protecting industrial networks

Innominate
Security Technologies

Innominate Device Manager

Release Notes
Version 1.4.3

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/

Copyright © 2006-2012 Innominate Security Technologies AG

May 2012

“Innominate” and “mGuard” are registered trademarks of Innominate Security Technologies AG. All other brand names or product names are trade names, service marks, trademarks, or registered trade marks of their respective owners.

mGuard technology is protected by the German patents #10138865 and #10305413. Further national and international patent applications are pending.

No part of this documentation may be reproduced or transmitted in any form, by any means without prior written permission of the publisher.

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.

This documentation may not be photocopied, duplicated or translated into another language, either in part or in whole, without the previous written permission of Innominate Security Technologies AG.

Innominate Document Number: RN301432512-038

Table of Contents

1. Introduction....3
1.1. System Requirements....3
2. Version History....3
2.1. Issues Fixed since IDM 1.4.2....3
2.2. Issues Fixed since IDM 1.4.1....3
2.3. Major Enhancements since IDM 1.3.4....4
3. Upgrading from an Earlier IDM Version....5
4. Usage Hints....6
4.1. Performance of Creating Configuration History Entries....6
4.2. Caching Behavior of the IDM Server....6
4.3. Default Values....6
4.4. Device Credentials / Replacement of Devices....6
4.5. Effect of Changing Templates....6
5. Known Issues and Limitations....7
5.1. Changing Meshed VPN Configuration Is Slow....7
5.2. “Accessible via” Setting....7
5.3. Certificate References in Devices Reconstructed from History....7
5.4. Pull Feedback Fails to Update History Entry....7
5.5. Firmware Upgrade Status Icon....7
5.6. ATV Import Requires Manual Adaption....7
5.7. PKCS#12 Files Must Be Password Protected....8
5.8. Automatic Configuration of the VPN Peer Device....8
5.9. Default VPN Connection Type....8
5.10. Server Preferences Cannot Be Removed....8
5.11. Loss of Connection between IDM Server and Database....8
5.12. Local Time Zone....8
5.13. Limited mGuard 4.2 Support....8
6. Known mGuard Issues....9
6.1. VPN Configuration Managed by Netadmin User....9
6.2. Firmware Upgrade Incorrectly Reported as Erroneous....9
6.3. Installation of Licenses during Firmware Upgrade....9
6.4. IDM Cannot Read Flash ID from Guard during SSH Upload....9
6.5. Firmware Upgrade with Automatic Target Version Selection....9
6.6. SSH Upload Connection Terminated during VPN Reconfiguration....10

1. Introduction

Innominate Device Manager (IDM) 1.4.3 supports all mGuard devices running firmware versions 4.2.*x* (with some limitations, cf. section 5.13), 5.0.*x*, 5.1.*x*, 6.0.*x*, 6.1.*x*, 7.0.*x*, 7.1.*x*, 7.2.*x*, 7.3.*x*, or 7.4.*x*. All mGuard hardware platforms are supported.

1.1. System Requirements

	IDM Client	IDM Server	IDM 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 6	• Windows 2000 SP2 / XP (or later), Windows Server 2003 (or later), or Linux • Java Runtime Environment JRE SE 6 • **PostgreSQL Version 9.0 (or later)**	• Windows 2000 SP2 / XP (or later), Windows Server 2003 (or later), or Linux • Java Runtime Environment JRE SE 6 • **PostgreSQL Version 9.0 (or later)**

System requirements that have changed since IDM 1.3.4 are shown in **bold text** in the above table.

2. Version History

2.1. Issues Fixed since IDM 1.4.2

- A bug in 32 bit versions of the Java Runtime Environment that could cause the communication between the IDM server and client to fail is no longer triggered.
- A bug that required a restart of the IDM client after viewing device configuration history entries has been fixed.
- A bug that could cause the import of devices from a “comma-separated values” (CSV) file to fail has been fixed.

2.2. Issues Fixed since IDM 1.4.1

- Changes to the “active root password” (i.e. the root password a device has according to the knowledge of the IDM) are now properly taken into account. Changing the active root password either through the “Set Current Device Credentials” menu action or by uploading a configuration with a modified root password now works correctly.
- A bug that could cause the overview table filter in the IDM client to become unusable if a filter was already in effect when logging into the IDM server has been fixed.
- The error that was sometimes logged when closing a configuration dialog no longer appears. (The logged error has been a “false positive” even in earlier IDM versions, i.e. it has been confusing, but has not had any impact on the functionality.)

- A bug that could cause the IDM client to unsolicitedly disconnect from the IDM server under rare circumstances has been fixed.
- A bug that prevented IDM from accessing the Windows Registry on Microsoft Windows 7 systems with enabled User Account Control (UAC) has been fixed. It could affect both the IDM server and the IDM client.
- The performance of storing modifications that affect a large number of devices or VPN connections (e.g. modifications to the central gateway device in a 1:N VPN network) has been enhanced.
- Interoperability with the “Microsoft Windows Server 2008 R2 NDES” service (via SCEP) has been enhanced:
  - The IDM server can now successfully enroll certificates if the NDES is operated as a sub-CA instead of a root-CA.
  - The RA certificates that are contained in the reply of the NDES to the IDM server, but are not part of the certificate chain, are no longer stored in the device.
- The “Web Configure” menu action now opens redundancy pairs with a single web browser invocation. This prevents the situation that both devices could be loaded into the same browser window in short succession, so that in effect only one was visible to the user.

  The recommended browser command for users of Firefox is `firefox {-new-tab url}`. It has the effect that if the Firefox browser is already running, a new tab is opened for each device. This is now the default in new IDM installations; upgrading users may consider opening the “Options » Default Browser” dialog and setting the browser command accordingly.

2.3. Major Enhancements since IDM 1.3.4

- IDM now supports firmware versions 7.0.*x*, 7.1.*x*, 7.2.*x*, 7.3.*x*, and 7.4.*x*.
- If two devices form a redundancy pair, the pair can be configured like a single device in IDM. The values of most configuration variables need to be entered only once.
- Every time a device configuration is changed directly or indirectly (e.g. by editing a template), IDM creates a history entry containing the resulting configuration of the device. History entries can be viewed, compared, or used to reconstruct a device containing the historic configuration.
- A HTML report listing the configuration differences between two points in time of an arbitrary number of devices can be generated.
- Fully or partially meshed VPN networks can be configured automatically. Similar to the “automatic configuration of the VPN peer” feature to support 1:N VPN networks, IDM adds VPN connections to the participating device configurations to establish a meshed VPN network.
- If IDM manages the X.509 certificates to be used in a VPN connection, it can now set the VPN identifiers (needed if CA certificate authentication is used) automatically.
- As an alternative to the IDM CA server, IDM can use SCEP (Simple Certificate Enrollment Protocol) to request X.509 certificates from a CA server.
- IDM now supports offline X.509 certificate generation. Certificate signing requests can be exported for a number of devices; the user generates certificates and re-imports them into IDM. During the re-import, the certificates are automatically assigned to the correct devices.
- IDM now uses a role-based approach to administer user permissions.

- IDM users can be authenticated through the RADIUS protocol.
- IDM supports configuration uploads to mGuards that authenticate through the RADIUS protocol.
- Server events are logged persistently (i.e. in the IDM database). They can optionally also be sent to a remote syslog server.
- Templates can have a default inheritance permission that affects all configuration variables set to “Inherited”.
- The “Accessible via” address (i.e. the address to which IDM uploads) is now available in the template configuration in addition to the device configuration. If e.g. all uploads are performed to the respective first external IP addresses of the devices, this can easily be configured in a common template. See also section 5.2.

3. Upgrading from an Earlier IDM Version

To upgrade from an earlier IDM version to IDM 1.4.3, 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 IDM version. Furthermore, IDM 1.4.3 requires PostgreSQL version 9.*x*, while IDM 1.3.*x* and earlier IDM versions require PostgreSQL version 8.*x*. It is therefore necessary to upgrade PostgreSQL as well.

- Stop the IDM server if it is running.
- Dump the content of the 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 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.
- Install PostgreSQL 9.*x*. Restore the content of the IDM database and the CA database (if applicable) from the dumps. The command line tool `psql` or another mechanism can be used for this. See the PostgreSQL documentation for details.
- Install the IDM 1.4.3 server. Since the server configuration file `preferences.xml` has been extended, it is recommended to use and customize the file provided with IDM 1.4.3. 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.
- IDM 1.4.3 requires the Java SE 6 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 6 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 IDM 1.4.3, i.e. the IDM 1.4.3 server can now be started.
- The first time the server is started after an upgrade from IDM 1.3.4 or an earlier version, it creates one initial configuration history entry for each device. This process can take a long time (typically 30 minutes per 1000 devices in the database) during which it is not possible to connect to the server with an IDM client. Subsequent server starts will not be affected.

4. Usage Hints

4.1. Performance of Creating Configuration History Entries

IDM 1.4.*x* 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 slower than in previous IDM versions, especially if it affects a large number of devices. Improvements to this process will be made in future IDM versions.

4.2. Caching Behavior of the IDM Server

Any RAM available to the IDM 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 IDM, the factory default setting is assumed. It is therefore strongly recommended to configure the mGuard passwords in IDM (mGuard configuration » Authentication » Administrative Users » Passwords). Otherwise, IDM will set them to the factory default passwords.

If SSH configuration uploads from IDM are to be performed via the mGuards' external interfaces, shell access must be configured to allow connections from IDM 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 IDM'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 IDM, 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 IDM refuses to upload to a device if its SSH host key has changed, so the host key has to be reset. Secondly, IDM'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. 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 IDM server is not responsive. 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.

5.2. “Accessible via” Setting

Issue: If “Accessible via” was set to “External interface address”, “Internal interface address”, or “Stealth management address” in IDM 1.3.*x*, the upgrade to IDM 1.4.3 replaces it with the actual IP address.

Solution: No immediate action is required since the actual address does not change. Since IDM 1.4.3 supports “Accessible via” as a template setting, it is recommended to set it to “External interface address”, “Internal interface address”, or “Stealth management address” in a template if that is applicable.

5.3. 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.

5.4. Pull Feedback Fails to Update History Entry

Issue: If the IDM server receives feedback from a configuration pull, it does not update the corresponding history entry to reflect the new state of the device.

Solution: The device state cannot be recovered. However, the information that a profile for configuration pull has been exported is correctly recorded in the configuration history.

5.5. Firmware Upgrade Status Icon

Issue: If an error occurs during an mGuard firmware upgrade, the “F” (firmware) status in the device overview table is not switched to the error icon.

Solution: The state is indicated correctly in the “U” (Upload) status, which is switched to the “Firmware upgrade failed” state.

5.6. ATV Import Requires Manual Adaption

Issue: If an ATV profile from an mGuard running a firmware version 7.0.*x* to 7.4.*x* is imported into an IDM device or template, some configuration variables (Network mode, IP and netmask of the internal and external interface, Quality of Service queue names) are not set properly.

Solution: Check the device or template configuration after the import and set variables that do not have the expected value manually.

5.7. 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).

5.8. 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 with firmware 5.0.*x* or newer, but to use the VPN tunnel group feature.

5.9. Default VPN Connection Type

Issue: The default VPN connection type is “Transport” in firmware version 4.2.*x*, while it is “Tunnel” in later firmware versions. When a device is upgraded from version 4.2.*x*, any VPN connection types that have not been set explicitly (i.e. that are “Inherited” in the device and all its ancestor templates) therefore change from “Transport” to “Tunnel” silently.

Solution: Set the VPN connection type explicitly before upgrading from firmware version 4.2.*x*.

5.10. 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.

5.11. Loss of Connection between IDM Server and Database

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

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

5.12. 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 IDM server and client.

5.13. Limited mGuard 4.2 Support

Issue: IDM supports only a subset of the settings in the 4.2.*x* firmware. Later firmware versions are fully supported.

Solution: Upgrade to a later firmware version, or use the “Additional ATV include” field in the device configuration dialog.

6. Known mGuard Issues

6.1. 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 IDM), 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.

6.2. 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 IDM even if the upgrade succeeded. IDM will indicate an upgrade failure in the device overview table.

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

6.3. Installation of Licenses during Firmware Upgrade

Applicable to: Firmware versions 4.2.0, 4.2.1, 4.2.2.

Issue: Attempts to initiate a firmware upgrade from version 4.2.0, 4.2.1, or 4.2.2 to any later version with IDM will fail to install the required licenses on the device even if they are available within IDM.

Solution: Upgrade to firmware 4.2.3 first.

6.4. IDM 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, IDM 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 4.2.*x*, 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 IDM knows the firmware version on the device when exporting the configuration profile. If IDM 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 4.2.*x*, 5.0.*x,* and 5.1.*x*.

Issue: If an SSH configuration upload changes the settings of a large number of VPN connections, IDM 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.