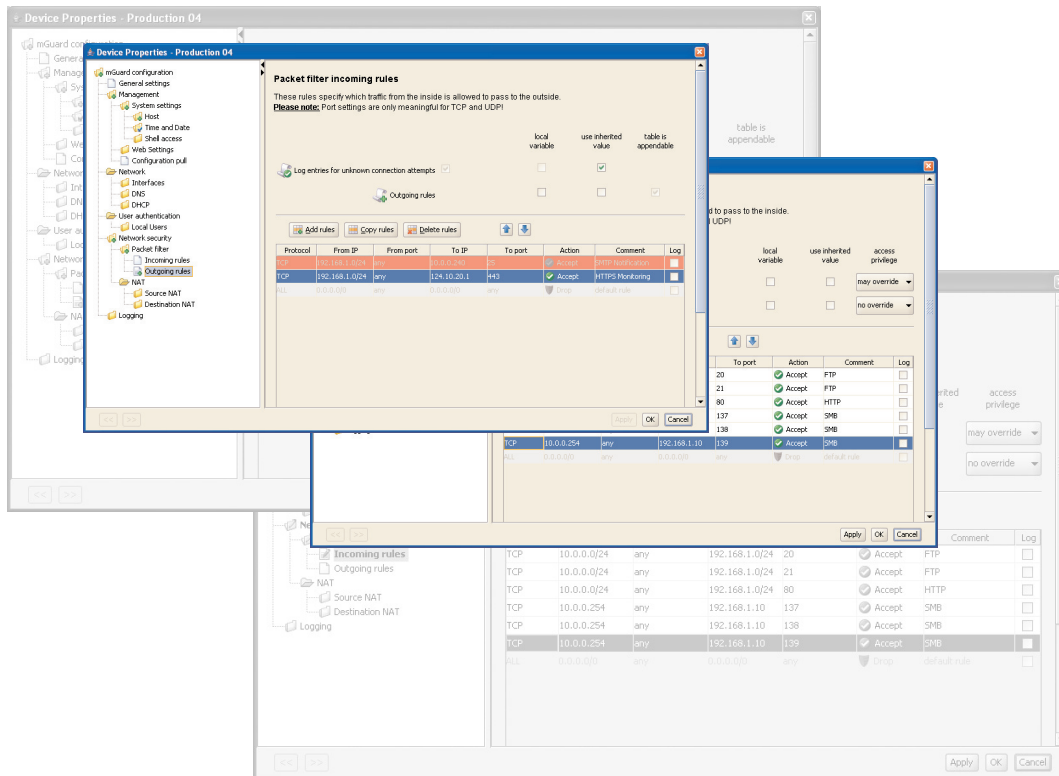


Innominate

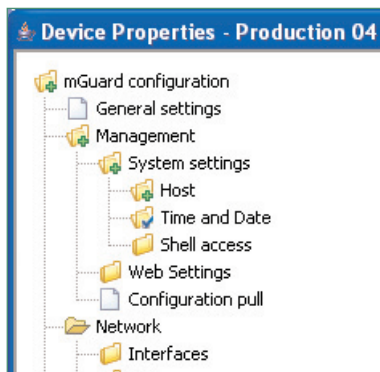
Device Manager

mGuard Konfigurations- und Roll-out Management



- Hochskalierbares Device Management
- Einfacher Roll-out
- Template-basierte Konfiguration
- Überwachung von Konfigurationsstatus und Updates

Durch den Innominate Device Manager (IDM) wird das Verwalten der mGuard Security Appliances ganz einfach. Das Tool bietet einen Template-Mechanismus, mit dem Sie als Anwender zentral alle mGuard Devices konfigurieren und verwalten können – von einigen hundert bis zu mehreren tausend.



Die wichtigsten Merkmale:

- Unterstützung der dezentralen mGuard Sicherheitslösung.
- Konfiguration großer Bestände verteilter mGuard Appliances.
- Template-Unterstützung (Gruppierung homogener konfigurierter Systeme).
- Verteilung von Konfigurationen über Upload- oder Download-Funktion (Push oder Pull).
- Architektur und Funktionalität des IDM sind auf die Anforderungen der Industrie zugeschnitten. Die mGuard Systeme können ohne IT-Personal konfiguriert und kontrolliert werden.
- Device-orientierte Struktur entsprechend der Konfiguration eines Einzelsystems. Die Parameter werden direkt konfiguriert, ohne dass abstrakte Security Policies definiert werden müssen.

Die Innominate mGuard Systeme sichern die M2M-Kommunikation. Mögliche Anwendungsbereiche sind der Schutz und die sichere Fernwartung von vernetzten Robotern in der Automotive Industrie und von Produktionsanlagen in der herstellenden und verarbeitenden Industrie.

Der Template-basierte Innominate Device Manager (IDM) ist ideal für den Roll-out und das Management großer Gruppen gleich konfigurierter Security Appliances. Weit verteilte Installationen mit tausenden von Systemen können schnell und effizient implementiert werden. Templates ermöglichen die Zusammenfassung von Konfigurationseinstellungen und vereinfachen den sicherheitskritischen und komplizierten Teil der Systemkonfiguration. Die gewünschten Firewall-Regeln und NAT-Einstellungen werden einfach per Mausklick generiert, über die Upload-Funktion auf alle aufgelisteten Appliances hoch geladen und so in einem Arbeitsgang bequem konfiguriert. Alternativ können die Konfigurationsdaten von den Devices automatisch herunter geladen werden.

Der IDM ist eine Client-Server-Applikation. Der Client bietet die volle Kontrolle über alle IDM Features, der Server speichert alle Konfigurationsdaten in einer Datenbank, aus der Konfigurations-Files erstellt und an die einzelnen Systeme übergeben werden. Die Files (ASCII) werden per SSH auf die mGuard Systeme geladen, die sofort betriebsbereit sind. Darüber hinaus kann der IDM Files generieren, die für den Konfigurations-Pull per HTTPS von den Systemen genutzt werden können.

IDM Client

Der IDM Client ist die grafische Benutzeroberfläche zur Nutzung aller Features des IDM. Als Anwender können Sie Templates erstellen und Systeme verwalten, um Konfigurationen auf die Devices zu laden oder um den Export von Systemkonfigurationen in ein Webserver Filesystem durchzuführen.

Anwendungsbeispiel

Remote Service Security ist ein typisches Anwendungsgebiet für mGuard Systeme, um Internet/VPN- oder Einwahl-Verbindungen für die Fernüberwachung, Ferndiagnose und Fernwartung industrieller Maschinen und Anlagen abzusichern.

Innominate Device Manager

| | |
|------------------------------|---|
| Architektur ▶ | Client-Server-Applikation für die Template-basierte Konfiguration von mGuard Systemen |
| Skalierbarkeit ▶ | Skalierbar bis zu 10.000 Systemen |
| VPN Topologie ▶ | 1:N VPNs oder VPN Endpunkte |
| Lokales Setup ▶ | Ja |
| Konfigurationsmodus ▶ | Push- und Pull-Konfiguration mit optionaler Status-Rückmeldung |
| Bedienoberfläche ▶ | Tabellen und Eingabemasken |

Hersteller solcher Anlagen mit tausenden installierter Systeme beim Kunden und hunderten neuer Systeme, die jährlich ausgeliefert werden, können den IDM nutzen, um die entsprechende Anzahl der in den Systemen installierten mGuard Sicherheits-Appliances effizient zu verwalten.

Roll-out Szenario

Wenn ein erfahrener Netzwerksicherheits-Administrator über die Templates des IDM die entsprechende Konfiguration einmal erstellt hat, kann jeder Techniker die mGuard Sicherheits-Appliance vor Auslieferung perfekt konfigurieren. Insbesondere die komplexe Konfiguration von VPN-Verbindungen, digitalen Zertifikaten und virtuellen Adressierungsformen wird von den Templates des IDM in Verbindung mit den Automatisierungsmechanismen übernommen. Die Konfiguration von Variablen wie der IP-Adresse zum Kundennetzwerk kann als lokale Variable von einem Administrator vor Ort ergänzt werden. Sobald das mGuard System beim Kunden aktiviert ist, kann der IDM den Konfigurationsstatus jederzeit überwachen und aktualisieren.

Die Übertragung vom IDM Server zur mGuard Appliance

1. Konfigurations-Push über SSH

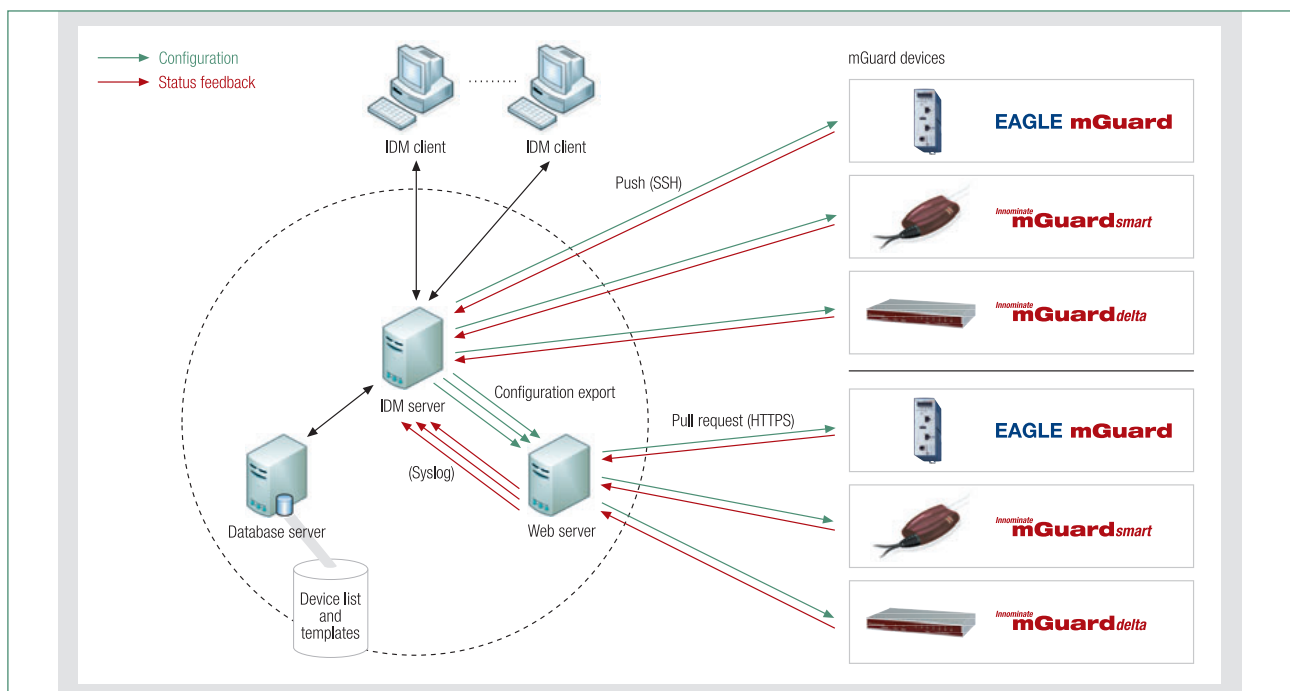
IDM Server und mGuard System sind über SSH (secure shell protocol) verbunden, um die Konfigurationsdatei auf das Device zu kopieren und zu aktivieren. Status und Fertigstellung des Upload-Vorganges sowie eventuelle Probleme werden vom IDM-Server überwacht und auf dem IDM-Client dargestellt. Der Upload-Prozess kann vom IDM-Client aus für eine individuelle Auswahl an Devices oder für alle Devices gleichzeitig erfolgen.

Template Eigenschaften

Mit Templates ist eine große Zahl von Devices bequem zu konfigurieren und zu verwalten. Die Templates enthalten eine Auswahl an Variablen für die mGuard Systeme. Sobald das Template einem Device zugewiesen ist, übernimmt das System die Einstellungen und nutzt die Werte für die Variablen des mGuard Systems. Abhängig von den Permission-Einstellungen können die Template-Einstellungen im Device überschrieben werden.

Device Eigenschaften

Über die Device Eigenschaften werden die Variablen des mGuard Systems und deren Eigenschaften für ein Device konfiguriert. Im Unterschied zu Templates enthält eine Device-Konfiguration immer ein komplettes Set an Variablen des mGuard Systems.



Konfiguration der mGuard Devices

2. Konfigurations-Pull über HTTPS

Der IDM Server kann auch neue oder aktualisierte Device-Konfigurationen auf ein Webserver Filesystem exportieren. Die entsprechenden mGuard Systeme können dann über eine sichere HTTPS-Verbindung auf dem Webserver verfügbare Updates selbst in bestimmten Zeitabständen oder bei jedem Boot-Vorgang prüfen und herunter laden. Die passende IDM-Konfiguration kann sowohl über die logische Management-ID als auch über die Seriennummer des Device zugeordnet werden.

Beide Methoden können kombiniert werden: unkritische Updates werden für den nächsten Konfigurations-Pull bereit gestellt, während kritische Updates sofort aktiv auf alle Devices übertragen werden (Push).

Konfigurierbare mGuard Features, die vom IDM unterstützt werden

- Systemeinstellungen (Host, Zeit und Datum, Shell Access)
- mGuard Web-Zugriff
- Konfigurations-Pull
- mGuard Schnittstellen (Netzwerkmodus, Stealth Modus Einstellungen, externe und interne Netzwerke, PPPoE Einstellungen)
- DNS
- Internes DHCP
- Anwender-Authentifizierungsebenen (lokale Anwender): Admin, Netzwerk-Admin, Audit
- Paketfilter (eingehende und ausgehende Regeln)
- NAT (Masquerading, 1:1 NAT, Portweiterleitung)
- Loggen zu einem Syslog-Server
- VPN Verbindungen
- Bequeme Autokonfiguration des Peer Gateway, wenn das Peer Device ebenfalls von IDM verwaltet wird
- Integrierte Certificate Authority (CA) für VPN Authentifizierung mit automatisch generierten X.509 Zertifikaten
- Intelligente Verwaltung von Werte-Pools, z. B. für automatisch zugewiesene, einmalige virtuelle Adressen und Netzwerke

Template

Eine Reihe von mGuard Variablen mit den entsprechenden Werten und Zugriffs-Privilegien. Es kann einem mGuard System immer nur ein Template zugewiesen werden. Eine Änderung des Templates wird auf alle Devices übertragen, die dieses Template nutzen, abhängig von den Einstellungen der Zugriffs-Privilegien. Das Template selbst wird nur im IDM verwendet und nicht auf die mGuard Appliance übertragen.

Lokale mGuard Variable

Innerhalb des IDM kann jede Konfigurationsvariable als „lokal“ gekennzeichnet werden (in der Maske der Template Eigenschaften oder der Device Eigenschaften). Lokale Variable werden nicht vom IDM verwaltet, sondern sind Teil der lokalen Konfiguration des mGuard Systems und können nur vom „Network Admin“-Anwender gesetzt werden.

Admin/Network Admin/Audit (Zugriffsregelung auf das mGuard System)

Die Regel „Admin“ kann alle Einstellungen für die mGuard Systeme verändern, während die Regel „Network Admin“ nur Variable setzen kann, die im IDM als lokal definiert sind. Die Regel „Audit“ kann alle Einstellungen lesen, aber keine Änderungen vornehmen (read only).

| System-Mindestanforderungen | Client | Server |
|-----------------------------|--|--|
| Hardware | 512 MB RAM 500 MB freier Speicherplatz Farbmonitor mit Mindestauflösung 1024 x 768 | 512 MB RAM 4 GB freier Speicherplatz |
| Software | Windows 2000 SP2 oder höher, Windows XP oder Linux Java Runtime Environment 5.0 | Windows 2000 SP2 oder höher, Windows XP oder Linux Java Runtime Environment 5.0 Postgre SQL Version 8.1 |