

Weidmüller 

u-link Remote Access Service

Technical User Guide
Version 1.5.1

October, 2020



Copyright Notice

Copyright © 2020 Weidmüller Interface GmbH & Co. KG

All rights reserved.

Reproduction without permission is prohibited.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Weidmüller.

Weidmüller provides this document "as is," without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Weidmüller reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Weidmüller assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Contact Information

Weidmüller Interface GmbH & Co. KG

PO box 3030

32760 Detmold

Klingenbergstrasse 16

32758 Detmold

Germany

Phone +49 (0) 5231 14-0

Fax +49 (0) 5231 14-2083

E-Mail info@weidmueller.com

Internet www.weidmueller.com

Table of Contents

	Page
Chapter 1 – Overview u-link Remote Access Service	4 Link
Chapter 2 – Starting with u-link / Registration of a new u-link system account	10 Link
Chapter 3 – Overview features and functions of u-link Web portal	15 Link
Chapter 4 – Setup of a remote access scenario (Example)	23 Link
Chapter 5 – Initiating a remote access to remote LAN devices	64 Link
Chapter 6 – Further functionality of u-link	73 Link
Chapter 7 – Standard Functions - Further functionality in Standard Version	79 Link
Appendix	
1 – Registration of Router to u-link failed (How to solve)	92 Link
2 – General support in case of Router problem issues	95 Link
3 – Functional diagram of u-link	96 Link
4 – Internet connection requirements of u-link VPN clients (Service PC / Router)	97 Link
5 – Activating / de-activating Router VPN connection by digital input	98 Link
6 – How to change Router LAN-IP address/netmask via u-link VPN connection	99 Link
7 – Technical u-link support	102 Link

Chapter 1: Overview u-link Remote Access Service

- 1.1 General information
- 1.2 How u-link is working / Involved components
- 1.3 Features of Entry Version (free of charge)
- 1.4 Features of chargeable Standard Versions
- 1.5 Link to buyable u-link licenses

1.1 General information

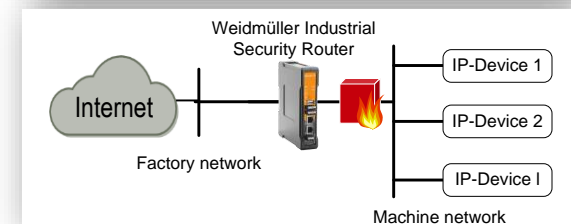
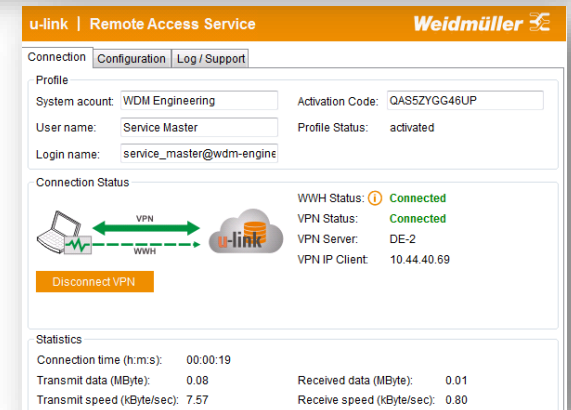
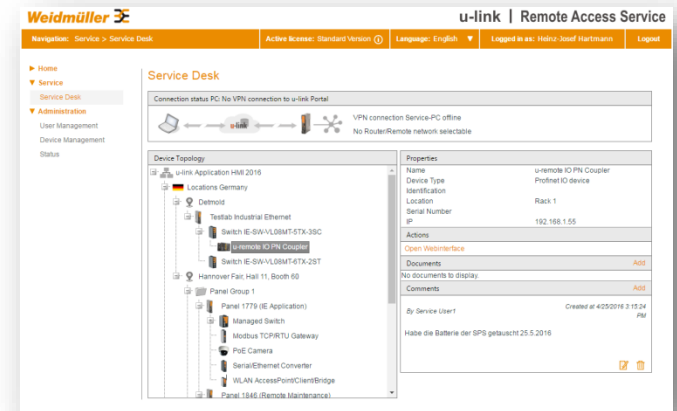
- The Weidmüller u-link Remote Access Service allows an easy and secure access of Service PCs to remote local Ethernet networks via the Internet.
- The VPN-based access of a Service PC to remote networks will be provided by the web-based u-link Portal service (VPN server) and a Weidmüller Router (VPN client) located in a remote target network.
- The u-link VPN server is used as a meeting point and connects a Service PC to a Router (both running as VPN clients) to allow an encrypted data communication between the PC and remote Ethernet devices connected to the LAN port of the Router.
- Using the u-link VPN server as public accessible meeting point both a Service PC and a Router only need to establish an outgoing VPN connection to the Internet which usually is allowed and compliant to IT security requirements.
- For secure data integrity the u-link Remote Access Service uses for each u-link system account its own server and database instances (secure separation of u-link accounts).
- The data communication between an account specific u-link VPN server and remote clients (Service PCs and Router) is based on a certificate-secured OpenVPN communication (Encryption RSA 2048, x509 certificates).
- Based on customer requirements the u-link Remote Access Service is offered with following variants:
 - **Entry Version** (free of charge, no time limitation of use)
 - **Versions Standard 150/300/500/ and more** (Extended features, buyable use license, 1 year license validity)
 - When using a “**Standard Version**” additional **VPN licenses** can be purchased to use more than 3 simultaneous VPN pass-through connections of a Service PC to a remote router/network.



1.2 How the u-link Remote Access Service is working / Involved hard and software components

The u-link Remote Access Service consists of the 3 components...

- **Web accessible u-link Portal servers** to manage the customer specific account.
 - Device configuration representing the real devices located in the field.
 - User configuration representing the Service PCs which do a remote access.
 - Providing the VPN based pass-through connection between a Service PC and a Router / Remote network.
 - Main u-link components: Web server (Portal access), VPN server, Database server and the WWH server (world wide heartbeat).
 - By creating/registering an u-link system account for each account the Portal server instances will be created exclusively.
-
- **Windows-based PC**
 - Uses Software 'u-link VPN client' for secure communication with remote devices via the u-link VPN server.
 - Browser based access to u-link Portal to select the target devices for remote access.
 - Currently MS Windows versions 7, 8, and 10 are supported.
-
- **Weidmüller Router** located in the remote network providing the access to connected devices at LAN port.
 - Useable models: All Weidmüller Router variants except model E-SR-2GT-LAN-FN (for routing/NAT/security applications, does not support VPN)
 - u-link is supported from firmware version 3.0.2 (Update downloadable).
 - Routers already installed in Security/Firewall applications can be extended to use u-link additionally.



1.3 Features of Entry Version (free of charge)

General features

- Can be used free of charge, no time limitation of use
- Maximum 50 Router objects configurable (Access points to a remote network)
- No limit on the number of configurable service users
- 2 VPN pass-through connections (Service PC → u-link VPN server → Router/Remote network) simultaneously usable.
- Bandwidth of VPN connection (calculated on total data volume of a system account)
 - max. 500 kBit/sec for data volume <= 1 GB/Month (not guaranteed)
 - max. 64 kBit/sec for data volume > 1 GB/Month
- No guaranteed system availability

Service Desk

Connection status PC: No VPN connection to u-link Portal

VPN connection Service-PC offline
No Router/Remote network selectable

Device Topology

- MyCompany Ltd.
 - Router Machine 1
 - PLC 1 (S7-300)
 - u-remote IO Device 1
 - u-remote IO Device 2
 - Router Machine 2
 - Managed Switch
 - PLC 2 (S7-300)
 - u-remote IO Device 1
 - u-remote IO Device 2
 - u-remote IO Device 3
 - Router Machine 3
 - PLC (Beckhoff)
 - Ethercat u-remote D1
 - Ethercat u-remote D2
 - Router Machine 4
 - IP Camera
 - Router Machine 5

Sample screenshot of a flat Device topology.
All Router objects (Entry version) always are arranged directly below the root container.
All configured objects (Routers and user-defined Ethernet devices) are visible and accessible for each Service user.

Functional features

- Device Management (Router/Device configuration representing the remote accessible devices)
 - Device topology can only be designed as a flat structure (All Router objects directly are arranged among the root container).
- User Management (Administration of Service users)
 - Each defined service user has access to any configured object (Router/Remote network devices)
 - Each created user is member of default “Service group” with pre-defined user permissions (not changeable)
- Administrator has full featured access, service users may maintain the Device management (no User Management).

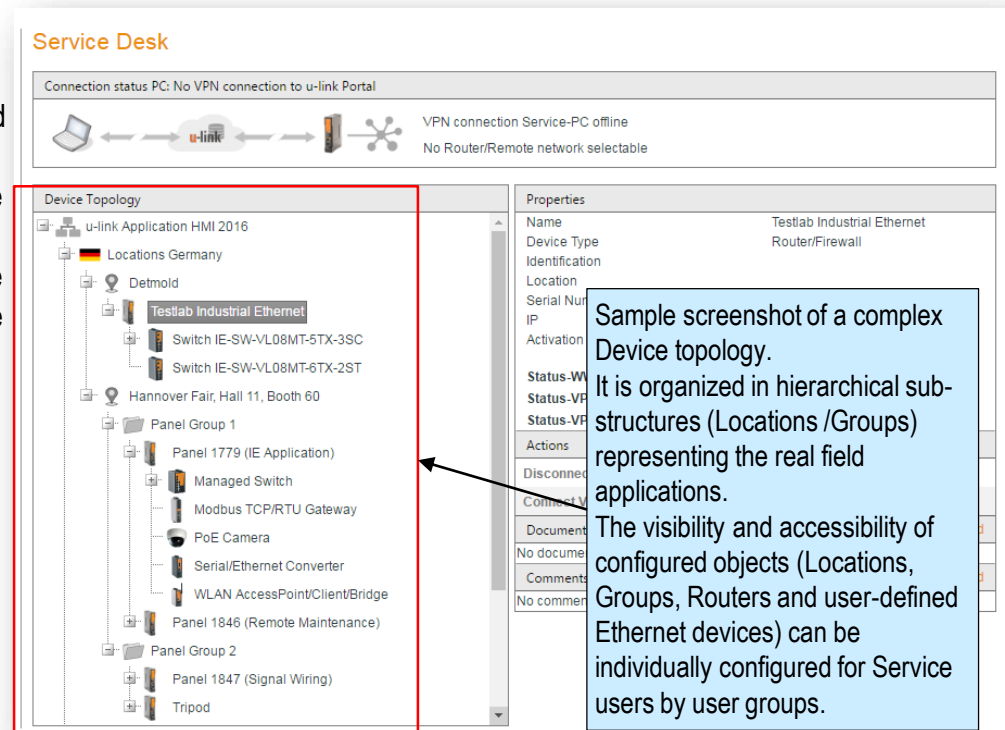
1.4 Features of chargeable Standard Versions

Variants

- Standard Versions having following extended features related to the Entry Version:
 - **Standard 150:** Maximum 150 Router objects configurable (Access points to a remote network)
 - **Standard 300:** Maximum 300 Router objects configurable
 - **Standard 500:** Maximum 500 Router objects configurable
 - **Standard more:** As many Router objects configurable as the customer needs
- To use a standard version a usage license has to be purchased having 1 year license validity.
- Upgrading from a lower version or extension of validity of a running version easily can be done by entering the purchased license key in Account Management by Account Administrator

General features of all Standard versions

- 3 VPN pass-through connections (Service PC → u-link VPN server → Router/Remote network) simultaneously usable
- Optional use of additional simultaneously VPN pass-through connections (buyable license key)
- Remote device topology can be organized by a tree-like structure (Locations, Groups, definable container objects)
- Group-based organization of service users with different permissions allows a selected access to device topology objects
- Advanced reporting and statistical information
- Bandwidth VPN connections (calculated on total data volume of a system account)
 - 1 Mbit/sec for each VPN tunnel up to a monthly data volume of 5 GB (guaranteed)
 - 500 kBit/sec for each VPN tunnel if the monthly data volume exceeds 5 GB
 - Additional 1 GB/Month at 1 Mbit/sec per additional purchased VPN connection
 - General bandwidth limitation of all VPN connections to 500 kBit/s if the monthly data volume exceeds 12 GB
- System availability: ≥ 99,6%



The screenshot displays the 'Service Desk' interface. At the top, it shows the connection status: 'Connection status PC: No VPN connection to u-link Portal'. Below this, there is a diagram of a VPN connection path and the text 'VPN connection Service-PC offline' and 'No Router/Remote network selectable'. The main area is divided into two panes. The left pane, titled 'Device Topology', shows a hierarchical tree structure starting with 'u-link Application HMI 2016'. Underneath, there are 'Locations Germany' and 'Detmold'. A red box highlights the 'Testlab Industrial Ethernet' section, which includes two switches: 'Switch IE-SW-VL08MT-5TX-3SC' and 'Switch IE-SW-VL08MT-6TX-2ST'. Below these are 'Hannover Fair, Hall 11, Booth 60', 'Panel Group 1' (containing 'Panel 1779 (IE Application)', 'Managed Switch', 'Modbus TCP/RTU Gateway', 'PoE Camera', 'Serial/Ethernet Converter', and 'WLAN AccessPoint/Client/Bridge'), 'Panel 1846 (Remote Maintenance)', 'Panel Group 2' (containing 'Panel 1847 (Signal Wiring)'), and 'Tripod'. The right pane, titled 'Properties', shows details for a selected device: 'Name: Testlab Industrial Ethernet', 'Device Type: Router/Firewall', and various identification and activation fields. A blue callout box with an arrow pointing to the 'Testlab Industrial Ethernet' section in the device topology contains the following text:

Sample screenshot of a complex Device topology. It is organized in hierarchical sub-structures (Locations /Groups) representing the real field applications. The visibility and accessibility of configured objects (Locations, Groups, Routers and user-defined Ethernet devices) can be individually configured for Service users by user groups.

1.5 Link to buyable u-link licenses

- For detailed information about available license types please check the Weidmüller product catalogue.
- Open www.weidmueller.com
- Select 'Product Catalogue'
- Select 'Active Industrial Ethernet'
- Then select section 'u-link Licences' in product group overview

[Hyperlink to u-link licenses \(Weidmüller product catalogue\)](#)

The screenshot shows the Weidmüller product catalogue website. The main content area is titled "U-LINK licenes" and provides an overview of the service. Below the overview, there is a "Products:" section with a list of license types and their details. A dashed box highlights the first product entry, and an arrow points to it from the text below.

Type	Order No.	Version
U-LINK-LIC-STD-150-1Y	2447050000	"Standard 150" version software licence for u-link Remote Access Service. Can be used to upgrade an entry version or to extend period of a "Standard 150" version
U-LINK-LIC-STD-300-1Y	2457840000	"Standard 300" version software licence for u-link Remote Access Service. Can be used to upgrade an entry version or to extend period of a "Standard 300" version
U-LINK-LIC-STD-500-1Y	2457850000	"Standard 500" version software licence for u-link Remote Access Service. Can be used to upgrade an entry version or to extend period of a "Standard 500" version
U-LINK-LIC-VPN-1Y	2447060000	"VPN connection" licence code for u-link Remote Access Service. Can be used as an additional VPN connection or to extend the period of a VPN connection that has already been activated

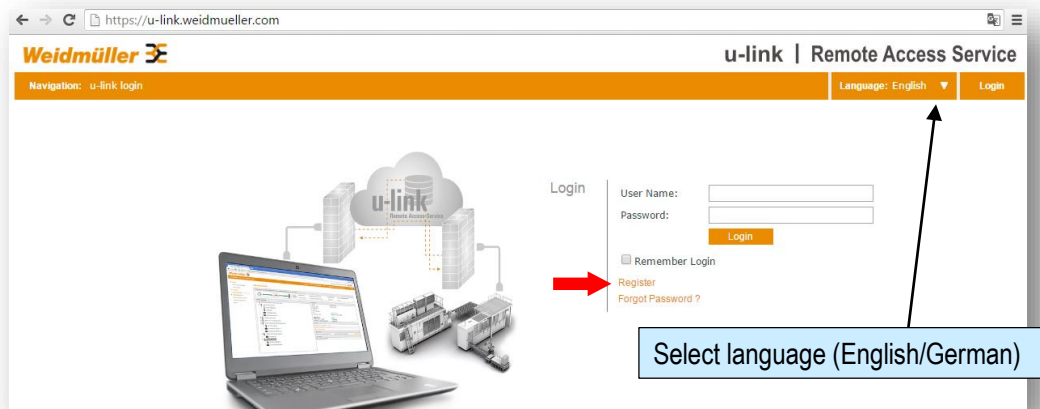
Chapter 2: Starting with u-link

2.1 Registration of a new u-link system account

2.1 Registration of a new u-link system account

Open u-link Web page (Step 1)

- Open a browser and enter **u-link.weidmueller.com**.
- Click button 'Register'.

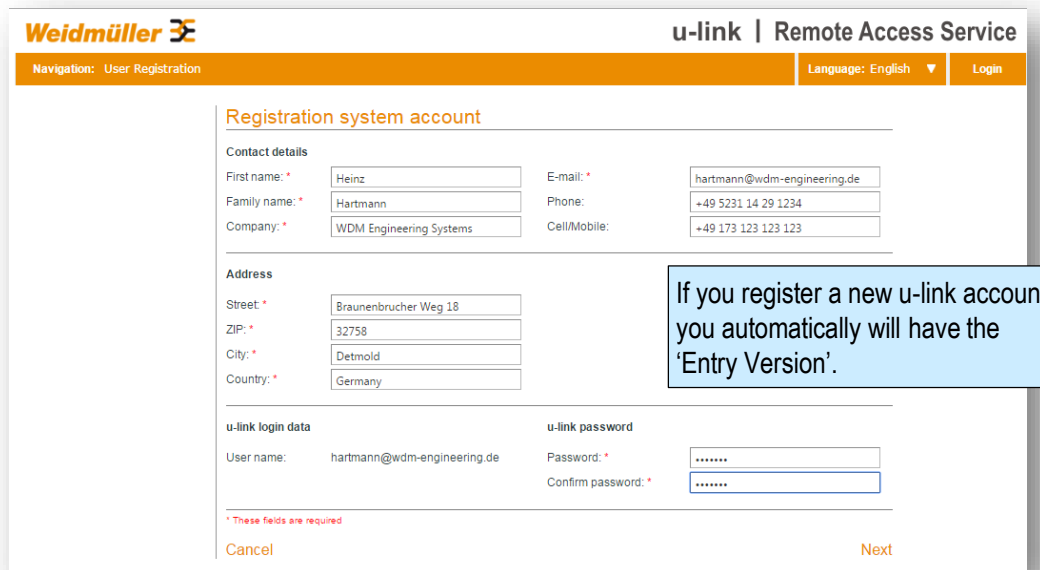


Starting the registration process (Step 2)

- Enter your registration data.
- Click button "Next".

Notes:

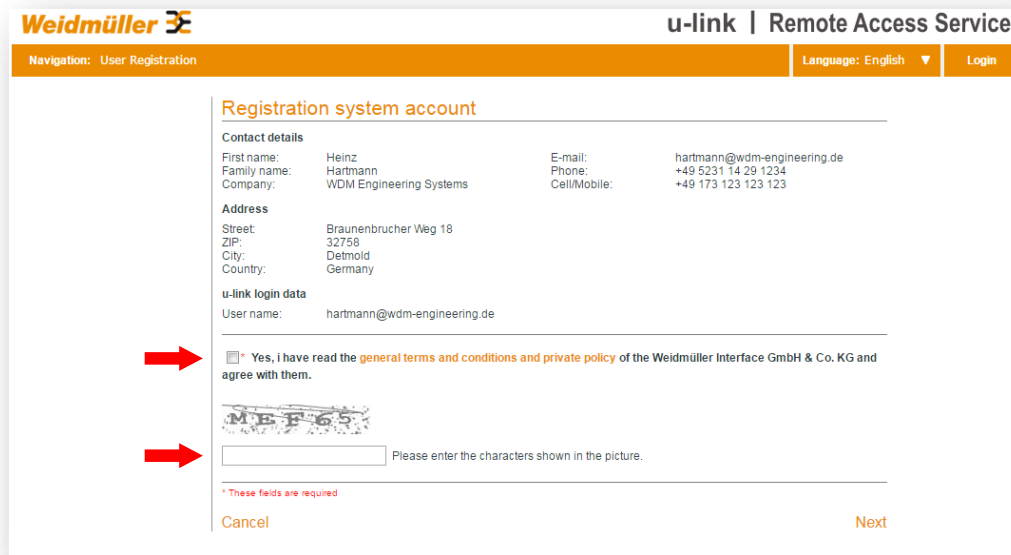
- This user will be the administrator of the u-link system account. Also this user can be used for remote access service.
- The mail address will be used for logon to the u-link account and must be unique in the global u-link system.
- The mail address must be existent because after registration a verification mail will be sent to the entered address.
- The entered password has to be used for logon to the u-link Portal after successful registration.




2.1 Registration of a new u-link system account

Registration process (Step 3)

- Set checkbox that you agree to the “General u-link terms and conditions”.
- Enter for security reasons the captcha characters displayed as graphical image.
- Click button “Next”.



Weidmüller  **u-link | Remote Access Service**

Navigation: User Registration Language: English ▼ Login

Registration system account

Contact details

First name:	Heinz	E-mail:	hartmann@wdm-engineering.de
Family name:	Härtmann	Phone:	+49 5231 14 29 1234
Company:	WDM Engineering Systems	CellMobile:	+49 173 123 123 123


Address

Street: Braunenbrucher Weg 18
 ZIP: 32758
 City: Detmold
 Country: Germany

u-link login data

User name: hartmann@wdm-engineering.de

* Yes, I have read the **general terms and conditions** and **private policy** of the Weidmüller Interface GmbH & Co. KG and agree with them.



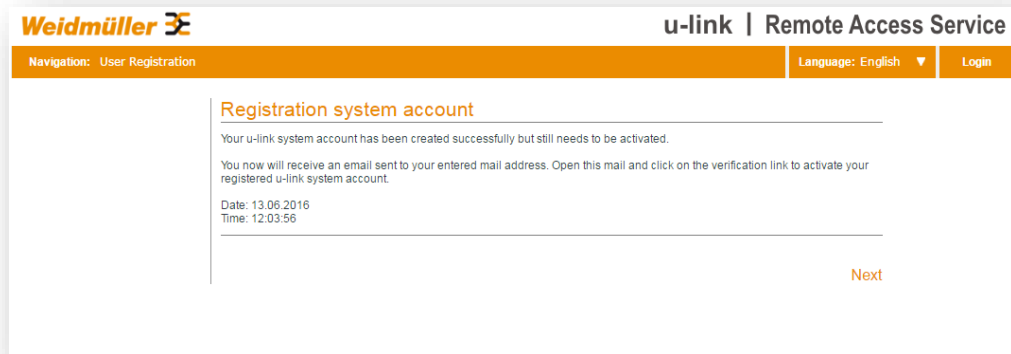
Please enter the characters shown in the picture.


* These fields are required

Cancel Next

Registration process (Step 4)

- An information will be displayed that your u-link account successfully has been created but it is not yet activated
- You now will now receive a mail containing a hyperlink to verify and activate your u-link account.
- When clicking button “Next” the u-link Login page will be displayed.
- **Before your first login you need to activate your account via verification mail (Check your mailbox).**



Weidmüller  **u-link | Remote Access Service**

Navigation: User Registration Language: English ▼ Login

Registration system account

Your u-link system account has been created successfully but still needs to be activated.

You now will receive an email sent to your entered mail address. Open this mail and click on the verification link to activate your registered u-link system account.

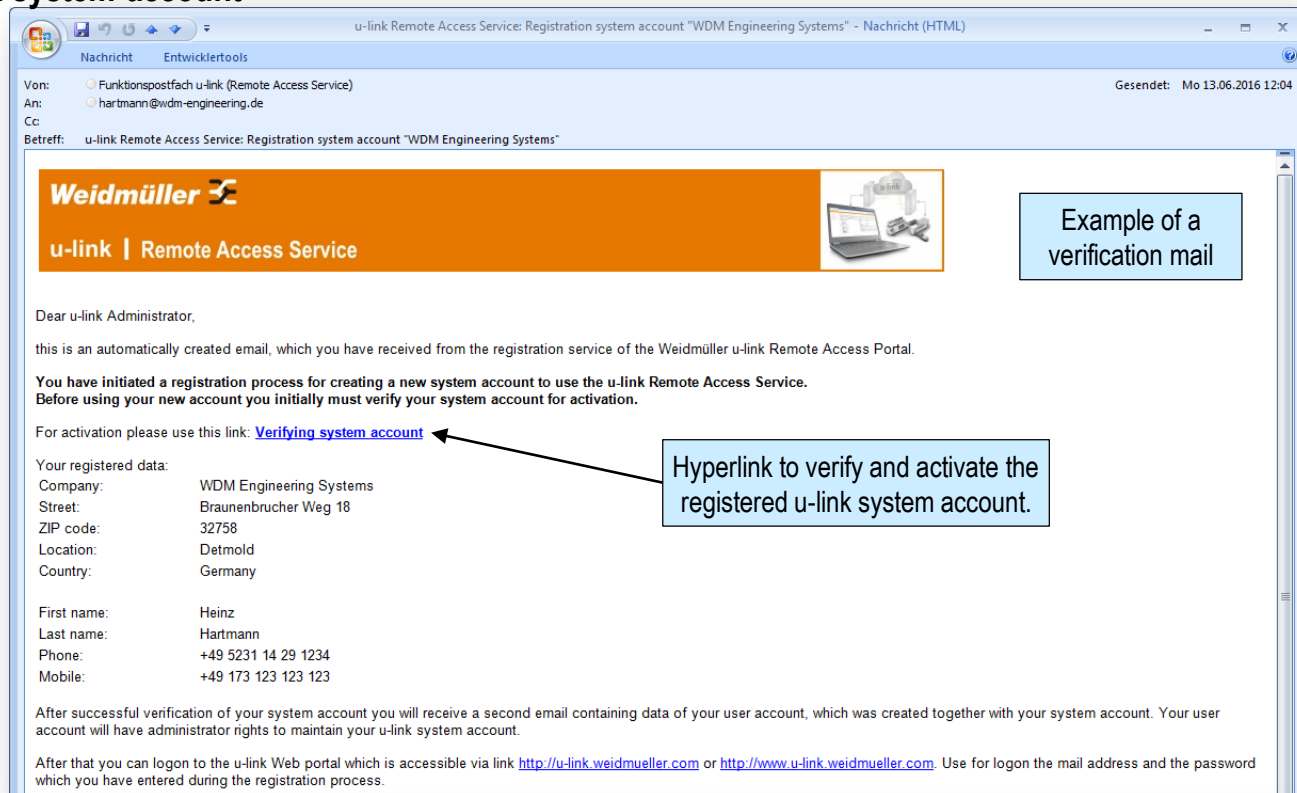
Date: 13.06.2016
 Time: 12:03:56

Next

2.1 Registration of a new u-link system account

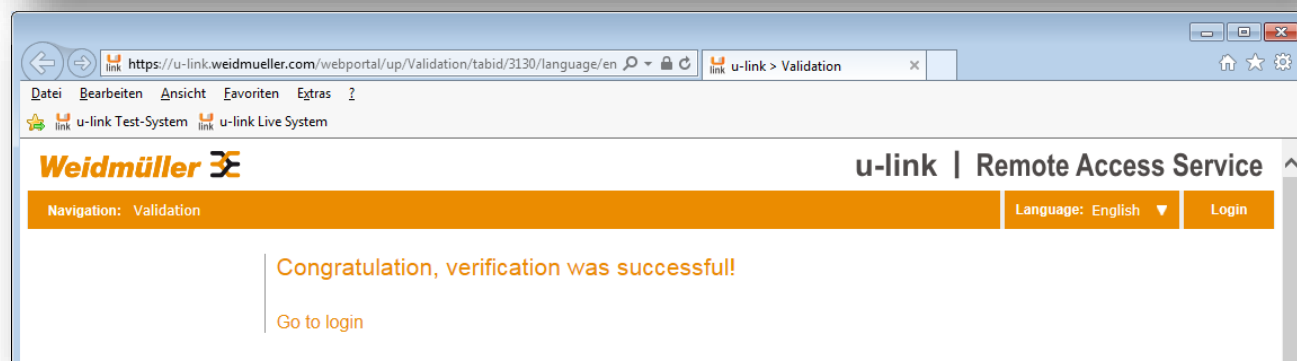
Registration process (Step 5)

- Open your received mail “Registration system account”.
- Click on hyperlink “Verifying system account”.



Registration process (Step 6)

- Now your standard browser will be opened displaying the information that your u-link successfully was activated.
- Additionally you will receive a second mail named “Registration Administrator” containing information about your user data (being the u-link administrator of the registered account).



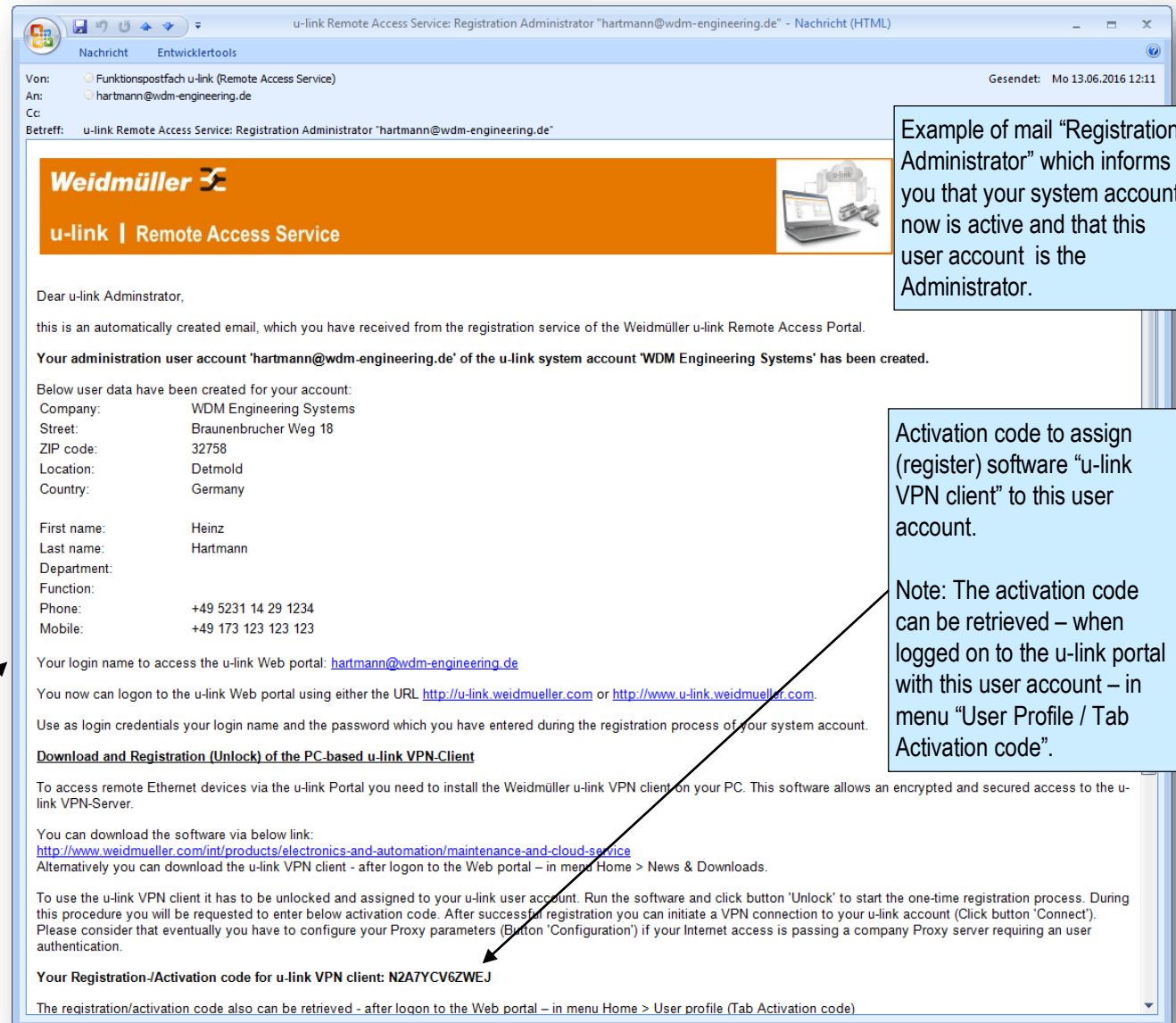
2.1 Registration of a new u-link system account

Registration process (Step 7)

- Check your mailbox regarding the mail “Registration Administrator”.
- This mail contains some information about your entered registration data and how to logon to the u-link Web portal.
- Additionally it contains the “Activation code” to register / unlock the software “u-link VPN client” using this account for remote access.

Registration process is finished after receiving this mail!

- Now you can logon to your u-link account via web page u-link.weidmueller.com using your registered mail address and entered password.




u-link Remote Access Service: Registration Administrator "hartmann@wdm-engineering.de" - Nachricht (HTML)

Nachricht Entwicklertools

Von: Funktionspostfach u-link (Remote Access Service)
An: hartmann@wdm-engineering.de
Cc:
Betreff: u-link Remote Access Service: Registration Administrator "hartmann@wdm-engineering.de"

Gesendet: Mo 13.06.2016 12:11

Weidmüller 

u-link | Remote Access Service

Dear u-link Administrator,

this is an automatically created email, which you have received from the registration service of the Weidmüller u-link Remote Access Portal.

Your administration user account 'hartmann@wdm-engineering.de' of the u-link system account 'WDM Engineering Systems' has been created.

Below user data have been created for your account:

Company:	WDM Engineering Systems
Street:	Braunenbrucher Weg 18
ZIP code:	32758
Location:	Detmold
Country:	Germany
First name:	Heinz
Last name:	Hartmann
Department:	
Function:	
Phone:	+49 5231 14 29 1234
Mobile:	+49 173 123 123 123

Your login name to access the u-link Web portal: hartmann@wdm-engineering.de

You now can logon to the u-link Web portal using either the URL <http://u-link.weidmueller.com> or <http://www.u-link.weidmueller.com>.

Use as login credentials your login name and the password which you have entered during the registration process of your system account.

Download and Registration (Unlock) of the PC-based u-link VPN-Client

To access remote Ethernet devices via the u-link Portal you need to install the Weidmüller u-link VPN client on your PC. This software allows an encrypted and secured access to the u-link VPN-Server.

You can download the software via below link:
<http://www.weidmueller.com/int/products/electronics-and-automation/maintenance-and-cloud-service>
Alternatively you can download the u-link VPN client - after logon to the Web portal - in menu Home > News & Downloads.

To use the u-link VPN client it has to be unlocked and assigned to your u-link user account. Run the software and click button 'Unlock' to start the one-time registration process. During this procedure you will be requested to enter below activation code. After successful registration you can initiate a VPN connection to your u-link account (Click button 'Connect'). Please consider that eventually you have to configure your Proxy parameters (Button 'Configuration') if your Internet access is passing a company Proxy server requiring an user authentication.

Your Registration-/Activation code for u-link VPN client: N2ATYCV6ZWEJ

The registration/activation code also can be retrieved - after logon to the Web portal - in menu Home > User profile (Tab Activation code)

Example of mail “Registration Administrator” which informs you that your system account now is active and that this user account is the Administrator.

Activation code to assign (register) software “u-link VPN client” to this user account.

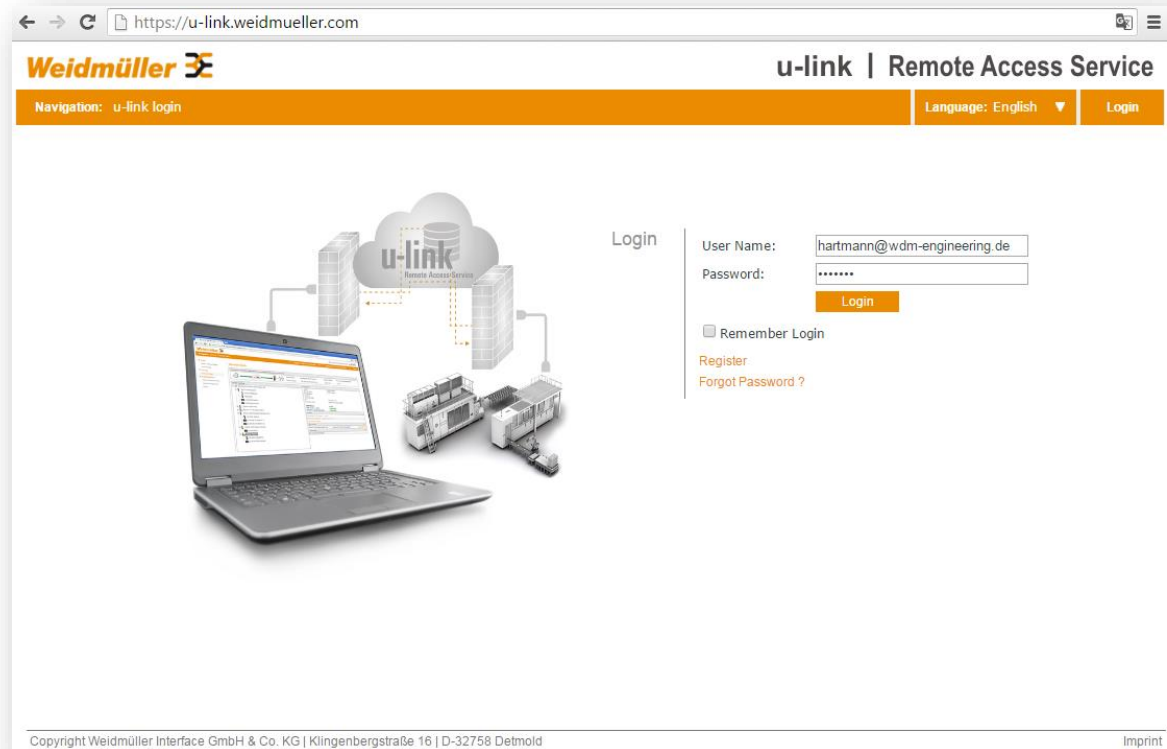
Note: The activation code can be retrieved – when logged on to the u-link portal with this user account – in menu “User Profile / Tab Activation code”.

Chapter 3: Overview features and functions of u-link Web portal

- 3.1 u-link Login page
- 3.2 Menu News & Downloads
- 3.3 Menu User Profile
- 3.4 Menu Service Desk
- 3.5 Menu User Management
- 3.6 Menu Device Management
- 3.7 Menu Account Management

3.1 u-link Login page

- For logon to the u-link Web portal any standard browser is supported.
- Open a browser and enter **u-link.weidmueller.com**
- Login with user name (Mail address) and password of the account creator (is automatically the Administrator).



3.2 Menu ‘News & Downloads’ (Initial state after registration)

- After successful login the menu “News & Downloads” automatically is opened (Home page).
- This page is separated into the 3 sections:
 - “Your profile” → Contains information about the data of the logged-on user.
 - “News from your administrator” → Here any text information can be provided by the local administrator of this account to all other users of this account (Button “Add news”). This text is seen by all users of this u-link system account.
 - “News and Downloads from the u-link global administration team (Weidmüller)” → Here the Weidmüller u-link administration team is providing data (any information, downloads, documents) to all u-link users of all u-link accounts.

The screenshot shows the 'News & Downloads' page of the u-link Remote Access Service. The page is titled 'News & Downloads' and includes a navigation bar with 'Home > News & Downloads', 'Active license: Entry Version', 'Language: English', and 'Logged in as: Heinz Hartmann'. The main content area is divided into three sections: 'News from your administrator', 'News and Downloads from the u-link global administration team (Weidmüller)', and 'Downloads'. A callout box points to the 'News from your administrator' section, stating 'Each created u-link user can see this Web page after login. The section ‘News from your administrator’ only can be maintained by the administrator.' Another callout box points to the 'News and Downloads from the u-link global administration team (Weidmüller)' section, stating 'Please check this section periodically regarding new information, software updates and documentation.' A third callout box points to the 'Active license: Entry Version' text, stating 'Current license is always the ‘Entry Version’ after registration.' A fourth callout box points to the 'Logged in as: Heinz Hartmann' text, stating 'Logged-on user'.

3.3 Menu 'User Profile' (Initial state after registration)

■ **Tab 'User data'**

- Show / Edit the data of logged-on user
- Change Password
- Select default language when logged on
- Select default Home page when logged on

Note: Group membership and User permissions cannot be changed in the Entry-Version. The system account creator automatically is member of group 'Administrators', additionally created users automatically become members of group 'Service'.

■ **Tab 'Status Information'**

- Shows several date and time values for information

■ **Tab 'Activation Code'**

- Activation code: Shows the activation key which this user has to use to register/unlock the PC software "u-link VPN Client".
- State: Has value "**Not used**" as long as the u-link VPN Client never has initiated a VPN connection to u-link.
Has value "**In Use**" after first establishing a VPN connection to u-link.
- Release for additional activation: *If state is 'In Use' and if you want to release a second PC as u-link VPN Client using this activation code you first must enable the checkbox.*

Note 1: Checkbox first can be set if state is 'In Use'!

Note 2: If you release several Service PCs with the same activation code (all are clones from the perspective of the VPN server) be aware that you do not start the VPN connection on these PCs at the same time (A new connection is interrupting the previous one).

The screenshot shows the 'User Profile' page with three tabs: 'User Data', 'Status Information', and 'Activation Code'. The 'User Data' tab is active, showing fields for personal information, contact details, and password management. A 'Save Changes' button is located at the bottom of the form.

Note: The login name is the unique identifier of this account and cannot be changed as long as this account exists.

Each logged-on u-link user can change his own - editable - profile data and set a new password via menu 'User Profile'.

If you change anything do not forget to click button "Save Changes".

Status Information:

Created Date	6/13/2016 12:03:56 PM
Last Login Date	6/14/2016 1:59:59 PM
Last Activity Date	6/14/2016 1:59:59 PM
Last Lock-out Date	-
Last Password Change	-
Password Expires	Never

Activation Code:

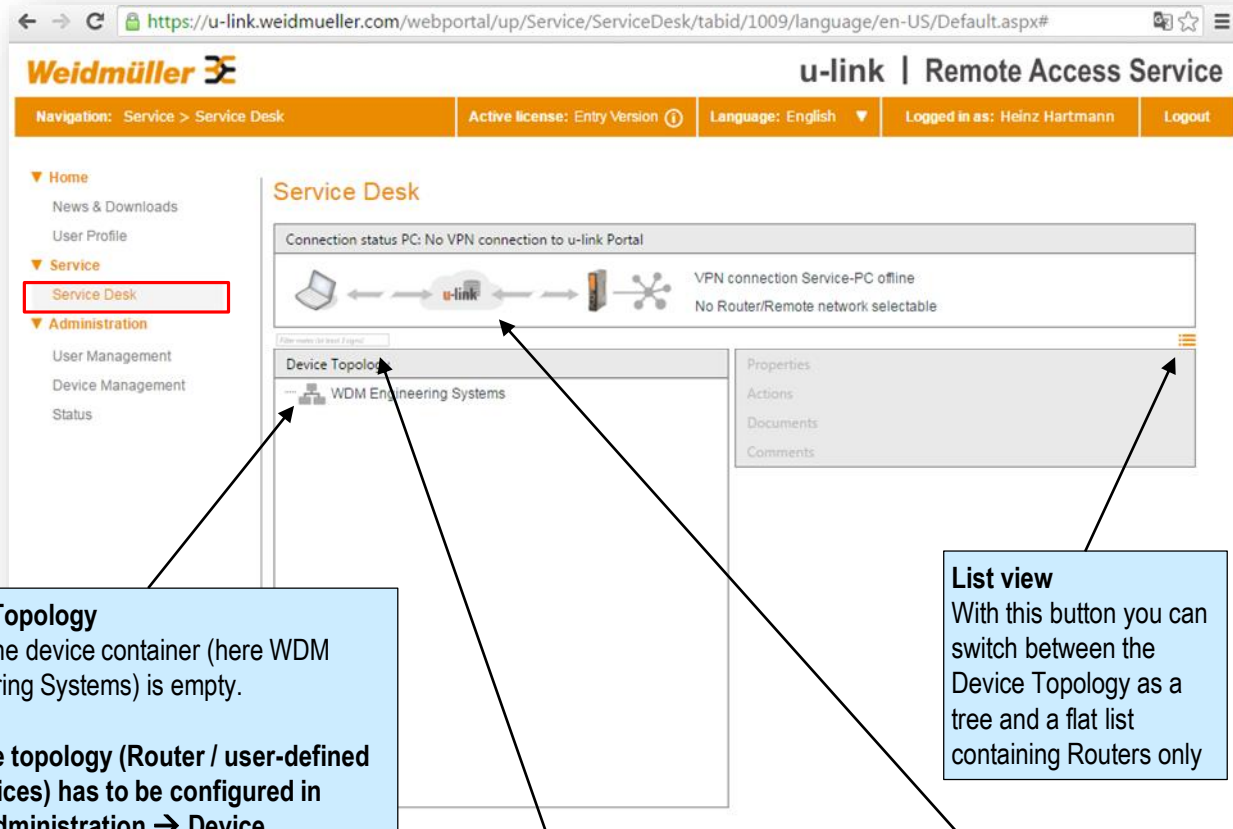
Activation ID	
Activation Code	N2A7YCV6ZWEJ
State	Not used
Release for additional activation	<input type="checkbox"/>

3.4 Menu 'Service Desk' (Initial state after registration)

- This menu will be used for access of remote devices (connecting to remote Router / Network devices).
- The screenshot is displaying the initial status after registering a new u-link system account:

Status after registration:

- No devices configured.
- No active VPN connection of this Service PC to the u-link Portal (The software 'u-link VPN client' still has to be installed and assigned/registered to this administrator account if this account shall be used for remote access).



Device Topology
Initially the device container (here WDM Engineering Systems) is empty.

A device topology (Router / user-defined end devices) has to be configured in menu Administration → Device Management.

The name of the device container automatically is set to the company name which you have entered during the registration process of this u-link system account.

Filter function
When inserting 3 or more characters the Device Topology will only show Routers and end-devices which include these characters

Connection Status PC
This section shows the connection status of the u-link VPN Client (Service PC) which is assigned (registered) to this user account.

The screenshot shows the initial status (no VPN connection to the u-link VPN Server).

List view
With this button you can switch between the Device Topology as a tree and a flat list containing Routers only

3.5 Menu ‘User Management’ (Initial state after registration)

- This menu will be used for creating and configuring the accounts of Service users.
- The screenshot is displaying the initial status after registering a new u-link system account. At this time only the account creator (Administrator) of this u-link account is existent.
- All users are organized into the 2 groups ‘Administrators’ and ‘Service’. In the Entry-Version the account creator automatically is the Administrator belonging to group ‘Administrators’.
- Each new created user will become a member of group ‘Service’.
- The Administrator is allowed to fully maintain the account.
- A Service user may maintain the device topology (creating Routers and user-defined Ethernet devices) via Menu ‘Device Management’ but may not maintain users (Menu ‘User Management’ is hidden).

Creation of a new user

The user who has registered the u-link system account automatically is the account administrator. You can identify him with the orange symbol. This administrator account also can be used for remote access.

A new user can be created via button ‘Add’. Each created user automatically is member of group ‘Service’.

Permissions of users are based on membership of groups ‘Administrators’ and ‘Service’. In the ‘Entry Version’ only these two groups exist and have pre-defined, **not changeable** permissions.

User Management: Maintain users (create, delete, edit)

Device Management: Maintain devices (create, delete, edit remote Routers)

Status: Menu “Account Administration” is visible or hidden

Comments: Add/Delete comments to defined objects (Menu Device Management)

Documents: Add/Delete documents (any file type) to defined objects (Menu Device Management)

New & Downloads: Add/Edit news in menu News & Downloads (This menu generally is visible for all created users)

Group permissions

Type	Name	Description	Permission Management					Actions
			Users	Devices	Status	Comments	Documents	
Group for administrators	Administrators	Group for administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group for service technicians	Service	Group for service technicians	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

3.6 Menu ‘Device Management’ (Initial state after registration)

- This menu will be used to configure device objects (Router, Ethernet-based devices connected to the Router) representing the physical remote devices.
- The screenshot is displaying the initial status after registering a new u-link system account.
 - No devices configured (Container ‘Device Topology’ is empty).
- After finishing the configuration the device topology will be displayed in menu ‘Service Desk’ to initiate a remote access to Ethernet devices via defined Router objects.

Device Topology
Initially the device container (here WDM Engineering Systems) is empty. The name of the device container automatically is set to the company name which you have entered during the registration process of this u-link system account.

Filter function
When inserting 3 or more characters the Device Topology will only show Routers and end-devices which include these characters

Creating new devices
Router objects and Ethernet-based devices for remote access have to be configured by clicking button “New”.

In chapter “4.4 Setup of the Device configuration (u-link Web portal)” you will find a detailed example how to setup a device configuration.

3.7 Menu 'Status' (Initial state after registration)

- This menu is displaying status and license information of this system account.
- When registering a new u-link system account the version always will be the 'Entry Version'. An upgrade to a chargeable 'Standard Version' can be done via button 'Upgrade to Standard-Level'.
- For logging and reporting purposes following information will be provided:
 - Current connections (Service user to Remote Router)
 - Monthly data volume (VPN traffic) of a Service user
 - Connection history (Service user to Remote Router)
 - The VPN traffic and the connection history additionally can be exported to a csv-based text file.

The screenshot shows the 'u-link | Remote Access Service' status page. The navigation bar includes 'Administration > Status', 'Active license: Entry Version', 'Language: English', and 'Logged in as: Heinz Hartmann'. The left sidebar has 'Account Management' selected. The main content area has tabs for 'Status / Statistics', 'Eventlog', 'Password Policy', and 'Account Informations'. The 'Status / Statistics' tab is active, showing:

- Version: Entry-Level (with 'Upgrade to Standard-Level...' button)
- Validity period: Unlimited
- Max. number of simultaneous VPN connections (PC ↔ u-link ↔ Router/Remote network): 2 (0 used)

Below this is a table for 'Currently connected u-link VPN clients':

Name	Type	Connected since	Connected to Router
Heinz-Josef Hartmann	User	1/17/2017 3:32:31 PM	Maschine 1
Maschine 1	Router	1/17/2017 3:33:07 PM	Heinz-Josef Hartmann

Next is the 'VPN Traffic' section for the period 1/1/2017-1/31/2017:

Name	Sent	Received	Total
> External Service User	0.50 MB	0.90 MB	1.40 MB
> Maschine 1	0.40 MB	0.48 MB	0.88 MB
	0.89 MB	1.38 MB	2.28 MB

Finally, the 'Connction Log' section shows a list of connections:

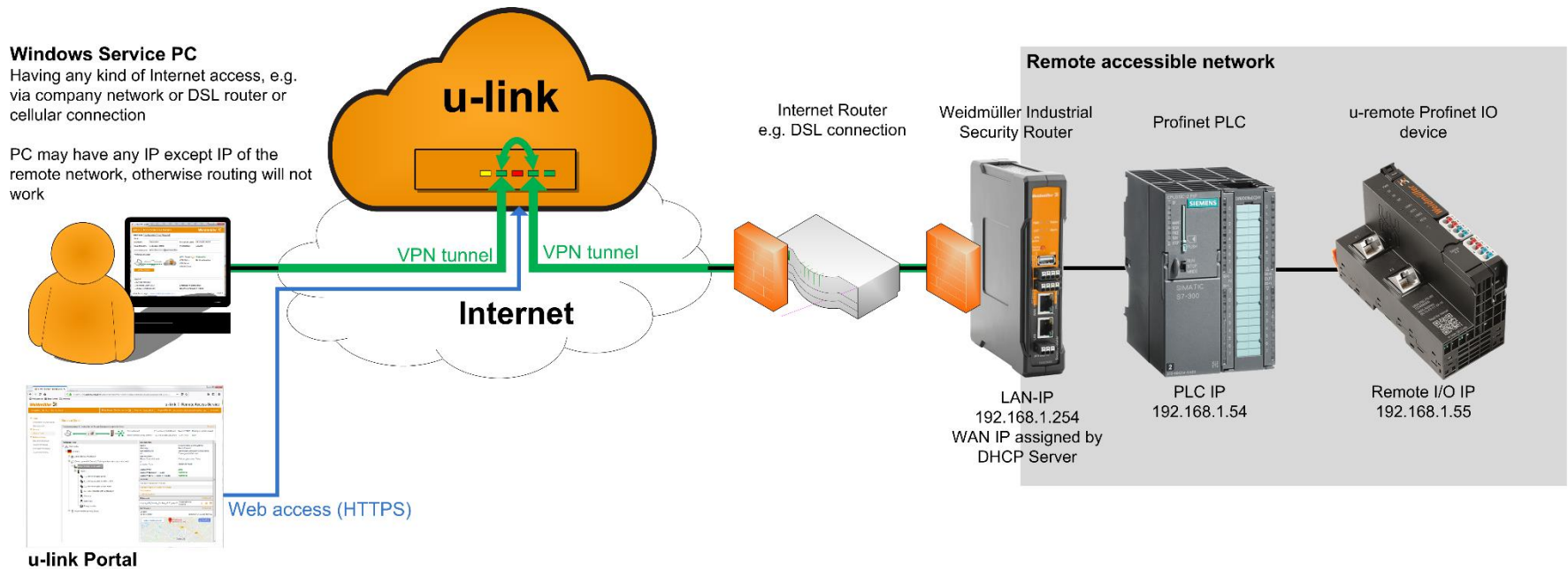
Router	User	Start	End
Maschine 1	External Service User	1/13/2017 2:04:41 PM	1/13/2017 2:24:28 PM
Maschine 1	External Service User	1/16/2017 11:07:27 AM	1/16/2017 12:08:00 PM
Maschine 1	External Service User	1/16/2017 11:07:27 AM	1/16/2017 12:08:00 PM
Maschine 1	External Service User	1/16/2017 12:42:58 PM	1/16/2017 12:44:21 PM
Maschine 1	External Service User	1/16/2017 12:42:58 PM	1/16/2017 12:44:21 PM
Maschine 1	External Service User	1/16/2017 12:44:29 PM	1/16/2017 2:50:36 PM
Maschine 1	External Service User	1/16/2017 4:04:27 PM	1/16/2017 4:05:45 PM
Maschine 1	External Service User	1/16/2017 4:06:27 PM	1/16/2017 4:49:11 PM

A callout box points to the 'Upgrade to Standard-Level...' button, stating: 'This button is only visible when logged-in as Administrator. When entering the license code of a 'Standard Version' the extended features will be provided immediately.'

Chapter 4: Setup of a remote access scenario (Example)

- 4.1 Illustration of sample application
- 4.2 Creating a new user account (u-link Web portal)
- 4.3 Administration of a user account (u-link Web portal)
- 4.4 Setup of the Device configuration (u-link Web portal)
- 4.5 Preparing of the Service PC
- 4.6 Configuration of the Router

4. 1 Illustration of sample application (Setup described on next slides)



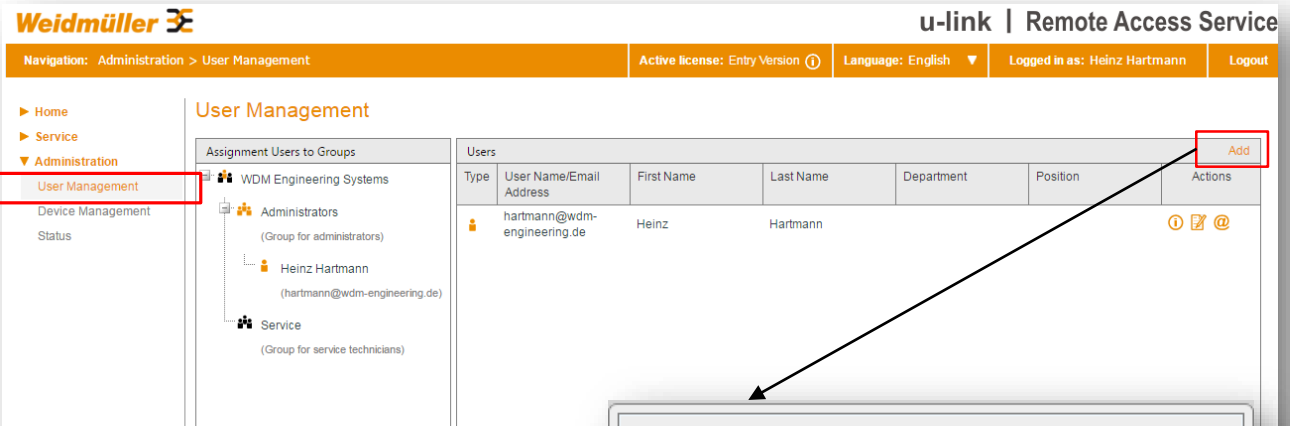
4.2 Creating a new user account (u-link Web portal)

Creating a new Service user (Step 1)

Note:

After registration of a new u-link system account only the administrator account exists. For doing a remote access the administration account also can be used, there is no need to create an additional service user. Next slides describe how to create and maintain a service user. For the later described example of a remote access session the administrator account is used, not the service user which we will create on the next slides.

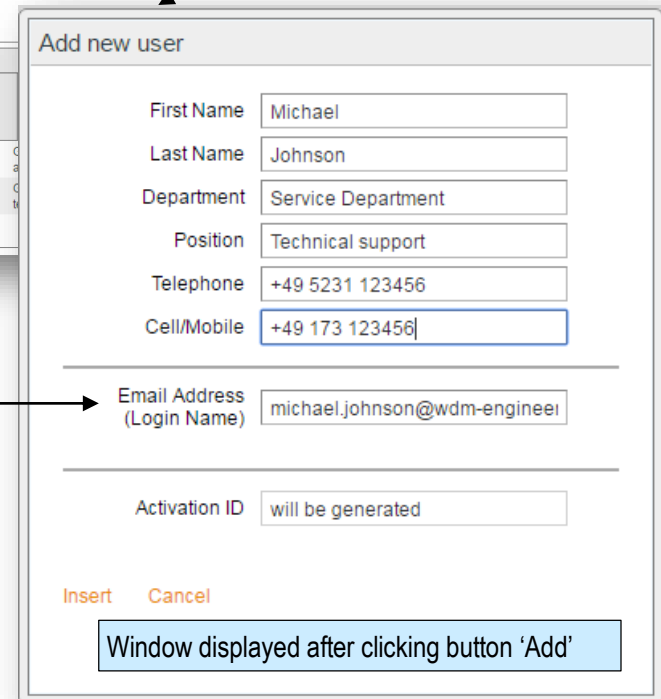
- Goto menu 'User Management'.
- Click button 'Add' in section 'Users'.
 - A new window will be displayed to enter the user data.
- Enter the describing user data.
- Enter the users mail address.
 - It will be used for Login to the u-link Web portal.
- Click button 'Insert'.
 - Now the user will be created.
 - The activation code for registering the u-link VPN client of this user automatically will be generated.



The screenshot shows the 'User Management' interface. The 'Users' table contains one entry for Heinz Hartmann. The 'Add' button in the 'Actions' column is highlighted with a red box. A black arrow points from this button to the 'Add new user' dialog box.

Attention:

- The Login name (mail address) is used as unique identifier of this user account inside of the global u-link system.
- It may be used only one time inside of the global u-link system.
- The Login name cannot be changed and cannot be used a second time as long as this user accounts exists.
- If a new user has been created using a wrong or not existent mail address (eg. happened due to a typo) then the automatically created 'User registration mail' (after clicking 'Insert') never can be delivered. In this case please delete the user and create a new one using the correct mail address.



The 'Add new user' dialog box contains the following fields:

- First Name: Michael
- Last Name: Johnson
- Department: Service Department
- Position: Technical support
- Telephone: +49 5231 123456
- Cell/Mobile: +49 173 123456
- Email Address (Login Name): michael.johnson@wdm-engineer
- Activation ID: will be generated

Buttons: Insert, Cancel

Window displayed after clicking button 'Add'

4.2 Creating a new user account (u-link Web portal)

Creating a new Service user (Step 2)

- As next step the new user will be informed by mail that the administrator has created a u-link user account.
- After clicking button 'Insert' this window will be displayed to send the 'User registration mail' to the mail address of field 'Destination address'.
- Click button 'Send email'.
 - The recipient will receive a mail of type 'Registration User' from sender address **u-link-noreply@weidmueller.com**.

The screenshot shows a web form titled "Add new user -> Info mail to user". The form contains the following fields:

- First Name: Michael
- Last Name: Johnson
- Department: Service Department
- Position: Technical support
- Telephone: +49 5231 123456
- Cell/Mobile: +49 173 123456
- Email Address (Login Name): michael.johnson@wdm-engineer
- Activation ID: UV84Z6XFJTZ2
- Destination address: michael.johnson@wdm-engineer
- Sender address: u-link-noreply@weidmueller.com

At the bottom of the form are two buttons: "Send email" and "Information".

Callouts from the screenshot:

- Window displayed after clicking button 'Insert' (points to the top of the form).
- Now the unique activation code is created to be used for registering the 'u-link VPN client' on a Service PC. (points to the Activation ID field).
- This window is displayed after clicking button 'Information' (points to the Information window below).

Information about u-link accessibility of this new user

The user account has been created. Now you have to send an email to the user containing the entered data and a Hyperlink for setting an initial password to log into the u-link Web portal.

The initial password setting via the Hyperlink is mandatory otherwise a login into the u-link Web portal is not possible.

Note:
If you - as administrator - would like to activate the users u-link access and to set a password by yourself then please change the content of parameter „Destination address“ to your mail address. Then you will receive the mail instead of the created user.

Note:
By default the 'User registration mail' is sent to the mail address which is used for user login. For this reason both the mail address (Login name) and the destination address are the same.

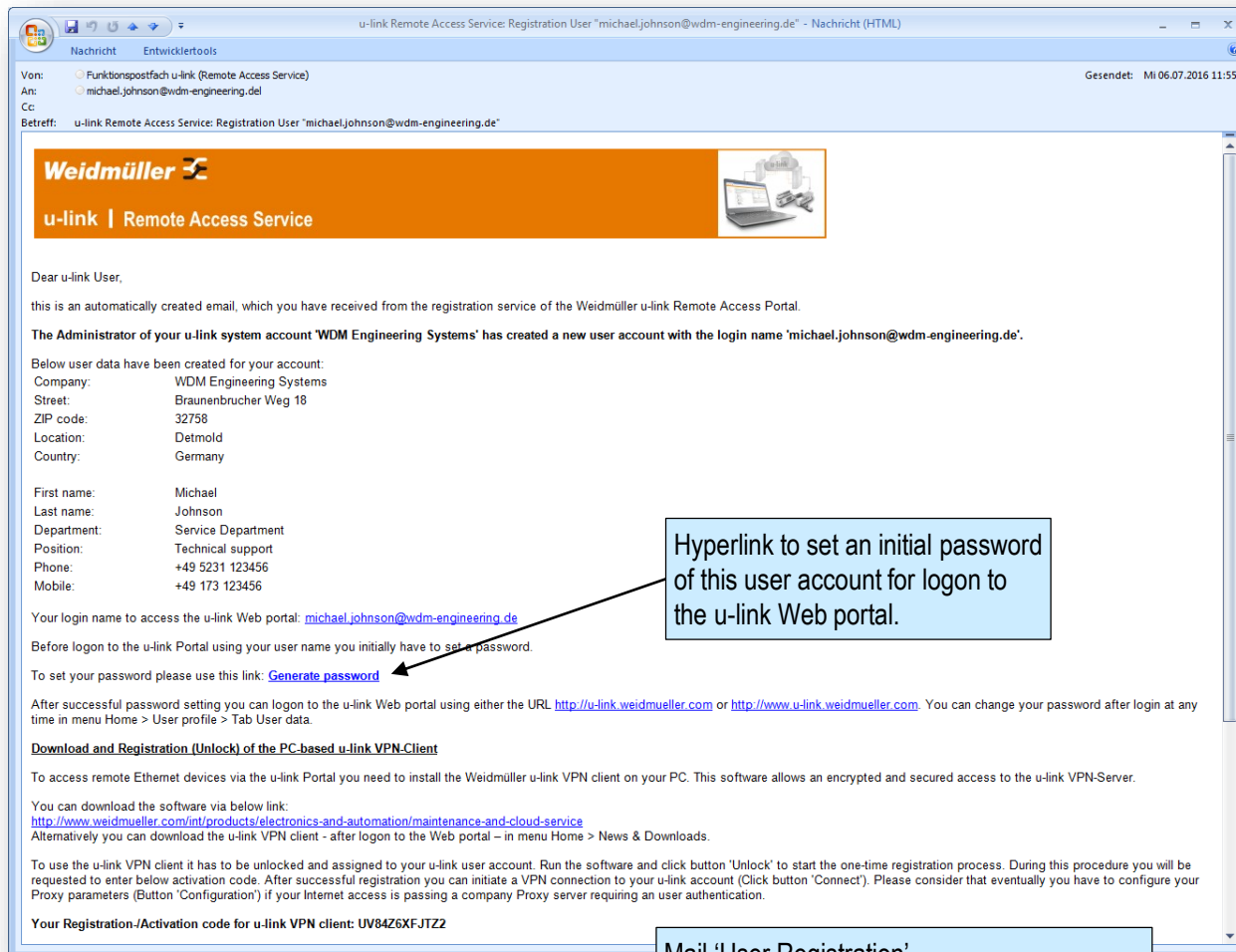
If the user registration mail shall be sent to a different mail address (for example to the administrator) then change the destination address to the desired target mail address.

4.2 Creating a new user account (u-link Web portal)

Creating a new Service user (Step 3)

(Note: Step 3 is a To-Do by new Service user)

- Screenshot shows the mail (Type 'User Registration') which the new user has received from the u-link administrator.
 - At his time the user account already is active but before login to the u-link Web portal the new user has to set an initial password.
- Open the mail.
- Click hyperlink 'Generate password'.
- Now the u-link Web page 'Create password' will be opened to enter the initial password of this user.



Hyperlink to set an initial password of this user account for logon to the u-link Web portal.

Mail 'User Registration' (sent by Administrator in previous step to recipient 'Destination address')

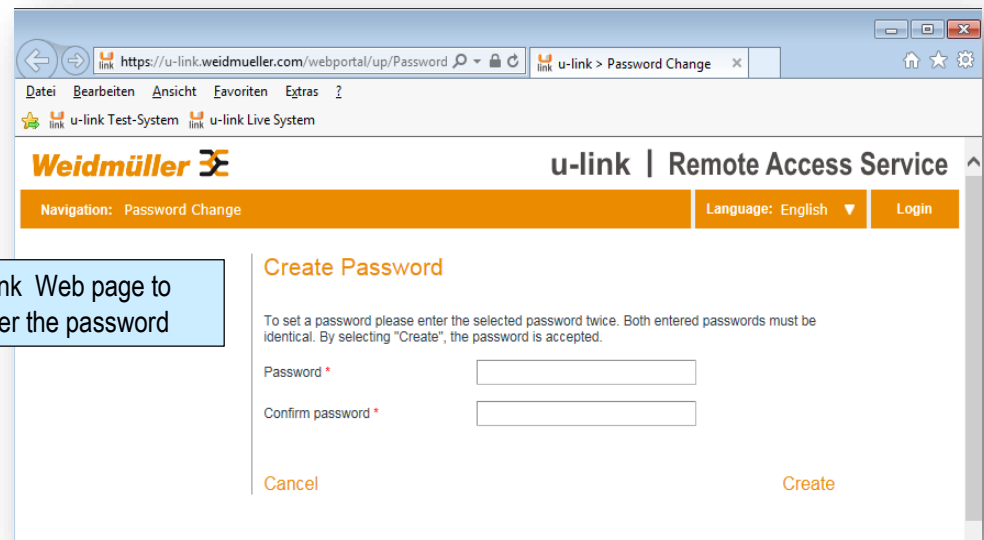
4.2 Creating a new user account (u-link Web portal)

Creating a new Service user (Step 4)

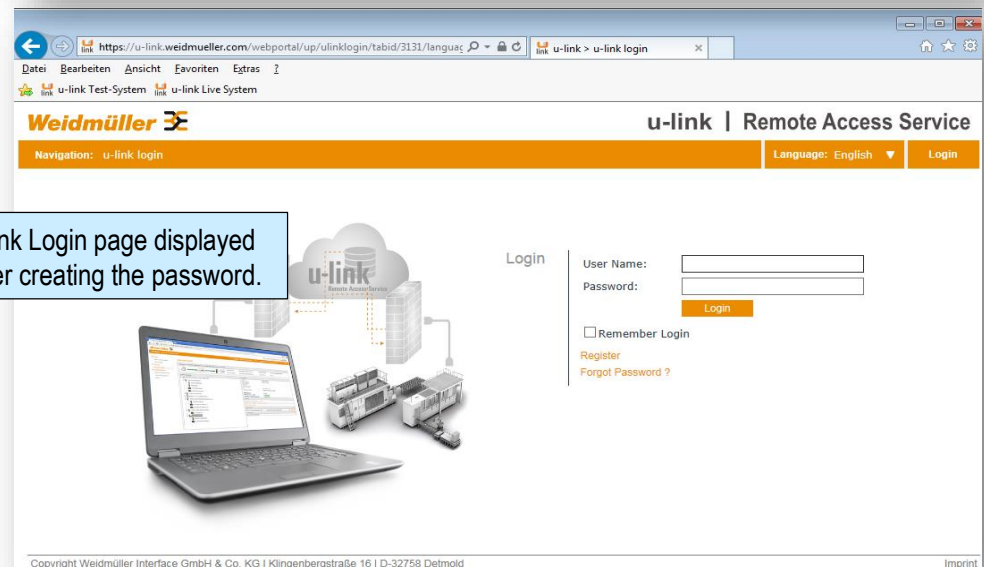
(Note: Step 4 is a To-Do by new Service user)

- Screenshot shows u-link Web page „Create password“ which will be opened after clicking hyperlink ‘Generate password’ in user registration’ mail.
 - Enter the password twice.
 - Click button ‘Create’.
 - After successful creation the u-link Login page is displayed.
- Now the user can login to the u-link Web portal using his login name (mail address) and the entered password.

u-link Web page to enter the password



u-link Login page displayed after creating the password.



4.2 Creating a new user account (u-link Web portal)

Creating a new Service user (Step 5)

- The new user now is displayed in section 'Users' and automatically assigned to group 'Service'.
- The permissions of this user are based on the permissions of group 'Service' having following rights:
 - User Management is prohibited (only allowed for Administrator account).
 - Device Management is allowed (Create/Maintain Routers and user-defined end devices).
 - Access to Menu 'Account Management' is allowed.
 - Documents and Comments can be stored to defined device objects (Menu Device Management).
 - Creation of information messages in Menu 'News & Downloads' is prohibited.
- The permissions cannot be changed in the Entry-Version.

Type	User Name/Email Address	First Name	Last Name	Department	Position	Actions
	hartmann@wdm-engineering.de	Heinz	Hartmann			🔍 📧 📧
	michael.johnson@wdm-engineering.de	Michael	Johnson	Service Department	Technical support	🔍 📧 📧 🗑️

Type	Name	Description	Permission Management					Actions	
			Users	Devices	Status	Comments	Documents		News & Downloads
	Administrators	Group for administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	🔍
	Service	Group for service technicians	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	🔍

Type	User Name/Email Address	First Name	Last Name	Department	Position	Actions
	hartmann@wdm-engineering.de	Heinz	Hartmann			🔍 📧 📧
	michael.johnson@wdm-engineering.de	Michael	Johnson	Service Department	Technical support	🔍 📧 📧 🗑️

Sort Ascending
Sort Descending
Clear Sorting
Best Fit
Columns

<input checked="" type="checkbox"/> Type
<input checked="" type="checkbox"/> User Name/Email Address
<input checked="" type="checkbox"/> First Name
<input checked="" type="checkbox"/> Last Name
<input checked="" type="checkbox"/> Department
<input checked="" type="checkbox"/> Position
<input type="checkbox"/> Telephone
<input type="checkbox"/> Cell/Mobile
<input type="checkbox"/> Activation code
<input type="checkbox"/> Authorised

4.3 Administration of an user account

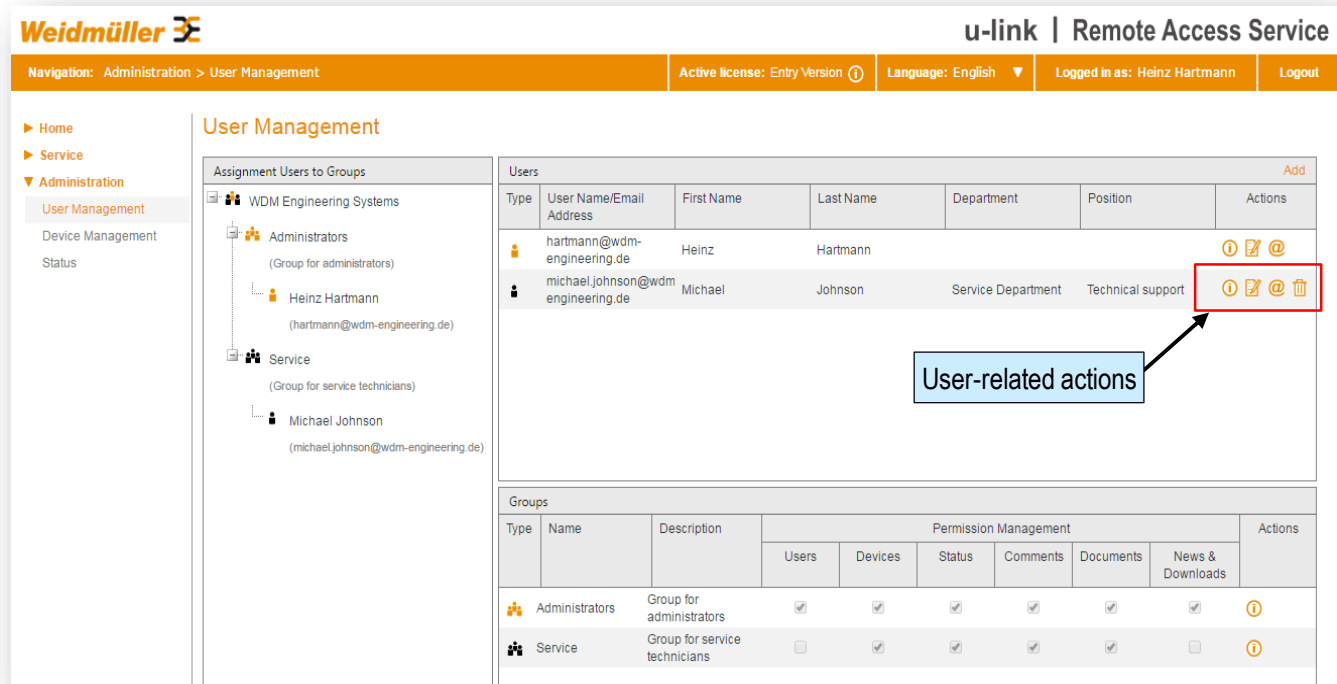
4.3 Administration of an user account (u-link Web portal)

Actions to maintain a service user

- Following user-related actions are provided:
 - View user data
 - Edit user data
 - Send an information mail to user containing the user data
 - Delete the user account

Note:

The administration of user accounts only can be done by the Administrator. The menu item 'User Management' is not visible for service users.



u-link | Remote Access Service

Navigation: Administration > User Management Active license: Entry Version Language: English Logged in as: Heinz Hartmann Logout

User Management

Assignment Users to Groups

- WDM Engineering Systems
 - Administrators (Group for administrators)
 - Heinz Hartmann (hartmann@wdm-engineering.de)
 - Service (Group for service technicians)
 - Michael Johnson (michael.johnson@wdm-engineering.de)

Type	User Name/Email Address	First Name	Last Name	Department	Position	Actions
	hartmann@wdm-engineering.de	Heinz	Hartmann			ⓘ ⚙ @
	michael.johnson@wdm-engineering.de	Michael	Johnson	Service Department	Technical support	ⓘ ⚙ @ 🗑

Groups

Type	Name	Description	Permission Management					Actions	
			Users	Devices	Status	Comments	Documents		News & Downloads
	Administrators	Group for administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ⓘ
	Service	Group for service technicians	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ⓘ

4.3 Administration of an user account (u-link Web portal)

Action 'View user data'

- Click button 'View' to open a new window showing the user data on tabs
 - User Data
 - Status Information
 - Activation Code
- In viewing mode no data can be changed.

Type	User Name/Email Address	First Name	Last Name	Department	Position	Actions
	hartmann@wdm-engineering.de	Heinz	Hartmann			
	michael.johnson@wdm-engineering.de	Michael	Johnson	Service Department	Technical support	

Button 'View User Data'

View user data (Michael Johnson)

User Data Status Information Activation Code

User data

First Name: Michael
 Last Name: Johnson
 Department: Service Department
 Position: Technical support
 Telephone: +49 5231 123456
 Cell/Mobile: +49 173 123456
 Email Address (Login Name): michael.johnson@wdm-engineer

Profile

Group member from: Service

User permission (Automatically assigned by group membership)

User management
 Device management
 Status
 Comment management
 Document management
 News&Downloads

Language: English
 Home page: News & Downloads
 Authorised: Yes
 Administrator: No

Close

View user data (Michael Johnson)

User Data **Status Information** Activation Code

Status Information

Created Date: 7/6/2016 11:43:52 AM
 Last Login Date: -
 Last Activity Date: -
 Last Lock-out Date: -
 Last Password Change: -
 Password Expires: Never

Close

View user data (Michael Johnson)

User Data Status Information **Activation Code**

Activation ID

Activation Code: UV84Z6XFJTZ2
 State: Not used

Close

After first VPN connection of this service user to the u-link VPN server the status is changed to 'In Use'.

4.3 Administration of an user account (u-link Web portal)

Action 'Edit user data'

- Click button 'Edit' to open a new window showing the user data on tabs
 - User Data
 - Activation Code
- In this mode data can be changed.

Type	User Name/Email Address	First Name	Last Name	Department	Position	Actions
	hartmann@wdm-engineering.de	Heinz	Hartmann			
	michael.johnson@wdm-engineering.de	Michael	Johnson	Service Department	Technical support	

Button 'Edit User Data'

Changeable parameters

Not changeable parameters (Permissions assigned by group membership)

Default language when logged in to u-link Portal

Default Home page when logged in to u-link Portal

Set if User is working from China or not.

Activate / Deactivate the users u-link access.

Activation Code

Activation Code: UV84Z6XFJTZ2

State: Not used

Release for additional activation:

Activation Code

Activation Code: UV84Z6XFJTZ2

State: Not used

Release for additional activation:

Activation Code

Activation Code: UV84Z6XFJTZ2

State: Not used

Release for additional activation:

If you want to use a second PC running as 'u-link VPN Client' using this activation code then - if state is 'In Use' - you first must enable the checkbox 'Release for additional activation' to allow an additional use.

Note 1: Checkbox first can be set if state is 'In Use' (is changed when service user first time connects to u-link).

Note 2: If you release several Service PCs with the same activation code be aware that you do not start a VPN connection on these PCs at the same time. All are VPN connections are identical clones from the perspective of the VPN server. If you would do this a new connection is interrupting the previous one).

If set to 'Yes' then this user will be the new Administrator having full permissions.
Attention: The current administrator will be become a Service user (Member of group 'Service') having these limited group permissions.

Password change by Administrator

4.3 Administration of an user account (u-link Web portal)

Action 'Send information mail to user'

- Click button '@' to open a new window for sending an information mail (containing the user data) to the users mail address.

Type	User Name/Email Address	First Name	Last Name	Department	Position	Actions
	hartmann@wdm-engineering.de	Heinz	Hartmann			
	michael.johnson@wdm-engineering.de	Michael	Johnson	Service Department	Technical support	

Button 'Send mail with user data'

This window will be displayed after clicking button '@'.

Send info mail to user again

First Name:

Last Name:

Department:

Position:

Telephone:

Cell/Mobile:

Email Address (Login Name):

Activation ID:

Destination address:

Sender address:

Note: Mail can be sent to a different recipient by changing the content of field "Destination address"

u-link Remote Access Service Information User "michael.johnson@wdm-engineering.de" - Nachricht (HTML)

Von: Funktionspostfach u-link (Remote Access Service)
An: michael.johnson@wdm-engineering.de
Cc:
Betreff: u-link Remote Access Service: Information User "michael.johnson@wdm-engineering.de"

Weidmüller
u-link | Remote Access Service

Dear u-link User,

this is an automatically created email, which you have received from the registration service of the Weidmüller u-link Remote Access Portal.

The Administrator of your u-link account 'WDM Engineering Systems' has sent this mail - containing your user account data - for your information.

Below user data have been created for your account:

Company: WDM Engineering Systems
Street: Braunenbrucher Weg 18
ZIP code: 32758
Location: Detmold
Country: Germany

First name: Michael
Last name: Johnson
Department: Service Department
Position: Technical support
Phone: +49 5231 123456
Mobile: +49 173 123456

Your login name to access the u-link Web portal: michael.johnson@wdm-engineering.de

For logon to the u-link Portal please enter your user name and your valid password. This you either have set initially during the activation process of your user account (refer to your received mail "u-link Registration User") or you have already changed it after first logon to the u-link Web portal.

Link to u-link login: <http://u-link.weidmueller.com> or <http://www.u-link.weidmueller.com>

Download and Registration (Unlock) of the PC-based u-link VPN Client

To access remote Ethernet devices via the u-link Portal you need to install the Weidmüller u-link VPN client on your PC. This software allows an encrypted and secured access to the u-link VPN-Server.

You can download the software via below link:
<http://www.weidmueller.com/int/products/electronics-and-automation/maintenance-and-cloud-service>
Alternatively you can download the u-link VPN client - after logon to the Web portal - in menu Home > News & Downloads.

To use the u-link VPN client it has to be unlocked and assigned to your u-link user account. Run the software and click button 'Unlock' to start the one-time registration process. During this procedure you will be requested to enter below activation code. After successful registration you can initiate a VPN connection to your u-link account (Click button 'Connect'). Please consider that eventually you have to configure your Proxy parameters (Button 'Configuration') if your Internet access is passing a company Proxy server requiring an user authentication.

Your Registration-/Activation code for u-link VPN client: UV84Z6XFJTZ2










The registration/activation code also can be retrieved - after logon to the Web portal - in menu Home > User profile (Tab Activation code)

Sample mail which the addressed service user will receive.

4.3 Administration of an user account (u-link Web portal)

Action 'Delete user'

- Click button 'Delete' to delete the user.
 - A window will appear asking you if you are sure to delete the user. After confirmation the user will be deleted.
 - The list user item in the section 'Users' will be removed.
 - After deletion the mail address used for user login then can be used again.

Users Add						
Type	User Name/Email Address	First Name	Last Name	Department	Position	Actions
	hartmann@wdm-engineering.de	Heinz	Hartmann			  
	michael.johnson@wdm-engineering.de	Michael	Johnson	Service Department	Technical support	   

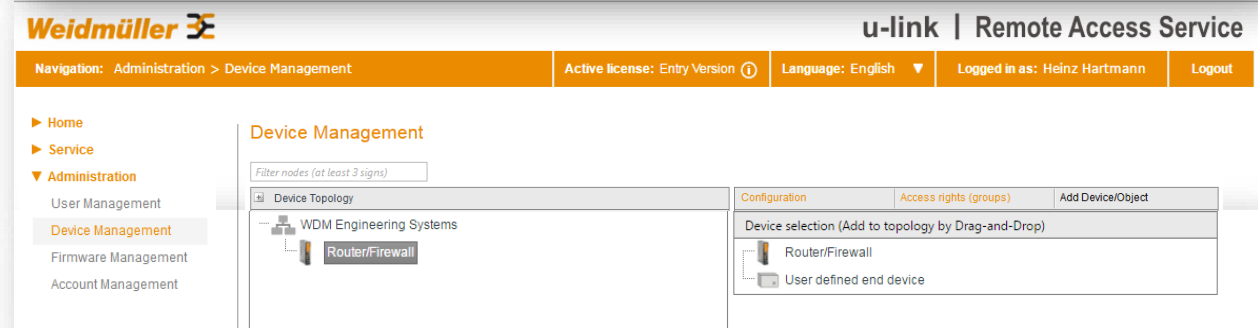
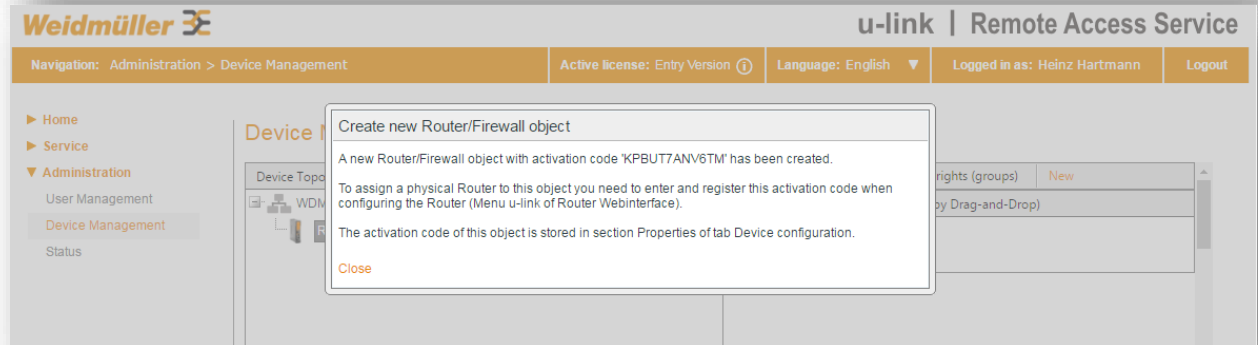
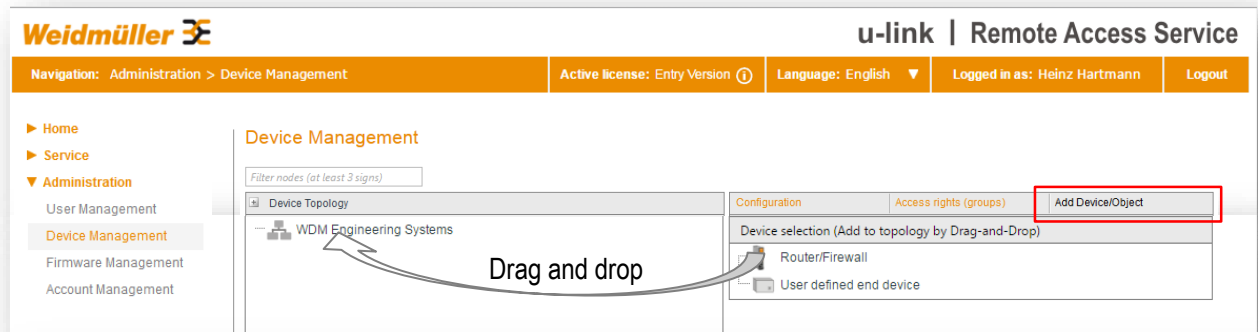
Button 'Delete user'

4.4 Setup of the Device configuration

4.4 Setup of the Device configuration (u-link Web portal)

Create a Router object (Step 1)

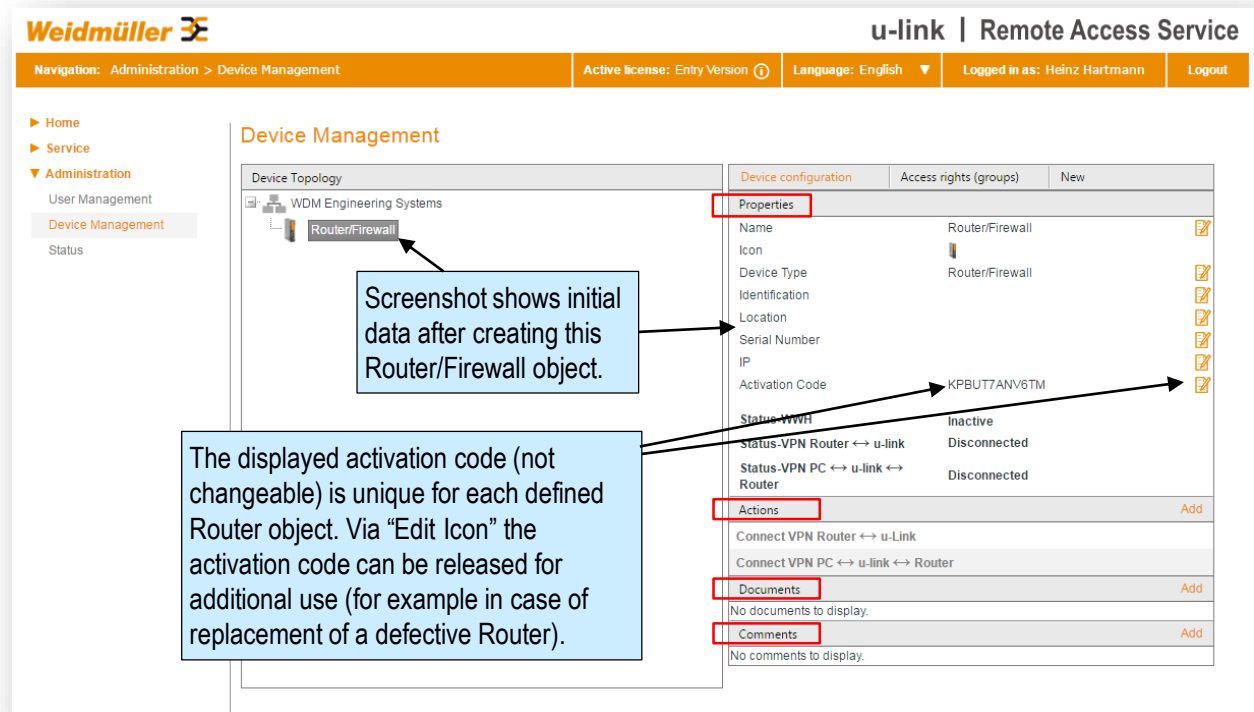
- Goto menu “Device Management”.
- Click Tab “New” to configure the first Router object (access point to devices at remote network).
- Drag the Router/Firewall object from “Device selection” and drop it on the container object in ‘Device Topology’.
- An information window will be displayed showing that this action was accepted. By creating a Router object an unique activation code will be created, which later has to be used to assign a physical Router to this defined object.
- Now the new Router object is defined as first device in the device topology container.
- Next the properties of this Router object have to be configured.



4.4 Setup of the Device configuration (u-link Web portal)

Configuration of properties of new Router object (Step 2)

- Highlight the Router/Firewall object and click Tab “Device configuration” to display object specific item parameters.
- Section **“Properties”**
All items with an “Edit Icon” (except parameter Activation code) can be edited to store individual data to this object. These parameters (text-based fields) are used only for information. They have no relevance regarding the remote access functionality.
- Section **„Actions“**
By default the 2 actions **Connect VPN Router ↔ u-link** and **Connect VPN PC ↔ u-link ↔ Router** are predefined.
First action can be used to start a VPN connection on the Router to the u-link VPN Server remotely from the u-link Portal (via WWH function).
Second action will be used to initiate a VPN pass-through connection from a Service PC via u-link VPN Server to the Router (to access remote devices).
Via button „Add“ customized actions (currently only http/https based calls) can be defined and started via mouse click.
Note: Actions are only active in menu „Service Desk“



u-link | Remote Access Service

Navigation: Administration > Device Management | Active license: Entry Version | Language: English | Logged in as: Heinz Hartmann | Logout

Device Management

Device Topology: WDM Engineering Systems > Router/Firewall

Device configuration	Access rights (groups)	New
Properties		
Name	Router/Firewall	[Edit]
Icon	[Icon]	[Edit]
Device Type	Router/Firewall	[Edit]
Identification		[Edit]
Location		[Edit]
Serial Number		[Edit]
IP		[Edit]
Activation Code	KPBUT7ANV6TM	[Edit]
Status-WWH	Inactive	
Status-VPN Router ↔ u-link	Disconnected	
Status-VPN PC ↔ u-link ↔ Router	Disconnected	
Actions Add		
Connect VPN Router ↔ u-Link		
Connect VPN PC ↔ u-link ↔ Router		
Documents Add		
No documents to display.		
Comments Add		
No comments to display.		

Screenshot shows initial data after creating this Router/Firewall object.

The displayed activation code (not changeable) is unique for each defined Router object. Via “Edit Icon” the activation code can be released for additional use (for example in case of replacement of a defective Router).

- Section **“Documents”**
Storing/Retrieving documents (any file type) assigned to this object. Can be done by all u-link account users.
- Section **„Comments“**
Creating any comments (information) to this object. Useable by all u-link account users.

Note:

For preparing a remote access session via a Router (which will be assigned to this Router object) you only need the activation code. Copy and save this activation code which later is necessary when preparing the physical Router for u-link access.

For a remote access session it is not necessary to edit anything. But we recommend to edit the text-based fields in section “Properties” to better identify the defined object.

4.4 Setup of the Device configuration (u-link Web portal)

Screenshot of created Router object after changing the values of some parameters in section Properties.

Changed name also is displayed in section Device Topology

This screenshot shows the - on previously slide - created Router object after changing the properties of this Router object.

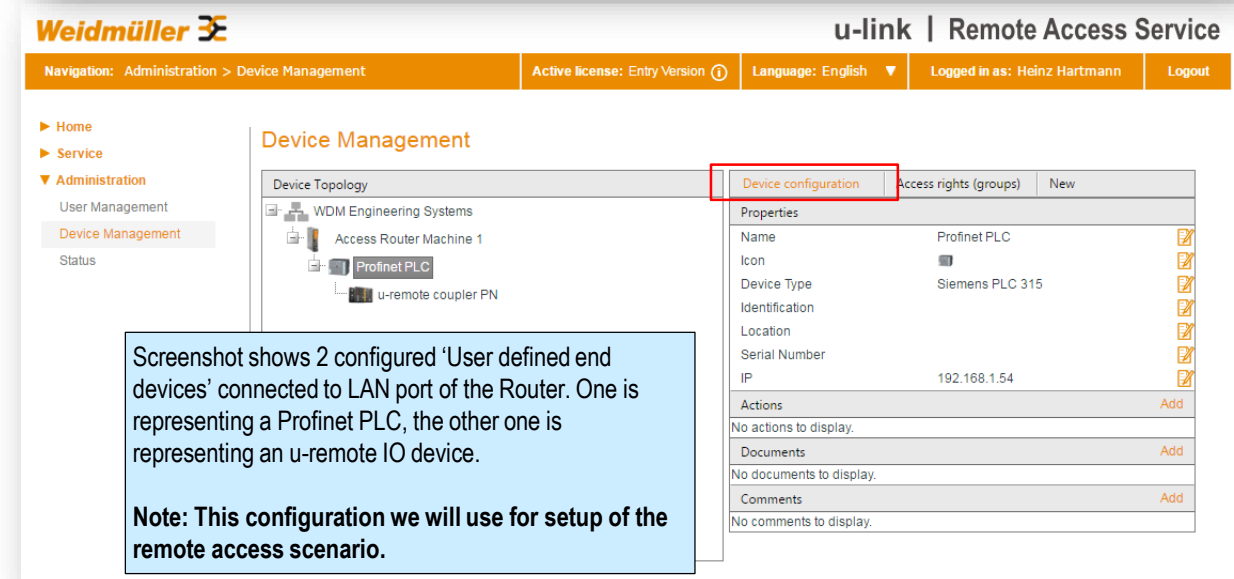
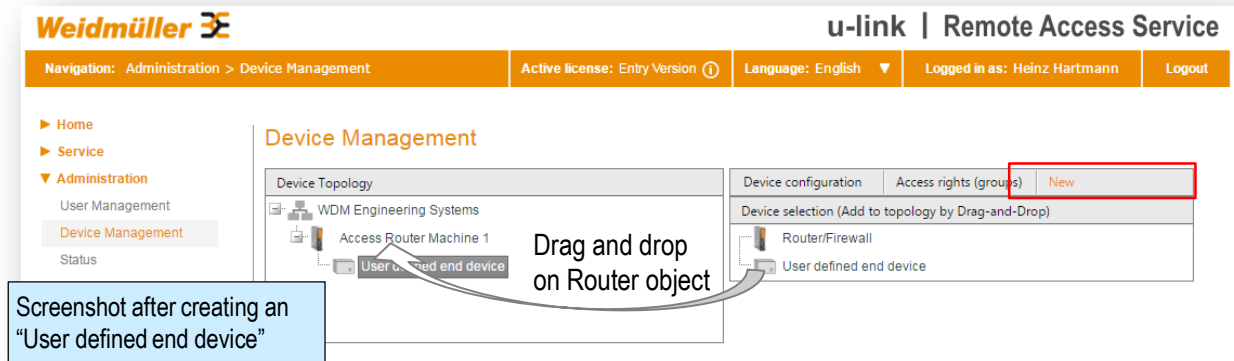
Device configuration		Access rights (groups)	New
Properties			
Name	Access Router Machine 1		
Icon			
Device Type	Router/Firewall		
Identification			
Location	Factory Detmold		
Serial Number			
IP	192.168.1.254 (LAN port)		
Activation Code	KPBUT7ANV6TM		
Status-WWH	Inactive		
Status-VPN Router ↔ u-link	Disconnected		
Status-VPN PC ↔ u-link ↔ Router	Disconnected		
Actions Add			
Connect VPN Router ↔ u-Link			
Connect VPN PC ↔ u-link ↔ Router			
Open Router Web page 📄 🗑️			
Documents Add			
Backup_Router_Configuration.cf2	Configuration Backup of this Router		↓ 📄 🗑️
Comments Add			
Comment to Machine 1			
By Heinz Hartmann		Created at 6/15/2016 4:03:49 PM	
Any information which is visible for all users of this u-link system account. 📄 🗑️			

4.4 Setup of the Device configuration (u-link Web portal)

Configuration of a 'User defined end device' connected to Router LAN port (Step 3)

- The object type „User defined end device“ can be used to define any device type being accessible by an Ethernet communication (TCP/UDP).
- This object type will be used to provide a mapping of remote accessible devices behind the Router. It is not necessary to create 'User defined end devices' for remote access because all IP addresses at Router LAN port are accessible when having a pass-through VPN connection to the Router.

- Select Tab 'New'
- Drag from 'Device selection' the object 'User defined end device' and drop to the container object 'Access Router Machine 1'.
- Click Tab 'Device configuration' and configure the object specific properties as you want (Screenshot shows 2 already configured 'User-defined end devices'). These parameters (text-based fields) are used only for information. They have no relevance regarding the remote access functionality.
- Same as for a Router object the features 'Actions', 'Storing documents and comments' are provided for this object type.



Preparing of the device configuration now is finished !

In the next steps both the Service PC (using this administrator account) and the physical Router (which later is located in the remote network) have to be configured.

4.5 Preparing of the Service PC

Install and configure the u-link VPN client software

4.5 u-link VPN Client → Download and Installation

Download u-link VPN Client

- Logon to the u-link Web portal using your user name and password
- Goto menu “News & Downloads”
- Download the provided software from section “News and Downloads from global u-link administration”

Unzip the downloaded file and install the software

- For installation you may need admin rights.

Important notes:

- A newer VPN client (e.g. V2.0.129) can be installed without de-installation of an already installed Client (e.g. V2.0.36).
- An already registered user account automatically is taken over. If no user account is registered then please go to tab „Configuration“ and click button „Register user profile“. This starts the registration process.



Navigation: Home > News & Downloads | Active license: Standard Version | Language: English | Logged in as

Home | News & Downloads | User Profile | Service | Administration

News & Downloads

Welcome to the u-link Remote Access Service

News from your administrator Add news

Dies ist eine Info vom lokalen Admin. 1/27/2016

News and Downloads from the u-link global administration team (Weidmüller)

Update September 20, 2018

- New Router firmware Version 3.2.3 / Build 86546 available!
- Update urgently recommended if earlier version 3.2.0 / Build 78729 is installed.

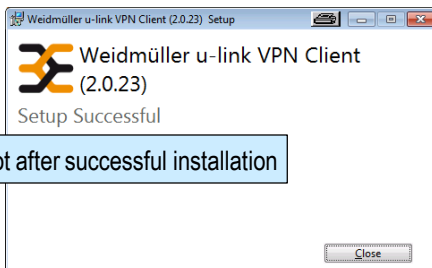
Downloads:

1. u-link Introduction / Overview (PDF, English): [Download](#) (Updated March 28, 2017)
2. u-link Technical User Guide V1.4.3 (PDF, English): [Download](#) (Updated July 18, 2018)
3. u-link VPN client for Windows PCs V2.0.129 (ZIP): [Download](#) (Updated July 16, 2018)

[Notes about upgrading to version 2.0.129](#)

1. New version provides major improvements regarding general useability and failure management.
2. Improvements regarding compatibility with other OpenVPN Tap adapters.
3. Implementation of new u-link WWW and VPN server addresses.
 vpn1-we.aw-cp-de 52.166.202.111
 vpn1-ne.aw-cp-de 52.169.106.31
 www1-we.aw-cp-de 13.81.4.92
 www1-ne.aw-cp-de 52.169.107.229
4. Uptade to new OpenVPN version 2.3.18

With installation of the new client also the new servers are used! This may cause the need to adapt firewall settings!



Screenshot after successful installation

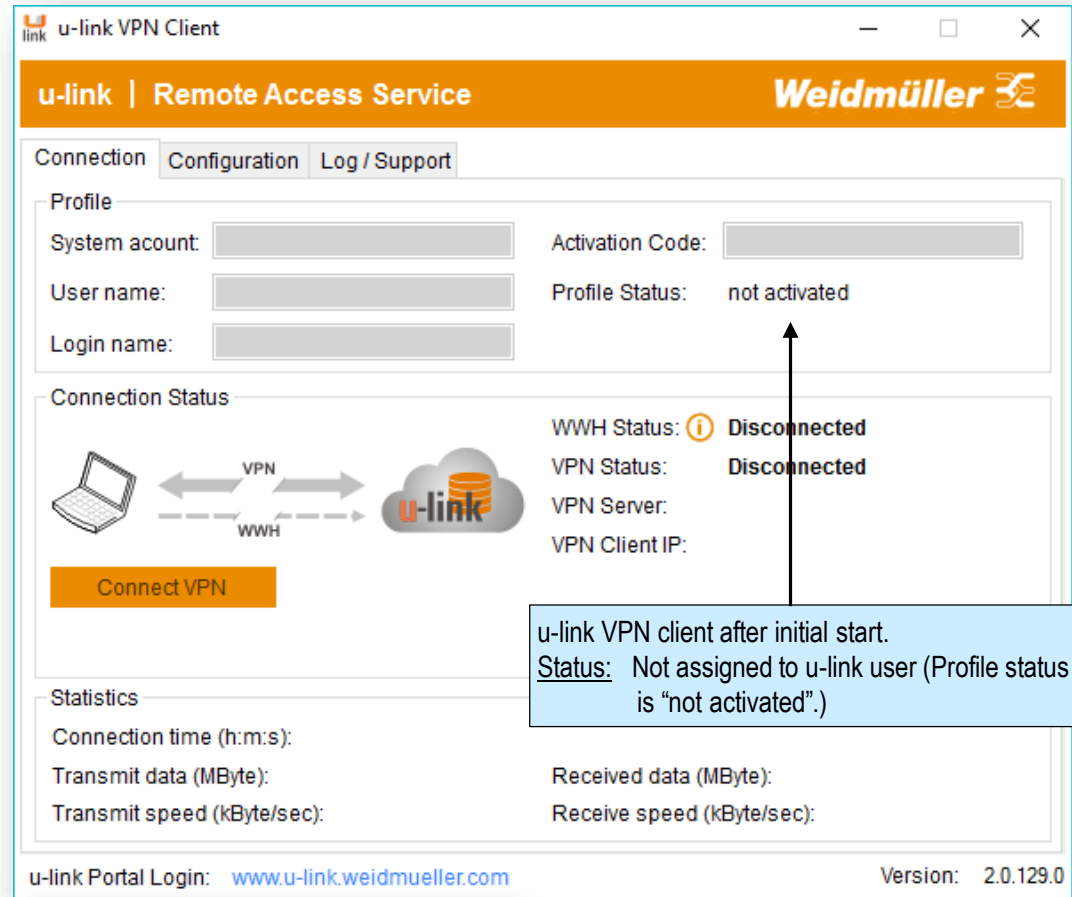


New u-link desktop icon

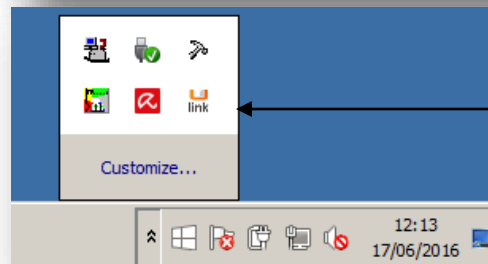
4.5 u-link VPN Client → Start program

Start software u-link VPN Client on the Service PC

- The program window will be opened and the u-link icon will be displayed in the notification area of the taskbar.
- Initially the software is not assigned to a u-link user account.
- Before starting a VPN connection to the u-link VPN server the software has to be registered using the unique activation code of the u-link user account which shall be used for remote access.



u-link VPN client after initial start.
Status: Not assigned to u-link user (Profile status is "not activated".)



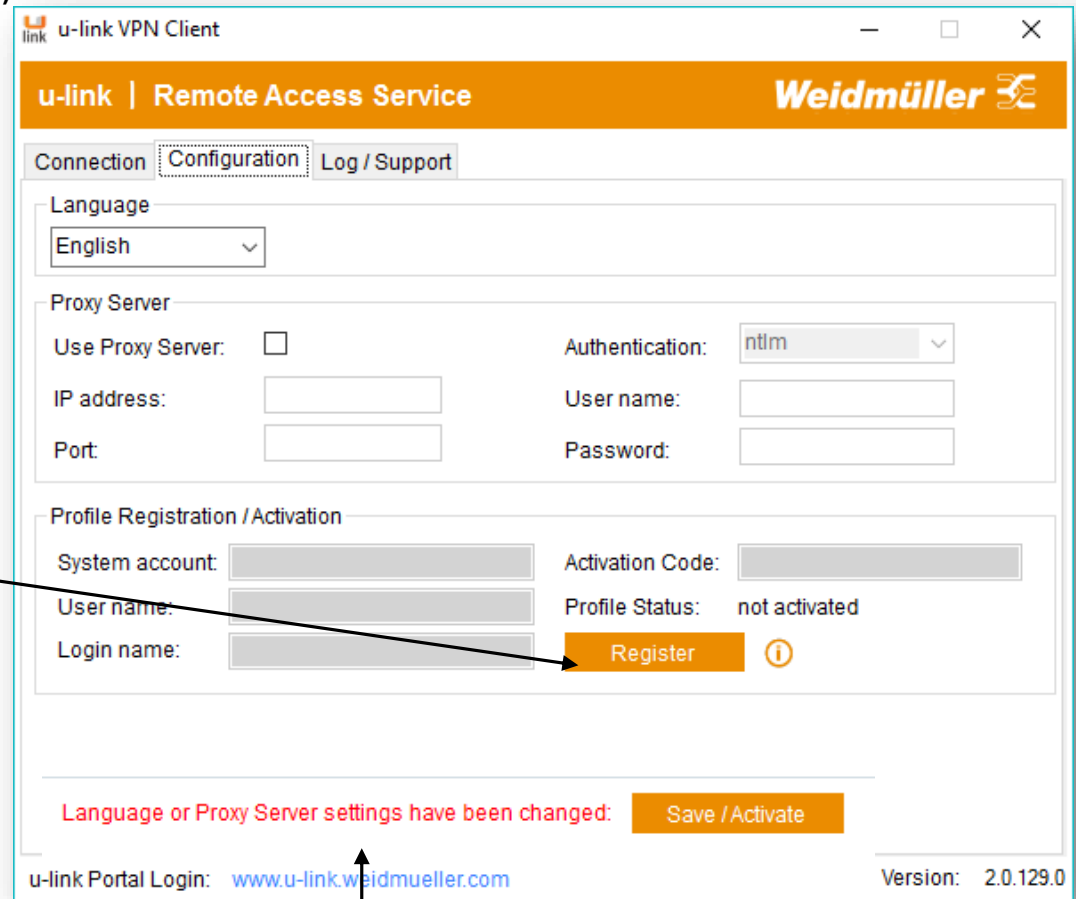
Notification area of the taskbar
 Icon of 'u-link VPN client' when the program has been started.
Status: Not connected

4.5 u-link VPN Client → Configuration (Step 1)

- Go to Tab Configuration
- Select your language (English / German)
- Dependant of your Internet connectivity configure your Proxy Server configuration (often necessary if your Internet access is controlled by corporate IT systems). The Proxy server parameters will be provided by your IT department).
 - Leave checkbox 'Use Proxy Server' unchecked if your PC is not passing a Proxy server for Internet access.

Initial registration of your u-link user account

- Click button "Register" to start the registration process.
 - For the registration process you need the user specific activation code. The activation code can be found either in the received mail 'User Registration' or in menu 'User Profile' on tab 'Activation Code' when logged-on to the u-link Web portal.



This message appears when changing the language or editing the proxy parameters.
Click button 'Save / Activate' before starting the registration process.

4.5 u-link VPN Client → Configuration (Step 2)

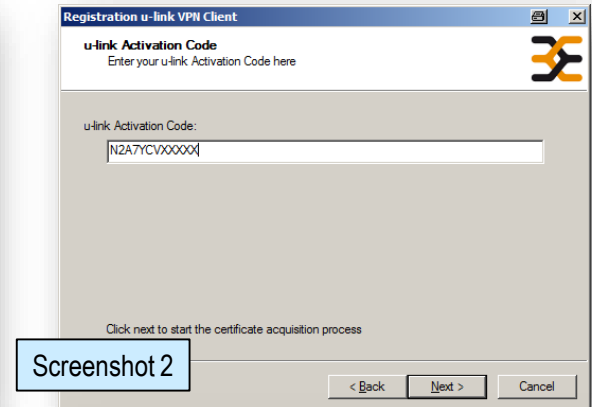
Steps of registration process after clicking button 'Register user profile'

- Click button 'Next' (Screenshot 1).
- Enter your activation code and click button 'Next' (Screenshot 2).
- Wait some seconds until the registration process is done (Screenshot 3). Finally the result is displayed.
- Click button 'Finish' (Screenshot 4).

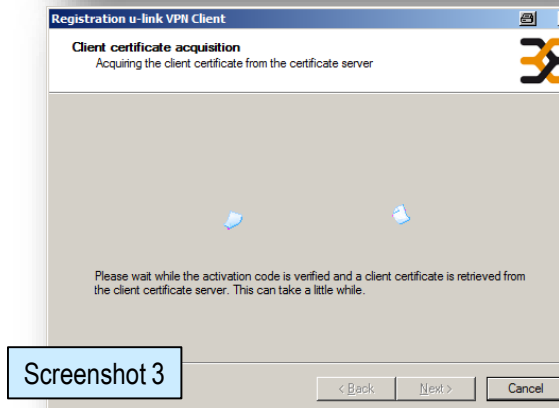
- Wait around 10..15 seconds until the data of the registered user account will be displayed in section "Profile Registration / Activation". Now the u-link VPN client is assigned to your u-link user account .
- Change to Tab "Connection" and try to start a VPN connection.



Screenshot 1



Screenshot 2

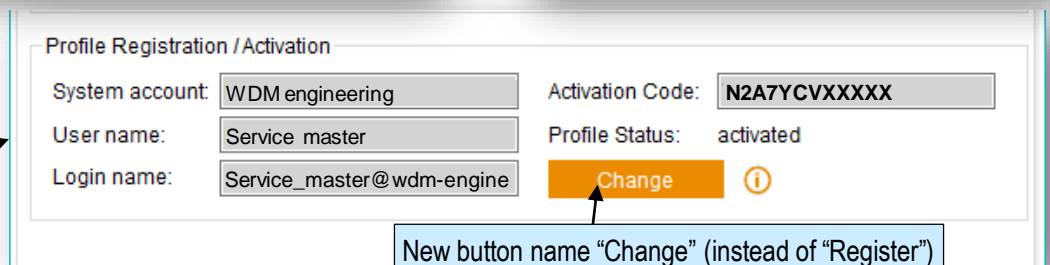


Screenshot 3



Screenshot 4

Screenshot of a successfully registered 'u-link VPN client'

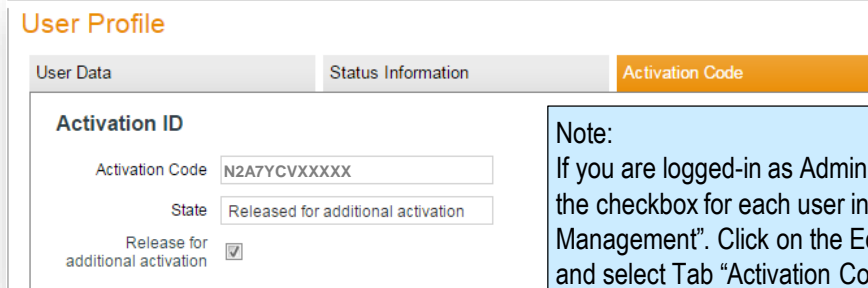
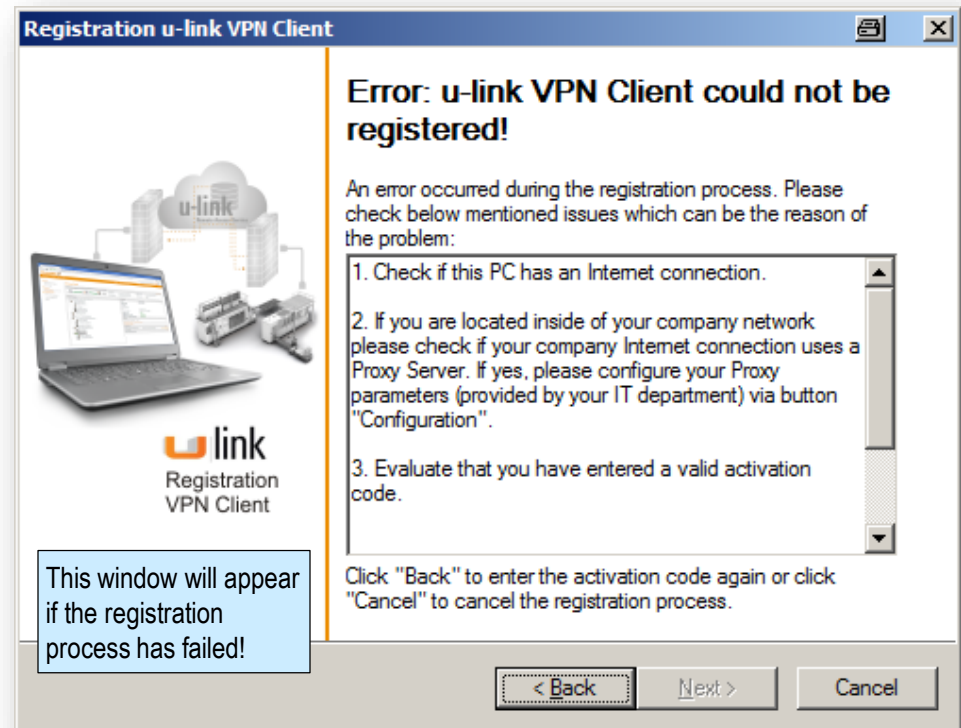


New button name "Change" (instead of "Register") after first registration process

4.5 u-link VPN Client → Configuration (Error handling when registration process failed)

Possible errors if the registration process has failed:

- **No Internet access**
Ensure that your PC can access the Internet.
- **Registration process blocked by Proxy Server**
If you are located inside of your company network please check if your company Internet connection uses a Proxy server. If yes, please configure your Proxy parameters (provided by your IT department) on tab "Configuration".
- **Wrong activation code**
Evaluate that you have entered a valid activation code.
- **Activation code already registered and not released for additional use (Status "In use")**
If you have entered an already registered activation code (now using on a second PC) you first must release the **additional** use of this activation code.
 - Login to u-link Web portal using your user account.
 - Goto menu User profile / Tab Activation Code.
 - Activate checkbox "Release for additional activation".
 - Click button "Update" (not displayed in screenshot below).



Note:

If you are logged-in as Administrator you can set the checkbox for each user in menu "User Management". Click on the Edit icon of a user item and select Tab "Activation Code".

Note:

If the problem cannot be solved please cancel this process. Then change to tab "Log / Support". Start the Support Wizard and send the log file (gathered by Support Wizard) to the Weidmüller u-link support mail address.

4.5 u-link VPN Client → Establish a VPN connection to the u-link VPN server

Conditions:

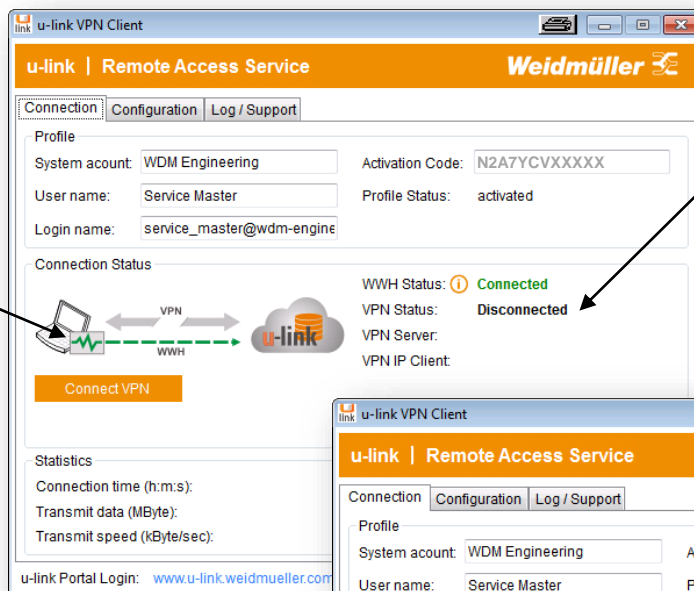
- The u-link VPN client is registered (Profile status 'activated' and displaying the user data).
- The WWH connection is established (Status 'Connected').

➤ Click button 'Connect VPN'.

- The Client is starting the VPN connection to the u-link VPN server (wait around 15..20 seconds).
- When successfully connected the online status, some additional information and statistic information will be displayed.
- The u-link icon in the task bar is displaying an established VPN tunnel by changing the background color to green.

➤ Open a browser and logon to the u-link Web portal with user name and password of the user having this activation code.

- In menu 'Service Desk' the PC's connection to the u-link VPN server will be signaled by a green colored double arrow.
- Now you are connected to the u-link VPN server but at this time you still do not have any pass-through connection to a Router/Remote network. This has to be configured in the next steps.

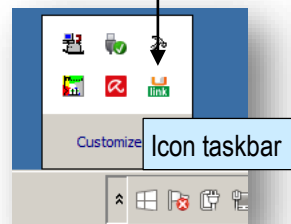
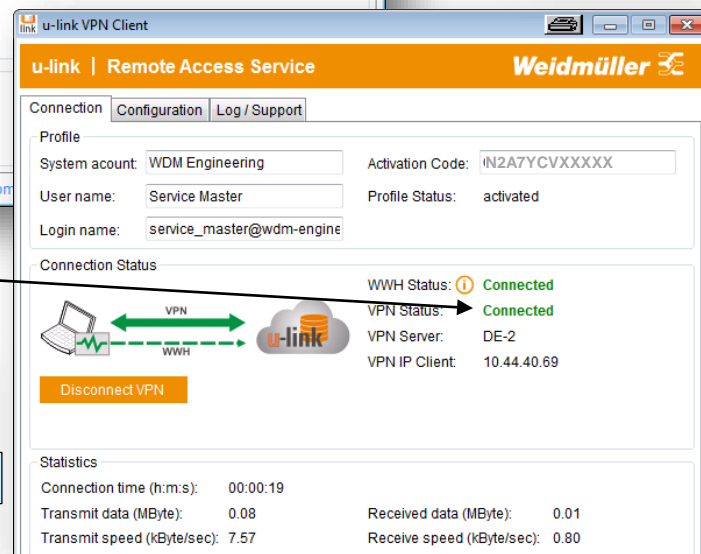


VPN status: Not connected



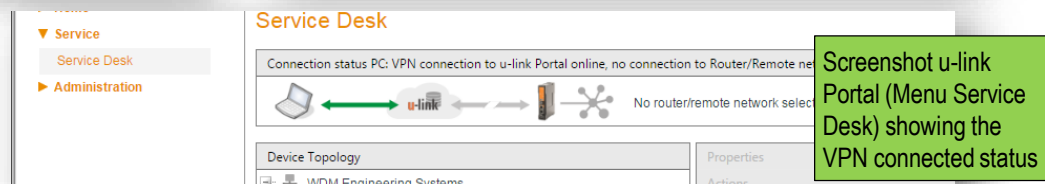
Icon taskbar

VPN status: Connected



Configuration of Service PC now is finished!

Next the physical Router (which later is located in the remote network) has to be configured.



Screenshot u-link Portal (Menu Service Desk) showing the VPN connected status

4.5 u-link VPN Client → Error management if the WHH connection or the VPN tunnel could not be established

WWH error (WWH connection failed)

After successful registration the u-link VPN client automatically is trying to initiate a WWH connection to the u-link WWH server. If this fails it can be caused by following reasons:

- PC cannot resolve DNS names
- An outgoing SSL connection using protocol TCP / port 443 cannot be established. Check if a corporate firewall is blocking the outgoing connection. Configure if necessary your proxy server settings.

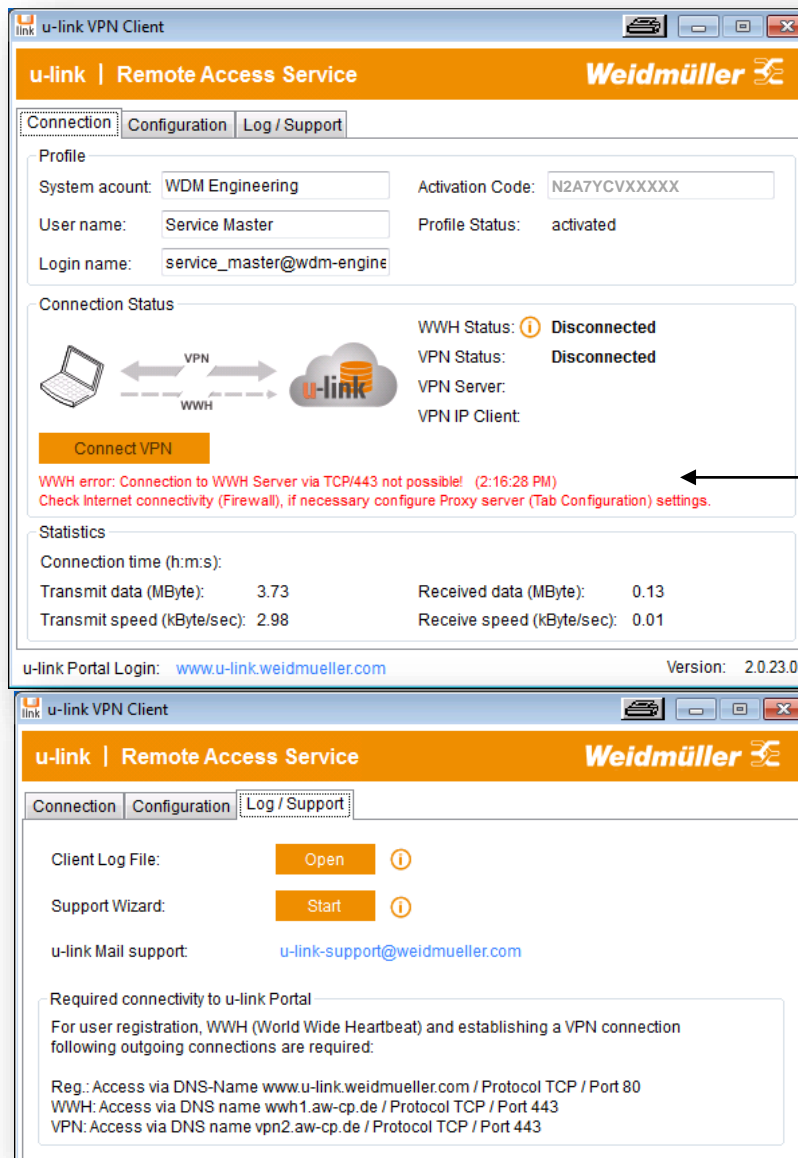
Note: An error message indicating the connection problem will be displayed.

VPN error (VPN connection failed)

Establishing a VPN connection (via button “Connect VPN”) is only possible if you have a running WWH connection. In case of a VPN failure – same as for a WWH error - an error message will be displayed indicating the connection problem.

General procedure in terms of solving a connection error (WWH and VPN):

- Go to tab “Log / Support”
- Click button “Open” to inspect the Log file
- If you cannot solve your connection problem please start the “Support Wizard” (which gathers all log information) and send the resulting ZIP file to the Weidmüller u-link Support



4.6 Configuration of the Router

4.6 Configuration of the Router

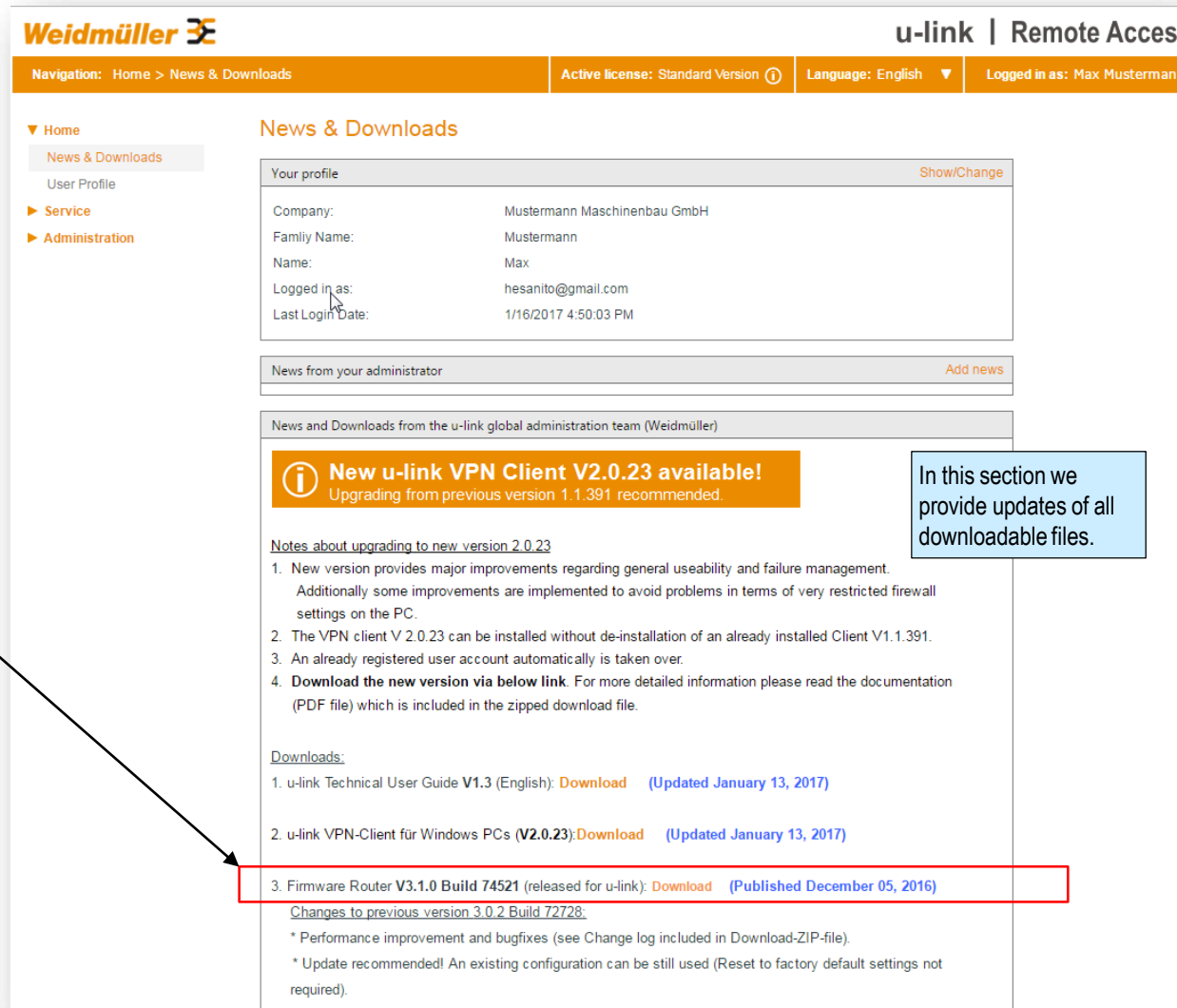
Download of latest Router firmware (Step 1)

- All the Router models except –FN version (which does not support VPN functions) can be used for u-link.
- If you would like to use an already running Router with u-link then you need a firmware version 3.0.2 or higher.

- Logon to the u-link Web portal using your user name and password.
- Goto menu 'News & Downloads'.
- Download the provided firmware from third section 'News and Downloads from global Weidmüller u-link administration'.

Unzip the downloaded firmware (Step 2)

- The ZIP file is containing the binary file (firmware) and a pdf-file (Change log).



The screenshot shows the Weidmüller u-link Remote Access portal. The navigation bar includes 'Home > News & Downloads', 'Active license: Standard Version', 'Language: English', and 'Logged in as: Max Mustermann'. The main content area is titled 'News & Downloads' and features a sidebar with 'Home', 'News & Downloads', 'User Profile', 'Service', and 'Administration'. The 'Your profile' section shows user details for Max Mustermann. The 'News and Downloads from the u-link global administration team (Weidmüller)' section contains a prominent orange banner for 'New u-link VPN Client V2.0.23 available!' and a list of download links. A red box highlights the link for 'Firmware Router V3.1.0 Build 74521 (released for u-link)'. A blue callout box points to the 'Downloads:' section.

News & Downloads

Your profile [Show/Change](#)

Company: Mustermann Maschinenbau GmbH
 Family Name: Mustermann
 Name: Max
 Logged in as: hesanito@gmail.com
 Last Login Date: 1/16/2017 4:50:03 PM

News from your administrator [Add news](#)

News and Downloads from the u-link global administration team (Weidmüller)

New u-link VPN Client V2.0.23 available!
 Upgrading from previous version 1.1.391 recommended.

[Notes about upgrading to new version 2.0.23](#)

1. New version provides major improvements regarding general useability and failure management. Additionally some improvements are implemented to avoid problems in terms of very restricted firewall settings on the PC.
2. The VPN client V 2.0.23 can be installed without de-installation of an already installed Client V1.1.391.
3. An already registered user account automatically is taken over.
4. **Download the new version via below link.** For more detailed information please read the documentation (PDF file) which is included in the zipped download file.

[Downloads:](#)

1. u-link Technical User Guide V1.3 (English): [Download](#) (Updated January 13, 2017)
2. u-link VPN-Client für Windows PCs (V2.0.23): [Download](#) (Updated January 13, 2017)
3. **Firmware Router V3.1.0 Build 74521 (released for u-link): [Download](#) (Published December 05, 2016)**

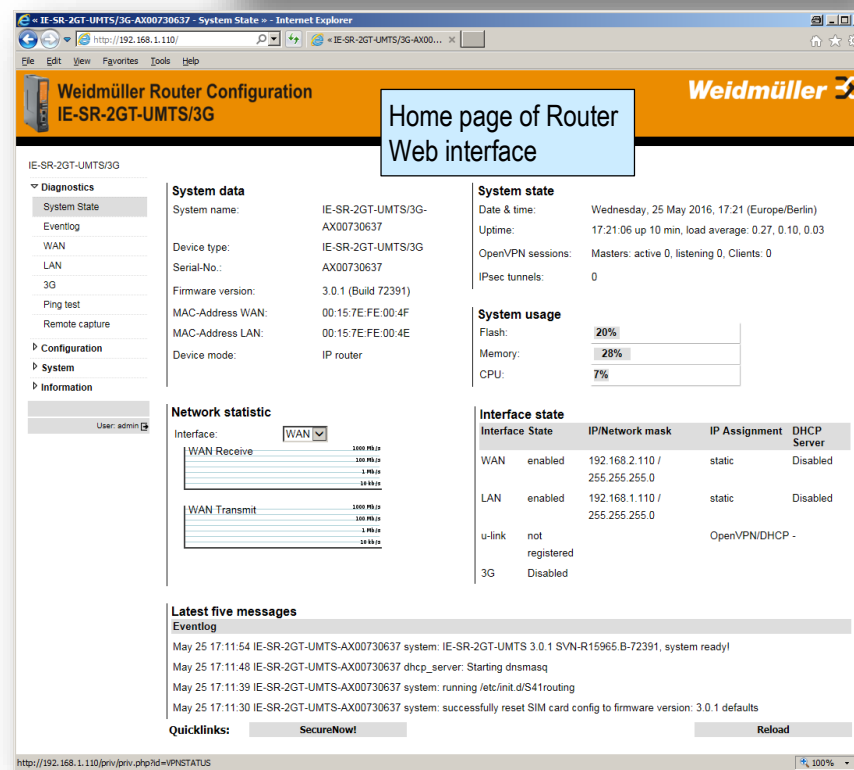
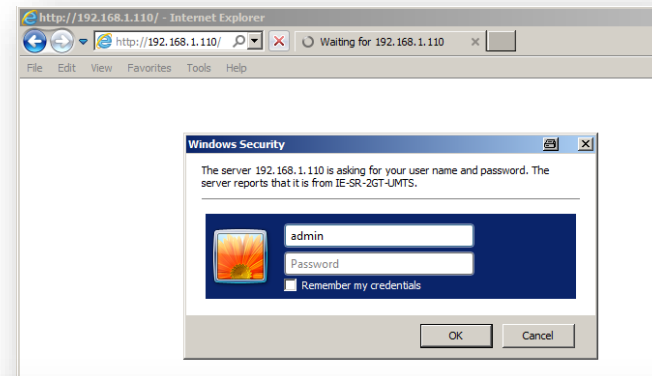
[Changes to previous version 3.0.2 Build 72728:](#)

- * Performance improvement and bugfixes (see Change log included in Download-ZIP-file).
- * Update recommended! An existing configuration can be still used (Reset to factory default settings not required).

4.6 Configuration of the Router

Connecting to the Router and open the Web interface (Step 3)

- We assume that the Routers configuration is set to factory default values (LAN IP: 192.168.1.110, WAN IP: 192.168.2.110 or DHCP for 6-Port models).
- Connect the PC to the Router LAN or WAN port (Here we use the LAN port).
- Configure the PCs Ethernet interface to the same IP network range as the Router (e.g. 192.168.1.99).
- Open a browser and enter IP address 192.168.1.110 to open the Router Web interface.
- Enter user name **admin** and password **Detmold**.
 - The home page (System state) will be displayed.



Note about help tool “Weidmüller Router Search Utility”

The software **Weidmüller Router-Search-Utility** can be used to find Weidmüller Routers and detect their IP addresses within a switched network. This software is very helpful if you don't know the current IP address of a Router. This e.g. can happen in cases that you have forgotten the current IP configuration or if you have lost the router access in case of configuring an unintended IP address. The main features of the software are

- Detecting a router and displaying the parameters IP address, subnet mask, MAC address, serial number, device name, device location and firmware version
- Change the IP address of a detected router
- Open the web interface of a detected router

The software can be downloaded via this link

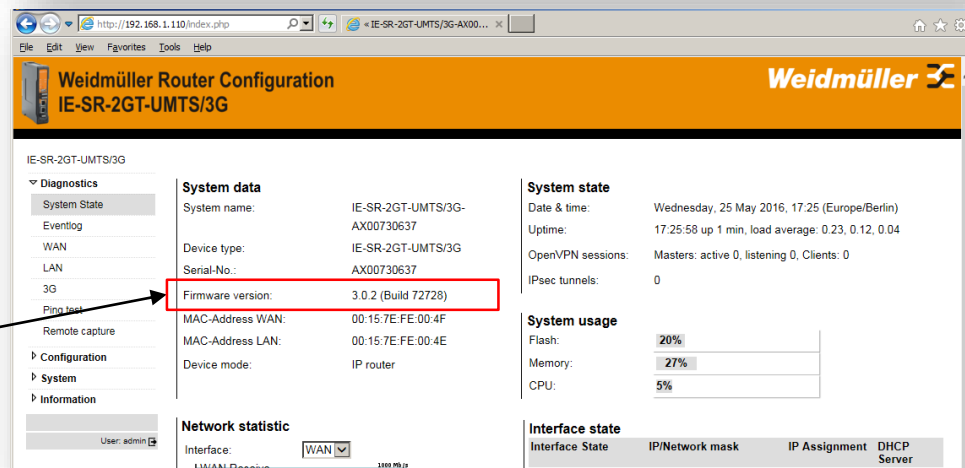
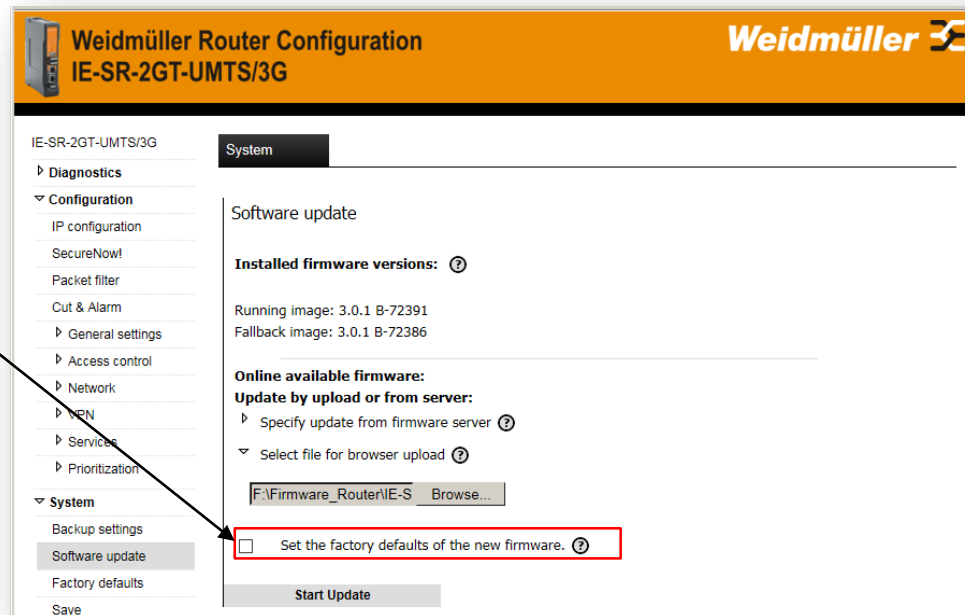
<http://www.weidmueller.com/int/products/electronics-and-automation/industrial-ethernet/software>

- Goto section Industrial Security Router (Firmware and Software for IE-SR-2/6GT-LAN/4G/LTE)
- Download entry **Weidmüller Router Search Utility**

4.6 Configuration of the Router

Updating the Router firmware to a u-link enabled version (Step 4)

- Note: If you update an individually configured Router with an older firmware version the stored configuration will not be changed as long as if you not enable checkbox “Reset to factory defaults”.
- Go to menu System → Software Update.
- Click button browse and select the firmware file (eg. IE-SR-2GT-LAN_FN_3G_V3.1.0_Build_74521.bin).
- Click button ‘Start Update’.
- Wait around 2 minutes (until the PWR LED is no longer blinking).
- Open the browser window again using the same IP address.
- In section ‘System data’ of menu ‘System state’ the new current firmware version is displayed.



Displays the current firmware version after update process

4.6 Configuration of the Router

Configuration of basic IP parameters (Step 5a)

Internet access via WAN port and using DHCP

- Now the IP parameters of the Routers Ethernet interfaces have to be configured. The LAN port has to be set according to the IP range of the remote network. The WAN port will be used for Internet access.
- Based on our example we will configure the IP parameters as shown in the screenshot. If you have a 4G Router (IE-SR-2/6GT-LTE/4G), inserted a SIM card (any provider with Internet flat) you alternatively can configure the Internet access via the 4G connection.

- Goto menu Configuration → IP Configuration.
- Set WAN port to DHCP (getting IP parameters from a DHCP server).
- Set LAN IP to 192.168.1.254.
- Enable checkbox 'NAT Masquerading' at LAN port.
- Click button 'Apply Settings'.
- Note: Now the Router will apply the settings. As result you will lose the browser connection to the Router due to changed LAN IP. Wait some seconds and re-open the Web interface using the new IP address 192.168.1.254.

Currently connected to PC via Router LAN port (IP: 192.168.1.110)

Screenshot after parameter configuration (but still not applied).

Internet access via WAN port (IP parameters via DHCP)

Important note
 "NAT Masquerading" has to be activated if devices – connected to Router LAN port - does **not** have configured the Router LAN IP as gateway.

Effect of NAT masquerading
 If the checkbox is enabled then the Router is replacing the source IP of an incoming IP packet (via u-link VPN tunnel) with its own LAN IP when the packet is outgoing out of the LAN port to a target device. Internally the Router stores the requesting source IP to be able to forward a reply packet back to the original sender. When the LAN device receives the request packet it believes that the request comes from a member of its own network (Router's LAN IP) and is able to reply without having configured a gateway.

Router receives Default gateway from DHCP server

Recommendation: Activate generally "NAT masquerading" at LAN port when using the Router with u-link.

4.6 Configuration of the Router

Configuration of basic IP parameters (Step 5b)

Internet access via WAN port and using a static IP address

- Goto menu Configuration → IP Configuration.
- Configure the WAN IP settings according to the network to which the WAN port will be connected.
 - Enter IP address and subnet mask.
 - Enable WAN checkbox 'NAT Masquerading'.
 - Enter the Default gateway (IP address of a Router located in the WAN side network which is providing the Internet access).
- In this example the LAN IP settings are configured with same value as used in previous slide.
 - Set LAN IP to 192.168.1.254 and subnet mask to 255.255.255.0.
 - Enable LAN checkbox 'NAT Masquerading'.
- Click button 'Apply Settings'.
 - Now the Router will apply the settings. As result you will lose the browser connection to the Router due to changed LAN IP. Wait some seconds and re-open the Web interface using the new IP address 192.168.1.254.

Currently connected to PC via Router LAN port (IP: 192.168.1.110)

Screenshot after parameter configuration (but still not applied).

Internet access via WAN port configured with static IP parameters.

Recommendation: Activate generally "NAT masquerading" at WAN port when using the Router with u-link.

IP parameters of LAN port same as configured on previous slide.

Recommendation: Activate generally "NAT masquerading" at LAN port when using the Router with u-link.

The Default gateway to get Internet access explicitly has to be configured.

The screenshot shows the 'IP configuration' page in an Internet Explorer browser. The address bar shows 'http://192.168.1.110/priv.php?id=1'. The page title is 'Weidmüller Router Configuration IE-SR-2GT-UMTS/3G'. The left sidebar shows a navigation menu with 'Configuration' expanded and 'IP configuration' selected. The main content area is titled 'Configuration' and contains 'IP configuration' settings. Under 'Operational mode', 'IP router' is selected. Under 'WAN', 'IP assignment' is set to 'static', 'IP address' is '192.168.99.205', 'Subnet mask' is '255.255.255.0', and 'NAT (Masquerading)' is checked. Under 'LAN', 'IP assignment' is set to 'static', 'IP address' is '192.168.1.254', 'Subnet mask' is '255.255.255.0', and 'NAT (Masquerading)' is checked. Under '3G', 'Dialmode' is set to 'disabled'. Under 'Default gateway', 'IP address' is '192.168.99.1'. At the bottom, there are 'Apply settings' and 'Reset changes' buttons. Red boxes highlight the WAN and LAN settings, and arrows point from text boxes to these areas.

4.6 Configuration of the Router

Configuration DNS server (Step 5c)

Only necessary if WAN port is using a static IP address for Internet access.

- Note: To resolve DNS names (like www.google.com) the Router must have access to a DNS Server. If the WAN port is configured using DHCP then the IP address of the DNS server automatically will be provided by the DHCP server.
- If the IP address of the WAN port is configured with a static IP then additionally a DNS server has to be set manually.
- Goto menu Configuration → Network → DNS.
- Enter your own Hostname (is optional).
- Enter at least 1 IP address of a DNS server (starting with parameter '1st DNS server').
- Click button 'Apply Settings'.

Skip this step if the WAN port of the Router is configured to DHCP.

Router now is connected via IP 192.168.1.254

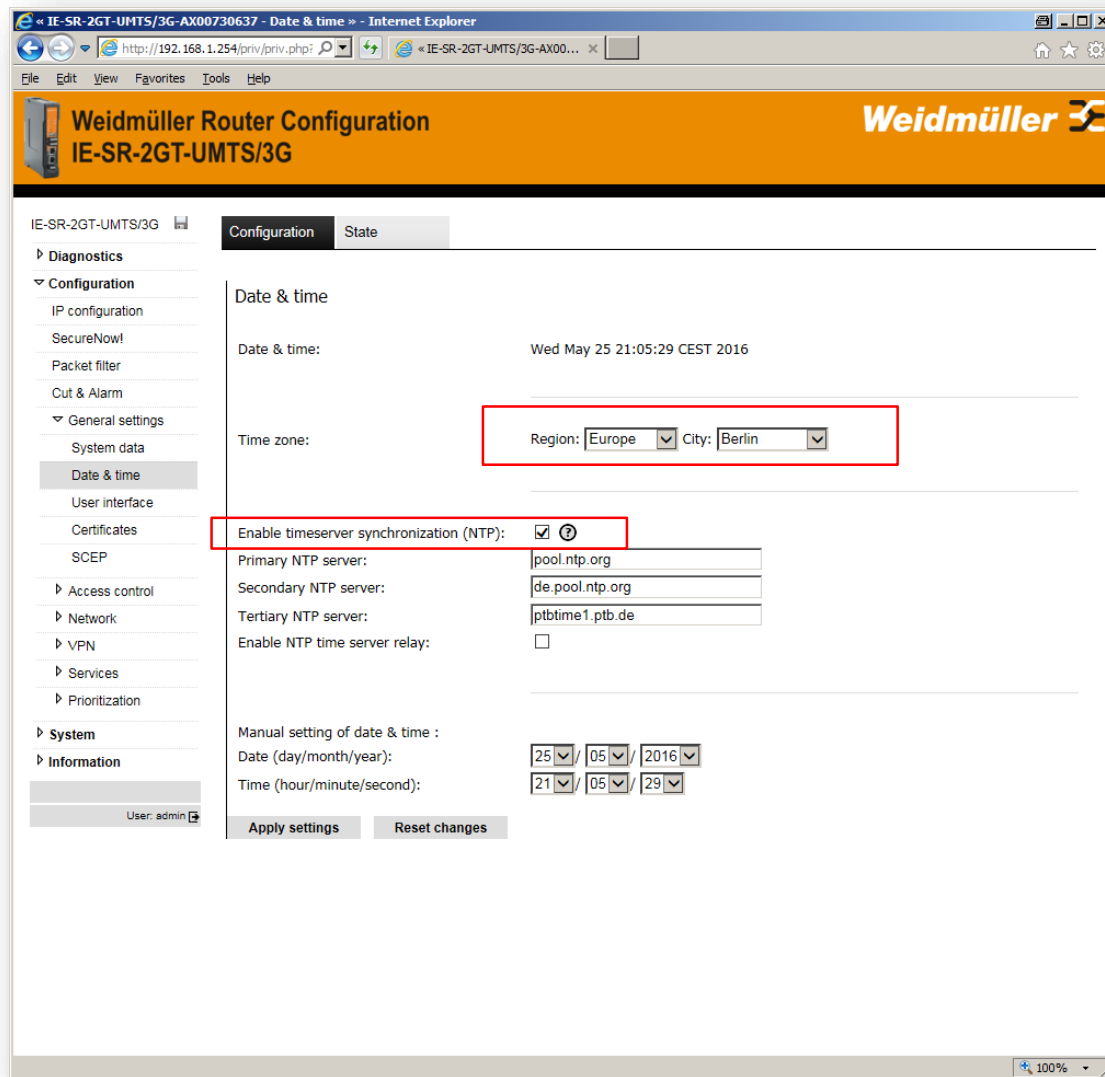
In this example the public Google DNS server (IP 8.8.8.8) is used.

Note: This IP address generally can be used to resolve DNS names.

4.6 Configuration of the Router

Configuration of date / time parameters (Step 6)

- Note: The VPN connection to the u-link VPN server will use a certificate for encryption. Generally the validity of a certificate depends on date/time stamps (valid from/valid until). For this reason the Routers date and time settings should be set to a current value. Due to the fact that for an u-link access the Router always must have an Internet connection it is recommended to enable the time server synchronization (NTP) that the Router automatically will update date and time. If no time synchronization is possible then date and time values have to be set manually.
- Go to menu Configuration → General settings → Date & Time.
- Select your time zone.
- Enable checkbox 'Time Server Synchronization'.
- Enter your preferred NTP servers or use the defaults ones.
- Click button 'Apply Settings'.



The screenshot displays the 'Date & time' configuration page for a Weidmüller router. The interface includes a navigation menu on the left with categories like 'Diagnostics', 'Configuration', 'General settings', 'System data', 'User interface', 'Certificates', 'SCEP', 'Access control', 'Network', 'VPN', 'Services', 'Prioritization', 'System', and 'Information'. The 'Date & time' section is currently selected. It shows the current date and time as 'Wed May 25 21:05:29 CEST 2016'. The 'Time zone' is set to 'Region: Europe' and 'City: Berlin'. The 'Enable timeserver synchronization (NTP)' checkbox is checked. Below this, three NTP servers are listed: 'pool.ntp.org', 'de.pool.ntp.org', and 'ptbtime1.ptb.de'. The 'Manual setting of date & time' section shows the date as '25/05/2016' and the time as '21:05:29'. The 'Apply settings' and 'Reset changes' buttons are visible at the bottom.

4.6 Configuration of the Router

Configuration of HTTP proxy parameters if the Internet connection is passing a Proxy server, requiring authentication by user name and password (Step 7)

- See section 'Preparing the Service PC (u-link VPN client)' for additional information in terms of proxy settings. Be aware that the Router proxy parameters depend on the network security settings of the Routers location.
- Go to menu Configuration → Network → HTTP Proxy.
- Enter the Proxy Server specific parameters (provided by IT department of remote network which the Router is using for Internet access).
- Click button 'Apply Settings'.

Skip this step if the Routers Internet access is not passing a Proxy server.

Factory default settings (No proxy parameters configured)

Example of configured proxy parameters.

Note: For an u-link connection the configured proxy parameters only are used if in the u-link configuration menu the checkbox "Use a system wide HTTP proxy" is activated.

4.6 Configuration of the Router

Establishing a network connection via WAN port (Step 8) / **In this example we use DHCP for IP settings of WAN port.**

- Connect the WAN port to a network which is providing DHCP and allowing Internet access.
 - Wait around 30 seconds that the Router is getting IP data from DHCP server.
- Goto menu Diagnostic → System state (Home page).
- Check menu 'System state' if date and time values have current values. **1**
- Check section 'Interface state' if WAN port has received an IP address. **2**

Check Internet access (Step 9)

- Goto menu Diagnostic → Ping test.
- Enter a DNS name (eg. www.google.com) or an IP address (eg. 8.8.8.8) and click button 'Apply Settings'.
 - When having an Internet connection the Router will displaying the result.

Router now connected via IP 192.168.1.254

1 System state

Date & time: Monday, 20 Jun 2016, 17:25 (Europe/Berlin)
 Uptime: 17:25:17 up 3:52, load average: 0.22, 0.11, 0.04
 OpenVPN sessions: Masters: active 0, listening 0, Clients: 0
 IPsec tunnels: 0

2 Interface state

Interface	State	IP/Network mask	IP Assignment	DHCP Server
WAN	enabled	192.168.99.20 / 255.255.255.0	DHCP	Disabled
LAN	enabled	192.168.1.254 / 255.255.255.0	static	Disabled
u-link	not registered		OpenVPN/DHCP	-
3G	Disabled			

Ping test

IP address or hostname:

Number of ping messages:

Apply settings Reset changes

Screenshot of menu "Ping test"

Result

```

PING www.google.com (216.58.213.36): 56 data bytes
64 bytes from 216.58.213.36: seq=0 ttl=56 time=54.673 ms

--- www.google.com ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 54.673/54.673/54.673 ms
    
```

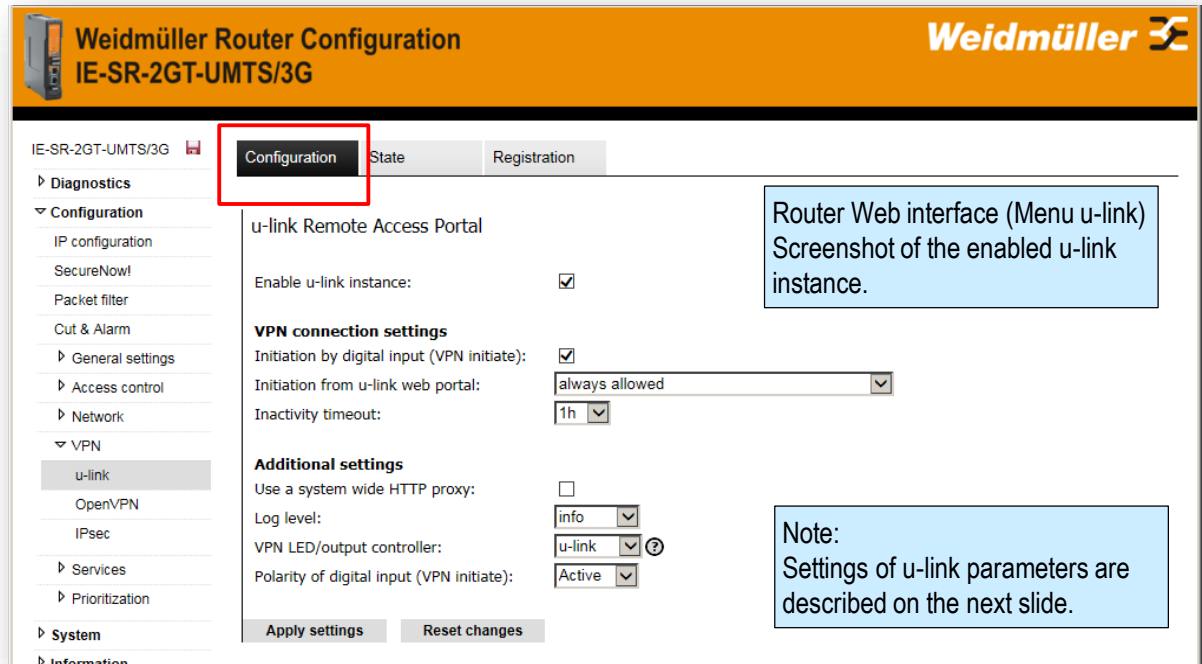
Continue...

Screenshot of a successful "Ping" test

4.6 Configuration of the Router

Activate the Router for u-link (Step 10)

- Goto menu Configuration → VPN → u-link (Tab 'Configuration').
- Enable checkbox 'Enable u-link instance'.
- Use default values of section 'VPN connection settings'.
- Enable checkbox 'Use a system wide HTTP proxy' if the Router Internet access is passing a Proxy Server.
 - Note: If the checkbox will be enabled the Proxy server settings must be configured as described previously.
- Use default settings of the other parameters.
- Click button 'Apply settings'.



Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G

Configuration State Registration

IE-SR-2GT-UMTS/3G

u-link Remote Access Portal

Enable u-link instance:

VPN connection settings

Initiation by digital input (VPN initiate):

Initiation from u-link web portal: always allowed

Inactivity timeout: 1h

Additional settings

Use a system wide HTTP proxy:

Log level: info

VPN LED/output controller: u-link

Polarity of digital input (VPN initiate): Active

Apply settings Reset changes

Router Web interface (Menu u-link)
Screenshot of the enabled u-link instance.

Note:
Settings of u-link parameters are described on the next slide.

4.6 Configuration of the Router

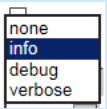
Explanation of u-link configuration parameters

Inactivity timeout (Dropdown box)
The Router automatically will shutdown a VPN connection after the selected time if no traffic was recognized during this time.



HTTP Proxy (Checkbox)
Enable if the Internet access is passing a Proxy server (Configure Proxy settings in menu Configuration → Network → HTTP Proxy)

Log Level (Dropdown box)
Selection of logging level (Messages shown in the Event Log).

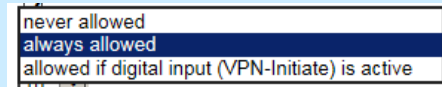


Initiation by digital input (Checkbox)
If enabled the 24VDC digital input can be used for activating a VPN tunnel to the u-link VPN server.

VPN LED / Output controller
If set to “u-link” an active VPN tunnel will be signaled at front LED “VPN” and the digital output “VPN-active”.

“Initiation from u-link web portal” (Dropdown box)
Controls if the u-link VPN tunnel can be activated/deactivated remotely from the u-link Web portal via the WWH (world wide heartbeat) function.
Selections:
Never allowed: Remote activation/deactivation of the VPN tunnel from u-link Web portal never is allowed.
Always allowed: Remote activation/deactivation of the VPN tunnel from u-link Web portal always is allowed.
Allowed if digital input (VPN-Initiate) is active: Means that remote activation/deactivation from u-link Web portal only is allowed when the digital input “VPN-Initiate” is set to 24VDC.

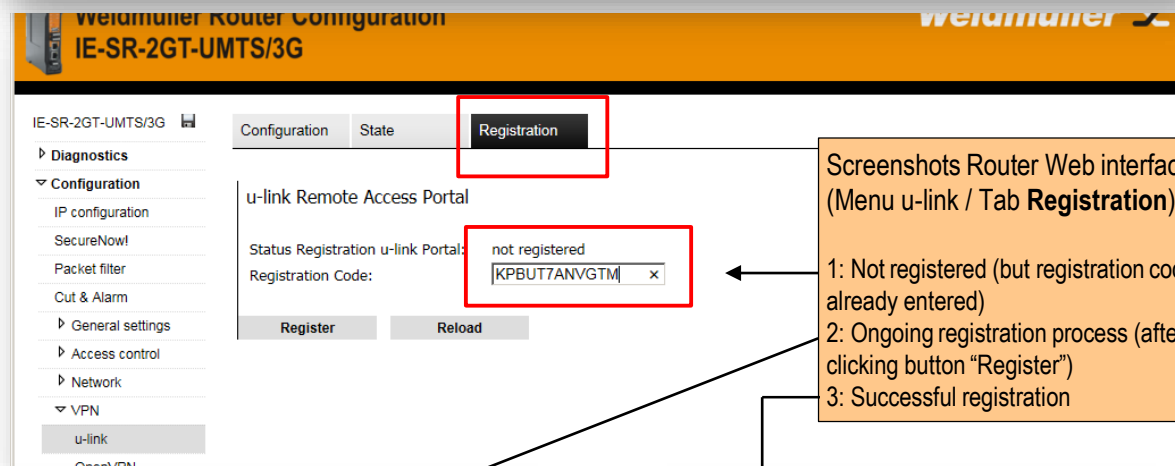
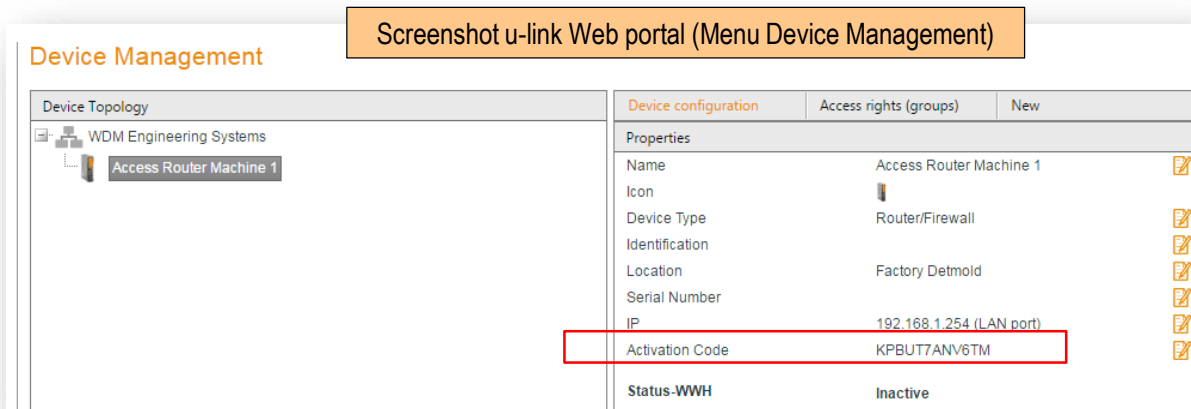
Explanation: If a machine operator at Router location has activated the 24VDC digital input “VPN-Initiate” (eg. by key switch) then the VPN tunnel will be started providing the remote access. But if the service guy will not immediately start the service (means no traffic on the VPN tunnel) then by default the Router automatically de-activates the VPN tunnel after 1 hour of no traffic. But to due to the fact that the key switch still is on (means the access permission is still granted), the remote Service user may re-activate the VPN tunnel remotely. If the key switch again is set to off (24VDC removed from digital input) then the VPN tunnel will be de-activated immediately and the remote Service user no longer is allowed to activate the VPN tunnel remotely.



4.6 Configuration of the Router

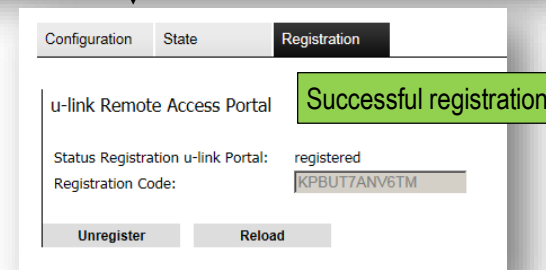
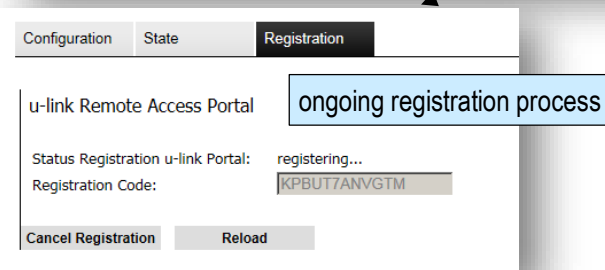
Register (Assign) the Router to the defined Router object configured in the u-link Web portal (Step 11)

- For the registration process we need the unique activation code of the Router object. The activation code can be found in the properties of the created Router object (u-link Portal: Menu 'Device Management').
- Select Tab 'Registration'.
- Enter the activation code of the defined Router object in field 'Registration code'.
- Click button 'Register'.
 - Now the Router is initiating the registration process to the u-link Portal server. This process typically takes time of around 30 seconds.
- Please click button "Reload" repeatedly to update the current registration status.



As result the Router should have the status "registered".

If the registration process has failed please refer to Appendix A (Registration of Router to u-link failed).



4.6 Configuration of the Router

Check the status of the u-link connection (Step 12)

➤ Select tab 'State'.

- After successful registration the Router is initiating the WWH communication to the u-link (Status 'Online').

Notes about WWH

The WWH function (World Wide Heartbeat) is an outgoing TLS/SSL connection (TCP/443, like HTTPS) to the u-link WWH server and is independent from a VPN connection which will be used for remote access.

The Router sends via this peer connection periodically a „Still alive“ message to the WWH server. The WWH server then signals the u-link Web server that the Router is alive. This status is displayed in the Service Desk of the u-link Web portal.

Via the WWH connection it is possible to activate/de-activate the VPN tunnel of the Router remotely from the u-link Web portal server.

The encrypted WWH connection automatically is started when the Router is powered on, having an Internet connection and is registered to a Router object in a u-link account.

Activating the VPN tunnel via menu "State"

Additionally to the most used methods to initiate a VPN tunnel (remotely via u-link Portal or by 24 VDC digital input) the VPN connection can be activated / de-activated via button 'Connect'.

Router Web interface (Menu u-link / tab State)
Status:
 • WWH online
 • No VPN connection to the u-link VPN server

u-link Remote Access Portal
 Status Registration u-link Portal: registered

WWH communication
 Status: ONLINE
 Last seen: Monday, 20 Jun 2016, 17:38
 Heartbeat interval: 300s

VPN connection u-link portal
 Status: VPN not connected

Connect

Service Desk
 Connection status PC: No VPN connection to u-link Portal

Device Topology
 WDM Engineering Systems
 Access Router Machine 1
 Profinet PLC
 u-remote coupler PN

This icon is representing the WWH online status of the Router.

Activate / De-activate a VPN tunnel via button 'Connect / Disconnect'.

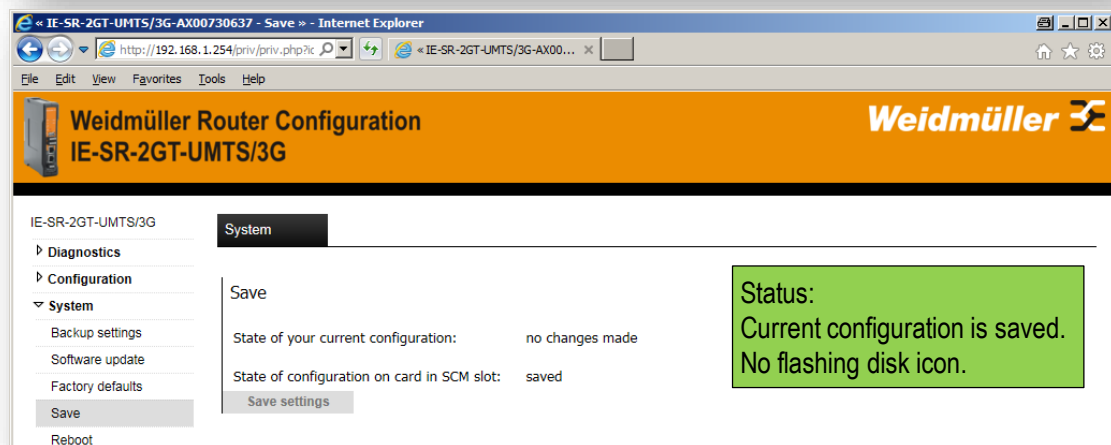
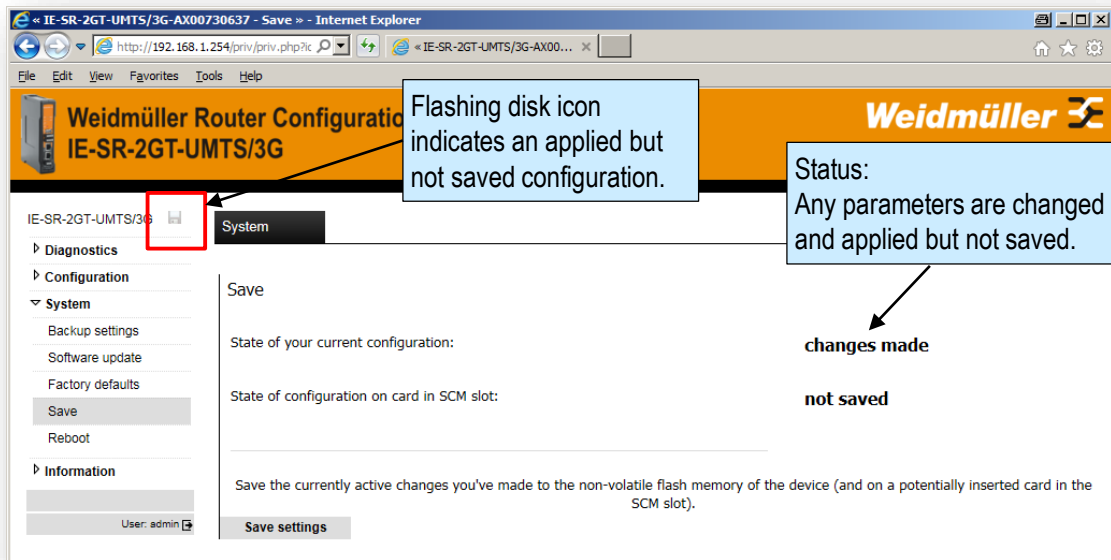
u-link Web portal Menu 'Service Desk'

Now the Router is ready for initiating a remote access session!

4.6 Configuration of the Router

Save the Router configuration (Step 13)

- Go to menu System → Save.
 - If you have changed and applied any settings then in each menu a flashing disk icon is displayed, indicating that the applied settings not yet are saved to the flash memory. By clicking on the disk icon the menu 'Save' directly will be opened.
- Click button 'Save settings' to store the configuration in the non-volatile memory.



Chapter 5: Initiating an access to remote LAN devices

Conditions

Device configuration in u-link Web portal has been done.

Software 'u-link VPN client' is installed on Service PC and registered.

Router has been configured and registered.

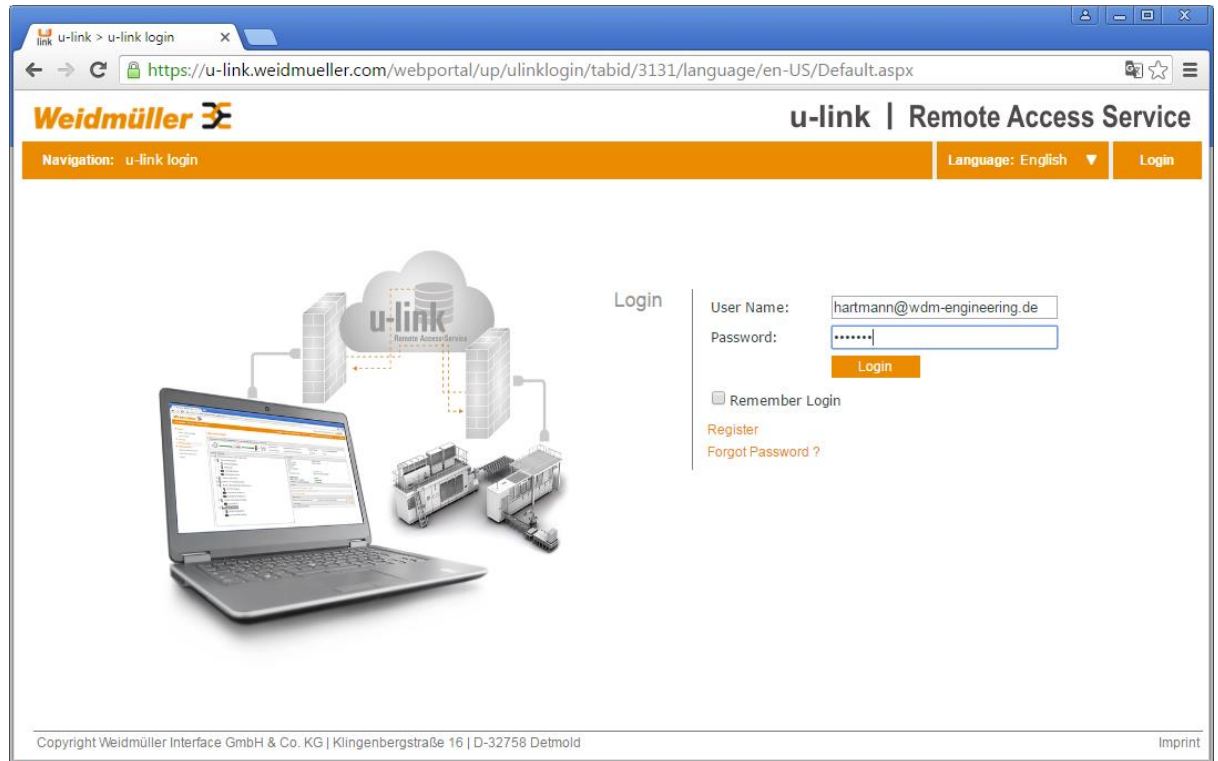
Note:

For demonstrating the access to remote LAN devices we will use the Administrator account.

5.1 Starting a remote access session

Logon to the u-link Web portal using your administrator account (Step 1)

- Enter user name and password of the u-link administrator.
- Click button 'Login'.



5.1 Starting a remote access session

Goto menu Service Desk (Step 2)

- In section 'Device Topology' the same defined objects are displayed which previously have been created in menu 'Device Management'.
- In section 'Connection status PC' the current VPN connection status (of this PC) to the u-link VPN server is displayed.
- In the 'Device Topology' the current connection status of a Router is signaled by following different icon symbols:



- The Router has no connection to u-link.
- Device not configured to use u-link or
 - Device is powered off or
 - Device has no Internet access.



The Router has an online connection to u-link WWH server.



The Router has an active VPN connection to the u-link VPN server.



The Service PC has a pass-through VPN connection via the Router to its LAN network.

u-link | Remote Access Se

Navigation: Service > Service Desk | Active license: Entry Version | Language: English | Logged in as: Heinz Hartmann

Service Desk

Connection status PC: No VPN connection to u-link Portal

VPN connection Service-PC offline
No Router/Remote network selectable

Device Topology

- WDM Engineering Systems
 - Access Router Machine 1
 - Profinet PLC
 - u-remote coupler PN

Status Service PC (u-link VPN client):

- Not connected to u-link

Status Router:

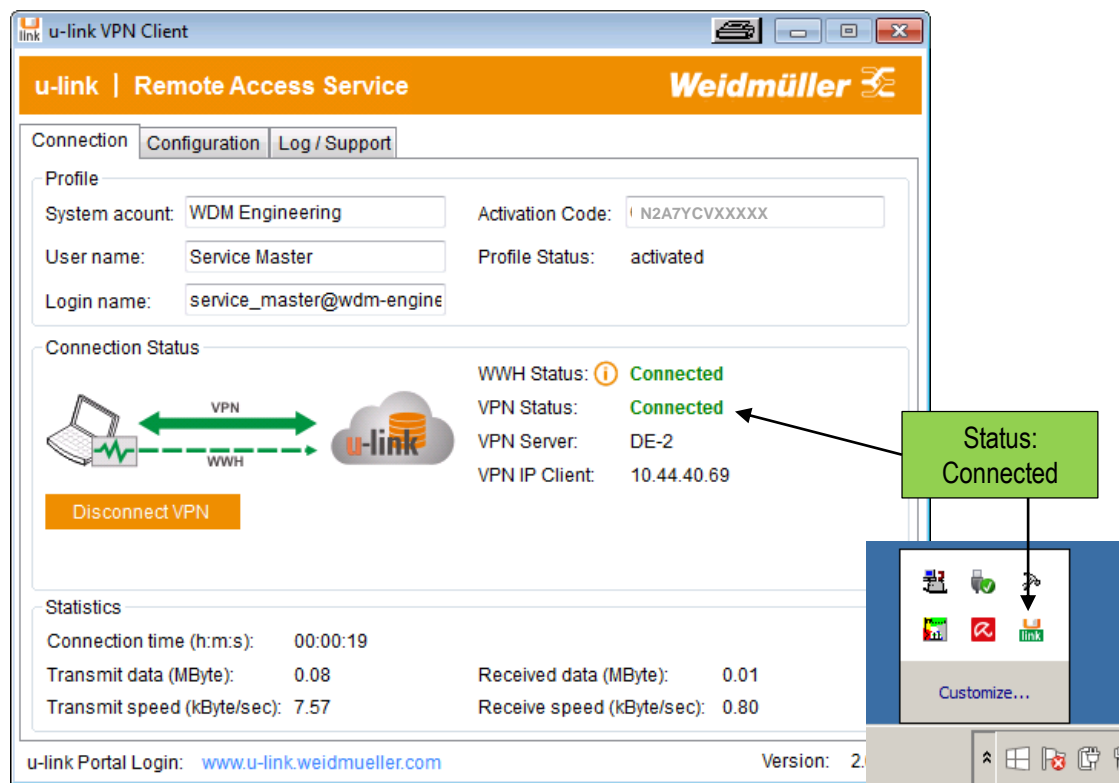
- Connected to u-link via WWH communication
- No VPN connection

For initiating a remote access session the Router must have at least one of these both states.

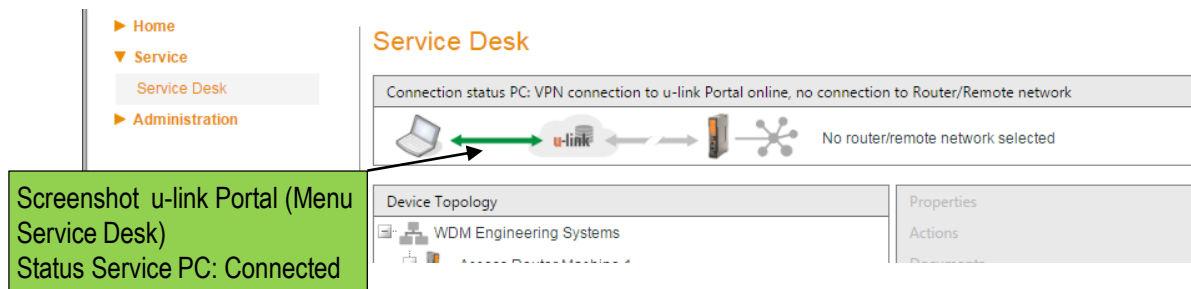
5.1 Starting a remote access session

Connect the Service PC to u-link VPN server (Step 3)

- Start program 'u-link VPN client'.
- Click button 'Connect VPN'.
 - When successfully connected the status and some additional information will be displayed in the program window.
 - The u-link icon in the task bar is displaying a connected status.



- Go back to menu 'Service Desk' of the u-link Web portal.
- The PCs connection to the u-link VPN server will be signalized by a green colored double arrow.
 - Now you are connected to the u-link VPN server but at this time you still do not have a pass-through connection to a Router/Remote network.



5.1 Starting a remote access session

Start the Router VPN connection remotely via Web-Portal (Step 4)

- The VPN connection of the Router to the u-link VPN server can be activated via WWH communication. The permission to activate the Router VPN tunnel remote via u-link Portal can be set or prohibited in menu 'u-link' of the Routers Web interface (default allowed).
- Select the Router by clicking on the Router object (Icon or name) to display the object parameters (Properties, Actions, ...)
- Start the VPN connection by clicking button 'Connect VPN Router ↔ u-link' (Section Actions).
 - Now a 'VPN activate command' will be sent to the Router via WWH connection.
 - Wait around 30...40 seconds then the new status 'Connected' will be displayed.
- Finally both the Service PC and the Router are connected to the u-link VPN server but no pass-through connection via the u-link VPN server is established until now.

Service Desk

Connection status PC: VPN connection to u-link Portal online, no connection to Router/Remote network

No router/remote network selected

Device Topology

- WDM Engineering Systems
 - Access Router Machine 1
 - Profinet PLC
 - u-remote coupler PN

Properties

Name	Access Router Machine 1
Device Type	Router/Firewall
Identification	
Location	Factory Detmold
Serial Number	
IP	192.168.1.254 (LAN port)
Activation Code	KPBUT7ANV6TM

Status-WWH: Active

Status-VPN Router ↔ u-link: Disconnected

Status-VPN PC ↔ u-link ↔ Router: Disconnected

Actions

- Connect VPN Router ↔ u-link
- Connect VPN PC ↔ u-link ↔ Router
- Open Router Web page

Documents

Configuration

Backup of files

Status Router **before** clicking 'Connect VPN Router ↔ u-link'

- Active WWH communication to u-link
- No VPN connection

Service Desk

Connection status PC: VPN connection to u-link Portal online, no connection to Router/Remote network

No router/remote network selected

Device Topology

- WDM Engineering Systems
 - Access Router Machine 1
 - Profinet PLC
 - u-remote coupler PN

Properties

Name	Access Router Machine 1
Device Type	Router/Firewall
Identification	
Location	Factory Detmold
Serial Number	
IP	192.168.1.254 (LAN port)
Activation Code	KPBUT7ANV6TM

Status-WWH: Active

Status-VPN Router ↔ u-link: Connected

Status-VPN PC ↔ u-link ↔ Router: Disconnected

Actions

- Disconnect VPN Router ↔ u-link
- Connect VPN PC ↔ u-link ↔ Router
- Open Router Web page

Documents

Add

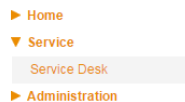
Status Router **after** clicking 'Connect VPN Router ↔ u-link'

- Active WWH communication to u-link
- VPN connection to u-link VPN server established

5.1 Starting a remote access session

Initiate a pass-through connection between Service PC and remote Router (Step 5)

- Click button 'Connect VPN PC ↔ u-link ↔ Router' to establish a pass-through connection between Service PC and the Router.
- A successful pass-through connection is displayed in section 'Connection Status PC' containing following information:
 - Connected to: Name of the selected accessible Router / remote network.
 - Accessible remote network: IP range of accessible remote network.
 - Router VPN IP: Additional VPN-IP address of the Router beside LAN/WAN IP's. Exists as long as the pass-through connection is established. Via this VPN-IP the Router's Web interface also is accessible.
 - Routing to remote network: Status 'active' means that the Service PC has accepted an additional setting in its routing table how to access devices at the remote network.



Service Desk

Connection status PC: VPN connection to u-link Portal online, no connection to Router/Remote network

No router/remote network selected

Device Topology

- WDM Engineering Systems
 - Access Router Machine 1
 - Profinet PLC
 - u-remote coupler PN

Properties

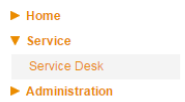
Name	Access Router Machine 1
Device Type	Router/Firewall
Identification	
Location	Factory Detmold
Serial Number	
IP	192.168.1.254 (LAN port)
Activation Code	KPBUT7ANV6TM
Status-WWH	Active
Status-VPN Router ↔ u-link	Connected
Status-VPN PC ↔ u-link ↔ Router	Disconnected

Actions

- Disconnect VPN Router ↔ u-link
- Connect VPN PC ↔ u-link ↔ Router**
- Open Router Web page

Documents Add

Click button to start a pass-through connection between Service PC and Router.



Service Desk

Connection status PC: Connected to Router/Remote network via u-link Portal Disconnect

Connected to: Access Router Machine 1 192.168.1.0/255.255.255.0 10.46.240.4 active

Accessible remote network: Router VPN IP: Routing to Remote network:

Device Topology

- WDM Engineering Systems
 - Access Router Machine 1
 - Profinet PLC
 - u-remote coupler PN

Properties

Name	Access Router Machine 1
Device Type	Router/Firewall
Identification	
Location	Factory Detmold
Serial Number	
IP	192.168.1.254 (LAN port)
Activation Code	KPBUT7ANV6TM
Status-WWH	Active
Status-VPN Router ↔ u-link	Connected
Status-VPN PC ↔ u-link ↔ Router	Connected

Actions

- Disconnect VPN Router ↔ u-link
- Disconnect VPN PC ↔ u-link ↔ Router
- Open Router Web page

Documents Add

Configuration

Changed Router icon signaling a pass-through connection to this Service PC

Established pass-through connection between Service PC and Router.

Now the remote devices (any IP address) connected to LAN port of remote Router can be accessed.

5.1 Starting a remote access session

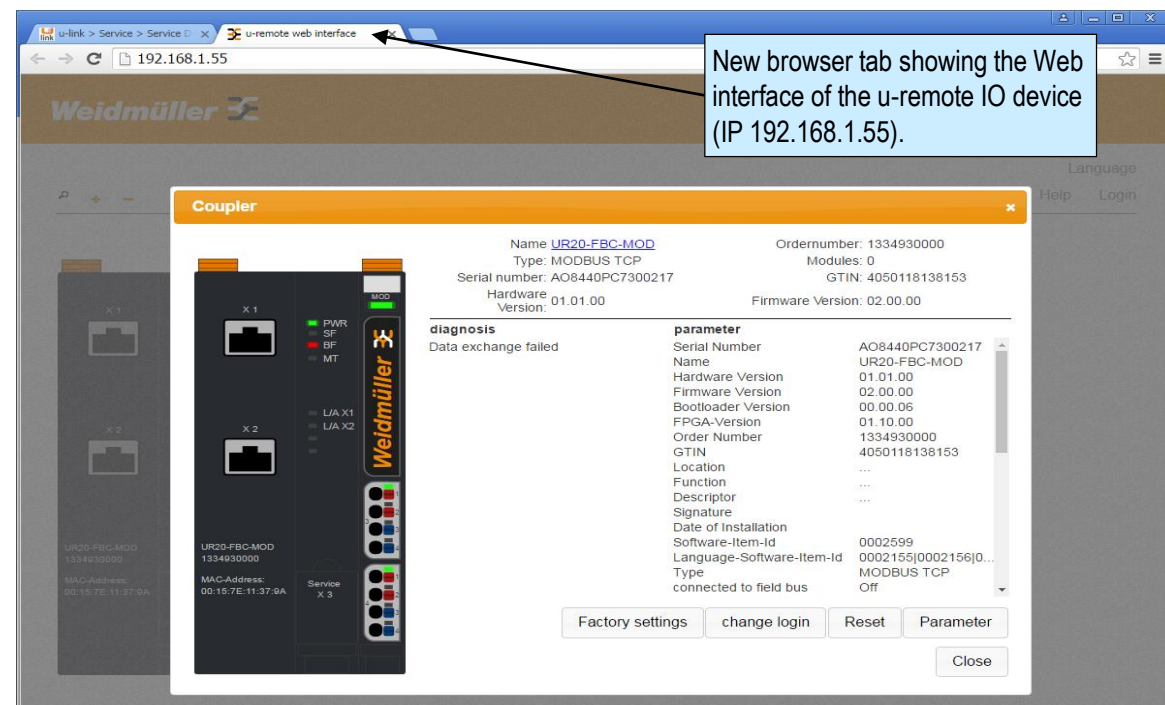
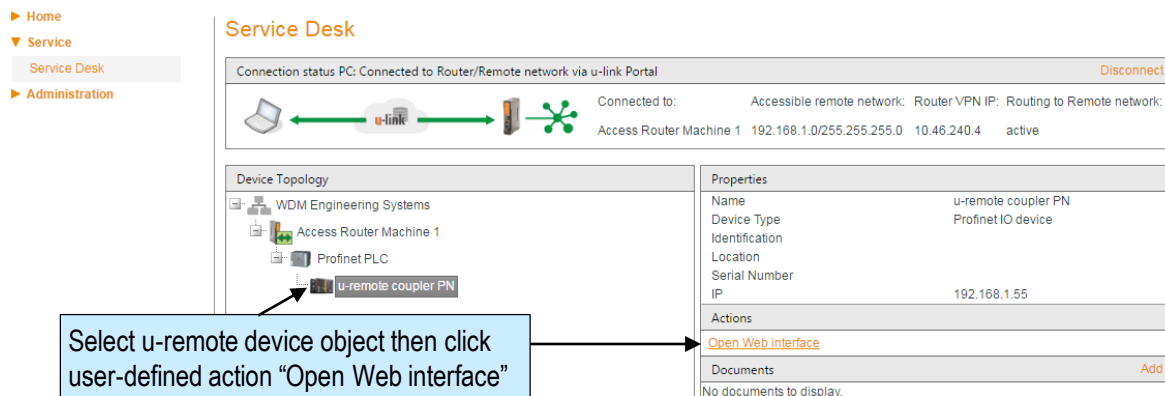
Accessing a remote LAN device (Step 6)

Example shows a Web access to an u-remote IO device.

- When having a VPN pass-through connection then generally all devices at the remote network - matching the LAN net/subnet - are accessible by the Service PC. In this example we will access the Web interface of device 'u-remote coupler PN' (is of type 'User defined end device') via IP 192.168.1.55. For the Web access we use the action "Open Web interface" defined for this object in menu 'Device Management'.
- Select (Highlight) item 'u-remote coupler PN'.
- Click button 'Open Web interface' in section Actions.
- Now a new browser tab will be opened showing the Web interface of the u-remote IO device.
- If no action is defined open a browser manually and enter the directly the IP address into the input line.

Note:

- For security reasons currently only a Web access can be defined as an u-link action.
- But as long as the pass-through connection is established you can run any program or application which needs access to an IP of the remote network.

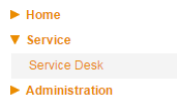


5.2 Closing the remote access session

Disconnect from the selected Router / remote network (Step 7)

(Finish the remote access session)

- First close all active sessions or programs which are accessing IP addresses of the remote network.
- Click button 'Disconnect'.
 - Now you will have the previous status that both the Service PC and the Router are still connected to the u-link VPN server but you have no longer a pass-through connection.
- Select the Router item and click 'Disconnect VPN Router ↔ u-link' to shutdown the Routers VPN tunnel.



Service Desk

Connection status PC: Connected to Router/Remote network via u-link Portal

Connected to: Accessible remote network: Router VPN IP: Routing to Remote network: Access Router Machine 1 192.168.1.0/255.255.255.0 10.46.240.4 active

Device Topology

- WDM Engineering Systems
 - Access Router Machine 1
 - Profinet PLC
 - u-remote coupler PN

Properties

Name	Access Router Machine 1
Device Type	Router/Firewall
Identification	
Location	Factory Detmold
Serial Number	
IP	192.168.1.254 (LAN port)
Activation Code	KPBUT7ANV6TM
Status-WWH	Active
Status-VPN Router ↔ u-link	Connected
Status-VPN PC ↔ u-link ↔ Router	Connected

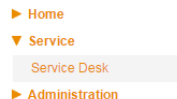
Actions

- Disconnect VPN Router ↔ u-link
- Disconnect VPN PC ↔ u-link ↔ Router**
- Open Router Web page

Documents Add

Configuration

Step 1: Close the VPN pass-through connection of the Service PC to Router / remote network (Use one of the 2 options).



Service Desk

Connection status PC: VPN connection to u-link Portal online, no connection to Router/Remote network

No router/remote network selected

Device Topology

- WDM Engineering Systems
 - Access Router Machine 1
 - Profinet PLC
 - u-remote coupler PN

Properties

Name	Access Router Machine 1
Device Type	Router/Firewall
Identification	
Location	Factory Detmold
Serial Number	
IP	192.168.1.254 (LAN port)
Activation Code	KPBUT7ANV6TM
Status-WWH	Active
Status-VPN Router ↔ u-link	Connected
Status-VPN PC ↔ u-link ↔ Router	Disconnected

Actions

- Disconnect VPN Router ↔ u-link**
- Connect VPN PC ↔ u-link ↔ Router
- Open Router Web page

Documents Add

Step 2: Shutdown the Router VPN connection to the u-link VPN server.

Device Topology

- WDM Engineering Systems
 - Access Router Machine 1
 - Profinet PLC
 - u-remote coupler PN

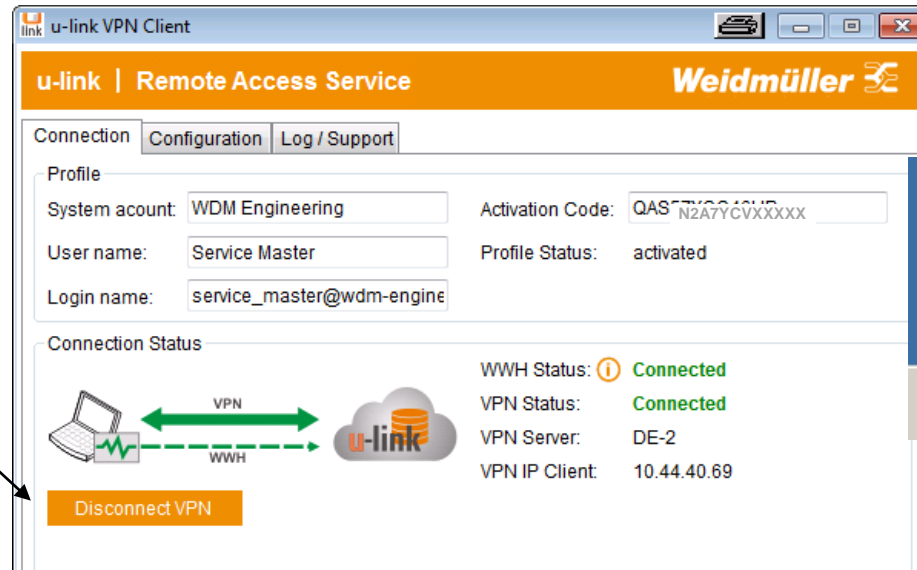
Status 3: New Router status after VPN shutdown showing an active WWH connection.

5.2 Closing the remote access session

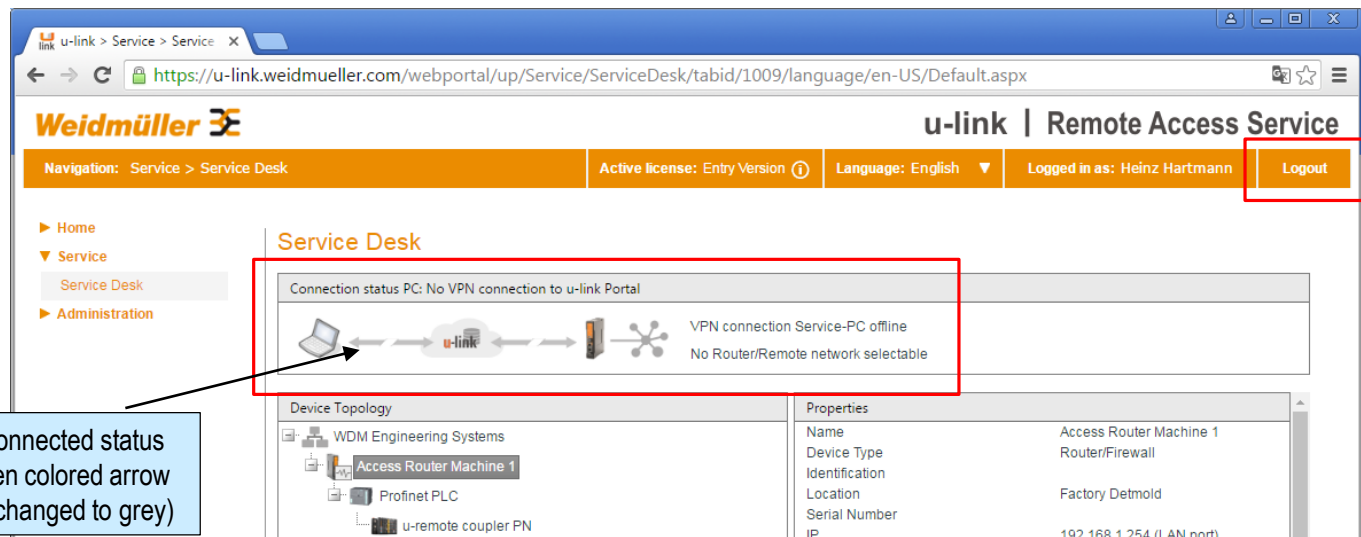
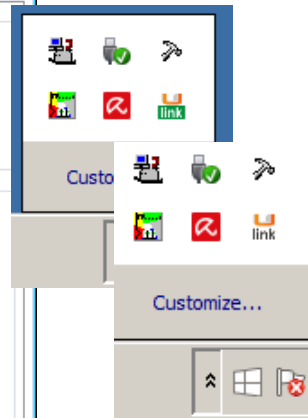
Shutdown the VPN connection of the Service PC / Logout from u-link Portal (Step 8)

- Open the window of the 'u-link VPN client' by clicking the u-link taskbar icon.
- Click button 'Disconnect VPN'.
- Go back to menu 'Service Desk' of the u-link Web portal.
 - After some seconds in section 'Connection status PC' the disconnected status is displayed.
- Click button 'Logout' to close the u-link portal session.
- Finally exit program 'u-link VPN client'.

Remote access procedure is finished!



Background color of u-link icon in the notification area will change from green to white.



Disconnected status (green colored arrow has changed to grey)

Chapter 6: Further functionality

- 1 – Dashboard
- 2 – User defined actions
- 3 – News from your administrator

6.1 Dashboard

- For Router objects there is a dashboard available, which will open in a new tab, when clicked on action button “Open Dashboard”
- On the dashboard you will get status information about the selected router.

- ▶ Home
- ▶ Service
- ▶ Service Desk
- ▶ Administration

Service Desk

Connection status PC: No VPN connection to u-link Portal

VPN connection Service-PC offline
No Router/Remote network selectable

Device Topology

- Weidmüller
 - Germany
 - Athex Klemmenbestücker
 - Demo case u-link Detmold Trainingcenter (see manual attached)
 - Router (Admin: Bernd Wittwer)
 - Hannover Messe OWL Stand

Properties

Name	Router (Admin: Bernd Wittwer)
Device Type	Router/Firewall
Identification	bernd-ulrich.wittwer@weidmueller.de
Location	Trainingcenter Detmold
Serial Number	
Router Location (Country)	
IP	
Activation Code	
Status-WWH	
Status-VPN Router ↔ u-link	Disconnected
Status-VPN PC ↔ u-link ↔ Router	Disconnected

Actions

- Connect VPN Router ↔ u-link
- Connect VPN PC ↔ u-link ↔ Router

Webinterface

- Open Dashboard

Documents

Manual_WM_Security_Routers_V2.02_en.pdf	Handbuch des Routers	↓	✎	🗑️
---	----------------------	---	---	----

Comments

11.07.2018 Problem u-remote behoben

Edited at 9/4/2018 4:17:10 PM

Open Dashboard to get status information

6.1 Dashboard

➤ The dashboard is divided into 4 zones: Device Information, Active Service Connections, WWH History and VPN History

Device Information:
Shows router specific information and offers the possibility to show the router event log. The function “Show event log...” is only available on active WWH connection
The router event log will be deleted by power-loss.

Active service connections:
Shows all users that are currently connected to the router.
The history can be displayed and exported by clicking “Show History...”.

The screenshot shows the Weidmüller dashboard interface. At the top, there is a navigation bar with 'Service > Service Desk > Dashboard' and an 'Active license' indicator. Below the navigation bar, the dashboard title is 'Dashboard for device: Router (Admin: Bernd Wittwer)' with a 'Close dashboard...' link.

The dashboard is divided into four main sections:

- Device Information:** A table-like view showing router details: Name (Router (Admin: Bernd Wittwer)), Type (IE-SR-2GT-LAN), Serial Nr. (AX01710951), Firmware Vers. (3.0.2 - 72728), Activation Code (QESEG58YZK8R), WWH Status (Connected), and VPN Status (Disconnected). A 'Show event log...' link is present at the bottom.
- WWH History (Router to u-link):** A chart showing connection status over time. The status is 'Connected' with a last update of '10/1/2018 10:25:18 AM'. The chart shows a green bar for connection, with a red bar indicating a disconnection on 2018/09/27 01:12:56. A legend indicates green for 'Connected' and red for 'Disconnected'.
- Active Service Connections (PC ↔ u-link ↔ Router):** A table with columns 'User' and 'Connected Since'. It shows 'No users connected to this device.' and a 'Show History...' link.
- VPN History (Router to u-link):** A chart showing VPN connection status over time. The status is 'Disconnected'. The chart shows green bars for VPN connections. A legend indicates green for 'Connected' and grey for 'Disconnected'.

WWH History: Shows the WWH connection of the router to the u-link WWH Server. Red bar represents no connection, while green bar shows connection. Can be used for troubleshooting connection problems e.g. identify fluctuating cellular connection or regular disturbances from firewalls. On mouse-over the exact time of a status change will be displayed. The WWH history can be exported as .csv file via “Export...”

VPN History: Shows the VPN connection of the router to the u-link VPN Server. The green bar represents VPN connection. On mouse-over the exact time of a status change will be displayed. The VPN history can be exported as .csv file via “Export...”

6.1 Dashboard

- Action button “Show event log...” opens a popup which shows the eventlog of the router. The router eventlog will be deleted after power-loss. It can be exported in a .csv file
- Action Button “Show History...” opens a popup which shows the history of service PC’s connected to the router. This information can be used to document service accesses and e.g. to invoice an exact service fee.

Event Log Export...

```

Sep 5 13:41:27 IE-SR-2GT-LAN-AX01710951 u-link: MANAGEMENT: >STATE:1536147687_TCP_CONNECT...
Sep 5 13:41:28 IE-SR-2GT-LAN-AX01710951 u-link: TCP connection established with 62.138.201.23:443
Sep 5 13:41:28 IE-SR-2GT-LAN-AX01710951 u-link: TCPV4_CLIENT link local: [undrt]
Sep 5 13:41:28 IE-SR-2GT-LAN-AX01710951 u-link: TCPV4_CLIENT link remote: 62.138.201.23:443
Sep 5 13:41:28 IE-SR-2GT-LAN-AX01710951 u-link: MANAGEMENT: >STATE:1536147688_WAT...
Sep 5 13:41:28 IE-SR-2GT-LAN-AX01710951 u-link: MANAGEMENT: >STATE:1536147688_AUTH...
Sep 5 13:41:28 IE-SR-2GT-LAN-AX01710951 u-link: TLS: Initial packet from 62.138.201.23:443, sid=ab51bb66_c7ade070
Sep 5 13:41:28 IE-SR-2GT-LAN-AX01710951 u-link: VERIFY OK: depth=2, /O=ads-tec_GmbH_ST/CN=Certificate_Authority
Sep 5 13:41:28 IE-SR-2GT-LAN-AX01710951 u-link: VERIFY OK: depth=1, /O=ads-tec_GmbH_ST/Remote_Service_Cloud/CN=Certificate_Authority
Sep 5 13:41:28 IE-SR-2GT-LAN-AX01710951 u-link: Validating certificate extended key usage
Sep 5 13:41:28 IE-SR-2GT-LAN-AX01710951 u-link: ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
Sep 5 13:41:28 IE-SR-2GT-LAN-AX01710951 u-link: VERIFY EKU OK
Sep 5 13:41:28 IE-SR-2GT-LAN-AX01710951 u-link: VERIFY X509NAME OK: /O=ads-tec/CN=server1
Sep 5 13:41:28 IE-SR-2GT-LAN-AX01710951 u-link: VERIFY OK: depth=0, /O=ads-tec/CN=server1
Sep 5 13:41:29 IE-SR-2GT-LAN-AX01710951 u-link: Data Channel Encrypt Cipher 'AES-256-CBC' initialized with 256 bit key
Sep 5 13:41:29 IE-SR-2GT-LAN-AX01710951 u-link: Data Channel Encrypt Using 160 bit message hash 'SHA1' for HMAC authentication
Sep 5 13:41:29 IE-SR-2GT-LAN-AX01710951 u-link: Data Channel Decrypt Cipher 'AES-256-CBC' initialized with 256 bit key
Sep 5 13:41:29 IE-SR-2GT-LAN-AX01710951 u-link: Data Channel Decrypt Using 160 bit message hash 'SHA1' for HMAC authentication
Sep 5 13:41:29 IE-SR-2GT-LAN-AX01710951 u-link: Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 2048 bit RSA
Sep 5 13:41:29 IE-SR-2GT-LAN-AX01710951 u-link: [server1] Peer Connection Initiated with 62.138.201.23:443
Sep 5 13:41:30 IE-SR-2GT-LAN-AX01710951 u-link: MANAGEMENT: >STATE:1536147690_GET_CONFIG...
                
```

Close

History - Connection User to Device Export...

User	Name	Connection Start	Connection End	Duration
bob.andrew@weidmueller.de	Bob Andrew	9/27/2018 1:09:21 PM	9/27/2018 1:51:39 PM	0:42:18
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 11:28:31 AM	9/27/2018 11:42:44 AM	0:14:13
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 11:24:32 AM	9/27/2018 11:26:45 AM	0:02:13
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 10:36:30 AM	9/27/2018 10:39:42 AM	0:03:12
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 10:31:55 AM	9/27/2018 10:34:54 AM	0:02:59
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 10:30:28 AM	9/27/2018 10:31:11 AM	0:00:43
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 10:29:05 AM	9/27/2018 10:30:23 AM	0:01:18
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 10:26:47 AM	9/27/2018 10:28:59 AM	0:02:12
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 10:22:14 AM	9/27/2018 10:24:14 AM	0:02:00
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 10:11:00 AM	9/27/2018 10:17:12 AM	0:06:12
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 10:07:14 AM	9/27/2018 10:10:13 AM	0:02:59
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 9:17:19 AM	9/27/2018 9:25:08 AM	0:07:49
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 9:12:45 AM	9/27/2018 9:15:10 AM	0:02:25
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 9:11:44 AM	9/27/2018 9:12:10 AM	0:00:26
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 9:09:46 AM	9/27/2018 9:10:11 AM	0:00:25
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 9:08:58 AM	9/27/2018 9:09:38 AM	0:00:40
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 9:07:42 AM	9/27/2018 9:08:15 AM	0:00:33
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 8:45:23 AM	9/27/2018 9:07:36 AM	0:22:13
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 8:45:09 AM	9/27/2018 8:45:17 AM	0:00:08
sebastian.stelzer@weidmueller.org	Sebastian Stelzer	9/27/2018 8:43:18 AM	9/27/2018 8:43:52 AM	0:00:34

Page size: 20 682 items in 35 pages

Close

Weidmüller Navigation: Service > Service Desk > Dashboard

Dashboard for device: Router (Admin: Bernd Wittwer)
Close dashboard...

Device Information

Name: Router (Admin: Bernd Wittwer)

Type: IE-SR-2GT-LAN
Serial-Nr.: AX01710951
Firmware Version: 3.0.2 - 72728
Activation Code: QE5E058YK8R
WWH Status: **Connected**
VPN Status: **Disconnected**

[Show event log...](#)

WWH History (Router to u-link) Based on time zone (UTC+01:00)

Status: **Connected** Last Update: 10/1/2018 10:25:18 AM

Zoom: Hour Day **Week** Month Year From: Sept 24, 2018 To: C

25. Sept 26. Sept 27. Sept 28. Sept 29. Sept 30. Sept

Connected Disconnected

Active Service Connections (PC ↔ u-link ↔ Router)

User	Connected Since
No users connected to this device.	

[Show History](#)

VPN History (Router to u-link) Based on time zone (UTC+01:00)

Status: **Disconnected**

Zoom: Hour Day **Week** Month Year From: Sept 24, 2018 To: C

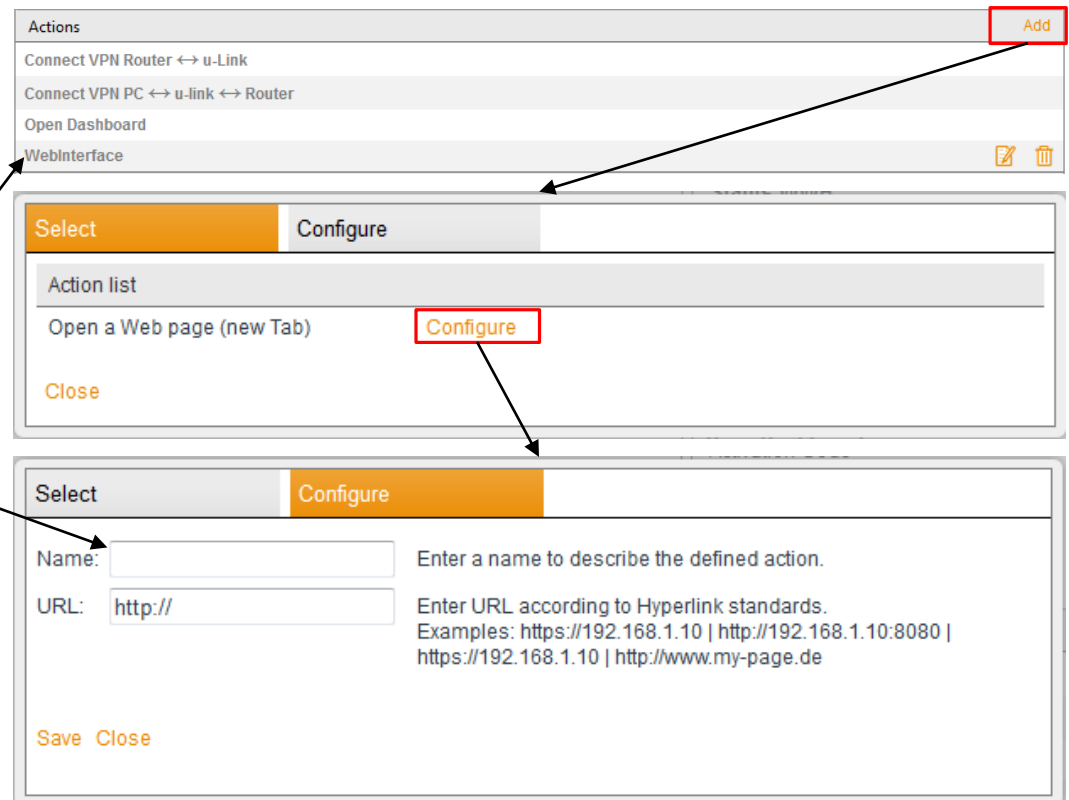
25. Sept 26. Sept 27. Sept 28. Sept 29. Sept 30. Sept

Connected Disconnected

6.2 User-defined actions

- For all objects (Routers, User defined end devices, Groups and Locations) actions can be defined in the Device Management.
- In section actions click on button “Add” to create a user-defined action
- A popup will appear with an actions list. The action “Open a Web page (new Tab)” is listed. More actions may be added later.#
- Klick on “Configure” to configure the action
- With save the action will be saved and can now be used in the Webinterface

Name: The name for the action, that will be shown in the service Desk e.g. Webinterface



The screenshot illustrates the process of adding and configuring a user-defined action in the Weidmüller interface. It is divided into three main sections:

- Actions List:** A table listing existing actions:

Connect VPN Router ↔ u-Link
Connect VPN PC ↔ u-link ↔ Router
Open Dashboard
Webinterface

 An **Add** button is located in the top right corner of this section.
- Action List Configuration:** A popup window with tabs for **Select** and **Configure**. The **Configure** tab is active, showing an **Action list** with the entry "Open a Web page (new Tab)". A **Configure** button is next to this entry.
- Configuration Form:** A form for configuring the selected action. It has two tabs: **Select** and **Configure**. The **Configure** tab is active.
 - Name:** An empty text input field. A text box on the left explains: "Name: The name for the action, that will be shown in the service Desk e.g. Webinterface".
 - URL:** A text input field containing "http://".
 - Instructions:** "Enter a name to describe the defined action." and "Enter URL according to Hyperlink standards. Examples: https://192.168.1.10 | http://192.168.1.10:8080 | https://192.168.1.10 | http://www.my-page.de".
 - Buttons:** **Save** and **Close** buttons at the bottom.

6.3 News from your administrator

- As administrator you can create news for all users in this u-link system account.
- To create news press “Add News” in the “News and Downloads” page
- A popup with an html editor will open

- ▼ Home
- News & Downloads
- User Profile
- Service
- Administration

News & Downloads

Welcome to the u-link Remote Access Service

Your login credentials

User name: Sebastian Stelzer
Login name: sebastian.stelzer@weidmueller.org

News from your administrator

Add news

Welcome to our demo equipment.

DEAR ALL, Friday 28. Sept. 2018 the Demoboard is partly not available!!!

Any question about the demoboard in Trainingscenter you may ask me

9/28/2018 [edit] [delete]

Bernd-Ulrich.Wittwer@Weidmueller.de

Design: Write text or copy and paste images in the editor. The editor will create html code out of the formatted text.
HTML: Write direct html code, copy it from another html editor or view/edit the html code of the news created in “Design”.
Preview: Web-preview of the html code.


Visible for: Decide which user groups are able to see your news.

Release your News

Chapter 7: Standard Functions - Further functionality in Standard Version

- 1 – Firmware Management
- 2 – China Access
- 3 – Password Policy
- 4 – Access Rights
- 5 – Eventlog
- 6 – Templates

7.1 Managing Firmware of connected Routers

- In the menu Firmware Management there is a list of all routers that were created in the portal.
- Only Routers with Internet Connection (as indicated by ) can be updated or selected for update.
- Information about Product, Serial No, Version and Build of the router are displayed (status of last WWH connection) and empty if router wasn't connected before.
- Update multiple selected routers by selecting them and click any "Schedule Update", if update method is restricted, these routers will not be selectable any more.

The screenshot shows the 'Firmware Management' page in the Weidmüller portal. The interface includes a navigation menu on the left, a main content area with a table of routers, and a right-hand sidebar. Callouts point to various elements:

- Logo shows, whether Router has connection to the server or not:** Points to the 'WWH' column containing router status icons.
- Displays further information:** Points to the 'Name' column.
- Unique Serial Number of device:** Points to the 'Serial Number' column.
- Clicking on column header will sort the list according to this attribute:** Points to the 'Status' column header.
- Filter allows easy navigation with many routers:** Points to the 'Activate Filter' button in the top right.
- Select one or multiple Routers for update:** Points to the checkboxes in the leftmost column.
- Name of the Router:** Points to the 'Name' column.
- Router type:** Points to the 'Product' column.
- Current Firmware version and Build number:** Points to the 'Version' and 'Build' columns.
- Perform an update:** Points to the 'Update' column with 'Schedule Update' buttons.
- Shows update history for the device:** Points to the 'History' links in the right sidebar.

WWH	Name	Product	Serial Number	Version	Build	Status	Update	Version	Build	Scheduled	Activate Filter
	IE-SR-2GT-UMTS/3G (AX00730637)	IE-SR-2GT-UMTS/3G	AX00759138	3.2.2	83558		Schedule Update				History
	IE-SR-6GT-LAN (AX02243509)	IE-SR-6GT-LAN	AX02243509	3.2.2	83558		Schedule Update				History
	IE-SR-2GT-LAN (AX01629720)	IE-SR-2GT-LAN	AX01629720	3.2.3	83128						History
	IE-SR-2GT-LTE/4G-M (AX02254366)	IE-SR-2GT-LTE/4G	AX02254366	3.2.2	83558						History
	IE-SR-6GT-LTE/4G (AX02244580)	IE-SR-6GT-LTE/4G	AX02244580	3.2.3	83368						History
	IE-SR-6GT-LTE/4G MESSE	IE-SR-6GT-LTE/4G	AX02253871	3.2.2	80973						History

7.1 Managing Firmware of connected Routers

- With the filter function it is possible to search for specific devices
- The History function shows all Firmware related information with timestamps
- The Schedule Update function is for updating.
 - Select which Firmware should be the new one. All Firmwares available are checked by Weidmüller and are located at Weidmüller Servers

Firmware Management ⓘ

WWH	Name	Product	Serial Number	Version	Build	Status	Update	Version	Build	Scheduled
All										
All	IE-SR-2GT-UMTS/3G (AX00730637)	IE-SR-2GT-UMTS/3G	AX00759138	3.2.2			Schedule Update			History
Online	IE-SR-6GT-LAN (AX02243509)	IE-SR-6GT-LAN	AX02243509	3.2.2			Schedule Update			History
Offline	IE-SR-2GT-LAN (AX01629720)	IE-SR-2GT-LAN	AX01629720	3.2.3						History
Unknown	IE-SR-2GT-LTE/4G-M (AX02254366)	IE-SR-2GT-LTE/4G	AX02254366	3.2.2						History
	IE-SR-6GT-LTE/4G (AX02244580)	IE-SR-6GT-LTE/4G	AX02244580	3.2.3						History
	IE-SR-6GT-LTE/4G (AX02253871)	IE-SR-6GT-LTE/4G	AX02253871	3.2.2	80973					History

With click on filter symbol, advanced settings for filtering can be chosen

Deactivate Filter

Deletes current Filter rules

Reset filter Deactivate Filter

Transmission of firmware over WWH, if actual firmware does not support update via WWH, the update can be performed using a VPN connection

By clicking on Schedule Update, a Firmware update can be performed, a new window will open

Choose new Firmware Version and Build

Manual: Immediate update
Schedule: Update on defined Timeslot

Attention! Scheduled time will be Server time (Winter UTC+1, Summer UTC+2)

Schedule Update

Please note: The amount of simultaneous updates is limited to 10 devices. More than 10 devices will be divided in groups of 10 devices each and these groups will be updated successively.

Update device using: WWH

Firmware Version: Select Version...

Build Number: Select Build...

Scheduled Date: Now

Update Close

VPN Update

Please note: The amount of simultaneous updates is limited to 10 devices. More than 10 devices will be divided in groups of 10 devices each and these groups will be updated successively.

Update device using: VPN

Firmware Version: Select Version...

Build Number: Select Build...

Scheduled Date: Now

Admin Password:

Update Close

Timestamp	Level	Mode	Message	User
7/19/2018 2:50:38 PM	Error	VPN	Firmware Update is finished: The password is incorrect	Sebastian Stetler
7/19/2018 2:50:18 PM	Info	VPN	Downloading the firmware file: New Version 3.2.1 with Build 79731	Sebastian Stetler
7/19/2018 2:49:58 PM	Info	VPN	Firmware Update is started: New Version 3.2.1 with Build 79731	Sebastian Stetler
7/19/2018 2:49:38 PM	Error	WWH	Firmware Update is finished: The new firmware can not be downloaded	Sebastian Stetler
7/19/2018 2:47:58 PM	Info	WWH	Downloading the firmware file: New Version 3.2.1 with Build 79731	Sebastian Stetler
7/19/2018 2:47:43 PM	Info	WWH	Firmware Update is started: New Version 3.2.1 with Build 79731	Sebastian Stetler
7/19/2018 10:10:50 AM	Error	VPN	Firmware Update is finished: The password is incorrect	Sebastian Stetler
7/19/2018 10:10:29 AM	Info	VPN	Downloading the firmware file: New Version 3.2.1 with Build 79731	Sebastian Stetler
7/19/2018 10:09:56 AM	Error	VPN	Firmware Update is finished: The password is incorrect	Sebastian Stetler
7/19/2018 10:09:35 AM	Info	VPN	Downloading the firmware file: New Version 3.2.1 with Build 79731	Sebastian Stetler
7/19/2018 10:09:14 AM	Info	VPN	Firmware Update is started: New Version 3.2.1 with Build 79731	Sebastian Stetler
7/19/2018 10:07:18 AM	Error	WWH	Firmware Update is finished: The new firmware can not be downloaded	Sebastian Stetler
7/19/2018 10:05:41 AM	Info	WWH	Downloading the firmware file: New Version 3.2.1 with Build 79731	Sebastian Stetler
7/19/2018 10:05:29 AM	Info	WWH	Firmware Update is started: New Version 3.2.1 with Build 79731	Sebastian Stetler
7/19/2018 10:03:32 AM	Error	WWH	Firmware Update is finished: There are unsaved settings	Sebastian Stetler
7/19/2018 10:03:28 AM	Info	WWH	Firmware Update is started: New Version 3.2.1 with Build 79731	Sebastian Stetler
7/19/2018 10:00:02 AM	Error	WWH	Firmware Update is finished: There are unsaved settings	Sebastian Stetler
7/19/2018 10:00:02 AM	Info	WWH	Firmware Update is started: New Version 3.2.1 with Build 79731	Sebastian Stetler

By clicking on History, all firmware update information regarding the specific device will be displayed

In case of Update via VPN, the admin password of the router is needed

7.1 Managing Firmware of connected Routers

- After scheduling an update, information about the update are displayed in the Firmware Management window.
- With “Change” the planned updates can be edited or deleted.
- When more than 10 devices per u-link account (including all users) are scheduled at the same, they will be bunched together in groups of 10, which will be updated successively. E.g. 27 devices are updated: First devices 1-10, then 11-20, then 21-27 are updated.

Firmware Management ⓘ

WWH	Name	Product	Serial Number	Version	Build	Status	Update	Version	Build	Scheduled	
<input type="checkbox"/>	IE-SR-2GT-UMTS/3G (AX00730637)	IE-SR-2GT-UMTS/3G	AX00759138	3.2.2	83558		Change	3.2.2	83558	8/21/2018 9:00 AM	History
<input type="checkbox"/>	IE-SR-6GT-LAN (AX02243509)	IE-SR-6GT-LAN	AX02243509	3.2.2	83558		Schedule Update				History
<input type="checkbox"/>	IE-SR-2GT-LAN (AX01629720)	IE-SR-2GT-LAN	AX01629720	3.2.3	83128						History
<input type="checkbox"/>	IE-SR-2GT-LTE/4G-M (AX02254366)	IE-SR-2GT-LTE/4G	AX02254366	3.2.2	83558						History
<input type="checkbox"/>	IE-SR-6GT-LTE/4G (AX02244580)	IE-SR-6GT-LTE/4G	AX02244580	3.2.3	83368						History
<input type="checkbox"/>	IE-SR-6GT-LTE/4G MESSE	IE-SR-6GT-LTE/4G	AX02253871	3.2.2	80973						History

Date and time, when update will be performed

New build number after update

New Firmware Version after update

Change Update

Please note:
The amount of simultaneous updates is limited to 10 devices. More than 10 devices will be divided in groups of 10 devices each and these groups will be updated successively.

Update device using:

Firmware Version:

Build Number:

Scheduled Date:

[Save](#) [Delete](#) [Close](#)

Possibility to change or cancel update

7.1 Managing Firmware of connected Routers

- After start of an update the current status will be displayed.
- The status will be updated by reloading of the website/the table which is every 5 seconds.
- After successful update the router will restart. The restarting of the router might take up to 60 seconds

Status of the update, will be renewed every 5 seconds
 After successful or disrupted update the status will be deleted after 10 minutes.
 The final status can then be found in the History

Firmware Management ⓘ

WWH	Name	Product	Serial Number	Version	Build	Status	Update	Version	Build	Scheduled	
<input type="checkbox"/>	IE-SR-2GT-UMTS/3G (AX00730637)	IE-SR-2GT-UMTS/3G	AX00759138	3.2.2	83558	Info: Firmware Update started: New Version 3.2.2 with Build 83558	Update	3.2.2	83558	8/20/2018 8:22 AM	History
<input checked="" type="checkbox"/>	IE-SR-6GT-LAN (AX02243509)	IE-SR-6GT-LAN	AX02243509	3.2.2	83558		Schedule Update				History
<input type="checkbox"/>	IE-SR-2GT-LAN (AX01629720)	IE-SR-2GT-LAN	AX01629720	3.2.3	83128						History
<input type="checkbox"/>	IE-SR-2GT-LTE/4G-M (AX02254366)	IE-SR-2GT-LTE/4G	AX02254366	3.2.2	83558						History
<input type="checkbox"/>	IE-SR-6GT-LTE/4G (AX02244580)	IE-SR-6GT-LTE/4G	AX02244580	3.2.3	83368						History
<input type="checkbox"/>	IE-SR-6GT-LTE/4G MESSE	IE-SR-6GT-LTE/4G	AX02253871	3.2.2	80973						History
<input type="checkbox"/>	Maschine 3										History
<input type="checkbox"/>	Router WK1										History
<input type="checkbox"/>	Windkraftanlage 2										History
<input type="checkbox"/>	WK1										History

7.2 China Access

- China prevents cross-border VPN connections with the so called Great China Firewall. As soon as VPN tunnels are detected they are shut down immediately, which also prevents remote access solutions to machines.
- As the u-link servers are located in Europe, a cross border connection is every connection with:
 - u-link VPN Client in China
 - Router in China
 - Both Router and Client in China
- With selecting “China” as Location the VPN tunnel will be routed via a server located in China and use a certified secure connection between Chinese and European servers
- The Server for single routers can be set in the Device Management by selecting the device in Device Configuration
- The Server for u-link Clients (Service PC’s) can be set for the specific user in the User Profile

The screenshot displays the Weidmüller web interface. On the left, a navigation menu includes 'Home', 'Service', 'Administration', 'User Management', 'Device Management' (highlighted with a red box), 'Firmware Management', and 'Account Management'. The main content area is divided into 'Device Management' and 'User Profile'.

Router Location (Country) dialog: A dropdown menu shows 'World except China' selected. Below it, text reads: 'and the appropriate VPN server for the'. A note states: 'If the device is connecting from China please make sure to select China.' Buttons for 'Save' and 'Cancel' are at the bottom.

Settings for Routers: A blue callout box points to the 'Router Location (Country)' field in the 'Device configuration' table, which is set to 'World except China'.

Settings for u-link VPN Client (Service PC): A blue callout box points to the 'User Location' dropdown in the 'User Profile' form, which is set to 'World except China'.

User Profile form: Shows 'User data' (First Name: Sebastian, Last Name: Stelzer) and 'Profile' (Group member from: Administratoren). The 'User Location' dropdown is at the bottom right.

7.3 Password Policy

- To ensure the security of the user accounts, a password policy can be set for the whole account
- In the password policy the settings for minimum amount of:
 - Characters (Password Length)
 - Symbols
 - Uppercase characters
 - Lowercase Characters
 - Number Characters

Can be set. The minimum is set to 8 at password length and 0 for all other requirements

- The new requirements will come into effect when a user changes his password and for all new created users
- To have a permanently renew of passwords, a password **Change Cycle** can be set. The value can be between 0 and 999 days, in which 0 disables the change cycle.
- After expiration of the password, the users will be forced at the next login to change their password.
- The last used password will not be allowed to be the new one.
- To force the new established policy to all users directly, use a Change Cycle of 1 day and afterwards set the Change Cycle to the desired amount of days



Navigation: Administration > Account Management

[Home](#) | [Service](#) | [Administration](#)

- User Management
- Device Management
- Firmware Management
- Account Management**

[Status / Statistics](#) | [Eventlog](#) | **[Password Policy](#)** | [Account Informations](#)

Password Policy

By modifying the values below you can enforce a specific password policy. Passwords must comply with this policy when creating new users or a users changes the password in the user profile.

Password Length: The password must be at least 8 characters!
 Symbols:
 Uppercase Characters:
 Lowercase Characters:
 Number Characters:

Change Cycle

Changing the following value sets the interval at which the user must change the password. Depending on the size of this interval, a note about the expiration of the password with the possibility to change it will be displayed after login one or several days before. The value 0 disables the password change cycle.

Days:

[Save](#) [Restore](#)

7.4 Access Rights

- Access rights can be set for every object in the Device Topology.
- It is a **whitelist** of groups, where at non-router objects the visibility and at router objects the visibility and accessibility of IP, Port and Protocol can be set
- By creating a new device, all user groups will get visibility and access to all IP's, Ports and all Protocols marked with “*”
- Settings:
 - Removing a group means that all users of that group won't be able to see this object in their device topology anymore
 - Specifying an IP address (range) – all users of the group can connect to the subnet, but have access to defined IP address (ranges) only
 - Specifying Port (range) - all users of the group can connect to the subnet, but have access to defined Port (ranges) only
 - Specifying Protocols - all users of the group can connect to the subnet, but can use defined Protocols only
- The entries of allowed IP-addresses, Ports and Protocols are handled **additively** within the list and over several user groups.
- To ensure that the settings come into effect, please reconnect the u-link VPN clients

- ▶ Home
- ▶ Service
- ▼ Administration
 - User Management
 - Device Management**
 - Firmware Management
 - Account Management

Device Management

Device Topology

Mustermann Maschinenbau GmbH

- Buero
 - IE-SR-2GT-LAN (AX00759082)
 - IE-SR-2GT-LTE/4G-M (AX02254366)

Device configuration		Access rights (groups)	New		
Object visible for listed groups / Assignment of accessible IP addresses via Router					Add
Group Name	IP address list	Ports	Protocols	Actions	
Administrators	*	*	ICMP TCP	ⓘ ⚙️ 🗑️	
Service	192.168.1.110	*	*	ⓘ ⚙️ 🗑️	

7.4 Access Rights

Examples for several entries:

IP address list	Ports	Protocols
*	*	*
192.168.1.110	80	UDP

Line 1 includes Line 2, so that all IP addresses with all Ports and Protocols are allowed.

IP address list	Ports	Protocols
*	*	TCP
192.168.1.110	80	UDP

Line 1 allows access to all IP addresses with all Ports and TCP Protocol.

Line 2 allows **additionally** access to IP 192.168.1.110 on Port 80 with UDP Protocol.

Examples for several groups (User is member on User group A, and User group B):

User group A:

IP address list	Ports	Protocols
*	*	TCP

User group B:

IP address list	Ports	Protocols
192.168.1.110	80	UDP

As at the previous example, the user is allowed to access all IP addresses on all Ports with TCP Protocol by rights of User group A. As he is also member of User group B he can **additionally** access the IP 192.168.1.110 on Port 80 with UDP Protocol.

Edit group-based access rights to IP addresses via Router

Selected group:

Administrators

Accessible via Router:

IP address list	Ports	Protocols	Actions
*	*	ICMP	
*	*	TCP	

Enter:

IP Addresses: * Ports: * Protocol: * [Add](#)

Enter character "*" (asterisk) to allow access to all IP addresses via the Router. For limited access please enter a single IP address, an IP address range separated by "-" character or an IP network range with subnet mask. An additional specification of communication ports and protocols will limit the access accordingly.

Examples:

IP address list	Ports	Protocol
*	*	*
192.168.1.10	*	ICMP
192.168.1.50-192.168.1.60	22,3389	TCP
192.168.20.0/24	80,10000,12333	TCP

The access limitation of a group member (User) always refers to target IP addresses reachable via the Router dependent of the communication protocol or application-specific ports.
If an user is member of 2 or more groups (assigned to this Router object) then the access rights of the user will be merged based on the group memberships.

Attention - changes on these access limitations will take effect not before the u-link client reconnects!

[Save](#) [Cancel](#)

u-link | Remote Access Service

Active license: Standard Version ⓘ Language: English ▼ Logged in as: sebastian.stelzer@weidmueller.de Logout

Device configuration	Access rights (groups)	New		
Object visible for listed groups / Assignment of accessible IP addresses via Router Add				
Group Name	IP address list	Ports	Protocols	Actions
Administrators	*	*	ICMP TCP	
Service	192.168.1.110	*	*	

7.4 Access Rights

- If a user has restricted access to the local network of a router, the information will be displayed in the service desk as “Accessible network (restricted)”
- To get more information the user can click at the info button. A window will turn up which will show the access settings.

The screenshot shows the Weidmüller service desk interface. The navigation bar includes 'Service > Service Desk' and 'Active license: Standard Ve'. The left sidebar has 'Home', 'Service', 'Service Desk', and 'Administration'. The main area is titled 'Service Desk' and shows 'Connection status PC: Connected to Router/Remote network via u-link Portal'. A diagram illustrates the connection between a PC and a router. The status 'Connected to: IE-SR-2GT-UMTS/3G (AX00730637)' is shown. A box labeled 'Accessible network (restricted): 192.168.1.0/255.255.255.0' has an info icon. A dialog box titled 'Restricted network access' is open, displaying the following table:

IP addresses	Ports	Protocol
192.168.1.0/24	80,8080,433	TCP

The dialog box also includes a 'Close' button.

7.5 Eventlog

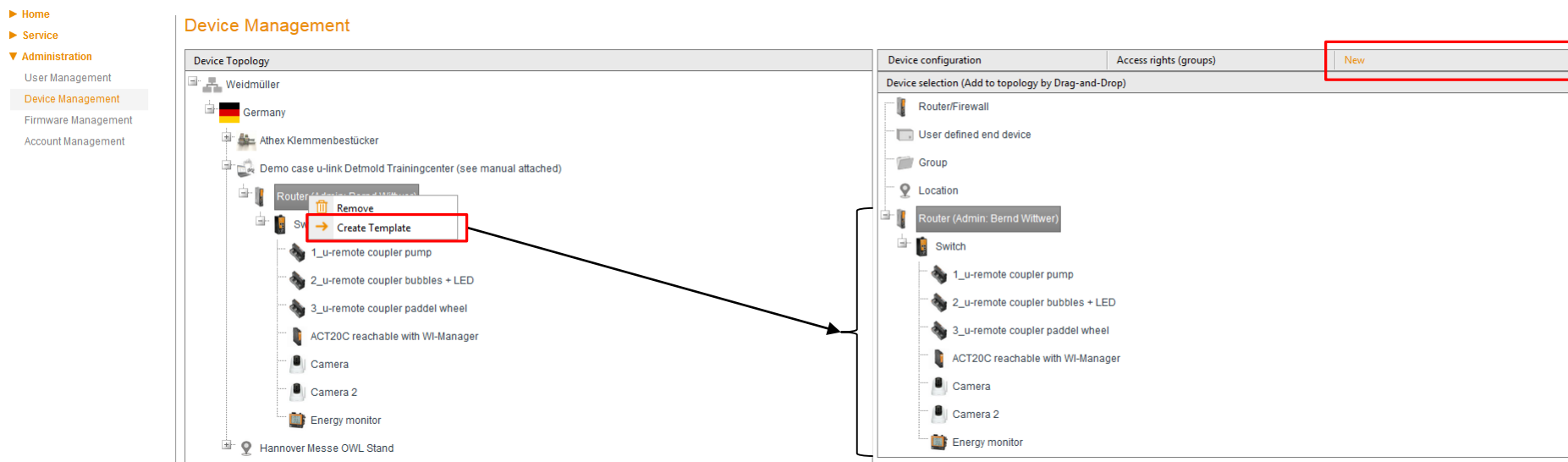
- The Eventlog displays all actions that happen in the portal.
- The Date for the Eventlog will be the Servedtime, which is (Winter UTC+1, Summer UTC+2).
- The eventlog can be filtered to show a specific timeframe, category level or messages with a specific text.
- The export-function will generate an .csv file with all entries fitting to actual filter rules

- ▶ Home
- ▶ Service
- ▼ Administration
 - User Management
 - Device Management
 - Device Management 1.2
 - Firmware Management
 - Account Management

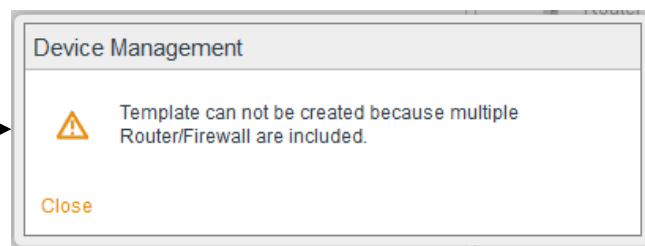
Status / Statistics		Eventlog	Password Policy	Account Information
From:	8/1/2018 12:00 AM	Till:	9/1/2018 12:00 AM	Category: All
				Level: All
				Text search: <input type="text"/>
				Apply filter...
				Export...
Date	Level	Category	User	Message
8/20/2018 9:50:56 AM	Info	Service	Sebastian Stelzer	User is disconnecting vpn for device 'IE-SR-2GT-UMTS/3G (AX00730637)'.
8/20/2018 9:50:53 AM	Info	Service	Sebastian Stelzer	User is disconnecting from device 'IE-SR-2GT-UMTS/3G (AX00730637)'.
8/20/2018 9:38:53 AM	Info	Service	Sebastian Stelzer	User is connecting to device 'IE-SR-2GT-UMTS/3G (AX00730637)'.
8/20/2018 9:38:32 AM	Info	Service	Sebastian Stelzer	User is activating vpn for device 'IE-SR-2GT-UMTS/3G (AX00730637)'.
8/20/2018 8:28:26 AM	Error	Firmware Update	Sebastian Stelzer	Firmware update failed for 'IE-SR-6GT-LAN (AX02243509)': Timeout while executing WWH command
8/20/2018 8:27:22 AM	Info	Firmware Update	Sebastian Stelzer	Firmware update started for 'IE-SR-6GT-LAN (AX02243509)': New Version 3.2.2 with Build 82950
8/20/2018 8:26:41 AM	Error	Firmware Update	Sebastian Stelzer	Firmware update failed for 'IE-SR-2GT-UMTS/3G (AX00730637)': Timeout while executing WWH command
8/20/2018 8:25:37 AM	Info	Firmware Update	Sebastian Stelzer	Firmware update started for 'IE-SR-2GT-UMTS/3G (AX00730637)': New Version 3.2.2 with Build 82950
8/20/2018 8:25:27 AM	Error	Firmware Update	Sebastian Stelzer	Firmware update failed for 'IE-SR-2GT-UMTS/3G (AX00730637)': Timeout while executing WWH command
8/20/2018 8:24:22 AM	Info	Firmware Update	Sebastian Stelzer	Firmware update started for 'IE-SR-2GT-UMTS/3G (AX00730637)': New Version 3.2.2 with Build 83558
8/20/2018 8:23:26 AM	Error	Firmware Update	Sebastian Stelzer	Firmware update failed for 'IE-SR-2GT-UMTS/3G (AX00730637)': Timeout while executing WWH command
8/20/2018 8:22:22 AM	Info	Firmware Update	Sebastian Stelzer	Firmware update started for 'IE-SR-2GT-UMTS/3G (AX00730637)': New Version 3.2.2 with Build 83558
8/20/2018 7:50:47 AM	Info	Portal	Sebastian Stelzer	User login ok
8/17/2018 1:19:49 PM	Info	Service	Sebastian Stelzer	Failed to connect to device with auth. name 'XA4STRKMKMVN'. VPN client of user failed to connect.
8/17/2018 1:19:44 PM	Info	Service	Sebastian Stelzer	User is connecting to device 'IE-SR-2GT-UMTS/3G (AX00730637)' with auth. name 'XA4STRKMKMVN'.
8/17/2018 1:19:03 PM	Info	Service	Sebastian Stelzer	Failed to connect to device with auth. name '94BMM8EJAXJR'. VPN client of user failed to connect.
8/17/2018 1:18:58 PM	Info	Service	Sebastian Stelzer	User is connecting to device 'IE-SR-6GT-LAN (AX02243509)' with auth. name '94BMM8EJAXJR'.
8/17/2018 1:18:38 PM	Info	Service	Sebastian Stelzer	Failed to connect to device with auth. name '94BMM8EJAXJR'. VPN client of user failed to connect.
8/17/2018 1:18:33 PM	Info	Service	Sebastian Stelzer	User is connecting to device 'IE-SR-6GT-LAN (AX02243509)' with auth. name '94BMM8EJAXJR'.
8/17/2018 1:17:39 PM	Info	Service	Sebastian Stelzer	Failed to connect to device with auth. name '94BMM8EJAXJR'. VPN client of user failed to connect.
8/17/2018 1:17:33 PM	Info	Service	Sebastian Stelzer	User is connecting to device 'IE-SR-6GT-LAN (AX02243509)' with auth. name '94BMM8EJAXJR'.
8/17/2018 1:17:26 PM	Info	Service	Sebastian Stelzer	User is disconnecting from device 'IE-SR-2GT-UMTS/3G (AX00730637)' with auth. name 'XA4STRKMKMVN'.
8/17/2018 1:14:58 PM	Info	Service	Sebastian Stelzer	User connected to device with auth. name 'XA4STRKMKMVN'.
8/17/2018 1:11:58 PM	Info	Service	Sebastian Stelzer	User is connecting to device 'IE-SR-2GT-UMTS/3G (AX00730637)' with auth. name 'XA4STRKMKMVN'.
8/17/2018 1:11:55 PM	Info	Service	Sebastian Stelzer	User is disconnecting from device 'IE-SR-2GT-UMTS/3G (AX00730637)' with auth. name 'XA4STRKMKMVN'.
8/17/2018 1:11:46 PM	Info	Service	Sebastian Stelzer	User connected to device with auth. name 'XA4STRKMKMVN'.
8/17/2018 1:10:49 PM	Info	Service	Sebastian Stelzer	User is connecting to device 'IE-SR-2GT-UMTS/3G (AX00730637)' with auth. name 'XA4STRKMKMVN'.
8/17/2018 1:10:44 PM	Info	Service	Sebastian Stelzer	Failed to connect to device with auth. name 'XA4STRKMKMVN'. VPN client of user failed to connect.
8/17/2018 1:10:44 PM	Info	Service	Sebastian Stelzer	User is connecting to device 'IE-SR-2GT-UMTS/3G (AX00730637)' with auth. name 'XA4STRKMKMVN'.
8/17/2018 1:10:36 PM	Info	Service	Sebastian Stelzer	User is disconnecting from device 'IE-SR-2GT-UMTS/3G (AX00730637)' with auth. name 'XA4STRKMKMVN'.

7.6 Templates

- For managing several similar remote IP networks, there is the possibility to create templates
- To create a template, right click on a Location/Folder/Router/User defined object in the Device Topology in menu Device Management and click “Create Template”
- Now a copy of all devices that are below the selected one in the topology will be created in the menu “Add Device/Object”
- This whole group can now be added to the device topology by drag and drop again.
- A template can not include more than 1 Router object



Error when creating a template including multiple routers



Appendix

- 1 – Registration of Router to u-link failed (How to solve)
- 2 – General support in case of Router problem issues
- 3 – Functional diagram of u-link
- 4 – Connection requirements of u-link VPN clients (Service PC / Router)
- 5 – Activating / de-activating Router VPN connection by digital input
- 6 – Technical u-link support

A1 - Router registration failed

Failure message 1: *Registration failed - Check registration code, ensure that status of activation code in u-link portal is set to 'not used' or 'Released for additional activation'*

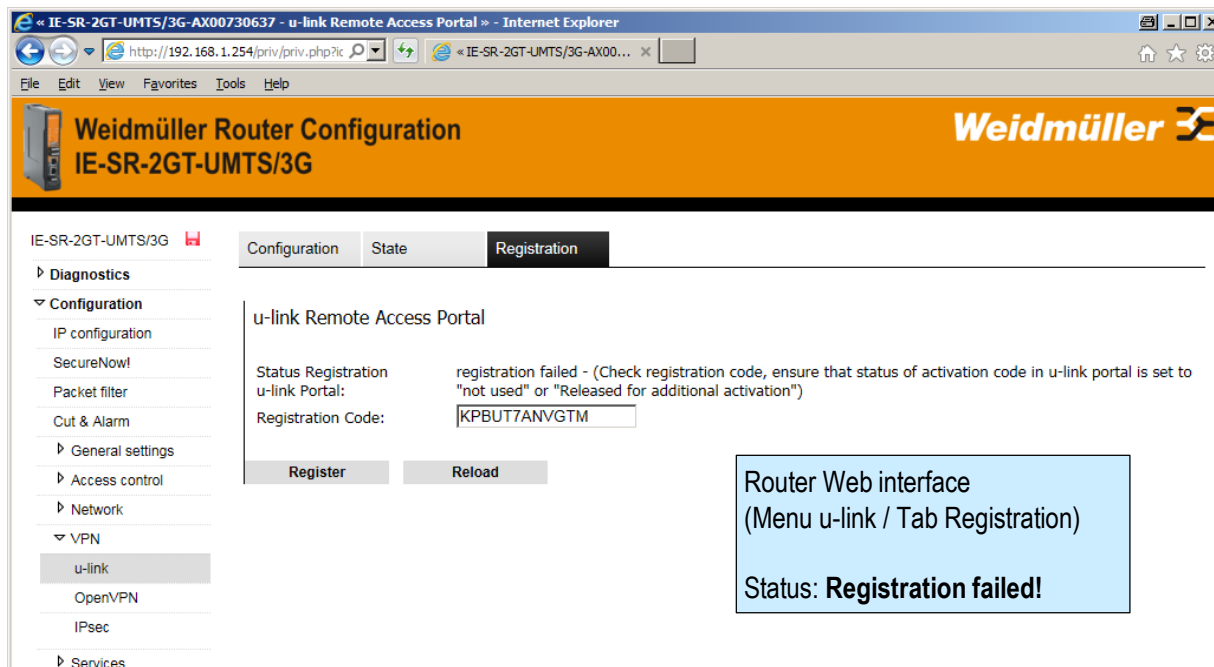
Following issues can cause this error:

Error 1 - A wrong activation code was entered.

- Please verify the activation code. If entered wrong repeat the registration process.

Error 2 - Values Date / Time of the Router are not set correctly.

- Goto menu 'General settings → Date&Time', enter values for Date/Time manually and enable checkbox NTP synchronization. Then click button 'Apply settings'. Then repeat the registration process.



The screenshot shows the Weidmüller Router Web interface in Internet Explorer. The browser title is "IE-SR-2GT-UMTS/3G-AX00730637 - u-link Remote Access Portal". The address bar shows "http://192.168.1.254/priv/priv.php?ic". The page title is "Weidmüller Router Configuration IE-SR-2GT-UMTS/3G". The navigation menu on the left includes "Diagnostics", "Configuration", "VPN", and "Services". The "u-link" menu item is selected. The main content area shows the "u-link Remote Access Portal" configuration page. The "Registration" tab is active, displaying the following information:

Status Registration	registration failed - (Check registration code, ensure that status of activation code in u-link portal is set to "not used" or "Released for additional activation")
u-link Portal:	
Registration Code:	<input type="text" value="KPBUT7ANVGTM"/>

Below the registration information are two buttons: "Register" and "Reload".

**Router Web interface
(Menu u-link / Tab Registration)**

Status: Registration failed!

A1 - Router registration failed

Failure message 1 continued

Error 3 - The entered activation code already has been used either for registering another Router or you have tried to register this Router a second time.

A registration / activation code may be used only one time for registering a Router. The activation code is used to dedicate uniquely a physical Router to a configured u-link Router object (u-link Device Management). In order to avoid an un-controlled multiple use of the same activation code an additional use has to be released before re-registering.

Normally there are only 2 use cases for additional use of an activation code:

1. A defective u-link Router has to be replaced by a new device (manually configured like the defective Router).
2. The configuration of an u-link Router was overwritten (eg. un-registered) or a reset to factory defaults has been done.

How to release for additional use:

- Logon-on to the u-link Web portal.
- Open menu 'Device Management' and highlight the Router object.
- In section 'Device Configuration' click icon 'Edit ' of parameter 'Activation code'.
- Then enable checkbox 'Release for additional activation'.
- Now try again to register the Router.

Note: The checkbox only can be set if the status is 'In Use', a new not assigned activation code displays the status 'Not used'.

u-link Web portal
Menu Device Management

Device configuration	Access rights (groups)	New
Properties		
Name	Access Router Machine 1	
Icon		
Device Type	Router/Firewall	
Identification		
Location	Factory Detmold	
Serial Number		
IP	192.168.1.254 (LAN port)	
Activation Code	KPBUT7ANV6TM	

Status / Reuse of activation code

Activation Code: KPBUT7ANV6TM

State: In use

Release for additional activation:

Note:
If an activation code with status „In use“ shall be used again, eg. in case of replacement of a defective Router which is assigned to this code, then the Checkbox „Release for additional activation“ must be set before registering the replacement Router. After registration of the new Router using this activation code the status automatically will be reset to value „In use“.

Attention:
You always may assign an activation code only to one Router, otherwise the unique assignment of a physical device to a defined device configured in the u-link device topology can not be ensured.

Close

A1 - Router registration failed

Failure message 2: *Registration failed - Network error (Check network and proxy settings)*

1. Investigate generally the Internet accessibility in terms of configured network parameters:

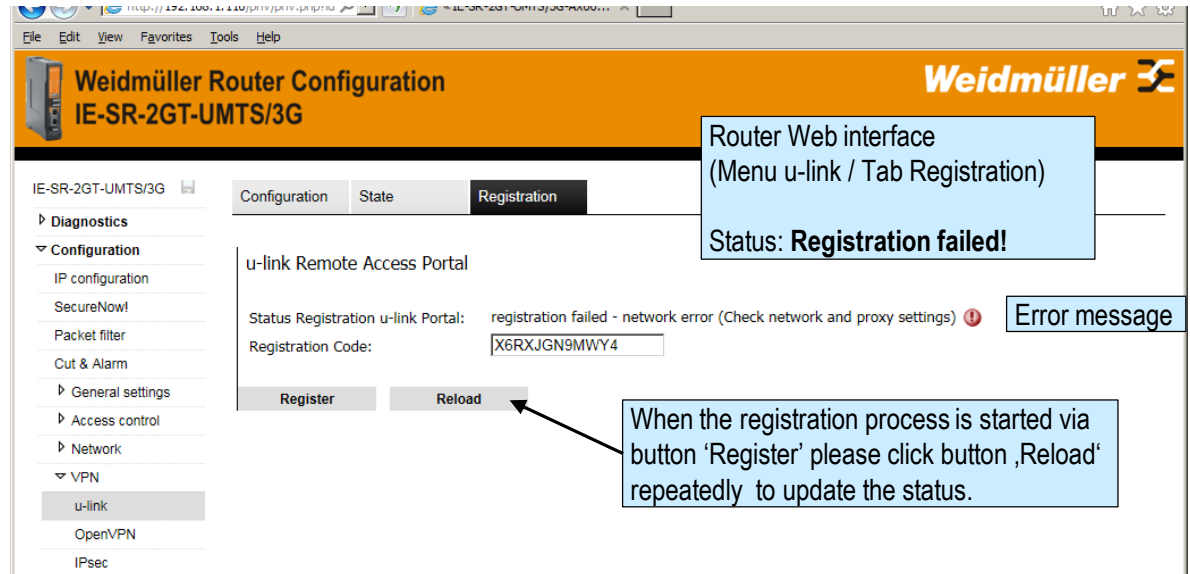
- Check via menu 'Diagnostics → Ping test' if an Internet IP (eg. 8.8.8.8) is accessible.
- Check via menu 'Diagnostics → Ping test' if an Internet device via DNS name (eg. www.google.com) is accessible.
- Please read Chapter 4.6 (Setup of a remote access scenario / Configuration Router).

2. Router Internet access is blocked by company-based Firewall rules

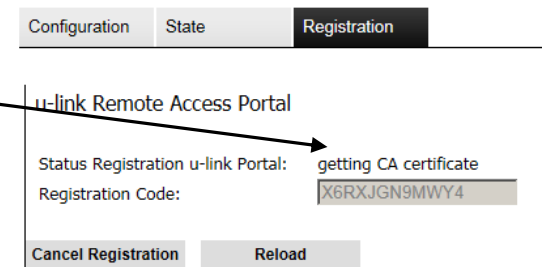
- Please read Appendix (Required Protocols and ports for u-link).
- Clarify with IT department to allow the outgoing u-link communication based on the required protocols / ports (see Appendix A4).

3. Router Internet access is passing a company-based Proxy server which requires an authentication to establish an Internet connection

- Configure in menu 'Network → HTTP proxy' the required settings (provided by IT department).
- Enable checkbox "Use system wide HTTP proxy" in menu u-link → Configuration.



Note:
 If during the registration process - before displaying the final status 'Registration failed' – only the status "getting CA certificate" is displayed in the meantime (and not the status 'enrolling certificate') then this is an Indication that a corporate Firewall or Proxy server is blocking the registration process.
 Please press button 'Reload' repeatedly to monitor the temporary status messages.



A2 - General Router support by Weidmüller

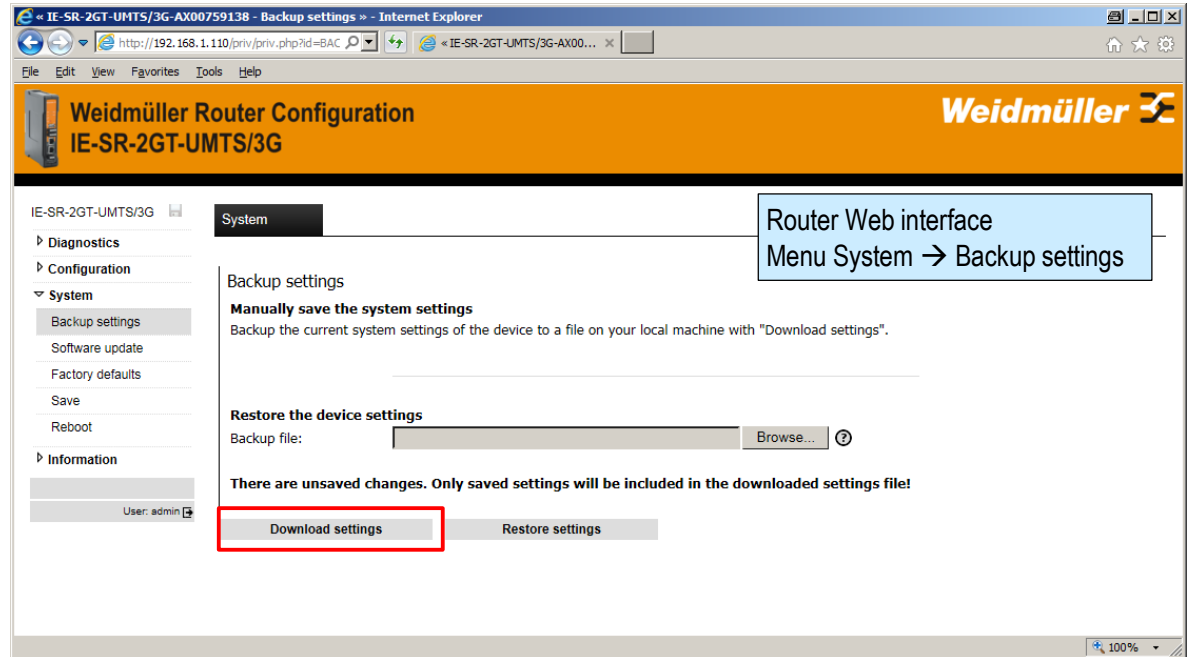
If any problems in terms of u-link connectivity or other Router features require support from Weidmüller please proceed as described below.

- Goto menu 'System → Backup settings'
- Click button 'Download settings' to export the configured Router settings (a file with extension .cf2) will be created.

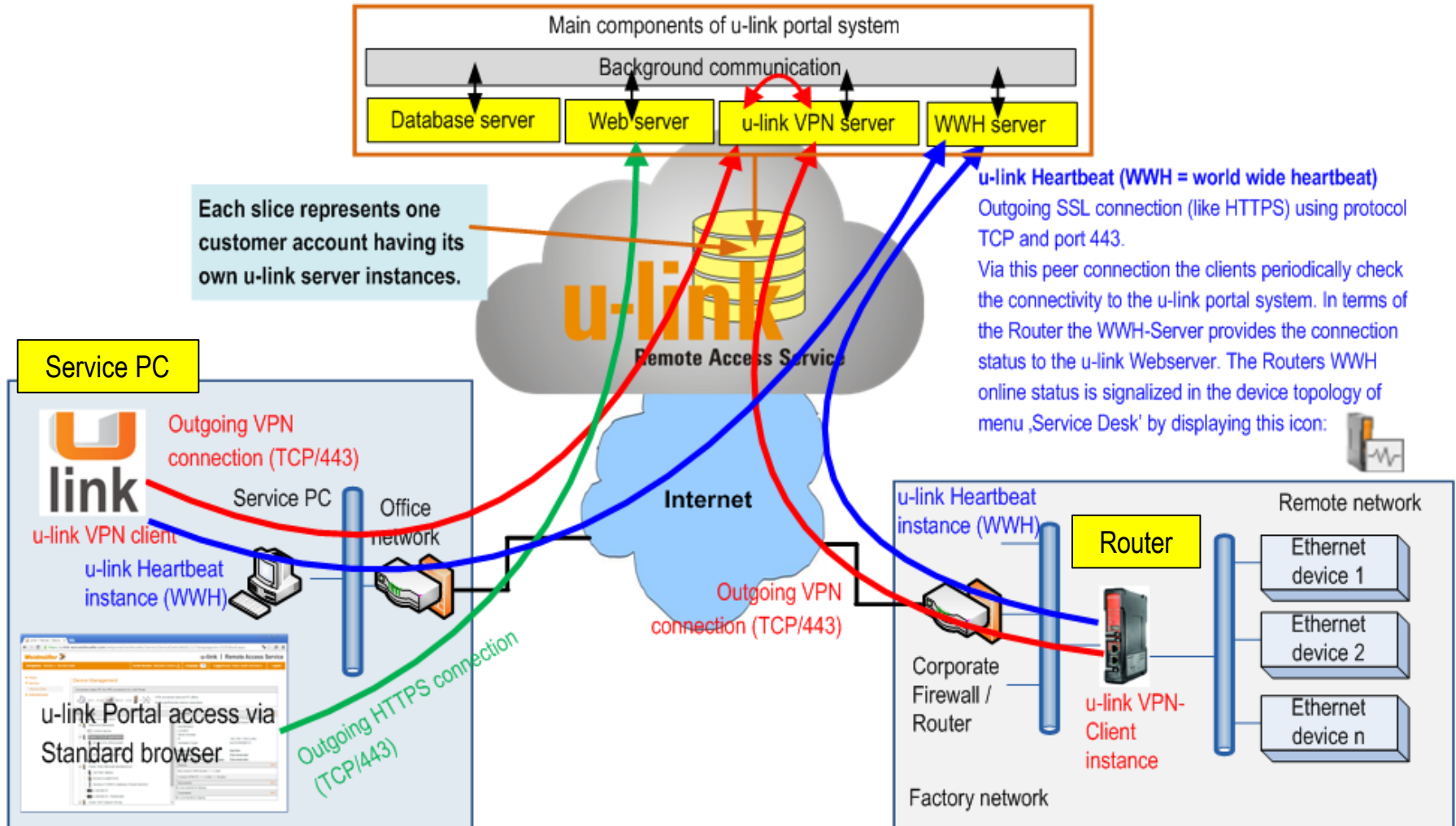
Note:

Only a saved configuration will be exported into a backup file. If you have changed and applied Router parameters but still not saved then you need to save the configuration before creating the backup file.

- Send the cf2-file to mail address u-link-support@weidmueller.com.
 - The u-link support department then will analyze the issue and contact you to solve the problem.



A3 - Functional diagram of involved u-link components



A4 - Overview of used u-link connection parameters

Minimum required communication parameters for u-link VPN Clients (PC and Router):						Updated October 09, 2020	
	Version	Protocol / Port	Used DNS name	Currently used Target IP	Comments	Connection type	
Registration							
Router		TCP / 443 / 80	u-link.weidmueller.com	13.69.30.109	Registration	Outgoing	
VPN Client (PC)		TCP / 443 / 80	www.u-link.weidmueller.com				
WWH (World Wide Heartbeat) for Registration, Still Alive messages and VPN Server request							
Router	≤	Version 3.2.2	TCP / 443 (SSL/TLS)	wwh.big-linx.de wwh2.big-linx.de	217.119.57.27 13.81.4.92	Main server Backup server	Outgoing
	≥	Version 3.2.3	TCP / 443 (SSL/TLS)	wwh1-we.aw-cp.de wwh1-ne.aw-cp.de	13.81.4.92 52.169.107.229	Main server Backup server	Outgoing
VPN Client (PC)	≤	Version 2.0.128	TCP / 443 (SSL/TLS)	wwh1.aw-cp.de	62.138.201.27	Main server	Outgoing
	≥	Version 2.0.129	TCP / 443 (SSL/TLS)	wwh1-we.aw-cp.de wwh1-ne.aw-cp.de	13.81.4.92 52.169.107.229	Main server Backup server	Outgoing
VPN Server							
Router	≤	Version 3.2.2	TCP / 443 (OpenVPN)	idaprof2.ads-tec.de	217.119.57.23	Main server	Outgoing
	≥	Version 3.2.3	TCP / 443 (OpenVPN)	vpn1-we.aw-cp.de vpn1-ne.aw-cp.de	52.166.202.111 52.169.106.31	Main server Backup server	Outgoing
VPN Client (PC)	≤	Version 2.0.128	TCP / 443 (OpenVPN)	vpn2.aw-cp.de	217.119.57.23	Main server	Outgoing
	≥	Version 2.0.129	TCP / 443 (OpenVPN)	vpn1-we.aw-cp.de vpn1-ne.aw-cp.de	52.166.202.111 52.169.106.31	Main server Backup server	Outgoing
Other port and protocols important for u-link communication							
DNS request for Router and VPN-Client (PC)		TCP / 53 UDP / 53	Mandatory for resolving the DNS names				Outgoing
NTP time request for Router		UDP / 123	Recommended to update the Router's time automatically (Correct Router time is important for validity of u-link certificate to be used for VPN connection to u-link VPN server).				Outgoing
Note:							
This are the recommended Servers used for u-link Remote Access Service. If these are prohibited, the Clients may change to other servers displayed in the extended list. If a Service PC (u-link VPN client) or Router is passing a corporate firewall to access the Internet, please clarify with the responsible IT administration that the listed connection types are allowed (if you have any connection problems). We recommend to use the listed DNS names for Firewall settings. If possible avoid using the currently used IP addresses.							

A4 - Overview of used u-link connection parameters including fallback and backward compatibility servers

All possible communication parameters for u-link VPN Clients (PC and Router):							Updated December 03, 2018
	Version	Protocol / Port	Used DNS name	Currently used Target IP	Comments	Connection type	
Registration							
Router		TCP / 443 / 80	u-link.weidmueller.com	13.69.30.109	Registration	Outgoing	
VPN Client (PC)		TCP / 443 / 80	www.u-link.weidmueller.com				
WWH (World Wide Heartbeat) for Registration, Still Alive messages and VPN Server tables							
Router	≤	Version 3.2.2	TCP / 443 (SSL/TLS)	wwh.big-linx.de wwh2.big-linx.de	217.119.57.27 13.81.4.92	Main server Backup server	Outgoing
	≥	Version 3.2.3	TCP / 443 (SSL/TLS)	wwh1-we.aw-cp.de wwh1-ne.aw-cp.de wwh.big-linx.de	13.81.4.92 52.169.107.229 217.119.57.27	Main server Backup server Backward compatibility	Outgoing
VPN Client (PC)	≤	Version 2.0.128	TCP / 443 (SSL/TLS)	wwh1.aw-cp.de	62.138.201.27	Main server	Outgoing
	≥	Version 2.0.129	TCP / 443 (SSL/TLS)	wwh1-we.aw-cp.de wwh1-ne.aw-cp.de	13.81.4.92 52.169.107.229	Main server Backup server	Outgoing
VPN Server							
Router		TCP / 443 & 5955; UDP 1194	vpn1-we.aw-cp.de vpn1-ne.aw-cp.de No DNS No DNS vpn2.aw-cp.de No DNS idaprof2.ads-tec.de No DNS No DNS	52.166.202.111 52.169.106.31 61.138.201.23 52.169.24.35 62.138.201.23 217.118.57.23 217.119.57.23 217.119.57.22 217.119.57.28	Main Server Main Server Backup Server Backup Server OBFS Backward compatibility Backward compatibility Backward compatibility Backward compatibility Backward compatibility OBFS	Outgoing	
VPN Client (PC)	≤	Version 2.0.128	TCP / 443 (OpenVPN)	vpn2.aw-cp.de	62.138.201.23	Main server	Outgoing
	≥	Version 2.0.129	TCP / 443 (OpenVPN)	vpn1-we.aw-cp.de vpn1-ne.aw-cp.de	52.166.202.111 52.169.106.31	Main server Backup server	Outgoing
VPN China (PC & Router)		TCP / 443 (OpenVPN)	No DNS	101.132.149.212	China Server	Outgoing	
VPN Server for future use			vpn3-we.aw-cp.de vpn4-we.aw-cp.de vpn3-ne.aw-cp.de vpn4-ne.aw-cp.de	51.136.30.13 51.144.182.20 40.115.121.76 40.114.121.69	Reserved for future use	Outgoing	
Not in use any more		TCP / 443 / 80	adst02.synserver.de	217.119.57.16	Server not in use	Outgoing	
		TCP / 443	No DNS	217.6.47.174	Former static VPN server	Outgoing	
Other port and protocols needed for u-link communication							
DNS request for Router and VPN-Client (PC)		TCP / 53 UDP / 53	Mandatory for resolving the DNS names			Outgoing	
NTP time request for Router		UDP / 123	Recommended to update the Router's time automatically (Correct Router time is important for validity of u-link certificate to be used for VPN connection to u-link VPN server).			Outgoing	
Note:							
This is the full Server-List for u-link. Most of these servers are only used, when the connection to the main servers is prohibited. Please don't use the Backward compatibility servers if not necessary! If a Service PC (u-link VPN client) or Router is passing a corporate firewall to access the Internet, please clarify with the responsible IT administration that the listed connection types are allowed (if you have any connection problems). We recommend to use the listed DNS names for Firewall settings. If possible avoid using the currently used IP addresses.							

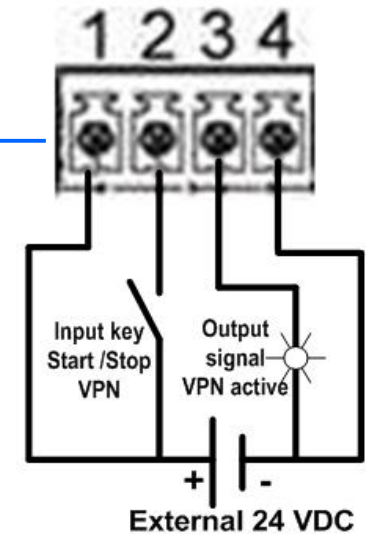
A5 - Activating / de-activating a u-link VPN tunnel via 24 VDC digital input

Start/Stop VPN tunnel:

- Establish VPN tunnel by connecting Pin 2 (VPN initiate) to 24 VDC and Pin 4 (GND) to ground of power supply.
- Deactivate VPN tunnel by removing 24 VDC from Pin 2.
- The status of the u-link VPN tunnel (on-/offline) is signaled by Pin 3 (Digital output “VPN active”). For output signaling you need to connect Pin 1 (VCC) to 24 VDC.



Pin number	SIGNAL NAME
1	24V DC (VCC)
2	Initiate VPN (24 V In)
3	VPN active (24 V Out)
4	GND



IE-SR-2GT-UMTS/3G

Configuration State Registration

u-link Remote Access Portal

Enable u-link instance:

VPN connection settings

Initiation by digital input (VPN initiate): Checkbox 'Initiation by digital input' must be enabled to establish a VPN tunnel by digital input 'VPN init' (default value).

Initiation from u-link web portal:

Inactivity timeout:

Additional settings

Use a system wide HTTP proxy:

Log level: Must be set to 'u-link' for signaling an active VPN tunnel by digital output 'VPN active' enabled (default value).

VPN LED/output controller: Must be set to 'Active' (default value).

Polarity of digital input (VPN initiate):

Apply settings Reset changes

A6 - Change LAN IP address/netmask of a remote Router via u-link VPN connection

Situation (Example):

- Current IP configuration of remote Router:
LAN port IP/Subnet: 192.168.1.110 / 255.255.255.0
WAN port IP/Subnet: 192.168.99.206 / 255.255.255.0

Requirement:

- The LAN port IP/Subnet shall be changed via u-link to:
IP address: 192.168.50.254
Subnet mask: 255.255.255.0

Solution:

- Connect to the remote Router via u-link.
 - The u-link VPN client (PC) now has got route settings how to access the IP networks 192.168.1.0/24 (Router LAN) and 192.168.99.0/24 (Router WAN). See upper screenshot.
 - The Routers Web interface can be accessed via LAN IP, WAN IP or via the Routers u-link VPN IP (see upper screenshot). Due to the fact that we want to change the LAN-IP we may not use the current LAN-IP for accessing the Web interface but we can use the Router VPN IP.
- Open the Routers Web interface by using the Routers VPN IP.
- Goto menu IP configuration.
- Change IP address data of LAN port.
- Click button 'Apply settings'.
 - Now the new LAN-IP address is active and the connected devices at Routers LAN port must be adapted to the new IP range.
- Save the configuration (Menu System → Save).

The screenshot shows the 'u-link | Remote Access' interface. It displays the connection status of a PC connected to a remote network via the u-link portal. The 'Accessible remote network' section lists two networks: 192.168.99.0/255.255.255.0 and 192.168.1.0/255.255.255.0. A callout box labeled 'Accessible networks at Routers LAN/WAN ports' points to these two networks. Another callout box labeled 'Router VPN IP' points to the 'Router VPN IP' field, which is circled in red and contains the value 10.46.240.6. The 'Routing to Remote network' status is shown as 'active'. Below this, the 'Device Topology' section shows a tree view of the network structure, including 'WDM Engineering Systems', 'Access Router Machine 1', 'Access Router Machine 2', 'Access Router Machine 3', 'SE-Konverter', and 'Switch'.

Note about provided accessible networks:
If the Router is connected to Internet via DHCP-enabled WAN port then the WAN network will not provided as accessible network (only the LAN side).
If the Router is connected to Internet via WAN port with static IP address then both network sides (LAN and WAN) are provided as accessible networks.



The screenshot shows the Router's Web interface for configuration. The browser address bar shows '10.46.240.6/print.php?id=IPCONF'. A callout box labeled 'Web access to Router via the Router's u-link VPN IP' points to the address bar. The 'Configuration' menu is open, and the 'IP configuration' section is selected. The 'Operational mode' is set to 'IP router'. Under the 'WAN' section, the 'IP assignment' is set to 'static', the 'IP address' is '192.168.99.206', and the 'Subnet mask' is '255.255.255.0'. Under the 'LAN' section, the 'IP assignment' is set to 'static', the 'IP address' is '192.168.50.254', and the 'Subnet mask' is '255.255.255.0'. A callout box labeled 'Screenshot shows the already set new IP address at LAN port.' points to the 'IP address' field in the LAN section.

A6 - Change LAN IP address/netmask of a remote Router via u-link VPN connection

Note:

The connected PC still has the routing entries to previous Router LAN and WAN IP networks 192.168.1.0/24 and 192.168.99.0/24.

To update the PCs routing table do following:

- Disconnect the PC from the remote Router.
- Disconnect the Router VPN connection to u-link.
 - Wait until the Router icon changes to this symbol: 
- Connect the Router again to u-link.
 - Wait until the Router icon changes to this symbol: 
- Finally re-connect the PC to the remote Router.
 - As result the PC's routing table should be updated and the new accessible networks **192.168.50.0/24** and 192.168.99.0/24 should be displayed in the connection status of the Service desk.

New accessible networks at Routers LAN/WAN ports

Connected to:	Accessible remote network:	Router VPN IP:	Routing to Remote network:
Access Router Machine 2	192.168.99.0/255.255.0	10.46.240.6	active
	192.168.50.0/255.255.0		

Device Topology	
WDM Engineering Systems	
Access Router Machine 1	
Access Router Machine 2	
Access Router Machine 3	
SE-Konverter	
Switch	

Properties	
Name	Access Router Machine 2
Device Type	Router/Firewall
Identification	
Location	
Serial Number	
IP	192.168.1.110 (LAN)
Activation Code	X6RXJGN9MWY4
Status-WWH	Active
Status-VPN Router ↔ u-link	Connected
Status-VPN PC ↔ u-link ↔ Router	Connected

A7 – Technical customer support

For any technical issues or support requests in terms of the u-link Remote Access Service
please send a mail to address

u-link-support@weidmueller.com.