

## **Industrial Ethernet Training 13**

### **Using u-link remote access service**

#### **Abstract:**

With Weidmueller's u-link VPN software, you can remotely connect to a device's web interface or a local visualization outside the network. The connection is secured via a VPN tunnel from the router, our own Weidmueller meeting point servers and from our computer connecting to the device. This application note demonstrates the usage of Weidmueller's u-link platform.

### Hardware reference

No.	Component name	Article No.	Hardware / Firmware version
1	IE-Training Kit-01	2881730000	1.1.2 (Build 125086)
2			
3			

### IE-Training Kit Content

No.	Component name	Article No.	Hardware / Firmware version
1	IE-SR-4TX	2751270000	1.4.7
2	IE-SW-AL08M-8TX	2682280000	1.08
3	IE-SW-AL05M-5TX	2682250000	1.14
4	IE-CS-MBGW-2TX-1COM	2682600000	3.11

### Software reference

No.	Software name	Article No.	Software version
1			
2			
3			

### File reference

No.	Name	Description	Version
1			
2			

### Contact

Weidmüller Interface GmbH & Co. KG  
Klingenbergstraße 26  
32758 Detmold, Germany  
[www.weidmueller.com](http://www.weidmueller.com)

For any further support please contact your  
local sales representative:  
<https://www.weidmueller.com/countries>

Content

1      Warning and Disclaimer..... 4

2      Why u-link?..... 5

3      Creating u-link account ..... 6

4      Installing u-link VPN client ..... 8

5      Configuring new device .....11

5.1   Connecting the VPN tunnel.....17

6      Results .....20

# 1 Warning and Disclaimer

## Warning

Controls may fail in unsafe operating conditions, causing uncontrolled operation of the controlled devices. Such hazardous events can result in death and / or serious injury and / or property damage. Therefore, there must be safety equipment provided / electrical safety design or other redundant safety features that are independent from the automation system.

## Disclaimer

This Application Note / Quick Start Guide / Example Program does not relieve you of the obligation to handle it safely during use, installation, operation and maintenance. Each user is responsible for the correct operation of his control system. By using this Application Note / Quick Start Guide / Example Program prepared by Weidmüller, you accept that Weidmüller cannot be held liable for any damage to property and / or personal injury that may occur because of the use.

## Note

The given descriptions and examples do not represent any customer-specific solutions, they are simply intended to help for typical tasks. The user is responsible for the proper operation of the described products. Application notes / Quick Start Guides / Example Programs are not binding and do not claim to be complete in terms of configuration as well as any contingencies. By using this Application Note / Quick Start Guide / Example Program, you acknowledge that we cannot be held liable for any damages beyond the described liability regime. We reserve the right to make changes to this application note / quick start guide / example at any time without notice. In case of discrepancies between the proposals Application Notes / Quick Start Guides / Program Examples and other Weidmüller publications, like manuals, such contents have always more priority to the examples. We assume no liability for the information contained in this document. Our liability, for whatever legal reason, for damages caused using the examples, instructions, programs, project planning and performance data, etc. described in this Application Note / Quick Start Guide / Example is excluded.

## Security notes

In order to protect equipment, systems, machines and networks against cyber threats, it is necessary to implement (and maintain) a complete state-of-the-art industrial security concept. The customer is responsible for preventing unauthorized access to his equipment, systems, machines and networks. Systems, machines and components should only be connected to the corporate network or the Internet if necessary and appropriate safeguards (such as firewalls and network segmentation) have been taken.

## 2 Why u-link?

Our Remote Access Service provided by our VPN-Client **u-link** allows an easy and secure remote access to our Ethernet devices, like a router or a u-control, with a computer via an Internet based VPN connection from outside the router's network.

This VPN-based access to the devices is done by linking an account from the u-link portal to the device itself (like the router), that has a VPN configuration pre-installed. The device needs to be activated with an individual registration code. The computer using our **u-link VPN client** is also activated with a registration code, to get into the VPN tunnel for a secure connection.

Our u-link VPN meeting point server is used as a tunnel between the computer and a remote device like the router, meaning we have direct access to the device and not just a clone of the device's user interface. Hence, there is also the risk of transferring malware or viruses from the computer outside of the network into the local network that is being accessed. To avoid such risks, we can also use the EasyAccess feature which only "clones" the web interface, but this will be dealt with in another Application Note.

### 3 Creating u-link account

First, create a u-link account. This is mandatory for accessing our devices remotely as we have to create unique registrations, connections and links for accessing our devices securely.

1. Go to the u-link web site <https://u-link.weidmueller.com> to create a new user account. Now, click on the “Register” field.

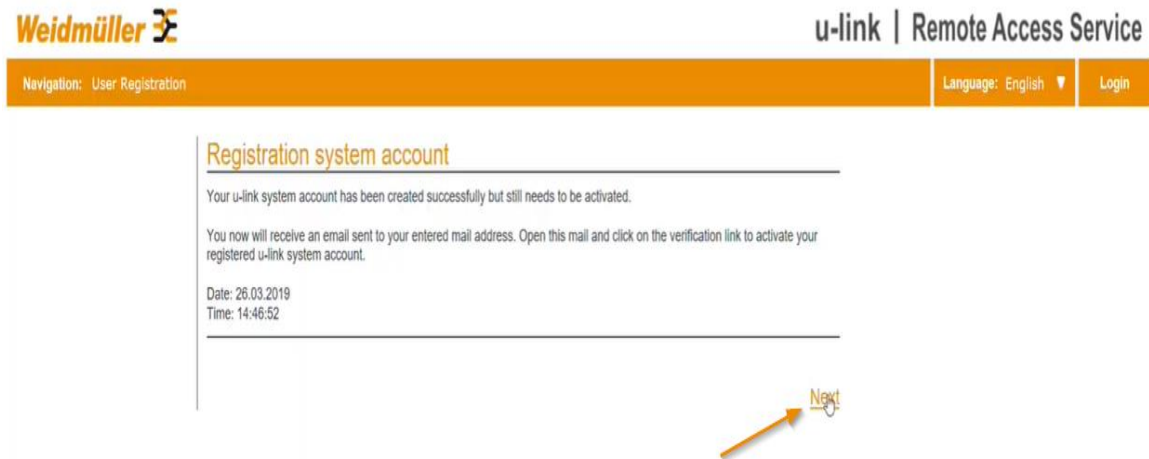
Figure 1: u-link login page

2. Fill in the user credentials in the required fields and click on “Next”.

Figure 2: Creating user account

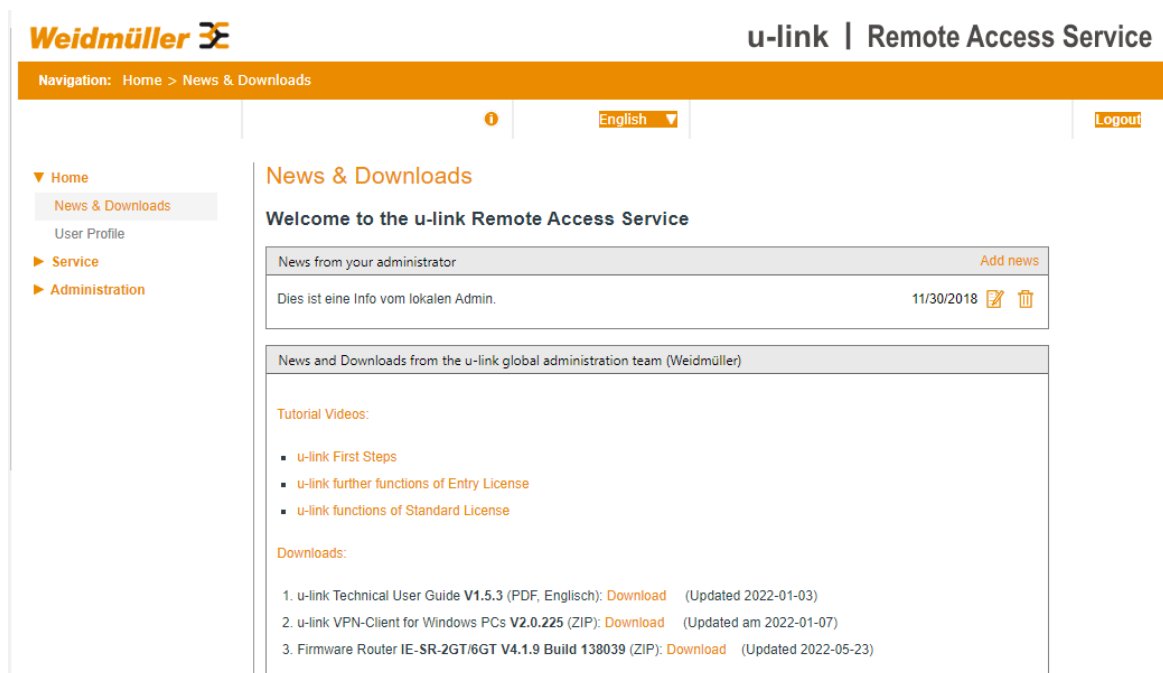
## Using u-link remote access service

3. After successfully entering the necessary credentials, we have to activate our account with an activation link sent via email. Please follow the instructions given in the email for activating the account.



**Figure 3: Verification email**

4. Now, we can log in to the created user account. Afterwards, we find ourselves on the homepage of u-link “News & Downloads”.



**Figure 4: Homepage u-link**

## 4 Installing u-link VPN client

After creating our user account, we must install the u-link VPN client to establish a secure connection to our services and devices through the VPN tunnel.

1. Navigate to “Home” then “News & Downloads” and download the **u-link VPN-Client**.

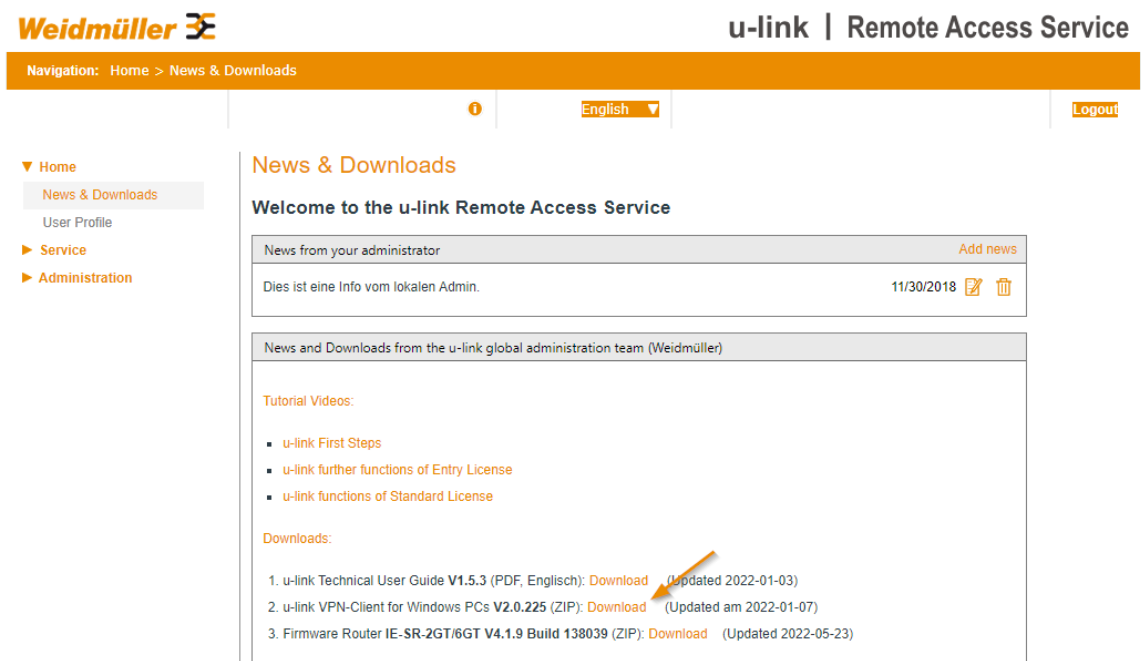


Figure 5: Download u-link VPN Client

2. Next, open the u-link setup folder and **run the setup as an administrator**. Then, click on install.

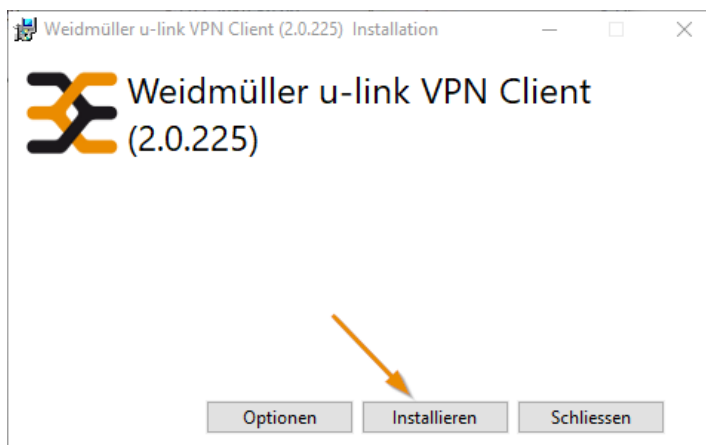
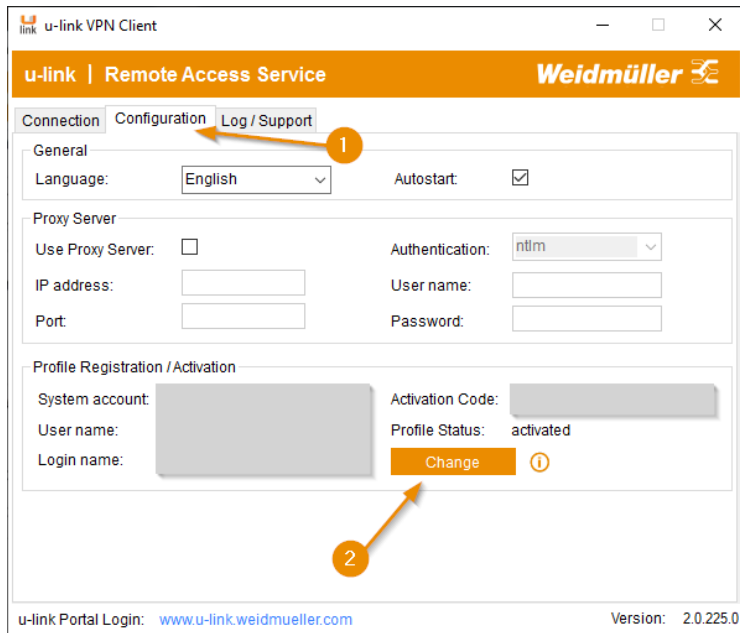


Figure 6: Installation VPN-Client



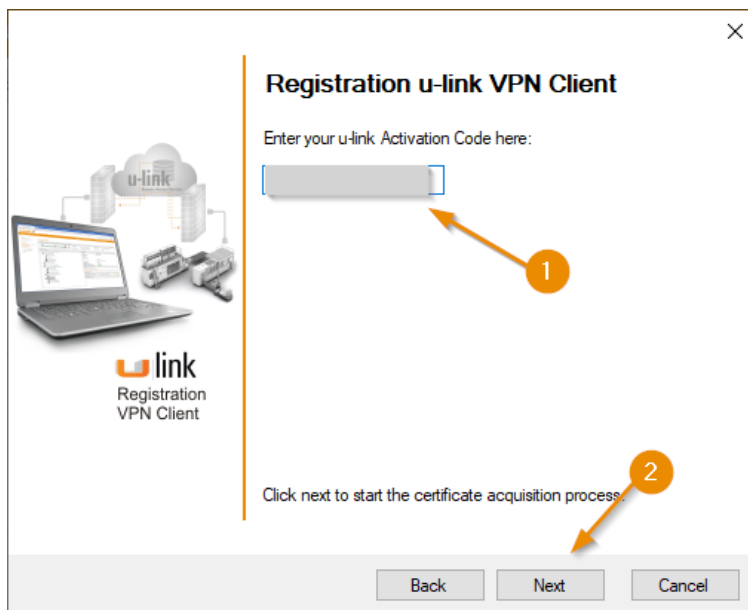
## Using u-link remote access service

3. We are now in the *connection* menu of our VPN software. As of now, the VPN client is not connected to the user account. To do this, we must select the “*Configuration*” menu and click on “*Activate*” (in our case it says change, as we already have a connected account).



**Figure 7: Activating VPN-Client**

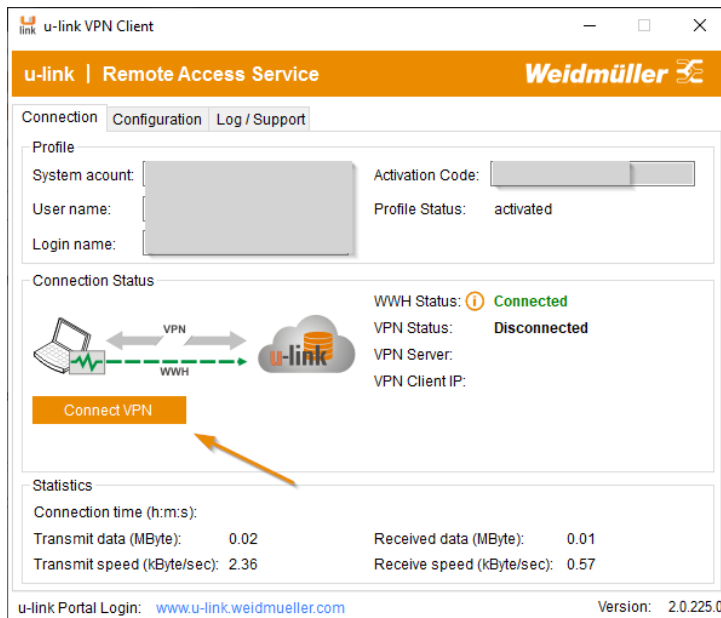
4. To activate the account, we must enter our activation code that can be found in the email with the activation link for the u-link account. Paste your activation code into the activation code field and press “*Next*”.



**Figure 8: Entering activation code**

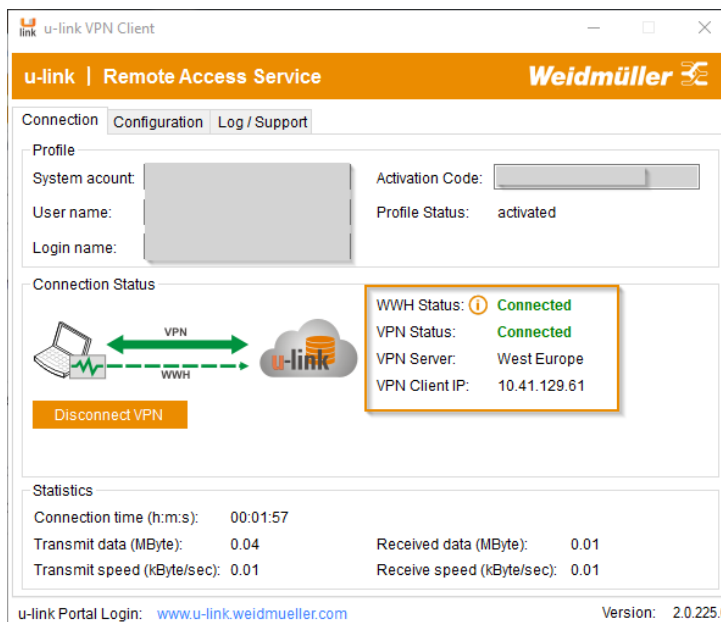
## Using u-link remote access service

- After a few moments, our account is activated and we can see our user credentials being displayed in the menu. Lastly, connect the VPN in order to access the devices remotely. We can do this by going back to the menu “*Connection*” and pressing on the button “*Connect VPN*” (This step is not mandatory, as it will connect to VPN automatically in the later steps).



**Figure 9: Connecting VPN**

- After connecting, we can see our VPN status and more information like our server location or our VPN Client IP. We are now successfully connected to Weidmüller’s VPN servers.



**Figure 10: VPN connection**

## 5 Configuring new device

The next step is adding a new device to the u-link account and configuring it to make it ready for usage with u-link VPN outside of the network.

1. First, visit the u-link web site and navigate the menu tree to “Administration” and then click on “Device Management”. We can now see the device tree with possible devices we have linked to our u-link account (our test environment has already devices linked).

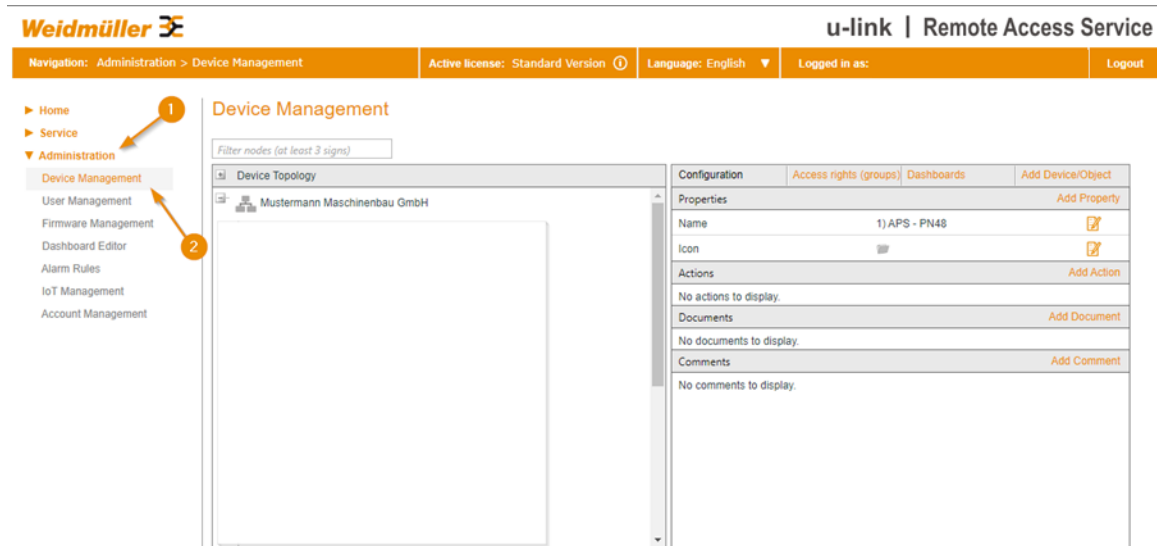


Figure 11: Device Management

2. Click on “Add Device/Object” and select the device you wish to add to your u-link account, in this case a router. You can now add the device via Drag & Drop to your device topology.

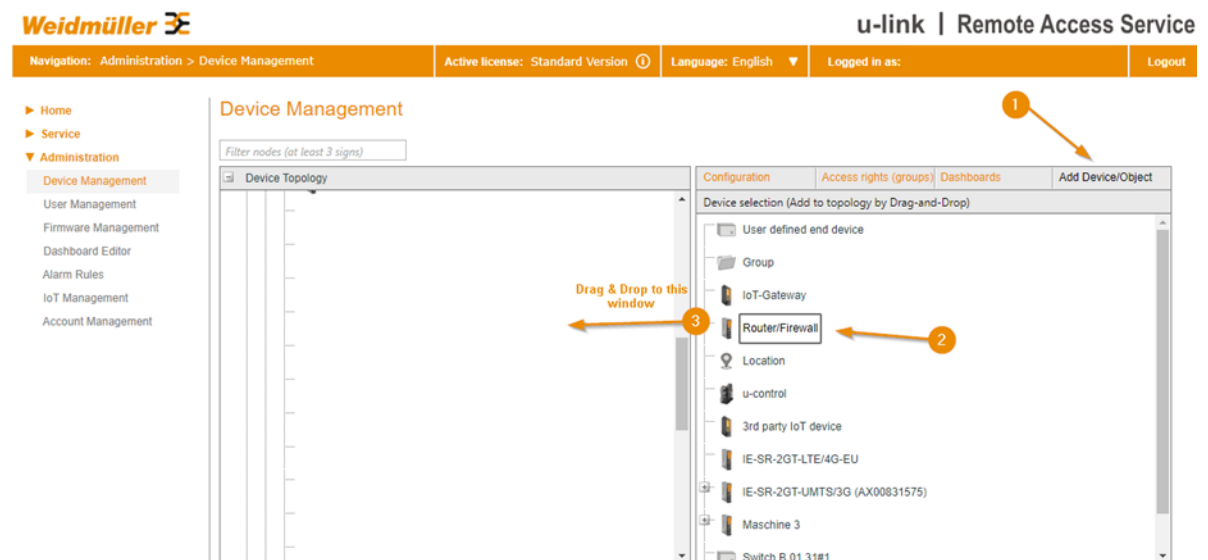


Figure 12: Adding new device

- After adding your router via Drag & Drop to the device topology, you get the following message. Please **note or copy** the activation code as we will need it for our router to activate its u-link status (note: if you forgot to copy the code, you can find your device in the device list again and look up the activation code in its properties (8)).

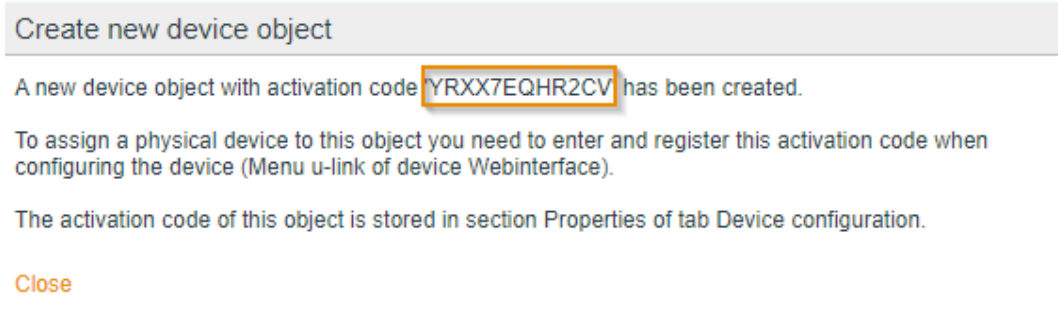


Figure 13: Activation code for device

- Next, connect to mentioned router with the IP address and default credentials, in this case type into the URL of your browser "192.168.1.10" and your credentials, like username "admin" with password "Detmold". First of all, check the date & time of the router as the VPN certificate only works properly when the date & time settings are configured correctly. In order to check this, we must navigate to "Configuration" then click on "General Settings" and lastly click on "Date & Time". Optimally, we want to have a Network Time Protocol (NTP) server to synchronize our date & time, but we can also do it manually (not recommended as the date & time get reset when the device has no power for over 30 minutes). Do not forget to "Apply" and "Save" your configuration in the menu "System".

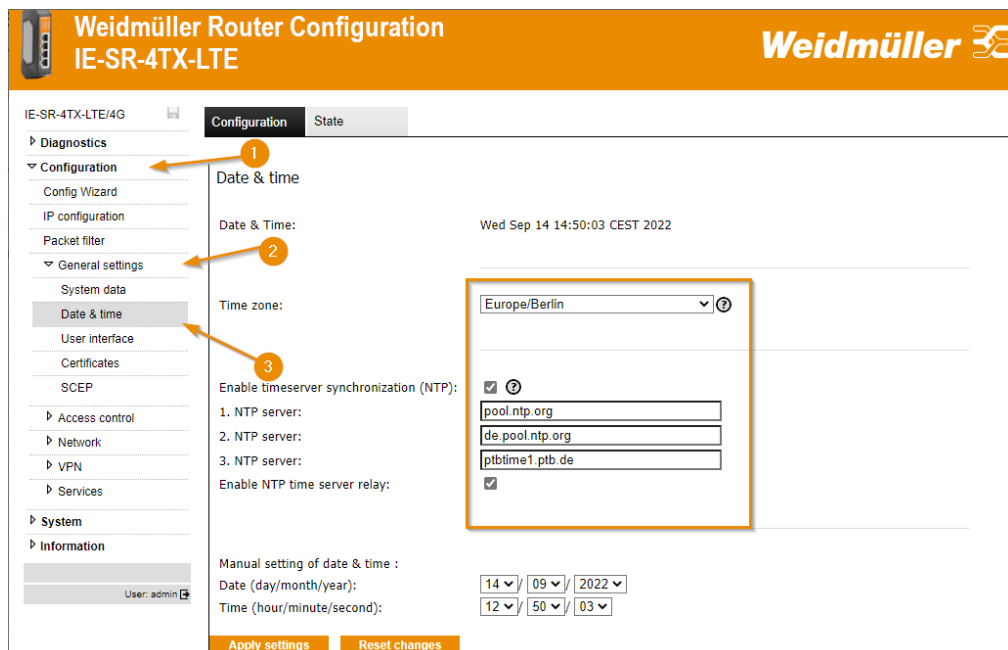
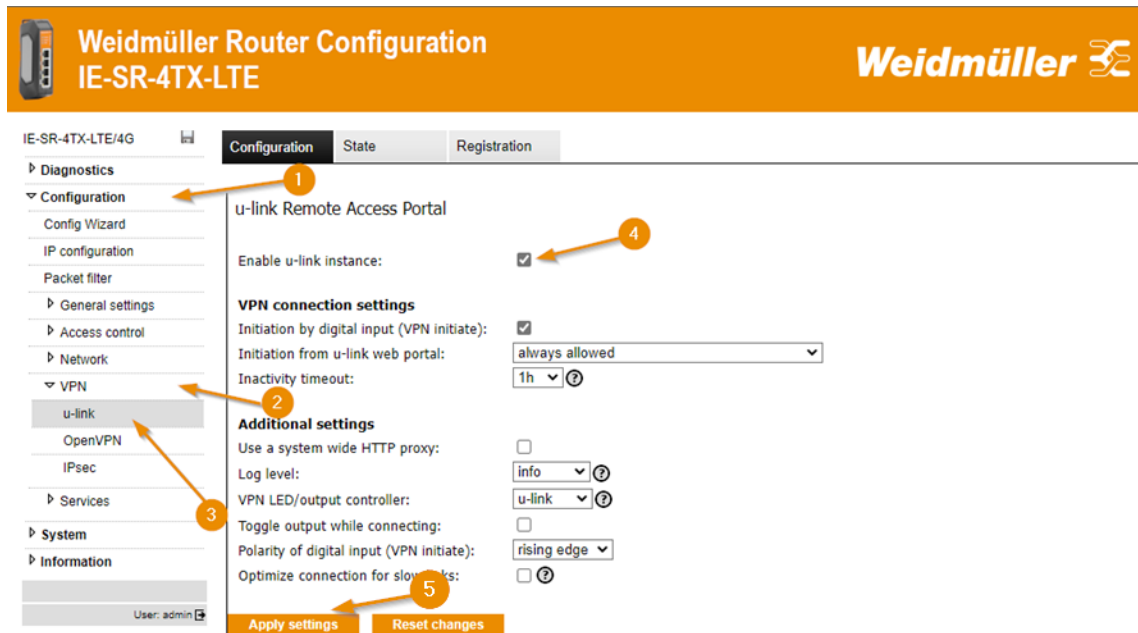


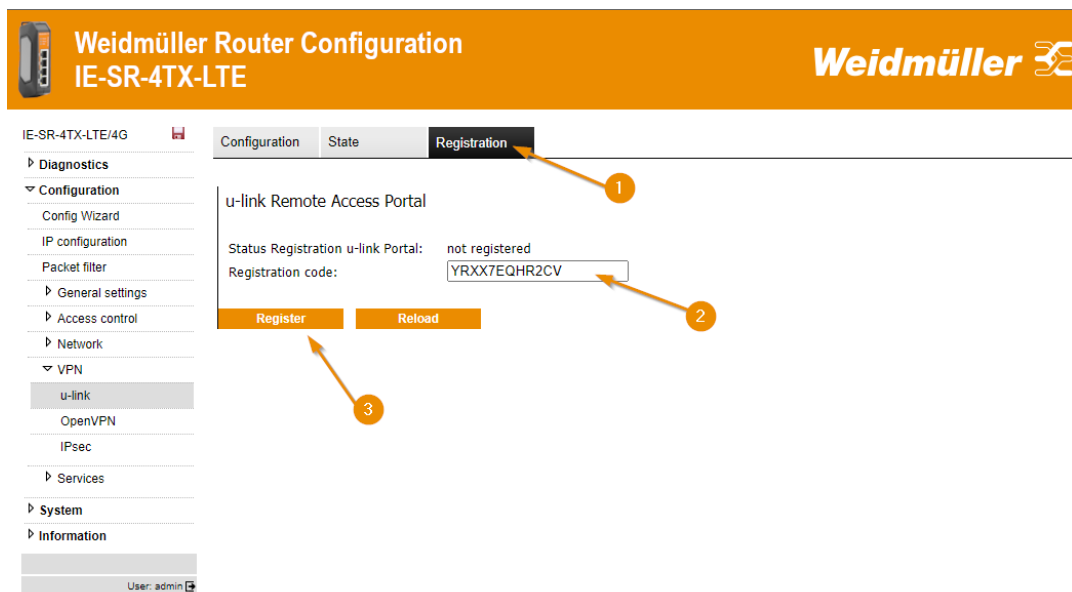
Figure 14: Date & Time settings router

- First, enable u-link VPN on the router's web interface. To do so, we want to navigate to "Configuration" then to "VPN" and select "u-link". Here, we enable the checkbox "Enable u-link instance" and "Apply Settings" hence activating the u-link option in our router.



**Figure 15: Activating u-link instance**

- u-link is now enabled on the router. In the next step, we need the activation code to activate the router for the u-link remote access portal. Click on the tab "Registration" in the same menu tree as before and paste/type in your activation code from earlier into the field and press register. A few moments later, the router should have a "registered" status.



**Figure 16: Entering activation key**

7. We may now proceed to connect the router to a VPN connection. Therefore, we must select the menu tab “*State*” in the same menu tree. Click on the button “*Connect*” to connect the router to the VPN. When done right, we have the following screen telling us we have an active VPN connection (This is also not mandatory to do beforehand, as it will connect to VPN automatically in the following step).

The screenshot displays the Weidmüller Router Configuration web interface for an IE-SR-4TX-LTE/4G router. The interface has a top orange header with the router model and the Weidmüller logo. Below the header, there are three tabs: Configuration, State (which is selected), and Registration. On the left, a navigation menu lists various settings categories, with 'VPN' expanded to show 'u-link', 'OpenVPN', and 'IPsec'. The main content area shows the 'u-link Remote Access Portal' status as 'registered'. Below this, the 'WWH communication' status is 'Connected', with the last seen time being 'Wednesday, 14 Sep 2022, 13:56'. Further down, the 'VPN connection u-link portal' status is 'Connected to VPN server', showing a VPN IP address of '10.41.129.73', a connection time of 'Wednesday, 14 Sep 2022, 13:54', and data transferred of '8 kByte'. A 'Disconnect' button is visible next to the VPN connection status. At the bottom, there is a 'Reload' button and a user login field showing 'User: admin'.

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

WWH communication	
Status:	Connected
Last seen:	Wednesday, 14 Sep 2022, 13:56

VPN connection u-link portal		
Status:	Connected to VPN server	<a href="#">Disconnect</a>
VPN IP address	10.41.129.73	
Connected since:	Wednesday, 14 Sep 2022, 13:54	
Data transferred:	8 kByte	


[Reload](#)

User: admin

**Figure 17: Establishing VPN connection with our router**

## Using u-link remote access service

- As mentioned before, the VPN connects automatically when you want to access the device remotely. To access the device remotely, go to “Service” and then “Service Desk”. Find the device in the topology and click on it to open its properties.

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

Navigation: Service > Service Desk    Active license: Standard Version ⓘ    Language: English ▼    Logged in as:    Logout

▶ Home    1  
▼ Service  
  Service Desk    2  
  IoT Dashboard  
  Alarming  
  EasyAccess  
▶ Administration

### Service Desk


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

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

Filter nodes (at least 3 signs)


Device Topology

Ioannis Router Testkit    3

Properties	
Name	Ioannis Router Testkit
Icon	
Device Type	IE-SR-4TX-LTE/4G
Identification	
Location	Paderborn Training Kit Ioannis
Serial Number	
IP	192.168.1.10
Router Location (Country)	Auto
Activation Code	YRXX7EQHR2CV
Status-WWW	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 Dashboard	
Easy Access: Device Webinterface	

**Figure 18: Selecting device in Service Desk**


9. To automatically connect to the VPN, we must have the u-link VPN client running in the background. Establishing the VPN connection between the computer and the router is done by clicking on “Connect VPN PC ↔ u-link ↔ Router” (in case it does not: please follow the steps in 5).

Actions
Connect VPN Router ↔ u-link
Connect VPN PC ↔ u-link ↔ Router 
Open Dashboard
Easy Access: Device Webinterface

**Figure 19: Starting u-link VPN connection**

What now happened is, that our u-link servers start the VPN connections on both ends, which results in the devices having the same IP addresses (e.g.: router and computer) thus theoretically being able to communicate with each other. But this is not enough, we need to have a connection internally at the meeting point server. This means that starting the VPN on the router and the computer is not enough to access the device outside the network as we need the tunnel and a routing to the corresponding IP address from the server.

Afterwards, we can see that the connection is successfully established in the status information above and moreover u-link offers the option to disconnect the current VPN connections.

Status-WWH	Active
Status-VPN Router ↔ u-link	Connected (West Europe)
Status-VPN PC ↔ u-link ↔ Router	Connected
Actions	
Disconnect VPN Router ↔ u-link	
Disconnect VPN PC ↔ u-link ↔ Router 	
Open Dashboard	
Easy Access: Device Webinterface	

**Figure 20: VPN connection successfully established**



## 5.1 Connecting the VPN tunnel

As of now, all preparations and necessary actions for the remote access of the network are done. The u-link page now states all the information to ensure that the VPN connection is working properly.

For example, we can find green circles around the devices and connections in the top left corner, symbolizing that every connection is established successfully. Moreover, one can also see the device's VPN IP with which we can connect to the router, and also a status of the routing to the remote network indicating that we have a routing through the VPN servers to the device.

The screenshot shows the Weidmüller u-link Remote Access Service interface. The top navigation bar includes the Weidmüller logo, navigation links (Service > Service Desk), active license (Standard Version), language (English), and login status (Logged in as: [user]). The left sidebar shows a menu with Home, Service (Service Desk, IoT Dashboard, Alarming, EasyAccess), and Administration.

The main content area is titled "Service Desk" and displays the connection status of a PC: "Connected to Device/Remote network via u-link". A diagram shows a PC connected to a router via a u-link cloud. The status is "Connected to: Ioannis Router Testkit" with an accessible remote network of "192.168.1.0/255.255.255.0". The device's VPN IP is "10.41.129.73" and the routing status is "active".

Below the status bar, there is a "Filter nodes (at least 3 signs)" input field. The "Device Topology" section shows a diagram of the "Ioannis Router Testkit". The "Properties" table on the right lists the following details:

Properties	
Name	Ioannis Router Testkit
Icon	[Router Icon]
Device Type	IE-SR-4TX-LTE/4G
Identification	
Location	Paderborn Training Kit Ioannis
Serial Number	
IP	192.168.1.10
Router Location (Country)	Auto
Activation Code	YRXX7EQHR2CV
Status-WWH	Active
Status-VPN Router ↔ u-link	Connected (West Europe)
Status-VPN PC ↔ u-link ↔ Router	Connected
Actions	
Disconnect VPN Router ↔ u-link	
Disconnect VPN PC ↔ u-link ↔ Router	
Open Dashboard	
Easy Access: Device Webinterface	

**Figure 21: u-link status after connecting VPN**

In case you are experiencing troubles establishing the connection, make sure that:

- Your own IP address is not in the range of the remote network you want to connect to
- You are not connected to the device directly in any way, e.g., via cable.
- You do not have any other VPN program running, which could lead to IP address conflicts
- You have a proper internet connection
- Your u-link VPN client is connected to the VPN. In case it did not automatically connect to the VPN, do it manually as described in step 5.

Lastly, we can now check whether the established VPN connection and routing is working as intended. For that, make sure that you are outside of the remote network's range, in different network. Accessing the devices in the remote network can be done in different ways.

1. The first way of accessing the remote device is via the depicted VPN IP as seen in Figure 21: u-link status after connecting VPN. We can simply click on it and the browser opens up a new tab where we can log in to the device and access it. The system state tab also shows the u-link IP at the interface state section.

**Weidmüller Router Configuration IE-SR-4TX-LTE**

IE-SR-4TX-LTE/4G

**Diagnostics**

- System State
- Eventlog
- WAN
- LAN
- WWAN
- Ping test
- Remote capture

**Configuration**

- System
- Information

User: admin

**System data**

System name: IE-SR-4TX-LTE/4G-AX20131010

Device type: IE-SR-4TX-LTE/4G

Serial-No.: AX20131010

Firmware version: 1.4.0 (Build 143757)

MAC-Address WAN: 00:18:92:07:D6:3F

MAC-Address LAN: 2A:18:92:07:D6:3F

Device mode: IP router

**System state**

Date & Time: Tuesday, 22 Nov 2022, 14:19 (Europe/Berlin)

Uptime: 15:19:07 up 5:56, load average: 1.07, 1.24, 1.27

u-link certificate: YRXX7EQHR2CV

OpenVPN sessions: Masters: active 0, listening 0, Clients: 0

IPsec tunnels: 0

**System usage**

Flash: 0%

Memory: 15%

**Network statistic**

Interface: LAN

**Interface state**

Interface	State	IP/Network mask	IP Assignment	DHCP Server
WAN	enabled	192.168.9.81 / 255.255.255.0	DHCP	disabled
LAN	enabled	192.168.1.10 / 255.255.255.0	static	enabled
u-link	connected	10.41.129.73 / 255.255.248.0	OpenVPN	-

**Figure 22: Connecting to remote device via VPN IP**

2. Besides, we can also access the devices in the remote network via their LAN IPs, for example the 8-port switch with the IP “192.168.1.20”. Even though this IP is not in the VPN IP network range, we can access it. This works because the VPN meeting point server also transmits every other IPs the router’s network interfaces have. Hence, we could theoretically also reach the router via its LAN IP “192.168.1.10”, which concludes that we can access every device in the remote network since it is in the IP range. The picture below demonstrates the working connection to the 8-port switch from the router, to which we are connected to with the VPN IP.

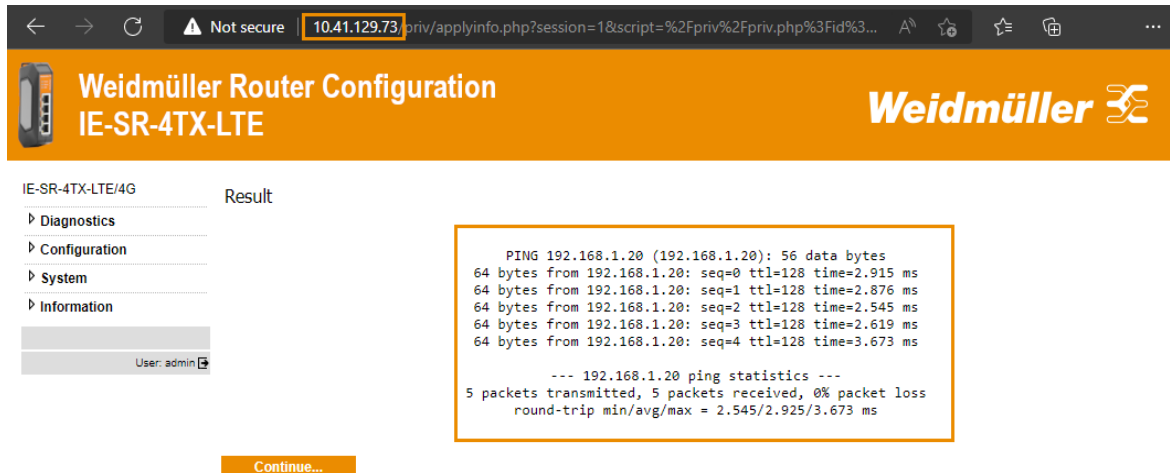


Figure 23: Pinging other devices inside remote network

## 6 Results

After completing the steps, we successfully learned how to use Weidmüller's u-link service. Furthermore, we know how to configure our VPN settings and gained the knowledge to connect to a device and its network remotely while being outside of this network.