RELEASE NOTES for Innominate Device Manager 1.1.2

Innominate Device Manager (IDM) 1.1.2 supports all mGuard devices running firmware version 4.2.x or 5.0.x.

The following device settings can be configured with IDM 1.1.2:

- System Settings (Host, Time and Date, Shell access)
- Web access
- Configuration pull
- Network Interfaces (Network mode, Stealth mode settings, External and internal networks, PPPoE settings)
- DNS
- Internal DHCP
- User authentication (Local users)
- Packet filter (Incoming and outgoing rules)
- NAT (Masquerading, 1:1 NAT, Port forwarding)
- IPsec VPN configuration
- Remote logging

A configuration profile fragment ("atv include") can be associated with each device to perform settings that IDM does not yet support directly.

When devices running firmware version 5.0.x are managed with IDM 1.1.2, the new features of this firmware version are not yet supported.

Changes from IDM 1.1.1 to IDM 1.1.2

IDM 1.1.2 is a "point release" which adds support for firmware version 5.0.x (without supporting the new features of this firmware version):

- The format of the feedback sent by the device when using pull configuration has changed since firmware version 4.2.x. IDM 1.1.2 supports the old and the new format. It is automatically detected which format is being sent.

Changes from IDM 1.1.0 to IDM 1.1.1

IDM 1.1.1 is a "point release" which fixes the following bugs that have been discovered in version 1.1.0:

- The amount of memory that the IDM client consumes when a device with a large number of VPN connections is opened has been reduced.

- If the VPN peer device setting was overridden in a VPN connection inherited from a template, the overriding value was not always stored in the database. This bug has been fixed.

- Deleting a VPN connection sometimes failed. This bug has been fixed.

- Devices and templates do not remain "locked" if the connection between IDM server and client is interrupted unexpectedly.

- If a device which has VPN peers is deleted, the configuration state of the (former) peers is set to "changed".

- Typos in the User’s manual have been corrected.

- The IDM CD now contains the "OpenSSL" package required to set up the CA server.

One enhancement has been made:

- The VPN connection name in peer devices now includes the Management ID of the originating device.

Major Enhancements since IDM 1.0.0

IDM 1.1.2 allows the configuration of single VPN endpoints or VPN tunnels between two devices. The interface to configure VPN endpoints is similar to the "IPsec VPN" menu in the mGuard’s web interface.

If both endpoints are managed by IDM, the VPN tunnel properties need to be set in only one Device or Template Properties dialog. It is possible to specify a "peer device" for which the VPN configuration is automatically synthesized. Settings of the VPN configuration of the peer device that cannot automatically be deduced must be set manually to make use of this feature; the Device and Template Properties dialogs contain special "Configuration of peer device" sections for this purpose.

IDM 1.1.2 includes a CA (Certification Authority) server which allows generating X.509 certificates and corresponding private keys. The CA server makes it possible to manage complete IPsec VPN tunnel configuations within IDM; no external tools are necessary to generate keys and certificates.

To support the configuration of VPN tunnels in a 1:N topology, IDM 1.1.2 can draw IP addresses or networks from value pools. Each tunnel automatically uses a different address or network from a set of values found in a previously defined pool.

Upgrading from an Eariler IDM Version

To upgrade from an earlier IDM version to IDM 1.1.2, 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 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 "pd_dump" (part of the PostgreSQL distribution) or another mechanism can be used for this. See the PostgreSQL documentation for details.

Install the IDM 1.1.2 server. Since the server configuration file "preferences.xml" has been extended, it is recommended to use and customize the file provided with IDM 1.1.2. 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.

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 1.1.2, i.e. the IDM 1.1.2 server can now be started.

Known Issues

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 Properties dialog. If a device inherits the location setting from a template, it is not shown in the device overview.

To configure a table to which the "netadmin" user on the mGuard is allowed to append rows, it is necessary to select both the "local variable" and "table is appendable" checkbox in the Device Properties. Selecting "table is appendable", but not "local variable" has no effect.

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.

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 > User 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 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 Properties dialog (mGuard configuration > User 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 device in the device overview. Secondly, the "Set current 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" (on devices running Innominate firmware) or "private" (on devices running Hirschmann firmware) for the admin accout.

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).