

RELEASE NOTES for Innominate Device Manager 1.2.0

=====

Innominate Device Manager (IDM) 1.2.0 supports all mGuard devices running firmware version 4.2.x (with some limitations; see below), 5.0.x, or 5.1.x.

Major Enhancements since IDM 1.1.x

-----

The usability of the IDM client has been improved. This affects the device and template configuration dialogs in particular. The meta information associated with each configuration variable (i.e. whether it is inherited, whether it is local to or appendable by the »netadmin« user on the device) is selected from a single combobox. The variable inheritance permission within IDM (i.e. »may override«, »may append«, »no override«) is selected from a separate combobox.

Every configuration setting of 5.0.x and 5.1.x devices can be managed with IDM.

Devices can be instructed to perform a firmware upgrade.

IDM 1.2.0 can manage user logins. Users can be added, modified, and removed. For each user, access permissions for devices, templates, pools, and user management can be configured.

License vouchers and mGuard licenses can be managed with IDM 1.2.0. Vouchers are redeemed at the Innominate license server upon user request; the issued licenses are automatically associated with the corresponding device configurations. Alternatively, existing license files can be imported into IDM. Licenses are installed on the corresponding devices when a SSH configuration upload or a pull configuration is performed.

Bulk creation of devices can be performed by importing a CSV (comma separated values) file.

SSH configuration uploads and pull configuration exports can be scheduled to be performed at a future time. Additionally, a timeout for these activities can be specified to account for fixed service/maintenance windows.

Upgrading from an earlier IDM Version

-----

To upgrade from any earlier IDM version to IDM 1.2.0, 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.

Install the IDM 1.2.0 server. Since the server configuration file »preferences.xml« has been extended, it is recommended to use and customize the file provided with IDM 1.2.0. 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.

Invoke the server with the following command:

```
java -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 1.2.0, i.e. the IDM 1.2.0 server can now be started.

The database upgrade automatically creates a new IDM user »root« with password »root«. This user has full access to all devices, templates, and pools, as well as to the user management functionality. It is therefore strongly recommended to change the password of the »root« user immediately after the database upgrade.

#### Known Issues

-----

IDM supports only a subset of the settings in the 4.2.x firmware. Firmware versions 5.0.x and 5.1.x 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 firmware versions 5.0 and 5.1. 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 »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).

If an IDM user is deleted and recreated without clicking the »Apply« or »OK« button between the two steps, an error occurs. Please click the »Apply« button before recreating the user.

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

-----

Attempts to initiate a firmware upgrade from version 4.2.0, 4.2.1, or 4.2.2 to any 5.0.x or 5.1.x. 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 a 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 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 a SSH configuration upload to a device running firmware version 4.2.x or 5.0.x 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.

#### Usage Hints

-----

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).