

RELEASE NOTES for Innominate Device Manager 1.3.0

=====

Copyright © 2006-2008 Innominate Security Technologies AG

Innominate Device Manager (IDM) 1.3.0 supports all mGuard devices running firmware version 4.2.x (with some limitations; see below), 5.0.x, 5.1.x, or 6.0.x.

Major Enhancements since IDM 1.2.0

Templates can now be assigned to other templates, so that arbitrarily deep template inheritance hierarchies can be constructed («multilayer template inheritance»).

Configuration profiles can be imported into devices or templates. This feature works for profiles downloaded from a device via web interface as well as profiles exported by IDM. Note that a configuration profile does not contain the full information about variable inheritance permissions, so the import process may not reconstruct the permissions exactly.

The usability of the device/template/pool overview tables has been improved. The table filters now remember the history of the last regular expressions entered. The width, position, and filter criterion of each column is stored in the database as a per-user setting.

IDM now supports firmware version 6.0.x.

Upgrading from an earlier IDM Version

To upgrade from any earlier IDM version to IDM 1.3.0, 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 the earlier IDM version.

Stop the IDM server if it is running.

It is strongly advised to create a backup copy of the IDM database before the upgrade. The command line tool »pg_dump« (part of the PostgreSQL distribution) or another mechanism can be used for this. See the PostgreSQL documentation for details.

It is recommended to upgrade the PostgreSQL database server software to the latest version (8.3.1). Security issues have been found in some earlier versions; see »<http://www.postgresql.org/about/news.905>« for details. Although IDM does not make use of the affected functionality, its database might still be vulnerable if the PostgreSQL server operates databases of other products.

Install the IDM 1.3.0 server. Since the server configuration file »preferences.xml« has been extended, it is recommended to use and customize the file provided with IDM 1.3.0. 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 1.3.0 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 -Xmx256m -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 1.3.0, i.e. the IDM 1.3.0 server can now be started.

Issues during Upgrade from an earlier IDM Version

Some default configuration values have been changed to the values that the mGuard uses by default. In particular, the SNMP system name is now empty by default, and the default DynDNS server is now »dyndns.example.com«. If these values are left unconfigured (»Inherited«), affected devices will have a configuration status (»C« column in the device overview table) of »changed« after the first configuration upload with IDM 1.3.0.

Known Issues

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

The automatic addition of VPN connection settings to a specifiable »peer device« only work 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. 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.

The default VPN connection type is »Transport« in firmware version 4.2, while it is »Tunnel« in later firmware versions. When a device is upgraded from version 4.2, any VPN connection types that have not been set explicitly (i.e. that are inherited in both template and device) therefore change from »Transport« to »Tunnel« silently. Similarly, if the »peer device« feature is used between devices with different firmware versions, the connection type must be set explicitly.

The IDM server does not automatically recover from a loss of the connection to the database server. If the connection is lost, it is necessary to restart the IDM server. The connection between the IDM CA server and the database server as well as the connection between the IDM server and the IDM CA server are recovered automatically after a connection loss.

The »Location« column in the device overview displays the location as specified on the mGuard configuration > Management > System settings > Host > SNMP information page in the Device configuration dialog. If a device inherits the location setting from a template, it is not shown in the device overview.

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

If two or all three of the »Stealth management IP address«, »IP of external interface«, and »IP of the internal interface« settings have the same value, and if the »Accessible via« combobox references one of

these values, changes to one of the values can silently change the »Accessible via« setting. This change is not reflected in the device configuration dialog until it is closed and reopened. The issue can be prevented by appending the string »:22« (i.e. the SSH port number) to the »Accessible via« value.

Known mGuard Issues

In firmware versions 5.0.x and 5.1.x, if configuration variables within the Tunnel and Transport Settings of a VPN connection are managed by the Network Admin user on the device (i.e. set to »Local« in IDM), the values set by the Network Admin user are reset to the default values on every configuration upload or pull. Users of »Local« Tunnel and Transport Settings should upgrade their devices to version 6.0.0 or later.

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 until it receives the next configuration pull feedback from the device.

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. Please upgrade to firmware version 4.2.3 first.

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 unless the Flash ID is entered manually in the Device configuration dialog. No other supported firmware version is affected.

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.

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. It is recommended to increase the SSH timeout values in the server configuration file »preferences.xml« when working with a lot of VPN connections.

If the »Additional ATV include« field on the mGuard configuration > General settings page in the Device configuration dialog is used to override the values of variables set in the configuration dialog with different values, the device will restart all services dependent on such variables during every reconfiguration, even if the overridden values have not changed.

Usage Hints

If a device or template configuration inherits VPN connections from an ancestor template, it is necessary to switch the »IPsec Connections« table from »Inherited« to »Custom« or »Custom+Locally appendable« before

the connection configurations can be edited. Likewise, this step is necessary for the »Tunnel and Transport Settings« table with a VPN connection.

Configuration values which 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.

If a configuration variable is set to »None«, its value must be set in an inheriting template or device configuration. Blue exclamation mark icons and blue tree node labels in the configuration dialog indicate that this requirement has not yet been fulfilled.

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 > Local Users). 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.

The »Set Current Device Passwords« dialog in the context menu of the »Devices« tab 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 > Local Users) instead.

When a device is replaced by a new one with factory default settings, two steps are 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 hostkey has changed, so the hostkey has to be reset through the »Reset SSH Hostkey« entry in the context menu of the »Devices« tab. Secondly, the »Set Current Device Passwords« entry in the same context menu must be used to set IDM's notion of the device's passwords to the factory defaults, i.e. »root« for the root account and »mGuard« for the admin account.

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

If the dialog opening when creating a new device or template is canceled, the device or template is nevertheless created (with default settings).