-Sicherheitseinstellungen der Zielzone auf das neue Mitglied der Zone übertragen werden sollen. Wenn erforderlich, kann der gesamte Vorgang abgebrochen werden.
Auf Löschen klicken.	Löscht die betreffende Gerätezone. Sämtliche Geräte werden aus der Zone entfernt und in den Container Nicht zugewiesene Geräte eingefügt. Vor dem Löschen fragt das System, ob die (im Standardgerät des betreffenden Standorts enthaltenen) Standard-Sicherheitseinstellungen des Standorts auf alle zu verschiebenden Geräte übertragen werden sollen. Wenn die Abfrage mit Nein beantwortet wird, behält das System die individuellen Sicherheitseinstellungen der einzelnen Geräte bei. Wenn erforderlich, kann der gesamte Vorgang abgebrochen werden.
Auf Umbenennen klicken.	Überschreibt den für die jeweilige Zone definierten Namen.
Auf Liste exportieren… klicken.	Speichert die vorhandenen Informationen in eine Datei.

Im Dialogfeld Set Description können Sie die für eine Zone definierte Beschreibung ändern. Die Beschreibung kann beliebig lang sein. Sie dürfen allerdings nur alphanumerische Zeichen verwenden. Die eingegebene Beschreibung können Sie in einem Bearbeitungsfenster ändern.

Intellex-Geräte in eine Sicherheitsone verschieben

Im Dialogfeld Gerät zuweisen können Sie Geräte einer Zone zuweisen.

In einer Liste werden die Zonen angezeigt, in die Ihre Geräte verschoben werden können. Die Zone, in der sich die Geräte zum betreffenden Zeitpunkt jeweils befinden, wird in der Liste nicht dargestellt.

Eingabe:	Beschreibung:
Eine Zone aus der Liste auswählen.	Definiert die Zone als Zielzone für das betreffende Gerät. Sie können immer nur eine einzige Zone auswählen.
Das Kontrollkästchen Voreinstellungen von Zielzone erben aktivieren.	Durch die Aktivierung des Kontrollkästchens wird veranlasst, dass das neue Mitglied (das in die Zone zu verschiebende Gerät) die als Voreinstellung definierten Sicherheitseinstellungen des Standardgeräts der betreffenden Zone erbt. Bleibt das Kontrollkästchen deaktiviert, wird das Gerät in die Zone verschoben, die Standard-Sicherheitseinstellungen der Zone werden beim Verschieben aber nicht auf das Gerät übertragen.
Auf Fertigstellen klicken.	Bestätigt die vorgenommenen Änderungen.
Auf Abbrechen klicken.	Verwirft die vorgenommenen Änderungen.
Auf Hilfe klicken.	Öffnet die kontextsensitive Hilfe mit einer Anleitung zum Ändern von Beschreibungen.

Sie können Geräte auch durch Ziehen und Ablegen aus einer Zone in eine andere Zone verschieben. Wenn Sie Geräte durch Ziehen und Ablegen verschieben möchten, fragt das System, ob die Voreinstellungen der Zone für das neue Gerät übernommen werden sollen.

Eingabe:	Beschreibung:
Auf Ja klicken.	Bewirkt, dass der Befehl zum Verschieben ausgeführt wird und die Voreinstellungen für das neue Mitglied übernommen werden.
Auf Nein klicken.	Bewirkt, dass der Befehl zum Verschieben ausgeführt wird, ohne die Voreinstellungen für das neue Mitglied zu übernehmen.
Auf Abbrechen klicken.	Bricht das Verschieben ab; das Gerät bleibt weiterhin Mitglied der Zone, der es zum betreffenden Zeitpunkt angehört.

Intellex-Geräte ersetzen

Unter verschiedenen Umständen müssen Sie ein bereits an Ihrem Standort registriertes Gerät ersetzen. Folgende Umstände kommen beispielsweise in Betracht:

- Sie haben das Gerät an einen anderen Standort verschoben und einen neueren Ersatz für den ursprünglichen Standort erworben.
- Sie mussten das Gerät wegen eines Hardware-Fehlers ersetzen.

Wenn Sie das neue Gerät installieren möchten, müssen Sie für dieses Gerät die Identität des zu ersetzenden Geräts definieren. Nehmen wir z.B. an, Sie haben das neue Gerät unter dem Namen des vorher eingesetzten Geräts in der Domäne angemeldet.

1. In diesem Fall müssen Sie die Policy Manager-Treiber wie gewohnt auf dem neuen Gerät installieren.
2. Starten Sie das Gerät, damit sich das Gerät im Policy Manager registriert.
3. Der Gerätename ist identisch. Die Erst- und die Zweitkennung (die MAC-Adresse und die vom Gerät erzeugte individuelle Kennung) sind jedoch verschieden. Der Policy Manager betrachtet das Gerät daher als neues Gerät, erfasst die betreffenden Informationen und benachrichtigt alle zum betreffenden Zeitpunkt aktiven Admin Clients über die gerade erfolgte Registrierung eines neuen Geräts.

4 Starten Sie den Admin Client und öffnen Sie den Bereich Alle gesicherten Geräte.

5 Dort werden zwei Einträge mit identischem Namen angezeigt. Einer bezieht sich auf das aktive (gerade installierte neue) Gerät; der andere enthält die Informationen des inaktiven (zu ersetzenden) Geräts.

6 Übertragen Sie die Sicherheitseinstellungen des alten (inaktiven) Geräts auf das neue Gerät.

7 Wenn das alte Gerät einer Zone zugewiesen war, verschieben Sie das neue Gerät in diese Zone.

Hinweis

Vergewissern Sie sich, dass die Standard-Sicherheitseinstellungen der Zone nicht auf das neue Gerät übertragen werden. (Sie haben bereits die zu verwendenden Einstellungen des alten Geräts kopiert.)

8 Löschen Sie das alte Gerät.

Eingabe:	Beschreibung:
Eingaben im Bearbeitungsfenster vornehmen.	Ändert die Beschreibung.
Auf OK klicken.	Bestätigt die vorgenommenen Änderungen.
Auf Abbrechen klicken.	Verwirft die vorgenommenen Änderungen.
Auf Hilfe klicken.	Öffnet die kontextsensitive Hilfe mit einer Anleitung zum Ändern von Beschreibungen.
Eingaben im Bearbeitungsfenster vornehmen.	Ändert die Beschreibung.

Sie können den Namen der Gruppe und die gewünschte Beschreibung in die beiden Bearbeitungsfenster eingeben.

Eingabe:	Beschreibung:
Eingaben im Fenster mit dem Gruppennamen vornehmen.	Ändert den definierten Gruppennamen.
Eingaben im Fenster zur Bearbeitung der Beschreibung vornehmen.	Ändert die Beschreibung.
Auf die Schaltfläche OK klicken.	Bestätigt die vorgenommenen Änderungen.
Auf die Schaltfläche Abbrechen klicken.	Verwirft die vorgenommenen Änderungen.
Auf die Schaltfläche Hilfe klicken.	Öffnet die kontextsensitive Hilfe mit einer Anleitung zum Ändern von Beschreibungen.

Mit dem Lizenz-Manager arbeiten

Das dritte im Policy Manager für Intellex enthaltene Modul ist der Lizenz-Manager. Unter dem Knoten Lizenz-Manager werden einer oder zwei Unterknoten angezeigt. Wenn Sie nur den Policy Manager installiert haben, ist der Unterknoten Policy Manager verfügbar. Wurde auch der Archive Manager installiert, erscheint außerdem der Unterknoten Archive Manager.

Der im Lieferumfang Ihres Produkts enthaltene USB-Kopierschutzstecker mit Seriennummer wird zur Ausführung des Policy Managers benötigt. Die Seriennummer des Kopierschutzsteckers ist mit einer Produkt-ID (PID) verknüpft. Wenn Sie das Produkt erhalten haben, installieren Sie zunächst die Software. Anschließend stecken Sie den Kopierschutzstecker auf den USB-Port Ihres Server-Rechners. Nach Abschluss der Installation muss der jeweilige Endbenutzer den Admin Client starten, den License Manager öffnen und die PID des Policy Managers aktualisieren, damit mit der Sicherung der in der erworbenen Lizenz genannten Anzahl an Intellex-Geräten im Netz begonnen werden kann.

Diese im Verwaltungsmodul des Lizenz-Manager einzugebende PID legt fest, für wie viele Intellex-Geräte gleichzeitig die erweiterten Sicherheitsfunktionen aktiviert werden können. Nachdem der Administrator die PID eingegeben hat, entnimmt der Policy Manager (Policy Manager) einem in die PID integrierten Wert die Anzahl der lizensierten Geräte, für die die erweiterten Sicherheitsfunktionen aktiviert werden können.

Außerdem beinhaltet die PID Informationen zur Unternehmenslizenz für den Network Client (wenn Sie diese Applikation erworben haben). Aufgrund einer Unternehmenslizenz können Sie eine Kopie des Network Client an beliebig viele Benutzer (Arbeitsplätze) in Ihrem Unternehmen weitergeben.

Hinweis

Der Policy Manager kann auch ohne Kopierschutzstecker gestartet werden. Installieren Sie den Policy Manager ohne den Kopierschutzstecker. Anschließend stecken Sie den Kopierschutzstekker auf. Dies können Sie vor dem Hochfahren des Policy Manager-Servers tun; Sie können den Kopierschutzstecker aber auch aufstecken, nachdem der Policy Manager-Server bereits hochgefahren wurde.

- Der Policy Manager-Admin Client kann ohne Kopierschutzstecker ausgeführt werden, und die gewünschten Berechtigungen für alle Benutzer können auch ohne Kopierschutzstecker definiert werden.
- Wenn ein Intellex-Gerät mit einem Policy Manager verbunden werden soll, muss allerdings der für den Policy Manager vorgesehene Kopierschutzstecker vorhanden sein. Wird der mit der CD-ROM ausgelieferte Kopierschutzstecker verwendet, kann ein Intellex-Gerät verbunden werden. Eine Lizenz für den Network Client ist dagegen nicht im Lieferumfang enthalten.
- Wenn mehrere Intellex-Geräte gleichzeitig mit dem Policy Manager verbunden werden sollen, müssen die betreffenden Benutzer eine PID bei American Dynamics anfordern.
- Im Intellex-System werden gleichzeitig verbundene Geräte nach dem FIFO-Prinzip („Bearbeitung in der Reihenfolge der übermittelten Aufforderungen“) versorgt.
- Wenn sämtliche Geräte im Netz eines Standorts über den Network Client verbunden werden sollen, muss bei American Dynamics eine PID angefordert werden.
- Die Kunden können eine PID beantragen, in der die zulässige Anzahl gleichzeitig zu verbindender Intellex-Geräte und die erworbenen NC-Standardlizenzen definiert sind.
- Lizenzen für den gleichzeitigen Einsatz mehrerer Intellex-Geräte sind als Lizenzen für 10 und für 25 Geräte sowie für beliebig viele Geräte (jeweils wahlweise mit Network Client-Standortlizenz) verfügbar. Der definierte Wert bezieht sich auf die Gesamtzahl; die zusätzliche Lizenz, die ergänzend zur kostenlosen Lizenz gewährt wird, ist nicht eingerechnet. Wenn Sie bereits eine PID besitzen, schicken Sie die Lizenz am besten an American Dynamics zurück und beantragen ein kostenpflichtiges Update auf die benötigte Anzahl an Lizenzen.

Die Network Client-Unternehmenslizenz

Aus der PID, die Sie mit Ihrer Policy Manager-Software erhalten haben, geht hervor, ob Sie eine Network Client- Unternehmenslizenz erworben haben.

Die PID ist auf einem Aufkleber auf der CD-Hülle abgedruckt und enthält folgende Angaben:

- Den Produkttyp (Policy Manager)
- Die Versionsnummer
- Die (individuelle) Seriennummer (Die Seriennummer ist unmittelbar an die im Kopierschutz-stecker gespeicherte Seriennummer geknüpft; eine Beziehung zur Seriennummer des Servers, auf dem der Policy Manager ausgeführt wird, besteht nicht)
- Die zu installierenden Komponenten (acht einzeln zu aktivierende Module) und
- Die Prüfsumme

Mit einer Unternehmenslizenz können Unternehmenskunden:

- Eine Kopie des Network Client erwerben
- Diese Kopie auf beliebig vielen Knotenrechnern installieren
- Für sämtliche Installationen dieselbe PID (NCCPID) verwenden und
- Automatisch eine zweite PID-Prüfung auf deaktivierten Intellex-Geräten ausführen lassen

So bestellen Sie ein Lizenz-Upgrade:

1. Öffnen Sie den License Manager.
2. Klicken Sie auf Upgrade.
3. Geben Sie die PID ein, um den Kopierschutzstecker so zu aktualisieren, dass die Network Client-Unternehmenslizenz freigeschaltet wird.

Mit der Ereignisanzeige arbeiten

Der Policy Manager erstellt ein eigenes Ereignisprotokoll; dieses Ereignisprotokoll kann der Administrator jederzeit mit der Ereignisanzeige öffnen (auf Betriebssystemebene). Die Ereignisse werden wie folgt protokolliert:

Applikation	Applikationsspezifische Fehlereinträge
Policy Manager	Fehlereinträge im benutzerdefiniertem Protokoll
Sicherheit	Einträge zu Sicherheitsprüfungen
System	Einträge zu Systemfehlern

Der Policy Manager fügt Einträge zum Policy Manager-Protokoll in den folgenden vier Kategorien hinzu:

Information

Routineverarbeitung des jeweiligen Schritts; ergänzend werden sonstige für Administratoren hilfreiche Informationen erfasst (z.B. dass auf dem Server eine neue Administrationssitzung gestartet wurde).

Warnung

Hinweis darauf, dass der veranlasste Schritt oder die vorgenommene Eingabe einen Fehler zur Folge haben könnte; Administratoren werden auf Fehler aufmerksam gemacht, deren Ursache sie selbst abstellen müssen. Wenn die betreffende Standortlizenz abgelaufen ist oder der Kopierschutzstecker mitteilt, dass die maximale Anzahl vorgesehener Lizenzen erreicht ist, wird ein Warnereignis protokolliert.

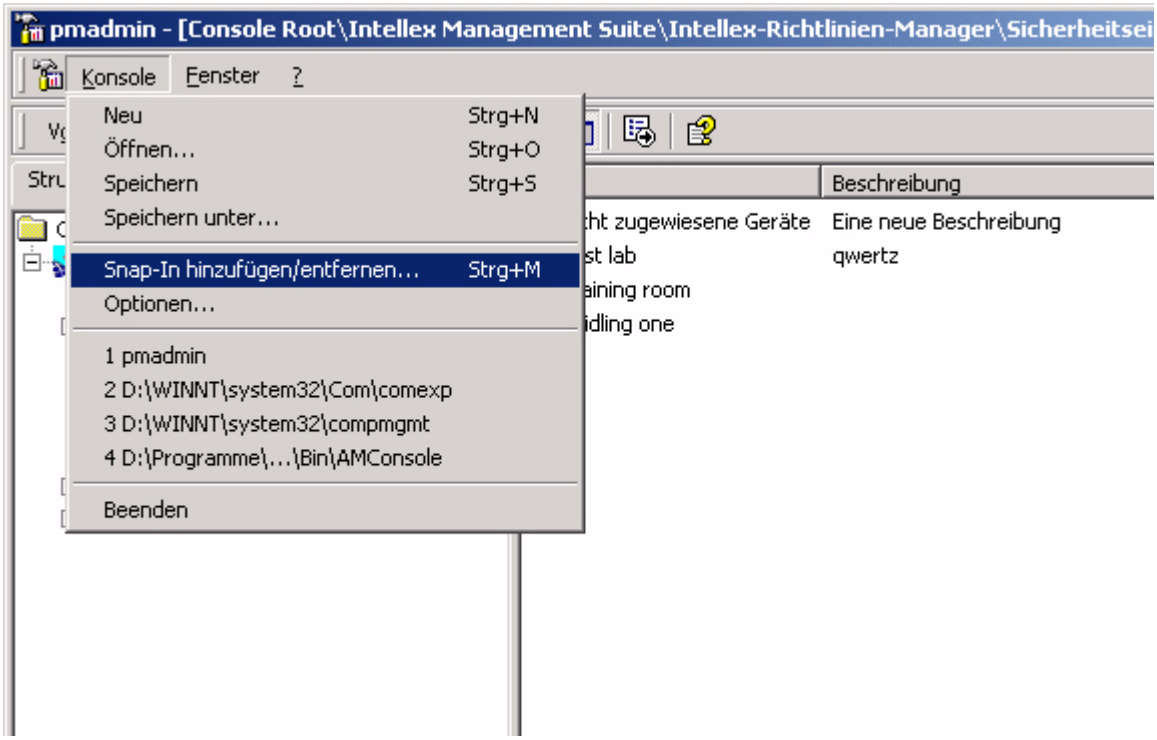
Fehler

Hinweis darauf, dass der ausgeführte Schritt oder die Dateneingabe zu einem kritischen (fatalen) Fehler geführt hat; Hinweis auf einen ungewöhnlichen Zustand im Server-Betrieb (z.B. dass ein registriertes Gerät plötzlich nicht mehr verfügbar ist).

Fehlerprüfung

Hinweis darauf, dass ein unbekannter Benutzer versucht hat, in das System einzudringen; dieses Ereignis wird außerdem erkannt, wenn ein registrierter Benutzer versucht, eine Funktion zu verwenden, ohne die entsprechende Berechtigung zu besitzen.

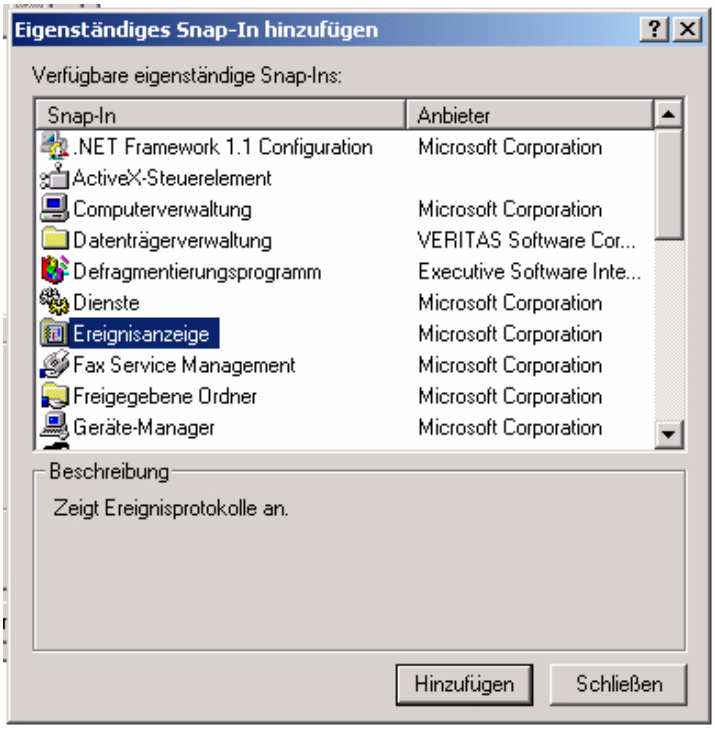
Das Snap-in Ereignisanzeige hinzufügen



So fügen Sie das Snap-in Ereignisanzeige zur während der Installation eingerichteten MMC hinzu:

1. Wählen Sie Konsole – SnapIn hinzufügen/entfernen…
2. Klicken Sie auf Hinzufügen…

Nun erscheint das Dialogfeld mit dem Eigenständiges Snap-In hinzufügen (siehe folgende Abbildung).



1 Wählen Sie die Ereignisanzeige aus und klicken Sie auf Hinzufügen.

2 Alternativ können Sie in der Liste auch auf den Eintrag Ereignisanzeige doppelklicken.

Nun erscheint das Dialogfeld Computer auswählen.

Hinweis

Achten Sie darauf, dass der Rechner ausgewählt wird, auf dem der Policy Manager tatsächlich ausgeführt wird. Klicken Sie ggf. auf die Schaltfläche Durchsuchen, um den richtigen Rechner in der grafischen Benutzeroberfläche auszuwählen.

1 Klicken Sie im Dialogfeld Computer auswählen auf Fertigstellen.

2 Klicken Sie im Eigenständiges Snap-In hinzufügen auf Schließen.

3 Klicken Sie auf OK.

Anhang A: Sicherheitskonzepte für den Policy Manager

Der Policy Manager integriert Ihre physische Sicherheitsinstallation in Ihre bestehende Netzumgebung. Die physische Sicherheit und die Netzsicherheit sind komplexe und sehr spezielle Bereiche, für die jeweils Spezialisten mit profunden Fachkenntnissen zuständig sind. Mit dem Policy Manager können beide Gruppen gemeinsam ein integriertes Sicherheitsnetz für ihre jeweiligen Arbeitsumgebungen herstellen. In beiden Bereichen steht umfangreiche Fachliteratur und umfangreiche technische Dokumentation von ersten Einführungen bis zu höchst differenzierten Darstellungen zur Verfügung. Im Interesse eines besseren Verständnisses sollten Sie sich ggf. mit dieser ergänzenden Literatur vertraut machen.

Da dieses Produkt in Verbindung mit den digitalen Intellex-Videorecordern eingesetzt wird, sind Ihre ersten Informationsquellen für Fragen bezüglich der physischen Sicherheit das Benutzerhandbuch und die sonstige Dokumentation, die Sie mit Ihrem Produkt erhalten haben. Dort finden Sie Informationen zu den in Anhang 2 zusammengestellten Menüs und Optionen, für die erweiterte Sicherheitseinstellungen aktiviert werden können.

Der Policy Manager ist vollständig in das Betriebssystem Windows 2000 integriert. Daher können Sie die Sicherheitseinstellungen für Ihr System nach den Anforderungen in Ihrem individuellen Unternehmensnetz konfigurieren. In der Standardkonfiguration bietet der Policy Manager ein angemessenes Sicherheitsniveau für die meisten Einsatzbereiche. Wenn bei Ihnen jedoch besondere Anforderungen bestehen, sind diese Voreinstellungen möglicherweise nicht ausreichend. In diesem Fall müssen Sie eine benutzerdefinierte Installation vornehmen. Die Behandlung benutzerdefinierter Installationen würde den Rahmen dieses Handbuchs sprengen. Wenn Sie eine benutzerdefinierte Installation vornehmen möchten, empfehlen wir nachdrücklich, die vorgesehene Konfiguration mit den für die Sicherheit Ihres Netzes zuständigen Mitarbeitern zu besprechen und einen der zuständigen Mitarbeiter zu bitten, Ihnen während der Installation behilflich zu sein. Außerdem müssen Sie bzw. der für die Sicherheit Ihres Netzes zuständige Mitarbeiter weitgehend mit der Windows-Sicherheitsphilosophie, mit COM+-Applikationen in Rechnernetzen, mit den jeweiligen Einstellungen und der Verwendung der Einstellungen und mit den DCOM-Sicherheitseinstellungen vertraut sein.

Grundlegende Fragen

Wenn Sie eine sichere Umgebung schaffen möchten, müssen die drei folgenden Fragen möglichst klar und zutreffend beantwortet werden:

1. Wer sind Sie, und sind Sie wirklich derjenige, als der Sie auftreten?
2. Wozu möchten Sie Zugang haben?
3. Was möchten Sie mit dem Objekt anfangen, zu dem Sie Zugang erhalten haben?

Im Zusammenhang mit der Sicherheit von Rechnernetzen wird die Beantwortung der ersten Frage als „Authentifizierung“ bezeichnet. Mit den Antworten auf die zweite und die dritte Frage erfolgt die „Authorisierung“.

Authentifizierung

Wer sind Sie, und sind Sie wirklich derjenige, als der Sie auftreten?

Die zuverlässige Beantwortung dieser Frage ist der einzige Gegenstand der Authentifizierung. Diese Frage begegnet uns immer dann, wenn wir uns in unseren Netzen anmelden. Um auf freigegebene Ressourcen, globale Ressourcen oder auch nur auf unsere E-Mail zugreifen zu können, müssen wir uns authentifizieren.

Die Netzsicherheit ist den physischen Sicherheitsvorkehrungen an vielen Arbeitsplätzen vergleichbar. Ebenso wie sich Mitarbeiter mit Keycards gegenüber einem Zugangskontrollsystem ausweisen, dienen die Anmeldeinformationen im Netz (Benutzername, Passwort und Authentifizierungsstelle (*Authentication Authority*)) zur individuellen Identifizierung von Benutzern in Unternehmensnetzen. Diese Anmeldeinformationen werden zentral gespeichert und abgerufen, damit sie auf jedem beliebigen Rechner verwendet werden können, der Zugang zur Authentifizierungsstelle hat (in der Regel ein Domänen-Controller).

Dem Begriff der Authentifizierungsstelle kommt wesentliche Bedeutung zu. Die Authentifizierungsstelle (in der Regel ein bestimmter Domänen-Controller im Unternehmen) verarbeitet die Authentifizierungsaufforderungen. Entsprechend muss der auffordernde Rechner sowohl physisch mit der Domäne verbunden sein als auch von der Domäne erkannt werden.

Wenn die Anmeldeinformationen gültig sind, d.h. wenn die Informationen eingegeben wurden, an denen die Authentifizierungsstelle eine bestimmte Person (z.B. JSchmitt) erkennt, wurde die Identität dieser Person ermittelt und die Person authentifiziert.

Im Policy Manager kommt diese Authentifizierung in zwei Bereichen zum Einsatz:

In der gesamten Kommunikation zwischen Client-Systemen (Admin Client und Intellex-Geräten) und dem Server authentifizieren COM+ und das zugrunde liegende DCOM-Untersystem die betreffende interaktive Sitzung auf dem Client-Rechner und erteilen den Benutzern abhängig vom Ergebnis der Authentifizierung unter Berücksichtigung der jeweils definierten Rollen entsprechende Berechtigungen.

Beim Datenaustausch zwischen einer Network Client-Workstation und einem Intellex-Gerät erfolgt eine explizite Authentifizierung im Gerät anhand der von der Client-Applikation gesendeten verschlüsselten Anmeldeinformationen. Durch diesen Authentifizierungsprozess wird auf dem betreffenden Gerät eine Windows-Sitzung gestartet. Anschließend erfolgt die Authorisierung aufgrund expliziter Berechtigungsprüfungen für die verschiedenen vom Client geforderten Funktionen.

Die Windows-Sitzung

Wenn die Anmeldeinformationen eines Benutzers erfolgreich verarbeitet wurden, wird für diesen Benutzer auf dem Host-Rechner eine Windows-Sitzung gestartet. Die maßgeblichen Regeln sind in einer Reihe von Richtlinien und Berechtigungen definiert, die der Policy Manager für den gesamten Standort sowie für die einzelnen Geräte verwaltet. Die individuelle Anwendung dieser Regeln auf jeden einzelnen Benutzer wird als Authorisierung bezeichnet.

Richtlinien und Berechtigungen für Standorte

Der Policy Manager wendet allgemeine und spezifische Regeln an. Allgemeine Regeln sind standortspezifische Richtlinien, die unabhängig vom gewünschten Gerät für alle Benutzer angenommen werden, die auf das jeweilige System zugreifen. Die Berechtigungen werden bezogen auf bestimmte Geräte erteilt und sind das zentrale Element der erweiterten Intellex-Sicherheitsfunktionen: Alle Geräte überwachen und erzwingen die Anwendung einer einheitlichen Gruppe von Berechtigungen (z.B. für den Bereich Live-Video). Intellex1 und Intellex2 z.B. überwachen den Zugriff auf Live-Videomaterial von Kamera 13, obwohl Kamera 13 vielleicht überhaupt nicht existiert. Aus diesen Berechtigungen ergibt sich die Sicherheitsumgebung zur Steuerung von Zugriffen und zum Schutz der Geräte.

Alle Geräte unterstützen und erzwingen dieselbe Gruppe von Berechtigungen; trotzdem werden Berechtigungen jedoch für bestimmte Geräte und für bestimmte Benutzer erteilt. Der authentifizierte Benutzer JSchmitt z.B. könnte berechtigt sein, Live-Videos auf Intellex1 anzuzeigen; für die Anzeige von Live-Videos auf Intellex2 dagegen, ist JSchmitt nicht berechtigt.

Nähere Informationen zu den möglichen Berechtigungen und Funktionen finden Sie in Ihrem Intellex-Benutzerhandbuch.

Authorisierung

Im Allgemeinen möchten die Benutzer auf bestimmte Intellex-Geräte zugreifen und bestimmte Funktionen dieser Geräte verwenden. Als Administrator möchten Sie (oder ein sonstiger Benutzer) vielleicht auf Daten zugreifen, die sich auf dem Server mit der Beschreibung Ihres Standorts befinden. Die angezeigten Daten möchten Sie möglicherweise bearbeiten. Entsprechend müssen sowohl Zugriffe auf die betreffenden Geräte als auch Zugriffe auf den Server kontrolliert werden.

Serverzugriffe steuern Sie über vordefinierte Rollen für die oben beschriebene Serverapplikation. Wenn der Zugriff auf bestimmte Serverfunktionen eingeschränkt ist (z.B. der Zugriff auf die Funktion zum Erstellen neuer Zonen), müssen Benutzer, die diese Funktionen verwenden möchten, der Rolle zugewiesen worden sein, der die Berechtigung zur Verwendung dieser Funktion erteilt wurde. In unserem Beispiel müssen die Benutzer also als Mitglieder der Rolle Standort-Administratoren registriert sein.

Zugriffe auf ein Gerät werden über die „Sicherheitsumgebung“ des jeweiligen Geräts gesteuert (siehe Abschnitt „Geräte und ihre Sicherheitsumgebungen“). Folglich kann vorausgesetzt werden, dass der Client authentifiziert und auf dem Zielgerät eine gültige Windows-Sitzung gestartet wurde.

Wozu möchten Sie Zugang haben?

Kehren wir zum Beispiel JSchmitt zurück; JSchmitt besitzt also eine Berechtigungskarte, und wir wissen, dass auf der Karte ausreichend Informationen (Anmeldeinformationen) gespeichert sind, an denen JSchmitt erkannt („authentifiziert“) werden kann. JSchmitt möchte mit seinen Anmeldeinformationen Zugang zum Hintereingang haben.

Da JSchmitt seine Karte in das Lesegerät am Hintereingang eingeschoben hat, erkennt das System diesen Hintereingang als aktuelles Zielobjekt. (JSchmitt möchte in das Gebäude und seine E-Mail abrufen.) Nun verfügt das System über zwei Informationen: Das System weiß zum einen, wer JSchmitt ist, und zum anderen, dass JSchmitt Zugang wünscht (in diesem Fall durch den Hintereingang).

Was möchten Sie mit dem Objekt anfangen, zu dem Sie Zugang erhalten haben?

In diesem einfachen Beispiel ist der Zweck klar: JSchmitt möchte den Hintereingang öffnen. Nun wurden dem System alle drei Fragen hinreichend beantwortet:

- Wer sind Sie, und sind Sie wirklich derjenige, als der Sie auftreten? (JSchmitt, Ja)
- Wozu möchten Sie Zugang haben? (zum Hintereingang)
- Was möchten Sie mit dem Objekt anfangen, zu dem Sie Zugang erhalten haben? (das Objekt öffnen)

Das System benötigt jedoch noch weitere Informationen, um zu entscheiden, ob JSchmitt Zutritt zum Gebäude erhalten darf. Dazu muss das System in einer Datenbank eine Liste der registrierten Benutzer abfragen, denen Zugang zum Hintereingang gewährt wurde. (Vielleicht darf JSchmitt das Gebäude ausschließlich durch den Mitarbeitereingang betreten.) Im einer Netzumgebung kann diese Datenbank z.B. die lokale SAM-Datenbank oder ein Active Directory-Server sein.

Nehmen wir an, es ist eine Datenbank vorhanden, und in der Datenbank wurde die Berechtigung zum Zutritt durch den Hintereingang registriert. Das Zugangskontrollsystem kann dann unsere drei allgemeinen Fragen in einer spezifischen Frage zusammenfassen:

Darf JSchmitt den Hintereingang öffnen?

Nun kann die Anforderung vollständig verarbeitet werden; das Ergebnis der Verarbeitung entscheidet darüber, ob JSchmitt an seinen Arbeitsplatz gelangt.

Sicherheitsdeskriptoren

In einer Windows-Sicherheitsumgebung wird die Datenbank aus dem beschriebenen Beispiel als Sicherheitsdeskriptor bezeichnet. Windows-Sicherheitsdeskriptoren beschreiben die Sicherheitsumgebung jeweils eines mit den erweiterten Sicherheitsfunktionen zu schützenden Objekts oder einer mit den erweiterten Sicherheitsfunktionen zu schützenden Objektgruppe (z.B. einer bestimmten Datei oder sämtlicher Dateien). In Deskriptoren sind bestimmte Berechtigungen für das jeweilige Objekt festgelegt (z.B. eine Datei lesen oder in eine Datei schreiben); außerdem geben Deskriptoren Aufschluss über gewisse allgemeine Berechtigungen, die für sämtliche Objekte gelten. Und schließlich enthalten Deskriptoren eine Liste der Benutzer oder Gruppen, denen bestimmte Berechtigungen erteilt oder verweigert wurden, und Angaben dazu, worauf sich die Berechtigungen beziehen (z.B. verfügt JSchmitt über die Berechtigung Lesen, nicht aber über die Berechtigung Schreiben).

Wenn JSchmitt mit seinem Rechner auf eine bestimmte Datei auf einem Server zugreifen möchte, erfasst die Windows-Sicherheitsumgebung sämtliche Informationen zur Beantwortung unserer grundlegenden Fragen (mit jeweils angepasster Formulierung). In unserem Beispiel würde etwa formuliert:

Darf JSchmitt auf die Datei Prognosen.xls auf MeinemFileServer zugreifen?

Das System führt zunächst die nötigen Funktionen zur Authentifizierung von JSchmitt durch. Wenn die Authentifizierung erfolgreich durchgeführt wurde, lädt das System den Sicherheitsdeskriptor der Datei, auf die JSchmitt zugreifen möchte (Prognosen.xls); im Deskriptor prüft das System...

- Ob JSchmitt explizit Zugriff gewährt wurde; in diesem Fall erscheint der individuelle Deskriptor dieses Benutzers im Sicherheitsdeskriptor

  BZW.

- Ob er die Zugriffsberechtigung aufgrund seiner Mitgliedschaft in einer Gruppe geerbt hat

Besitzt JSchmitt die erforderliche Berechtigung, kann er die Datei öffnen.

Dem Policy Manager und den erweiterten Intellex-Sicherheitsfunktionen liegen die gleichen Prinzipien zugrunde. Ergänzend zu einigen gerätespezifischen Informationen wie z.B. dem Gerätenamen oder der MAC-Adresse enthält die Sicherheitsumgebung eines Geräts eine Liste der Sicherheitsdeskriptoren, mit denen Zugriffe auf Betriebssystemebene zugelassen werden. Das Betriebssystem entscheidet dann aufgrund dieser Informationen sowie aufgrund der Informationen über die Windows-Sitzung des auffordernden Benutzers, ob ein Benutzer oder eine Benutzergruppe die benötigten Berechtigungen besitzt.

Nehmen wir z.B. an, JSchmitt möchte Live-Videomaterial von Kamera 13 anzeigen. Die drei grundlegenden Fragen lauten dann:

- Wer sind Sie, und sind Sie wirklich derjenige, als der Sie auftreten? (JSchmitt, Ja)
- Wozu möchten Sie Zugang haben? (zu Kamera 13)
- Was möchten Sie mit dem Objekt anfangen, zu dem Sie Zugang erhalten haben? (Live-Videomaterial anzeigen)

Mit den erweiterten Sicherheitsfunktionen in Intellex wird zunächst der Sicherheitsdeskriptor für Live-Videomaterial aus der Sicherheitsumgebung geladen. Anschließend wird auf Betriebssystemebene aufgrund der bei der Authentifizierung für die Anmeldung von JSchmitt definierten Informationen für die betreffende Sitzung folgende Frage beantwortet:

Darf JSchmitt auf Live-Videomaterial von Kamera 13 zugreifen?

Das System behandelt diese Frage so, als würde JSchmitt im vorstehenden Beispiel Zugriff auf die Datei fordern; nun wird allerdings ein speziell vom betreffenden Intellex-Gerät erstellter und verwalteter Sicherheitsdeskriptor berücksichtigt. Wie im vorstehenden Beispiel wird aufgrund der in diesem Deskriptor enthaltenen Einstellungen entschieden, ob JSchmitt Live-Videomaterial von Kamera 13 anzeigen darf.

Benutzer, Gruppen und geerbte Berechtigungen

Der Policy Manager berücksichtigt die in Ihrem bestehenden Unternehmensnetz definierten Benutzer und Gruppen. Die Verwaltung einer eigenen Liste ergänzend zur normalen Netzumgebung ist nicht erforderlich. Entsprechend sind im Admin Client keinerlei Funktionen definiert, mit denen neue Benutzer oder Gruppen hinzugefügt werden könnten. Die benötigten Benutzer und Gruppen sind bereits vorhanden.

Wenn ein Benutzer oder eine Benutzergruppe Zugriff auf ein Gerät haben soll, muss die Domäne, in der der Policy Manager installiert wird, diesen Benutzer bzw. diese Gruppe kennen. Benötigen Sie weitere Benutzer oder Benutzergruppen, müssen Sie (oder Ihr Netzwerkadministrator) die Benutzer bzw. Gruppen zum Unternehmen hinzufügen.

Sie können ausschließlich Benutzer authentifizieren. Gruppen sind Zusammenstellungen von Benutzern mit gemeinsamen Berechtigungen. Wenn JSchmitt z.B. Mitglied der Gruppe Marketing ist und die Gruppe Marketing uneingeschränkte Berechtigungen für die Datei Prognosen.xls auf einem File-Server besitzt, hat auch JSchmitt uneingeschränkten Zugriff auf diese Datei (selbst wenn JSchmitt die entsprechenden Berechtigungen nicht explizit erteilt wurden). Die Zugriffsberechtigungen eines Benutzers ergeben sich also aus der Summe sämtlicher Berechtigungen, die diesem Benutzer explizit erteilt wurden, sowie aus den Berechtigungen der Gruppen, denen der betreffende Benutzer angehört.

Dieses Prinzip gilt auch für die erweiterten Sicherheitsfunktionen. Wenn im vorstehenden Beispiel etwa die Gruppe Berlin Zugriff auf Live-Videomaterial von den Kameras 1 bis 16 auf Intellex-Gerät 1 („Intellex1“) hat, kann auch JSchmitt diese Kameras anzeigen (selbst wenn er in der Liste der Benutzer und Gruppen, denen die Berechtigung für diese Kamera erteilt wurde, nicht enthalten ist).

Die vorstehenden Beispiele beschreiben ein weiteres Grundkonzept der Netzsicherheit: die Vererbung von Berechtigungen. Im vorstehenden Beispiel hat JSchmitt die Berechtigungen der Gruppe Berlin geerbt. JSchmitt erbt allerdings nicht nur die definierten Berechtigungen, sondern auch die expliziten Verweigerungen aus den Gruppen, denen er als Mitglied angehört. Wenn Berlin also explizit der Zugriff auf Live-Videomaterial von Kamera 3 verweigert wird, kann auch JSchmitt Kamera 3 nicht anzeigen. Die Verweigerung hat Vorrang vor den definierten Berechtigungen; entsprechend könnte JSchmitt Kamera 3 selbst dann nicht anzeigen, wenn er explizit oder indirekt über eine Vererbung die Berechtigung für Zugriffe auf Kamera 3 erhalten hätte.

Drei Typen von Zugriffsberechtigungen

Bei Zugriffsberechtigungen sind drei grundlegende Typen zu unterscheiden, die Administratoren für einzelne Benutzer oder für Benutzergruppen definieren können:

- Impliziter Zugriff
- Expliziter Zugriff
- Explizite Verweigerung

Impliziter Zugriff

Der implizite Zugriff ist praktisch synonym zum geerbten Zugriff zu verstehen. Wenn JSchmitt Mitglied der Gruppe Berlin ist und diese Gruppe Zugriff auf die Datei Prognosen.xls hat, kann auch JSchmitt auf die Datei zugreifen. Muss der Administrator Zugriffe regeln, ist dieser Zugriffstyp am problematischsten, weil der Sicherheitsdeskriptor einen Eintrag für JSchmitt enthält und der Name JSchmitt daher nicht in der Zugriffsdefinition dieses Deskriptors vorkommt.

Expliziter Zugriff

Administratoren können Benutzern oder Benutzergruppen explizit Zugriff auf ein Objekt gewähren. Nehmen wir z.B. an, im System existiert eine zweite Datei (Prognosen2.xls), auf die die Gruppe Berlin nicht zugreifen darf. Der zuständige Administrator kann dann explizit Berechtigungen für JSchmitt definieren, indem er JSchmitt in die Liste der Benutzer oder Benutzergruppen im Sicherheitsdeskriptor für die betreffende Datei aufnimmt. Der Administrator erteilt die vorgesehene Berechtigung im Zugriffseditor, indem er JSchmitt zum Sicherheitsdeskriptor der Datei hinzufügt und dann das Kontrollkästchen Zulassen aktiviert. Anschließend erscheint der Name JSchmitt, sobald ein Administrator den Sicherheitsdeskriptor zum Bearbeiten öffnet.

Explizite Verweigerung

Administratoren können Benutzern oder Benutzergruppen explizit den Zugriff auf ein Objekt verweigern. Nehmen wir an, der Leiter der Gruppe Berlin hat entschieden, dass JSchmitt keinen Zugriff mehr auf die Datei Prognosen.xls haben soll. JSchmitt hat die Zugriffsberechtigung für diese Datei geerbt (d.h. er erscheint nicht im Sicherheitsdeskriptor der Datei). Die einzige Möglichkeit, die implizite (geerbte) Zugriffsberechtigung zu übergehen, besteht darin, dem betreffenden Benutzer bzw. der betreffenden Benutzergruppe die Berechtigung explizit zu verweigern. Die explizite Verweigerung hat Vorrang vor allen sonstigen Zugriffsdefinitionen. Um die Verweigerung zu definieren, fügt der Administrator JSchmitt im Zugriffseditor zum Sicherheitsdeskriptor der Datei hinzu, um dann für JSchmitt das Kontrollkästchen Verweigern zu aktivieren.

Anhang B: Häufig gestellte Fragen (FAQ)

Was bedeutet der Begriff „Übertragen“?

Über das Dialogfenster Einstellungen übertragen können Sie die Sicherheitseinstellungen eines Geräts auf eines oder mehrere weitere Geräte kopieren. Kopiert werden nur die eigentlichen Sicherheitseinstellungen; der Gerätename und die Beschreibung werden nicht übernommen.

Was bedeutet „vererben“?

Wenn Sie die Sicherheitseinstellungen eines Geräts bearbeiten und ein „Container“-Objekt auswählen, wird ein allgemeiner Editor geöffnet. Als Container-Objekte werden die Objekte in der Liste bezeichnet, deren Namen ein kleines Kästchen vorangestellt ist. Container-Objekte sind z.B. die Objekte Multimedia Data oder Administration. Da ein Container keine bestimmten Objekte enthält, können Sie für Container nur die Einstellungen Lokaler Zugriff oder Remote-Zugriff definieren. Auf Container-Ebene hinzugefügte Benutzer und Gruppen „erben“ als Kindobjekte des unmittelbaren Container-Elternobjekts jedoch sämtliche Berechtigungen, die für die im Container enthaltenen Funktionen definiert wurden.

Wenn Sie z. B. den Benutzer JSchmitt zum Container Multimedia Data hinzufügen und für diesen Benutzer die Einstellung Uneingeschränkter Zugriff aktivieren, kann JSchmitt unabhängig davon, ob er sich direkt am Gerät befindet (lokaler Zugriff) oder über den Network Client oder die API von einem Remote-System zugreift, alle vorhandenen Informationen anzeigen. Für sämtliche Medien-Streams (d.h. für sämtliche untergeordneten Funktionen im Container Multimedia Data) wurde die Voreinstellung definierte Einstellung „Zugriff zugelassen“ definiert. Diese Berechtigung wurde vom Eltern-Container auf sämtliche Kindobjekte und somit auch auf JSchmitt vererbt. Die Berechtigungen für die Kindobjekte werden durch eine besondere vom Server erzwungene Gruppe von Regeln ergänzt. Diese Regeln sind für jedes Kindobjekt (Funktionsobjekt) unterschiedlich. (Bei Multimedia-Streams sind Zugriffe z.B. auf alle 16 Streams erlaubt. Im Verzeichnis Administration\Utility hingegen sind Zugriffe nur auf die Funktionen Alarme erstellen, Vordergrundalarme löschen und CD-RW löschen zulässig. Alle sonstigen Funktionen sind nicht verfügbar.)

Die Vererbung ist eine leistungsfähige Funktion, wenn mehreren Benutzern oder Gruppen möglichst einfach bestimmte Standardberechtigungen erteilt werden sollen.

Was geschieht, wenn ich Einstellungen auf ein einzelnes Gerät oder eine Gerätegruppe übertrage?

Beim Übertragen von Sicherheitseinstellungen von einem Gerät auf eines oder mehrere andere Geräte werden die Einstellungen des Ausgangsgeräts (des Geräts, auf dem Sie im Menü den Befehl Übertragen... gewählt haben) auf alle Geräte kopiert, die im Policy Manager im Dialogfeld Einstellungen übertragen als Zielgeräte ausgewählt wurden.

Wenn Sie z.B. die für das Standardgerät der Zone definierten Einstellungen ändern und die neuen Einstellungen dann auf andere Geräte oder Zonen übertragen, kann der Administrator eine einheitliche Sicherheitsumgebung unter gleichzeitiger Einbeziehung unterschiedlicher Einzelsysteme erzeugen. Sie können die Sicherheitseinstellungen des Standardgeräts auf eines oder auch beliebig viele Geräte in den betreffenden Zonen sowie in nicht mit dieser Zone verbundenen Zonen übertragen. Außerdem können Sie die Einstellungen auf Geräte außerhalb der Zone übertragen, in der sich das Ausgangsgerät befindet. Zonen werden alle ähnlich dargestellt wie der Knoten Alle gesicherten Geräte. (Der Knoten Alle gesicherten Geräte stellt eine eigenständige Zone dar.)

Wenn sich ein Gerät neu im Policy Manager registriert, erhält dieses Gerät eine Kopie der aktuellen Sicherheitseinstellungen des Standardgeräts am betreffenden Standort. In gewisser Hinsicht wurden die Einstellungen für dieses Standardgerät also automatisch auf das neue Gerät übertragen.

Beim Übertragen werden Name und Beschreibung der Zielgeräte NICHT geändert.

Was sind Standardgeräte?

Standardgeräte sind im Grunde Sicherheitsvorlagen, die Administratoren helfen, eine einheitliche Sicherheitsumgebung für einen gesamten Standort oder für unterschiedliche Zonen innerhalb eines Standorts herzustellen.

Jede Zone enthält z.B. ein Standardgerät mit den für alle in dieser Zone enthaltenen Geräte maßgeblichen Sicherheitseinstellungen. (Diese Voreinstellungen können allerdings überschrieben werden.)

Ein besonderes Standardgerät ist das Standort-Standardgerät in der Zone Unassigned Instrument. Diese Vorlage wird immer dann verwendet, wenn sich ein neues Gerät im Policy Manager registriert. Entsprechend sollte diese Vorlage die gewünschte grundlegende Sicherheitsumgebung für den gesamten Standort beschreiben.

Was ist der Unterschied zwischen einem aktiven und einem inaktiven Gerät?

Als aktive Geräte werden betriebsbereite Geräte bezeichnet, d.h. Geräte, mit denen Videomaterial aufgezeichnet werden kann und die Befehle zur Ausführung z.B. zur Ausführung von Suchfunktionen von einem lokalen Client oder von einem Remote-Client empfangen können.

Inaktive Geräte reagieren nicht auf Aufforderungen eines Servers. Dies bedeutet nicht zwangsläufig, dass die Geräte gerade kein Videomaterial aufzeichnen; vielleicht ist die Kommunikation zwischen Server und Client durch einen Netzfehler beeinträchtigt: Diese Kommunikationsprobleme sind vom zuständigen Administrator zu untersuchen.

Die Geräte werden regelmäßig abgefragt um sicherzustellen, dass die Geräte noch aktiv und verfügbar sind. Wenn ein aktives Gerät auf diese Abfragen nicht antwortet oder einen Fehler meldet, gilt das Gerät als inaktiv. In diesem Fall wird eine entsprechende Benachrichtigung an alle zum betreffenden Zeitpunkt aktiven Administrationssitzungen gesendet und das Ereignis im Ereignisprotokoll erfasst.

Anhang C: Menüs und Optionen, für die erweiterte Sicherheitseinstellungen aktiviert werden können

Hinweis

In diesem Anhang sind alle Menüs und Optionen zusammengestellt, für die zurzeit in Intellex 3.2 erweiterte Sicherheitseinstellungen aktiviert werden können. Nähere Beschreibungen der verschiedenen Funktionen finden Sie im Intellex-Installations- und Konfigurationshandbuch.

Kategorie	Menü	Optionen	Voreinstellung
Gerät	Für sämtliche Menüs maßgeblich	Höchste Ebene eines Geräts; Benutzer und Gruppen, denen Zugriff erteilt oder verweigert wird, vererben diese Einstellung an sämtliche Menüs. Wenn Einstellungen von einem Container auf die jeweiligen Kinder vererbt werden, definiert das System nur die spezifischen Standardeinstellungen für die verschiedenen Kindobjekte (Menüs und Optionen).	
Administration	Utilities (Dienste)	Generate Alarms (Alarme erstellen) – Ermöglicht die manuelle Erstellung von Alarmen zu Testzwecken.	X
		Clear Latched Alarms (Vordergrund löschen) - Ermöglicht das Löschen sämtlicher Alarmmeldungen im Modus Vordergrundalarm.	X
		Erase CD-RW (CD-RW löschen) – Ermöglicht das Löschen von Daten auf einem eingelegten CD-RW-Medium.	
		View Activity Log (Aktivitäts-Log anzeigen) – Ermöglicht das Anzeigen des internen Aktivitäts-Log.	
	Setup	Setup Record Mode (Aufzeichnungsmodus konfigurieren) – Ermöglicht das Umschalten zwischen dem linearen und dem zirkularen Modus sowie das Definieren der Warnschwelle für den linearen Modus.	
		Setup Alarm (Alarme konfigurieren) – Ermöglicht das Ändern von Alarmnamen und -einstellungen.	X
		Setup Archive Schedule (Archivierungszeitplan konfigurieren) **–** Ermöglicht die individuelle Anpassung von Archivierungszeitplänen.	
		Setup Cameras (Kameras konfigurieren) **–** Ermöglicht das Ändern von Kameranamen und -heinstellungen.	

Kategorie	Menü	Optionen	Voreinstellung
		Setup Covert Camera (Verdeckte Kamera konfigurieren) **–** Ermöglicht das Ändern der Einstellungen von verdeckten Kameras und das Anzeigen von als verdeckt definierten Kameras.	
		Setup Schedule (Zeitplan konfigurieren) – Ermöglicht Änderungen am Aufzeichnungszeitplan.	X
		Setup Display (Anzeige konfigurieren) – Ermöglicht das Ändern der Live-Anzeige und das Abrufen von Bildschirmeinstellungen.	
		Setup Security (Sicherheit konfigurieren) – Ermöglicht das Definieren und Ändern von Sicherheitseinstellungen.	
		Setup Text (Text konfigurieren) – Ermöglicht Änderungen an den Einstellungen für Text-Streams.	
		Setup Audio (Audio konfigurieren) – Ermöglicht Änderungen an den Einstellungen für Audio-Streams.	
		Email Notification (E-Mail-Benachrichtigung) - aktiviert die E-Mail-Benachrichtigung bei System-Ereignissen wie Alarmen usw.	
	System	Upgrade or Modify License (Lizenz-Upgrade oder -Änderung) – Ermöglicht Lizenz-Upgrades.	
		Begin Record (Aufzeichnung starten) – Ermöglicht die Fortsetzung einer unterbrochenen Aufzeichnung.	
		Shutdown the System (System herunterfahren) – Ermöglicht das Herunterfahren des Systems.	X
		Exit to System Permission (Beenden und Betriebssystem anzeigen) – Ermöglicht den Wechsel in die Betriebssystemoberfläche.	
		Access Sytem Storage Settings (Speichereinstellungen des Systems öffnen) – Ermöglicht Änderungen an den Einstellungen für das verwendete Speicher-Volume.	
		Access Server Settings (Server-Einstellungen öffnen) – Ermöglicht Änderungen an den Port-Adressen.	
		Access Data and Time Settings (Einstellungen für Datum und Uhrzeit öffnen) – Ermöglicht Änderungen der Systemzeit.	
Multi Media Data (Multimedia-Daten)	Live Video (Live-Video)	Cameras 1-16 (Kameras 1-16) – Ermöglicht das Anzeigen von Live-Videomaterial auf den ausgewählten Kameras.	Alle

Kategorie	Menü	Optionen	Voreinstellung
	Recorded Video (Aufgezeichnete Videodaten)	Cameras 1-16 (Kameras 1-16) – Ermöglicht das Suchen/ Wiedergeben aufgezeichneten Videomaterials von ausgewählten Kameras.	Alle
	Recorded Text (Aufgezeichnete Textdaten)	Text Streams 1-16 (Text-Streams 1-16) – Ermöglicht das Suchen/ Wiedergaben aufgezeichneter Textdaten in ausgewählten Text-Streams.	Alle
	Live Audio (Live-Audio)	Audio Stream 1 (Audio-Stream 1) – Ermöglicht das Hören von Live-Audiomaterial von Audio-Stream 1.	Alle
	Recorded Audio (Aufgezeichnete Audiodaten)	Audio Stream 1 (Audio-Stream 1) – Ermöglicht die Wiedergabe aufgezeichneter Audiodaten von Audio-Stream 1.	Alle
Advanced (Erweiterte Sicherheit)	Dome Control (Dome-Steuerung)	Cameras 1-16 (Kameras 1-16) – Ermöglicht die Steuerung des Domes der ausgewählten Kamera.	Alle
	Dome Programming (Dome-Programmierung)	Cameras 1-16 (Kameras 1-16) – Ermöglicht den Zugriff auf die Dome-Programmierung der ausgewählten Kamera(s).	
	Local Archive (Lokales Archiv)	Archive Enable (Archivierung aktivieren) – Ermöglicht den Zugriff auf das Menü Archivieren.	X
	Remote Features Sub-permissions (Remote-Funktionen: Untergeordnete Berechtigungen)	Download Alarm Log (Alarm-Log herunterladen): Berechtigt zum Herunterladen des für das betreffende Gerät erzeugten Alarmprotokolls.	
		Download Activity Log (Aktivitäts-Log herunterladen): Berechtigt zum Herunterladen des für das betreffende Gerät erzeugten Aktivitäts-Log.	
		Download System Status (Systemstatus herunterladen): Berechtigt zum Abrufen von Informationen zum Systemstatus des betreffenden Geräts.	
		Remote Access to Record Settings (Remote-Zugriff auf Aufzeichnungs-einstellungen): Berechtigt für Remote-Zugriffe auf die Aufzeichnungseinstel-lungen des betreffenden Geräts (API-spezifisch).	
		Remotely Generate Alarms (Alarme auf Remote-System erzeugen): Berechtigt zum Erzeugen von Alarmen für das betreffende Gerät auf Remote-Systemen (API-spezifisch).	

Index

A

Allgemeine Standort-Richtlinien verwenden 7
Ausschneiden 10

B

Beschreibung definieren 10

D

Dauer der Sperre 8
Die erweiterten Intellex-Sicherheitsfunktionen in der Kategorie Sicherheitseinstellungen definieren 9
Die verwendeten Symbole und ihre Bedeutung 5

E

einer Zone zuweisen 10
Einstellungen übertragen 10
Ereignisprotokolle 2
erweiterte Sicherheit 1

F

Funktionen 2

G

Garantie iv
Geräte hinzufügen 11

I

Intellex-Archive Manager 3
Intellex-Policy Manager 3
Intervall für Geräteabfrage 8

L

Lizensierungsschlüssel v
Lizenz
  Erteilung iv
  Software iv
  Upgrade iv
Lizenzinformationen iv
Lizenz-Manager 3
LIZENZVEREINBARUNG iv
Löschen 10

M

Maximale Anzahl Anmeldeversuche 8
Mehrere gleichzeitige Administrationssitzungen zulassen 8
Modul Alle gesicherten Geräte 9

O

Objekte, die unter Intellex 3.2 mit erweiterten Sicherheitsfunktionen geschützt werden können 9

P

Policy Manager 1.1 für Intellex® DVMS (PM 1.1) 1

R

Ressourcen 3

U

Upgrade, Lizenz iv