

# Innominate mGuard v4.x

## Update, Recovery and Flash Procedure



*mGuard smart*



*mGuard PCI*



*mGuard blade*



*mGuard industrial*



*mGuard delta*

© Innominate Security Technologies AG

July 2006

“Innominate” and “mGuard” are registered trademarks of the 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: 574009-201

## Table of Contents

<b>1</b>	<b>In which case do I need to execute which procedure?</b>	<b>4</b>
1.1	<i>Update Procedure</i>	4
1.2	<i>Recovery Procedure</i>	4
1.3	<i>Flash Procedure</i>	4
<b>2</b>	<b>Where is the Rescue Switch located?</b>	<b>5</b>
<b>3</b>	<b>Update Procedure</b>	<b>6</b>
3.1	<i>How to retrieve the currently installed firmware version</i>	6
3.2	<i>Online Update</i>	6
3.2.1	Configuring the Update Server	6
3.2.2	Automatic Update	7
3.2.3	Online (Manual) Update	7
3.3	<i>Local (Offline) Update</i>	8
<b>4</b>	<b>Recovery Procedure</b>	<b>9</b>
<b>5</b>	<b>Flash Procedure</b>	<b>10</b>
5.1	<i>Prerequisites</i>	10
5.2	<i>Windows Client and DHCP-/TFTP Server setup</i>	10
5.3	<i>Flash Process</i>	13

## 1 In which case do I need to execute which procedure?

### 1.1 Update Procedure

The *Update* procedure is used for updating the mGuard to a newer firmware release. This will be done user friendly through the web interface. The update can be installed offline as well as online. If possible, the online update should be the preferred method.

The purchase of mGuard security appliances entitles our customers to 180 days software update free of charge upon registration. Please register through our homepage ([www.innominate.com](http://www.innominate.com), *Services -> Registration Software Updates*) for obtaining the login account. After the initial 180 days a **Software Maintenance Contract** may be purchased from your dealer.

### 1.2 Recovery Procedure

You need to perform the *Recovery* procedure if the internal IP of the mGuard (*Router*, *PPPoE*, *PPTP* mode) or if the management IP (*Stealth* mode) is unknown. In those cases you won't have access to the user interface of the mGuard, neither through the web browser nor through SSH. The *Recovery* procedure will also remove SSH access rules and enable internal HTTPS access.

The *Recovery* procedure will reset the **mGuard delta** and the **mGuard blade control unit** into *Router* mode and the internal IP to 192.168.1.1. Those devices will be accessible again through <https://192.168.1.1>.


All other products (**mGuard smart**, **mGuard industrial**, **mGuard blade** and **mGuard PCI**) will be reset into *Stealth* mode. These devices will be accessible again through <https://1.1.1.1>.

The *Recovery* procedure won't affect current configured VPN connections, firewall settings or passwords, only the SSH and HTTPS access rules as mentioned above.

### 1.3 Flash Procedure

You only need to flash the firmware of the mGuard if the root password is unknown. **Note that this procedure will erase existing configurations on the mGuard.** The mGuard will be restored to the factory default settings, also the passwords. You need to reconfigure the mGuard after flashing the firmware.

---

 **Note:** If you want to update the version of the firmware, the *Update* procedure should be the preferred method.

---

## 2 Where is the Rescue Switch located?

The **Rescue Switch** is used for executing one of the following options:

- Reboot of the device.
- Perform the *Recovery* procedure.
- Start the *Flash* procedure.



**mGuard smart**



**mGuard PCI**



**mGuard blade**



**mGuard industrial**



**mGuard delta**

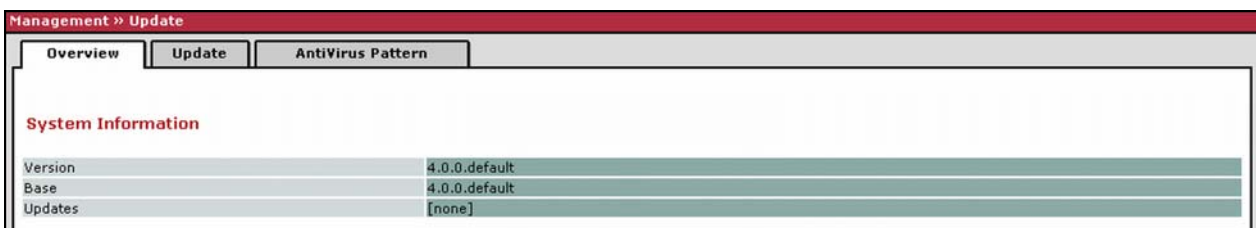
### 3 Update Procedure

The firmware of the mGuard can be updated user friendly through the web interface. The update can be installed locally (offline) as well as online through the Internet. If possible, the online update should be the preferred method.

The purchase of mGuard security appliances entitles our customers to 180 days software update free of charge upon registration. Please register through our homepage ([www.innominate.com](http://www.innominate.com), *Services -> Registration Software Updates*) for obtaining the login account. After the initial 180 days a **Software Maintenance Contract** may be purchased from your dealer.

#### 3.1 How to retrieve the currently installed firmware version

Go to the menu **Management -> Update**, tab **Overview**. The currently installed version is displayed in the line *Version*. *Base* informs about the version which was installed when you have received the device and *Updates* about the installed updates.




The screenshot shows the 'Management >> Update' section with the 'Update' tab selected. Under 'System Information', the following details are listed:

Version	4.0.0.default
Base	4.0.0.default
Updates	[none]

#### 3.2 Online Update

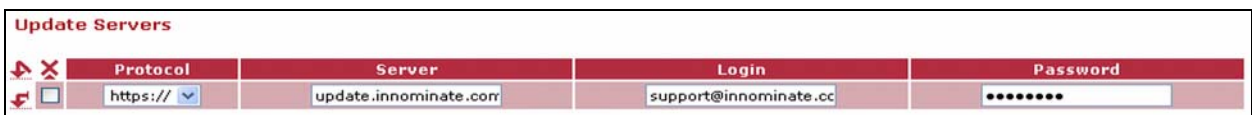
---

 **Note:** The mGuard must have access to the Internet for performing the online update.

---

##### 3.2.1 Configuring the Update Server


- Go to the menu **Management -> Update**, tab **Update**.
- In the section *Update Servers*, select **https://** as *Protocol* and specify **update.innominate.com** as update server.
- Enter your login parameters (*user/password*) for accessing the download area as stated in our response mail to your registration.



The screenshot shows the 'Update Servers' configuration table with the following entries:

	Protocol	Server	Login	Password
<input checked="" type="checkbox"/>	https://	update.innominate.com	support@innominate.cc	*****

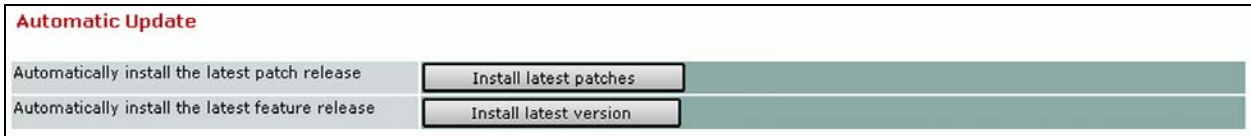
---

 **Note:** The login (username) and password are case sensitive. You need to enter them as stated in our response mail to your registration.

---

### 3.2.2 Automatic Update

- Go to the menu **Management -> Update**, tab **Update**.
- Click either **Install latest patches** for updating the device within one major release version (e.g. from 4.0.0 to 4.0.1) or click **Install latest version** for updating to the next major release (e.g. from 4.x.x to 5.x.x).

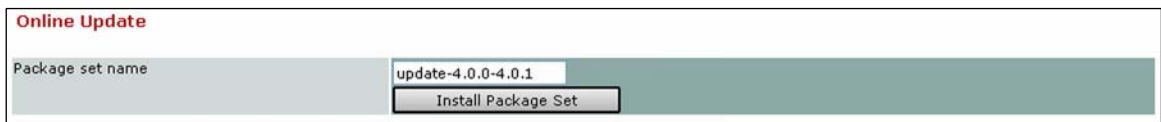


### 3.2.3 Online (Manual) Update

Due to the *Automatic Update* this option is obsolete but it is still available in version 4.x for maintaining the backward compatibility. This option might be removed in a future release.

- At first you need to retrieve the firmware version which is currently installed on the device (refer to chapter 3.1 *How to retrieve the currently installed firmware version*).
- Check our homepage ([www.innominat.com](http://www.innominat.com), *Download -> Updates*) for the latest released version. If there is no update from the device's current version to the latest release available, for example from v3.0.0 to v4.0.1, you need to update the device step by step, from v3.0.x to v3.1.1 and then from v3.1.x to v4.0.1.
- Go to the menu **Management -> Update**, tab **Update**.
- In the section *Online Update*, enter as **Package Set Name** the name of the update package which should be installed. The format of the package set name is as follows:

**update-<current version>-<target version>**, e.g. update-4.0.0-4.0.1.



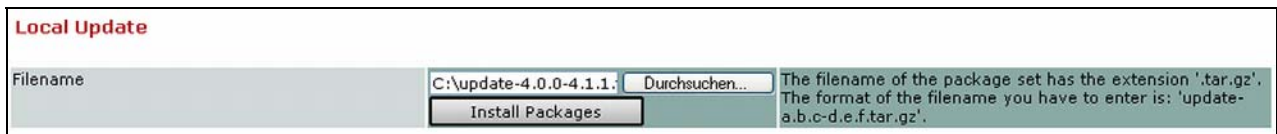
The appropriate *Package Set Name* can be obtained from our homepage ([www.innominat.com](http://www.innominat.com), *Download-> Updates*):



- Click **Install Package Set**.
- ⇒ The Online Update is started.
- Examine the output.
  - When the update is finished, reboot the device if prompted.

### 3.3 Local (Offline) Update

- At first you need to retrieve the firmware version which is currently installed on the device (refer to chapter 3.1 *How to retrieve the currently installed firmware version*).
- Check our homepage ([www.innominat.com](http://www.innominat.com), *Download -> Updates*) for the latest released version. If there is no update from the device's current version to the latest release available, for example from v3.0.0 to v4.0.1, you need to update the device step by step, from v3.0.x to v3.1.1 and then from v3.1.x to v4.0.1.
- Download the appropriate update file (e.g. update-4.0.0-4.0.1.tar.gz) from our homepage. You don't need to extract the files. This will be done automatically by the mGuard.
- Verify that the file extension of the downloaded file is \*.tar.gz. Sometimes the Microsoft Internet Explorer saves the file as \*.tar.tar which is an unusable format for the mGuard. In this case you'll get the error message "**tar: Invalid gzip magic**".
- Go to the menu **Management -> Update**, tab **Update**.
- In the section *Local Update*, click **Browse** and specify the downloaded update file.



**Local Update**

Filename

The filename of the package set has the extension '.tar.gz'.  
The format of the filename you have to enter is: 'update-a.b.c-d.e.f.tar.gz'.

- Click **Install Packages**.
- ⇒ The update is started.
- Examine the output.
  - When the update is finished, reboot the device if prompted.

## 4 Recovery Procedure

The *Recovery* procedure will reset the **mGuard delta** and the **mGuard blade control unit** into *Router* mode and the internal IP to 192.168.1.1. Those devices will be accessible again through <https://192.168.1.1>.

All other products (**mGuard smart**, **mGuard industrial**, **mGuard blade** and **mGuard PCI**) will be reset into *Stealth* mode. These devices will be accessible again through <https://1.1.1.1>.

The *Recovery* procedure will also remove SSH access rules and enable internal HTTPS access.

The *Recovery* procedure won't affect current configured VPN connections, firewall settings or passwords, only the SSH and HTTPS access rules as mentioned above.

- Press the **Rescue Switch** slowly 6 times (once per second).

⇒ The response of the device depends on the used product:


<b>mGuard smart</b>	<ul style="list-style-type: none"> <li>- The middle LED switches off for one second.</li> <li>- The middle LED lights green for one second.</li> <li>- Finally the middle LED starts flickering green.</li> </ul>
<b>mGuard PCI &amp; mGuard blade</b>	<ul style="list-style-type: none"> <li>- The red WAN LED will flash 6 times.</li> <li>- The red LAN LED will flash once.</li> </ul>
<b>mGuard industrial</b>	<ul style="list-style-type: none"> <li>- The <i>Status</i> LED switches off for one second.</li> <li>- The <i>Status</i> LED lights orange for one second.</li> <li>- Finally the <i>Status</i> LED light green.</li> </ul>
<b>mGuard delta</b>	<ul style="list-style-type: none"> <li>- The <i>Status</i> LED switches off for one second.</li> <li>- The <i>Status</i> LED lights green for one second.</li> <li>- Finally the <i>Status</i> LED starts flickering green.</li> </ul>

- Press the **Rescue Switch** slowly 6 times (once per second) again.

⇒ The response of the device depends on the used product:

<b>mGuard smart</b>	<ul style="list-style-type: none"> <li>- The middle LED switches off for one second.</li> <li>- The middle LED lights green for one second.</li> <li>- The device reboots. The middle LED lights red briefly.</li> </ul>
<b>mGuard PCI &amp; mGuard blade</b>	<ul style="list-style-type: none"> <li>- The device will perform a reboot.</li> </ul>
<b>mGuard industrial</b>	<ul style="list-style-type: none"> <li>- The <i>Status</i> LED switches off for one second.</li> <li>- The <i>Status</i> LED lights orange for one second.</li> <li>- The device reboots. The <i>Fault</i> LED lights red until the device is ready.</li> </ul>
<b>mGuard delta</b>	<ul style="list-style-type: none"> <li>- The <i>Status</i> LED switches off for one second.</li> <li>- The <i>Status</i> LED lights green for one second.</li> <li>- The device reboots.</li> </ul>

---


 **Note:** If the mGuard is in *Stealth* mode and the specified default gateway is not reachable because the external interface of the mGuard is not connected to the network, you need to assign a static MAC address to the IP address of the default gateway by using the arp command (e.g. arp -s <IP address of the default gateway> aa-aa-aa-aa-aa-aa). Otherwise the mGuard won't be accessible through <https://1.1.1.1>. Please refer to the *mGuard User's Manual* for further information.

---

## 5 Flash Procedure

You only need to flash the firmware of the mGuard if the root password is unknown. **Note that this procedure will erase existing configurations on the mGuard.** The mGuard will be restored to the factory default settings, also the passwords. You need to reconfigure the mGuard after flashing the firmware.

---

 **Note:** If you want to update the version of the firmware, the *Update Procedure* should be the preferred method.

---

**ATTENTION: Do not interrupt the power supply when the flashing procedure is running. Otherwise the device could be damaged, may be left inoperable, and may require your device to be sent to the manufacturer.**


### 5.1 Prerequisites

The following data/programs must be located on the client you want to use for flashing the mGuard. You may copy them from the mGuard CD or download them from our homepage ([www.innominat.com](http://www.innominat.com), *Download -> Firmware*).

1. The image software (install.p7s and jffs2.img.p7s) of the desired firmware version.
2. Windows: TFTP-/DHCP-Server (tftpd32.exe).

The purchase of mGuard security appliances entitles our customers to 180 days software update free of charge upon registration. Please register through our homepage ([www.innominat.com](http://www.innominat.com), *Services -> Registration Software Updates*) for obtaining the login account. After the initial 180 days a **Software Maintenance Contract** may be purchased from your dealer.

---

 **Note:** When using the Windows TFTP-/DHCP Server you should use at least version 2.80.


---

### 5.2 Windows Client and DHCP-/TFTP Server setup

- Copy the image software (install.p7s and jffs2.img.p7s) into a local directory of the Windows client.
- **If the external interface of the mGuard is connected to the network: disconnect it!**
- If you want to flash an mGuard PCI which is operated in *Power-over-PCI* mode, you must connect the LAN interface of the mGuard PCI to the Ethernet card of the Windows client.
- Configure the Windows client to use the following IP settings. When using the mGuard PCI in **Driver** mode, you need to apply those settings to the mGuard PCI card.

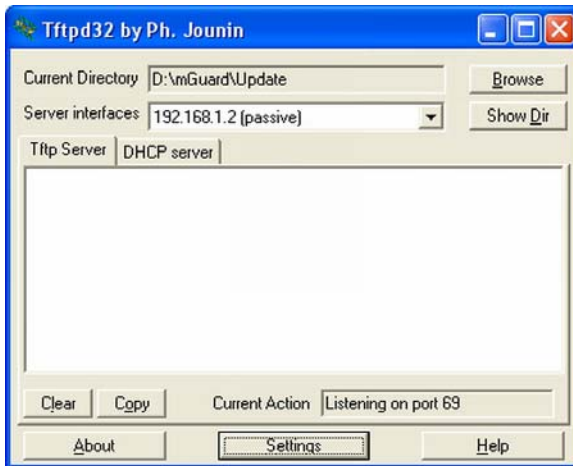
<b>IP address</b>	192.168.1.2
<b>Subnet mask</b>	255.255.255.0
<b>Default gateway</b>	192.168.1.1

---

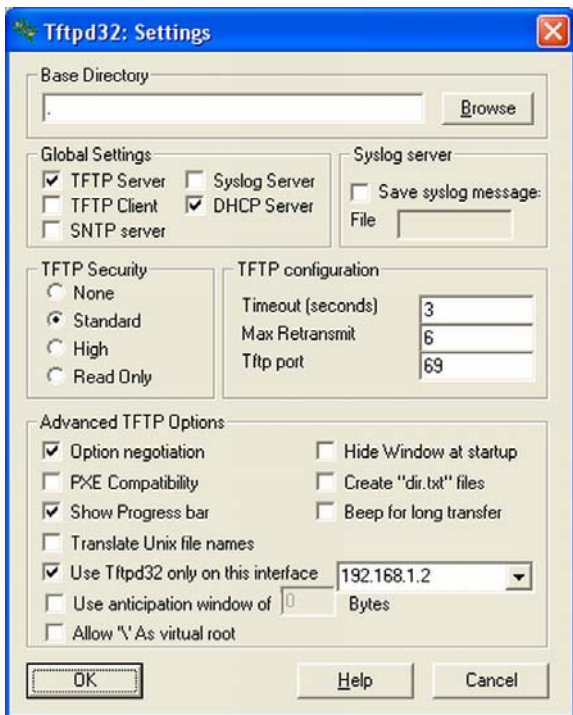
 **Note:** If you are familiar with the configuration of the TFTP/DHCP Server then you can keep the IP settings of the client and configure the TFTP/DHCP Server accordingly, as long as the client does not receive its IP settings via DHCP. Otherwise you should use the above mentioned IP settings and configure the TFTP/DHCP Server as described below.

---

- Start the program tftpd32.exe. You may ignore appearing error messages. They won't appear anymore after configuring and restarting the TFTP-/DHCP Server.

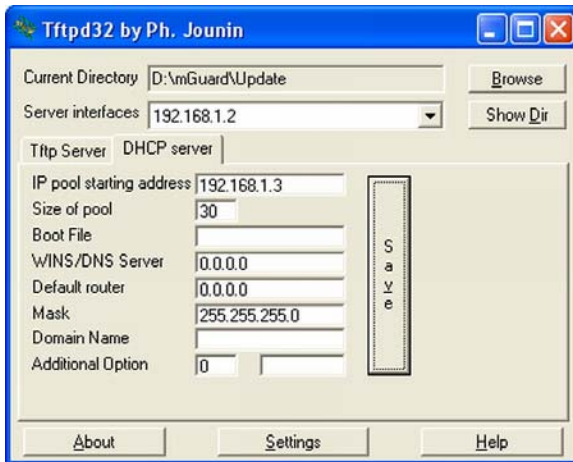


- The program should display the IP 192.168.1.2 as **Server interfaces**. The mark *passive* won't be displayed anymore after configuring and restarting the program.
- Click **Settings**.



- Ensure that only the options displayed in the screenshot are enabled.
- Click **OK**.

- Restart the program for applying the changes.
- Switch to the tab **DHCP Server**.



- Enter the following parameters:
  - IP pool starting address** = 192.168.1.3
  - Size of pool** = 30
  - Mask** = 255.255.255.0
- Click **Save** and switch to the tab **Tftp Server**. Information about the flash progress will be displayed in this screen.

- Click **Browse** and select the directory, which contains the image software *install.p7s* and *jffs2.img.p7s*.


The Windows client and TFTP-/DHCP Server setup is finished. Now the flash procedure can be started on the mGuard.

### 5.3 Flash Process

To start the *Flash* procedure, press the *Rescue* switch for approximately 3 seconds, until:

<b>mGuard smart</b>	All LEDs light green.
<b>mGuard PCI &amp; mGuard blade</b>	Both green LEDs (LAN and WAN) and the red LAN LED switch on.
<b>mGuard industrial</b>	The three LEDs LS/DA 1, LS/DA 2 and V.24 light green.
<b>mGuard delta</b>	The <i>Status</i> LED begins to fade out.

---

 **Note:** If you release the *Rescue* switch too late or too early, the mGuard restarts again.

---

This starts the *Flash* procedure and information about the flash progress is displayed in the tab *Tftp server* of the program Tftpd32. It takes about 60 seconds before the first information appears. The complete flash procedure may take about 5-10 minutes.

The status display changes as follows during the flash process:

<b>mGuard smart</b>	<ul style="list-style-type: none"> <li>• The middle LED flashes.</li> <li>• The 3 green LEDs form a bouncing ball display in which the light shifts from one LED to the next.</li> <li>• The middle LED lights continuously.</li> <li>• All 3 LEDs flash green at the same time.</li> </ul> <p>⇒ The <i>Flash</i> procedure is finished and you need to reboot the device.</p>
<b>mGuard PCI &amp; mGuard blade</b>	<ul style="list-style-type: none"> <li>• The red LAN LED flashes and flickers then.</li> <li>• The green LEDs and the red LAN LED form a bouncing ball display in which the light shifts from one LED to the next.</li> <li>• The red LAN LED lights continuously.</li> </ul> <p>⇒ The mGuard reboots automatically when the <i>Flash</i> procedure is finished.</p>
<b>mGuard industrial</b>	<ul style="list-style-type: none"> <li>• The LEDs LS/DA 1, LS/DA 2 and V.24 light orange briefly.</li> <li>• The LEDs LS/DA 1, LS/DA 2 and V.24 form a bouncing ball display in which the light shifts from one LED to the next.</li> <li>• The LEDs LS/DA 1, LS/DA 2 and V.24 are switched off. The LEDs p1, p2 and <i>Status</i> light green continuously.</li> <li>• The LEDs LS/DA 1, LS/DA 2 and V.24 flash green at the same time.</li> </ul> <p>⇒ The <i>Flash</i> procedure is finished and you need to reboot the device.</p>
<b>mGuard delta</b>	<ul style="list-style-type: none"> <li>• The <i>Status</i> LED flashes.</li> <li>• The <i>Status</i> LED flashes fast.</li> <li>• The <i>Status</i> LED lights continuously.</li> <li>• The <i>Status</i> LED flashed once per second.</li> </ul> <p>⇒ The <i>Flash</i> procedure is finished and you need to reboot the device.</p>

At the end of the flash procedure the program tftpd32 displays the error message that the file *rollout.sh* couldn't be found. You can ignore this message. The file *rollout.sh* is only required if the mGuard should also be configured during the flash procedure.

**mGuard delta** and **mGuard blade control unit** are in *Router* mode after flashing it. The user interface can be accessed through <https://192.168.1.1>. All other products (**mGuard smart**, **mGuard industrial**, **mGuard blade** and **mGuard PCI**) are in *Stealth* mode. The user interface can be accessed through <https://1.1.1.1>.

If you need to flash more than one mGuard, simply connect the next mGuard and press the *Rescue* switch as described above. The *Flash* procedure will start again.