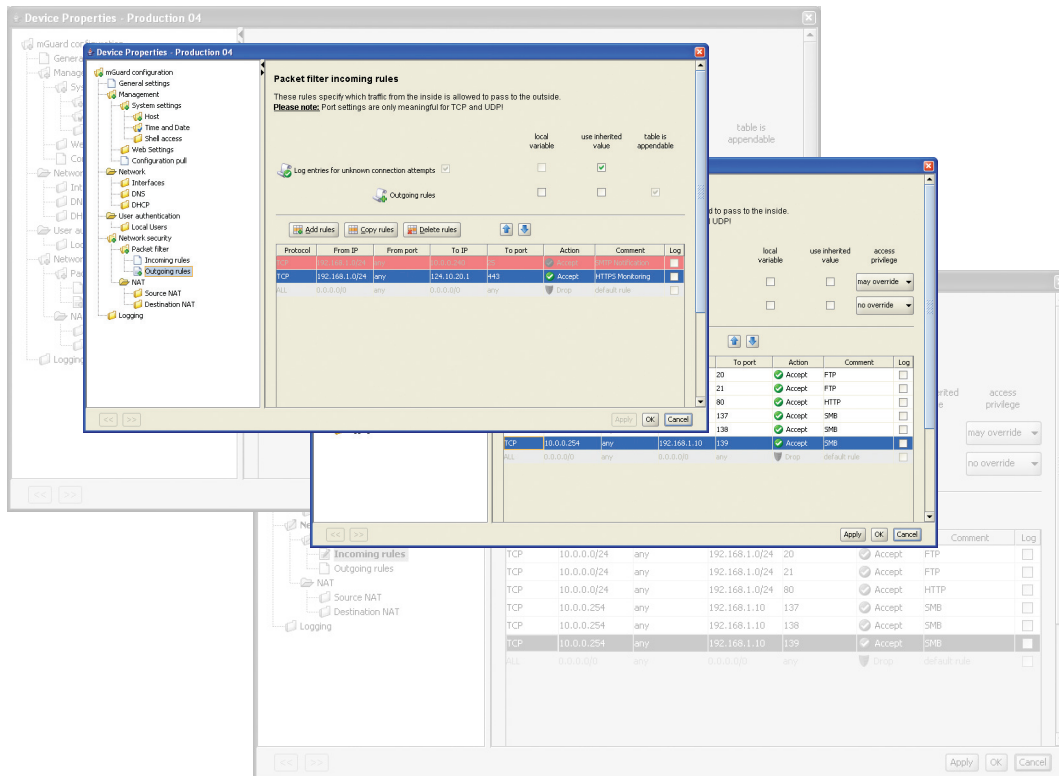


Innominate

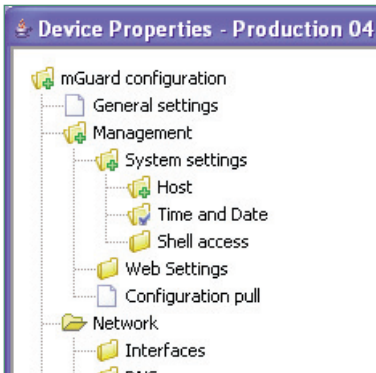
Device Manager

Configuration and Roll Out Tool for mGuard Appliances



- Highly scalable device management
- Easy roll out
- Template-based configuration
- Control of configuration status and updates

The Innominate Device Manager (IDM) enables the convenient management of Innominate mGuard security appliances. The tool offers a template mechanism that allows users to centrally configure and manage hundreds up to several thousand Innominate mGuard devices.



Key Benefits

- Supports the mGuard end-point security approach.
- Configuration of large populations with distributed mGuard appliances.
- Template support (grouping of homogeneously configured devices).
- Distribution of the configurations via upload function (push) or download (pull).
- Architecture and functionality of the IDM is adapted to industrial requirements. It enables even non-IT experts to roll out and maintain the mGuard appliances.
- Device-oriented structure equivalent to single device configuration. Features are configured directly without the need for defining abstract security policies.

Innominate's mGuard security appliances safeguard machines for M2M communication. Application scenarios include the protection and/or secure remote maintenance of networked robots in the automotive industry, production systems in the manufacturing and process industries, medical technology systems, printing machinery, point of sales systems and ATMs, telematics and monitoring systems where the installation of distributed security appliances requires a clearly organised and easy-to-use management tool.

The template-based Innominate Device Manager (IDM) is particularly suitable for the roll out and configuration management of large groups of homogeneously configured mGuard devices. Templates enable the centralisation of settings for several devices at once and typically capture the security-critical and knowledge-intensive portions of device configurations. Via the upload function, all security appliances on the manager's device list can be conveniently configured in one go. Alternatively, the configuration data can automatically be downloaded following the activation of the remote appliance. With the Innominate Device Manager, the roll out of broadly distributed installations involving thousands of appliances can be carried out quickly and efficiently.

With a mouse click, the desired firewall rules and NAT settings can be generated and uploaded to the devices in the network, deploying the desired device configurations in one process. The IDM is a client-server application, the client offering full control of all IDM features, the server storing the configuration in a database, generating configuration files and uploading those files to the devices upon request. If a configuration is uploaded to a device, the IDM generates an (ASCII) configuration file. This configuration is transferred via SSH to the device and is subsequently placed in operation by the Innominate mGuard. Furthermore, the IDM can generate configuration files to be used for a configuration pull by the devices via HTTPS.

IDM client overview

The IDM client is the graphical user interface for accessing all features of the IDM. It allows users to create and manage devices and templates, to initiate the upload of configurations to devices, or to command the export of device configurations to a web server file system.

Application example: mGuard secured remote services

Remote service security is a prominent application area in which mGuard appliances are deployed in order to secure Internet/VPN or dial-up based connections for the remote monitoring, diagnostics, and maintenance of industrial machinery and equipment.

Innominate Device Manager

Architecture ▶	Client/server application for template based device configuration
Scalability ▶	Scales up to 10,000 devices
VPN topology ▶	1:N VPNs or VPN endpoints
Local setup ▶	Yes
Configuration mode ▶	Push and pull configuration with optional status feedback
User interface ▶	Tables and masks

Manufacturers of such equipment with thousands of their systems in the field and hundreds of new systems being shipped each year can apply the IDM to efficiently manage corresponding numbers of mGuard security appliances attached to their machines.

Roll out scenario

Once an experienced network security administrator has put the appropriate IDM configuration templates in place, regular technical staff working on assembly and packaging of the equipment can configure mGuard devices before shipment to end customer premises with only minimal training. In particular, the complexities of configuring VPN connections, digital certificates and virtual addressing schemes are completely taken away at the device level by the IDM's template and combined automation mechanisms. Configuration of a restricted set of variables that may not be known before the actual on-site commissioning phase, such as an available IP address for the external interface to the customer network, may be delegated as so-called local variables to an on-site

technician taking on mGuard's "Network Admin" user role. Once the mGuard appliances are installed in the field, the IDM can continuously be applied to update, maintain and monitor their configuration status over time.

Deploying device configurations from the IDM server to mGuard appliances

1. Configuration push via SSH

The IDM server connects to the mGuard device using the SSH secure shell protocol. Subsequently the configuration file is copied to the device and put into operation. The status and success of the upload process as well as any possible problems are monitored by the IDM server and visualized in the device list in the IDM client. The upload process can be initiated from the IDM client for individual selections of devices or simultaneously for all devices with changed configurations pending upload.

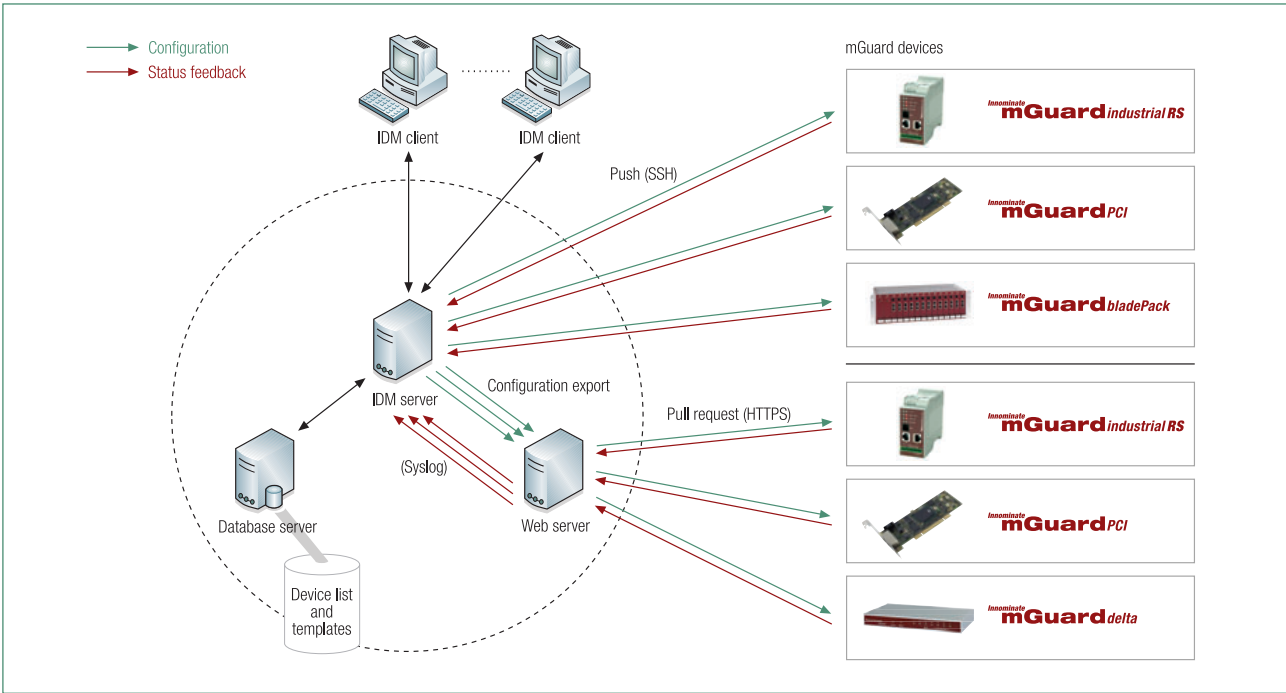
The Template Properties dialog

Templates offer a powerful mechanism for conveniently configuring and managing a large number of devices. Templates contain a selectable subset of mGuard variables and can be assigned to a device.

Once the template is assigned to a device, the device takes over the template settings and will use the values for the mGuard variables. Depending on the permission settings, the template settings could be overridden in the device configuration.

The Device Properties dialog

The Device Properties dialog allows users to configure the mGuard variables and their associated settings for a device. Unlike templates, a device configuration always contains a complete set of mGuard variables.



Configuration of mGuard devices

2. Configuration pull via HTTPS

The IDM server can also be instructed to export new or updated device configurations to a web server file system. The respective mGuard devices themselves can then check for and download available configurations from that web server using the secure HTTPS protocol on a regular schedule or each time they boot. The correctly matching IDM configuration for a device can be identified both by logical management ID or the serial number of the physical device. The process includes an optional mechanism to report successful configuration pulls back from the device via the web server to the IDM server for monitoring purposes.

Both methods may be combined as appropriate, e. g. non-critical configuration updates may be provided for the next configuration pull whereas critical, emergency type updates may be immediately pushed to all available devices.

Configurable mGuard features supported by the Innominate Device Manager

- Control of system settings (host, time and date, shell access)
- mGuard web access
- Configuration pull
- mGuard interfaces (Network mode, Stealth mode settings, external and internal networks, PPPoE settings)
- DNS
- Internal DHCP
- User authentication (local mGuard users): Admin, Network Admin and Audit
- Packet filter (incoming and outgoing rules)
- NAT (masquerading, 1:1 NAT, port forwarding)
- Remote logging to Syslog server
- VPN connections
- Convenient auto-configuration of peer VPN gateway if the peer device is also managed by the IDM
- Integrated Certificate Authority (CA) for VPN authentication with auto-generated X.509 certificates
- Intelligent value pool management, e. g. for auto-assigned unique virtual addresses and networks

Template

A set of mGuard variables and the corresponding values and access privileges. Only one template can be used by a device. A change in the template might be applied to all devices using the template, depending on the access privilege settings. The "template" is used in the IDM only, not on the physical mGuard appliance.

Local (mGuard) variables

Within the IDM (in the Template Properties or the Device Properties dialog) each configuration variable can be designated as "local". Local variables are not managed by the IDM, but are subject to local configuration on the mGuard by the Network Admin user.

Admin/Network Admin/Audit (mGuard user roles)

The role Admin is entitled to change all settings for the mGuard, whereas the role Network Admin can only set variables designated as "local" within the IDM. The role Audit is entitled to read all settings, but not make any modifications (read only).

Management ID

A unique logical identifier independent from the physical hardware that identifies each device, in contrast to an identifier for the physical device, e. g. the serial number.

Minimum System Requirements	Client	Server
Hardware	A minimum of 512 MB RAM 500 MB free hard disk space Color-monitor with at least 1024 x 768 resolution	A minimum of 512 MB RAM 4 GB free hard disk space
Software	Windows 2000 SP 2 (or higher), Windows XP or Linux Java Runtime Environment 5.0	Windows 2000 SP 2 (or higher), Windows XP or Linux Java Runtime Environment 5.0 PostgreSQL Version 8.1