Chipsmall Limited consists of a professional team with an average of over 10 year of expertise in the distribution of electronic components. Based in Hongkong, we have already established firm and mutual-benefit business relationships with customers from,Europe,America and south Asia,supplying obsolete and hard-to-find components to meet their specific needs.

With the principle of “Quality Parts,Customers Priority,Honest Operation,and Considerate Service”,our business mainly focus on the distribution of electronic components. Line cards we deal with include Microchip,ALPS,ROHM,Xilinx,Pulse,ON,Everlight and Freescale. Main products comprise IC,Modules,Potentiometer,IC Socket,Relay,Connector.Our parts cover such applications as commercial,industrial, and automotives areas.

We are looking forward to setting up business relationship with you and hope to provide you with the best service and solution. Let us make a better world for our industry!

Contact us

Tel: +86-755-8981 8866 Fax: +86-755-8427 6832
Email & Skype: info@chipsmall.com Web: www.chipsmall.com
Address: A1208, Overseas Decoration Building, #122 Zhenhua RD., Futian, Shenzhen, China

Configuration of the mGuard security appliances Firmware 8.6

User Manual

PHOENIX CONTACT
INSPIRING INNOVATIONS

User Manual
Configuration of the mGuard security appliances (Reference Manual)
Firmware 8.6

2018-01-15

Designation: UM EN MGUARD 8.6

Revision: 07

Order No.: —

This user manual is valid for the mGuard software release 8.6 when using devices of the mGuard product range (for further information see mGuard firmware – Version 8.6.x – Release Notes):

FL MGUARD RS4000	FL MGUARD GT/GT
FL MGUARD RS2000	FL MGUARD CENTERPORT
FL MGUARD RS4004	FL MGUARD DELTA
FL MGUARD RS2005	FL MGUARD SMART2
TC MGUARD RS4000 3G	FL MGUARD CORE TX
TC MGUARD RS2000 3G	FL MGUARD PCI(E)4000
TC MGUARD RS4000 4G	FL MGUARD RS
TC MGUARD RS2000 4G	FL MGUARD PCI 533/266
FL MGUARD RS4000-P	FL MGUARD SMART 533/266
FL MGUARD RS4000 VPN-M	mGuard Centerport (Innominate)
FL MGUARD RS2000-B	mGuard delta (Innominate)

Please observe the following notes

User group of this manual

The use of products described in this manual is oriented exclusively to:

- Qualified electricians or persons instructed by them, who are familiar with applicable standards and other regulations regarding electrical engineering and, in particular, the relevant safety concepts.
- Qualified application programmers and software engineers, who are familiar with the safety concepts of automation technology and applicable standards.

Explanation of symbols used and signal words

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety measures that follow this symbol to avoid possible injury or death.

There are three different categories of personal injury that are indicated with a signal word.

DANGER This indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING This indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION This indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

This symbol together with the signal word **NOTE** and the accompanying text alert the reader to a situation which may cause damage or malfunction to the device, hardware/software, or surrounding property.

This symbol and the accompanying text provide the reader with additional information or refer to detailed sources of information.

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:
phoenixcontact.com

Make sure you always use the latest documentation.
It can be downloaded at:
phoenixcontact.net/products

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.
Subsidiary contact information is available at phoenixcontact.com.

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to:
tecdoc@phoenixcontact.com

General terms and conditions of use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular user documentation) does not constitute any further duty on the part of Phoenix Contact to furnish information on modifications to products and/or technical documentation. You are responsible to verify the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

In general, the provisions of the current standard Terms and Conditions of Phoenix Contact apply exclusively, in particular as concerns any warranty liability.

Phoenix Contact reserves the right to register its own intellectual property rights for the product identifications of Phoenix Contact products that are used here. Registration of such intellectual property rights by third parties is prohibited.

Other product identifications may be afforded legal protection, even where they may not be indicated as such.

Table of Contents

1 mGuard basics

The mGuard protects IP data links by combining the following functions:

– Industrial security network router (with built-in 4 or 5-port switch and DMZ port depending on the model).
– VPN router for secure data transmission via public networks (hardware-based DES, 3DES, and AES encryption, IPsec and OpenVPN protocol).
– Configurable firewall for protection against unauthorized access. The dynamic packet filter inspects data packets using the source and destination address and blocks undesired data traffic.

1.1 Basic properties of the mGuards

Network features

– Stealth (auto, static, multi), router (static, DHCP client), PPPoE (for DSL), PPTP (for DSL), and modem
– VLAN
– DHCP server/relay on the internal and external network interfaces
– DNS cache on the internal network interface
– Dynamic routing (OSPF)
– GRE tunneling
– Administration via HTTPS and SSH
– Optional conversion of DSCP/TOS values (Quality of Service)
– Quality of Service (QoS)
– LLDP
– MAU management
– SNMP

Firewall features

– Stateful packet inspection
– Anti-spoofing
– IP filter
– L2 filter (only in stealth mode)
– NAT with FTP, IRC, and PPTP support (only in “Router” network mode)
– 1:1 NAT (only in “Router” network mode)
– Port forwarding (not in “Stealth” network mode)
– Individual firewall rules for different users (user firewall)
– Individual rule sets as action (target) of firewall rules (apart from user firewall or VPN firewall)

Anti-virus features

– CIFS integrity check of network drives for changes to specific file types (e.g., executable files)

VPN features (IPsec)

– Protocol: IPsec (tunnel and transport mode, XAuth/Mode Config)
– IPsec encryption in hardware with DES (56 bits), 3DES (168 bits), and AES (128, 192, 256 bits)
– Packet authentication: MD5, SHA-1, SHA-265, SHA-384, SHA-512
– Internet Key Exchange (IKE) with main and quick mode
– Authentication via:

  - Pre-shared key (PSK)
  - X.509v3 certificates with public key infrastructure (PKI) with certification authority (CA), optional certificate revocation list (CRL), and the option of filtering by subject

  or

  - Remote certificate, e.g., self-signed certificates
- Detection of changing peer IP addresses via DynDNS
- NAT traversal (NAT-T)
- Dead Peer Detection (DPD): detection of IPsec connection aborts
- IPsec/L2TP server: connection of IPsec/L2TP clients
- IPsec firewall and 1:1 NAT
- Default route via VPN tunnel
- Data forwarding between VPNs (hub and spoke)
- Depending on the license: up to 250 VPN tunnels, in the case of mGuard centerport (Innominate)/FL MGUARD CENTERPORT up to 3000 active VPN tunnels
- Hardware acceleration for encryption in the VPN tunnel (except for mGuard centerport (Innominate)/FL MGUARD CENTERPORT)

VPN features (OpenVPN)

- OpenVPN client
- OpenVPN encryption with Blowfish, AES (128, 192, 256 bits)
- Dead Peer Detection (DPD)
- Authentication via user identifier, password or X.509v3 certificate
- Detection of changing peer IP addresses via DynDNS
- OpenVPN firewall and 1:1 NAT
- Routes via VPN tunnels can be configured statically and learned dynamically
- Data forwarding between VPNs (hub and spoke)
- Depending on the license: up to 50 VPN tunnels

Additional features

- Remote Logging
- VPN/firewall redundancy (depending on the license)
- Administration using SNMP v1 - v3 and Phoenix Contact Device Manager (mGuard device manager (FL MGUARD DM))
- PKI support for HTTPS/SSH remote access
- Can act as an NTP and DNS server via the LAN interface
- Compatible with mGuard Secure Cloud
- Plug-n-Protect technology
- Tracking and time synchronization via GPS/GLONASS positioning system
- COM Server

Support

In the event of problems with your mGuard, please contact your supplier.

For additional information on the device as well as release notes and software updates, visit: phoenixcontact.net/products.

1.2 Typical application scenarios

This section describes various application scenarios for the mGuard.

- Stealth mode (Plug-n-Protect)
- Network router
- DMZ (demilitarized zone)
- VPN gateway
- WLAN via VPN tunnel
- Resolving network conflicts
- Mobile router via integrated mobile network modem

1.2.1 Stealth mode (Plug-n-Protect)

In **stealth mode**, the mGuard can be positioned between an individual computer and the rest of the network.

The settings (e.g., for firewall and VPN) can be made using a web browser under the URL https://1.1.1.1/.

No configuration modifications are required on the computer itself.

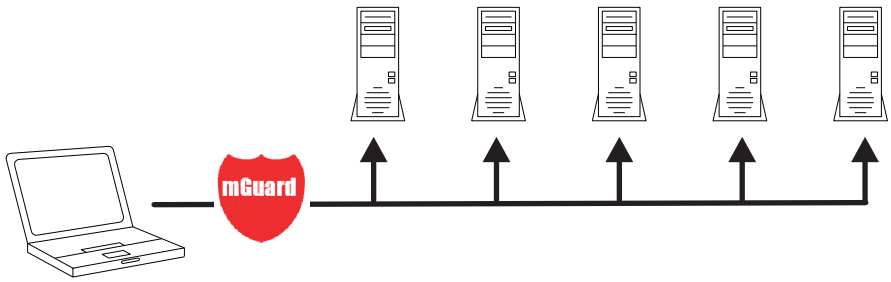


Figure 1-1 Stealth mode (Plug-n-Protect)

1.2.2 Network router

When used as a **network router**, the mGuard can provide the Internet connection for several computers and protect the company network with its firewall.

One of the following network modes can be used on the mGuard:

– *Router*, if the Internet connection is, for example, via a DSL router or a permanent line.
– *PPPoE*, if the Internet connection is, for example, via a DSL modem and the PPPoE protocol is used (e.g., in Germany).
– *PPTP*, if the Internet connection is, for example, via a DSL modem and the PPTP protocol is used (e.g., in Austria).
– *Modem*, if the Internet connection is via a serial connected modem (compatible with Hayes or AT command set).
– *Built-in mobile network modem*, mobile router via integrated mobile network modem

For computers in the Intranet, the mGuard must be specified as the default gateway.

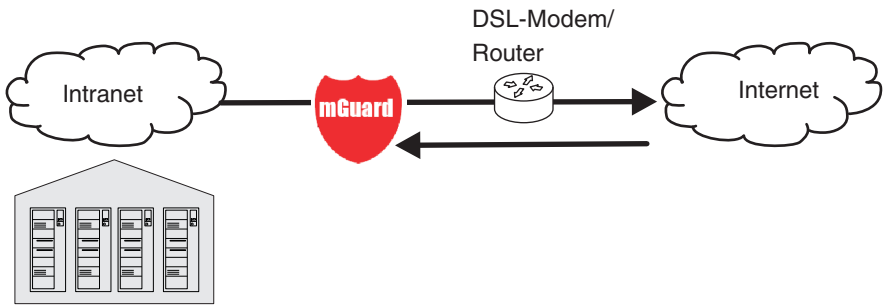


Figure 1-2 Network router

1.2.3 DMZ

A **DMZ** (demilitarized zone) is a protected network that is located between two other networks. For example, a company's website may be in the DMZ so that new pages can only be copied to the server from the Intranet via FTP. However, the pages can be read from the Internet via HTTP.

IP addresses within the DMZ can be public or private, and the mGuard, which is connected to the Internet, forwards the connections to private addresses within the DMZ by means of port forwarding.

A DMZ scenario can be established either between two mGuards (see Figure 1-3) or via a dedicated DMZ port of the TC MGUARD RS4000 3G, TC MGUARD RS4000 4G or FL MGUARD RS4004.

The DMZ port is only supported in router mode and requires at least one IP address and a corresponding subnet mask. The DMZ does not support any VLANs.

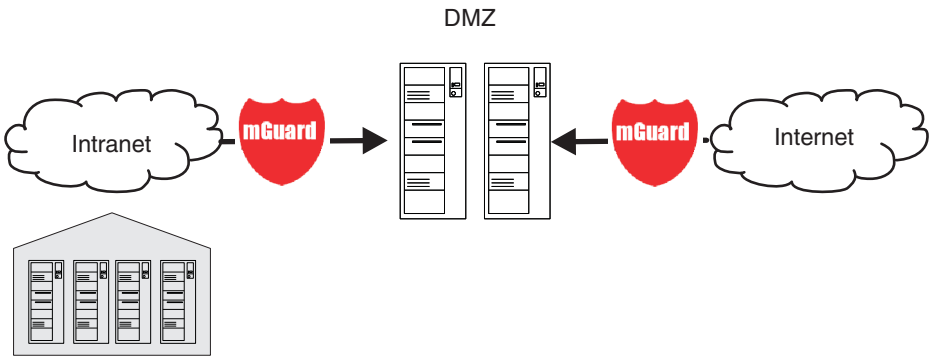


Figure 1-3 DMZ

1.2.4 VPN gateway

The **VPN gateway** provides company employees with encrypted access to the company network from home or when traveling. The mGuard performs the role of the VPN gateway.

IPsec-capable VPN client software must be installed on the external computers or failing that, the computer is equipped with an mGuard.

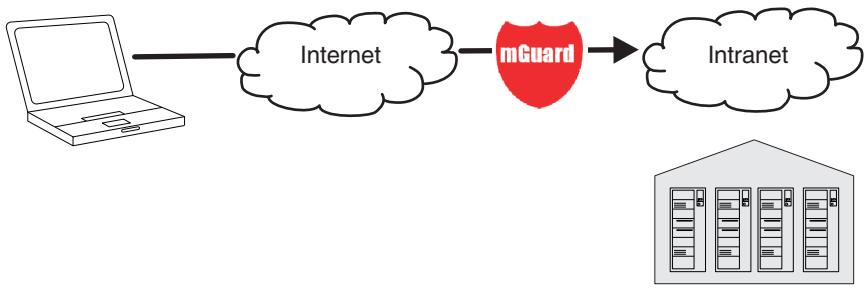


Figure 1-4 VPN gateway

1.2.5 WLAN via VPN

WLAN via VPN is used to connect two company buildings via a WLAN path protected using IPsec. The adjacent building should also be able to use the Internet connection of the main building.

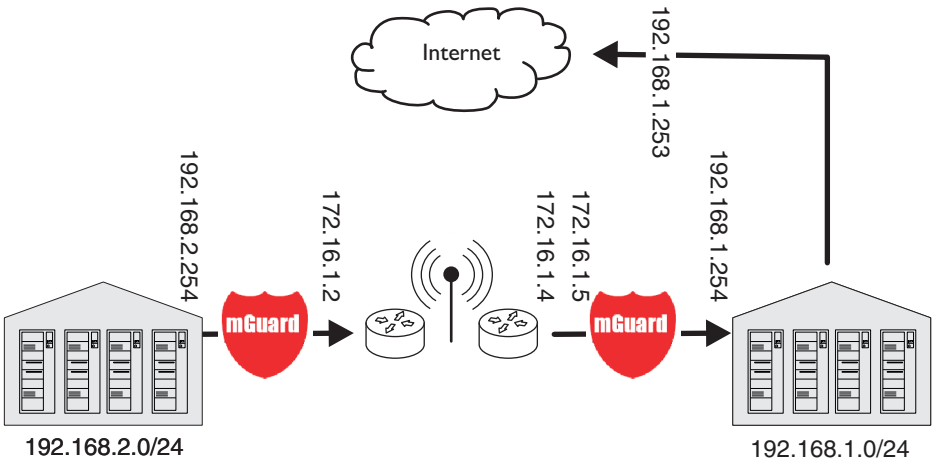


Figure 1-5 WLAN via VPN

In this example, the mGuards were set to *router* mode and a separate network with 172.16.1.x addresses was set up for the WLAN.

To provide the adjacent building with an Internet connection via the VPN, a default route is set up via the VPN:

Tunnel configuration in the adjacent building

Connection type	Tunnel (network <-> network)
Address of the local network	192.168.2.0/24
Address of the remote network	0.0.0.0/0

In the main building, the corresponding counterpart is configured:

Tunnel configuration in the main building

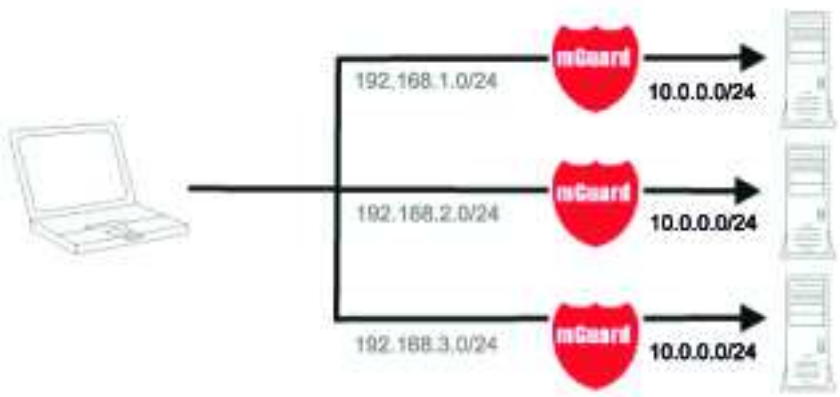
Connection type	Tunnel (network <-> network)
Local network	0.0.0.0
Address of the remote network	192.168.2.0/24

The default route of an mGuard usually uses the WAN port. However, in this case the Internet can be accessed via the LAN port:

Default gateway in the main building:

IP address of the default gateway	192.168.1.253

1.2.6 Resolving network conflicts



Resolving network conflicts

In the example, the networks on the right-hand side should be accessible to the network or computer on the left-hand side. However, for historical or technical reasons the networks on the right-hand side overlap.

The 1:1 NAT feature of the mGuard can be used to translate these networks to other networks, thereby resolving the conflict.

(1:1 NAT can be used in normal routing and in IPsec tunnels and in OpenVPN connections.)

2 Configuration help

2.1 Secure encryption

The mGuard generally offers the option to use different encryption and hash algorithms.

Some of the algorithms available are dated and are no longer regarded as reliable. This is why they are not to be recommended. Due to downwards compatibility, they can continue to be selected and used in mGuard.

In the following areas of the mGuard, the user must ensure that secure encryption and hash algorithms are used:

– IPsec VPN connections
– OpenVPN connections
– Shell Access (SSH)
– HTTPS Web Access (TLS/SSL)
– Encrypted State Synchronization of redundancy pairs

The secure use of encryption is explained in the following sections.

Further information can be found in the technical directive of the Federal office for information security: “BSI TR-02102 Cryptographic procedure: recommendations and key lengths”.

Using secure encryption and hash algorithms

Phoenix Contact recommends using encryption and hash algorithms according to the following table.

The following generally applies: the longer the key length (in bits), which is used in the encryption algorithm (specified by the appended number), the more secure it is.

Encryption	**Algorithm**	**Use**
	AES-256 AES-192 AES-128	Recommended
	3DES Blowfish	Do not use, if possible
	DES	Do not use
Hash/checksum	**Hash function**	**Use**
	SHA-512 SHA-384 SHA-256	Recommended
	SHA-1	Do not use, if possible
	MD5	Do not use

Use of secure SSH clients

Establishing encrypted SSH connections to the mGuard is initiated by the SSH client used. If the SSH client uses dated and thus insecure encryption algorithms, these are generally accepted by the mGuard.

Always use **Current SSH clients** (e.g. *putty*), to avoid use of weak encryption algorithms.

Use of secure web browsers

Establishing encrypted HTTPS connections (TLS/SSL) to the mGuard is initiated by the web browser used. If the web browser uses dated and thus insecure encryption algorithms, these are generally accepted by the mGuard.

Always use **Current web browsers** to avoid use of weak encryption algorithms.

Creation of secure X.509 certificates

X.509 certificates are generated using various software tools.

Always use **Current program versions** of the software tools to avoid use of weak encryption algorithms when creating X.509 certificates. The MD5 hash algorithm should not be used and SHA-1 not used as far as possible.

When creating X.509 certificates, use **key lengths of at least 2048 bits**.

2.2 ISA 62443-4-2 compliant use of the mGuard device

In order to operate the mGuard device in an environment compliant with Security Level SL 2-2-3-2-3-3-3-3-3-3 according to ISA 62443-4-2 Draft D4E1 dated January 12,2017, the conditions described below must be complied with:

1. The use of factory-set passwords (default passwords) is prohibited. This applies to the users *root* and *admin*.
2. Use a RADIUS server for user authentication. This concerns a user's logon to the mGuard device via web interface or SSH.

   Configure the mGuard device to allow RADIUS authentication as the only way to verify passwords (see "Use RADIUS authentication for shell access" on page 60 and "Enable RADIUS authentication" on page 75).
3. To configure the mGuard devices, use the management software *mGuard device manager* (mdm / FL MGUARD DM).

   Local configuration of the devices may only be performed by unique users with the "Netadmin" user role. The access rights of these users must be restricted individually as far as possible.

   The Netadmin user is created and managed in mdm. Use the mdm to restrict the user's rights (see *mdm User Manual 1.9.x*, available online or as a PDF in the PHOENIX CONTACT Web Shop).
4. The use of SNMP is prohibited! There is no unique user ID in this protocol.
5. Only use encrypted ECS files to back up mGuard configuration profiles. The use of unencrypted ECS files or ATV configuration profiles is prohibited (see "Configuration Profiles" on page 91).
6. Configure and use an external *syslog server* that triggers an alarm at least in the following cases:
   - failed login to the mGuard device (via all interfaces)
   - failed firmware update on the mGuard device due to corrupted update files
7. Operate the mGuard device only in a control cabinet whose door is connected to a service I/O of the mGuard device via a contact (switch or button). Configure the mGuard device in such a way that an alarm (e. g. by e-mail or SMS) is triggered each time the control cabinet door is opened (see "Trap" on page 102 and "Management >> Service I/O" on page 116).

2.3 Suitable web browsers

The device is configured via a graphic user interface in the web browser.

Always use **Current web browsers** to avoid use of weak encryption algorithms.

Current versions of the following web browsers are supported:

– Mozilla Firefox
– Google Chrome
– Microsoft Internet Explorer
– Apple Safari

Limitation of login attempts

In the event of a Denial of Service attack, services are intentionally made unable to function. To prevent this type of attack, the mGuard is provided with a choke for different network requests.

This feature is used to count all the connections going out from one IP address and using a specific protocol. When a specific number of connections is counted without a valid login, the choke becomes effective. If no invalid connection attempt is made for 30 seconds, the choke is reset. Each new request without valid login from this IP address resets the timer by 30 seconds.

The number of connection attempts that need to fail until the choke becomes effective depends on the protocol.

– 10 when using HTTPS
– 6 when using SSH, SNMP, COM server

2.4 User roles

root	User role without restrictions
admin	Administrator
netadmin	Administrator for the network only
audit	Auditor/tester
mobile	Sending text messages

The predefined users (*root*, *admin*, *netadmin*, *audit*, and *mobile*) have different permissions.

– The *root* user has unrestricted access to the mGuard.
– The *admin* user also has unrestricted functional access to the mGuard, however the number of simultaneous SSH sessions is limited.
– Permissions are explicitly assigned to the *netadmin* user via the mGuard device manager (FL MGUARD DM). This user only has read access to the other functions. Passwords and private keys cannot be read by this user.
– The *audit* user only has read access to all functions. By default, the *audit* user role can only be activated via the mGuard device manager (FL MGUARD DM), in the same way as *netadmin*.
– The *mobile* user can send text messages with the mGuard using a CGI script. Further functions cannot be accessed by the *mobile* user (see "CGI actions" on page 449).

2.5 Input help during configuration (system messages)

With firmware 8.0 or later, modified or invalid entries are highlighted in color on the web interface.

System messages which explain why an entry is invalid, for example, are also displayed.

In order to support this, JavaScript must be enabled in the web browser used.

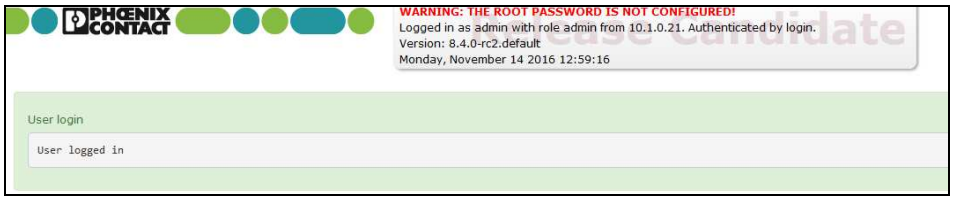


Figure 2-1 Example system message

– **Modified entries** are highlighted in **green** on the relevant page and in the associated menu item until the changes are applied or reset. In the case of tables, it is only indicated that a table row has been modified or removed; the modified value is not indicated.
– **Invalid entries** are highlighted in **red** on the relevant page and tab and in the associated menu item.

The modified or invalid entries remain highlighted even when you close a menu.

When necessary, information relating to the system is displayed at the top of the screen.