

SIEMENS

SIMATIC NET

Industrial Remote Communication Remote Networks SCALANCE M875

Operating Instructions




Preface

Description of the device	1
Configuration examples	2
Installation, connecting up, commissioning	3
Configuration	4
Maintenance and diagnostics	5
Technical specifications	6
Certification	7
Additional Internal Routes	A
Training, Service & Support	B

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

 DANGER
indicates that death or severe personal injury will result if proper precautions are not taken.
 WARNING
indicates that death or severe personal injury may result if proper precautions are not taken.
 CAUTION
indicates that minor personal injury can result if proper precautions are not taken.
NOTICE
indicates that property damage can result if proper precautions are not taken.


If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

 WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Preface

Purpose of this documentation

This manual will help you during the configuration, installation, commissioning and operation of the 3G/UMTS router SCALANCE M875.

Device name

In the remainder of the text, the SCALANCE M875 is also simply known as the "M875".

Validity of the documentation

This manual is valid for the following product:

SCALANCE M875
Firmware version 2.112
Hardware product version 1.0

Order number:
6GK5 875-0AA10-1AA2
6GK5 875-0AA10-1CA2 (variant for Japan)

New in this release

- Optimization of several functions with the firmware version named above
- Editorial revision

Replaced documentation

This manual replaces the manual release 01/2012.

Current manual release on the Internet

You will also find the current version of this manual on the Internet pages of Siemens Automation Customer Support under the following entry ID:

61505654 (<http://support.automation.siemens.com/WW/view/en/61505654>)

Purpose of the device

SCALANCE M875 is a 3G/UMTS router with HSPA and VPN functionality for industrial applications.

 **WARNING**

Impairment of medical devices and data media

The device contains a wireless transmitter that could, under certain circumstances, impair the functionality of electronic medical devices such as hearing aids or pacemakers. Do not use the device in places where the operation of wireless devices is prohibited. You can obtain advice from your physician or the manufacturer of such devices.

To prevent data media from being demagnetized, do not keep disks, credit cards or other magnetic data media near the device.

Connection costs

Note

Note that both when establishing a connection and when attempting to establish a connection and when a connection is obtained, frames are exchanged that will be charged by the provider.

Firmware with open source GPL/LGPL

The firmware of the M875 includes open source software under terms of GPL/LGPL. According to section 3b of GPL and section 6b of LGPL we offer you the source code. Please write to:

s_opsource@gmx.net
s_opsource@gmx.de

Please enter 'Open Source M875' as the subject of your e-mail, so that we can filter out your e-mail easier.

Firmware with OpenBSD

The firmware of M875 contains sections from the OpenBSD software. The use of OpenBSD software obligates the user to publish the following copyright notice:

```
* Copyright (c) 1982, 1986, 1990, 1991, 1993
* The Regents of the University of California. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
```

* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above
* copyright notice, this list of conditions and the following
* disclaimer in the * documentation and/or other materials
* provided with the distribution.
* 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgement:
* This product includes software developed by the University of
* California, Berkeley and its contributors.
* 4. Neither the name of the University nor the names of its
* contributors may be used to endorse or promote products derived
* from this software without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS"
* AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
* THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
* PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE
* REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
* INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
* (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
* INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
* WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
* NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
* USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
* OF SUCH DAMAGE.

Security messages

Note

Siemens offers IT security mechanisms for its automation and drive product portfolio in order to support the safe operation of the plant/machine. Our products are also continuously developed further with regard to IT security. We therefore recommend that you regularly check for updates of our products and that you only use the latest versions. You will find information in:

<http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo2&aktprim=99&lang=en>

Here, you can register for a product-specific newsletter.

For the safe operation of a plant/machine, however, it is also necessary to integrate the automation components into an overall IT security concept for the entire plant/machine, which corresponds to the state-of-the-art IT technology. You will find information on this in:

<http://www.siemens.com/industrialsecurity>

Products from other manufacturers that are being used must also be taken into account.

Where to find Siemens documentation

- You will find the order numbers for the Siemens products of relevance here in the following catalogs:
 - SIMATIC NET Industrial Communication / Industrial Identification, catalog IK PI
 - SIMATIC Products for Totally Integrated Automation and Micro Automation, catalog ST 70

You can request the catalogs and additional information from your Siemens representative.

- You will find SIMATIC NET manuals on the Internet pages of Siemens Automation Customer Support:

Link to Customer Support (<http://support.automation.siemens.com/WW/view/en>)

Enter the entry ID of the relevant manual as the search item. The ID is listed below some of the reference entries in brackets.

As an alternative, you will find the SIMATIC NET documentation on the pages of Product Support:

10805878 (<http://support.automation.siemens.com/WW/view/en/10805878>)

Go to the required product group and make the following settings:

→ Entry list → Entry type "Manuals / Operating Instructions"

You will find the documentation for the SIMATIC NET products relevant here on the data medium that ships with the product:

- Product CD / product DVD or
- SIMATIC NET Manual Collection

Table of contents

	Preface	3
1	Description of the device	11
1.1	Connection via mobile wireless and Internet	11
1.2	Functions.....	12
1.3	Appearance of the device	14
1.4	Interfaces	15
1.5	LEDs to display operation	15
1.6	Service button SET	16
1.7	Requirements for operation	17
2	Configuration examples	19
2.1	Internet access via the mobile wireless network.....	19
2.2	TELECONTROL via the mobile wireless network	20
2.3	Direct communication between stations using mobile wireless	21
2.4	Remote maintenance solutions.....	22
2.4.1	Mobile access to plants and plant sections	23
2.4.2	Plant access via a remote maintenance center	24
3	Installation, connecting up, commissioning	25
3.1	Safety notices.....	25
3.2	Connecting	26
3.3	Steps in commissioning	30
3.4	Inserting the SIM card.....	31
3.5	Installation	32
4	Configuration	33
4.1	Settings on the admin PC	33
4.1.1	TCP/IP configuration in Windows XP	34
4.1.2	Permitted characters.....	35
4.1.3	Establishing the configuration connection	36
4.1.4	Basics of configuration.....	38
4.1.5	Language selection.....	39
4.2	Start page of the Web user interface - Overview.....	40
4.3	System	44
4.3.1	System time	44
4.3.2	Log	47
4.3.3	Device identification	48

4.4	Local Network	49
4.4.1	Local interface	49
4.4.2	Local IP addresses.....	49
4.4.3	DHCP server on local network.....	51
4.4.4	Local hostname.....	54
4.4.5	DNS server on local network.....	55
4.4.6	Additional Internal Routes	57
4.5	External Network.....	58
4.5.1	External interface	58
4.5.2	UMTS/EDGE - access parameters	58
4.5.3	Installation mode - aligning antennas	64
4.5.4	Traffic volume supervision	65
4.5.5	Checking the connection - Connection monitoring	68
4.5.6	Hostname by DynDNS	71
4.5.7	SRS - Siemens Remote Service.....	73
4.5.8	NAT - Network Address Translation	75
4.6	Security	76
4.6.1	Firewall rules	76
4.6.2	Port Forwarding.....	81
4.6.3	Advanced security functions	83
4.6.4	Firewall Log	84
4.7	IPsec VPN - Virtual Private Network.....	85
4.7.1	Explanation of VPN connections.....	85
4.7.2	Connections - Roadwarrior mode	89
4.7.2.1	Creating connections	89
4.7.2.2	Editing connections	90
4.7.2.3	IKE settings	91
4.7.3	Connections - Standard mode	95
4.7.3.1	Creating connections	95
4.7.3.2	Editing connections	96
4.7.3.3	IKE settings	99
4.7.3.4	Firewall rules for VPN tunnel.....	103
4.7.4	Managing certificates and keys.....	105
4.7.5	Supervision of the VPN connections.....	106
4.7.6	Advanced settings.....	109
4.7.7	Status	111
4.8	Remote access	112
4.8.1	Changing the password	112
4.8.2	HTTPS.....	113
4.8.3	CSD.....	115
4.9	SMS.....	116
4.9.1	Service Center (SMSC).....	116
4.9.2	Alarm SMS	116
4.9.3	Sending SMS over IP messages from the local area network.....	118
4.10	SNMP	121
4.10.1	Settings	121
4.10.2	SNMP traps	124

5	Maintenance and diagnostics	129
5.1	Calling the Maintenance Web pages	129
5.2	Updating the firmware	129
5.3	Configuration profiles	131
5.4	Reboot.....	134
5.5	Remote logging	135
5.6	Firmware information	137
5.7	Hardware Info.....	138
5.8	Snapshot.....	138
5.9	Factory settings.....	139
6	Technical specifications.....	141
7	Certification.....	145
A	Additional Internal Routes.....	149
B	Training, Service & Support.....	151
	Glossary	153
	Index.....	163

Description of the device

1.1 Connection via mobile wireless and Internet

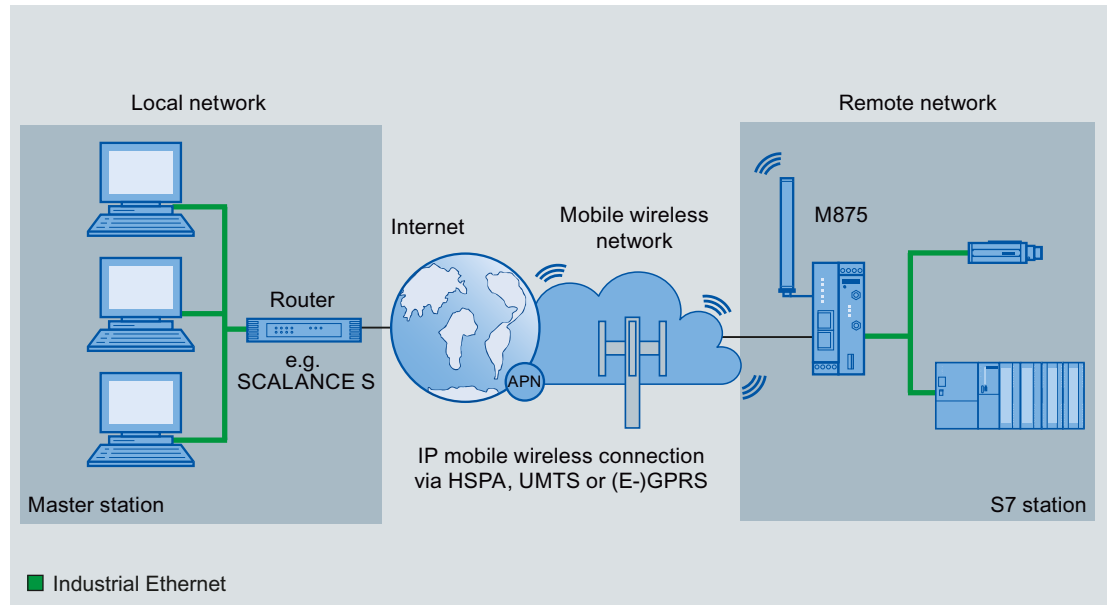


Figure 1-1 Example of connecting a station to the master station via Internet and mobile wireless

Wireless connection via the mobile wireless network

With the M875, you can establish wireless access to the Internet or to a private network. This is possible at any location at which a mobile wireless network is available that provides packet-oriented data services.

With UMTS, these are the data services HSPA Data Service or UMTS Data Service.

With GSM, these are the data services EGPRS or GPRS.

For the wireless connection, you require a SIM card of a mobile wireless provider with the required data services activated.

The M875 can then connect locally attached applications or entire networks to the Internet. Direct connections via an intranet to external partners connected to it are also possible with the M875.

Private and public VPN

Via the public mobile wireless network, the M875 can establish a Virtual Private Network (VPN) between one or more local networks and one or more remote networks. These connections are protected from access by third parties by Internet Protocol Security (IPsec).

Here, communication is possible both via a public as well as a private VPN tunnel.

You will find detailed examples of the potential uses of the M875 in the following section Configuration examples (Page 19).

This means that the device performs various functions:

- Router for connecting networks via mobile wireless
- Wireless modem for flexible data communication using UMTS, HSPA, EGPRS or GPRS
- VPN router for secure data transfer in public networks with IPsec, 3DES data encryption and AES encryption.
- Firewall for protection against unauthorized access. The dynamic packet filter examines frames based on their source and destination addresses (stateful inspection firewall) and blocks undesirable data traffic (anti-spoofing).

1.2 Functions

Configuration

The device can be configured using a Web user interface that can be displayed simply using a Web browser.

You can access the Web user interface in the following ways:

- Via the local interface X2
- Via the mobile wireless connections HSPA, UMTS, EGPRS and GPRS

This requires access via DynDNS and an accessible public IP address.

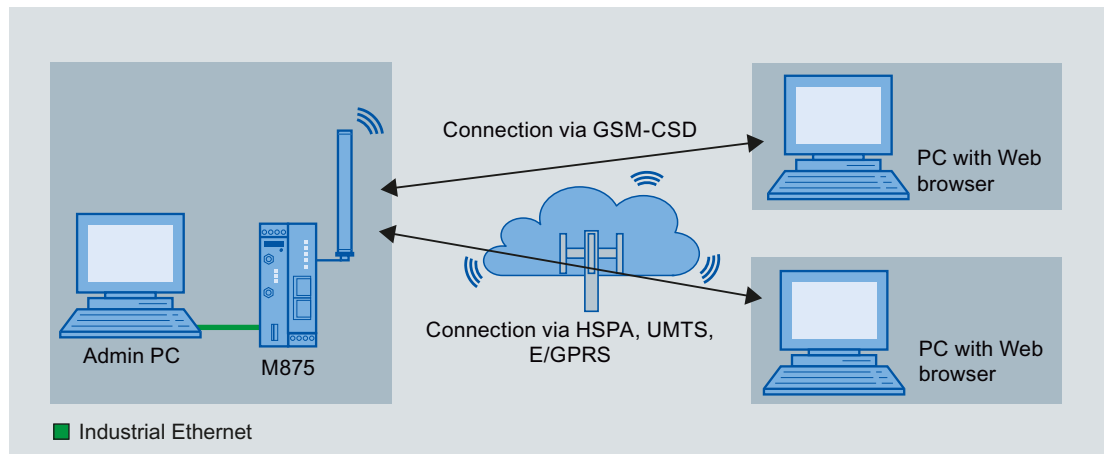


Figure 1-2 Configuration connections

VPN functions

To establish a VPN, the following functions are available:

- Private and public VPN
- IPsec as VPN tunnel protocol
- IPsec-3DES encryption with 168 bits
- IPsec-AES encryption with 128, 192 and 256 bits
- Packet authentication MD5 and SHA-1
- Internet Key Exchange (IKE) with main mode and aggressive mode
- Authentication by pre-shared key (PSK), X.509v3 certificate and CA
- Dead peer detection (DPD)

The M875 also supports the SOFTNET Security Client (SSC) as of version 3.0 in Windows XP and Windows 7.

Firewall functions

The M875 provides the following firewall functions to protect the local network and itself from external attacks:

- Stateful inspection firewall
- Anti-spoofing
- Port forwarding

Further functions

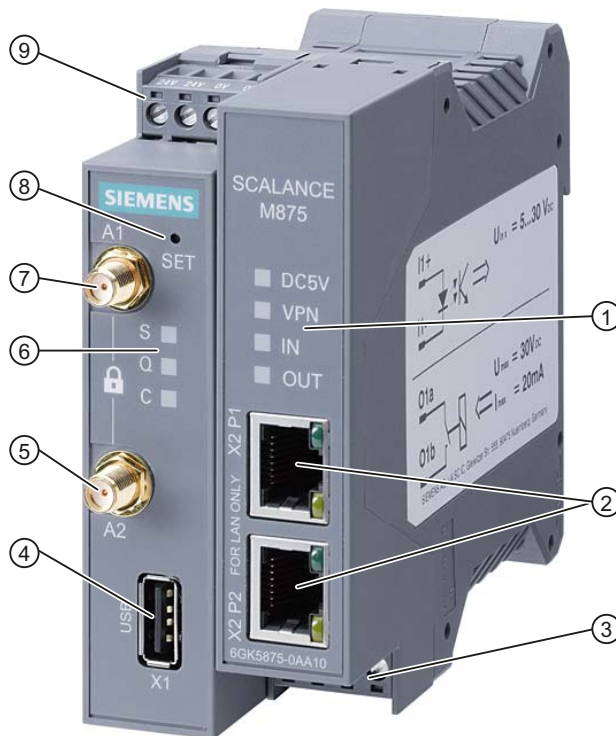
The M875 also supports the following extra functions:

- DNS caching
- DHCP server
- NAT, NAT-T, 1:1-NAT
- NTP
- Remote logging
- In port for triggering alarm SMS messages
- Out port for signaling existing VPN connections
- Web user interface for configuration
- Sending freely configured alarm SMS messages
- Sending SMS messages from the local area network
- DynDNS client
- Remote access with HTTPS
- SNMP and SNMP traps
- Traffic volume supervision

1.3 Appearance of the device

- Installation mode for aligning the antennas
- Information for device identification

1.3 Appearance of the device



- ① LEDs DC5V, VPN, IN, OUT
- ② 2-port switch with the ports "X2P1" and "X2P2" for connection to the local area network, RJ-45 jacks each with 2 LEDs
- ③ Terminals for in port and out port (on the underside of the device)
- ④ X1, USB connector (currently without function)
- ⑤ Antenna socket "A2", type SMA (only for the extra antenna)
- ⑥ LEDs S, Q, C
- ⑦ Antenna socket "A1", type SMA (for the first connected antenna)
- ⑧ Service button SET
- ⑨ Terminals for connecting the supply voltage (top of device)

1.4 Interfaces

Connection to a the local area network

For the LAN connection to the local area network, the M875 has a switch with the two ports "X2P1" and "X2P2". The two ports can be configured with different IP addresses.

Connect your local area network via port X2P1 or X2P2.

Note

No use of the M875 as a router between internal subnets

Do not use the M875 as a router between internal subnets.

Connection to the remote network

For the wireless connection to the remote network, the M875 has two SMA sockets. If you only connect a single antenna, use the upper SMA socket "A1" of the M875.

1.5 LEDs to display operation

The LEDs on the M875 provide information about the operating status of the device.

Meaning of the LEDs on the left-hand side of the device

LED	Status	Meaning
S (Status)	Flashing slowly	PIN transfer
	Flashing quickly	PIN error/ SIM error
	On	PIN transfer successful
Q (Quality)	Off	Not logged into GSM network
	Flashing briefly	Poor signal strength (CSQ < 6)
	Flashing slowly	Medium signal strength (CSQ= 6 to 10)
	On, with brief interruptions	Good signal strength (CSQ 11 to 18)
C (Connect)	On	Very good signal strength (CSQ > 18)
	Off	No connection
	Flashing slowly	EGPRS/GPRS connection active
S, Q, C simultaneousl y	On	HSPA/UMTS connection active
	Flash on and off in sequence (fast)	Device startup
	Flash on and off in sequence (slow)	Transfer of new firmware
	Flashing fast (in sync)	Error

Meaning of the LEDs on the right-hand side of the device

LED	Status	Meaning
DCV5	On	Device turned on, power supply present.
	Off	Device turned off, no power supply.
VPN	On	At least one VPN connection established
	Off	No VPN connection established
IN	On	In port active
	Off	In port not active
OUT	On	Out port active
	Off	Out port not active

Meaning of the two LEDs on the connectors X2P1 or X2P2

LED	Status	Meaning
Green LED (top)	RX/TX	
	Flashing	Data transfer via the Ethernet connection
	Off	No data transfer via the Ethernet connection
Yellow LED (bottom)	Link status	
	On	Existing Ethernet connection to the local application or the local area network
	Off	No Ethernet connection to the local application or the local area network

1.6 Service button SET

In the small hole labeled SET, there is a button that is used to reboot the device. During a reboot, the device is reset to its factory settings.

You can press the button with a thin object, for example a straightened paper clip.

You will find more information on resetting the device in the section Factory settings (Page 139).

1.7 Requirements for operation

Antenna

To operate the M875, you require one or two antennas that are tuned to the frequency bands of the mobile wireless provider you have selected.

- With GPRS transmission: 850 MHz, 900 MHz, 1800 MHz or 1900 MHz
- With UMTS transmission: 850 MHz, 1700 MHz, 1900 MHz or 2100 MHz.

Use only antennas from the accessories for the SCALANCE M875.

For more detailed information, refer to section Connecting (Page 26).

Power supply

You require a power supply with a voltage between 12 VDC and 30 VDC that can provide sufficient current.

For more detailed information, refer to section Connecting (Page 26).

SIM card

You require a SIM card of your mobile wireless provider with the corresponding PIN (Personal Identification Number).

- Activation for packet-oriented data services

The SIM card must be activated for packet-oriented data services HSPA (HSUPA and HSDPA), UMTS, EGPRS and GPRS by your mobile wireless provider.

- Access data for the mobile wireless network

The following access data must be present:

- Access point name (APN)
- User name
- Password

For more detailed information, refer to section UMTS/EDGE - access parameters (Page 58).

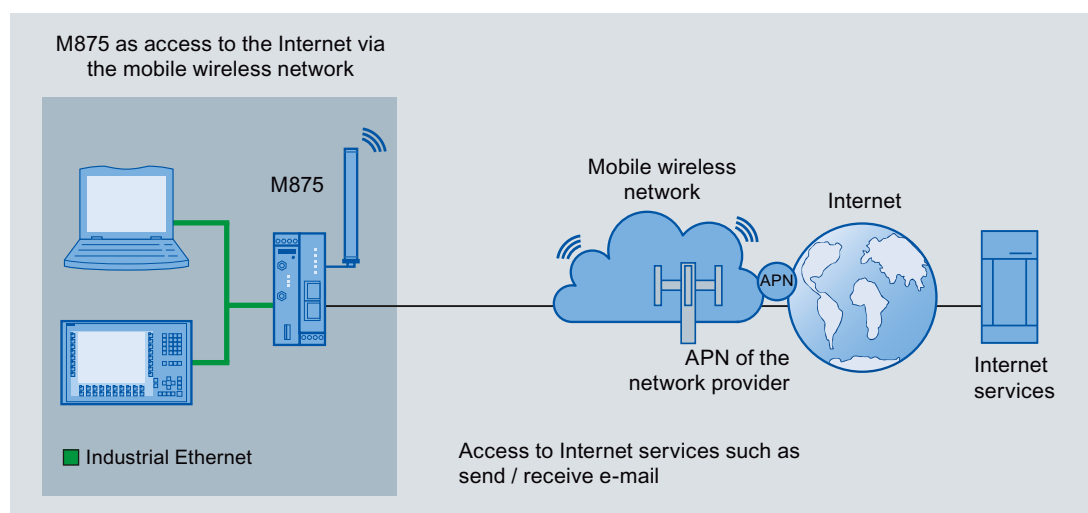
Configuration examples

The UMTS router SCALANCE M875 has a wide variety of possible uses in various areas of application. In this section, you will find configuration examples for the following:

- Internet access via the mobile wireless network
- Direct communication from station to station via mobile wireless with VPN
- TELECONTROL via the mobile wireless network
- Mobile access to plants
- Plant access via a remote maintenance center

With all the examples, you should first familiarize yourself with the security instructions and commission the device as described in section Installation, connecting up, commissioning (Page 25).

2.1 Internet access via the mobile wireless network



With the M875, you can access the Internet via the mobile wireless network. This means that the Internet services, for example sending and receiving e-mail or information from the World Wide Web are available to you.

Procedure

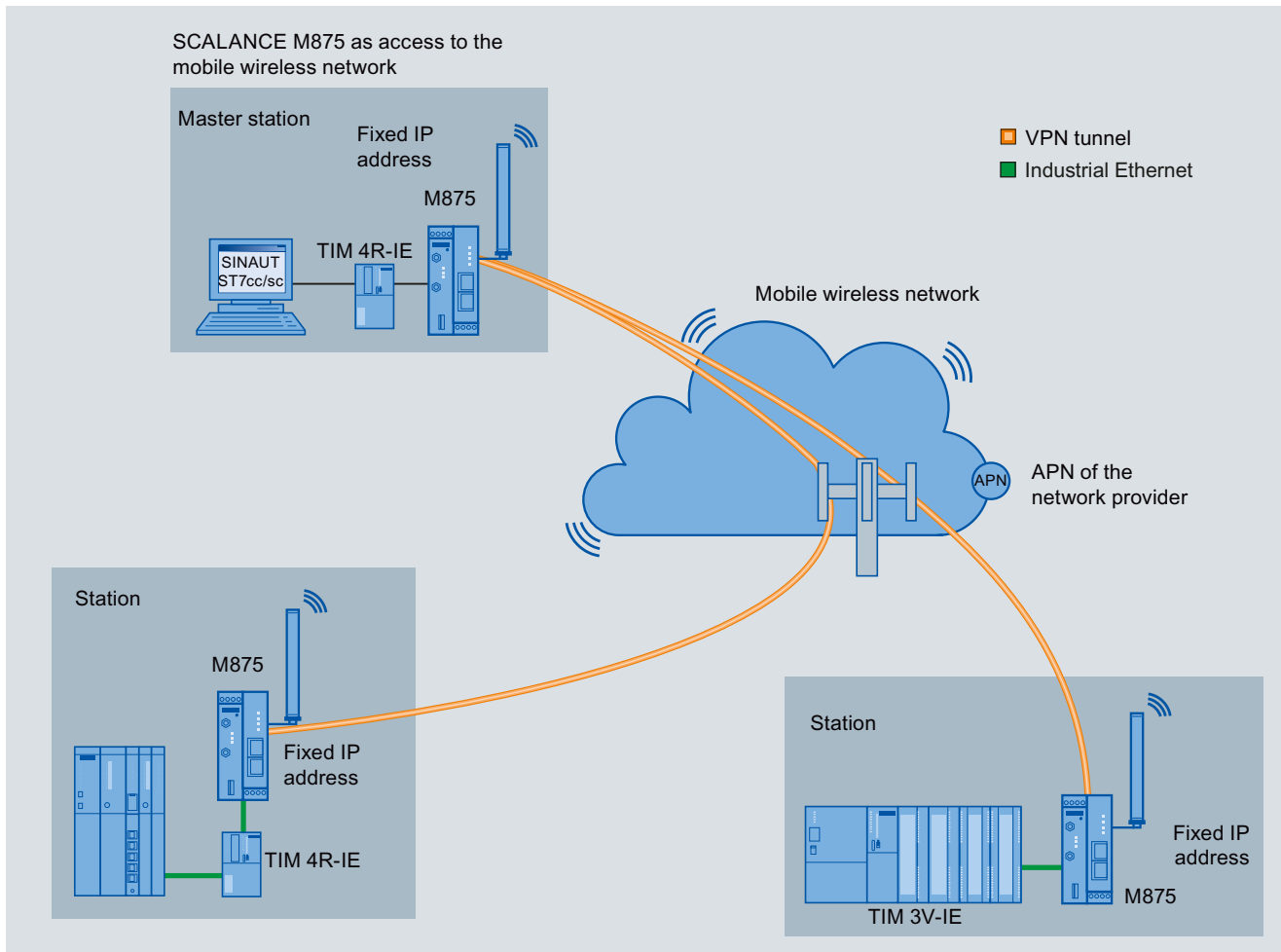
To configure Internet access via the mobile wireless network, follow the steps below:

1. Establish a configuration connection between the M875 and the connected PC.
See section Settings on the admin PC (Page 33).
2. Establish a connection to the mobile wireless network.
See section UMTS/EDGE - access parameters (Page 58).

2.2 TELECONTROL via the mobile wireless network

3. To allow access to the required Internet services, set up firewall rules. See section Security (Page 76).
4. Set up your application for the Internet services, for example for sending/receiving e-mails.

2.2 TELECONTROL via the mobile wireless network



You can use the M875 to transfer process data from remote stations via the mobile wireless network to the master station. The VPN function provides the necessary protection during data transfer in the public mobile wireless network.

Requirements

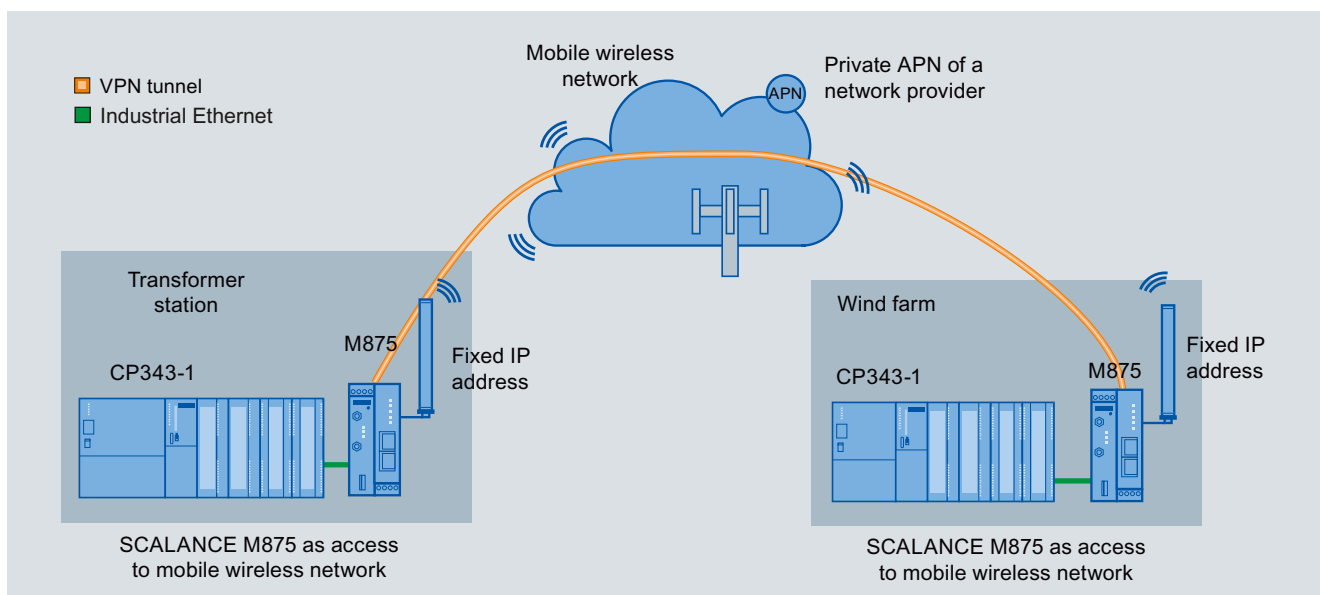
You require Internet access capable of VPN at both ends, for example using the M875 and a SCALANCE S6xx. To establish a VPN tunnel, you also require additional services from your mobile wireless provider that support direct communication between mobile wireless routers. This requires a fixed IP address for mobile wireless devices and/or an access to the Internet via a private APN.

Procedure

To set up one or more VPN tunnels for data transfer, follow the steps below:

1. Establish a configuration connection between the M875 and the connected Admin PC. See section Settings on the admin PC (Page 33).
2. Establish a connection to the mobile wireless network. See section UMTS/EDGE - access parameters (Page 58).
3. Set up the local SINAUT applications for data communication.
4. Connect the local SINAUT applications, for example TIM 4R-IE to the local interface of the M875. See Connecting (Page 26) and section Local Network (Page 49).
5. Establish a VPN connection. See section Connections - Standard mode (Page 95). Requirement: Fixed IP addresses and private APN.

2.3 Direct communication between stations using mobile wireless



You can also connect controllers to the M875 and transfer data via the mobile wireless network event-driven, for example between a wind farm and a transformer station. Communication is direct between the mobile wireless devices and not via a server. The VPN function provides the necessary protection during data transfer in the public mobile wireless network.

Requirements

To establish a VPN tunnel, you require additional services from your mobile wireless provider that support direct communication between mobile wireless routers. This requires a fixed IP address for mobile wireless devices and/or an access to the Internet via a private APN.

Procedure

To configure data transfer via a VPN tunnel, follow the steps below:

1. Set up the connected controllers, for example CP 343-1 for data communication.
2. Establish a configuration connection between the M875 and the connected Admin PC. See section Settings on the admin PC (Page 33).
3. Establish a connection to the mobile wireless network. See section UMTS/EDGE - access parameters (Page 58).
4. Connect a controller, for example a CP 343-1 to the local interface of the M875. See section Connecting (Page 26) and Local Network (Page 49).
5. Establish a VPN connection between the two M875 devices. See section Connections - Standard mode (Page 95). Requirement: Fixed IP addresses and private APN.

2.4 Remote maintenance solutions

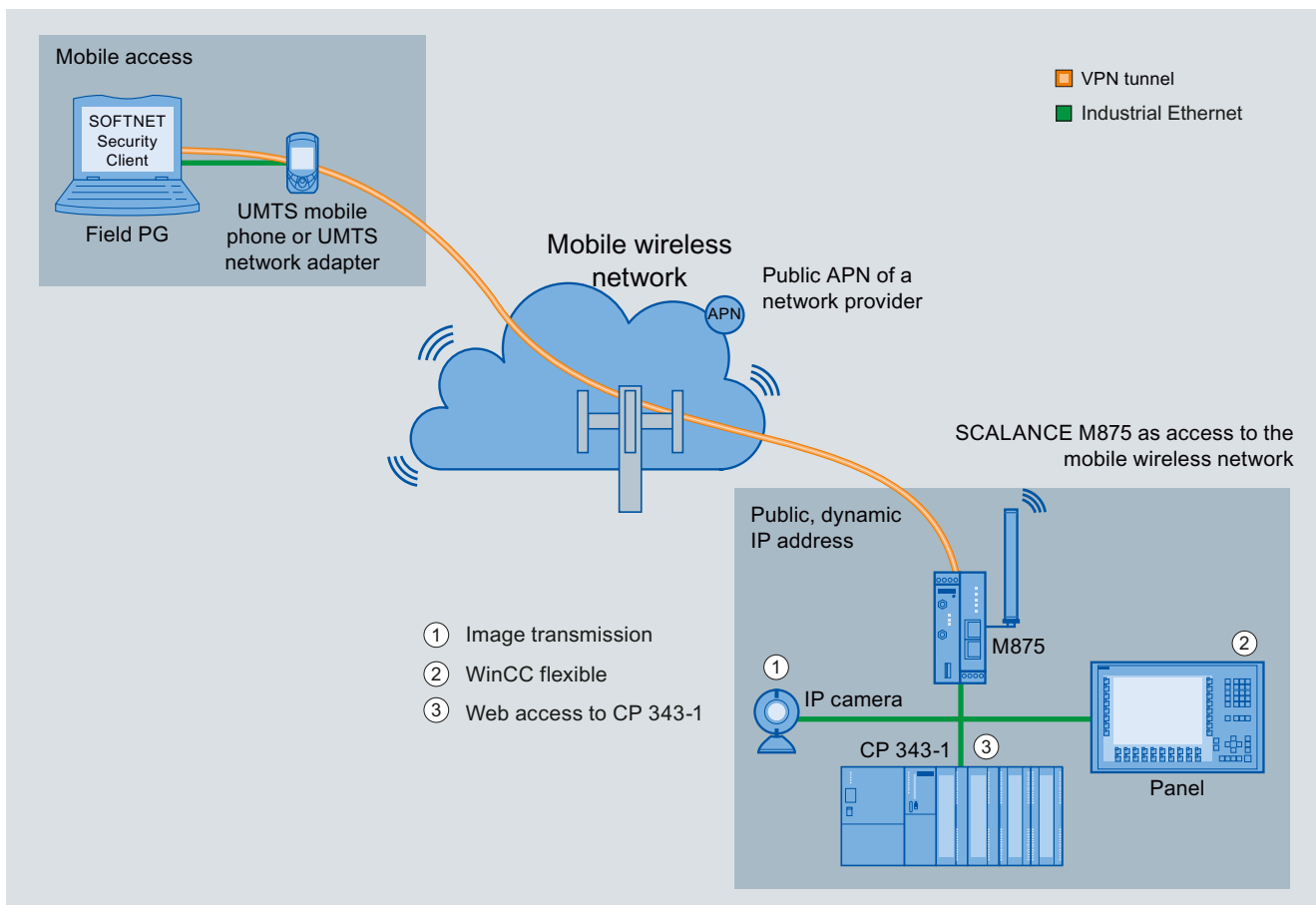
With the SCALANCE M875, you can implement the following remote maintenance tasks:

- Remote diagnostics
- Remote programming
- Status monitoring, for example with condition monitoring systems

You can access remote plants while traveling and perform remote maintenance work via the M875. To be able to do this, you require mobile field PGs equipped with a mobile phone capable of UMTS or a network adapter capable of UMTS. The example in the section Mobile access to plants and plant sections (Page 23) describes this use case.

Another variant is access via the M875 to a plant from a remote maintenance master station. You have the option of linking several subnets of the master station with several subnets of a plant. This situation is described in the section Plant access via a remote maintenance center (Page 24).

2.4.1 Mobile access to plants and plant sections



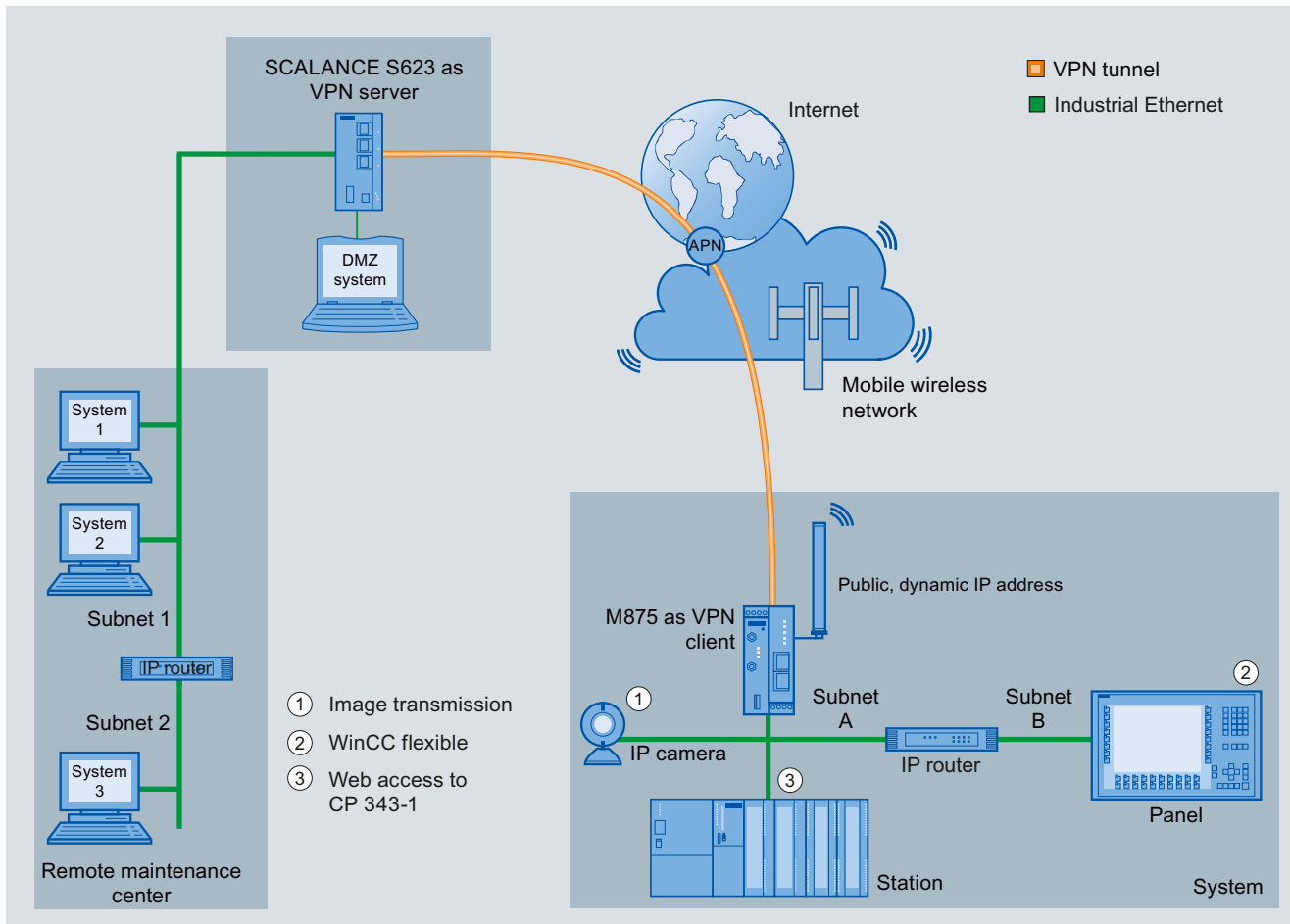
Procedure

To be able to access a plant via a VPN tunnel when traveling, note the following points and the relevant sections in these operating instructions:

1. Establish a configuration connection between the M875 and the connected Admin PC. See section Settings on the admin PC (Page 33).
2. Establish a connection to the mobile wireless network. See section UMTS/EDGE - access parameters (Page 58).
3. Connect the local applications to the local interface of the M875. See Connecting (Page 26) and section Local Network (Page 49).
4. Set up the connected applications of the plant for data communication.
5. Set up a VPN tunnel in Roadwarrior mode for the M875. See section Connections - Roadwarrior mode (Page 89).
Note: You can also perform this step with the Security Configuration Tool.
6. Set up a VPN tunnel on the mobile access page in the SOFTNET Security Client.
Note: You can also perform this step with the Security Configuration Tool.

To establish a connection from a remote station with SOFTNET Security Client to the M875, a VPN connection in Roadwarrior mode with IKE settings "Main mode" and certificate exchange needs to be set up on the M875.

2.4.2 Plant access via a remote maintenance center



Procedure

To be able to access a plant via a remote maintenance master station, note the following points and the relevant sections in these operating instructions.


1. Establish a configuration connection between the M875 and the connected Admin PC. See section Settings on the admin PC (Page 33).
2. Establish a connection to the mobile wireless network. See section UMTS/EDGE - access parameters (Page 58).
3. Connect the local applications to the local interface of the M875. See Connecting (Page 26) and section Local Network (Page 49).
4. Set up the connected applications of the plant for data communication.
5. Configure the VPN connection for the remote maintenance master station on the SCALANCE S623 with the Security Configuration Tool.
6. Set up a VPN tunnel in standard mode. See section Connections - Roadwarrior mode (Page 89).

Installation, connecting up, commissioning

3.1 Safety notices

Safety notices on the use of the device

The following safety notices must be adhered to when setting up and operating the device and during all associated work such as installation, connecting up or replacing devices.

<p> WARNING</p> <p>The equipment is designed for operation with Safety Extra-Low Voltage (SELV) by a Limited Power Source (LPS).</p> <p>This means that only SELV / LPS complying with IEC 60950-1 / EN 60950-1 / VDE 0805-1 must be connected to the power supply terminals. The power supply unit for the equipment power supply must comply with NEC Class 2, as described by the National Electrical Code (r) (ANSI / NFPA 70).</p> <p>If the equipment is connected to a redundant power supply (two separate power supplies), both must meet these requirements.</p>
--

External power supply

Use only an external power supply that complies with EN60950. The output voltage of the external power supply must not exceed 30 VDC. The output of the external power supply must be short-circuit proof.

<p>NOTICE</p> <p>The power supply unit to supply the SCALANCE M875 must comply with the requirements for a limited power source according to IEC/EN 60950-1, section 2.5.</p> <p>The external power supply for the SCALANCE M875 must meet the requirements for NEC class 2 circuits as specified in the National Electrical Code ® (ANSI/NFPA 70).</p>
--

Refer to the section Connecting (Page 26) and the installation instructions and instructions for use of the manufacturer of the power supply, the battery or the accumulator.

In ports / out ports

The in port and the out port are electrically isolated from the other connectors of the M875.

If an installation connected to the M875 electrically connects a signal of the in port or out port with the power supply, the following applies: A voltage of 60 V between each signal of the in port or out port and each connector of the power supply must not be exceeded.

3.2 Connecting

Interface X2

Connect your local area network via port X2P1 or X2P2.

Note

No use of the M875 as a router between internal subnets

Do not use the M875 as a router between internal subnets.

Connect the local network with the local applications to Ethernet interface X2, for example a programmable logic controller, a machine with an Ethernet interface for remote monitoring or a PC.

To set up the M875, connect the Admin PC with a Web browser to one of the two connectors.

For the connection, use a crossover cable or a patch cable with an RJ-45 plug. You will find the properties of the X2 interface in the technical specifications.

In port and out port

The M875 has an in port and an out port. The connecting terminals are on the underside of the device.



Figure 3-1 Connectors for in port and out port on the underside of the device

In port I1

The connecting terminals of the in port are labeled I1+ and I1-.

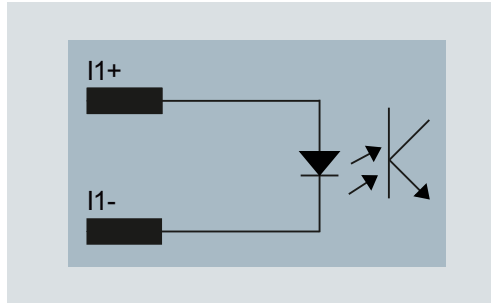


Figure 3-2 In port I1

The in port is used to trigger an alarm SMS message, see section Alarm SMS (Page 116).

Out port O1

The connecting terminals of the out port are labeled O1a and O1b.

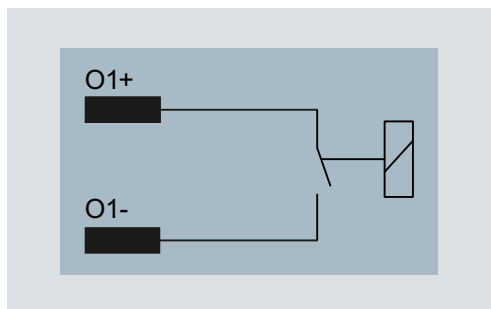


Figure 3-3 Out port O1

The out port signals an existing VPN connection. If at least one VPN connection is established, the out port is active (switch closed).

Note

Remember the maximum load of the out port.

The electrical values for the in port and out port can be found in the section Technical specifications (Page 141).

USB interface X1**Note****Interface X1 without function**

Do not connect any devices to the USB interface. Otherwise operation of the M875 could be impaired.

This interface is reserved for later applications and does not currently have any function.

SMA antenna sockets

 **WARNING**

Risk of lightning strikes when installed outdoors

If you install an antenna outside, the antenna must be grounded to protect it from lightning strikes. This work must only be carried out by qualified personnel.

NOTICE

Damage to devices due to incorrect accessories

Use only antennas from the accessories for the M875. Other antennas could interfere with product characteristics or lead to defects.

The M875 has two antenna sockets of the type SMA for connecting the antenna. If you only connect a single antenna, use the upper SMA socket "A1" of the M875.

If the full reception bandwidth cannot be reached with a single antenna, for example due to inadequate field strength or reflections, you can also connect a second antenna with a supporting role. Remember that even with two antennas, only the simple bandwidth of the frequency band is reached as a maximum.

If you connect two antennas, keep to a minimum distance of 30 cm between the antennas.

The antennas must have an impedance of approx. 50 ohms.

The VSWR (Voltage Standing Wave Ratio) of the antennas must be 1:2.5 or better.

Follow the operating instructions of the antennas used.

Frequency bands in Europe, China, the USA and other regions

Depending on the frequency bands used by your mobile wireless provider, antennas must be tuned to the following frequencies:

- In Europe, America, Africa, Asia and Australia:
 - GSM 900 MHz
 - DCS 1800 MHz
 - UMTS 2100 MHz
- In the USA:
 - GSM 850 MHz
 - PCS 1900 MHz (also for UMTS)

Check with your network provider for the suitable frequencies.

Signal quality

During installation, make sure that you have a good signal quality of CSQ > 11. If when the "Q" LED on the left-hand side of the device is lit permanently or only with brief interruptions, the signal quality is good.

Large metallic objects, for example reinforced concrete impare the signal quality.

Screw terminals for power supply

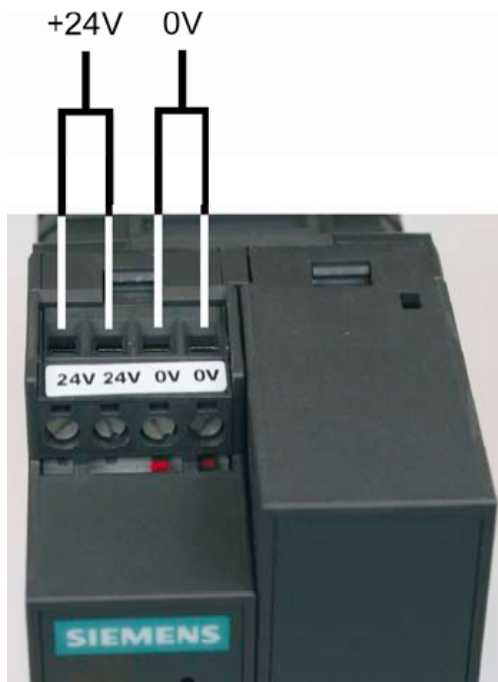


Figure 3-4 Screw terminals for power supply

Note

The power supply unit of the M875 is not electrically isolated.

The M875 works with a voltage of 12 to 30 VDC, nominally 24 VDC. The current consumption is approx. 450 mA at 12 V.

Connect a suitable power supply to the screw terminals.

Use copper wires only.

Wire:	0.5 to 3 mm ² (20 to 18 AWG)
Stranded wire:	0.5 to 2.5 mm ²
Tightening torque for screw terminals:	0.6 to 0.8 Nm

3.3 Steps in commissioning

To commission the M875-0, follow the steps below:

Overview of commissioning

1. Note the requirements for operating the M875.
See section Requirements for operation (Page 17).
2. Connect a PC with a Web browser (Admin PC) to the local interface X2P1.
See section Settings on the admin PC (Page 33), section TCP/IP configuration in Windows XP (Page 34) and section Establishing the configuration connection (Page 36).
3. Enter the PIN of the SIM card via the Web user interface of the M875.
See section UMTS/EDGE - access parameters (Page 58).
4. Disconnect the M875 from the power supply.
See section Connecting (Page 26).
5. Insert the SIM card in the device.
See section Inserting the SIM card (Page 31).
6. Connect and align the antennas.
See section Connecting (Page 26) and section Installation mode - aligning antennas (Page 64).
7. Connect the M875 to the power supply.
See section Connecting (Page 26).
8. Set up the M875 according to your requirements.
See section Configuration (Page 33).
9. Connect your application to the second local interface.
See section Connecting (Page 26).

3.4 Inserting the SIM card

NOTICE

Turn off the power supply before replacing SIM cards

Before you insert or remove the SIM card, turn off the power supply of the M875.

Do not open the compartment for the SIM card during operation. This can damage the SIM card and the device.

Note

First enter the PIN

Enter the PIN of the SIM card via the Web user interface before you insert the card in the device. See section UMTS/EDGE - access parameters (Page 58).



Figure 3-5 SIM card compartment

1. After you have entered the PIN of the SIM card, disconnect the M875 completely from the power supply.

The compartment for the SIM card is located on the back of the device. Directly beside to the compartment for the SIM card in the opening in the housing, there is a small yellow button.

2. To open the drawer, press the yellow button with a sharp object, for example a pencil.
3. Place the SIM card in the tray so that the card audibly locks in place and so that its gold-plated contacts remain visible.
4. Then push the tray with the SIM card completely back into the housing.

3.5 Installation

The M875 is suitable for rail mounting on 35 mm DIN EN 50022 rails. On the rear of the device there is a locking mechanism with a spring catch.



Figure 3-6 Installation on a DIN rail

Installation

1. Fit the upper part of the locking mechanism of the device on to the DIN rail.
2. Press the device down against the DIN rail until the spring catch locks in place.

Uninstalling

1. Using a screwdriver, pull down the spring catch on the rear of the device.
2. Remove the device from the DIN rail.

Configuration

4.1 Settings on the admin PC

To configure the M875 you require a PC with a Web browser that is known as the Admin PC in the text below. Configuration is performed with the Web-based administration user interface of the M875. You have the following options available:

- Configuration via the local interface X2P1
This is necessary for the initial configuration.
- Configuration by remote access using HTTPS
This is only possible if remote access was set up earlier for the M875.

Configuration via the local interface

The following requirements for configuration via the local interface must be met:

- The Admin PC must be connected either directly to the Ethernet socket of the M875 or have access to the M875 via the local network.
- The network adapter of the admin PC must have the following TCP/IP configuration:
 - IP address: 192.168.1.2
 - Subnet mask: 255.255.255.0

Instead of IP address shown above, you can also use other IP addresses from the range 192.169.1.x.

If you want to access the external network with the M875, the following settings are also necessary on the Admin PC:

- Default gateway: 192.168.1.1
- The preferred DNS server is the address of the domain name server.

The IP address 192.168.1.1 can also be used since DNS forwarding is supported by the M875.

Remote configuration

Remote configuration using HTTPS is only possible if the M875 is configured for remote access. If you want to use the remote configuration option, follow the steps described in section HTTPS (Page 113).

4.1.1 TCP/IP configuration in Windows XP

Configuring the LAN connection

Note

The path to the "Internet Protocol (TCP/IP) Properties" dialog box depends on your Windows settings. If you cannot find this dialog box, search in the Windows Help function for "LAN Connection" or "Internet Protocol (TCP/IP) Properties".



Figure 4-1 "Internet Protocol (TCP/IP) Properties"

1. In the Start menu, select the command "Settings" > "Control Panel"> "Network Connections".
The "Network Connections" dialog opens.
2. Select a LAN connection by double clicking on it.
The "Status" dialog of the selected LAN connection opens.
3. Select the "General" tab.
4. Click the "Properties" button.
The "Properties" dialog of the selected LAN connection is opened.
5. Select the "General" tab.
6. Enable the "Internet Protocol (TCP/IP)" option under the entry "This connection uses the following elements".
7. Select the "Internet Protocol (TCP/IP)" option.

8. Click the "Properties" button.
The "Internet Protocol (TCP/IP) Properties" dialog opens.
9. Select the "Use the following IP address" option.
10. Enter the following values:
 - IP address: 192.168.1.2
 - Subnet mask: 255.255.255.0
11. To store the settings, click the "OK" button.

Preferred DNS server

If you call up addresses via a domain name (for example `www.siemens.com`), then the domain name system (DNS) is checked to find out what IP address is behind the name. As the DNS server, you can either specify the DNS address of the network provider or the local IP address of the M875.

The local IP address of the M875 must then be configured so that it can resolve host names in IP addresses, see section . For more detailed information, refer to section DNS server on local network (Page 55).

1. To specify the DNS server in the TCP/IP configuration of your network adapter, enter the following values in the dialog shown above:
 - Default gateway: 192.168.1.1
 - Preferred DNS server: 192.168.1.1
2. To store the settings, click the "OK" button.

4.1.2 Permitted characters

When entering user names, passwords, host names, APN and PIN, the following ASCII characters are permitted:

User names, passwords and PIN

Unless exceptions are specifically mentioned, the following characters are permitted:

- a b c d e f g h i j k l m n o p q r s t u v w x y z
- A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
- 0 1 2 3 4 5 6 7 8 9
- ! \$ % & ' () * + , . / : ; < = > ? @ [\] ^ _ ` { | }

Host names and APN

Permitted characters:

- a b c d e f g h i j k l m n o p q r s t u v w x y z
- A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
- 0 1 2 3 4 5 6 7 8 9
- . -

4.1.3 Establishing the configuration connection

To configure the M875, you must first establish a connection to the device with a Web browser. Follow the steps outlined below:

Setting up the Web browser

1. Start the Web browser on the Admin PC.
The Web browser must support SSL (HTTPS), for example MS Internet Explorer Version 7 or later or Mozilla Firefox Version 2 or later.
2. Set the browser so that it does not automatically select a connection when it starts up. In the MS Internet Explorer, for example, make the settings as follows:
 - Select the "Tools" > "Internet Options" menu command.
 - Select the "Connections" tab.
 - Remove the entries under "Dial-up and Virtual Private Network settings".
 - Enable the "Never dial a connection" option.

Calling the start page of the M875

1. In the address line of the browser, enter the IP address of the M875 in full.
In the factory setting, the address is: `https://192.168.1.1/`
At the end of the IP address of the M875, type in the slash.
A message relating to the security certificate appears.
2. Acknowledge this message and continue loading the page.

Note

Information on the security certificate

Because the device can only be administered using encrypted access, it is delivered with a self-signed certificate. If certificates with signatures that the operating system does not know are used, a security message is displayed. You can display the certificate.

It must be clear from the certificate that it was issued for Siemens AG. The Web user interface is opened when the device is accessed using an IP address and not a name, which is why the name specified in the security certificate, is not the same as the one in the certificate.

Entering the user name and password

You will be prompted to enter the user name and the password. The factory setting is as follows:

User name: admin (cannot be modified)
Password: scalance

NOTICE**Changing the password**

Change the factory set password immediately after commissioning. This password is public knowledge and does not provide adequate protection.

How to change the password is described in the section Changing the password (Page 112).

The start page is displayed

After entering the user name and password, the start page of the M875 opens in the Web browser. The start page provides an overview of the operating status of the device, see also the section Start page of the Web user interface - Overview (Page 40).

The start page is not displayed

If, after several attempts, the browser still reports that the page cannot be displayed, try the following:

Check the hardware connection

1. Open the DOS command prompt by selecting the menu command "Start" > "Programs" > "Accessories" > "Command Prompt".

The "Command Prompt" window appears.

2. Enter the command "ping 192.168.1.1".
3. To confirm the entry, press the "Return" key.

When operating correctly, 4 feedback messages will arrive within a few seconds.

If this is not the case:

4. Check whether the network cable, the connectors and the network adapter are correctly connected.

Do not use a proxy server

Follow the steps outlined below depending on the operating system.

1. Select the "Tools" > "Internet Options" menu command.
2. Select the "Connections" tab.
3. Click the "Settings" button below the "LAN Settings" entry.

The "Settings for local area network (LAN)" dialog is displayed.

4. Under the "Proxy server" entry, disable the "Use proxy server for your LAN" option.

Disable other LAN connections

If other LAN connections are active on the Admin PC, disable them while you are setting the configuration.

In the MS Internet Explorer (version 7.0), follow the steps outlined below:

1. In the Start menu, select the command "Settings" > "Control Panel"> "Network Connections".

The "Network connections" dialog opens.

2. Select a LAN connection.
3. Right-click and select "Disable" in the shortcut menu.

4.1.4 Basics of configuration

To configure the M875, a Web-based administration user interface is available to you.

At the left-hand page you will find an expandable navigation panel. The main window displays the pages called according to your navigation. There are also drop-down lists on the individual pages for making selections and the normal buttons such as "Save", "Reset", "Edit" etc.

Basic procedure

Follow the steps below to configure the M875:

1. Select the required Web page in the navigation panel.
2. Make your settings on the page you have opened.

With the "Reset" button, the display is reset to the status when it was opened. Entries you have not saved are reset to the value that had been saved previously.

3. Confirm your entries by clicking the "Save" button.

Your settings are then adopted by the device.

Note

- After configuration of the M875, it may be necessary to adapt the network interface of the locally connected computer or network.
 - When entering IP addresses, enter the address sections without leading zeros, for example: 192.168.0.8.
-

Invalid entries

The M875 checks your entries. Errors are detected automatically when you save and the input box in question is displayed in a red frame.

Configuration profiles

You can save your settings in profiles. These profile files can, when necessary, be reloaded or transferred to other devices of the same type. For more detailed information, refer to the section Configuration profiles (Page 131).

4.1.5 Language selection

You can display the Web-based user interface of the M875 either in English or German. On the starting page, there is a drop-down list at the top right that allows you to make the following selections:

- **Automatic:** The M875 selects the language of the administration user interface according to the settings of the Web browser you are using.
If the Web browser is set to German, the user interface of the M875 is automatically displayed in German. In all other cases, the user interface is displayed in English.
- **German:** The M875 uses German, regardless of the Web browser you are using.
- **English:** The M875 uses English, regardless of the Web browser you are using.

Changing the language setting

Follow the steps below to change the language setting:

1. Open the drop-down list for the language setting at the top right of the start page.
2. Click the required language.
3. Confirm your selection by clicking the "Go" button.

If the language is not changed immediately, use the update function of your Web browser (function key "F5").

4.2 Start page of the Web user interface - Overview

Description of the user interface

The start page provides an overview of the current operating status of the M875 as shown in the figure below:

The screenshot displays the 'System - Overview' page for a Siemens SCALANCE M875. The interface includes a navigation menu on the left and a main content area with two columns of data.

System - Overview	
Current system time	2012-11-07, 17:05
Connected since	Mon Oct 29 13:57:20 CET 2012
External host name	m875-15.dyndns.org
Assigned IP address	88.128.235.8
Connection	UMTS, 3G
Signal strength CSQ (dbm)	15 (-83 dbm)
APN in use	internet.t-d1.de
IMSI	262011442115545
NTP synchronization	✓
DynDNS	✓
Remote access HTTPS	✓
Remote access SSH	✗
CSD dial-In	✗
SNMP	✗
SNMP Trap	✗
Volume monitoring	✗
ID of the current wireless cell	5580846
Number of WAN connection attempts (24h)	0
Bytes sent on this connection	1346930
Bytes received on this connection	539330
Bytes sent since loading the factory settings	908550405
Bytes received since loading the factory settings	1845906748
Traffic volume (bytes / current month)	0
Maximum data volume (bytes/month)	100000
Number of activated firewall rules	1
Firmware version	2.112

Update of the displayed values

The values displayed here are refreshed every 30 seconds.

To refresh the displayed values immediately, press the "F5" function key.

Current system time

Shows the current system time of the M875 in the format:

Year-month-day, hours-minutes

Connected since

With the date and time of day, this shows the time since the current wireless connection was established.

External host name

Shows the host name of the M875 (for example M875.mydns.org) if a DynDNS service is used.

Assigned IP address

Shows the IP address at which the M875 can be reached in the mobile wireless network. This IP address is assigned to the M875 by the service of the network provider.

Connection

Shows whether a wireless connection exists, and, if it does, which one:

- UMTS: IP connection via HSDPA+HSUPA, UMTS
- GPRS: IP connection via EGPRS or GPRS

Note

Using connection monitoring

It is possible that you will see both an IP data connection and an assigned IP address although the connection quality is not adequate to transfer data. For this reason, we recommend that you use the connection monitoring. For more detailed information, refer to the section [Checking the connection - Connection monitoring \(Page 68\)](#).

Signal strength CSQ (dbm)

The bar display and the number above it indicate the strength of the GSM signal as a CSQ value.

CSQ = 0	No connection to the GSM network
CSQ < 6	Bad signal strength
CSQ 6 ... 10	Medium signal strength
CSQ 11 ... 18	Good signal strength
CSQ > 18	Very good signal strength

The dBm value is shown in brackets after the CSQ value.

If the "Installation mode" function is enabled, the display is not active.

Used APN

Shows the APN (= Access Point Name) of the wireless link that is being used.



IMSI

This entry shows the subscriber ID that is stored on the SIM card being used.

This ID (IMSI = International Mobile Subscriber Identity) is used by the mobile wireless provider to detect the authorizations and agreed services for the SIM card.



NTP synchronization

Shows whether or not the system time is obtained from an NTP server using NTP.

-  The service is activated.
-  The service is not activated.

DynDNS



Shows whether or not a DynDNS service is activated.

-  The service is activated.
-  The service is not activated.

You will find information indicating whether or not the logon with a DNS service was successful in the log.



HTTPS remote access

Shows whether remote access to the Web user interface of the M875 via the wireless network is permitted, see the section HTTPS (Page 113).

-  Access is permitted.
-  Access is not permitted.

Remote access SSH

Shows whether remote access to the SSH console of the M875 via the wireless network is permitted.

-  Access is permitted.
-  Access is not permitted.

CSD dial-in

Shows whether remote CSD service calls are allowed.



Access is permitted.



Access is not permitted.

SNMP

Indicates whether access via SNMP is permitted.



Access is via SNMP is permitted.



Access is via SNMP is permitted.

SNMP trap

Shows whether alarm events are transferred using SNMP traps.



One or more events are transferred.



No alarm events are transferred.

Traffic volume supervision

Shows whether the volume monitoring is on or off.



The function is enabled.



The function is disabled.

ID of the current wireless cell

With the identification number, this entry shows the wireless cell in which the device is logged in (Cell ID).

Number of WAN connection attempts (24 h)

This counter shows how often the M875 attempted to establish a connection to the mobile wireless network in the last 24 hours.

Bytes sent and bytes received on this connection

These entries show the number of bytes that have been sent or received during the current connection to the mobile wireless network.

The counters are reset when a new connection is established.

Note

These figures serve only as a general indication of the data volume, and can differ significantly from the mobile wireless provider's accounting.

Bytes sent since loading the factory settings

These entries show the number of bytes that have been sent or received via the mobile wireless network since the last restart of since the last time the factory settings were loaded.

The counters are reset when the factory settings are loaded.

Traffic volume (bytes / current month)

This counter shows the data volume in bytes that was transferred via the M875 since the beginning of the month.

Maximum data volume (bytes/month)

This entry shows the limit value to which the volume supervision was set.

Number of activated firewall rules

This entry shows how many firewall rules are currently active.

Firmware version

This shows the version number of the currently installed firmware of the M875.

4.3 System

4.3.1 System time

The system time is used as a time stamp for all log entries and serves as the basis for all time-driven functions.

You can set the system time of the M875 yourself manually or have it synchronized automatically with a time server using NTP (Network Time Protocol). There are a number of NTP servers on the Internet that can be used to obtain the current time precisely.

Calling the Web page

In the navigation panel, select "System "> "System Time".

The screenshot shows the Siemens SCALANCE M875 web interface. The navigation panel on the left includes: Overview, System (expanded), System Time, Log, Device Identification, Local Network, External Network, Security, IPsec VPN, Remote access, SMS, SNMP, and Maintenance. The main content area is titled 'System - System time/NTP' and contains the following sections:

- Current system time:** 2012-11-07, 17:06
- Set system time:** Fields for Year, Month (Nov), Day (7), Hour (17), and Minute (6), with a 'Set' button.
- Local timezone / region:** A dropdown menu set to 'Berlin'.
- Enable NTP synchronization:** A dropdown menu set to 'Yes'.
- List of NTP servers for synchronization:** A table with columns for 'NTP server' (192.53.103.108) and 'Polling interval' (1,1h), with 'New' and 'Delete' buttons.
- Serve system time to local network:** A dropdown menu set to 'Yes'.

At the bottom of the main content area are 'Save' and 'Reset' buttons.

Current system time

This entry shows the currently set date and time.

Set system time

Below this entry, you set the date and time of the system yourself manually.

In the default setting, the time of the admin PC with which you are connected to the M875 is displayed.

1. Enter the date and time.
2. Click the "Set" button.
The entered system time is displayed at the top below "Current system time".

Local timezone / region

NTP servers provide UTC (Universal Time Coordinated).

From the drop-down list, select the time zone in which the M875 is being used. The date and time in this time zone will be used as the system time.

Activate NTP synchronization

Note

Increased costs due to extra data traffic

Synchronization of the system time via NTP creates additional data traffic on the mobile wireless connection. This may result in additional costs, depending on your user agreement with the mobile wireless provider.

If you want to synchronize the date and time using an NTP time server, select "Yes" from the drop-down list.

List of NTP servers

You can specify several NTP servers.

To specify an additional NTP server, click the "New" button.

- NTP server

Enter the IP address of a DNS server in the input box.

You can also use the NTP server set in the factory (see below).

It is not possible to enter the NTP address as a host name (for example timeserver.org).

- Poll interval

The time is synchronized automatically at the latest every 36 hours.

From the "Polling interval" drop-down list, you can select a different interval for synchronization.

Serve system time to local network

The M875 can itself function as an NTP time server for the applications connected to its local interface.

To enable this function, select "Yes" from the drop-down list.

The NTP time server in the M875 can be reached via the local IP address set for the M875. For more detailed information, refer to the section Local IP addresses (Page 49).

Factory settings

Local timezone:	UTC
Enable NTP synchronization:	No
NTP server:	192.53.103.108
Polling interval:	1.1 hours
Serve system time to local network:	No

4.3.2 Log

Important events while the M875 is operating are saved in the log:

- Reboot
- Changes to the configuration
- Connection establishment
- Interruption of connections
- Signal strength
- Operational messages

The log is saved to the log archive of the M875 when a file size of 1 MB, is reached, but after 24 hours at the latest.

Calling the Web page

In the navigation panel, select "System" > "Log".

The screenshot shows the Siemens SCALANCE M875 web interface. The top header features the Siemens logo and a language selection dropdown set to 'English' with a 'Go' button. The left navigation panel is expanded to 'System' > 'Log'. The main content area is titled 'System - Log' and contains a 'Download current log' button with a 'Download' link. Below this is a 'Log archive' section with a table listing log files. Each row in the table has a 'Download' button.

Name	
LOG0_2012_10_31_2358.tar.gz	Download
LOG1_2012_11_1_2358.tar.gz	Download
LOG2_2012_11_2_2358.tar.gz	Download
LOG3_2012_11_3_2358.tar.gz	Download
LOG4_2012_11_4_2358.tar.gz	Download
LOG5_2012_11_5_2358.tar.gz	Download
LOG6_2012_11_6_2358.tar.gz	Download
LOG7_2012_10_28_2358.tar.gz	Download
LOG8_2012_10_29_2358.tar.gz	Download
LOG9_2012_10_30_2358.tar.gz	Download

Downloading the current log and log archive

If you click the "Download" button, a dialog opens in which you can open or save the current or archived log files. Follow the on-screen instructions.

Meaning of the entries in the log

Column A:	Time stamp with the date and time
Column B:	Product name
Column C:	Signal quality (CSQ value)
Column D:	GSM login status STAT=- - -: Function not started STAT=1: Logged into home network STAT=2: Not logged in, network search STAT=3: Logging in denied STAT=5: Logged in to third-party network (roaming)
Column E:	Shows of the network provider identification with the 3-digit country code (MCC) and the 2 to 3-digit network provider code (MNC), for example 26201: 262 = country code Germany, 01 = network provider code T-Mobile
Column F:	Coded operating status (for Siemens Customer Support)
Column G:	Category of the log report (for Siemens Customer Support)
Column H:	Internal source of the log report (for Siemens Customer Support)
Column I:	Internal report number (for Siemens Customer Support)
Column J:	Log report in plain text
Column K - P:	Additional information on the plain language message, for example <ul style="list-style-type: none">• Cell ID (ID of the active wireless cell)• Software version (current firmware version)• TXS, RXS (IP packets transmitted on the current connection)• TX, RX (IP packets transmitted since the last time the factory settings were loaded)

4.3.3 Device identification

The information for device identification can be read out from a management station via SNMP.

Calling the Web page

In the navigation panel, select "System "> "Device Identification".

Enter any text you require in the input boxes of rows 1 to 4.

4.4 Local Network

4.4.1 Local interface

Interface

The 2-port interface is used to connect the local network to the M875. You will find the properties of the X2 interface in the technical specifications. Due to autonegotiation, which of the two transmission speeds is being used on Ethernet is detected automatically.

Local network

The local network is the network of the station connected to the Ethernet interface of the M875. The local area network contains at least one local application.

Local application

A local application is an application software for a network component in the local network, for example a programmable controller, a machine with an Ethernet interface for remote monitoring, or a notebook, desktop PC or the Admin PC.

4.4.2 Local IP addresses

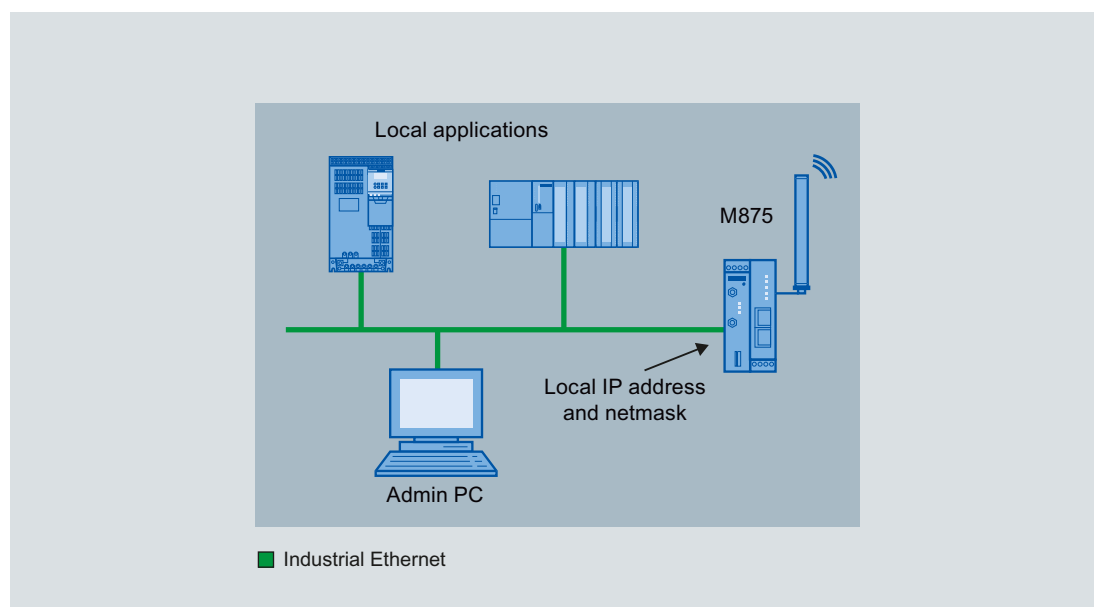


Figure 4-2 Configuration of a local network

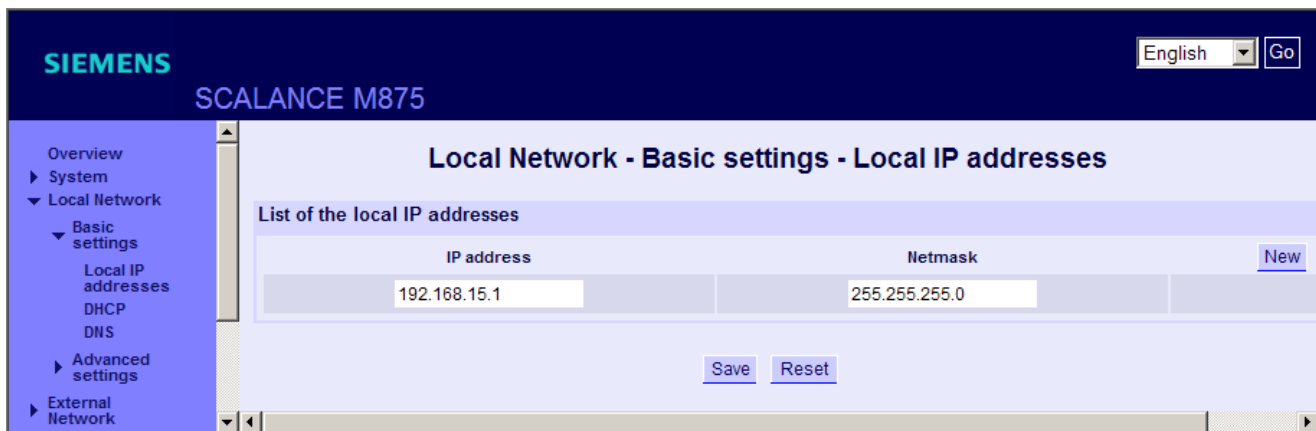
Note

IP addresses and net mask according to RFC 1918

The factory-set IP addresses and netmasks can be changed as required, but must keep to the specification RFC 1918.

Calling the Web page

Select "Local Network > "Basic settings" > "Local IP addresses" in the navigation panel.



Creating and managing IP addresses

In the factory settings, the M875 can be reached at the following address:

- IP address: 192.168.1.1
- Network mask: 255.255.255.0

You can specify additional addresses at which the M875 can be reached by local applications. Additional addresses are useful, for example, when the local area network is divided into subnets. Several local applications from different subnets can then reach the M875 using different addresses.

1. Click the "new" button.
2. Enter the IP address and the network mask in the input boxes.
3. Save your entries by clicking the "Save" button.

With the "Delete" button, you can delete additional addresses that were created.

Note

Modified addresses with DHCP

If you change addresses and, at the same time use the DHCP function of the M875, remember to make any changes that may be necessary there, see section DHCP server on local network (Page 51).

Note

No use of the M875 as a router between internal subnets

Do not use the M875 as a router between internal subnets.

4.4.3 DHCP server on local network

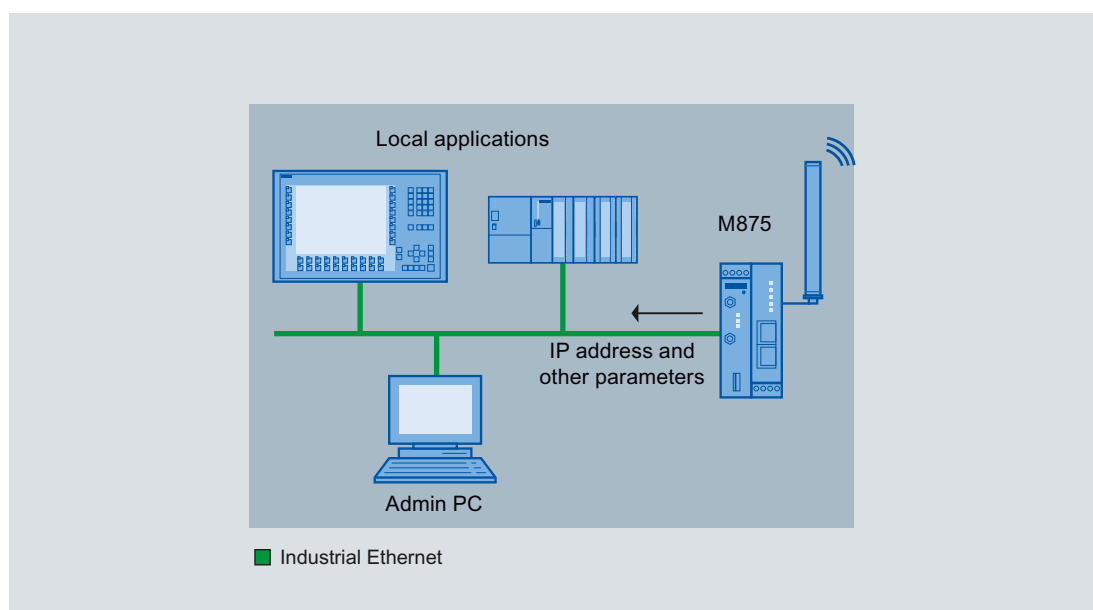


Figure 4-3 Configuration of a local network

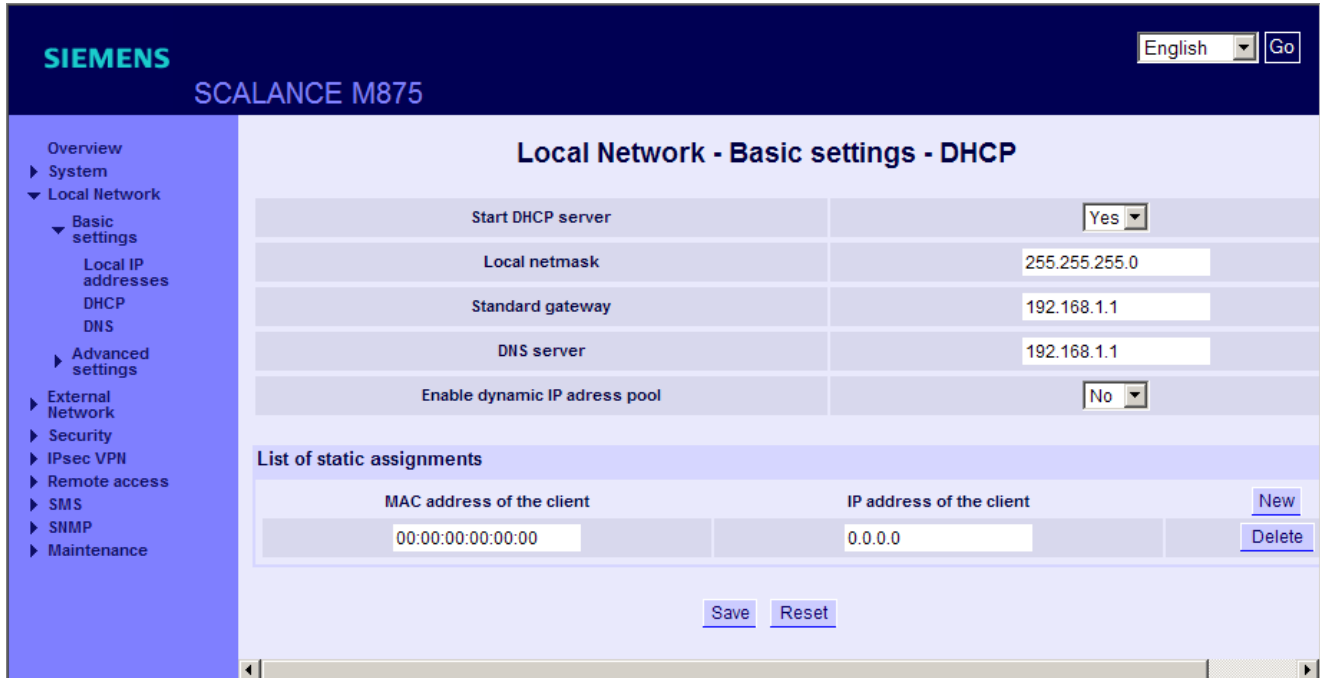
A DHCP server is integrated in the M875. When the server is activated, it automatically assigns the following parameters to the applications connected to the local interface:

- IP address
- Network masks
- Gateway
- DNS server

The local applications must be set so that they can obtain the IP addresses and configuration parameters using DHCP.

Calling the Web page

Select "Local Network > "Basic Settings" > "DHCP" in the navigation panel



Start DHCP server

1. Select "Yes" in the "Start DHCP server" drop-down list.
2. Select "Yes" in the "Enable dynamic IP address pool" drop-down list.
3. Click the "New" button under "List of static assignments".

The following options are available:

- Yes: The DHCP server is switched on.
- No: The DHCP server is switched off.

Local netmask

Here, enter the local netmask to be assigned to the local applications.

Standard gateway

Here, enter the standard gateway to be assigned to the local applications.

DNS server

Here, enter the DNS server to be assigned to the local applications.

Enable dynamic IP address pool

Select one of the two options:

- Yes: The IP addresses assigned by the DHCP server of the M875 are taken from a dynamic address pool.
- No: At the bottom of the page in the "List of static assignments " area assign the IP addresses to the MAC addresses of the local applications yourself.

Range start

Enter the first address of the dynamic address pool in the input box.

Range end

Enter the last address of the dynamic address pool in the input box.

List of static assignments

You can specify corresponding IP addresses for the MAC addresses of the local applications.

If a local application requests the assignment of an IP address using DHCP, the application transfers its MAC address. If you assign a static IP address for this MAC address, this IP address is assigned to the local application.

Enter the following information in the relevant input boxes:

- MAC address of the client
- IP address of the client

Factory settings

Start DHCP server:	No
Local netmask:	255.255.255.0
Standard gateway:	192.168.1.1
DNS server:	192.168.1.1
Enable dynamic IP address pool:	No
Range start:	192.168.1.100
Range end:	192.168.1.199

4.4.4 Local hostname

Note

Creating firewall rules

The security concept of the M875 requires an outgoing firewall rule for each local application that uses this hostname function. For more detailed information, refer to the section Firewall rules (Page 76).

The M875 can also be addressed from the local network using a hostname. To do this, specify a host name, e.g. SCALANCE M875. The device can then be called up using this name, for example from a Web browser.

Calling the Web page

Select "Local Network > "Basic Settings" > "DNS" in the navigation panel. The "Local Network - Basic Settings - DNS" page opens.

Host name

Enter a host name in the input box with which the M875 will be called up, for example "SCALANCE".

Search path

Note

DHCP

If you do not use DHCP, you will need to enter identical search paths on the M875 and in the locally connected applications yourself.

If you do use DHCP, the locally connected applications receive the search path entered in the M875 automatically.

Factory settings

Search path: example.local

Hostname: SCALANCE

4.4.5 DNS server on local network

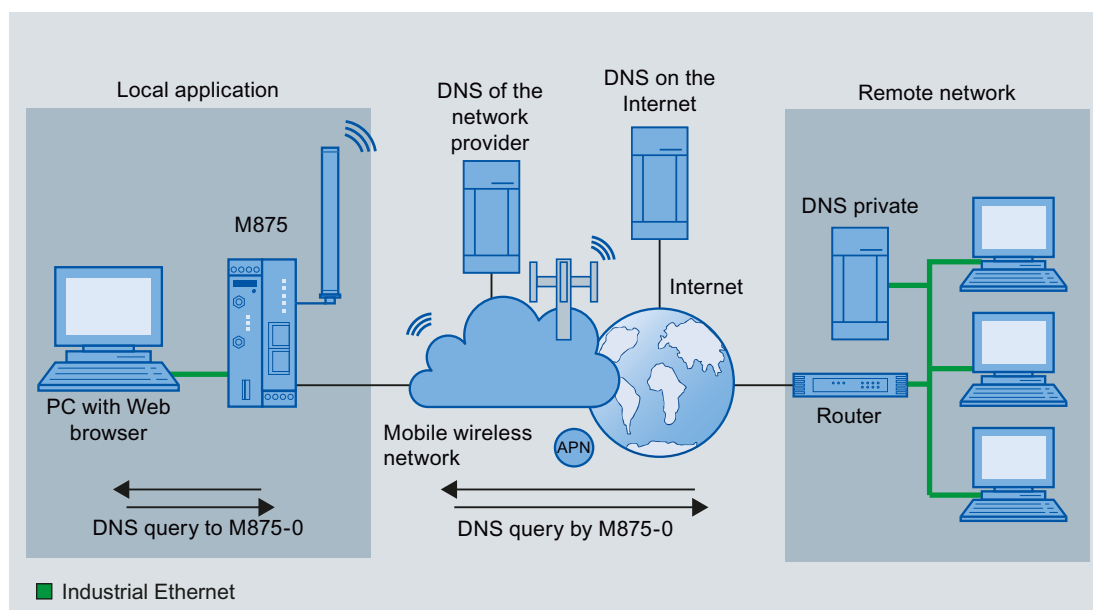


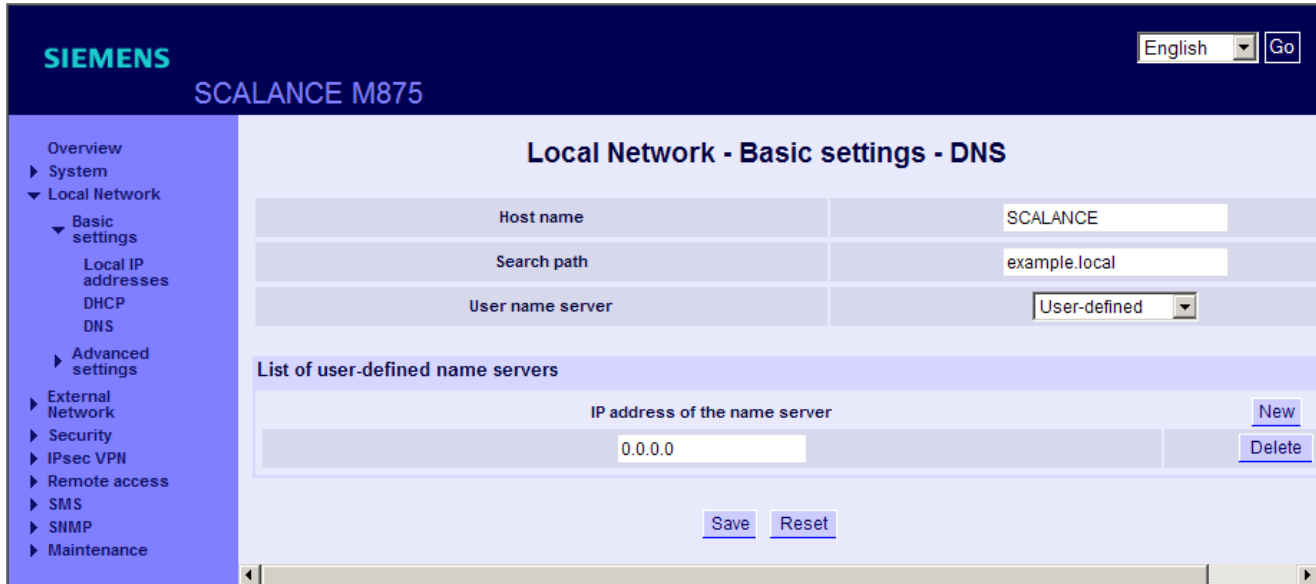
Figure 4-4 DNS function configuration

The M875 provides a DNS server for the local network.

If you enter the IP address of the M875 in your local application as a DNS server, then the M875 answers the DNS requests from its cache. If the M875 does not know the IP address for a domain address, it forwards the query to an external DNS server. How long the M875 keeps a domain address in the cache depends on the host being addressed. In addition to the IP address, a DNS request to an external DNS server also supplies the life span of this information. The external DNS server used can be a server of the network provider, a server on the Internet, or a server in the private external network.

Calling the Web page

Select "Local Network > "Basic Settings" > "DNS" in the navigation panel.



Name server used

From the drop-down list, select the DNS server to which queries are forwarded. The following selections are available:

- Provider defined: When a connection is established to UMTS/GPRS, the network provider automatically sends one or more DNS server addresses that are used.
- User defined: As the user, you select your preferred DNS server. The DNS servers can be connected to the Internet, or can be private DNS servers in your network.

List of user-defined name servers

This entry appears if you have selected the "User-defined" option.

1. To create a name server, click the "New" button.
2. Enter the IP address of the required DNS server in the input box below "IP address of the name server".
3. Click the "Save" button.

Factory settings

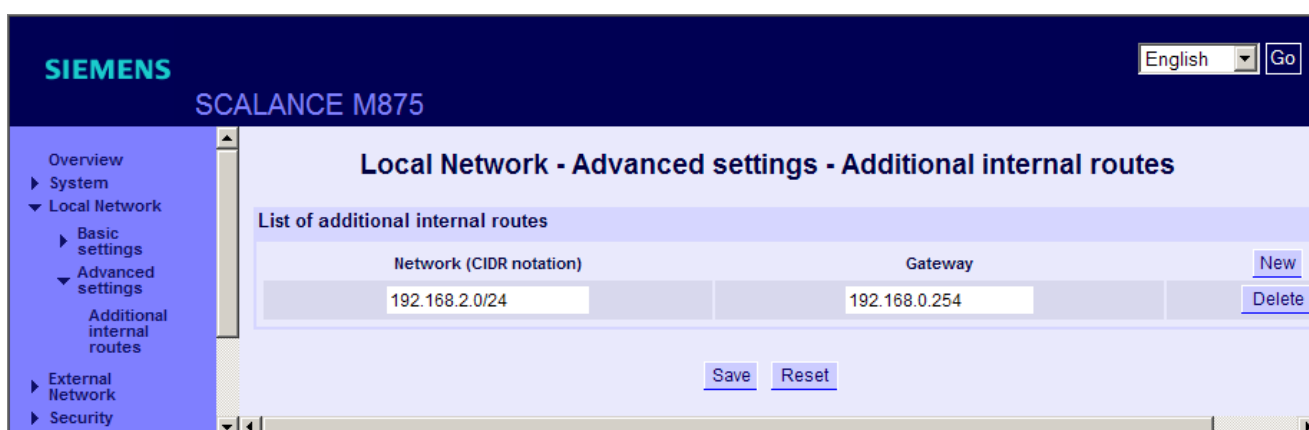
Name server used:	Provider-defined
List of user-defined name servers If the entry is new:	0.0.0.0

4.4.6 Additional Internal Routes

If the local network is divided into subnets, you can define additional routes to link subnets to the M875.

Description of the user interface

1. Select "Local Network > "Advanced Settings" "Additional Internal Routes" in the navigation panel.
2. Click the "New" button
The page shown below appears.



Setting up an additional internal route

1. Under "Network" enter the IP address of the subnet in the input box.
2. Under "Gateway", enter the IP address of the gateway via which the subnet is connected.
3. Then click the "Save" button.

You will find further information in the appendix Additional Internal Routes (Page 149).

Factory settings

Default for new routes:	No
Network::	192.168.2.0/24
Gateway:	192.168.0.254

4.5 External Network

4.5.1 External interface

The external interface of the M875 connects the device to the external network. The two antenna sockets of the type SMA are available for this. HSDPA, HSUPA, UMTS, EGPRS or GPRS are used for communication on these interfaces.

- **External networks**

External networks are, for example, the Internet or a private intranet.

- **External partners**

External remote stations are network components in an external network, for example Web servers on the Internet, routers on an intranet, a central company server, an Admin PC.

The following sections describe how the external interface and the associated functions are configured.

4.5.2 UMTS/EDGE - access parameters

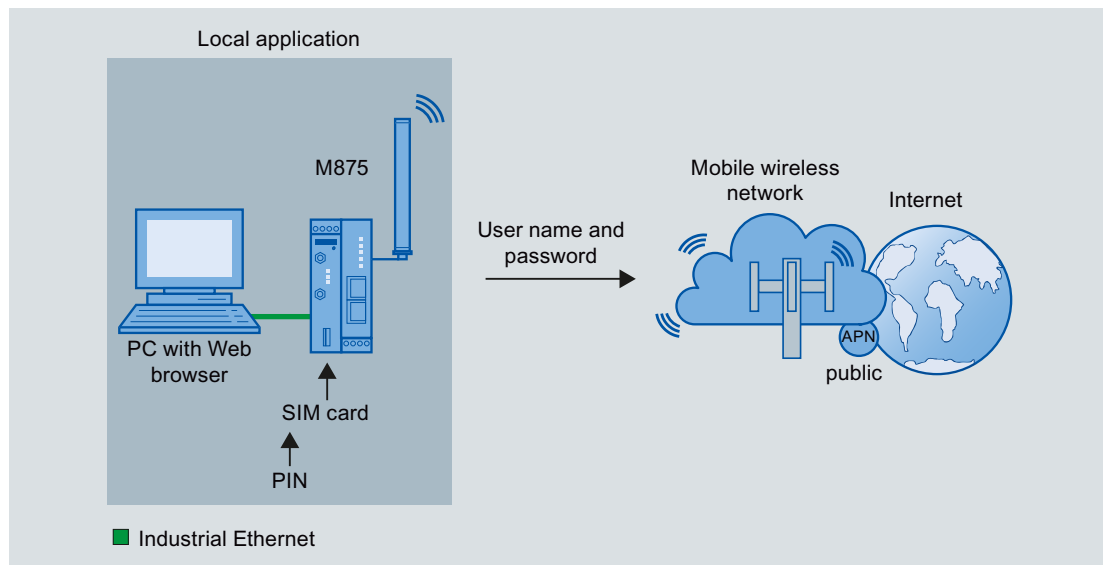


Figure 4-5 Configuration with access to the Internet

For access to the GSM network and the services HSPA, UMTS,E/GPRS, the following access parameters are required:

- The PIN protects the SIM card against unauthorized use of the device.
- The user name and password protect access to the mobile wireless network.
- The APN (Access Point Name) is the name of the access point from the mobile wireless network to other connected IP networks, here to the Internet.

You will receive these access parameters from your mobile wireless provider.

Calling the Web page

Select "External Network > "UMTS/EDGE" in the navigation panel.

The screenshot shows the Siemens SCALANCE M875 web interface. The top navigation bar includes the Siemens logo, the device model 'SCALANCE M875', and a language dropdown set to 'English' with a 'Go' button. A left-hand navigation menu lists various system settings, with 'External Network' expanded to show 'UMTS/EDGE'. The main content area is titled 'External Network - UMTS/EDGE' and contains several configuration fields:

- PIN:** A text input field containing four dots and a green checkmark icon.
- Change PIN:** A button labeled 'Change'.
- Network selection:** A dropdown menu currently set to 'UMTS or GSM'.
- Allow roaming:** A dropdown menu currently set to 'No'.
- Method of the provider authentication PAPI/CHAP:** A dropdown menu currently set to 'Automatic'.
- Mode of the provider selection:** A dropdown menu currently set to 'Automatic'.

Below these fields is a section titled 'List of mobile wireless providers' containing a table with the following data:

Provider	Network ID (PLMN)	APN	Username	Password	
T-Mobile	26201	internet-t-d1.de	guest	New Delete
Vodafone	26202	web.vodafone.de	guest	Delete
Eplus	26203	internet.eplus.de	guest	Delete
O2	26207	internet	guest	Delete

At the bottom of the configuration area are 'Save' and 'Reset' buttons.

PIN

Note

SIM card without PIN

The M875 also works with SIM cards without a PIN. In this case, enter "NONE" in the input box.

If no entry is made, the input box for the PIN is shown with a red margin after saving. The function cannot be executed.

If you make incorrect entries, the SIM card is blocked

Make sure that you enter the PIN correctly. If you enter the PIN incorrectly more than three times, the SIM card will be blocked.

To unblock the card, it must be taken out of the device and placed in a mobile telephone where it can then be unblocked by entering the PUK. If necessary, contact your mobile wireless provider.

You have received a PIN for your SIM card from your network provider.

1. Enter the PIN for your SIM card in the input box.
2. Confirm your entry by clicking the "Save" button (not "Change").
 - A green dot with a white check mark beside the input box indicates that the PIN was stored successfully on the device.
 - A red dot with a white cross beside the input box indicates that the PIN was entered incorrectly and / or no PIN was stored on the device.

Changing the PIN

You have the option of replacing the PIN stored on the SIM card by your network provider with your own PIN. To do this, click the "Change" button.

Note

Check with your mobile wireless provider to find out whether this function is supported.

1. Enter the your own PIN in the "New PIN" input box.

The entry is displayed as hidden characters.

2. Repeat the entry in the next input box.
3. Save your entry by clicking the "Set" button.

A message appears with the information that the PIN was changed successfully or could not be changed.

4. Confirm this message by clicking the "OK" button.

This brings you automatically back to the "External Network - UMTS/EDGE" page.

Network selection

Select the type of mobile wireless network to be used from the drop-down list. The following options are available:

- UMTS or GSM: All available services.
As first choice, the device attempts to establish a connection to the UMTS network.
- GSM only: The EGPRS and GPRS services
The device ignores the UMTS network and establishes a connection to the GSM service that provides the highest bandwidth locally.
- UMTS only: The UMTS service
The device ignores the EGPRS and GPRS services and establishes a connection in the UMTS network.

Allow roaming

Specify whether or not the device automatically logs on with a different network if the specified GSM network is unreachable. Select one of the two options from the drop-down list.

- Yes: The device automatically logs on with an available network.
- No: The device does not automatically log on with an available network.

Authentication method

From the drop-down list, select a method according to which the user name and password of the device will be transferred to the communications partner:

- Automatic User name and password are transferred automatically with one of the following two methods. CHAP has the higher priority. If the communications partner does not support CHAP, the user name and password are transferred using PAP.
- CHAP Encrypted transfer of user name and password using the Challenge Handshake Authentication Protocol (CHAP)
- PAP Unencrypted transfer of user name and password using the Password Authentication Protocol (PAP)

Mode of provider selection

You have the option of entering the access parameters of a mobile wireless provider manually yourself, or the M875 selects suitable access parameters from a list of providers automatically. This automatic selection is based on the PLMN ID on the SIM card, see below.

Select one of the two options from the drop-down list:

- **Manual:** Enter the user name, password and APN for the mobile wireless service manually.
- **Automatic:** The "List of mobile wireless providers" appears on the Web user interface as shown above. In the factory settings, access parameters of four network providers are already set, see table below.

List of mobile wireless providers

Here, enter the relevant data of your access to the GSM network.

Provider

Enter a name for the mobile wireless service in the input box, for example "My GPRS access".

Network ID (PLMN)

Each mobile wireless provider has an identification number assigned to it that is unique worldwide, the PLMN. This ID known here as the network ID is stored on the SIM card. The M875 reads the PLMN from the SIM card automatically and selects the corresponding access data from "List of mobile wireless providers".

APN

The APN (Access Point Name) is the DNS host name of the access point of a network provider to an external packet data network such as UMTS, GPRS etc.

Enter the APN of your mobile wireless provider in the input box.

User name

In the input box, enter the user name supplied to you by your mobile wireless provider.

Some providers do not use access control with user names. In this case, enter "guest" in the corresponding input box.

Password

Enter the password of the relevant provider in the input box.

Some mobile wireless providers do not use access control with a password. In this case, enter "guest" in the corresponding input box.

Note

Searching for APN, user name and password

You can obtain information about this access data from your mobile wireless provider or from the Internet.

Enter, for example, the keywords "APN mobile wireless provider" in a search engine. The search result provides an overview of various providers with all the required access parameters.

Factory settings

Defaults for manual selection of the mobile wireless provider

In the factory settings, the "Mode of provider selection" is set to "Manual" as default. In this case, the following values are preset:

PIN:	NONE
APN:	NONE
User name:	guest
Password:	guest

Defaults for automatic selection of the mobile wireless provider

For automatic selection of the mobile wireless provider, the following values are preset:

1. Provider:	T-Mobile
PLMN ID:	26201
APN:	internet.t-mobile
User name:	guest
Password:	guest

2. Provider:	Vodafone
PLMN ID:	26202
APN:	web.vodafone.de
User name:	guest
Password:	guest

3. Provider:	Eplus
PLMN ID:	26203
APN:	internet.eplus.de
User name:	guest
Password:	guest

4. Provider:	O2
PLMN ID:	26207
APN:	internet
User name:	guest
Password:	guest
nth provider:	NONE
PLMN ID:	NONE
APN:	NONE
User name:	NONE
Password:	NONE

4.5.3 Installation mode - aligning antennas

To find the ideal alignment of the antenna connected to the A1 socket, you can use the installation mode. This function makes it easier to test the signal strength in various antenna positions.

The information on the "Installation Mode" page is refreshed at intervals of a few seconds. This provides you with fast information about the signal quality at the test positions so that you can identify the optimum position.

No mobile wireless connection is necessary for the installation mode.

Note

Reboot when enabling and disabling

If you enable or disable the "Installation mode" function, when you click the "Save" button, the device automatically goes through a reboot.

Calling the Web page

Select "External Network" > "Installation mode" in the navigation panel.

In the factory settings, the installation mode is disabled.

1. To enable the function, select a time from the drop-down list during which the installation mode is enabled (15/30/60/120 minutes).
2. Click the "Save" button.
The M875 restarts and the entries described below appear:
3. You can stop the enabled function prematurely by selecting the "No" option.

Status of the current wireless cell

In this area of the page you will find information that relates to the mobile wireless cell in which the M875 is currently logged in.

Status of the neighboring wireless cells

In this area of the page, you will find information that relates to the neighboring, available mobile wireless cells.

Information about the wireless cell

Signal strength

- The bar display indicates the strength of the GSM signal.
- The numbers above the bar display indicate the CSQ value of the signal.
- The dBm value is shown in brackets after the CSQ value.

ID of the wireless cell

ID for the wireless cell in the mobile wireless network

LAC (Location Area Code)

ID for the current location of the M875 within the mobile wireless network

ARFCN (Absolute Radio Frequency Channel Number)

Based on the ARFCN, the uplink and downlink frequencies can be calculated.

BSIC (Base Station Identity Code)

This ID is used to be able to distinguish neighboring channels when the frequency bands overlap.

4.5.4 Traffic volume supervision

This function monitors when a specified limit value for data transfer is reached. The upper limit that you specify defines the maximum data volume per month.

The current data volume of the particular month and the upper limit are displayed on the "System - Status" page opened under the "Overview" entry.

The M875 can send SMS messages automatically as soon as 80% and 100% of the specified data volume are reached.

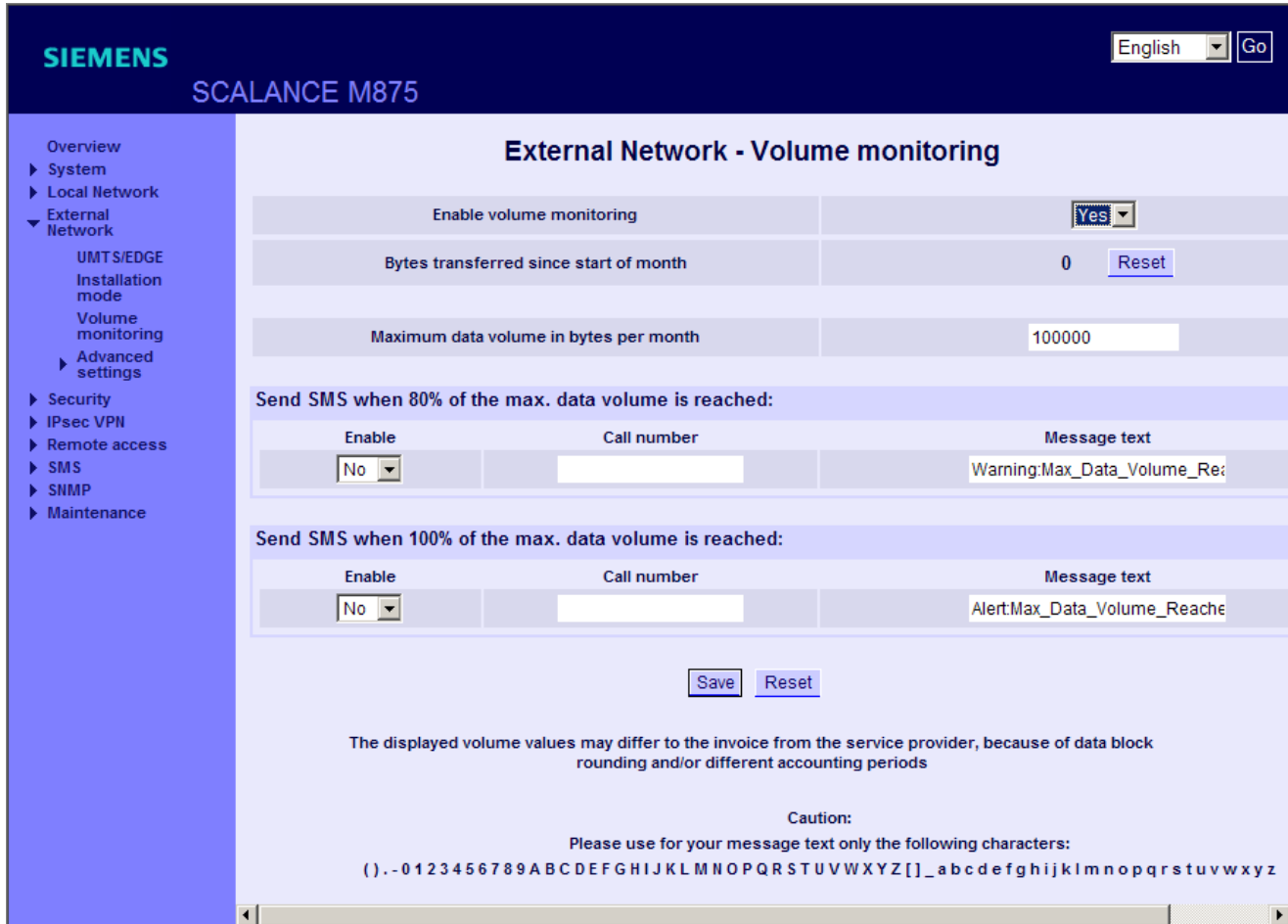
In the factory settings the volume monitoring is deactivated.

Note

The data volume per month calculated here can significantly differ from the billing of the mobile wireless provider due to block rounding and different billing periods.

Calling the Web page

Select "External Network" > "Volume Supervision" in the navigation panel.



Enabling volume supervision

The following options are available:

- Yes: The volume supervision is enabled.
- No: The volume supervision is disabled.

Current monthly byte count

This counter shows the data volume in bytes that was transferred via the M875 since the beginning of the month.

On the first of the month, the counter is automatically reset. If you click the "Reset" button, the counter is set to 0 manually.

Maximum bytes per month

Enter the limit value for the monthly data volume in bytes in the input box.

In the factory settings, the value is set to 1,000,000 bytes.

Send SMS when 80% of the max. data volume is reached

If you want the M875 to send a warning SMS message as soon as 80 % of the data volume has been reached, make the following settings:

1. Enable the SMS function by selecting the "Yes" option from the drop-down list.
2. Enter the call number of a subscriber that can receive the SMS messages.
3. If necessary change the message text from the factory settings.
4. Then click the "Save" button.

Send SMS when 100% of the max. data volume is reached

If you want the M875 to send an alarm SMS message as soon as 100 % of the data volume has been reached, make the following settings:

1. Enable the SMS function by selecting the "Yes" option from the drop-down list.
2. Enter the call number of a subscriber that can receive the SMS messages.
3. If necessary change the message text from the factory settings.
4. Then click the "Save" button.

Factory settings

Enabling volume supervision:	No (turned off)
Maximum bytes per month:	1,000,000
Send SMS when 80% of the max. data volume is reached	
Enable:	<ul style="list-style-type: none"> • Yes: Turned on • No: Turned off
Call number:	Call number of the receiving telephone
Message text:	Warning:Max_Data_Volume_nearly_reached
Send SMS when 100% of the max. data volume is reached	
Enable:	<ul style="list-style-type: none"> • Yes: Turned on • No: Turned off
Call number:	Call number of the receiving telephone
Message text:	Alert:Max_Data_Volume_reached

4.5.5 Checking the connection - Connection monitoring

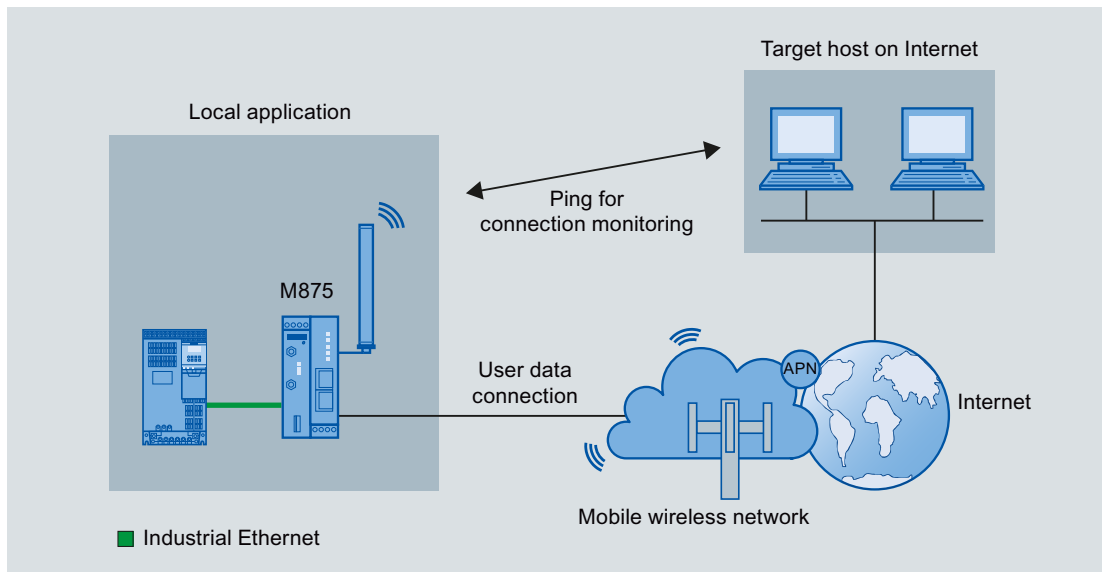


Figure 4-6 Connection monitoring

With the "Connection Check" function, the M875 checks its connection to the mobile wireless network and to the connected external networks, such as the Internet or an intranet. To do this, the M875 sends ping packets (ICMPs) to up to four configurable ping targets at regular intervals. Sending ping packets depends on the user data connections. If the M875 receives a reply from at least one of the remote stations, this means that the device is still connected to the mobile wireless service and is therefore operational.

Some mobile wireless providers interrupt connections when they are inactive. This is prevented by the "Connection Check" function.

Note

Increased costs due to extra data traffic

By sending the ping packets, the data traffic on the UMTS/GPRS connection is increased. This may result in additional costs, depending on your user agreement with the mobile wireless provider.

Calling the Web page

Select "External Network > "Advanced settings" > "Connection Check" in the navigation panel.

The screenshot shows the Siemens SCALANCE M875 web interface. The top navigation bar includes the Siemens logo, the model name 'SCALANCE M875', and a language dropdown set to 'English' with a 'Go' button. The left sidebar contains a navigation menu with the following items: Overview, System, Local Network, External Network (expanded), UMTS/EDGE, Installation mode, Volume monitoring, Advanced settings (expanded), Checking the connection (selected), DynDNS, SRS, NAT, Security, IPsec VPN, Remote access, SMS, SNMP, and Maintenance. The main content area is titled 'External Network - Advanced settings - Checking the connection'. It features a table with the following settings:

Enable connection check	Yes
List of the destination hosts	
	Host name
	<input type="text"/>
	<input type="text"/>
	<input type="text"/>
	<input type="text"/>
Interval for connection check (minutes)	2
Number of permitted unsuccessful attempts	2
Activity on faulty connection	Renew Connection

At the bottom of the main content area, there are 'Save' and 'Reset' buttons.

Checking the connection

The following options are available:

- Yes: The connection check is enabled.
- No: The connection check is disabled.

Note

Restart after turning off the function

If connection monitoring is enabled and you disable the function, you will need to restart the M875 for the change to take effect.

List of the destination hosts

Note

Reachability of the partners

To be able to respond to the ping at any time, the remote stations must be reachable constantly. You should therefore select a remote station where you can influence its reachability yourself.

Enter the host name of a remote station in the individual input boxes.

Interval for connection check (minutes)

Make an entry to specify the period in minutes after which the connection check is repeated.

Number of permitted unsuccessful attempts

Make an entry to specify the number of failures after which the selected "Action on faulty connection" is triggered (see below).

How it works

If at least one of the remote stations replies to the ping packet, the connection check counts as being successful.

If no remote station replies, the attempt counts as a failure. After the period specified above has elapsed, the connection check is repeated until the number of permitted failures is reached. Following this, the selected "action on faulty connection" is triggered (see below).

As soon as a remote station replies to the connection test, the counter for failures is reset.

Activity on faulty connection

Select one of the following options from the drop-down list:

- Renew Connection: Once the permitted number of failures has been reached, the M875 re-establishes the connection to the UMTS/GPRS network.
- M875 reboot: Once the number of permitted unsuccessful attempts has been reached, the M875 is restarted, see also section Reboot (Page 134).

Factory settings

Connection Check:	No (turned off)
Hostname:	-
Connection check interval:	5 (minutes)
Allowable number of failures:	3 (failed attempts)
Activity on faulty connection:	Renew Connection

4.5.6 Hostname by DynDNS

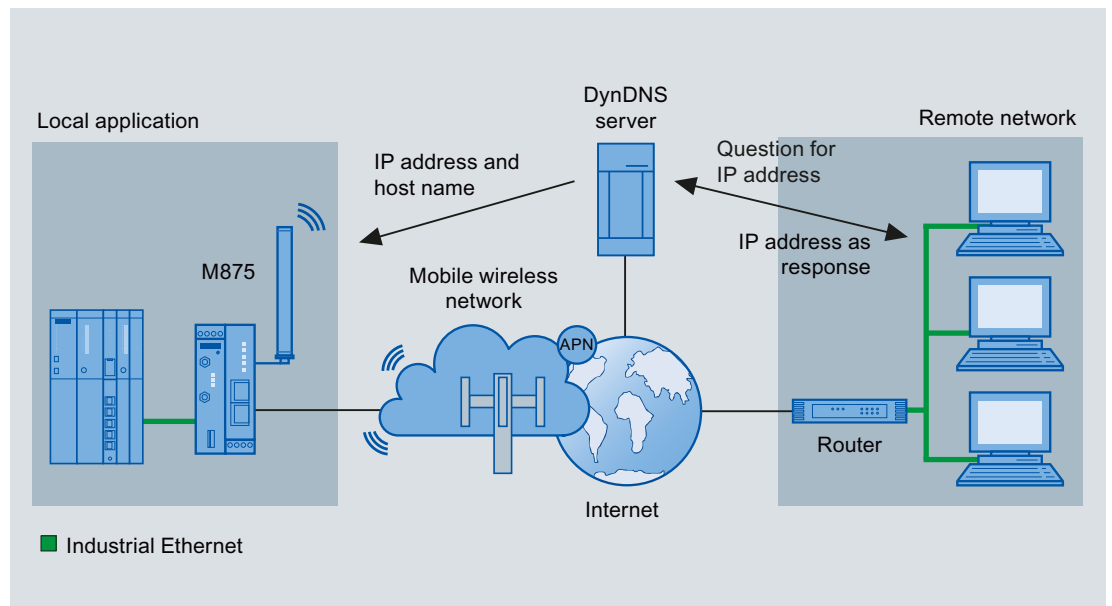


Figure 4-7 DynDNS connection configuration

Even if applications do not have a fixed IP address and are not registered under a host name, it is possible to make them reachable on the Internet. This is possible with a Dynamic Domain Name System (DynDNS).

If you log the M875 on to a DynDNS service, the device can be reached from the external network under a hostname, for example "myName.dyndns.org".

Requirements

Note that only public IP addresses can be made known using a DynDNS service.

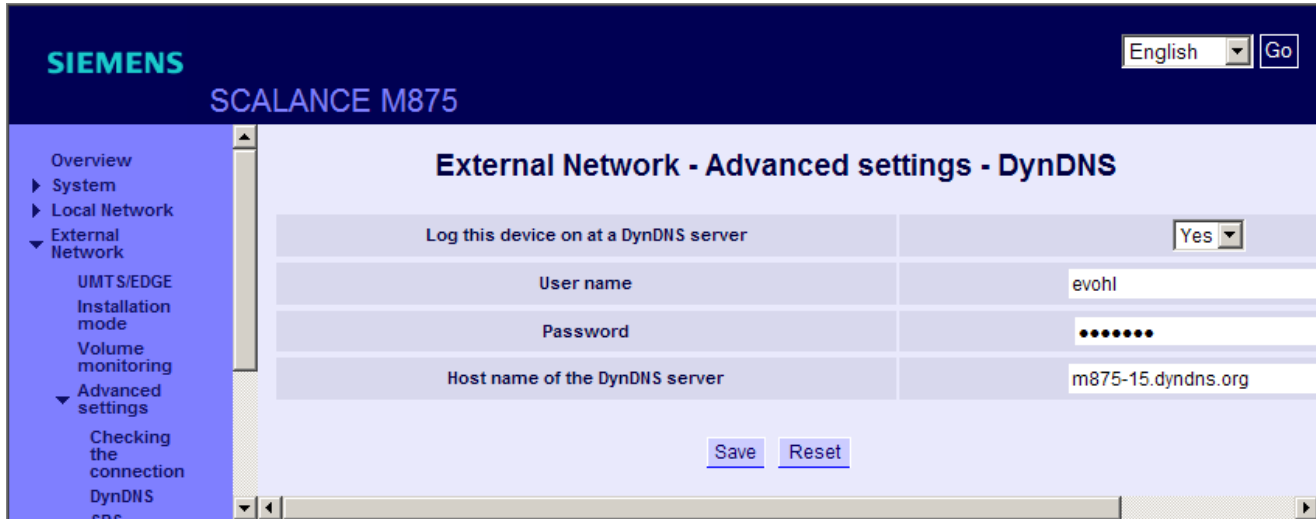
The reachability of the IP address from the Internet must also be enabled by your network provider.

DynDNS provider

The M875 is compatible with the DNS services provided by DynDNS.org.

Calling the Web page

Select "External Network > "Advanced settings" > "DynDNS" in the navigation panel.



Log this device on at a DynDNS server

Select "Yes" from the drop-down list.

The following options are available:

- Yes: Logon to a DynDNS service.
- No: No logon to a DynDNS service.

User name and password

Enter here the user name and the password that authorize you to use the DynDNS service. Your DynDNS provider will give you this information.

Host name of the DynDNS server

Here enter the hostname that you have agreed with your DynDNS provider for the M875, e.g. myName.dyndns.org.

Note

Successful logon

You will find information indicating whether or not the logon with a DNS service was successful in the log.

Factory settings

Log on to DynDNS server:	No (turned off)
User name:	guest
Password:	guest
Host name of the DynDNS server:	myname.dyndns.org

4.5.7 SRS - Siemens Remote Service

Note

Using the services provided by the "SIMATIC Remote Support Services", remote access to machines and plants is available.

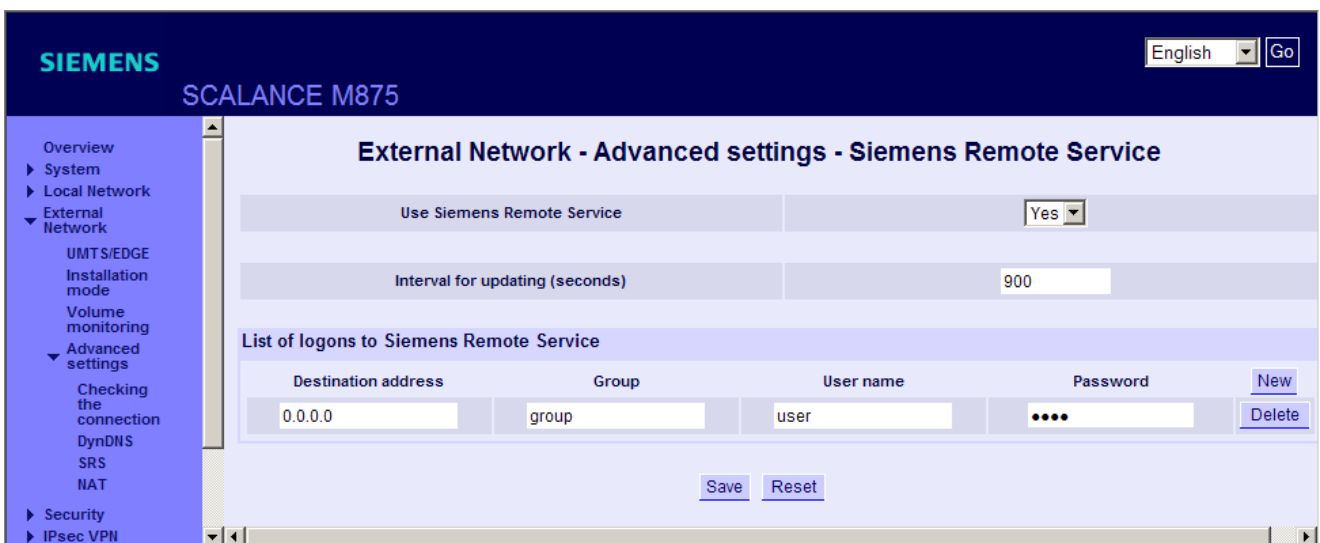
To use the services, additional service agreements are necessary and certain constraints must be kept to. If you are interested in the Siemens Remote Service, speak to your local Siemens contact.

If the Siemens Remote Service is activated, the M875 transfers its external IP address assigned by the UMTS/EDGE service to a selectable destination server. This transfer is made using the secure HTTPS protocol.

The procedure is comparable with the DynDNS service and requires suitable access to the server.

Calling the Web page

Select "External Network > "Advanced settings" > "SRS" in the navigation panel.



Use Siemens Remote Service

The following options are available:

- Yes: Use Siemens Remote Service.
- No: Do not use Siemens Remote Service.

To use the Siemens Remote Service, select "Yes" in the drop-down list.

Interval for updating (seconds)

Enter the interval in seconds at which the IP address of the M875 is transferred to the specified destination server.

Logons to Siemens Remote Service

To log on with the Siemens Remote Service, click the "New" button.

- **Destination address**
Enter the IP address of the destination server.
- **Group**
Enter the group name.
- **User name**
Enter the user name for access to the destination server.
- **Password**
Enter the password for access to the destination server.

Note

Permitted characters for user name and password:

- a b c d e f g h i j k l m n o p q r s t u v w x y z
 - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
 - 0 1 2 3 4 5 6 7 8 9
-

Factory settings

Use Siemens Remote Service:	No (turned off)
Interval for updating (seconds):	900
Remote host:	0.0.0.0
Group:	group
User name:	user
Password:	pass

4.5.8 NAT - Network Address Translation

NAT

With NAT, for outgoing frames, the device can change the specified sender IP addresses from its internal network to its own external address. This NAT technology is used if the internal addresses cannot or should not be forwarded externally, for example because a private address range such as 192.168.x.x is used or because the local network structure should remain hidden. This method is also known as IP masquerading.

Calling the Web page

Select "External Network > "Advanced settings" > "NAT" in the navigation panel.

The specified rules are listed on the "NAT" page. You also have the option of setting new rules or deleting rules.

Use NAT in the external network

Select the "Yes" option from the drop-down list.

The following options are available:

- Yes: The NAT function is enabled.
- No: The NAT function is enabled.

Use NAT for the following networks

In the input box, enter the networks for which NAT will be used. Enter an address range in the CIDR notation.

Factory settings

Use NAT for the external network: Yes (turned on)

IP address range (CIDR notation): 0.0.0.0/0

4.6 Security

4.6.1 Firewall rules

The security functions of the M875 include a stateful inspection firewall. This is a method of packet filtering or packet checking. The IP packets are checked based on firewall rules in which the following is specified:

- The permitted protocols
- IP addresses and ports of the permitted sources
- IP addresses and ports of the permitted destinations

If an IP packet fits the specified parameters, it is allowed to pass through the firewall.

The rules also specify what is done with IP packets that are not allowed to pass through the firewall.

Simple packet filter techniques require two firewall rules per connection:

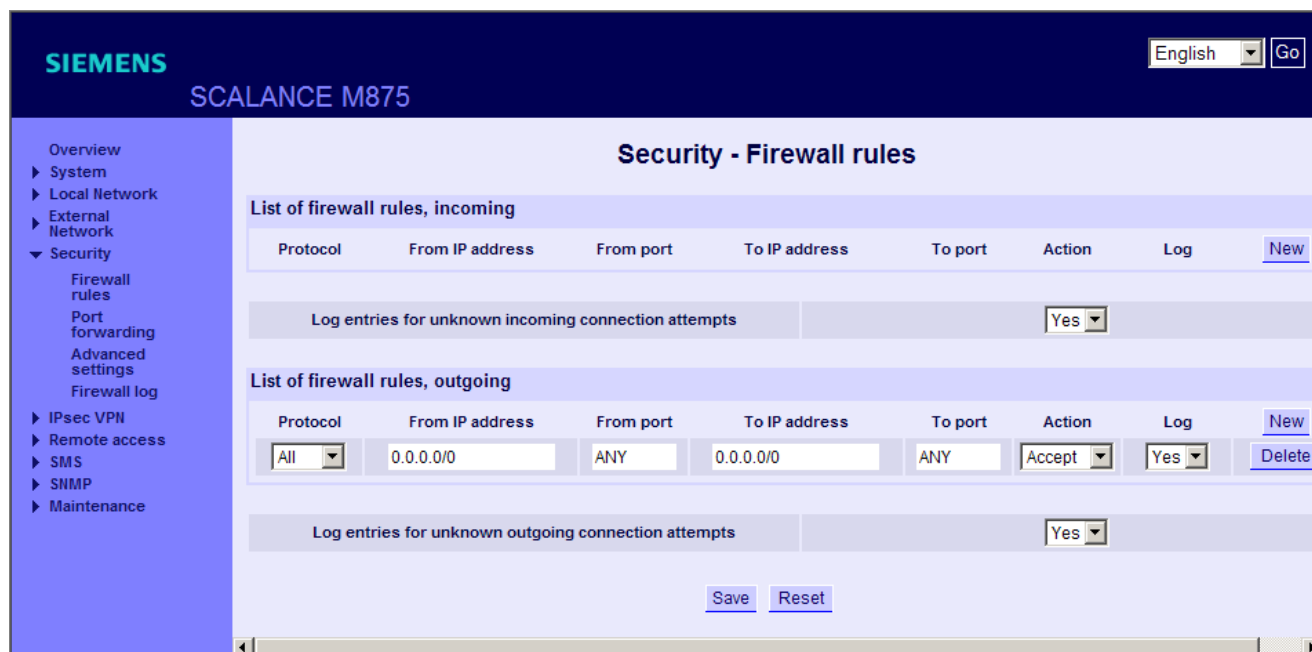
- One rule for the query direction from the source to the destination.
- A second rule for the response direction from the destination to the source.

With a stateful inspection firewall, on the other hand, you only need to specify one firewall rule for the query direction from the source to the destination since the second rule is added implicitly. The packet filter recognizes when, for example, computer "A" is communicating with computer "B" and only then does it allow replies. When the reply arrives, or after a specified timeout, no further IP packets from computer "B" are allowed to pass through. A query by computer "B" is therefore not possible without a prior request by computer "A".

Due to a special procedure, it is possible for the UPD data and ICMP data to pass through even if this data was not previously requested.

Calling the Web page

In the navigation panel, select "Security" > "Firewall Rules".



Creating firewall rules

In the factory settings, there are no firewall rules set. This means that no IP packets are allowed to pass through.

To define firewall rules, so that IP packets can pass through, follow the steps below:

1. Click the "New" button in the incoming firewall rules area.
2. Click the "New" button in the outgoing firewall rules area.

Note

Display of the firewall rules

If you create so many firewall rules that the list is limited by the window of the Web browser, refresh the view of the Web browser with the F5 function key.

Incoming firewall rules

In this area you specify what happens to IP packets received from the external network.

The sender of the IP packets counts as the source. The local applications on the M875 count as the destination.

The following entries are required:

- **Protocol**

Select a protocol from the drop-down list for which this rule will be used. The following options are available:

- All (meaning: TCP + UDP)
- TCP
- UDP
- ICMP

- **From IP address**

Enter the IP address or the IP range of the external remote stations from which IP packets may be received in the input box. To specify an address range, use the CIDR notation.

The entry "0.0.0.0/0" from the factory settings stands for all addresses.

- **From port**

Specify the port of an external remote station from which IP packets may be received. Enter the port number in the input box.

This information is only evaluated if you have selected "TCP", "UDP" or "All" as protocol.

- **To IP address**

Enter the IP address or the IP range of the local applications to which IP packets may be sent in the input box. To specify an address range, use the CIDR notation.

The entry "0.0.0.0/0" from the factory settings stands for all addresses.

- **To port**

Specify the port of a local application to which the IP packets may be sent. Enter the port number in the input box.

This information is only evaluated if you have selected "TCP", "UDP" or "All" as protocol.

- **Action**

From the drop-down list, select one of the following actions that specifies what happens to incoming IP packets:

- Allow: The IP packets are allowed to pass through.
- Reject: The IP packets are rejected, and the sender receives a corresponding message.
- Discard: The data packets are deleted without any notification to the sender.

- **Log**

For each firewall rule, specify whether an event will be logged in the firewall log if the rule is put into effect.

For more detailed information, refer to the section Firewall Log (Page 84).

Select the relevant option from the drop-down list.

- Yes: Log entry.
- No: No log entry.

Log entries for unknown incoming connection attempts

Specify whether the connection attempts not covered by the specified rules will be logged.
Select the relevant option from the drop-down list.

- Yes: Log entry
- No: No log entry

Outgoing firewall rules

In this area, you specify what happens to IP packets sent from the local network.

A local application on the M875 that sends IP packets counts as the source. An external remote station, for example on the Internet, counts as the destination.

- **Protocol**

Select a protocol from the drop-down list for which this rule will be used. The following options are available:

- All (meaning: TCP + UDP)
- TCP
- UDP
- ICMP

- **From IP address**

Enter the IP address or the IP range of the local applications that may send IP packets to the external network in the input box. To specify an address range, use the CIDR notation.

The entry "0.0.0.0/0" from the factory settings stands for all addresses.

- **From port**

Specify the port from which the local application is allowed to send IP packets. Enter the port number in the input box.

This information is only evaluated if you have selected "TCP", "UDP" or "All" as protocol.

- **To IP address**

Enter the IP address or the IP range of the external remote stations to which IP packets may be sent in the input box. To specify an address range, use the CIDR notation.

The entry "0.0.0.0/0" from the factory settings stands for all addresses.

- **To port**

Specify the port to which the external partner is allowed to send IP packets. Enter the port number in the input box.

This information is only evaluated if you have selected "TCP", "UDP" or "All" as protocol.

- **Action**

From the drop-down list, select one of the following actions that specifies what happens to outgoing IP packets:

- **Allow:** The IP packets are allowed to pass through.
- **Reject:** The IP packets are rejected, and the sender receives a corresponding message.
- **Discard:** The data packets are deleted without any notification to the sender.

- **Log**

For each firewall rule, specify whether an event will be logged in the firewall log if the rule is put into effect.

For more detailed information, refer to the section Firewall Log (Page 84).

Select the relevant option from the drop-down list:

- **Yes:** Log entry
- **No:** No log entry

Log entries for unknown outgoing connection attempts

Specify whether the connection attempts not covered by the specified rules will be logged.

Select the relevant option from the drop-down list.

- **Yes:** Log entry
- **No:** No log entry

Factory settings

Incoming firewall rules

Incoming firewall rules:	None (everything blocked)
Protocol:	All
From IP address:	0.0.0.0/0
From port:	ANY
To IP address:	0.0.0.0/0
To port:	ANY

Action:	Allow
Log:	No (turned off)
Log entries for unknown incoming connection attempts:	No (turned off)

Outgoing firewall rules

Outgoing firewall rules:	None (everything blocked)
Protocol:	All
From IP address:	0.0.0.0/0
From port:	ANY
To IP address:	0.0.0.0/0
To port:	ANY
Action:	Allow
Log:	No (turned off)
Log entries for unknown outgoing connection attempts:	No (turned off)

4.6.2 Port Forwarding

A further security function of the M875 is port forwarding. You will also need to create rules for port forwarding.

When a frame from the external network arrives at a specified port, the header of the frame is changed. Due to the rules for port forwarding, the frame can be forwarded to a defined IP address at a defined port.

This method is also known as destination NAT.

Port forwarding can be configured for the TCP or UDP protocols.

Note

Firewall rule for port forwarding

For incoming frames to be forwarded to the defined IP address in the local network, you need to set up a corresponding incoming firewall rule for this IP address. For more detailed information, refer to the section Firewall rules (Page 76).

Calling the Web page

In the navigation panel, select "Security"> "Port Forwarding".



List of rules for forwarding

Based on the following parameters, define a rule for port forwarding.

To add a further rule, click the "New" button.

To remove an existing rule, click the "Delete" button.

Save your settings by clicking the "Save" button.

- **Protocol**

Select a protocol from the drop-down list for which the rule will be used. The following are available:

- TCP
- UDP

- **Arrives at port**

Specify the port at which the frames to be forwarded arrive from the external network. Enter the port number in the input box.

- **Is forwarded to IP address**

Specify the local application to which the incoming frames will be forwarded. Enter the IP address of the local application in the input box.

- **Is forwarded to port**

Specify the port for the IP address of the local application. Enter the port number in the input box.

- **Log entry**

Specify whether an event will be logged in the firewall log if the rule takes effect.

For more detailed information, refer to the section Firewall Log (Page 84).

Select the relevant option from the drop-down list.

- Yes: Log entry
- No: No log entry

Factory settings

Protocol:	TCP
Arrives at port:	80
Is forwarded to IP address:	127.0.0.1
Is forwarded to port:	80
Log entry:	No (turned off)

4.6.3 Advanced security functions

The advanced security functions serve to protect the M875 and the connected local applications against attacks. It is assumed that in normal operation a certain number of connections or a certain number of ping packets will not be exceeded. Specify upper limits for these incoming and outgoing packets. If the specified upper limits are exceeded, all further packets are rejected.

Calling the Web page

In the navigation panel, select "Security"> "Advanced settings". The "Security - Advanced settings" page appears with the entries and options described below (factory settings).

Factory settings

The factory settings were selected so that they will never be reached in normal use. If, however, there is an attack, the upper limits specified below can be exceeded easily.

If there are special requirements in your operating environment, enter suitable values in the input boxes.

- Maximum number of new incoming TCP connections per second: 25
- Maximum number of new outgoing TCP connections per second: 75
- Maximum number of new incoming ping packets per second: 3
- Maximum number of new outgoing ping packets per second: 5
- External ICMP: Drop

External ICMP

Specify what happens to ICMP packets that are sent from the external network in the direction of the M875.

Note

Increased costs due to extra data traffic

By sending and replying to the ICMP packets, the data traffic is increased on the UMTS/GPRS connection. This may result in additional costs, depending on your user agreement with the mobile wireless provider.

Select one of the following options from the drop-down list:

- Allow: All types of ICMP packets are accepted and replied to.
- Allow ping: Only ping packets are accepted and replied to.
- Discard: All types of ICMP packets are blocked.

4.6.4 Firewall Log

Each time individual firewall rules are applied, this is recorded in the firewall log. To do this, you must first activate the log function for the individual firewall rules and for the rules for port forwarding.

You can view the firewall log with a text editor or store the log file on your Admin PC.

Calling the Web page

In the navigation panel, select "Security" > "Firewall Log".

Click "Download". A dialog for opening and saving the log file appears. Select the required option and follow the instructions in the displayed dialogs.

Note

The entries in the firewall log are lost if the device is rebooted.

4.7 IPsec VPN - Virtual Private Network

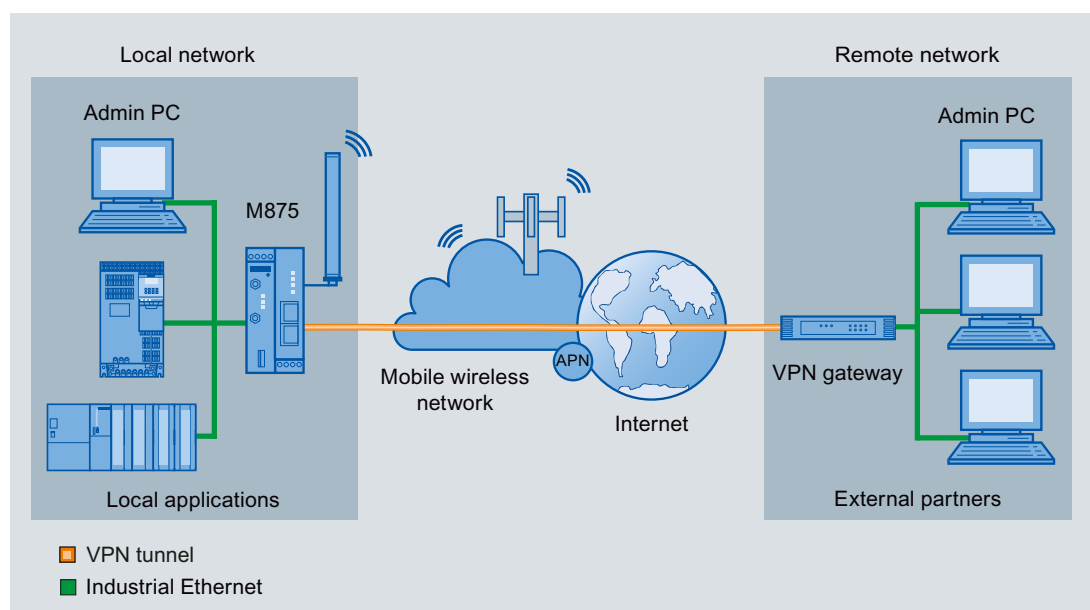


Figure 4-8 Example of a VPN connection configuration

The M875 can connect the local network with a "friendly" remote network via a VPN tunnel. The frames that are exchanged between the two networks are encrypted and protected from illegal manipulation by the VPN tunnel. This means that unprotected public networks such as the Internet can also be used to transport the data without the confidentiality or data integrity being put at risk.

To allow the M875 to establish a VPN tunnel, the remote network must have a VPN Gateway as the partner.

4.7.1 Explanation of VPN connections

The IPsec protocol suite

The M875 uses the IPsec method in the tunnel mode for the VPN tunnel. Here, the frames to be transferred are completely encrypted and provided with a new header before they are sent to the VPN gateway of the partner. The frames received by the partner are decrypted and forwarded to the recipient.

Roadwarrior mode and standard mode

There are two modes for VPN connections:

- **Roadwarrior mode**

In the Roadwarrior mode, the M875 can accept up to 10 VPN connections from partners with an unknown address. These partners can, for example, be mobile partners that obtain their IP address dynamically. In addition to this, VPN connections can also be operated in standard mode.

The VPN connection must be established by the partner. In Roadwarrior mode, the M875 can only accept VPN connections but cannot establish them actively.

- **Standard mode**

In standard mode, the address of the VPN gateway of the partner must be known so that the VPN connection can be established. The VPN connection can either be established by the M875 or by the VPN gateway of the remote station.

Authentication method

The M875 supports three authentication methods:

- X.509 certificate
- CA certificate
- Pre-shared Key (PSK)

X.509 certificate and CA certificate

With the authentication methods X.509 certificate and CA certificate, keys are used for authentication that were previously signed by a certification authority (CA). This method is considered particularly secure. A CA can be a provider but also, for example the system administrator of your project as long as the required software tools are available. The CA creates a certificate file (PKCS12) for both ends of a VPN connection with the file extension ".p12". This certificate file contains the public and private key of the local station, the signed certificate of the CA and the public key of the CA. With the authentication method X.509, there is also a key file (*.pem, *.cer or *.crt) for both of the partner stations with the public key of the local station.

The two methods differ in the exchange of the public key. With X.509 certificate, the key and the key file are exchanged between the M875 and the VPN gateway manually, for example using a CD-ROM or e-mail. You will find more information on loading the certificate in the section "Managing certificates and keys (Page 105)".

With CA certificate, the key is exchanged between the M875 and VPN gateway of the remote station via the data connection when the VPN connection is established. Here, there is no manual exchange of key files.

Pre-shared Key (PSK)

This method is supported in the main by older IPsec implementations. Here, the authentication is made with a previously agreed character string. To achieve a high degree of security, use character strings made up of approximately 30 uppercase and lowercase characters as well as numbers selected at random.

Local ID and ID of the partner

The local ID and the ID of the partner are used by IPsec to uniquely identify the partners during establishment of the VPN connection. The device's own local ID forms the remote ID of the remote station and vice versa.

- **When authenticating with X.509 certificate and CA certificate:**
 - If you leave the default setting "NONE", the distinguished names from the device's own certificate and from the certificate transferred by the partner are automatically adopted and used as the local ID and ID of the partner.
 - If you change the entries for the local ID or the ID of the partner manually, adapt the entries of the partner accordingly. The manual entry for the IDs must be made in the ASN.1 format, for example "C=XY/O=XY Org/CN=xy.org.org".
- **With authentication using Pre-shared Key:**
 - In Roadwarrior mode, you need to enter the ID of the partner manually. It must have the format of a host name or the format of an e-mail address and must match the local ID of the partner.
 - If you leave the local ID set to "NONE", the IP address is used as the local ID.
 - If you enter the local ID manually, this must have the format of a host name or the format of an e-mail address and must match the ID of the partner.

1:1 NAT

When a VPN tunnel is being established, a special variant of the NAT is used with the M875, the 1:1 NAT, also known as bidirectional NAT. This variant allows connection establishment both from the local network to the external network and from the external network to the local network. With the M875, the network addresses of the frames are changed.

For each VPN connection and for both connection directions, you can specify individually whether or not the 1:1 NAT function is enabled. You can make the relevant settings on the "IPsec VPN - Edit connection" page.

IKE

Abbreviations/acronyms

- IKE: Internet Key Exchange
- SA: Security Association
- ISAKMP: Internet Security Association and Key Management Protocol
- IPsec: Internet Protocol security

Connection establishment

The VPN connection is established in two phases.

1. Initially, in phase 1, the security association (SA) is established using the ISAKMP protocol. Phase 1 is used for the exchange of keys between the M875 and the VPN gateway of the remote station.
2. Following this, in phase 2, the SA is established via the IPsec protocol. Phase 2 is the actual IPsec connection between the M875 and the VPN gateway of the remote station.

ISAKMP SA and IPsec SA encryption

The M875 also supports the following methods:

- 3DES-168
- AES-128
- AES-192
- AES-256

AES-128 is a commonly used method and is therefore set as default.

Note

The more bits in an encryption algorithm - specified by the appended number - the safer the algorithm is. The AES-256 method is therefore considered the most secure. However the encryption procedure takes more time and requires more computing power the longer the key is.

NAT-T

There may be a NAT router between the M875 and the VPN gateway of the remote network. Not all NAT routers allow IPsec frames to pass through. This means that it may be necessary to encapsulate the IPsec frames in UDP packets to be able to pass through the NAT router.

Dead peer detection

If the remote station supports the Dead Peer Detection protocol (DPD), the partners can recognize whether the IPsec connection is still valid or needs to be re-established. Without DPD and depending on the configuration, it may be necessary to wait until the SA lifetime has expired or the connection must be reinitiated manually. To check whether the IPsec connection is still valid, the Dead Peer Detection itself sends DPD queries to the remote station. If the remote station does not reply, the IPsec connection is considered to be interrupted after a number of permitted failures.

Note

Sending DPD queries increases the amount of data sent and received. This can lead to increased costs.

Requests to the VPN gateway of the remote network

To allow an IPsec connection to be established successfully, the VPN remote station must support IPsec with the following configuration:

- Authentication with X.509 certificates, CA certificates or Pre Shared Key
- ESP
- Diffie-Hellman group 1, 2 or 5

- 3DES or AES encryption
- MD5 or SHA-1 hash algorithms
- Tunnel mode
- Quick mode
- Main mode
- SA lifetime (1 second to 24 hours)

If the remote station is a computer with Windows 2000, the Microsoft Windows 2000 High Encryption Pack or at least service pack 2 must be installed.

If the remote station is downstream from a NAT router, the remote station must support NAT-T. Or, the NAT router must know the IPsec protocol (IPsec/VPN passthrough).

4.7.2 Connections - Roadwarrior mode

4.7.2.1 Creating connections

The Roadwarrior mode allows the M875 to accept VPN connections initiated by a partner with an unknown IP address. The remote station must authenticate itself correctly. In Roadwarrior mode, however, identification of the partner based on the IP address or the host name of the remote station is omitted.

Set up the M875 after consulting the system administrator of the remote station.

Calling the Web page

Select "IPsec VPN" > "Connections" in the navigation panel.

The screenshot shows the web interface for the SIEMENS SCALANCE M875. The navigation panel on the left includes 'Overview', 'System', 'Local Network', 'External Network', 'Security', 'IPsec VPN', 'Remote access', 'SMS', 'SNMP', and 'Maintenance'. The 'IPsec VPN' section is expanded to show 'Connections'. The main content area is titled 'IPsec VPN - Connections' and contains two tables. The first table, 'VPN connections in roadwarrior mode', has columns for 'Enabled', 'Name', 'Connection settings', and 'IKE settings'. It shows one entry named 'Roadwarrior' with 'Enabled' set to 'No'. The second table, 'VPN connections in standard mode', has columns for 'Enabled', 'Name', 'Connection settings', 'IKE settings', and 'New'. It shows one entry with 'Enabled' set to 'No'. At the bottom of the page, there are 'Save' and 'Reset' buttons.

VPN connections in Roadwarrior mode

Enabled

The following options are available:

- Yes: The Roadwarrior mode is enabled.
- No: The Roadwarrior mode is disabled.

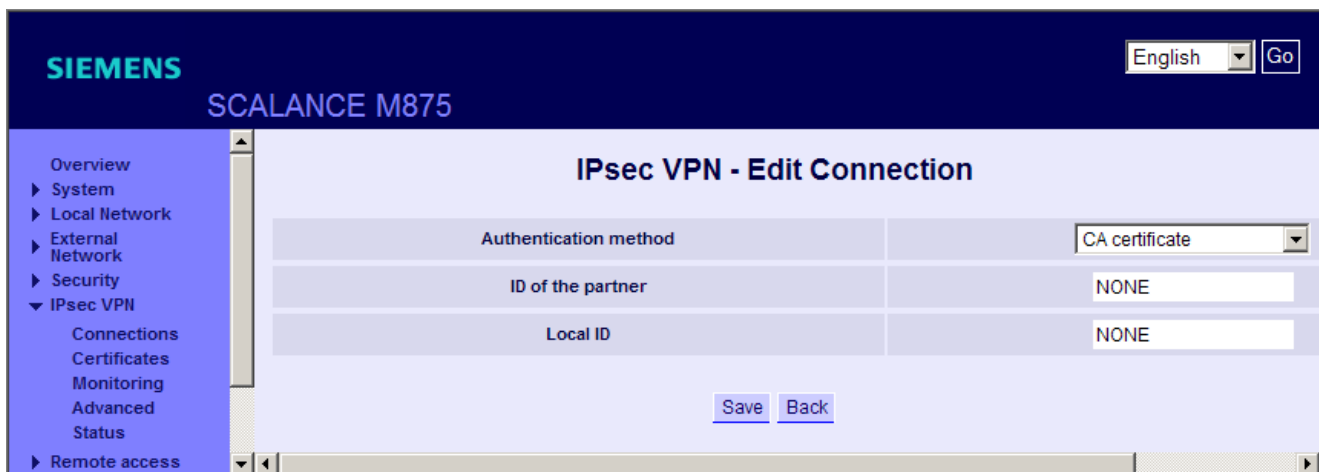
Name

The name of the VPN connection in Roadwarrior mode is fixed and cannot be modified.

4.7.2.2 Editing connections

Connection settings

Click the "Edit" button under "Connection settings".
The following page appears:



Authentication method

You will find more information on the authentication method in the section Explanation of VPN connections (Page 85).

In consultation with the administrator of the remote station, select one of the three following options from the drop-down list:

- CA certificate -
- X.509 partner certificate: Specifies a X.509 partner certificate loaded on the M875 as the authentication method and you select the certificate from the following drop-down list.
See also section Managing certificates and keys (Page 105).

- **Pre-shared key:** With this option, you enter the pre-shared key that needs to be known by the communications partner.
With self-selected keys, you can enter a character string consisting of up to 30 upper and lowercase letters or numbers.

Partner certificate

In the drop-down list you will find the certificates of the remote station that have already been loaded on the M875.

Select the certificate for the VPN connection.

ID of the partner

Enter the ID of the remote station in the input box or leave the setting "NONE". For more detailed information, refer to the section Explanation of VPN connections (Page 85).

Local ID

Enter the local ID in the input box or leave the setting "NONE". For more detailed information, refer to the section Explanation of VPN connections (Page 85).

4.7.2.3 IKE settings

IKE settings

Set up the IKE settings in consultation with the administrator of the partner. You can specify different methods for ISAKMP SA and IPsec SA.

For more detailed information on encryption, refer to section Explanation of VPN connections (Page 85).

On the "IPsec VPN - Connections" page, you will find the "Edit" button in the "VPN connections in roadwarrior mode" area under "IKE settings". If you click on this, the page shown below opens:



Phase 1 and phase 2: ISAKMP SA and IPsec SA

- Encryption

Note

The more bits in an encryption algorithm - specified by the appended number - the safer the algorithm is. The AES-256 method is therefore considered the most secure. However the encryption procedure takes more time and requires more computing power the longer the key is.

From the drop-down list for phase 1 and phase 2, select one of the following options for each:

- 3DES-168
- AES-128
- AES-192
- AES-256

- **Hash (checksum)**

To calculate checksums (hash) during phases 1 (ISAKMP SA) and 2 (IPsec SA), three methods are available:

- MD5 or SHA-1 (automatic detection)
- MD5
- SHA-1

From the drop-down lists, select a method for phase 1 and a method for phase 2. You can specify different methods for ISAKMP SA and IPsec SA.

- **Mode**

To negotiate the ISAKMP SA, two methods are available:

- Main mode
- Aggressive mode

Select a mode from the drop-down list.

Note

When using the pre-shared key authentication method, you need to set "Aggressive mode" in the Roadwarrior mode and specify a remote ID.

- **Lifetime (seconds)**

The keys of a connection are renewed at certain intervals to increase the effort needed for an attack on the connection.

In the input box, enter a period in seconds to specify the lifecycle of the agreed keys. You can specify different periods for ISAKMP SA and IPsec SA.

NAT-T

Select one of the three following options from the drop-down list:

- On: If the M875 recognizes a NAT router, that does not allow the IPsec frames to pass through, the UDP encapsulation starts automatically.
- Off: The NAT-T function is disabled.
- Force: When negotiating the connection parameters of the VPN connection, the device insists that the frames are transferred on the connection encapsulated.

Enabling Dead Peer Detection (DPD)

Note

Sending DPD queries increases the amount of data sent and received via EGPRS or GPRS. This can lead to increased costs.

Select one of the two options from the drop-down list:

- Yes: Dead peer detection is enabled. Regardless of whether user data is being transmitted, the M875 recognizes loss of the connection. In this case, the device waits for the connection to be re-established by the remote stations.
- No: Dead peer detection is disabled.

If you select "Yes", the following three input boxes appear:

Delay after DPD query (seconds)

Enter a period in seconds in the input box after which DPD queries are sent. These queries test whether or not the remote station is still available.

Timeout after DPD query (seconds)

Enter a length of time in seconds in the input box. If there is no response to the DPD queries, the connection to the remote station is declared to be invalid after this time has elapsed.

DPD: maximum number of unsuccessful attempts

In the input box, enter the number of permitted failures before the IPsec connection is considered to be interrupted.

For more detailed information on the NAT-T function and Dead Peer Detection in section Explanation of VPN connections (Page 85).

Factory settings in Roadwarrior mode

Enabled: No (turned off)
Name: Roadwarrior

Connection settings

Authentication method: CA certificate
Remote certificate: -
Pre-shared key: Hidden character string that is overwritten.
Remote ID: NONE
Local ID: NONE

IKE settings

Phase 1: ISAKMP-SA

Encryption: AES-128
Hash (checksum): MD5
Mode: Main mode
Lifetime (seconds): 86400

Phase 2: IPsec SA

Encryption: AES-128
 Hash (checksum): MD5
 Lifetime (seconds): 86400

NAT-T: On
 Enable Dead Peer Detection (DPD): Yes
 Delay after DPD query (seconds): 150
 Timeout after DPD query (seconds): 60
 DPD: Maximum number of failed attempts: 5

4.7.3 Connections - Standard mode**4.7.3.1 Creating connections****Calling the Web page**

In the factory settings, there are no connections created in standard mode.

Select "IPsec VPN" > "Connections" in the navigation panel.

SIEMENS SCALANCE M875

English Go

IPsec VPN - Connections

VPN connections in roadwarrior mode

Enabled	Name	Connection settings	IKE settings
No	Roadwarrior	Edit	Edit

VPN connections in standard mode

Enabled	Name	Connection settings	IKE settings
			New

[Save](#) [Reset](#)

VPN connections in standard mode

To add a VPN connection, click the "New" button below "VPN connections in standard mode".

Enabled

It is possible to enable or disable each individual connection. Select the following from the drop-down list:

- Yes: The standard mode is enabled.
- No: The standard mode is disabled.

Name

Enter a name for the VPN connection in the input box.

4.7.3.2 Editing connections

Calling the Web page

Under "Connection settings", click the "Edit" button.

The screenshot shows the 'IPsec VPN - Edit connection' configuration page in the SIEMENS SCALANCE M875 web interface. The page has a dark blue header with the SIEMENS logo and 'SCALANCE M875' text. A language dropdown menu is set to 'English' with a 'Go' button. A navigation menu on the left lists various system settings, with 'IPsec VPN' expanded to show 'Connections', 'Certificates', 'Monitoring', 'Advanced', and 'Status'. The main configuration area contains the following fields and controls:

Connection name	<input type="text" value="NewConnection"/>
Address of the VPN gateway of the partner	<input type="text" value="NONE"/>
Authentication method	<input type="text" value="X.509 partner certificate"/>
Partner certificate	<input type="text" value="---"/>
ID of the partner	<input type="text" value="NONE"/> ID from SCALANCE S
Local ID	<input type="text" value="NONE"/>
IP address of the remote network	<input type="text" value="192.168.2.1"/>
Netmask of the remote network	<input type="text" value="255.255.255.0"/>
Enable 1:1 NAT for the remote network	<input type="text" value="No"/>
IP address of the local network	<input type="text" value="192.168.1.1"/>
Netmask of the local network	<input type="text" value="255.255.255.0"/>
Enable 1:1 NAT for the local network	<input type="text" value="No"/>
Wait for connection establishment by the partner	<input type="text" value="No"/>
Firewall rules for VPN tunnel	Edit

At the bottom of the configuration area, there are 'Save' and 'Back' buttons.

Connection name

The previously entered connection name appears in this box. You can change the name here.

Address of the VPN gateway of the partner

Enter the address of the remote station in the input box either as a hostname or as an IP address.

Authentication method

You will find more information on the authentication method in the section Explanation of VPN connections (Page 85).

In consultation with the administrator of the remote station, select one of the three following options from the drop-down list:

- CA certificate -
- X.509 partner certificate: Specifies a X.509 partner certificate loaded on the M875 as the authentication method and you select the certificate from the following drop-down list.
See also section Managing certificates and keys (Page 105).
- Pre-shared key: With this option, you enter the pre-shared key that needs to be known by the communications partner.
With self-selected keys, you can enter a character string consisting of up to 30 upper and lowercase letters or numbers.

Partner certificate

In the drop-down list you will find the certificates of the remote station that have already been loaded on the M875.

Select the certificate for the VPN connection.

ID of the partner

Enter the ID of the remote station in the input box or leave the setting "NONE". For more detailed information, refer to the section Explanation of VPN connections (Page 85).

Local ID

Enter the local ID in the input box or leave the setting "NONE". For more detailed information, refer to the section Explanation of VPN connections (Page 85).

The "ID from Scalance S" button

If you have loaded the certificate of a SCALANCE S device on the M875, you can read out the remote ID from the certificate by clicking the "ID from Scalance S" button. The value read out is then automatically adopted as the remote ID.

IP address of the remote network

Enter the IP address of the remote network in the box. The remote network can also be a single computer.

Netmask of the remote network

Enter the subnet mask of the remote network in the box. The remote network can also be a single computer.

Enable 1:1 NAT for the remote network

Select one of the following two options from the drop-down list:

- Yes: 1:1 NAT is enabled for the remote network.
- No: 1:1 NAT is disabled.

If you have enabled 1:1 NAT, the address of the frames sent from the local network to a remote network is changed. See the input box below.

Address for 1:1 NAT to the remote network

In the input box, enter a network address for frames that are sent to a remote network.

Local net address

Enter the IP address of the local network (for example 123.123.123.123) in the box. The local network can also be a single computer.

Local subnet mask

Enter the subnet mask of the local network (for example 255.255.255.0) in the box. The local network can also be a single computer.

Enable 1:1 NAT for the local network

Select one of the following two options from the drop-down list:

- Yes: 1:1 NAT is enabled for the local network.
- No: 1:1 NAT is disabled.

If you have enabled 1:1 NAT, the address of the frames sent from a remote network to a local network is changed. See the input box below.

Address for local 1:1 NAT in local network

In the input box, enter a network address for frames that are received from the remote network.

Wait for remote connection

Select one of the following two options from the drop-down list:

- **Yes:** The M875 waits for the VPN gateway of the remote network to initiate establishment of the VPN connection.
- **No:** The M875 initiates the connection establishment itself.

Firewall rules for VPN tunnel

If you click the "Edit" button beside this entry, the mask appears in which you specify firewall rules for incoming and outgoing messages.

You will find more information on this topic in the section "Firewall rules for VPN tunnel (Page 103)".

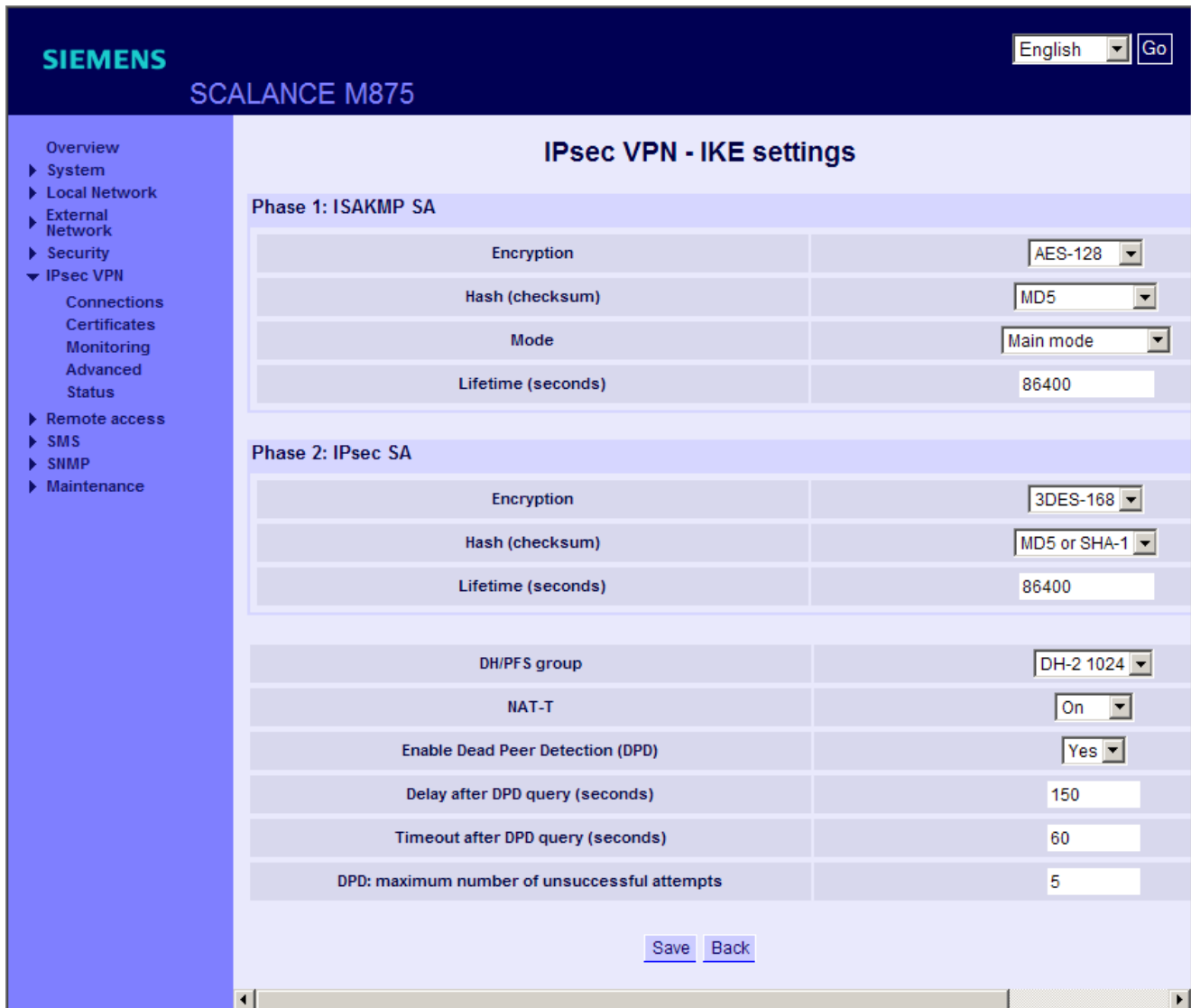
4.7.3.3 IKE settings

IKE - "Edit" button

Set up the IKE settings in consultation with the administrator of the partner. You can specify different methods for ISAKMP SA and IPsec SA.

For more detailed information on encryption, refer to section Explanation of VPN connections (Page 85).

On the "IPsec VPN - Connections" page, you will find the "Edit" button in the "VPN connections in standard mode" area under "IKE settings". If you click on this, the page shown below opens.



Phase 1 and phase 2: ISAKMP SA and IPsec SA

- Encryption

Note

The more bits in an encryption algorithm - specified by the appended number - the safer the algorithm is. The AES-256 method is therefore considered the most secure. However the encryption procedure takes more time and requires more computing power the longer the key is.

From the drop-down list for phase 1 and phase 2, select one of the following options for each:

- 3DES-168
- AES-128

- AES-192
- AES-256
- **Hash (checksum)**

To calculate checksums (hash) during phases 1 (ISAKMP SA) and 2 (IPsec SA), three methods are available:

 - MD5 or SHA-1 (automatic detection)
 - MD5
 - SHA-1

From the drop-down lists, select a method for phase 1 and a method for phase 2. You can specify different methods for ISAKMP SA and IPsec SA.
- **Mode**

To negotiate the ISAKMP SA, two methods are available:

 - Main mode
 - Aggressive mode

Select a mode from the drop-down list.
- **Lifetime (seconds)**

The keys of a connection are renewed at certain intervals to increase the effort needed for an attack on the connection.

In the input box, enter a period in seconds to specify the lifecycle of the agreed keys. You can specify different periods for ISAKMP SA and IPsec SA.

DH/PFS group

The M875 supports the Diffie Hellmann key exchange (DH) with the Perfect Forward Secrecy (PFS) property. You have three DH groups available for the key exchange.

Select one of the three following options from the drop-down list:

- DH-1 768
- DH-2 1024
- DH-5 1536

NAT-T

Select one of the three following options from the drop-down list:

- On: If the M875 recognizes a NAT router, that does not allow the IPsec frames to pass through, the UDP encapsulation starts automatically.
- Off: The NAT-T function is disabled.
- Force: When negotiating the connection parameters of the VPN connection, the device insists that the frames are transferred on the connection encapsulated.

Enabling Dead Peer Detection (DPD)

Note

Sending DPD queries increases the amount of data sent and received via EGPRS or GPRS. This can lead to increased costs.

Select one of the two options from the drop-down list:

- **Yes:** Dead peer detection is enabled. Regardless of whether user data is being transmitted, the M875 recognizes loss of the connection. In this case, the device waits for the connection to be re-established by the remote stations.
- **No:** Dead peer detection is disabled.

If you select "Yes", the following three input boxes appear:

Delay after DPD query (seconds)

Enter a period in seconds in the input box after which DPD queries are sent. These queries test whether or not the remote station is still available.

Timeout after DPD query (seconds)

Enter a length of time in seconds in the input box. If there is no response to the DPD queries, the connection to the remote station is declared to be invalid after this time has elapsed.

DPD: Maximum number of failed attempts

In the input box, enter the number of permitted failures before the IPsec connection is considered to be interrupted.

You can find more detailed information on the NAT-T function and Dead Peer Detection in chapter Explanation of VPN connections (Page 85).

Factory settings in standard mode

Enabled:	No (turned off)
Name:	NewConnection

Connection settings

Address of the VPN gateway of the partner	NONE
Authentication method:	X.509 remote certificate
Partner certificate:	-
Pre-shared key	Hidden character string that is overwritten.
ID of the partner:	NONE

Local ID:	NONE
IP address of the remote network:	192.168.2.1
Netmask of the remote network:	255.255.255.0
1:1 NAT for the remote network:	No (turned off)
Local net address:	192.168.1.1
Local subnet mask:	255.255.255.0
Enable 1:1 NAT for the local network:	No (turned off)
Wait for remote connection:	No
Firewall rules for VPN tunnel:	No rules set.

IKE settings**ISAKMP SA**

Encryption:	3DES-168
Hash (checksum):	MD5 or SHA-1
Mode:	Main mode
Lifetime (seconds):	86400

IPsec SA

Encryption:	3DES-168
Hash (checksum):	MD5 or SHA-1
Lifetime (seconds):	86400
DH/PFS group	DH-2 1024
NAT-T:	On
Enable Dead Peer Detection (DPD):	Yes
Delay after DPD query (seconds):	150
Timeout after DPD query (seconds):	60
DPD: Maximum number of failed attempts:	5

4.7.3.4 Firewall rules for VPN tunnel

The IPsec VPN connection is considered to be secure. This means that data traffic via this connection is not normally restricted. It is, nevertheless possible to create firewall rules for VPN connections in standard mode.

Calling the Web page

Select "IPsec VPN" > "Connections" in the navigation panel.



To create the firewall rules, follow exactly the same steps as described in section Firewall rules (Page 76).

1. Click the "Edit" button under "Connection settings" in the "VPN connections in standard mode" area.
2. In the "Firewall rules for VPN Tunnel" line, click the "Edit" button.

Note that the rule specified here only applies to the individual, selected VPN connection.

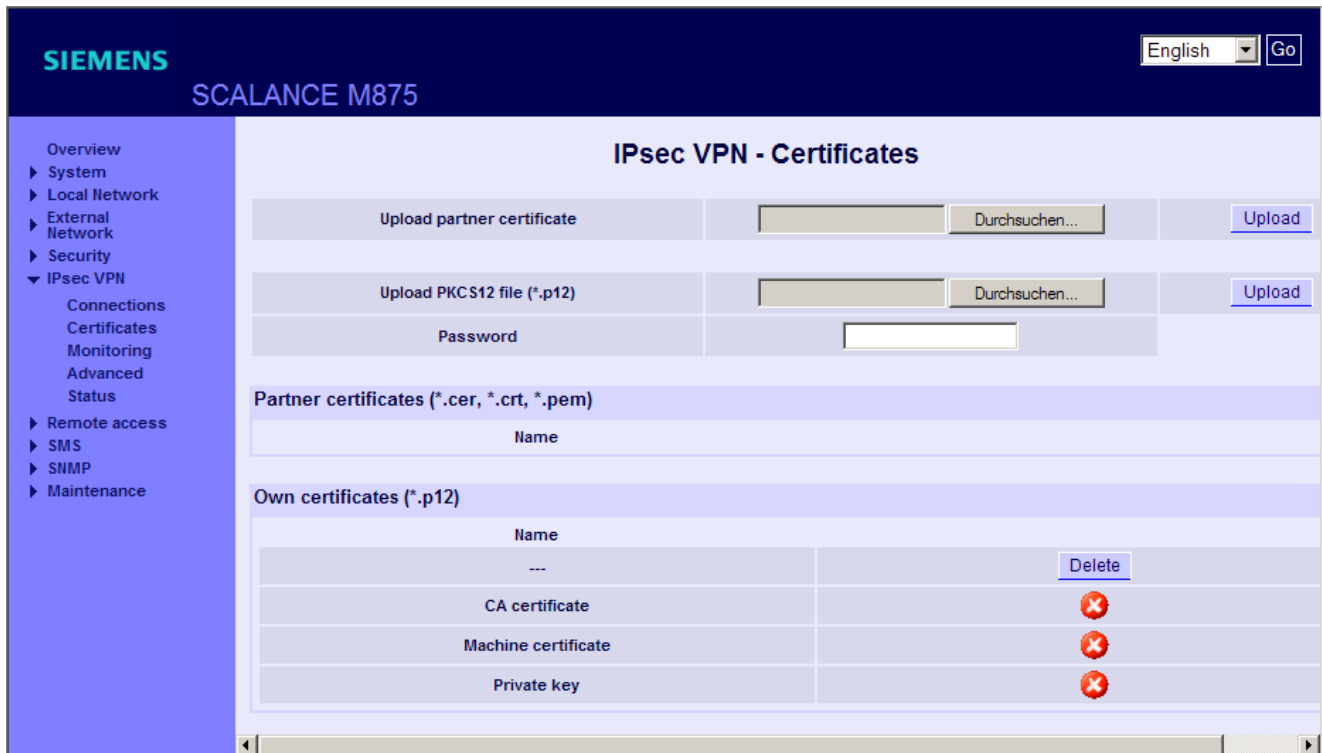
Factory settings

In the factory settings, there are no restrictions by firewall rules.

4.7.4 Managing certificates and keys

Calling the Web page

Select "IPsec VPN" > "Certificates" in the navigation panel.



Upload partner certificate

You require the partner certificate only if you have selected the option "X.509 partner certificate" as the authentication method.

To be able to upload a suitable certificate, the corresponding key file (*.pem, *.cer or *.crt) must be stored on the Admin PC.

1. Click the "Browse..." button.
A dialog for the file selection opens.
2. Select a key file and click the "Open" button in the dialog.
The path information appears in the input box on the Web user interface.
3. Click the "Upload" button to load the key file on the M875.

Upload PKCS12 file (*.p12)

PKCS stands for "Public Key Cryptography Standards" and covers a series of cryptographic specifications. The PKCS#12 specification defines a file format that is used to store private keys along with the corresponding certificate password protected.

Note

If there is already a certificate file on the device, this file must be deleted before loading a new file. See below under "Device certificates".

To be able to upload a PKCS12 file, the corresponding file (*.p12) must be stored on the Admin PC.

1. Click the "Browse..." button.

A dialog opens in which you can select the file.

2. Select the PKCS12 file and click the "Open" button in the dialog.

The path information appears in the input box on the Web user interface.

3. Enter the password for the PKCS12 file in the input box.
4. Click the "Upload" button to load the file on the M875.

Partner certificates (*.cer, *.crt, *.pem)

At this point, all the loaded remote certificates are displayed in a list.

By clicking the "Delete" button, you can remove certificates that are no longer required.

Device certificates (.p12)

At this point, the name and status of the loaded PKCS12 file are displayed.

- A white check mark on a green dot shows that the relevant part of the certificate file exists.
- A white cross on a red dot indicates that the relevant part is missing.

If you click the "Delete" button, the current PKCS12 file is deleted from the M875.

4.7.5 Supervision of the VPN connections

With the "Supervision" function, the M875 checks established VPN connections. To do this, the M875 sends ping packets (ICMP) to one or more remote stations (target hosts) at regular intervals via the VPN connection. This takes place independently of the user data.

If the M875 receives a reply to a ping from at least one of the addressed remote stations, the VPN connection is still functioning.

If none of the remote stations replies to the ping, the ping is repeated after a selectable delay. If all the repetitions are unsuccessful, the VPN client on the M875 is restarted. This leads to re-establishment of all existing VPN connections.

The settings the supervision apply to all VPN connections.

Note

Send the ping packets directly to the internal interface of the VPN gateway and not to a host downstream from the gateway. If this host is not reachable, the tunnel supervision responds.

Calling the Web page

Select "IPsec VPN" > "Monitoring" in the navigation panel.

The screenshot shows the 'IPsec VPN - Monitoring' configuration page. The left navigation menu includes: Overview, System, Local Network, External Network, Security, IPsec VPN (expanded), Connections, Certificates, Monitoring, Advanced, Status, Remote access, SMS, SNMP, and Maintenance. The main configuration area has the following settings:

- Use VPN monitoring: Yes
- Interval for connection checks (minutes): 5
- Waiting time before repetition (minutes): 1
- Number of unsuccessful connection checks up to restarting the VPN client: 3

Below these settings is a table titled 'List of destination hosts' with columns for 'Name of the tunnel', 'IP address of the host', and 'IP address of the client'. A 'New' button is next to the 'IP address of the client' column. The table contains one entry:

Name of the tunnel	IP address of the host	IP address of the client
---	192.168.2.1	192.168.1.1

Buttons for 'Save' and 'Reset' are located below the table. A 'Delete' button is also present next to the client IP address in the table row.

Use VPN monitoring

Note

Increased costs due to extra data traffic

Sending ping packets increases the data traffic. This may result in additional costs, depending on your user agreement with the mobile wireless provider.

- Yes: VPN supervision is enabled.
- No: VPN supervision is disabled.

If you select "Yes", the following entries appear on the page.

Interval for connection check (minutes)

Specify the interval at which ping packets are sent via the supervised VPN connections (VPN tunnel).

Enter the interval in minutes.

Waiting time before repetition

Specify the wait time after which the check is repeated following an unsuccessful ping check (no reply to the ping).

Enter the waiting time in the input box in minutes.

Number of unsuccessful connection checks up to restarting the VPN client

Specify how often the ping check is made before the VPN client is restarted on the M875.

Enter the number of checks in the input box.

List of the destination hosts

In the "List of destination hosts" area, specify which of your VPN connections will be supervised according to the pattern set above.

Click the "New" button to specify the supervision for a specific VPN connection.

- **Tunnel name**

From the drop-down list, select the VPN connection (VPN tunnel) to be monitored.

- **IP address of the host**

Enter the IP address of the destination host in this box.

- **IP address of the client**

In this box enter any unused IP address from the local network range of the relevant VPN connection as the sender IP.

If you click the "Delete" button, this VPN connection is taken out of the supervision.

Factory settings

Use VPN monitoring:	No
Connection check interval (Minutes):	5
Waiting time before repetition:	1
Number of unsuccessful connection checks up to restarting the VPN client:	3
Tunnel name:	-
IP address of the host:	192.168.2.1
IP address of the client:	192.168.1.1

4.7.6 Advanced settings

Calling the Web page

Select "IPsec VPN" > "Advanced" in the navigation panel.

The screenshot shows the Siemens SCALANCE M875 web interface. The top header displays the Siemens logo and the device name 'SCALANCE M875'. A language dropdown menu is set to 'English' with a 'Go' button. The left navigation panel is expanded to 'IPsec VPN', with sub-items: Connections, Certificates, Monitoring, Advanced, and Status. The main content area is titled 'IPsec VPN - Advanced settings' and contains the following configuration table:

Keepalive interval for NAT-T (seconds)	<input type="text" value="60"/>
Phase 1 timeout (seconds)	<input type="text" value="15"/>
Phase 2 timeout (seconds)	<input type="text" value="10"/>
Maximum number of connection establishment attempts up to restarting the VPN client	<input type="text" value="5"/>
Maximum number of connection establishment attempts after restarting the VPN client until the next device restart	<input type="text" value="2"/>
DynDNS tracking	<input type="text" value="No"/>
Restart of the VPN clients with DPD	<input type="text" value="No"/>

At the bottom of the configuration area, there are 'Save' and 'Reset' buttons.

Keepalive interval for NAT-T (seconds)

If the NAT-T function is enabled, keepalive frames are sent periodically by the M875 through the VPN connection. This prevents a NAT router between the M875 and the remote station from interrupting the connection during idle times with no data traffic.

Enter an interval in seconds in this input box at which the keepalive frames are sent.

Phase 1 timeout (seconds)

With this setting, you specify how long the M875 waits until an authentication method of the ISAKMP-SA is completed. If there is a timeout, the authentication method is aborted and restarted.

Enter a length of time in seconds.

Phase 2 timeout (seconds)

With this setting, you specify how long the M875 waits until an authentication method of the IPsec SA is completed. If there is a timeout, the authentication method is aborted and restarted.

Enter a length of time in seconds.

Maximum number of connection establishment attempts up to restarting the VPN client

If a VPN connection establishment fails, the M875 automatically attempts to re-establish the connection. After the number of unsuccessful attempts specified here, the VPN client is restarted by the M875. Following this, the M875 initiates the VPN connection establishment again.

In this box, enter the number of unsuccessful attempts before the M875 restarts its VPN client.

Maximum number of connection establishment attempts after restarting the VPN client until the next device restart

If the VPN connection establishment continues to be unsuccessful even following the restart of the VPN client, the M875 is also automatically restarted and then initiates connection establishment again.

In this box, enter the number of renewed VPN connection attempts following a restart of the VPN client before the M875 is restarted.

DynDNS tracking

With DNS tracking, the M875 checks regularly whether or not the VPN gateway of the remote station is still reachable. Enable this function in particular when the VPN gateway of the remote station obtains the IP address from a DynDNS service and when in addition to this, no Dead Peer Detection is used.

Select one of the two options:

- Yes: The DynDNS tracking function is enabled.
- No: The DynDNS tracking function is not enabled.

If you have selected "Yes", the following entry appears.

Interval for DynDNS tracking (minutes)

Specify an interval at which there is a check to find out whether the remote station is still reachable.

Enter a length of time in minutes.

Restart of the VPN client with DPD

If the M875 does not receive any reply to its DPD queries from the remote station, the IPsec connection is considered to be interrupted after a number of permitted unsuccessful attempts. You can specify whether or not the M875 is rebooted in such a situation.

Remember that if you reboot, not only the failed connection but all existing VPN connections will be interrupted.

Select one of the two options:

- Yes: The device is restarted as soon as DPD is detected.
- No: The device is not restarted following DPD.

Factory settings

Keepalive interval for NAT-T (seconds):	60
Phase 1 timeout (seconds):	15
Phase 2 timeout (seconds):	10
Maximum number of connection establishment attempts up to restarting the VPN client:	5
Maximum number of connection establishment attempts after restarting the VPN client until the next device restart:	2
DynDNS tracking:	No
Interval for DynDNS tracking (minutes):	5
Restart of the VPN client with DPD:	No

4.7.7 Status

The status of the active VPN connections is displayed on the "IPsec VPN - Status" page. Here, you also have the option of loading a protocol file on the Admin PC.

Calling the Web page

Select "IPsec VPN" > "Status" in the navigation panel.

List of active VPN connections

Below this entry, the active VPN connections are listed with their names, remote station and their security relations ISAKMP and IPsec.



The security relation is successfully established.



The security relation is not established.

Number of VPN connection attempts (24 h)

This entry shows how often in the last 24 hours there was an attempt to establish a VPN connection.

Download VPN protocol

Information about establishing and terminating VPN connections is logged in a log file. To access this information, follow these steps:

1. Click the "Download" button.
A dialog for opening and saving files opens.
2. Follow the instructions in the dialog to save the log file with the VPN protocol on the Admin PC.

4.8 Remote access

4.8.1 Changing the password

Access to the M875 is protected by a password. This password protects the following access routes:

- Via the local interface to the Web user interface and the SSH console.
- Via the mobile wireless connection with HTTPS to the Web user interface.

NOTICE
Change the factory set password immediately
Change the factory set password immediately after commissioning. This password is public knowledge and does not provide adequate protection.

Changing the password

To change the access password, follow the steps below:

1. In the navigation panel, select "Remote Access"> "Password".
2. Enter a new password in the "New access password" input box.
3. Enter the new password again in the "Repeat new access password" input box.
4. Confirm your entry by clicking the "Save" button.
The message "Password changed" appears.
5. Confirm this message by clicking the "OK" button.
A dialog appears that prompts you to log on again.
6. Enter the user name "admin" and your newly specified password.
7. Save your entry by clicking the "OK" button.

Factory settings

User name: admin (cannot be modified)
Password: scalance

4.8.2 HTTPS

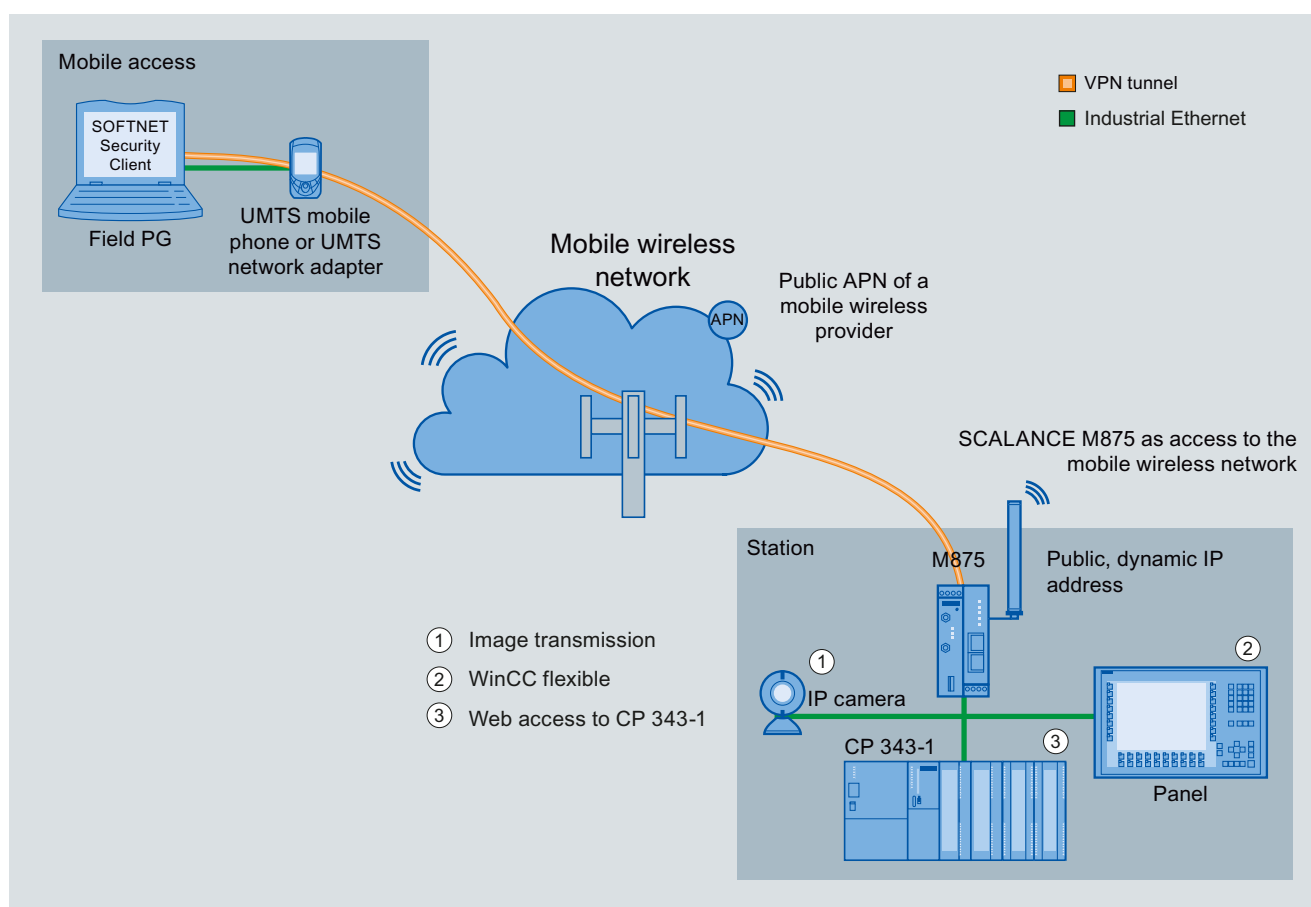


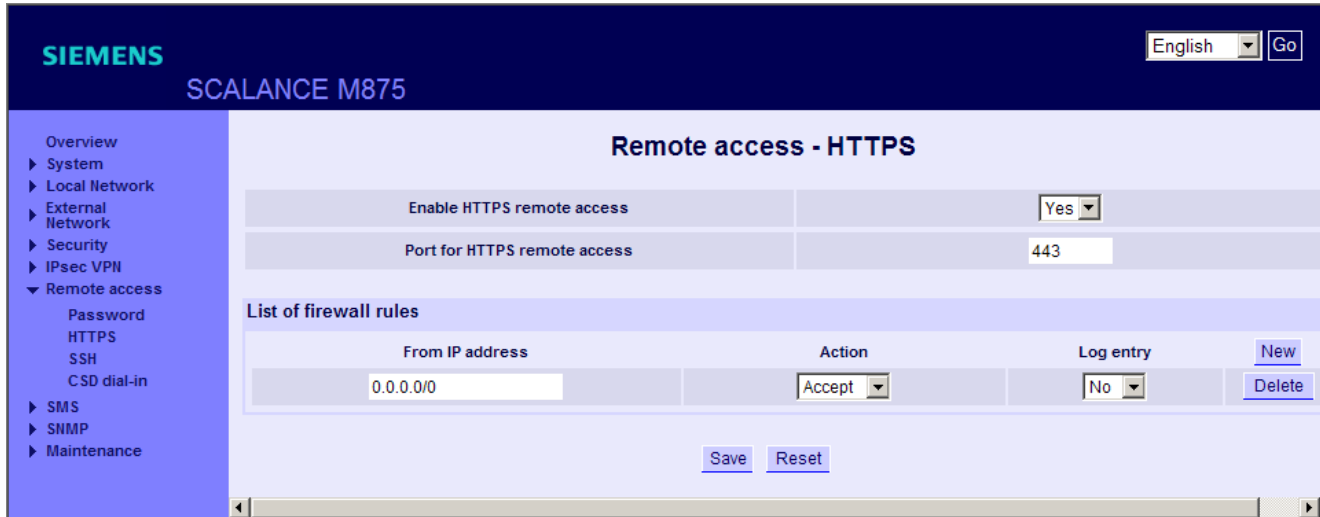
Figure 4-9 Configuration with HTTPS access

HTTPS remote access provides access to the Web user interface of the M875 via a mobile wireless connection.

The remote access via HTTPS (Secure HyperText Transfer Protocol) allows secure access from an external network to the Web user interface of the M875. To be able to use this option, it must first be enabled as described below. You can then configure the M875 via the HTTPS remote access in exactly the same way as with the Web browser as described in the section Local Network (Page 49).

Calling the Web page

In the navigation panel, select "Remote Access"> "HTTPS".



Enable HTTPS remote access

Specify whether or not remote access using HTTPS will be enabled. Select one of the following two options from the drop-down list:

- Yes: Access to the Web user interface of the M875 from the external network using HTTPS is allowed.
- No: Access to the Web user interface of the M875 from the external network using HTTPS is not allowed.

The factory setting is "No".

HTTPS remote access port

In the factory settings, the standard port 443 is specified.

You can change the port number in the input box. Remember, however, that the external partner accessing remotely must then specify the port number after the IP address in the address information.

Example: If the M875 can be reached via the Internet at the IP address 192.144.112.5, and when in addition to this port number 442 was specified, the following information must be specified for the remote station in the Web browser:

- `https://192.144.112.5:442`

Note

The standard port for HTTPS access remains open along with the newly selected port.

Firewall rules

To create a new firewall rule for the HTTPS remote access, click the "New" button.

To remove an existing rule, click the "Delete" button.

Save your settings by clicking the "Save" button.

- **From IP address**

Enter the IP address of the computer that is permitted remote access in the input box.

The factory setting is "0.0.0.0/0" and represents "all IP addresses".

To specify an address range, use the CIDR notation.

- **Action**

From the drop-down-list, select one of the following actions that specifies what happens when the specified HTTPS port is accessed.

- Allow: The IP packets are allowed to pass through.
- Reject: The IP packets are rejected, and the sender receives a corresponding message.
- Discard: The data packets are deleted without any notification to the sender.

- **Log entry**

For each firewall rule, specify whether an event will be logged in the firewall log if the rule is put into effect.

Select the relevant option from the drop-down list.

For more detailed information, refer to the section Firewall Log (Page 84).

- No: No log entry
- Yes: Log entry

Factory settings

Enable HTTPS remote access: No (turned off)

HTTPS remote access port: 443

Firewall rules

From IP address: 0.0.0.0/0

Action: Allow

Log: No (turned off)

4.8.3 CSD

CSD (Circuit Switched Data) is not supported.

4.9 SMS

4.9.1 Service Center (SMSC)

The M875 also uses the Short Message Service (SMS) of GSM. For the SMS function to work reliably, you will need to specify a certain service center of your mobile wireless provider, depending on your contract. To do this, enter a suitable call number on the Web user interface of the M875. You obtain this call number from your mobile wireless provider.

If you do not enter a call number, the standard service center of your mobile wireless provider is used automatically.

Calling the Web page

In the navigation panel, select "SMS"> "Service Center (SMSC)".

Call number of the SMSC

Enter the call number of the preferred SMS service center in the input box.

4.9.2 Alarm SMS

The M875 can send short alarm messages using SMS. The sending of an alarm SMS message can be triggered by two events:

- Event 1: The in port is set.
- Event 2: There is no UMTS/GPRS connection.

For both events, a separate call number is specified to which the alarm message is sent. You can enter any text as the alarm message.

Calling the Web page

In the navigation panel, select "SMS"> "Alarm SMS".

Alarm SMS for event 1: in port becomes active

If an adequate switching voltage is applied to the in port, the requirement for event 1 is met.

This means that, for example a local application connected to the in port can trigger an alarm message by SMS outside the IP data connection.

Alarm SMS for event 2: No GPRS connection

If the mobile wireless connection cannot be established despite multiple attempts, the requirement for event 2 is met. If the alarm SMS function is enabled, an SMS message is sent.

Activate

Select one of the two options from the drop-down list:

- Yes: The function is enabled.
- No: The function is not enabled.

Call number

In the input box, enter the call number of the end device to which the alarm message will be sent using SMS.

The end device must support receipt of SMS messages via GSM or fixed network.

Message text

In the input box, enter the text that will be sent as an alarm message.

Factory settings

Alarm SMS for event 1: in port becomes active:	No (turned off)
Call number:	-
Message text:	-
Alarm SMS for event 2: No GPRS connection:	No (turned off)
Call number:	-
Message text:	-

4.9.3 Sending SMS over IP messages from the local area network

With the SMS messaging function, applications connected to the local interface of the M875 can send SMS messages via the GSM network. To do this, the local application needs to establish a TCP/IP connection to the M875.

The local application sends the message text in a specific frame format to the M875 via this TCP/IP connection. The M875 packs the message text in an SMS format and sends the SMS via the GSM network.

Frame format for the SMS message

The message sent by the local application must conform with the following frame format:

Username#Password#CommandCode#Seq-Num;Callnumber;Message:

Example: `User#password#105#01;0049043465789;my SMS text:`

- **User name**

The user name must match the user name specified for this function, see below "Description of the user interface".

- **Password**

The password must match the password specified for this function, see below "Description of the user interface".

- **CommandCode**

This part of the frame, is the command to send an SMS message from the local network. This value of 105 is specified and must not be modified.

- **Seq-Num**

The frame section "Seq-Num" is the sequence number and is used to identify several simultaneous queries.

This function is not currently supported. For this reason, "01" must always be used.

- **Call number**

The call number of the SMS recipient can be a maximum of 40 characters long. International numbers (for example "+49" or "0049") are permitted.

- **Message**

The message text can be up to a maximum of 160 characters long. The following characters must not occur in the SMS text:

- # Separator for the first command level
- ; Separator for the second command level
- : Identifies the end of the message

Calling the Web page

In the navigation panel, select "SMS"> "SMS over IP".

The screenshot shows the 'SMS - SMS over IP' configuration page. The left navigation menu is expanded to 'SMS' > 'SMS over IP'. The main content area has the following elements:

- Enable sending of SMS from local network:** A drop-down menu set to 'Yes'.
- User name:** An input field containing 'User'.
- Password:** An input field containing 'Password'.
- Port number:** An input field containing '26864'.
- List of firewall rules:** A table with columns for 'From IP address (internal)', 'Action', and 'Log entry'. The first rule has '0.0.0.0/0' in the first column, 'Accept' in the second, and 'No' in the third. There are 'New' and 'Delete' buttons for each rule.
- Buttons:** 'Save' and 'Reset' buttons are located at the bottom of the configuration area.

Enable SMS messaging from the local network

Select one of the two options from the drop-down list:

- **Yes:** The function is enabled.
- **No:** The function is not enabled.

User name

In the input box, specify a user name that must be included in the frame, see above "Frame format".

Password

In the input box, specify a password that must be included in the frame, see above "Frame format".

Port number

In the input box, specify a TCP/IP port on which the M875 accepts the TCP/IP connection for sending SMS messages.

Firewall rules

To allow the TCP/IP connection to be established for sending SMS messages, a firewall rule must be set up on the M875. To do this, click the "new" button.

In the factory settings, the firewall rule for sending SMS messages is that all frames from the local network are allowed to pass.

- **From IP address (internal)**

This entry specifies the source for the TCP/IP connection for sending SMS messages.

In the input box, enter the IP address of the locally connected application that is allowed to send SMS commands to the M875.

To specify an address range, use the CIDR notation.

- **Action**

From the drop-down list, select one of the following actions that specifies how the frames of the nodes specified earlier in "From IP address (internal)" are handled via TCP/IP.

- Allow: The IP packets are allowed to pass through.
- Reject: The IP packets are rejected, and the sender receives a corresponding message.
- Discard: The data packets are deleted without any notification to the sender.

- **Log entry**

For each firewall rule, specify whether an event will be logged in the firewall log if the rule is put into effect.

Select the relevant option from the drop-down list.

For more detailed information, refer to the section Firewall Log (Page 84).

- No: No log entry
- Yes: Log entry

Factory settings

Enable sending of SMS from local network:	No (turned off)
User name:	User
Password:	Password
Port number:	26864
Firewall rules:	-
From IP address (internal):	0.0.0.0/0
Action:	Allow
Log entry:	No

Detailed application example

You will find a detailed description of an example with a SIMATIC S7 station on the pages of Siemens Automation Customer Support at the following address:

54361177 (<http://support.automation.siemens.com/WW/view/en/54361177>)

the example, the function is described based on the EDGE/GPRS router SINAUT MD741-1. You can transfer this information to the SCALANCE M875.

4.10 SNMP

4.10.1 Settings

SNMP parameters

SNMP (Simple Network Management Protocol) is a network protocol with which individual network subscribers as well as the M875 can be monitored and controlled from a management station. So-called agents are used for the individual network subscribers. These programs are capable of detecting the status of the subscriber, making settings or triggering actions. The management station can communicate with the individual agents via SNMP.

With this communication, the following parameters can be queried by the M875:

- Information for device identification
- IP address of the external network
- PIN of the SIM card
- MAC address
- Network provider
- APN
- IMSI
- IMEI
- CSQ value
- ID of the current wireless cell
- ID of the neighboring wireless cell
- Host name
- Maximum data volume
- 80% warning threshold of the maximum data volume
- Current monthly byte count
- Hardware ID
- Software version
- Firmware version

The following parameters can be modified on the M875 using SNMP:

- Maximum data volume
- Access password
- PIN of the SIM card
- Information for device identification

The M875 supports the version SNMPv2.

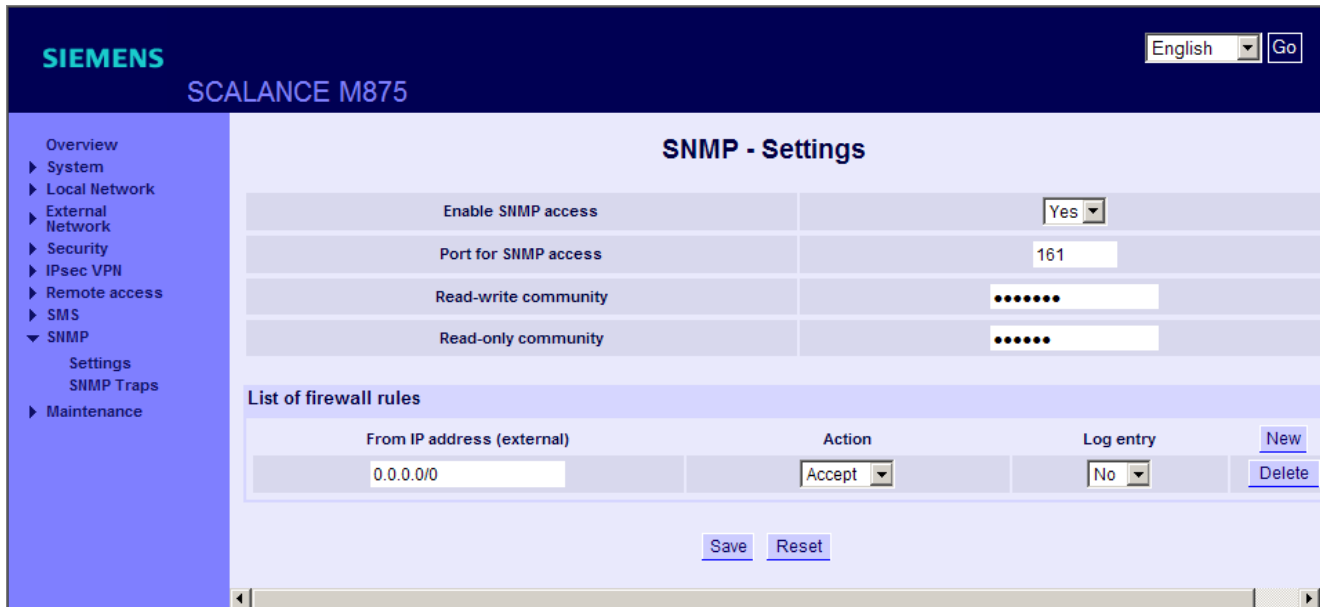
Note

SNMP only via VPN

The SNMP functionality can only be used via an existing VPN connection.

Calling the Web page

In the navigation panel, select "SNMP"> "Settings".



Enable SNMP access

Specify whether or not access via SNMP will be enabled.

- Yes: Access is via SNMP is enabled.
- No: Access is via SNMP is disabled.

Port for SNMP access

In the input box enter the number of the port via which SNMP access is enabled.

Read-write community

Specify a community string (password) for the SNMP access with read and write permissions.

Read-only community

Specify a community string (password) for SNMP access with read permissions.

Note

Change community strings (passwords)

Change the passwords set in the factory. The passwords are public knowledge and do not provide adequate protection.

Firewall rules

To allow the TCP/IP connection to be established for the SNMP access, a firewall rule must be set up on the M875. To do this, click the "new" button.

In the factory settings, the firewall rule for SNMP access is set so that all queries are allowed to pass.

- **From IP address (external)**

This entry specifies the source of the SNMP queries.

In the input box, enter the IP address of the application that is allowed to access the M875 via SNMP.

To specify an address range, use the CIDR notation.

- **Action**

From the drop-down list, select one of the following actions that specifies how SNMP queries from the nodes specified earlier under "From IP address (external)" are handled.

- **Allow:** The IP packets are allowed to pass through.
- **Reject:** The IP packets are rejected, and the sender receives a corresponding message.
- **Discard:** The data packets are deleted without any notification to the sender.

- **Log entry**

For each firewall rule, specify whether an event will be logged in the firewall log if the rule is put into effect.

Select the relevant option from the drop-down list.

For more detailed information, refer to the section Firewall Log (Page 84).

- **No:** No log entry
- **Yes:** Log entry

Factory settings

Enable SNMP access:	No (turned off)
Port for SNMP access:	161
Read-write community:	private
Read-only community:	public
Firewall rules:	No rules set.

Management using SIMATIC NET or SINEMA Server

The SIMATIC NET IE SNMP OPC server and the SINEMA Server provide convenient options for network management.

- **SIMATIC NET IE SNMP OPC server**

The SNMP OPC server software allows diagnostics and assignment of parameters for any SNMP device. The data exchange with these devices is handled by the OPC server using the SNMP protocol. All the information can be integrated in OPC-compatible systems, for example in the HMI system WinCC. This makes combined process and network diagnostics possible in the HMI system.

- **SINEMA server**

SINEMA Server automatically recognizes the devices in the network and detects the topology of the network. Information such as the device name, IP and MAC address, vendor, status and supported protocols are collected about the devices detected in the network.

SINEMA Server allows monitoring, maintenance and diagnostics of the devices in the network. Changes in operating states and errors or faults on the network are detected as an event and alarms are generated automatically for the detected events.

The collected device information, the detected topology, the alarms and network statistics are displayed using a Web browser and/or a browser integrated HMI/SCADA systems. The network statistics show the status of the devices in the network based on the events and device types.

Downloading MIB files

The MIB files for the M875 are available for downloading on the pages of Siemens Automation Customer Support at the following address:

55050627 (<http://support.automation.siemens.com/WW/view/en/55050627>)

4.10.2 SNMP traps

If certain events occur, the M875 can send alarm frames (traps) to the management station. For this, the M875 has six different event types available. Specify whether or not an alarm frame will be sent for each event type individually.

In addition to the events that can be set, the M875 automatically sends an alarm frame via SNMP if a VPN Tunnel is established or terminated.

Calling the Web page

In the navigation panel, select "SNMP"> "SNMP Traps".

The screenshot shows the configuration page for SNMP Traps on a Siemens SCALANCE M875 device. The interface includes a navigation menu on the left with options like Overview, System, Local Network, External Network, Security, IPsec VPN, Remote access, SMS, SNMP (selected), Settings, SNMP Traps, and Maintenance. The main content area is titled 'SNMP - SNMP Traps' and contains the following settings:

Enable SNMP Traps	Yes
Destination host	NONE
Destination port	162
Destination name	public
Destination community	public
Event: device sends keepalive frames	Yes
Keepalive interval (minutes)	600
Event: 80% of the max. data volume (bytes/month) reached	Yes
Event: 100% of the max. data volume (bytes/month) reached	Yes
Event: connection established	Yes
Event: change at the IIN port	Yes
Event: change to a configuration profile	Yes

At the bottom of the configuration area, there are 'Save' and 'Reset' buttons.

Enable SNMP traps

Specify whether alarm frames will be sent for selected events.

- Yes: Alarm frames are sent.
- No: Alarm frames are not sent.

Destination host

Enter the IP address of the management station to which the alarm frames will be sent.

Destination port

Enter the port number of the target host in the input box.

Destination name

If necessary, enter the name of the frame recipient. Otherwise, you can retain the name from the factory settings.

Destination community

If necessary, enter the target community of the frame recipient. Otherwise, you can retain the community from the factory settings.

Event: device sends keepalive frames

The M875 can send keepalive frames periodically. In the next input box "Keepalive interval (minutes)", you can specify the interval for sending the keepalive frames.

Here, you specify whether the M875 sends an alarm frame to the management station when a keepalive frame is sent. Select one of the two options from the drop-down list:

- Yes: Alarm frame is sent if the event occurs.
- No: No alarm frame is sent.

Keepalive interval (minutes)

In this input box, enter an interval in minutes at which the keepalive frames are sent.

Event: 80% of the max. data volume (bytes/month) reached

Specify whether or not an alarm frame will be sent when 80 % of the specified maximum traffic volume per month has been reached, see also section Traffic volume supervision (Page 65). Select one of the two options from the drop-down list:

- Yes: Alarm frame is sent if the event occurs.
- No: No alarm frame is sent.

Event: 100% of the max. data volume (bytes/month) reached

Specify whether or not an alarm frame will be sent to the management station if the specified maximum traffic volume per month has been reached. Select one of the two options from the drop-down list:

- Yes: Alarm frame is sent if the event occurs.
- No: No alarm frame is sent.

Event: connection established

Specify whether or not an alarm frame will be sent to the management station when the M875 establishes or terminates a connection to the mobile wireless network. Select one of the two options from the drop-down list:

- Yes: Alarm frame is sent if the event occurs.
- No: No alarm frame is sent.

Event: Change at the in port

Specify whether an alarm frame will be sent if there is a change at the in port. Select one of the two options from the drop-down list:

- Yes: Alarm frame is sent if the event occurs.
- No: No alarm frame is sent.

Event: change to a configuration profile

Specify whether an alarm frame will be sent if the configuration of the M875 has been changed. Select one of the two options from the drop-down list:

- Yes: Alarm frame is sent if the event occurs.
- No: No alarm frame is sent.

Factory settings

Enable SNMP traps:	No (turned off)
Destination host:	0.0.0.0
Destination port:	162
Destination name:	public
Destination community:	public
Event: Device sends keepalive frames:	No (turned off)
Keepalive interval (minutes)	600
Event: 80% of the max. data volume reached:	No (turned off)
Event: 100% of the max. data volume reached:	No (turned off)
Event: connection established	No (turned off)
Event: Change at the in port	No (turned off)
Event: change to a configuration profile	No (turned off)

Maintenance and diagnostics

5.1 Calling the Maintenance Web pages

The Web pages of the M875 are available for maintenance and diagnostics purposes. You will find information about the requirements and calling the Web pages from an admin PC in the section Settings on the admin PC (Page 33).

The individual functions are described in the following sections.

5.2 Updating the firmware

With the update function, you can update the firmware version for the M875.

After loading the relevant files on the M875, the new firmware is unpacked. This process can take several minutes. The actual update then begins, which is indicated by the LEDs lighting up in sequence. After the update, the device automatically reboots.

The settings of the M875 are retained assuming that the settings still have the same effect in the new firmware as they did before the update.

Note

Do not make any settings during the update

In the time between unpacking the firmware and the actual update through to the rebooting of the device, the Administration user interface is not blocked. During this time, do not make any settings in the user interface otherwise you cannot be certain that these settings will be adopted correctly.

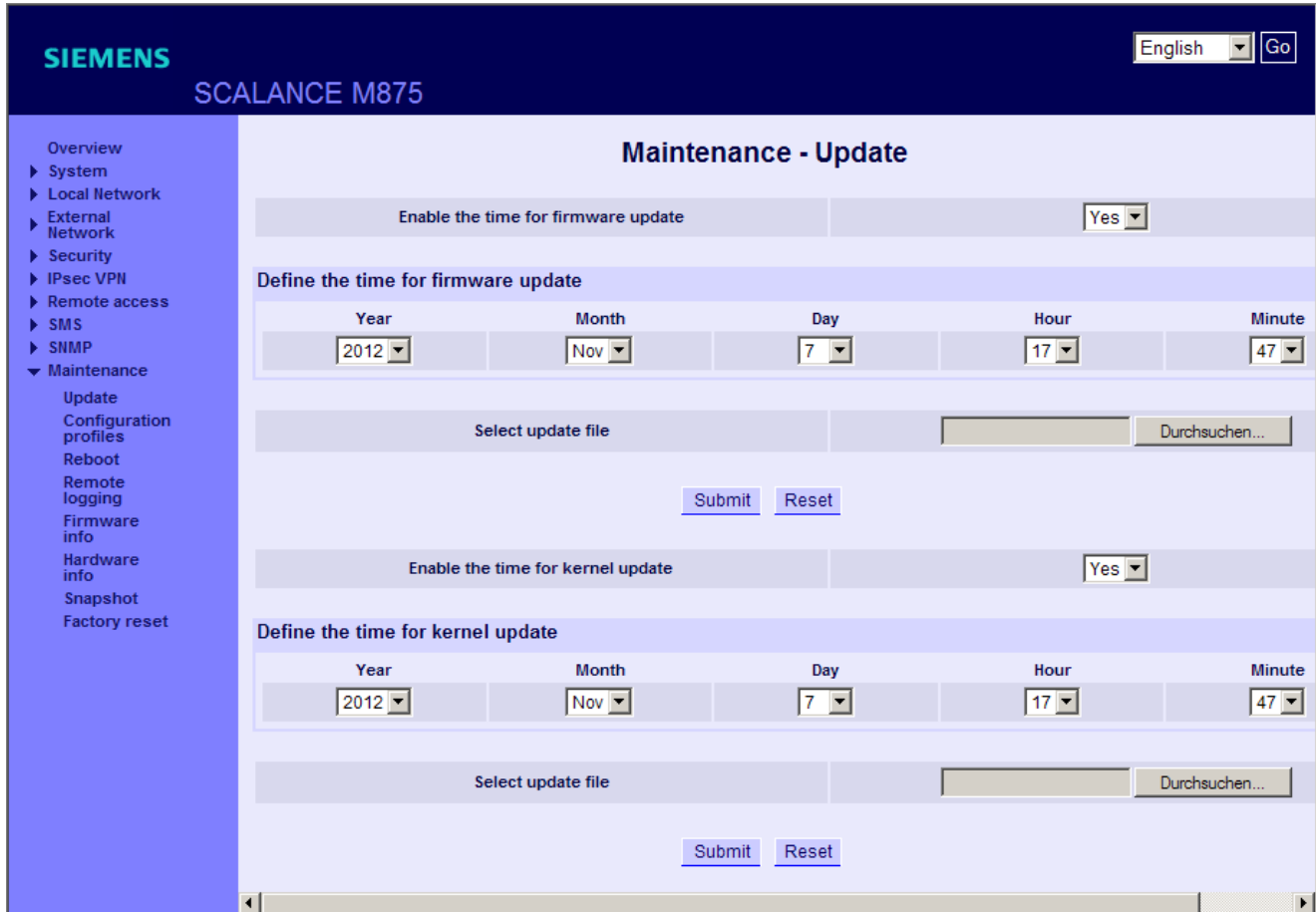
Do not turn the device off

Do not turn off the device during the update.

There is an option with which the update can be performed automatically at a specified time. To use this, you must first load the new firmware on the device as described below.

Calling the Web page

In the navigation panel, select "Maintenance" > "Update".



Define the update time

Select one of the following options from the drop-down list:

- Yes: The update of the new firmware is time-driven and takes place at the time specified below. The firmware must first be loaded, see below "Selecting the update file".
- No: The firmware is updated after you have loaded the relevant firmware files and clicked the "Submit" button.

Defining the firmware update time

Enter the date and time for the time-driven update.

Selecting the firmware update file

To reduce the data volume required to update the firmware, the firmware files for the M875 are tailored exactly to the specific update step. If, for example, you update the firmware from version 2.0 to 2.1, select the relevant firmware file "M875_v2.0-v2.1.tgz".

Follow the steps below to load a new firmware version on the M875:

1. Click the "Browse..." button.
A dialog opens.
2. Select the relevant firmware file, for example "M875_v2.0-v2.1.tgz".
3. Click the "Open" button in the dialog.
The dialog closes and the path information appears in the input box.

"Submit" button

Click the "Submit" button.

Depending on the setting, the firmware is updated immediately or at the specified time.

Following the update, the device reboots automatically.

Note

Check the update

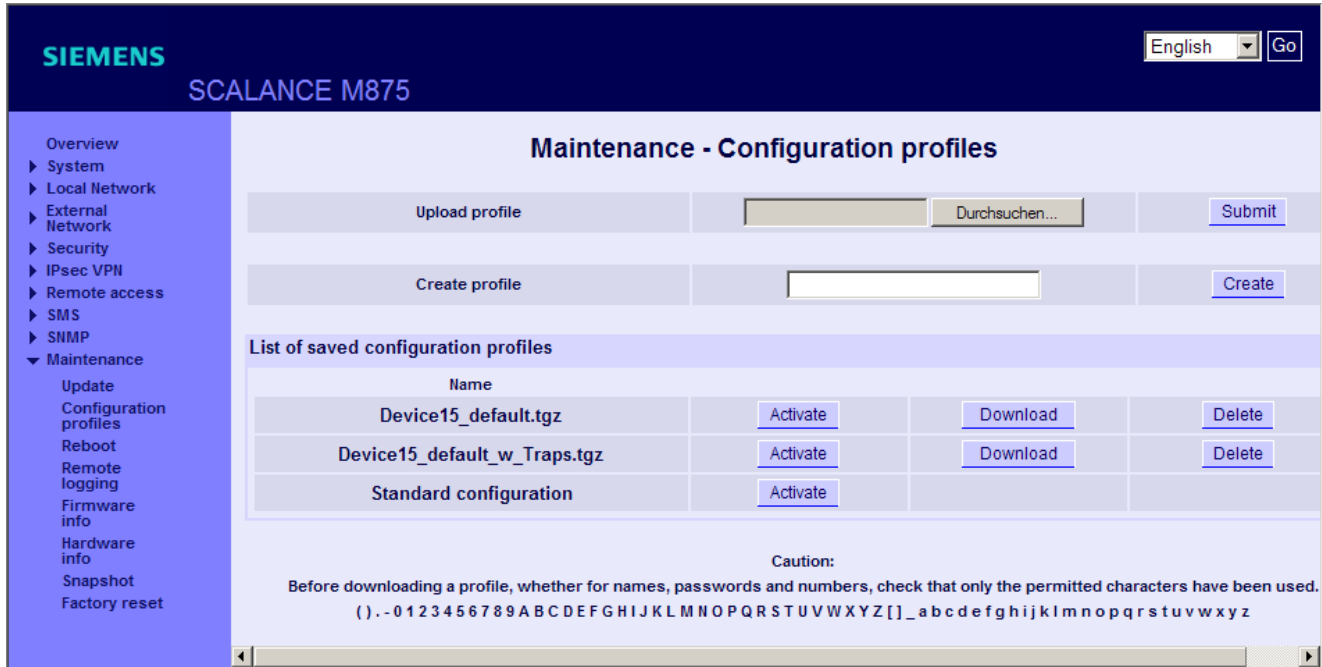
After rebooting, open the "Status" starting page and check whether the current firmware version was successfully installed in "Current system version".

5.3 Configuration profiles

You can save your settings on the M875 in profile files. These profiles can, when necessary, be reloaded or transferred to other devices of the same type. Note that the PIN of the SIM card is not stored in the configuration profile.

Calling the Web page

In the navigation panel, select "Maintenance" > "Configuration profiles".



Upload Profile

With this function, a configuration profile that was created previously and saved on the Admin PC is uploaded to the M875. Files with configuration profiles have the file extension "tgz".

1. Click the "Browse" button to search for configuration profiles on the Admin PC. The "Upload File" dialog opens.
2. Select the required configuration file with the extension "tgz" by double clicking on it. The path of the configuration file is displayed in the input box.
3. Click the "Submit" button to load the profile on the M875. The configuration profile is displayed in the "List of saved configuration profiles" further down on the page.

The uploaded profile is not yet used. Before the device works with this profile, you still need to activate it in the list, see below.

Create profile

With this function, you create a new profile with the current settings of the M875.

1. Enter a name for the profile in the input box.
2. Click the "Create" button. The new configuration profile is displayed in the "List of saved configuration profiles".

List of saved configuration profiles

This list displays all the configuration profiles stored on the M875. The three buttons next to the profiles have the following functions:

- **"Activate" button**

The M875 adopts the settings from the selected configuration profile and continues to work with it.

- **"Download" button**

Dialog for saving the configuration profile of the M875 on the Admin PC.

- **"Delete" button**

The configuration profile is deleted.

- **Default configuration**

The "Standard configuration" profile contains the factory settings. The profile cannot be saved or deleted.

Resetting to the default configuration

NOTICE
Deleting data Note the following effects before you reset the device to the default configuration: <ul style="list-style-type: none">• All the configuration data that was entered is deleted. This also includes user names and access passwords.• The PIN of the SIM card is deleted in the configuration data.• The device loads the factory settings and runs a restart. This may take several minutes.
Reachability of the device The device can once again be reached at the IP address 192.168.1.1 that was set in the factory.
Data not deleted <ul style="list-style-type: none">• Created configuration profiles are retained.• Loaded certificates are retained.• Log files are retained.

Procedure

1. In the "List of saved configuration profiles" table, click the "Activate" button in the "Standard configuration" row.
2. Change the factory set password, see section Changing the password (Page 112).
3. Enter the PIN of the SIM card again, see section UMTS/EDGE - access parameters (Page 58).

Note

If you reset the device to its factory settings in the Web user interface or using the SET button, all created configuration profiles, certificates and log files are deleted. For information on this, refer to section Factory settings (Page 139).

5.4 Reboot

Although the M875 is designed for permanent operation, disturbances are possible in such a complex system. Disturbances are normally triggered by external influences. A reboot can rectify such problems.

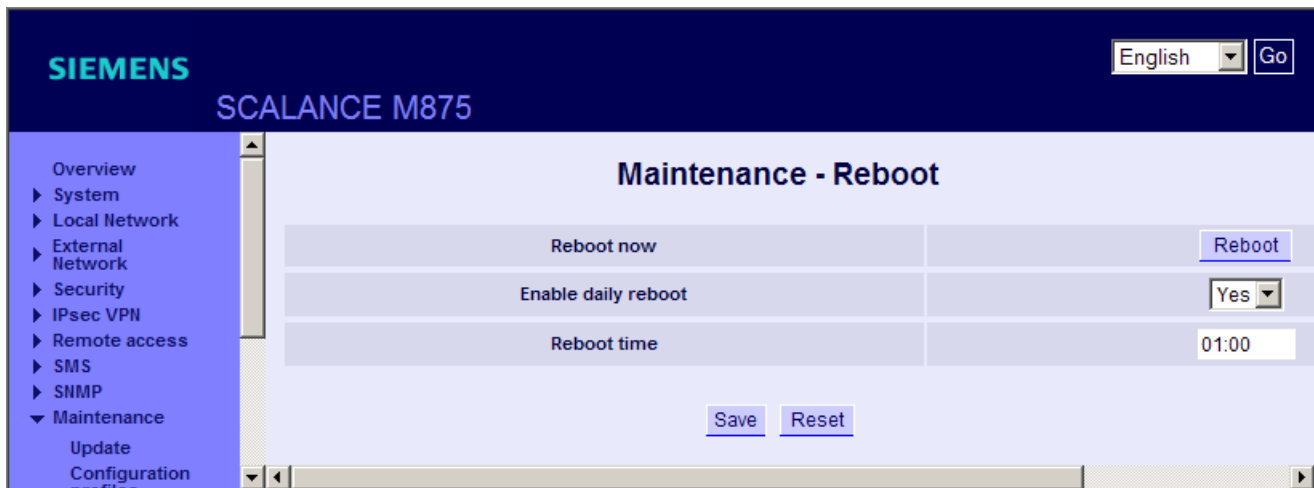
When rebooting, existing connections are interrupted.

The settings from the current configuration profile do not change. The M875 continues to work using these settings after the reboot.

You can set the M875 so that the device reboots automatically once a day at a particular time.

Calling the Web page

In the navigation panel, select "Maintenance" > "Reboot".



Reboot now

If you click the "Reboot" button, the device reboots immediately.

Enable daily reboot

Select the following from the drop-down list:

- Yes: The M875 reboots once daily at the time shown below.
- No: No daily reboot.

Reboot time

In the input box, enter a time in 24 hour format for the daily reboot.

Factory settings

Enable daily reboot:	No
Reboot time:	01:00

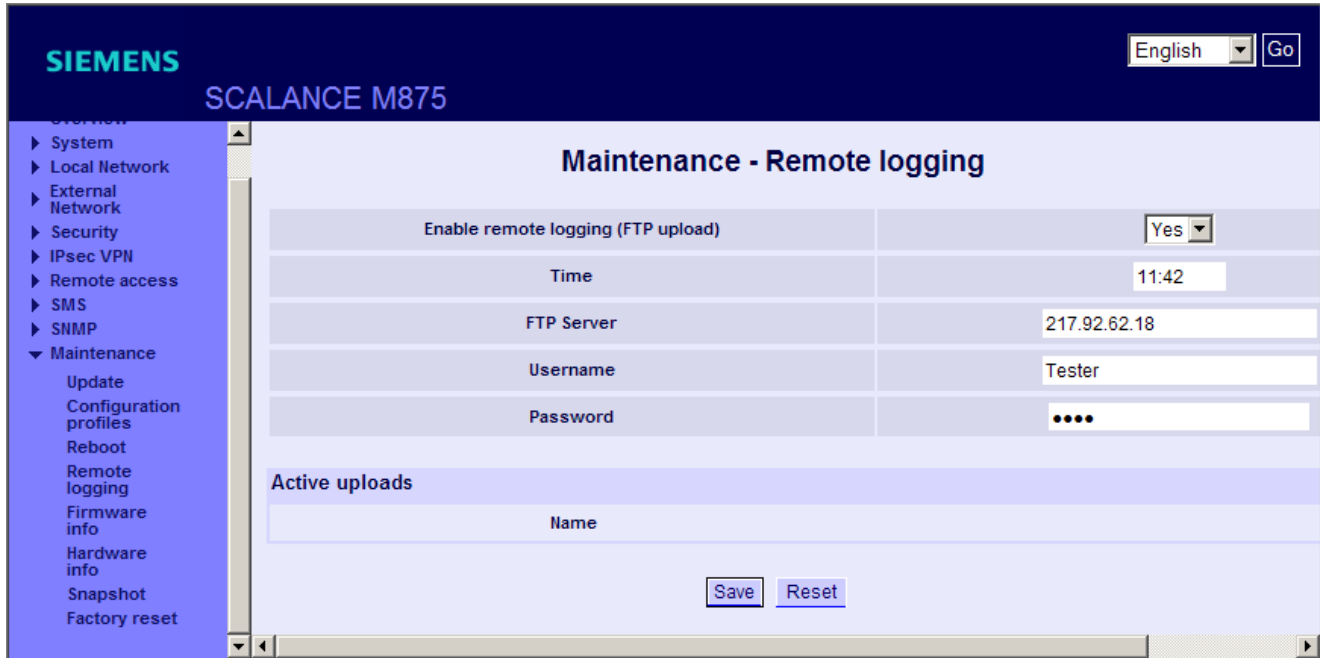
5.5 Remote logging

The M875 can automatically transfer the system log once a day using the File Transfer Protocol (FTP) to an FTP server. The current system log and the archived log files are transferred.

After successful transfer, the logs are deleted on the M875. If the transfer fails, the M875 tries once again to transfer the log files after 24 hours. Log files that have not yet been transferred are displayed under "Active uploads".

Calling the Web page

In the navigation panel, select "Maintenance" > "Remote Logging".



Enable remote logging (FTP upload)

Specify whether or not the function will be used. Select one of the following two options from the drop-down list:

- Yes: The function is enabled.
- No: The function is disabled.

Time of day

Enter a time in 24 hour format at which the logs will be transferred.

FTP Server

Specifies an FTP server, to which the log files will be transferred. The address can be specified as a host name, e.g. ftp.server.de, or as an IP address.

User name

Specify a user name for logging on at the FTP server.

Password

Specify a password for logging on at the FTP server.

Active uploads

Here, the log files are displayed that will be transferred to the FTP server in the next cycle.

Factory settings

Enable remote logging (FTP upload):	No (turned off)
Time:	00:00
FTP server:	NONE
User name:	guest
Password:	guest

5.6 Firmware information

With "Maintenance" > "Firmware info" in the navigation panel, you open the "Firmware information" page:

The screenshot displays the 'Maintenance - Firmware Information' page for a Siemens SCALANCE M875 device. The page is organized into several sections:

- Current firmware version:** 2.112
- Control application:** 2.042
- Mobile handler:** 2.032
- CGI applications:** 2.034
- German Web pages:** 2.033
- English Web pages:** 2.033
- SNMP MIB:** 1.005
- Kernel version:** Linux 2.6.35.3-dnt-0.53.872 #1 Thu Aug 9 11:04:57 CEST 2012 armv5tej1

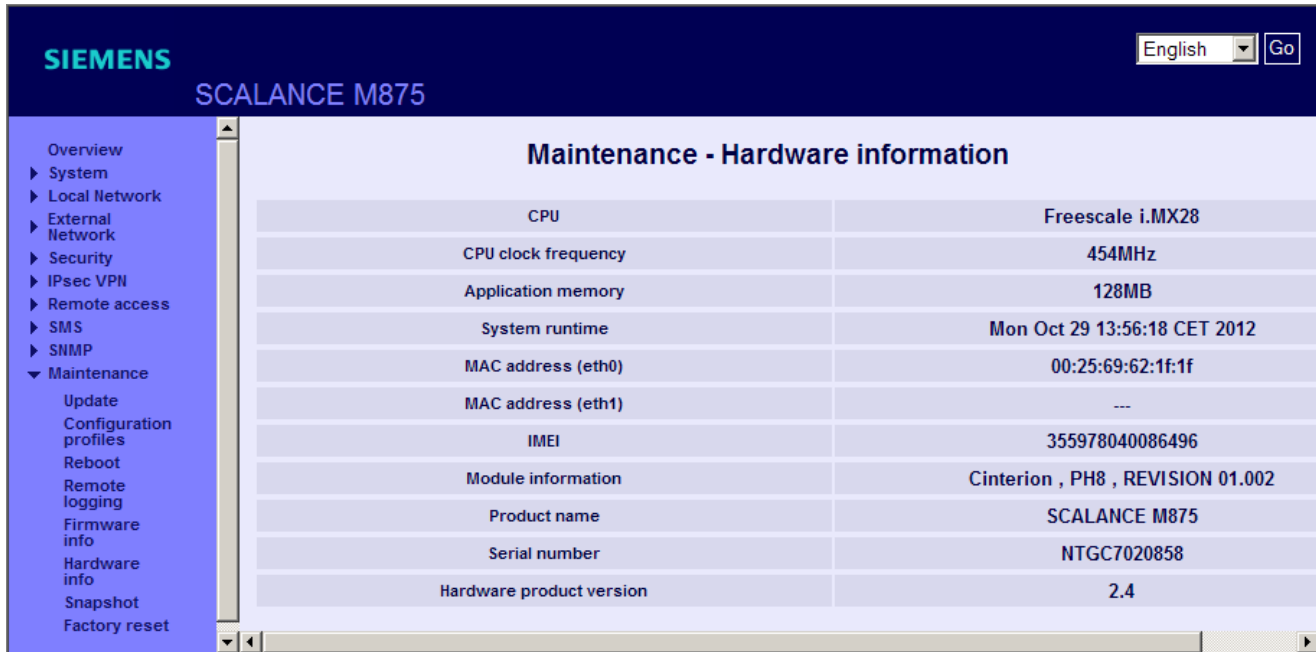
Below the current versions, there are two sections for scheduled updates:

- List of scheduled firmware updates:** A table with columns for Update Id, From version -> to version, and Timestamp.
- List of scheduled kernel update:** A table with columns for Version and Timestamp.

You will find information about the "Scheduled updates" entry in the section "Updating the firmware (Page 129)".

5.7 Hardware Info

With "Maintenance" > "Hardware info" in the navigation panel, you open the "Hardware information" page:



5.8 Snapshot

This snapshot function is used for support purposes.

The service snapshot saves important log files and current device settings in a file that can be used for fault diagnostics. If you have a problem with the M875 and contact our hotline, they may well ask you for the snapshot file.

Note

The snapshot file contains the access parameters for the mobile wireless network and the addresses of the remote station. It does not contain the user name and password for access to the M875.

Calling the Web page

In the navigation panel, select "Maintenance" > "Snapshot".

Load snapshot file on PC

If you click the "Download" button, a dialog opens in which you can open or save the snapshot files. Follow the on-screen instructions.

Advanced diagnostics (requires restart)

Note

Only activate this function after being requested to do so by the hotline

Only enable "Advanced diagnostics" if asked to do so by the hotline. When advanced diagnostics is active, frequent write access to the non-volatile memory of the M875 can lead to a reduced service life.

If advanced diagnostics is enabled, the log information is written to the logs more often. Additional information is also saved. This is useful for systematic troubleshooting.

5.9 Factory settings

Alternative options for resetting to factory settings

There are two different ways of resetting the M875 to its factory settings:

- Menu command "Maintenance" > "Factory reset"
- By pressing the service button "SET"

Effects of resetting to factory settings

NOTICE

Deleting data

Note the following effects before you reset the device to the factory settings:

- The device is reset to the factory settings and runs a restart.
This may take several minutes.
- All the configuration data that was entered is deleted.
This also includes user names and access passwords.
- The PIN of the SIM card is deleted in the configuration data.
- Created configuration profiles are deleted.
- Loaded certificates are deleted.
- Log files are deleted.

Reachability of the device

The device can once again be reached at the IP address 192.168.1.1 that was set in the factory.

Note

Save configuration profiles externally first

If you do not want to discard the entire data you have entered, you can save this in a configuration profile, store it externally and load it again after resetting to factory settings. For information on this, refer to section Configuration profiles (Page 131).

As an alternative: Resetting to the default configuration

If you do not want to delete created configuration profiles, certificates and log files, instead of resetting to factory settings, you also have the alternative of resetting the device to the standard configuration. For information on this, refer to section Configuration profiles (Page 131).

Resetting with the "Maintenance" > "Factory reset" Web page

Follow the steps outlined below:

1. In the navigation panel, select "Maintenance" > "Factory Reset".
2. Click the "Reset" button.
3. Restart the application.
4. Change the factory set password, see section Changing the password (Page 112).
5. Enter the PIN of the SIM card again, see section UMTS/EDGE - access parameters (Page 58).

Reset using the "SET" service button

Follow the steps outlined below:

1. Press the SET button with a thin object, for example a straightened paper clip.
2. Hold down the button for longer than 5 seconds.
3. Restart the application.
4. Change the factory set password, see section Changing the password (Page 112).
5. Enter the PIN of the SIM card again, see section UMTS/EDGE - access parameters (Page 58).

Technical specifications

Technical specifications	
Attachment to Industrial Ethernet	
Interface X2 for local applications	Number of ports: 2 (X2P1 and X2P2) Implementation: RJ-45 jack Characteristics: 10/100BASE-T, Ethernet IEEE 802, 10/100 Mbps; autocrossover; autonegotiation
Service interface	
Interface X1	Reserved (no function)
Electrical data	
Power supply	Power supply: 24 VDC Permitted range: 12 ... 30 V Implementation: 4-pin terminal strip, not floating
Power consumption (typical)	<ul style="list-style-type: none"> • at 12 V: 4.4 W • at 24 V: 4.0 W • at 30 V: 3.5 W
Current consumption	<ul style="list-style-type: none"> • I_{max}: 450 mA • I_{burst}: 1.26 A
In port	Number: 1 Implementation: 2-pin terminal block Permitted voltage range: 5 to 30 VDC Voltage in status "On": ≥ 5 V Voltage in status "Off": ≤ 1.2 V
Out port	Number: 1 Implementation: 2-pin terminal block Operating voltage: 30 VDC Load capability: 20 mA
Wireless interface	
Antenna connector	Number: 2 Implementation: SMA socket Nominal impedance: 50 ohms Connector A1 for the main antenna Connector A2 for the supplementary antenna
Frequency bands	<ul style="list-style-type: none"> • UMTS: 800, 850, 1700 (AWS), 1900, 2100 MHz • GPRS: 850, 900, 1800, 1900 MHz
UMTS with HSPA+	Transmission rates: <ul style="list-style-type: none"> • HSDPA (downlink): 14.4 Mbps • HSUPA (uplink): 5.76 Mbps

Technical specifications

EGPRS	Multislot class 12, mobile station class B Downlink coding schemes - CS 1-4, MCS 1-9 Uplink coding schemes - CS 1-4, MCS 1-9 Transmission rates: <ul style="list-style-type: none">• Downlink: 237 kbps• Uplink: 237 kbps
-------	---

GPRS	Multislot class 12, mobile station class B Coding schemes 1-4 Transmission rates: <ul style="list-style-type: none">• Downlink: 85.6 kbps• Uplink: 85.6 kbps
------	---

SMS (TX)	Text mode, SMSoverIP
----------	----------------------

Permitted ambient conditions

Ambient temperature	<ul style="list-style-type: none">• During operation: -40°C to +75°C• During storage: -40°C to +85°C
---------------------	---

Relative humidity at 25°C	0 ... 95% no condensation
---------------------------	---------------------------

Design, dimensions and weight

Design	Compact design, for DIN rail mounting
--------	---------------------------------------

Materials	Plastic
-----------	---------

Degree of protection	IP20
----------------------	------

Dimensions (W x H x D)	45 x 99 x 114 mm
------------------------	------------------

Weight	280 g
--------	-------

Product functions

Firewall and security	<ul style="list-style-type: none">• Stateful Inspection• Packet filter• Anti spoofing• IPsec VPN for up to 10 connections• Password protection
-----------------------	--

Technical specifications

Router functions

- Port forwarding
- NAT (IP masquerading)
- NAT traversal
- 1:1 NAT
- DynDNS client
- DNS cache
- DHCP server on internal (local) network
- NTP
- Remote logging
- Connection monitoring
- Alarm SMS
- Sending SMS messages from the local area network
- Traffic volume supervision
- Installation mode for aligning the antennas

Configuration / management

- Web-based administration user interface (WBM)
 - Remote access with HTTPS
 - SNMP and SNMP traps
-

Approvals issued

Note

Issued approvals on the type plate of the device

The specified approvals apply only when the corresponding mark is printed on the product. You can check which of the following approvals have been granted for your product by the markings on the type plate.

Current approvals on the Internet

SIMATIC NET products are regularly submitted to the relevant authorities and approval centers for approvals relating to specific markets and applications.

You will also find the current approvals for the product on the Internet pages of Siemens Automation Customer Support under the following entry ID:

39971776 (<http://support.automation.siemens.com/WW/view/en/48284698>)

→ "Entry list" tab, entry type "Certificates"

National approvals

You will find an overview of the country-specific wireless approvals of SIMATIC NET devices with GSM or UMTS services on the Internet pages of Siemens Automation Customer Support. You will find the link to the document on the following page:

ik-Info (www.siemens.com/simatic-net/ik-info)

EU declaration of conformity



When used for its intended purpose, the product is compliant with the requirements of the following European directives:

- Directive 1999/5/EC (R&TTE) of 9 March 1999 of the European Parliament and of the Council on Radio Equipment and Telecommunications Terminal Equipment and the mutual recognition of their conformity

Applied standards:

- EN 301 511: v.9.0.2
- 3GPP TS 51.010-1: v. 5.10.0

Classification

- Telecommunication equipment,
- Wireless device
- Device class 1

- Directive 2006/95/EC (Low Voltage Directive) of the European Parliament and of the Council of 12 December 2006 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits

Applied standards:

- EN 60950:2006

- Directive 2004/108/EC (EMC) of the European Parliament and of the Council of December 15, 2004 on the approximation of the laws of the member states relating to Electromagnetic Compatibility and repealing Directive 89/336/EEC

Applied standards:

- EN 55022:2006 limit class A
- EN 55024:1998 + A1:2001 + A2:2003
- EN 61000-6-2:2001

Note

The SCALANCE M875 is a device of class A. This device can cause wireless interference in domestic areas. In this case, the operator may be required to take suitable measures.

You will find the EC Declaration of Conformity for this product on the Internet at the following address:

Link to the declaration of conformity:

(<http://support.automation.siemens.com/WW/view/en/10805878>) "Entry list" tab

Filter: → Entry list → Entry type "Certificates" → Type of certificate: "Declaration of Conformity" → "Search word(s): <Name of the module>

UL/CSA certification



Certificate No. E301659, Report No. E301826

- UL 60950-1, 2nd Edition, 2011-12-19 (Information Technology Equipment - Safety - Part 1: General Requirements)
- CSA C22.2 No. 60950-1-07, 2nd Edition, 2011-12 (Information Technology Equipment - Safety - Part 1: General Requirements)

FCC Part 15

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy.

If not installed and used in accordance with the instructions, this may cause harmful interference to wireless communications. There can be no guarantee with certain installations, even when complying with the instructions, that no interference will be caused. If this equipment does cause harmful interference to radio or television reception that can be determined by turning the equipment off and on, the user is recommended to try to combat the interference with the following measures:

- Change the orientation of the receiving antenna or install it at a different location.
- Increase the distance between the SCALANCE M875 and the radio or television receiver.
- Connect the device to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer / installer or an experienced radio / TV technician for help.

FCC Part 15.19

This device complies with Part 15 of the FCC Rules. Operation is subject to the following conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Part 15.21

Modifications not expressly approved by this company could void the user's authority to operate the equipment.

The SCALANCE M875 may only be operated with an antenna belonging to the accessories of the SCALANCE M875.

The installation of the SCALANCE M875 and the antenna as well as servicing must be performed by qualified technical personnel only. When servicing the antenna, or working at distances closer than those listed below, make sure that the transmitter has been disabled.

FCC ID of the GSM module: QIPPH8

This device contains GSM, GPRS Class 12, EGPRS Class 10, and UMTS functions in the 900 and 1800 MHz band that may not be used in territories of the USA.

This device can be used for mobile and fixed applications. Internal / external antennas used with this device must be at a distance of at least 20 cm from all persons and must not be located so that they operate in combination with any other antenna or transmitter.

Users and installers must be provided with antenna installation instructions and transmitter operating conditions that must be kept to avoid exceeding the permitted RF exposure. Antennas used for this GSM module must not exceed 8.4 dBi antenna gain (GSM 1900) and 2.9 dBi (GSM 850) for mobile and fixed operating configurations. This device is approved as a module for installation in other devices.

GCF and PTCRB

The mobile wireless module of the SCALANCE M875 conforms to the requirements of Global Certification Forum (GCF) and PTCRB.

Railway applications

EN 50155

German Federal Motor Transport Authority

E1

Additional Internal Routes

The following sketch shows how the IP addresses could be distributed in a local network with subnets, what network addresses result from this, and what the specification for an additional internal route could look like.

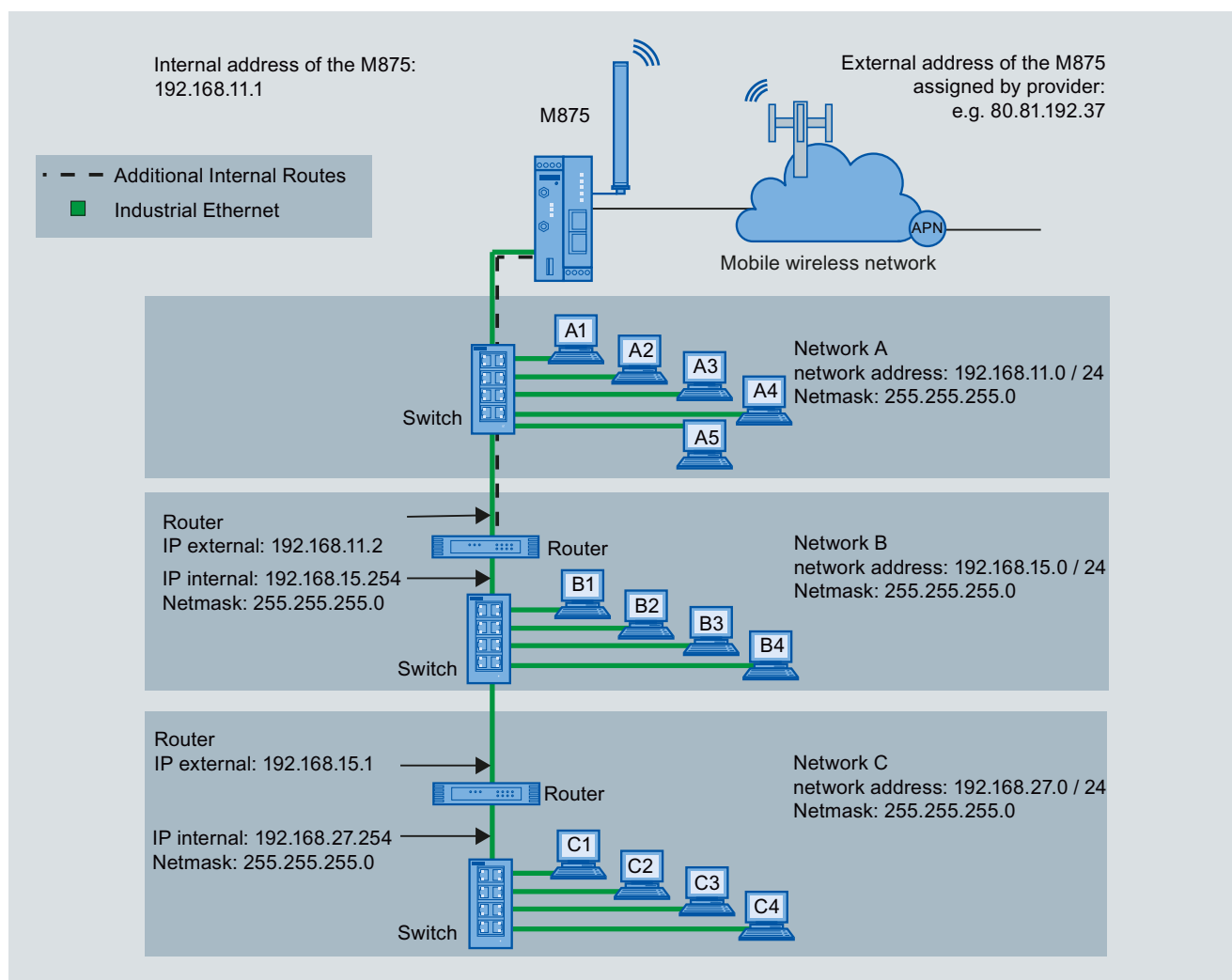


Figure A-1 Additional Internal Routes

Network A is connected to the M875 and via this to a remote network.

Additional internal routes show the path to the additional networks B and C that are connected to each other via gateways (routers). In the example shown, networks B and C can both be reached via gateway 192.168.11.2 and network address 192.168.11.0/24 by the M875.

Additional Internal Routes

Network A					
Computer:	A1	A2	A3	A4	A5
IP address:	192.168.11.3	192.168.11.4	192.168.11.5	192.168.11.6	192.168.11.7
Subnet mask:	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Network B					
Computer:	B1	B2	B3	B4	Additional internal routes: Network:: 192.168.15.0/24 Gateway: 192.168.11.2
IP address:	192.168.15.3	192.168.15.4	192.168.15.5	192.168.15.6	
Subnet mask:	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	
Network C					
Computer:	C1	C2	C3	C4	Additional internal routes: Network:: 192.168.27.0/24 Gateway: 192.168.11.2
IP address:	192.168.27.3	192.168.27.4	192.168.27.5	192.168.27.6	
Subnet mask:	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	

Training, Service & Support

Service & Support

In addition to the product documentation, the comprehensive online information platform of Siemens Automation Customer Support supports at any time and at any location in the world. You will find the Service & Support pages on the Internet at the following address:

<http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo2&aktprim=99&lang=en>

Apart from news, you will also find the following information there:

- Product information, Product Support, Applications & Tools
- Technical Forum
- Technical Support - Ask the Siemens experts
- Our service offer:
 - Technical Consulting, Engineering support
 - Field Service
 - Spare parts and repairs
 - Maintenance, optimization, modernization and more

You will find contact data on the Internet at the following address:

<http://www.automation.siemens.com/partner/guiwelcome.asp?lang=en>

SITRAIN - Siemens training for automation and industrial solutions

With over 300 different courses, SITRAIN covers the entire Siemens product and system spectrum in the field of automation and drive technology. Apart from the classic range of courses, we also offer training tailored for individual needs and a combination of different teaching media and sequences, for example self-learning programs on CD-ROM or on the Internet.

You will find detailed information on the training curriculum and how to contact our customer consultants at the following Internet address:

www.siemens.com/sitrain

Glossary

2G

Digital mobile wireless networks of the second generation, for example GSM

3G

Digital mobile wireless networks of the third generation, for example UMTS

AES

Advanced Encryption Standard

Symmetric block cipher. Specification for cryptography of data in wireless LAN networks.

Anti-spoofing

→ *Spoofing*

APN

Access point name

DNS host name of the access point of a network to an external network.

In telecontrol, the APN is the name of the access point of a GPRS network to the Internet or to a private company network. Depending on the type of network connected, this is a public or private APN. Information about the APN is provided by the GSM network provider.

Asymmetrical encryption

Public key method

Method for converting plain language into a "secret" text and vice versa, where the key pair consists of a public key for encrypting and a private key for decrypting.

CIDR

Classless Inter-Domain Routing

Notation for grouping several IP addresses into an address range by representing an IP address combined with its network mask. To do this, a suffix is appended to the IP address that specifies the number of bits of the network mask set to 1. Using the CIDR notation, routing tables can be reduced in size and the available address ranges put to better use.

Example: IP address 192.168.0.0 with network mask 255.255.255.0

The network part of the address covers 3 x 8 bits in binary representation; in other words 24 bits. This results in the CIDR notation 192.168.0.0/24.

In binary representation, the host part covers 1 x 8 bits. This results in an address range from 2^8 , in other words 256 possible addresses.

CSD

Circuit switched data

Service in the mobile wireless network for wireless transmission of data at 14.4 Kbps full duplex. Connections can be established to other mobile wireless devices, to analog modems or to ISDN modems in the fixed network. The connection establishment can be started at both ends. Only dial-up connections are supported.

CSQ

Value for specifying the signal quality in mobile wireless. The CSQ values correspond to the dBm values of the received field strength (RSSI Received Signal Strength Indication). A CSQ value of < 6 (-101 dBm) counts as a bad quality, a CSQ value of > 18 (75 dBm) counts as a very good quality.

DES

Data Encryption Standard

Method for encrypting data (56-bit encryption)

DES3

Data Encryption Standard

Symmetrical encryption scheme in which the same key is used to encode and decode the data. DES3 means that the algorithm is used three times to increase security.

DHCP

Dynamic Host Configuration Protocol

You can operate SCALANCE S on the internal network as a DHCP server. This allows IP addresses to be assigned automatically to the devices connected to the internal network. The IP addresses are assigned either dynamically from an address band you have specified or you can select a specific IP address for a particular device.

DNS

Domain Name System

Distributed database that manages the name space on the Internet.

Domain Name System

→ *DNS*

Dynamic Domain Name System

→ *DynDNS*

Dynamic Host Configuration Protocol

→ *DHCP*

DynDNS

Dynamic Domain Name System

Network service similar to DNS for subscribers with changing IP addresses. The service updates the address entries on the name server in real time so that the subscriber is always accessible under a specified host name.

EDGE

Enhanced Data Rates for GSM Evolution

Further development of GSM technology. With an additional modulation method, the available transmission speeds in mobile wireless networks are increased. With EDGE, the packet-oriented mobile wireless service GPRS becomes EGPRS and HSCSD becomes ECSD.

EGPRS

Enhanced GPRS

Packet-oriented service for IP-based data transmission in GSM networks. By using an additional modulation procedure (EDGE technology), a higher transmission speed is achieved compared with GPRS.

Enhanced GPRS

→ *EGPRS*

External partners

Network components in a network other than the local area network, for example Web servers on the Internet, routers in the intranet, central company servers, an Admin PC.

Global System for Mobile Communication

→ *GSM*

GPRS

General Packet Radio Service

Packet-oriented service for IP-based data transmission in GSM networks. GPRS data packets can also be transferred via the Internet. The data is transmitted using the Internet protocols TCP/IP or UDP/IP.

GSM

Global System for Mobile Communication

Worldwide standard for mobile communication

HSDPA

→ *HSPA*

HSPA

High Speed Packet Access

Further development of the UMTS technology that allows higher data transmission speeds. HSPA consists of HSDPA to increase the download rate and HSUPA to increase the upload rate.

HSUPA

→ *HSPA*

HTTPS

Secure Hypertext Transfer Protocol or HyperText Transfer Protocol Secured Socket Layer (SSL)

Protocol for transmission of encrypted data. Expansion of HTTP for secure transmission of confidential data with the aid of SSL.

Internet Protocol

→ *IP*

IP

Internet Protocol

Represents the network layer of the OSI model for TCP/IP-based networks.

The most important information is the unique IP address. The blocks of data are sent to the destination computer independently. IP does not negotiate anything with the destination computer. There is no end-to-end error check. Frames can arrive in a different order from the order they were sent in. TCP is responsible for putting them together in the correct order.

IP address

Address consisting of a numeric code made up of four numbers each from 0 to 255 (for example 192.168.1.1). It is the unique digital address of a node in an IP-based network.

IPsec

IP protocol expansion for VPN at OSI layer 3

IPsec only allows encryption of IP packets but does not transfer multicast frames and only supports static routing.

Local application

Application software on a network component in the local network, for example a programmable controller, a machine with an Ethernet interface for remote monitoring, a notebook, desktop PC or the Admin PC.

MCC - Mobile Country Code

→ *PLMN*

MNC - Mobile Network Code

→ *PLMN*

NAPT

Network Address Port Translation

Procedure with which an IP address is replaced on the router by another address and the port number by another port number.

NAT

Network Address Translation

Routine with which an IP address in a message is replaced on the router by another.

NAT traversal

Method with which IPsec data can traverse NAT devices.

NAT/NAPT router

Mechanism with which the addresses of the nodes in the internal subnet are not made known to the outside in the external network. The addresses in the external network are visible only via the external IP addresses defined in the translation list.

Network Address Port Translation

→ *NAPT*

Network Address Translation

→ *NAT*

PKCS

Public Key Cryptography Standards

Specifications for cryptographic keys developed by RSA Security and others. A certificate links data of a cryptographic key (or key pair consisting of a public and private key) with data of the owner and a certification issuer.

PKCS#12 format

Standard that specifies a PKCS format suitable for exchange of the public key and an additional password-protected private key.

PLMN

Public Land Mobile Network

Worldwide unique identifier of mobile wireless networks. The PLMN is made up of the three-digit Mobile Country Code (MCC) and the two-or three-digit Mobile Network Code (MNC).

Port number

Part of an address that assigns data segments to a network protocol. Among other things, this includes permanently assigned and generally known port numbers for specific applications, for example 80 for the HTTP transmission protocol.

PPPoE

Point to Point Protocol over Ethernet

Name for the use of the PPP network protocol via an Ethernet connection.

Preshared keys

Symmetric key procedure. The key must be known at both ends prior to communication.

Public Key Cryptography Standards

→ *PKCS*

Public key method

→ *Asymmetrical encryption*

Secure Hypertext Transfer Protocol

→ *HTTPS*

SNMP

Simple Network Management Protocol

Standardized protocol for transporting network management information

Spoofing

Methods for undermining authentication and identification procedures based on trustworthy addresses or host names. In IP spoofing, for example, a falsified source IP address is used.

Anti-spoofing describes mechanisms to discover or prevent spoofing.

SSH

Secure SHell

Protocol that allows secure and encrypted data exchange between computers. SSH is used for remote access to the input console of LINUX-based machines.

Stateful inspection firewall

Also Stateful Packet Inspection

A stateful inspection firewall is a method of packet filtering. Packet filters only let IP frames through if they comply with previously defined firewall rules. The following is defined in the firewall rule:

- which protocol (TCP, UDP, ICMP) can pass through?
- Which source of the frame (IP / port) is permitted?
- Which destination of the frame (IP / port) is permitted?

The rules also define what will be done with IP frames that are not allowed through (discarded or rejected).

With a simple packet filter, it is always necessary to create two firewall rules for a connection:

- One rule for the query direction from the source to the destination
- A second rule for the response direction from the destination to the source.

This is different with a stateful inspection firewall. Here a firewall rule is only created for the query direction from the source to the destination. The firewall rule for the response direction from the destination to the source results from analysis of the data previously sent. The firewall rule for the responses is closed again after the responses are received or after a short period of time has elapsed. This means that responses can only pass through if there was a previous query. This means that the response rule cannot be used for unauthorized access. What is more, special procedures make it possible for UDP and ICMP data to pass through as well, even though this data was not requested before.

Subnet

Part of a network delineated from the total network by suitable devices, for example gateways. The subnet includes bus components and all the attached stations.

A system usually consists of several subnets with unique subnet numbers. A subnet consists of several nodes with unique addresses or MAC addresses (Industrial Ethernet).

Subnet mask

The subnet mask specifies which parts of an IP address are assigned to the network number. The bits in the IP address whose corresponding bits in the subnet mask have the value 1 are assigned to the network number.

Symmetrical encryption

Method for converting plain language into "secret" text and vice versa where both communications partners use the same private key for encrypting and decrypting. The key usually consists of a series of bits. Examples include the DES or the AES method.

TCP

Transmission Control Protocol

Protocol for connection-oriented data transmission in networks; it belongs to the family of Internet protocols. In the OSI layer model, the protocol operates at layer 4.

TCP/IP

Transmission Control Protocol / Internet Protocol

The name of a collection of protocols that due to their great significance for data transmission in heterogeneous networks are also known as the Internet protocol family. In the OSI layer model, these protocols operate at layer 3 (IP) and layer 4 (TCP).

Tunnel

A tunnel or tunneling means the use of the communications protocol of a network service as a vehicle for data that does not belong to this service.

UDP

User Datagram Protocol

Datagram service for simple and data transfer beyond the boundaries of a network without acknowledgment.

UMTS

Universal Mobile Telecommunication System

Mobile wireless specification of the 3rd generation (3G) that allows significantly higher data transmission speeds than the GSM networks of the 2nd generation so that, for example, video applications can also be transferred.

User Datagram Protocol

→ *UDP*

Virtual Private Network

→ *VPN*

VPN

Virtual Private Network

Technology for secure transportation of confidential data in public IP networks, for example the Internet.

VSWR

Voltage Standing Wave Ratio

Ratio of the effective voltages of the outgoing and returning waves in an electrical cable that leads to reflection of the electromagnetic waves if the termination is unsuitable. An unsuitable termination may be a resistor that does not correspond to the cable impedance or a second connected cable with a different impedance, for example an antenna. The VSWR is a measure of the transmission losses in electrical cables.

VSWR = 1 means no losses (but also practically no radiation of power from an antenna).

VSWR = ∞ means total reflection.

X.509 certificate

Specification of a cryptographic procedure for creating digital certificates

Certificates attest the authenticity of a public key (asymmetrical encryption) and associated data.

An X.509(v3) certificate contains among other things a public key, information about the key owner (specified as distinguished name (DN)), permitted designated uses, etc. and the signature of the certification authority (CA).

Involving certification authorities means that not every key owner needs to know the other, only the certification authority used. The additional key information also simplifies the administrability of the key.

X.509 certificates are used for example in e-mail encryption, using S/MIME or IPsec.

Index

1

1:1 NAT, 87

A

Admin PC, 33
APN, 62
Application, local, 49

C

CA certificate, 86
Calling the start page, 36
Changing the password, 112
Checking the connection, 68
Checking the hardware connection, 37
Checksum, 93, 101
Contact, 151
CSQ, values, 41

D

Dead peer detection, 88
Destination NAT, 81
Device name, 3

E

Entering/changing the PIN, 60
Error diagnostics, 138
External network, 58
External partner, 58
External power supply, 25

F

Firmware version, 3
Frequency bands, 28
FTP, 135

H

Hardware product version, 3
Hash, 93, 101

I

IKE, 87
Installation mode (antenna), 64
Internet Key Exchange, 87
Invalid entries, 38
IP address
 Configuring, 50
 Factory setting, 50
 Factory settings, 33
IP masquerading, 75
IPsec protocol suite, 85
IPsec SA, 88, 93, 101
ISAKMP SA, 88, 93, 101

L

LAC, 65

M

MIB files, 124

N

NAT
 1, 87
 Destination NAT, 81
 IP masquerading, 75
 NAT traversal, 88
NAT traversal, 88

O

Order number of the M875, 3

P

Password

- Changing, 37, 112
- Factory setting, 36
- Phase 1
 - ISAKMP SA, 92, 100
- Phase 2
 - IPsec SA, 92, 100
- PLMN, 62
- Pre-shared key, 86
- Proxy server, 37

R

- Reset
 - Default configuration, 133
 - Factory settings, 139
- Roadwarrior mode, 86

S

- Safety notices, 25
- SCALANCE S, 98
- Signal strength, 41, 64
- SIMATIC NET IE SNMP OPC server, 124
- SINEMA server, 124
- Standard mode, 86
- Stateful inspection firewall, 76
- Subnets of the local network, 57
- Support, 151

T

- Training, 151

U

- User name, 36

W

- Web user interface, 33

X

- X.509 certificate, 86