

# Innominate mGuard v7

## Application Note

### Update, Recovery and Flash Guide



*mGuard smart*



*mGuard centerport*



*mGuard blade*



*mGuard industrial RS*



*mGuard PCI*



*mGuard delta*

Innominate Security Technologies AG  
Rudower Chaussee 13  
12489 Berlin, Germany

Phone: +49 (0)30-921028 0  
Fax: +49 (0)30-921028 020  
contact@innominate.com  
<http://www.innominate.com>

## Table of Contents

<b>1 Disclaimer</b>	<b>3</b>
<b>2 In which case do I need to execute which procedure?</b>	<b>4</b>
2.1 Update Procedure	4
2.2 Recovery Procedure	4
2.3 Flash Procedure	4
<b>2 The Rescue Button</b>	<b>5</b>
<b>3 Recovery Procedure</b>	<b>6</b>
<b>4 Major Release Update (MRU) License</b>	<b>7</b>
<b>5 Update Procedure</b>	<b>9</b>
5.1 How to retrieve the currently installed Firmware Version	9
5.2 Local (offline) Update	9
5.3 Online and Automatic Update	10
5.3.1 Configuring the Update Server	10
5.3.2 Online Update	10
5.3.3 Automatic Update	11
<b>6 Flash Procedure</b>	<b>12</b>
6.1 Prerequisites	12
6.2 Windows Client and DHCP-/TFTP Server Setup	13
6.3 Flash Process	15

## **1 Disclaimer**

© Innominate Security Technologies AG

September 2009

“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.

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

### 2.1 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 locally (offline) or online. If possible, the online update should be the preferred method.

---

 **Note:** Starting with an update to version 5 a *Major Release Update License* must be installed on the device for being able to update to the next major release (X.y.z). Please refer to the chapter [Major Release Update License](#).

---

### 2.2 Recovery Procedure

You need to perform the *Recovery* procedure if you lost access to the mGuard and can't contact the device, neither through the web browser nor through SSH. This may be caused by one of the following reasons:

- The internal IP of the mGuard (*Router*, *PPPoE*, *PPTP*, *Modem Mode*) is unknown.
- The management IP (*Stealth mode*) is unknown.
- SSH and HTTPS access rules were defined which do not allow accessing the device.

The *Recovery* procedure will reset the **mGuard delta**, the **mGuard centerport** 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 RS**, **mGuard blade** and **mGuard PCI**) will be reset into *Stealth (autodetect)* mode. Those 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. Apart from this the *Recovery* procedure won't affect currently configured VPN connections, firewall settings or passwords.

### 2.3 Flash Procedure

You only need to flash the firmware of the mGuard if the root password is unknown. It might also be useful to flash the device with the target version instead of executing several updates. **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.
- Starting with version 5 afterwards installed licenses, as for example VPN-10 licenses, will be stored permanently on the device and won't be erased by the flash procedure. In prior versions afterwards installed licenses will be erased and need to be re-installed.
- Starting with an update to version 5 a *Major Release Update License* must be installed on the device for being able to flash the device with the next major release (X.y.z) (refer to [Major Release Update License](#)).
- If you need to flash an already configured device, save the current configuration as configuration profile and download it to the local system before flashing the unit. This way you can restore the configuration after flashing the device.

---

## 2 The Rescue Button

The **Rescue Button** is used for executing one of the following actions:

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

Its location depends on the product, as shown in the pictures below:



**mGuard smart**



**mGuard PCI**



**mGuard blade**



**mGuard industrial RS**



**mGuard delta**

### 3 Recovery Procedure

The *Recovery* procedure will reset the **mGuard delta**, the **mGuard centerport** 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 RS**, **mGuard blade** and **mGuard PCI**) will be reset into *Stealth (autodetect)* mode. Those 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. Apart from this the *Recovery* procedure won't affect currently configured VPN connections, firewall settings or passwords.

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

⇒ The response of the device depends on the 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 LAN LED switches on for one second.</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>
<b>mGuard industrial RS</b>	<ul style="list-style-type: none"> <li>- The <i>State</i> LED switches off for one second.</li> <li>- The <i>State</i> LED lights green for one second.</li> <li>- Finally the <i>State</i> LED starts flickering green.</li> </ul>

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

⇒ The response of the device depends on the 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 red LAN LED switches on for one second.</li> <li>- The device will perform a reboot.</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>
<b>mGuard industrial RS</b>	<ul style="list-style-type: none"> <li>- The <i>State</i> LED switches off for one second.</li> <li>- The <i>State</i> LED lights green for one second.</li> <li>- The device reboots.</li> </ul>

**mGuard centerport:** Executing the *Recovery Procedure* requires a terminal and a keyboard connected to the *mGuard centerport*. To execute the *Recovery Procedure*, press the following key combination:

- German keyboard: **Alt + S-Abf + a** (or **Alt + Druck + a** if the key label **S-Abf** is missing)
- English keyboard: **Alt + SysRq + a** (or **Alt + Print + a** if the key label **SysRq** is missing)

A corresponding message is displayed on the terminal when the *Recovery Procedure* is finished.

---

 **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> 00-aa-aa-aa-aa-aa) on your computer. Otherwise the mGuard won't be accessible through <https://1.1.1.1>. Please refer to the *mGuard User Manual* for further information.

---

## 4 Major Release Update (MRU) License

Starting with an update to version 5 a *Major Release Update (MRU) License* must be installed on the unit for being able to update to the next major release (**X.y.z**), as for example from 4.x.x to 5.0.0. Minor releases (x.**Y.z**) and patch releases (x.y.**Z**) are free of charge until further notice. Please contact your local dealer for obtaining a *Major Release Update Voucher* for requesting the *Major Release Update License*.

There exist two different kinds of *Major Release Update* licenses:

- **Innominate mGuard MRU:** Upgrade of the mGuard firmware by one Major Release step for one mGuard field appliance.
- **Innominate mGuard LFS:** Lifetime Firmware Subscription for one mGuard field appliance, granting the right to install any standard firmware image or upgrade available from Innominate for the respective appliance platform.

For an **update to version 5** an *MRU License* is required for devices which were produced before 01.01.2007.

For an **update to version 6** an *MRU License* is required for devices which were produced before 01.10.2007.

For an **update to version 7** an *MRU License* is required if the device was produced with a version less than 6 and if there is no *MRU License* for version 6 present on the device. All devices with version 6 are automatically entitled to be updated to version 7 without *MRU License*.

For each update to the next major release one *MRU License* is required. If you want to update a device from version 4 to version 6, two *MRU Licenses* are required, one license for the update to version 5 and another license for the update to version 6.

The production date is displayed in the menu *Management -> Licensing* (tab *Overview*) in the base license of the device. The base license is the license where the option *licence\_type* displays the product name (e.g. *Innominate mGuard enterprise XL*).

The screenshot shows the 'Management > Licensing' interface with the 'Overview' tab selected. It displays a 'Feature License' for a device with 'mGuard Flash ID 0004000b413ff0d9-0485'. The license has a priority of 1124964364. The table below lists various license attributes and their values.

License with priority 1124964364	
licence_id	0
licence_date	2005-08-25T10:06:04
flash_id	0004000b413ff0d9
serial_number	2T800081
hardware_revision	000007dc
product_code	51011
vpn_channels	-1
l2tp_server	1
snmp	1
remote_syslog	1
mau_management	1
licence_version	1
licence_type	Innominate mGuard enterprise XL
fw_redundancy	1
auth_x509	1
nw_extended	1
nwsec_base	1
cifs_integrity_monitoring	1

Menu: *Management -> Licensing*

An *MRU License* is also required when flashing the device with the next major release. Starting with version 5 afterwards installed licenses are stored permanently on the device which means that they won't be erased during the flash procedure. When flashing a unit with an installed v5 with v6, you can request the *MRU License* from the device and then flash it with the new major release. Flashing a device with version 5 requires that the *MRU License* is uploaded to the device during the flash process. The *MRU License* must be located in the same directory as the firmware image files and must have either the filename *licence.lic* or *<serialnumber>.lic*. The flash process looks automatically for those files being available.

The *Major Release Update Voucher* consists of a voucher serial number (e.g. 2730200089) and a corresponding voucher key (e.g. cb30-09e5-cf8c-2cdf-bc56-2a45). After receiving the voucher you need to request the *MRU License* for the device:

- Go to the menu **Management -> Licensing**, tab **Install**.
  - Enter the voucher serial number and the voucher key.
  - Click **<Online License Request>**.
- ⇒ The license will be issued and installed automatically onto the device.

Overview	Install
<b>Automatic License Installation</b>	
Voucher Serial Number/Voucher Key	2730200089    cb30-09e5-cf8c-2cdf-bc56-2a45
	Online License Request
Reload Licenses	Online License Reload
<b>Manual License Installation</b>	
Order License	Edit License Request Form
Filename	Durchsuchen...
	Install license file

Menu: *Management -> Licensing*

If the device does not have access to the Internet, use the following URL from a workstation with Internet access: [http://license.innominate.com/request\\_license.cgi](http://license.innominate.com/request_license.cgi). You also need to provide the complete flash ID of the device (including the checksum) when requesting the license through this URL. The flash ID of the unit is displayed in the menu **Management -> Licensing**, tab **Overview** (e.g. *003c000b414efbe7-0282*). After entering the required data and clicking **<Submit>** the license file will be made available for download. The license needs to be installed in the section *Manual License Installation*:

- Click **<Browse>**.
- Select the license file.
- Click **<Install license file>**.


Once the *MRU License* is installed on the device it can be updated to the next major release version or flashed with this version.

The devices behave in the following manner if the *MRU License* is missing:

- After starting a local or an online update the message **The update is not intended for the currently installed version** is displayed and the update is aborted.
- After flashing the device an LED displays the morse signal SOS (three times short, three times long, three times short). If this happens you need to flash the device again with the previous installed version or upload the license during the flash procedure. Which LED displays SOS depends on the product:
  - **mGuard smart**: The middle LED in red.
  - **mGuard blade** and **mGuard delta**: The red WAN LED.
  - **mGuard industrial RS**: The fault LED.
  - **mGuard delta**: The status LED in green.

## 5 Update Procedure

The firmware of the mGuard can be updated conveniently through the web interface. The update can be installed either locally (offline) or online through the Internet. If possible, the online update should be the preferred method.

 **Note:** Starting with an update to version 5 an installed *Major Release Update License* is required for installing major release updates (refer to chapter [Major Release Update License](#)).

### 5.1 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 the device was produced and *Updates* about the installed updates.

Overview	Update	AntiVirus Pattern
<b>System Information</b>		
Version	4.2.1.default	
Base	4.1.1.default	
Updates	update-4.1.x-4.2.0.default update-4.2.0-4.2.1.default	


### 5.2 Local (offline) Update

- At first you need to retrieve the firmware version which is currently installed on the device as described in the previous chapter.
- Check our homepage ([www.innominate.com](http://www.innominate.com), *Downloads -> 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 v4.2.x to v7.0.0, you need to update the device step by step, from v4.2.x to v6.1.4 and then from v6.1.x to v7.0.0.
- Download the appropriate update file (e.g. update-4.2.x-6.1.4.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.

Overview	Update
<b>Local Update</b>	
Filename	D:\update-4.2.x-6.1.4.tar <input type="button" value="Durchsuchen..."/>
<input type="button" value="Install Packages"/>	

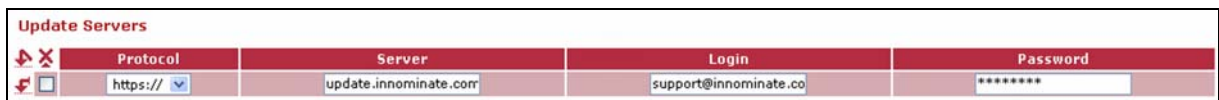
- Click **<Install Packages>**.
- ⇒ The update is started.
- Examine the output.
- When the update is finished, reboot the device if prompted.

### 5.3 Online and Automatic Update

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

#### 5.3.1 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 the account information (login/password) you have received after registering through our homepage ([www.innominate.com](http://www.innominate.com) -> Services -> Software Updates).



Protocol	Server	Login	Password
https://	update.innominate.com	support@innominate.co	*****

- Click **<Apply>**.

#### 5.3.2 Online Update

Due to the *Automatic Update* this option is obsolete but it is still available for maintaining 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 as described previously.
- Check our homepage ([www.innominate.com](http://www.innominate.com), *Downloads -> 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 v4.2.x to v7.0.0, you need to update the device step by step, from v4.2.x to v6.1.4 and then from v6.1.x to v7.0.0.
- 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-4.2.x-6.1.4.



Online Update
Package set name
update-4.2.x-6.1.4
Install Package Set

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

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

### 5.3.3 Automatic Update


- Go to the menu **Management -> Update**, tab **Update**.

**Automatic Update**

Install the latest patch release (x.y.z)	<input type="button" value="Install latest patches"/>
Install the latest minor release (x.Y.z) for the currently installed major version	<input type="button" value="Install latest minor release"/>
<small><b>Note:</b> It might be possible that there is no direct update from the currently installed version to the latest published minor release available. Therefore, after updating the system to a new minor release, press this button again until you receive the message that there is no newer update available.</small>	
Install the next major release (X.y.z)	<input type="button" value="Install next major version"/>
<small><b>Note:</b> It might be possible that there is no direct update from the currently installed version to the next major release available. Therefore execute the minor release update first and repeat this step until you receive the message that there is no newer minor release available. Then install the next major release.</small>	

- Select one of the following options:
  - **<Install latest patches>** for updating the device within one minor release version (e.g. from 6.1.3 to 6.1.4).
  - **<Install latest minor release>** for updating to the next minor release (e.g. from 6.0.0 to 6.1.4).
  - **<Install next major version>** for updating the device to the next major release (e.g. from 6.1.x to 7.0.0). Selecting this option may require the presence of a *Major Release Update License* (refer to chapter [Major Release Update License](#)).

---

 **Note:** It might be possible that there is no direct update available from the currently installed version to the latest published minor or major release. Therefore, after updating the system to a new minor or patch release, press the same button again until you receive the message that there is no newer update available.

---

### 6 Flash Procedure

If you want to flash the **mGuard centerport**, please refer to the *mGuard User Manual, Software-Release 7*. The *mGuard centerport* supports the flash procedure via DHCP/BOOTP+TFTP, from CD/DVD or from USB mass storage.

You only need to flash the firmware of the mGuard if the root password is unknown. It might also be useful to flash the device with the target version instead of executing several updates. **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.
- Starting with version 5, flashing the mGuard with the next major release requires an *MRU License* (refer to chapter [Major Release Update License](#)).
- Starting with version 5 afterwards installed licenses are stored permanently on the device which means that they won't be erased during the flash procedure. When flashing a unit with an installed version 5 with version 6, you can request the *MRU License* from the device and then flash it with the new major release. Flashing a device with version 5 requires that the *MRU License* is uploaded to the device during the flash process. The *MRU License* must be located in the same directory as the firmware image files and must have either the filename *licence.lic* or *<serialnumber>.lic*. The flash process looks automatically for those files being available.
- If you want to flash a device, which was produced with version 5, 6 or 7, with a lower version than 5, you need to use the file *install.p7s* of the firmware image of version 5, 6 or 7.

---

**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.**

#### 6.1 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.innominate.com](http://www.innominate.com), *Downloads -> Firmware*).

1. The image software (*install.p7s* and *jffs2.img.p7s*) of the desired firmware version.
2. Windows: TFTP-/DHCP-Server (tftpd32.exe).
3. If there is a desktop firewall running on the client, disable it.
4. If the *MRU License* should be uploaded to the device during the flash procedure, put the license file into the same directory which contains the image software, either as *licence.lic* or as *<serialnumber>.lic*.
5. If the mGuard should also receive a configuration during the flash procedure, put the script *rollout.sh* and the configuration file (*preconfig.atv* or *<serial number>.atv*) into the same directory which contains the image software (refer to the application note *Rollout Support* which can be downloaded from our homepage, [www.innominate.com](http://www.innominate.com), *Downloads -> Application Notes*).

---

#### Note:

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


---

## 6.2 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.

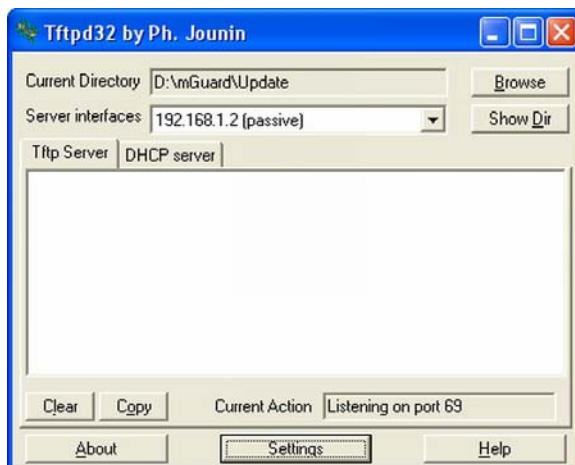
<b>IP address</b>	192.168.1.2
<b>Subnet mask</b>	255.255.255.0
<b>Default gateway</b>	192.168.1.1

---

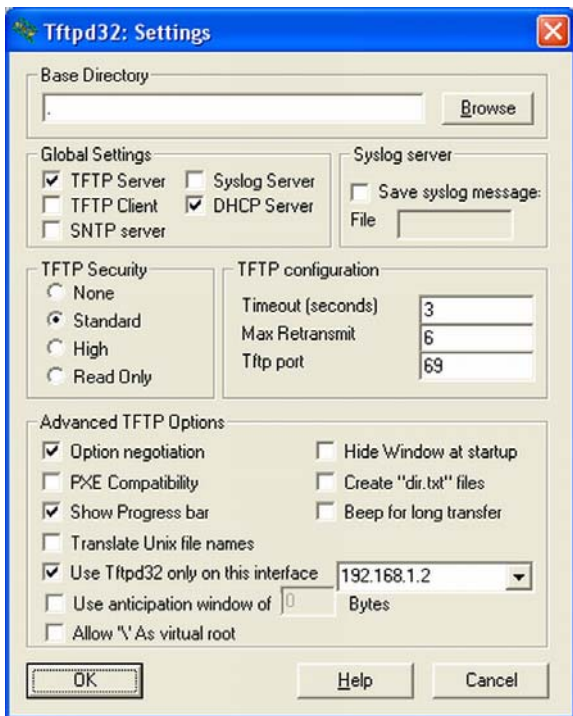
 **Note:** If you are familiar with the configuration of the TFTP/DHCP Server then you can keep the IP settings of the client and configure the TFTP/DHCP Server accordingly, as long as the client does not receive its IP settings via DHCP. Otherwise you should use the above mentioned IP settings and configure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

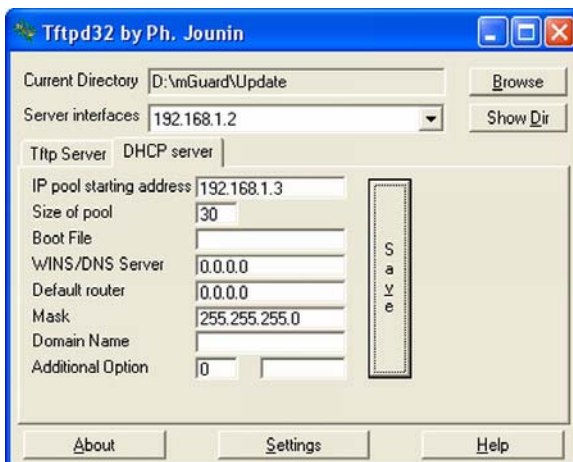


- The program should display the IP 192.168.1.2 as **Server interfaces**. The mark *passive* won't be displayed anymore after configuring and restarting the program.
- Click **Settings**.



- 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.

### 6.3 Flash Process

To start the *Flash* procedure, press the *Rescue* button 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 delta</b>	The <i>Status</i> LED begins to fade out.
<b>mGuard industrial RS</b>	The three LEDs <i>State</i> , <i>LAN</i> and <i>WAN</i> light green.

 **Note:**

- If you release the *Rescue* button too late or too early, the mGuard restarts again.
- Starting with version 6 it is also possible to initiate the flash procedure by creating the file **RESCUE\_me\_now** in the top level directory of the mGuard with a subsequent reboot of the devices. This feature is really helpful when flashing an **mGuard PCI** because the rescue button is usually not accessible from the outside.

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 20 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 three 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> </ul> <p>⇒ All three LEDs flash at the same time. 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 green LEDs flicker and the red LAN LED lights continuously.</li> </ul> <p>⇒ <b>mGuard PCI</b>: The mGuard reboots automatically when the <i>Flash</i> procedure is finished.</p> <p>⇒ <b>mGuard blade</b>: The green LEDs and the red WAN LED flash at the same time. 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> </ul> <p>⇒ The <i>Status</i> LED flashed once per second. The <i>Flash</i> procedure is finished and you need to reboot the device.</p>
<b>mGuard industrial RS</b>	<ul style="list-style-type: none"> <li>• The <i>State</i> LED flickers green.</li> <li>• The LEDs <i>Modem</i>, <i>State</i> and <i>LAN</i> form a bouncing ball display.</li> <li>• The <i>State</i> LED lights continuously.</li> <li>• The LEDs <i>Modem</i>, <i>State</i> and <i>LAN</i> flash green at the same time.</li> </ul> <p>⇒ The LEDs <i>Modem</i>, <i>State</i> and <i>LAN</i> flash green at the same time. The <i>Flash</i> procedure is finished and you need to reboot the device.</p>

The following error message of the TFTP server can be ignored if you do not use the script *rollout.sh* for uploading a configuration during the flash procedure:

**File rollout.sh: error 2 in system call CreateFile The system cannot find the file specified.**

The following error messages of the TFTP server can be ignored if a license file should not be uploaded during the flash procedure:

**File <serial number>.lic : error 2 in system call CreateFile The system cannot find the file specified.**

**File licence.lic: error 2 in system call CreateFile The system cannot find the file specified.**

**mGuard delta, mGuard centerport** and **mGuard blade control unit** are in *Router* mode after flashing it. The web interface can be accessed through <https://192.168.1.1>.

All other products (**mGuard smart, mGuard industrial RS, mGuard blade** and **mGuard PCI**) are in *Stealth* mode. The web 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* button as described above. The *Flash* procedure will start again. Of course you may also connect several mGuards to a switch and flash them at the simultaneously.