

Innominate mGuard 7.4

Application Note

Update, Recovery and Flash Guide



mGuard smart
mGuard smart²



mGuard centerport



mGuard blade



mGuard industrial rs



mGuard pci



mGuard rs2000
mGuard rs4000

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

1 Disclaimer	3
2 In which case do I need to execute which procedure?	4
2.1 Update Procedure	4
2.2 Recovery Procedure	4
2.3 Flash Procedure	4
2 The Rescue Button	5
3 Recovery Procedure	6
4 Major Release Update (MRU) License	7
5 Update Procedure	9
5.1 How to retrieve the currently installed Firmware Version	9
5.2 Local (offline) Update	9
5.3 Automatic (online) Update	10
5.3.1 Configuring the Update Server	10
5.3.2 Online Update	10
5.3.3 Automatic Update	10
6 Flash Procedure	11
6.1 Prerequisites	12
6.2 Windows System and DHCP-/TFTP Server Setup	13
6.3 Flash Procedure	15
6.4 TFTP Server Error Messages	16

1 Disclaimer

© Innominate Security Technologies AG

January 2012

"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 to update the mGuard to a newer firmware release. This will be done conveniently through the mGuard web interface. The update can be installed locally (offline) or online. If possible, the online update should be the preferred method.



Starting with an update to mGuard firmware 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 cannot 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 resets the **mGuard centerport** and the **mGuard blade control unit** into *Router* mode and the internal IP address to 192.168.1.1. Those devices will be accessible again through <https://192.168.1.1>.

All other products (**mGuard smart/smart²**, **mGuard industrial rs**, **mGuard blade**, **mGuard rs2000/rs4000** and **mGuard pci**) are reset as follows, depending on the installed firmware version:

- Firmware version < 7.2.0: *Stealth (autodetect)* mode. The device is accessible through <https://1.1.1.1>.
- Firmware version >= 7.2.0: *Stealth (multiple-clients)* mode. The device can be accessed either through <https://1.1.1.1> or through <https://192.168.1.1> or through a BootP assigned IP address. Please refer to the *mGuard User Manual* for further information.

The *Recovery* procedure will also delete SSH access rules and create a HTTPS access rule to allow access from the internal network. This rule is marked with the comment "*+++ created by recovery procedure +++*" and can be removed afterwards. Apart from this, the *Recovery* procedure will not 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 if an update to a target version requires several single update steps. **This procedure will erase all existing configurations on the mGuard.** The mGuard will be restored to the factory default settings, including all passwords. Thus, you need to reconfigure the mGuard after performing the flash procedure.



- If you want to update the version of the firmware, the *Update* procedure should be the preferred method.
- Starting with firmware version 5, afterwards installed licenses (e.g. VPN-10 licenses) will be stored permanently on the device and will not be erased by the flash procedure. In prior versions afterwards installed licenses were deleted and needed 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 a configuration profile and download it to the local system before flashing the mGuard device. In this case the configuration can be restored afterwards.

2 The Rescue Button

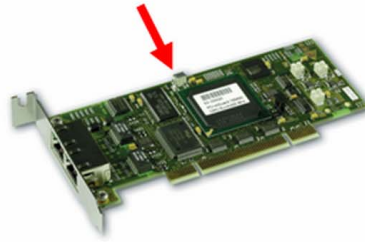
The **Rescue Button** is used for executing one of the following actions:

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

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



mGuard smart/smart²



mGuard pci



mGuard blade



mGuard industrial rs



mGuard rs2000/rs4000

3 Recovery Procedure

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

All other products (**mGuard smart/smart²**, **mGuard industrial rs**, **mGuard rs2000/rs4000**, **mGuard blade** and **mGuard pci**) are reset as follows, depending on the installed firmware version:

- Firmware version < 7.2.0: *Stealth (autodetect)* mode. The device is accessible through <https://1.1.1.1>.
- Firmware version >= 7.2.0: *Stealth (multiple-clients)* mode. The device can be accessed either through <https://1.1.1.1>, through <https://192.168.1.1>, or through a BootP assigned IP address. Please refer to the *mGuard User Manual* for further information.

The *Recovery* procedure will also delete SSH access rules and create a HTTPS access rule to allow access from the internal network. This rule is marked with the comment "*+++ created by recovery procedure +++*" and can be removed afterwards. Apart from this, the *Recovery* procedure will not 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:

mGuard smart mGuard smart²	- The middle LED switches off for one second. - The middle LED lights green for one second. - Finally the middle LED starts flickering green.
mGuard pci & mGuard blade	- The red LAN LED switches on for one second.
mGuard industrial rs	- The <i>State</i> LED switches off for one second. - The <i>State</i> LED lights green for one second. - Finally the <i>State</i> LED starts flickering green.
mGuard rs2000 mGuard rs4000	- The <i>STAT</i> LED lights green for one second. - Finally the middle LED starts flickering green.

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

⇒ The response of the device depends on the product:

mGuard smart mGuard smart²	- The middle LED switches off for one second. - The middle LED lights green for one second. - The device reboots. The middle LED lights red briefly.
mGuard pci & mGuard blade	- The red LAN LED switches on for one second. - The device reboots.
mGuard industrial rs	- The <i>State</i> LED switches off for one second. - The <i>State</i> LED lights green for one second. - The device reboots.
mGuard rs2000 mGuard rs4000	- The <i>STAT</i> LED lights green for one second. - The device reboots.

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.

4 Major Release Update (MRU) License

Starting with an update to version 5 a *Major Release Update (MRU) License* must be installed on the device under certain conditions for being able to update to the next major release (**X.y.z**), as for example from version 5 to 6.

Minor releases (**x.Y.z**) and patch releases (**x.y.Z**) are free of charge until further notice.

An *MRU license* is required for:

- an **update to version 5** if the device was produced before 2007-01-01.
- an **update to version 6** if the device was produced before 2007-10-01.
- an **update to version 7** if the device was produced with a version less than 6 and if there is no *MRU License* to version 6 present on the device. All devices with version 6 or with an installed *MRU License* to version 6 are automatically entitled for an update to version 7 without *MRU License*.

The production date is displayed in the mGuard web interface *Management >> Licensing (tab Overview)* in the base license of the device, parameter *licence_date*. The base license is the license where the option *licence_type* displays the product name (in the screenshot below: *Innominate mGuard*).

License with priority 1287582701	
licence_id	0
licence_date	2010-10-20T13:51:41
flash_id	N205d1f31343512302ca2e0cecbcaedcfd3
serial_number	2004010271
hardware_revision	00003000
product_code	HW-101130
pxc_product_code	2700446
firmware_max_version	7
firmware_flavours	default
tpm_pubkey_hash	62f272534f3144f5b392716fdbb0219cf7d34445
tpm_key_hash	22c3b0915e987198b7311e0769e4b7d8ce7f6d6f
vpn_channels	0
I2tp_server	1
licence_version	1
licence_type	Innominate mGuard
auth_extended	1

Menu: *Management -> Licensing*

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.

Please contact your local mGuard dealer to obtain 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.

A *MRU License* is also required when flashing the device with the next major release. Starting with firmware version 5 afterwards installed licenses are stored permanently on the mGuard device. They will not be erased during the flash process. When flashing a device with an installed version 5 to 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 *<serial number>.lic*. The mGuard checks automatically for those files being available during the flash process.

4. Major Release Update (MRU) License

A *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, the MRU license needs to be requested:

- In the mGuard web interface, 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.

The screenshot shows the 'Install' tab of the 'Licensing' menu. It is divided into two sections: 'Automatic License Installation' and 'Manual License Installation'. In the 'Automatic' section, there are input fields for 'Voucher Serial Number/Voucher Key' containing '2730200089' and 'cb30-09e5-cf8c-2cdf-bc56-2a45', and a button labeled 'Online License Request'. Below this is a 'Reload Licenses' section with an 'Online License Reload' button. The 'Manual License Installation' section has an 'Order License' section with an 'Edit License Request Form' button, and a 'Filename' section with a text input field, a 'Durchsuchen...' button, and an 'Install license file' button.

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. 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 device is displayed in the menu **Management >> Licensing**, tab **Overview** (e.g. 003c000b414efbe7-0282).

The license file will be made available for download after entering the required data and clicking **<Submit>**. The license needs then to be installed via the mGuard web interface onto the respective device in the section *Manual License Installation*:

- Click **<Browse>**.
- Select the downloaded 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 automatic (online) update the message **The update is not intended for the currently installed version** is displayed and the update is aborted.
- After flashing and rebooting the device, an LED displays the morse signal SOS (three times short, three times long, three times short). If this happens, flash the device again with the previously installed version or upload the license during the flash procedure. Depending on the product, the following LED displays SOS:
 - **mGuard smart/smart²**: The middle LED in red.
 - **mGuard blade, mGuard pci**: The red WAN LED.
 - **mGuard industrial rs**: The fault LED.
 - **mGuard rs2000/rs4000**: The FAULT LED.

5 Update Procedure

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



Starting with an update to firmware 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

In the mGuard web interface, go to the menu **Management >> Update**, tab **Overview**. The currently installed version is displayed in the row *Version*. *Base* informs about the version which was installed when the device was produced and *Updates* about afterwards installed updates.

System Information	
Version	7.4.1.default
Base	7.4.0.default
Updates	update-7.4.x-7.4.1.default

5.2 Local (offline) Update

- First of all you need to retrieve the firmware version which is currently installed on the device as described in the previous chapter.
- Check the Innominate website (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 version 6.1.x to 7.4.1, you need to update the device step by step, from 6.1.x to 7.1.1, from 7.1.x to 7.2.0, and finally from 7.2.x to 7.4.1. In such cases it could be faster to flash the mGuard with the target version instead of performing several updates.
- Download the appropriate update file (e.g. update-7.2.x-7.4.1.default.ixp4xx_be.tar.gz) from the Innominate website. Do not extract the file. 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 will get the error message "**tar: Invalid gzip magic**".
- In the mGuard web interface, 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.

5.3 Automatic (online) Update



The mGuard must have access to the Internet to perform an online or automatic update.

5.3.1 Configuring the Update Server

- In the mGuard web interface, 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 (default settings).
- Enter the account information (login/password) you have received after registering through the Innominate website (www.innominate.com >> Services >> Software Updates).

Update Servers					
Protocol	Server	Via VPN	Login	Password	
<input type="checkbox"/> <input type="checkbox"/> https://	update.innominate.com	No	support@innominate.com	

- Click **<Apply>**.

5.3.2 Online Update



This option is obsolete due to the *Automatic Update*. It is still available for maintaining backward compatibility but it might be removed in a future release. Please perform the *Automatic Update* only.

5.3.3 Automatic Update

- In the mGuard web interface, 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>Note: 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>Note: 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 version 7.4.0 to 7.4.1).
 - **<Install latest minor release>** for updating to the next minor release (e.g. from version 7.3.1 to 7.4.1).
 - **<Install next major version>** for updating the device to the next major release (e.g. from version 6.1.x to 7.2.0). Selecting this option may require the presence of a *Major Release Update License* (refer to chapter [Major Release Update License](#)).



It might be possible that there is no direct update available from the currently installed version to the latest published minor or major release. Thus, after updating the system to a new minor or major release, repeat the procedure until you receive the message that there is no newer update available.

6 Flash Procedure

This chapter explains how to flash an mGuard using the TFTP/DHCP server on a Windows system.

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

If you want to flash an **mGuard rs2000/rs4000** from the SD card, please refer to the *mGuard User Manual* or to the application note *Rollout Support*. Both documents are available at the Innominate website.

Usually 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 update steps. **This procedure will erase all existing configurations on the mGuard.** The mGuard will be restored to the factory default settings, including all passwords. Thus, you need to reconfigure the mGuard after performing the flash procedure.



- If you want to update the firmware version, the *Update Procedure* should be the preferred method.
- Starting with version 5, flashing the mGuard with the next major release requires an *MRU License* under certain conditions (refer to chapter [Major Release Update License](#)).
- Starting with version 5 afterwards installed licenses are stored permanently on the device. They will not be erased during the flash procedure. When flashing a device with an installed firmware version 5 to 6, the MRU license can be requested via the devices web interface online and then flash it with the new major release. Flashing a device with firmware 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 *<serial number>.lic*. The mGuard uploads and installs those files automatically during the flash procedure if they are available.
- If you want to flash a device, which was produced with firmware version 5, 6, or 7, with a lower version than 5, you need to use the file *install.p7s* of the target production firmware image only.



ATTENTION: Do not interrupt the power supply while flashing an mGuard device. 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 system you want to use for flashing the mGuard, downloadable from the Innominate website (www.innominate.com, *Downloads >> Firmware*).

1. The firmware image of the desired version. The firmware file downloaded from the Innominate website has the filename *mguard_firmware<version>.zip* (e.g. *mguard_firmware741.zip*). This packed file contains the following product dependent files:

Product	Firmware files
mGuard smart mGuard industrial rs mGuard pci mGuard blade	install.p7s jffs2.img.p7s
mGuard smart ² mGuard rs2000 mGuard rs4000	install-ubi.mpc83xx.p7s ubifs.img.mpc83xx.p7s
mGuard centerport	install.x86_64.p7s firmware.img.x86_64.p7s

Each mGuard product needs its corresponding firmware files for the flash procedure. For a simplified notation, the following chapters mention only the firmware files *install.p7s* and *jffs2.img.p7s* representatively.

2. Windows: TFTP-/DHCP server (tftpd32.exe, downloadable from the Innominate website).
3. If there is a desktop firewall running on the system, disable it first.
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 firmware image, either as *licence.lic* or as *<serial number>.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 firmware image (refer to the application note *Rollout Support* which can be downloaded from the Innominate website, www.innominate.com, *Downloads >> Application Notes*).



When using the Windows TFTP-/DHCP server at least version 2.80 is required.

6.2 Windows System and DHCP-/TFTP Server Setup

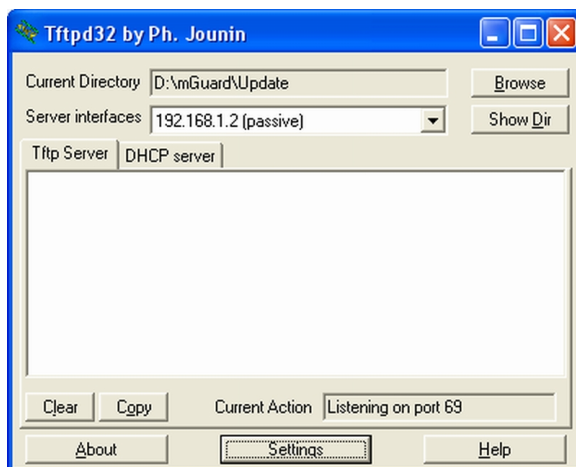
- Unpack and copy the firmware image (install.p7s and jffs2.img.p7s) to a local directory of the Windows system.
- **If the external interface of the mGuard is connected to a network: disconnect it!**
- If you want to flash an mGuard pci which is operated in *Power-over-PCI* mode, connect the LAN interface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

IP address	192.168.1.2
Subnet mask	255.255.255.0
Default gateway	192.168.1.1

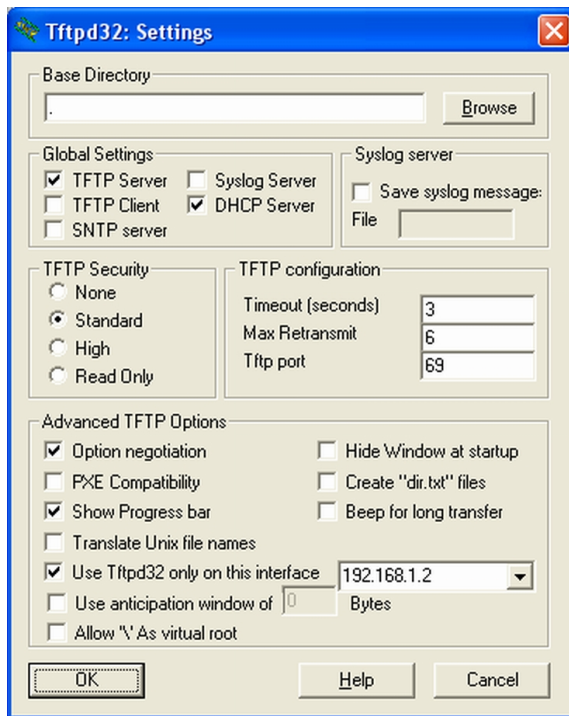


If you are familiar with the configuration of the TFTP/DHCP server you can keep the IP settings of the system and configure the TFTP/DHCP server accordingly, as long as the system does not receive its IP settings from a DHCP server. Otherwise you should use the above mentioned IP settings and configure the TFTP/DHCP server as described below.

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

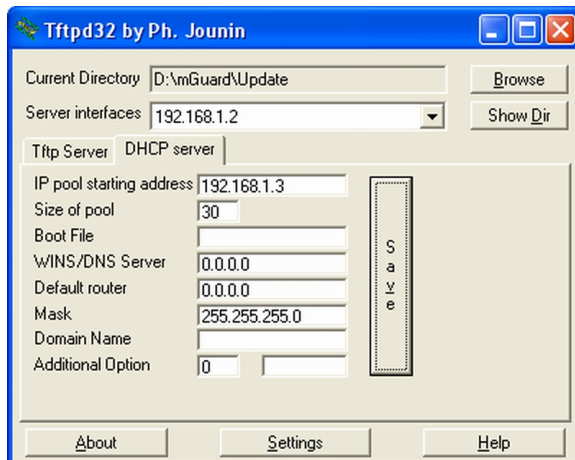


- The program should display the IP address 192.168.1.2 as **Server interfaces**. The mark *passive* won't be displayed anymore after configuring and restarting the program.
- Click **<Settings>**.



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

- Restart the program to apply 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.

- In the main panel of the program, click **<Browse>** and select the directory which contains the firmware image files *install.p7s* and *jffs2.img.p7s*.

The setup of the TFTP-/DHCP server on the Windows system is finished now. The flash procedure has to be initiated on the mGuard.

6.3 Flash Procedure

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

mGuard smart mGuard smart²	All LED light green.
mGuard pci & mGuard blade	Both green LED (LAN and WAN) and the red LAN LED switch on.
mGuard industrial rs	The three LED <i>State</i> , <i>LAN</i> and <i>WAN</i> light green.
mGuard rs2000 mGuard rs4000	The three LED <i>STAT</i> , <i>MOD</i> and <i>SIG</i> light green.



- If you release the *Rescue* button too late or too early, the mGuard restarts.
- The flash procedure can also be initiated from the SSH console (requires root access) by executing the command *rescue-on-next-boot* followed by a subsequent reboot of the device. This feature is really helpful when flashing an **mGuard pci** because its rescue button is usually not accessible from the outside.

This initiates 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 15 minutes.

The status display changes as follows during the flash process:

mGuard smart mGuard smart²	<ul style="list-style-type: none"> • The middle LED flashes. • The three green LED form a bouncing ball display in which the light shifts from one LED to the next. • The middle LED lights continuously. <p>⇒ All three LED flash at the same time. The <i>Flash</i> procedure is finished and you need to reboot the device.</p>
mGuard pci & mGuard blade	<ul style="list-style-type: none"> • The red LAN LED flashes and flickers then. • The green LEDs and the red LAN LED form a bouncing ball display in which the light shifts from one LED to the next. • The green LED flicker and the red LAN LED lights continuously. <p>⇒ mGuard pci: The mGuard reboots automatically when the <i>Flash</i> procedure is finished.</p> <p>⇒ mGuard blade: The green LED 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>
mGuard industrial rs	<ul style="list-style-type: none"> • The <i>State</i> LED flickers green. • The LED <i>Modem</i>, <i>State</i> and <i>LAN</i> form a bouncing ball display. • The <i>State</i> LED lights continuously. <p>⇒ The LED <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>

mGuard rs2000 mGuard rs4000	<ul style="list-style-type: none">• The <i>STAT</i> LED flickers green.• The LED <i>STAT</i>, <i>SIG</i> and <i>MOD</i> form a bouncing ball display.• The <i>STAT</i> LED lights continuously. <p>⇒ The LED <i>STAT</i>, <i>SIG</i> and <i>MOD</i> flash green at the same time. The <i>Flash</i> procedure is finished and you need to reboot the device.</p>
--	---

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

All other products (**mGuard smart/smart²**, **mGuard industrial rs**, **mGuard rs2000/rs4000**, **mGuard blade** and **mGuard pci**) are accessible as follows, depending on the firmware version on the device:

- Firmware version < 7.2.0: *Stealth (autodetect)* mode. The device is accessible through <https://1.1.1.1>.
- Firmware version >= 7.2.0: *Stealth (multiple-clients)* mode. The device can be accessed either through <https://1.1.1.1> or through <https://192.168.1.1> or through a BootP assigned IP address. Please refer to the *mGuard User Manual* for further information.

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 same time.

6.4 TFTP Server Error Messages

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

This error message can be ignored if you do not use the script *rollout.sh* for uploading a configuration during the flash procedure.

- 2) **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.

These error messages can be ignored if a license file should not be uploaded during the flash procedure.