protecting industrial networks

Innominate
Security Technologies

mGuard Device Manager

Release Notes
Version 1.5.2.1
Document Revision 1

Innominate Security Technologies AG
Rudower Chaussee 13
12489 Berlin
Germany
Phone: +49 30 921028 0
Fax: +49 30 921028 020
contact@innominate.com
http://www.innominate.com/

June 2014

All information contained in this documentation is subject to change without previous notice. Innominate offers no warranty for these documents. This also applies without limitation for the implicit assurance of scalability and suitability for specific purposes. In addition, Innominate is neither liable for errors in this documentation nor for damage, accidental or otherwise, caused in connection with delivery, output or use of these documents.

Innominate Document Number: RN301522614-055

Table of Contents

1. Introduction

mGuard Device Manager (mdm) 1.5.2 supports all mGuard devices running firmware versions 5.0.*x*, 5.1.*x*, 6.0.*x*, 6.1.*x*, 7.0.*x*, 7.1.*x*, 7.2.*x*, 7.3.*x*, 7.4.*x*, 7.5.*x*, or 7.6.*x*. All mGuard hardware platforms are supported.

1.1. System Requirements

	mdm Client	mdm Server	mdm CA
Hardware	• A minimum of 512 MB RAM • 500 MB free hard disk space • Color monitor with at least 1280×1024 resolution	• A minimum of 4 GB RAM • 100 GB free hard disk space	• A minimum of 512 MB RAM • 5 GB free hard disk space
Software	• Windows 2000 SP2 / XP (or later), Windows Server 2003 (or later), or Linux • **Java Runtime Environment JRE SE 7**	• Windows 2000 SP2 / XP (or later), Windows Server 2003 (or later), or Linux • **Java Runtime Environment JRE SE 7** • PostgreSQL Version 9.0 (or later)	• Windows 2000 SP2 / XP (or later), Windows Server 2003 (or later), or Linux • **Java Runtime Environment JRE SE 7** • PostgreSQL Version 9.0 (or later)

System requirements that have changed since IDM 1.4.3 are shown in **bold text** in the above table.

2. Version History

2.1. Changes in mdm 1.5.2.1

The 1.5.2.1 release upgrades third-party software installed by the mdm Microsoft Windows installer. It does not upgrade or modify mdm itself in any way.

Third party components are upgraded to the following versions:

- Java Runtime Environment 7u60
- OpenSSL 1.0.1h
- Apache web server 2.4.9

The OpenSSL and Apache web server versions contain **fixes for security vulnerabilities** (CVE-2014-0160, CVE-2014-0224). See Innominate Security Advisory 2014/06/13 for more details.

For customers who installed mdm 1.5.2 with the mdm Microsoft Windows installer, it is strongly recommended to upgrade the installation using the mdm Microsoft Windows installer 1.5.2.1, and to replace the HTTPS web server certificate while doing so, by following the installer's instructions.

2.2. Changes in mdm 1.5.2

The following bug has been fixed:

- The mdm server refused to start after 24 November 2013. (It stopped immediately with the message “Failed to verify license: Certification path could not be validated.”)

2.3. Changes in mdm 1.5.1

The following bugs have been fixed:

- Editing firewall rules in the “sets of rules” or in VPN connections caused sibling tables (i.e. the same table in other sets of rules or VPN connections) to be modified as well.
- Assigning a template to a device was denied for users without write permission for templates.
- Inheritance of the SSH remote access certificate from a template corresponding to firmware version 7.4 or earlier to a template or device corresponding to firmware version 7.5 or 7.6 caused the SSH remote access certificate field to be empty.
- In synthesized (read-only) VPN group connections, “peer device” variables were displayed in the mdm client, although they did not contain sensible values.

2.4. Major Enhancements in mdm 1.5.0

- Innominate Device Manager (IDM) has been renamed to mGuard Device Manager (mdm).
- mdm now supports firmware versions 7.5.*x* and 7.6.*x*.
- mdm can encrypt configuration profiles (for pull configuration) with a device-specific key. This feature is available in firmware version 7.6.*x*.
- mdm can generate *External Configuration Storage* (ECS) files encrypted with a device-specific key. This feature is available in firmware version 7.6.*x*.
- mdm has dedicated support for configuring of the mGuard *rs2000*, which has limited configuration options.
- mdm can import configuration profiles by logging into an existing device (Online ATV Import).
- mdm includes an installer for the following Microsoft Windows Server operating systems:
  - Windows Server 2012 (64 Bit)
  - Windows Server 2008 R2 SP1 Enterprise Edition (64 Bit)
  - Windows Server 2008 SP1 Enterprise Edition (64 Bit)
  - Windows Server 2008 SP1 Enterprise Edition (32 Bit)
  - Windows Server 2003 SP2 Enterprise Edition (64 Bit)
  - Windows Server 2003 SP2 Standard Edition (64 Bit)
  - Windows Server 2003 SP2 Standard Edition (32 Bit)

2.5. Further Enhancements and Bugfixes in mdm 1.5.0

- ATV import works reliably for all supported firmware versions.
- Passwords of the mGuard users *root*, *admin*, *netadmin* and *audit* are stored in hashed form instead of plain text form in configuration profiles generated by mdm. (Note that configuration profiles still contain the previous *root* password in plain text form.)
- mdm can instruct mGuard devices running firmware version 7.5.*x* or newer to generate a new SSH key and a new HTTPS certificate.
- The CRL functionality of the mdm has been improved. CRLs can be generated periodically, and the *Next Update* field can be set.

2.6. Removed Functionality

- mdm 1.5.0 no longer supports firmware versions 4.2.*x*.

3. Upgrading from mdm 1.5.0 or an Earlier IDM Version

Since mdm 1.5.0 and later no longer supports firmware versions 4.2.*x*, all devices and templates must be set to at least firmware versions 5.0 before installing mdm 1.5.2.

To upgrade from an earlier mdm/IDM version to mdm 1.5.2, it is necessary to make irreversible changes to the backing PostgreSQL database. Once these changes have been made, the database can no longer be accessed with an earlier mdm/IDM version.

- **Preparation**
  - Stop the mdm/IDM server if it is running.
  - Dump the content of the mdm/IDM database. The command line tools *`pg_dump`* or *`pg_dumpall`* (part of the PostgreSQL distribution) or another mechanism can be used for this. See the PostgreSQL documentation for details.
  - If the mdm/IDM CA is used, dump the content of the CA database.
  - It is strongly advised to keep a copy of the database dumps as a backup.
- **Upgrade**
  - Install the mdm 1.5.2 server.
  - If upgrading from IDM 1.4.*x* or an earlier IDM version:

    Since the server configuration file *`preferences.xml`* has been extended, it is recommended to use and customize the file provided with mdm 1.5.2. By default, the passwords for the Java trust store, Java key store, and database connection are read from environment variables; set these environment variables accordingly.

    Note that the CA type “IDM-CA” has been renamed to “mdm-CA”. It is necessary to adapt the key *com » innominate » innomms » is » CA » type* in *`preferences.xml`* accordingly or communication with the mdm CA will fail.
  - mdm 1.5.2 requires the Java SE 7 Runtime Environment (JRE). Make sure the *`java`* command refers to a JRE of this version, or use an appropriate pathname to run a Java SE 7 JRE.
  - Invoke the server with the following command:

    ```
    java -Xmx1024m -jar idm_server.jar update preferences.xml
    ```

    The server will connect to the PostgreSQL database, upgrade it, and terminate. After this step, the database is ready to be used by mdm 1.5.2, i.e. the mdm 1.5.2 server can now be started.

4. Usage Hints

4.1. Performance of Creating Configuration History Entries

mdm 1.5.2 creates a configuration history entry for each affected device after every modification to a device, template, or VPN group configuration. Such a modification can therefore be slow, especially if it affects a large number of devices. Further improvements to this process will be made in future mdm versions.

4.2. Caching Behavior of the mdm Server

Any RAM available to the mdm server beyond what it requires is used to cache data. It is therefore normal behavior if the memory usage increases to the configured maximum as soon as there is some activity, and subsequently remains on that level.

4.3. Default Values

If a setting is not configured in mdm, the factory default setting is assumed. It is therefore strongly recommended to configure the mGuard passwords in mdm (mGuard configuration » Authentication » Administrative Users » Passwords). Otherwise, mdm will set them to the factory default passwords.

If SSH configuration uploads from mdm are to be performed via the mGuards' external interfaces, shell access must be configured to allow connections from mdm to the mGuards (mGuard configuration » Management » System Settings » Shell access). No such access is allowed by default.

4.4. Device Credentials / Replacement of Devices

The “Set Current Device Credentials” dialog in the context menu of the device overview table refers to mdm's notion of the device's current passwords and should be used if the passwords have been modified by external means (e.g. through the device's web interface). To change the passwords with mdm, use the Template or Device configuration dialog (mGuard configuration » Authentication » Administrative Users » Passwords) instead.

When a device is physically replaced by a new one with factory default settings, some preparation is necessary before SSH uploads can be performed to the new device. First of all, out of security considerations mdm refuses to upload to a device if its SSH host key has changed, so the host key has to be reset. Secondly, mdm's notion of the device's passwords has to be set to the factory defaults. These steps can be performed in the “Set Current Device Credentials” dialog in the context menu of the device overview table. Check the “root”, “admin”, and “Reset SSH Host Key” boxes and type the “root” and “admin” passwords into the respective fields.

4.5. Effect of Changing Templates

Configuration values that override values in a VPN connection inherited from an ancestor template are retained as long as the ancestor template is assigned. If it is deassigned, or another parent template is assigned, overridden configuration values are lost. Likewise, pool values change when another parent template is assigned.

5. Known Issues and Limitations

5.1. JRE Uses IPv4/IPv6 Dual Network Stack

Issue: The Java Runtime Environment uses an IPv4/IPv6 dual network stack be default. This can cause long delays (several minutes) in an IPv4-only environment. A typical phenomenon is that the mdm client appears to hang after connecting to the mdm server.

Solution: Add *`-Djava.net.preferIPv4Stack=true`* to the Java command line to start the mdm server, client, and CA server.

5.2. JRE Prevents Usage of AES-256 Cipher by Policy

Issue: The Java Runtime Environment has a default policy that prevents Java programs from using the AES-256 cipher. This affects encrypted configuration profiles and ECS files, which mdm encrypts with AES-128 if it is prevented from using AES-256. Note that the generated files are fully interoperable, but only have the limited crypto strength.

Solution: Download unrestricted policy files from

http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html

and install them according to the instructions provided by Oracle.

5.3. Passwords Are Hashed only after Modification

Issue: Passwords of the mGuard users *root*, *admin*, *netadmin* and *audit* are stored in hashed form (instead of plain text form) in configuration profiles only after a device has been modified.

Solution: Modify the device by changing a configuration variable. An indirect modification in a template is sufficient. This step is necessary only once for each device after upgrading from an eralier IDM version.

5.4. Change from Firmware 7.4 to 7.5

Issue: The variable “Network Mode” with the possible values “Stealth”, “Router”, “PPPoE”, “Modem” … and the variable “Obtain external configuration via DHCP” have been replaced with the variable “Network Mode” with the possible values “Stealth” or “Router”, and the variable “Router Mode”. Although this change has been made in mGuard firmware 7.0.0, mdm implements it for firmware 7.5 or newer.

If one of the original variables is defined in a template and the other in an inheriting template or device, the mapping may cause unexpected results, especially if one of the special “Local” or “None” values is involved.

Solution: When changing firmware version 7.4 to 7.5 in mdm, make sure the variables are both defined or both inherited, or adapt the configuration after changing the firmware version.

5.5. Exhausted Pools May Cause Unexpected Errors

Issue: If a pool is exhausted, the may cause unintelligible error messages. Affected devices may become invalid.

Solution: Extend pools before they are exhausted.

5.6. Limitations of Referenced Table Variables

Issue: If a table with content that is referenced from elsewhere (e.g. firewall rulesets) is switched from “Inherited” to “Custom”, referencing variables (e.g. targets in firewall rules) become invalid.

Solution: Set the referencing variables after switching the referenced table from “Inherited” to “Custom”.

5.7. “Local Certificate” Not Displayed in VPN Peer Connection

Issue: If a device with firmware version 7.5 or 7.6 is configured as a VPN peer device, the “Local Certificate” is not displayed in the synthesized VPN connection in the mdm client. The generated configuration is not affected.

Solution: Look up the “Local Certificate” variable in the original device (under the “Configuration of the VPN peer” settings).

5.8. Changing Meshed VPN Configuration Is Slow

Issue: Changing the configuration of a device that is a member of a large VPN mesh (i.e. a VPN group) can take several minutes, during which the mdm server does not respond to further requests from the client. This issue arises when the configuration change affects all devices in the mesh, so that history entries for all of them are generated.

Solution: Wait until the history entries have been written.

5.9. Certificate References in Devices Reconstructed from History

Issue: If a new device is created by reconstructing it from a history entry of an existing device, it can happen that the machine certificate is not properly referenced in the VPN connections in the reconstructed device.

Solution: Set the “Local X.509 Certificate” variable(s) in the reconstructed device.

5.10. PKCS#12 Files Must Be Password Protected

Issue: Machine certificates in PKCS#12 format can only be imported if the PKCS#12 file is protected by a non-empty password.

Solution: If it is necessary to import a machine certificate stored in an unprotected PKCS#12 file, convert it to PEM format first (as described in the User's Manual).

5.11. Automatic Configuration of the VPN Peer Device

Issue: The automatic addition of VPN connection settings to a specifiable “peer device” only works if the peer device has the same or a newer firmware version than the originating device. Otherwise, the VPN connection is silently omitted from the peer device.

Solution: Ensure that the peer device has the same or a newer firmware version than the originating device. It is recommended not to make use of the “peer device” feature, but to use the VPN tunnel group feature.

5.12. Server Preferences Cannot Be Removed

Issue: It is not possible to remove server configuration settings by removing them from the server configuration file *`preferences.xml`*. The contents of the configuration file are copied to a system-specific location upon startup, so removing entries has no effect.

Solution: To override existing settings, specify new values in the configuration file.

5.13. Loss of Connection between mdm Server and Database

Issue: The mdm server does not automatically recover from a loss of the network connection to the database server.

Solution: If the connection is lost, restart the mdm server.

5.14. Local Time Zone

Issue: The Java Runtime Environment fails to recognize the local time zone under some circumstances.

Solution: If the timestamps in the logging panel do not match your system clock, set the environment variable *`TZ`* to the correct time zone description (e.g. *`Europe/Berlin`* for Central European Time) and restart the mdm server and client.

5.15. Microsoft Windows Installer Does Not Set Up Pull Configuration Feedback

Issue: If mdm is installed with the Microsoft Windows installer, and the Windows system is also used as a pull configuration server, there is no feedback to the mdm server when mGuard devices apply configurations pulled from the server.

Solution: This functionality will be provided with a future version of the mdm installer.

5.16. Microsoft Windows Installer Fails to Discover Used TCP Ports

Issue: If mdm is installed with the Microsoft Windows installer, and TCP port 443 (https) or 5432 (PostgreSQL service) are already used by a service, the installation fails (instead of aborting before it has started).

Solution: Remove the service using TCP port 443 or 5432 and restart the mdm installer.

5.17. Microsoft Windows Installer May Display Error Message When mdm Is Uninstalled

Issue: If mdm is uninstalled with the Microsoft Windows installer, an error message that `installer.dll` could not be found may be displayed. This issue occurs only if an installation has been upgraded from version 1.5.2.0 or earlier.

Solution: Click the OK button. The uninstallation process will continue normally.

5.18. Microsoft Windows Installer May Fail to Remove a File When mdm Is Uninstalled

Issue: If mdm is uninstalled with the Microsoft Windows installer, a file `jre\bin\msvcr100.dll` in the installation directory (`C:\Program Files\mGuard Device Manager\jre\bin\msvcr100.dll` by default) may remain. This issue occurs only on 32 bit Windows variants, and only if an installation has been upgraded from version 1.5.2.0 or earlier.

Solution: Remove the remaining file manually.

5.19. Error Message After Uninstalling

Issue: If mdm has been installed with the Microsoft Windows installer, after uninstalling and rebooting the system an error message pertaining to `IDMSvc.exe` may be displayed.

Solution: No user action is required; mdm has been uninstalled successfully. The message is displayed once by the Microsoft Windows operating system and can be ignored.

6. Known mGuard Issues

6.1. VPN Connections with Pre-Shared Secret Authentication

Applicable to: Firmware versions 7.0.0 or later.

Issue: If pre-shared secret authentication is used in a VPN connection, the local certificate must be set to “No certificate” explicitly.

Solution: Configure the VPN connection accordingly.

6.2. VPN Configuration Managed by Netadmin User

Applicable to: Firmware versions 5.0.*x* and 5.1.*x*.

Issue: If configuration variables within the “Tunnel and Transport Settings” of a VPN connection are managed by the Netadmin user on the device (i.e. set to “Local” in mdm), the values set by the Netadmin user are reset to the default values on every configuration upload or pull.

Solution: Upgrade to firmware 6.0.0 or later.

6.3. Firmware Upgrade Incorrectly Reported as Erroneous

Applicable to: Firmware versions 5.0.*x* and 5.1.*x*.

Issue: If a firmware upgrade to version 6.0.*x* is triggered by a configuration pull, the device incorrectly reports a firmware upgrade failure to mdm even if the upgrade succeeded. mdm will indicate an upgrade failure in the device overview table.

Solution: Wait until mdm receives the next configuration pull feedback from the device. This feedback contains the correct status and therefore causes mdm to no longer indicate an upgrade failure.

6.4. mdm Cannot Read Flash ID from Guard during SSH Upload

Applicable to: Firmware version 5.0.0.

Issue: If an SSH configuration upload is performed to a device with firmware version 5.0.0, mdm cannot read back the Flash ID. This prevents licenses from being associated with the device.

Solution: Enter the Flash ID manually in the device configuration dialog, or upgrade to firmware 5.0.1 or later.

6.5. Firmware Upgrade with Automatic Target Version Selection

Applicable to: Firmware versions 5.0.*x,* and 5.1.*x*.

Issue: Firmware upgrades from version 5.1.*x* or earlier with automatic selection of the target version (i.e. upgrades to latest patches, latest minor release, or next major version) are only triggered by a configuration pull if mdm knows the firmware version on the device when exporting the configuration profile. If mdm lacks this information, any scheduled firmware upgrade request remains so until the version on the device is known. Upgrades triggered by an SSH configuration upload are not affected.

Soultion: Enter the firmware version on the device manually in the device configuration dialog.

6.6. SSH Upload Connection Terminated during VPN Reconfiguration

Applicable to: Firmware versions 5.0.*x,* and 5.1.*x*.

Issue: If an SSH configuration upload changes the settings of a large number of VPN connections, mdm declares the SSH connection dead before the upload is complete.

Solution: Increase the SSH timeout values in the server configuration file *`preferences.xml`* when working with a lot of VPN connections.