



DELTA LOGIC



DELTA LOGIC Connectivity Service User Manual

This manual is aimed at users and fitters who use the VPN portal DELTA LOGIC Connectivity Service. The user should be shown and explained how to operate the DELTA LOGIC Connectivity Service. The installer should be provided with all the data required for installation.

© 2015 - 2024

DELTA LOGIC Automatisierungstechnik GmbH

Stuttgarter Straße 3

73525 Schwäbisch Gmünd

Germany

Phone sales: +49 7171 916-120

Phone Support: +49 7171 916-112

Fax sales: +49 7171 916-220

Fax support: +49 7171 916-212

E-Mail sales: sales@deltalogic.de

E-Mail support: support@deltalogic.de

Website: www.deltalogic.de

All rights reserved. No part of this work is allowed to be copied, reproduced, conferred, processed, and stored into electronic media or translated into any other language without a written permission of the author.

Note:

We have checked the content of this manual for conformity with the hardware and software described. Nevertheless, because deviations cannot be ruled out, we cannot accept any liability for complete conformity. The data in this manual have been checked regularly and any necessary corrections will be included in subsequent editions. We always welcome suggestions for improvement.

Last Update: 2024-01-08. All technical changes reserved.

S7-200®, S7-1200®, S7-1500®, S7-300®, S7-400®, HMI®, WinCC®, WinCC flexible®, ProTool®, STEP®, TIA®, TIA Portal®, SINUMERIK®, SIMOTION® und SIMATIC® are registered trademarks of Siemens AG, ACCON® and DELTALOGIC® are registered trademarks of DELTA LOGIC Automatisierungstechnik GmbH.

Table of Contents

1	General	5
2	VPN-Service Background	6
2.1	Networking via DELTA LOGIC Connectivity Service	6
2.2	Secure Communication	6
2.3	Simple Setup and Management	6
2.4	China VPN	7
3	Login	8
3.1	Registration for the DELTA LOGIC Connectivity Service	8
3.2	Registration on DELTA LOGIC Connectivity Service	8
3.3	Managing the own Password	8
3.4	Activate the China VPN	8
4	Configuration VPN service	9
4.1	Devices	9
4.1.1	Creating a device in the DELTA LOGIC Connectivity Service	9
4.1.2	Managing Devices	11
4.1.3	Downloading the device list	12
4.1.4	Addressing via netmapping	12
4.1.5	Direct Addressing	13
4.1.6	Activating time-restricted access for a device	14
4.1.7	Configuring the two-factor authentication (TOTP)	15
4.1.8	Replacement of Certificates	17
4.2	Groups	18
4.2.1	Creating a group	18
4.2.2	Manage the groups	18
4.2.3	Rules of Communication	19
4.3	Monitoring	20
4.3.1	Adding a Check	21
4.3.2	Managing the Checks	22
4.3.3	Adding a Host	22
4.3.4	Managing the Hosts	23
4.3.5	Configuring the check options	23
4.4	Licenses	25
4.4.1	Ordering a Licence	25
4.4.2	Managing the Licenses	25
4.5	Web Proxies	26
4.5.1	Setting Up a Web Proxy	27
4.5.2	Managing the Web Proxies	28
4.6	My VPN	29
4.6.1	Changing the Default Code	30
4.6.2	Downloading the VPN-Log	30
4.6.3	Restarting the VPN instance	30
4.6.4	Ordering licences	30
4.6.5	Managing the two-factor authentication	30
5	Configuration of the VPN participants	32
5.1	Configuration of an icom OS router	32
5.1.1	Configuration using the Quick Start Wizard	32
5.1.2	Manual configuration	32
5.2	Configuration of an INSYS OS router	33
5.2.1	Configuration using the Quick Start Wizard	33
5.2.2	Manual configuration	33

5.3	Configuration of a PC/third-party device.....	34
6	VPN Activity Log.....	34
7	User management	35
7.1.1	Creating a user.....	35
7.1.2	Managing users.....	35
7.1.3	Enforce two-factor authentication for a user	36
7.1.4	Downloading the User List.....	36

1 General

This additional manual serves as a description of the DELTA LOGIC Connectivity Service and is only to be used together with the user manual and any other documentation of the respective VPN router. Safety instructions, technical data and functional descriptions can be found in the user manual for the respective device. The DELTA LOGIC Connectivity Service is supported by all DELTA LOGIC VPN routers.

For other DELTA LOGIC devices, contact us at support@deltalogic.de.

For third-party devices (PCs/controllers, etc.), we recommend installing a current version of the OpenVPN client on third-party devices.

The DELTA LOGIC Connectivity Service provides a secure VPN service: PCs, routers, and locally connected network devices (e.g., controllers, measuring devices, webcams) can be reached in all networks and addressed at any time.

Proceeding in the following order has proven advantageous when setting up a VPN network with the DELTA LOGIC Connectivity Service:

1. Planning the network topology
2. Creation of the devices (clients) in the DELTA LOGIC Connectivity Service
3. Client configuration; There are two options for devices from DELTA LOGIC:
 - a) Configuration via the quick start wizard (advantageous for devices that have not yet been configured (factory settings))
 - b) Configuration via the configuration file (advantageous for devices that have already been configured)

2 VPN-Service Background

The DELTA LOGIC Connectivity Service is a service of DELTA LOGIC for the simple and secure network connection of locations, plants, control centers and mobile devices via a VPN network.

2.1 Networking via DELTA LOGIC Connectivity Service

The PCs and routers (VPN clients) as well as locally connected network devices (e.g. controls, measuring devices, web cams) connected via the DELTA LOGIC Connectivity Service are accessible in all networks and can always be addressed. Simple rules enable to define which participants are allowed to connect with each other and which connections are not permitted.

The DELTA LOGIC Connectivity Service (VPN server) provides for the exchange of the routing information by informing each VPN client about it with the registration. In case of changes at the VPN network, the server will be restarted so that an anew automated registration of each client is necessary whereat the routing information will be updated.

If the clients are routers or fault monitors of DELTA LOGIC, these can be configured such that they can be accessed directly via netmapping. The latter is useful if the addresses in the local network behind the router are not to be reconfigured, for example in case of standard machines. Refer to the Configuration – Devices section of this manual for further information about this.

The DELTA LOGIC Connectivity Service does not only contain the VPN server, but also a web server for accessing the management portal of the VPN service configuration as well as an init server that provides the DELTA LOGIC routers with the required configuration during startup.

2.2 Secure Communication

The server of this VPN network is hosted secure in a German data processing center. The VPN network is protected with certificates. These certificates are generated, managed and renewed regularly by the VPN server. VPN access takes place via the UDP port shown on the “My VPN” tab.

2.3 Simple Setup and Management

The VPN service is managed via an easy-to-use management portal. You don't have to care for generation and management of the certificates since this is all taken over by the DELTA LOGIC Connectivity Service. HTTPS access to the management portal takes place via TCP port 443.

You benefit from the DELTA LOGIC Connectivity Service, because you don't have to operate an own OpenVPN server in your network and can save its operation and administration costs therefore. Moreover, it enables a highly flexible and easy to use rights management for all OpenVPN clients as well as a clearly laid out management of the field devices.

Your technicians benefit from an automated OpenVPN configuration of the field clients that allows an installation without any further OpenVPN know-how. The complete VPN configuration is transferred securely to DELTA LOGIC routers via the startup wizard.

2.4 China VPN

The DELTA LOGIC Connectivity Service permits a secure and reliable connection to devices in mainland China. Your DELTA LOGIC Connectivity Service account must be configured for this purpose. See the section "Activating China VPN" in this manual.

Following this reconfiguration, it is possible to select whether a device is installed in China or Rest of World when creating a device. Devices with China selected as the device location are automatically configured to maintain a secure and reliable connection to the DELTA LOGIC Connectivity Service from within mainland China. Devices configured as Rest of World will be configured the same as all other devices in the DELTA LOGIC Connectivity Service.

3 Login

To be able to use the DELTA LOGIC Connectivity Service, you must register for it first. You register for a 30-day free test access, with which you can create and manage a maximum of 4 devices for operation in the OpenVPN network. The free test phase ends automatically after 30 days. Two licences can be used permanently for free afterwards. Refer to the Licenses section at the end of this manual for further information about licensing.

3.1 Registration for the DELTA LOGIC Connectivity Service

1. Open the page <https://connectivity.deltalogic.de>
2. Choose your language and click Register. The access registration page opens.
3. Fill out the registration form accordingly and click Submit. The company name entered here then becomes the customer's name with which you register in the quick start wizard of the DELTA LOGIC devices for the DELTA LOGIC Connectivity Service.
Pay attention to the correct spelling of the e-mail address and password as well as the required mandatory fields and acceptance of the terms and conditions.
4. An email with an activation link will be sent to the specified email address. Click on the activation link in the email to activate your access.
5. You will receive another email with your access and customer data.
6. Now you can use the DELTA LOGIC Connectivity Service in test mode or order licenses for regular operation.

3.2 Registration on DELTA LOGIC Connectivity Service

You have already registered for the DELTA LOGIC Connectivity Service and received the e-mail with the access data.

1. Go to the website <https://connectivity.deltalogic.de>
2. Enter your credentials, choose your language, and click *Register*.

You have successfully registered with the DELTA LOGIC Connectivity Service.

3.3 Managing the own Password

A secure password for the access to the DELTA LOGIC Connectivity Service is essential for the security of the VPN network. It is highly recommended to change the password to a password only known to this user upon first login of the user added by the administrator. The password shall also be changed if it is suspected that it might have been disclosed to a third party.

Changing the Password

1. You are logged in to the icom Connectivity Suite
2. Click on "Settings" in the title bar and select "Password".
3. Enter your old password, enter your new password, confirm your new password by a second entry and click on "Change Password".

(The Reset button deletes all entries in the fields again.)

3.4 Activate the China VPN

Contact the DELTA LOGIC support team (support@deltalogic.de) if you wish to convert the DELTA LOGIC Connectivity Service for use with devices in mainland China. The DELTA LOGIC Connectivity Service is then manually reconfigured for China VPN.

4 Configuration VPN service

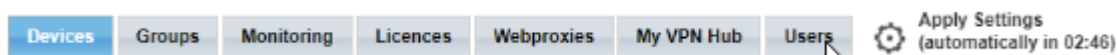
4.1 Devices

On the Devices tab, the individual VPN participants can be created and managed as devices (device management). A distinction is made between routers and fault indicators from INSYS icom and other third-party devices. These can be PCs, controllers, cameras, other routers, etc. that support OpenVPN and are collectively referred to as PCs in the DELTA LOGIC Connectivity Service. Moreover, a list of all added devices can be downloaded.



Following the creation of a device or a modification of a device, a timer will appear the menu bar, which indicates the time until the settings are fully applied. If the changes require a restart of the OpenVPN server instance, a restart will be made after the timer expires. A click on the gear symbol expires the timer and applies the settings immediately (with restart if necessary).

This shortens the configuration processes by combining all changes and executing them at the same time. An active timer will continue its countdown after logout from the Management Portal and apply the changes upon expiration (with restart if necessary)



An e-mail will be sent to the e-mail address allocated in your account upon each adding or deleting of a device as additional security and proof function. This function cannot be disabled.

4.1.1 Creating a device in the DELTA LOGIC Connectivity Service

When creating a device, a basic distinction is made as to whether it is a VPN router with icom OS, with INSYS OS or a PC. Depending on the selection, different parameters are available.

Configuration ("Devices" tab, "Add device" button)

With the **device type**, you select whether the device is a VPN router of the corresponding series or a PC. Depending on the selection, the configuration of the device address described below changes.

The **Device location** must be specified for devices installed on the **mainland** China. See "2.3 China VPN" on page 5.



Note:

This drop-down list is only available if your DELTA LOGIC Connectivity Service is configured for China VPN.

The **device name** is a name that uniquely describes the device so that it can be distinguished from other devices.

The **serial number** only must be entered for routers from the manufacturer INSYS and is located on the sticker on the device.

The **device code** can optionally be specified for a VPN router and is used to configure the router via the quick start wizard. If no own device code is specified here, the standard code is used (configurable under the "My VPN" tab). In addition, this code is also used as a password to access the router through a web proxy.

The **password for the certificate** can optionally be specified for third-party devices for additional security. If a password is specified here, it must be entered on the OpenVPN client of the PC.



Note:

DELTA LOGIC recommends protecting the certificate with a strong password, as this provides additional security, especially for PCs and mobile devices.

If a password for a certificate is specified later, a new certificate must be generated ("New certificate" button). A new connection must then be initiated with this configuration for the additional password protection to take effect.

The device can be assigned to a group in the **Group** tab. If no groups have been created yet, only the standard group is available here.

In the **License** tab, one of the available licenses is assigned to the device.

The **Default monitoring** checkbox can be used to specify whether the availability of the device should be monitored. See the Monitoring section of this guide for more information.



Note:

Depending on whether you configure an INSYS router with INSYS OS, icom OS or a third-party device (PC), only one of the following paragraphs is relevant. Information about addressing via Netmapping can be found in the "Addressing via Netmapping" paragraph. Information about direct addressing can be found in "Direct Addressing" paragraph.

IP address configuration (Directly accessible/Netmapping)

- For an **icom OS** router, the local IP address of the device under which the device (and other local devices) should be accessible is specified in the **Local IP address** field. This address is assigned to the router through router configuration.
- For an **icom OS** router, a virtual IP address is specified with the field **reachable only via Netmapping IP**, the device (and other local devices) can only be reached via this address. This address is assigned to the router through router configuration. With Netmapping, the local IP address must also be preconfigured, even if the router cannot be reached via it in the VPN.
- For an **INSYS OS** router, the **directly accessible** radio button can be used to determine whether the device should be reconfigured to an IP address by the DELTA LOGIC Connectivity Service. The local IP address of the device under which the device (and other local devices) should be accessible is then specified in the field **available local IP address**.
- For an **INSYS OS** router, the radio button **accessible via Netmapping** can be used to determine whether a (unique) virtual IP address should be redirected to the unchanged local address of the device. The virtual IP address of the device under which the device (and other local devices) should be accessible is then specified in the field **accessible Netmapping address**. The **local IP address** field can be used to specify the local IP address of the device. The local IP address cannot be addressed externally.
- For a **PC**, the IP address of the PC under which the PC (and other local devices) should be accessible can be entered in the field **Accessible IP address**.
- The **netmask** determines the size of the network that is made known via routing around the local IP address. The netmask can be entered in long form (255.255.255.0) or in CIDR format (/24). If a netmask other than the default (255.255.255.0) is entered, the DHCP server in the device will be disabled.

Save your settings by clicking "OK".

4.1.2 Managing Devices

The "Devices" tab shows a list of the created devices. The devices can be managed and adjusted here.

Configuration ("Devices" tab)

Another device can be added with the **Add device** button.



The **Replace** button allows to replace a device used in the field by a new device by taking over the existing settings regarding VPN connectivity within the DELTA LOGIC Connectivity Service easily.



The **Copy** button in a device's row allows you to add another device based on the data of that device.



The **Delete** button in a device's row allows you to remove that device.



The **Manage** button allows the settings of this device to be edited. Furthermore, a new certificate can be created here, and older certificates can be invalidated. It is also possible to switch off the router in the DELTA LOGIC Connectivity Service, i.e., it will be rejected by the VPN network if the "switched off" checkbox is marked. This is necessary, for example, if a device can no longer be trusted (e.g., a stolen notebook).

The serial numbers for all certificates issued for this device are displayed (see Exchanging Certificates on page 22).

Optionally, a time-limited access (TR access) can be activated and configured for each device. Two-factor authentication using TOTP can optionally be activated for PCs (see Configuring two-factor authentication (TOTP)).



Note:

If modifications are made here, it must be ensured that the changes are also made in the respective device. ICOM-OS devices accept the saved changes (with an established VPN connection) after approx. 10 minutes. This carried out for INSYS-OS-routers either once a day automatically (if the router is online at this point in time) or manually by manually activating the automatic update function in the web interface of the router. In case of PCs, the modifications must always be carried out manually.

If the Device Code is changed here, this must be changed manually in the update server settings in the web interface of the router, because no automatic update would be possible any more otherwise.



The **Download** button downloads a configuration file for this device and a container with the certificates and keys.

The **More Info (i)** button can be used to display additional information about this device, such as the volume of data transferred or the VPN IP address.

The **status** of the device is displayed in the **Status** column with a delay of 1-2 minutes. The device can be online, offline, powered off, or unlicensed.

The **since** column shows how long the device has been in its current state.

The **Group** column indicates which group the device is assigned to.

The IP address under which the device can be reached is specified in the **reachable IP** column.

The serial number of the device is displayed in the **S/N** column (only for DELTA LOGIC devices).

The scope of the license is specified in the **License** column.

4.1.3 Downloading the device list

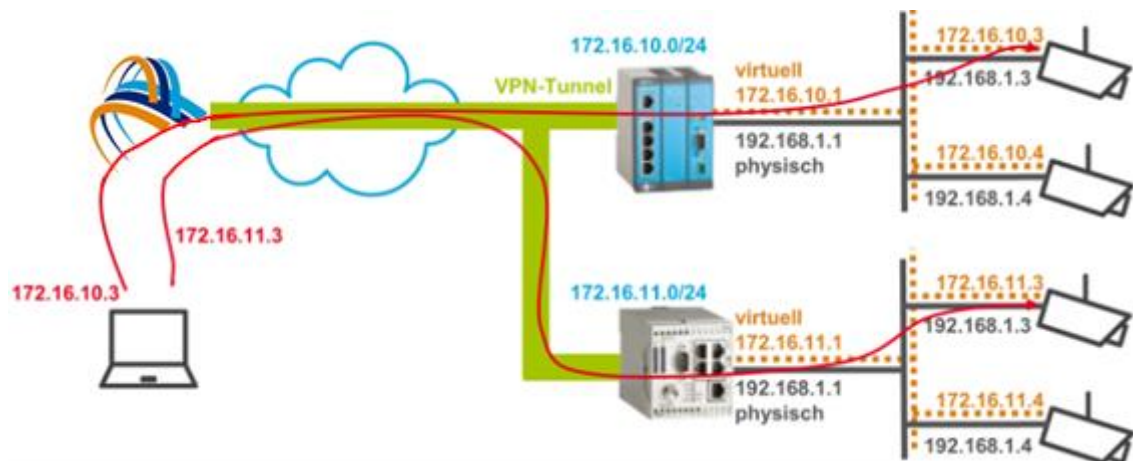
The "Devices" tab shows a list of the created devices. This list can be downloaded as a CSV file. In addition to the information shown in the list, the file also contains information about the data volume used in the current month, in the previous month and over the entire period since the device was created. The CSV file contains the columns analogous to the device list, separated by an "=" (equals sign).

Configuration ("Devices" tab, "Download device list" button)

The device list is downloaded in the download window by clicking on **Device list**.

4.1.4 Addressing via netmapping

Using netmapping allows that devices in the local network behind an VPN router do not have to be reconfigured. A virtual network address is assigned to the local network. Devices in the local network can then be addressed with the virtual address via the DELTA LOGIC Connectivity Service. The router exchanges the network part of the virtual IP address for the network part of the local network and forwards the packet to the destination.



In the above example, netmapping was activated in the routers and the virtual network addresses "172.16.10.0" in the upper local network and "172.16.11.0" in the lower local network were configured. As a result, the devices in the local network (192.168.1.0/24) can also be reached via the virtual network address (172.16.10.0/24 above and 172.16.11.0/24 below) and do not have to be reconfigured, even though they have the same local network addresses. The upper camera with the local network address 192.168.1.3 can thus be reached from outside via the address 172.16.10.3 and the lower one via the address 172.16.11.3.

4.1.4.1 Netmapping in VPN routers with icom OS

If the router is configured via the DELTA LOGIC Connectivity Service, netmapping will be set up automatically. Appropriate NAT rules will be configured for this. The NAT rules below can be configured manually in the "Netfilter" menu on the "NAT" page. For more information, see the router's inline and online help.

In the above example, the following NAT rules are created in the upper router:

Source NAT rule:

Type: Netmap

Protocol: All

Outgoing interface: openvpn1 – DELTA LOGIC Connectivity Service

Sender IP address: 192.168.1.0/24

Source NAT on address: 172.16.10.0

Destination NAT rule:

Type: Netmap

Protocol: All

Incoming interface: openvpn1 – DELTA LOGIC Connectivity Service

Sender IP address: 172.16.10.0/24

Source NAT on address: 192.168.1.0

The DNAT rule causes packets in the VPN service that are addressed to addresses in the 172.16.10.0/24 network to be forwarded to the corresponding addresses in the local network 192.168.1.0/24. The SNAT rule causes packets from the devices in the local network 192.168.1.0/24, which are directed to the VPN network, to be provided with a sender IP address in the network 172.16.10.0/24.

This means that the devices in the local network (192.168.1.0/24) can also be reached via the virtual network address (172.16.10.0/24) and do not have to be reconfigured. The camera with the local network address 192.168.1.3 can thus be reached externally via the address 172.16.10.3.

4.1.4.2 Netmapping in VPN routers with INSYS OS

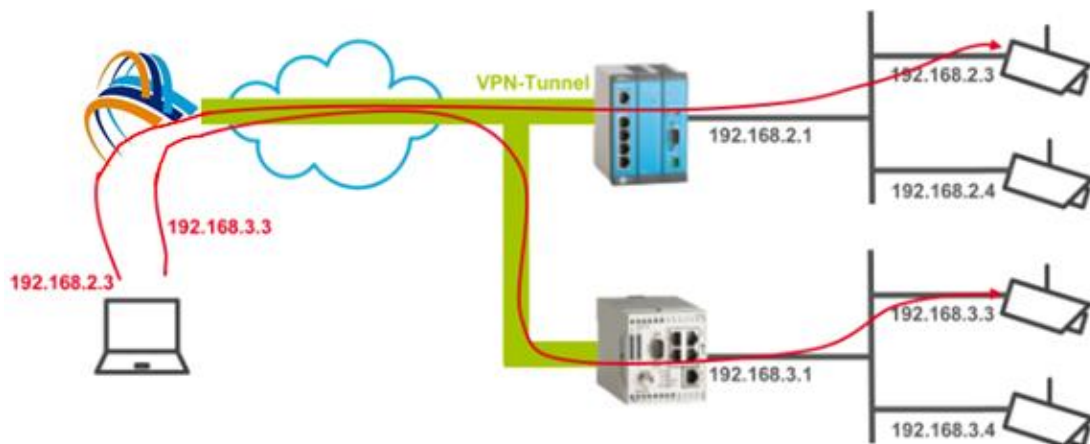
If the router is configured via the DELTA LOGIC Connectivity Service, netmapping is set up automatically. Netmapping can be set up manually in the "Basic Settings" menu on the "IP Address (LAN)" page of the VPN router. For more information, see the router's user manual.

In the above example, netmapping is activated in the lower router and the virtual network address "172.16.11.0" is configured in the local network.

This means that the devices in the local network (192.168.1.0/24) can also be reached via the virtual network address (172.16.11.0/24 below) and do not have to be reconfigured. The camera with the local network address 192.168.1.3 can thus be reached from outside via the address 172.16.11.3.

4.1.5 Direct Addressing

With direct addressing, the devices in the local network are addressed directly with their address via the DELTA LOGIC Connectivity Service. In the example below, this is shown in contrast to addressing via netmapping.




4.1.6 Activating time-restricted access for a device

Time-restricted (TR) access is not part of the standard functional scope and available on request. A time-restricted access can be set up for each device, in particular the device type PC. This permits to grant a device access for a specified time. Without time-restricted access, each device is able to establish a connection to the VPN network. To do this, only its OpenVPN client needs to be configured with the configuration file downloaded from the DELTA LOGIC Connectivity Service for a PC type device. If time-restricted access is activated for a device, connections from this device to the VPN network will only be released for a specified time, if the user acknowledges this using a token sent via e-mail.

Two different releases are possible here:

- Activating the connection for a specified time window
- Activating the connection for a specified duration

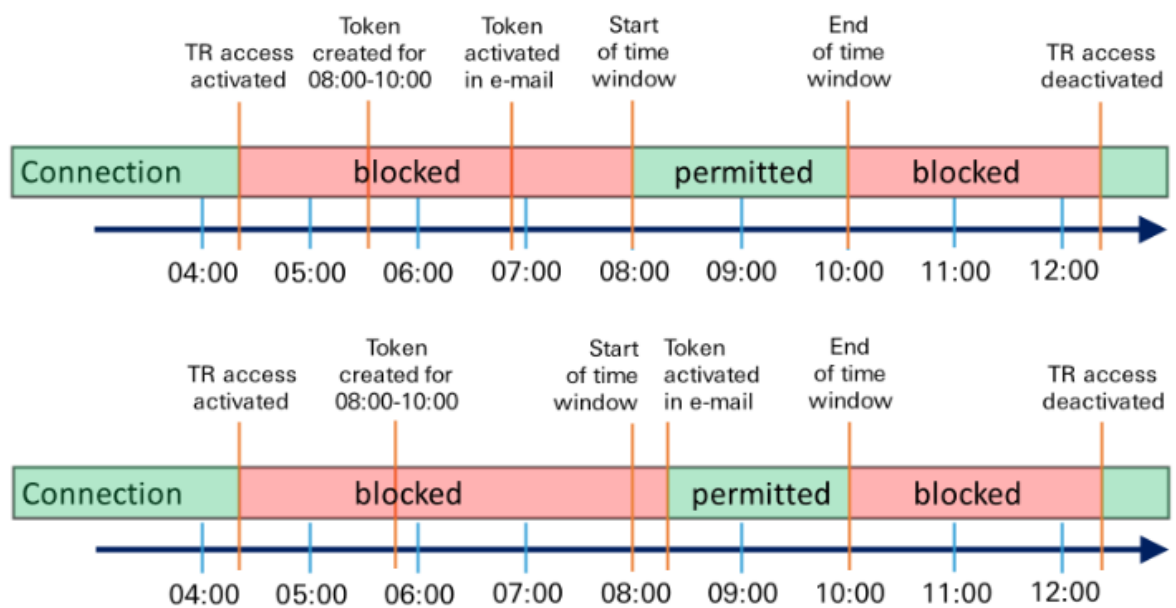
The time-restricted access is configured in the device list (**Devices** tab) in the device settings (**Manage** () button of the respective device) using the **Manage TR access** button.

The function is activated here using the **Activate time-restricted access** checkbox. The token will be sent to the specified e-mail address.

4.1.6.1 Activating the connection for a specified time window

In **Time window** mode, the time window is specified, in which connections from this device to the VPN network are released upon authentication using the link in the e-mail.

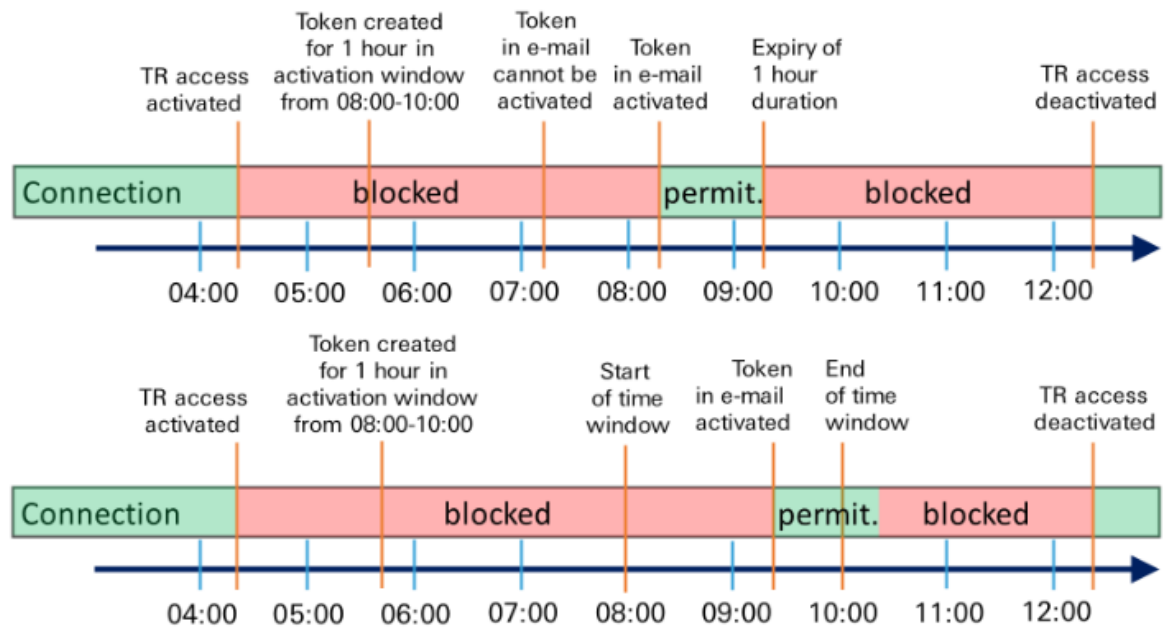
The following diagram shows different examples for the sequence of time-restricted access for a specified time window:



4.1.6.2 Activating the connection for a specified duration

In **Duration** mode, the duration is specified, for which connections from this device to the VPN network are released upon authentication using the link in the e-mail. In addition, a time window is determined, in which the authentication using the link in the e-mail can be made (activation window).

The following diagram shows different examples for the sequence of time-restricted access for a specified duration:



4.1.7 Configuring the two-factor authentication (TOTP)

To increase security, two-factor authentication can be set up using TR for PC-type devices.

Two-factor authentication adds another level of security to certificate login (with or without password protection) by requiring the additional entry of a one-time password. The password is generated using the TOTP (Time-based One-time Password) process with the help of an app on a separate device (e.g., smartphone). During setup, the app that provides the TOTP needs to be synchronized (once) with the device of type PC in the DELTA LOGIC Connectivity Service. TOTP is an open standard, and a variety of apps are available for different platforms such as the open-source software FreeOTP (<https://freeotp.github.io/>). Since the one-time passwords are generated based on time and are only valid for a limited time, it is necessary for the time on the separate device to be accurate and synchronized regularly.

To enable two-factor authentication for the PC type device, do the following.

Setting up two-factor authentication for a PC

- You have logged on to the DELTA LOGIC Connectivity Service.
- The device for which two-factor authentication is to be activated has already been created.
- You have opened the "Devices" tab.
 1. Click on the **Manage** button in the device row.
 2. Click the **Setup TOTP for this device** button.
 3. Scan the displayed QR code with the TOTP app.

4. Generate the one-time password in the app and enter it in the DELTA LOGIC Connectivity Service.
5. Click "Configure One-Time Password".
 - You have now set up two-factor authentication for this device.
6. Click the **Download** button in the device row.
7. Import this configuration file into your PC's OpenVPN client and initiate a connection.
8. To authenticate the connection, enter:
 - User: insys
 - password: a one-time password from your TOTP app
 - Private key password: the password for the certificate that was specified when creating the device of type PC - if no password is configured here, the certificate is not password-protected, and no key is requested

(The OpenVPN client connects to the DELTA LOGIC Connectivity Service.)

Follow these steps to disable two-factor authentication for a PC-type device.

Disable two-factor authentication for a PC

- You have logged on to the DELTA LOGIC Connectivity Service
- Two-factor authentication is active for the device in question
- You have opened the "Devices" tab
- Click on the **Manage** button in the device row.
- Click the **Disable TOTP for this device** button.
- You have deactivated the two-factor authentication for this device again.



Note:

After disabling two-factor authentication, you need to download the configuration file again and import it back into your PC's OpenVPN client. If there is also no password for encrypting the certificate, no authentication takes place when it is reconnected.

If two-factor authentication is deactivated for a device, it should also be deleted from the app. If it is activated again, it must be set up again in the app.

4.1.8 Replacement of Certificates

In addition to the regular rotation of the certificates every 90 days, the CA certificate also expires after 10 years and must then be replaced. The user will be informed 120 days in advance (by e-mail and notification upon registration). Client certificates created with this CA must then be exchanged so that the device can continue to connect to the DELTA LOGIC Connectivity Service.

The Manage Device dialog box displays the serial numbers for the certificates issued for this device. If the serial number is shown in bold and black, the certificate is current. A yellow number means that the certificate was issued by the old CA and will only work for 30-120 days (if the old CA certificate is valid). If the validity period is less than 30 days, the serial number is displayed in red. If more than one serial number is shown, these are certificates that have been issued but not yet applied, or certificates that have expired but not yet been deleted. Usually, expired certificates are deleted after 15-30 minutes. If multiple serial numbers are displayed, replacing the certificate, and updating the configuration for the DELTA LOGIC Connectivity Service on the router is recommended.

Depending on the device and its condition, the following measures are required to exchange the certificate and update the configuration:

4.1.8.1 INSYS router that can still be reached in the DELTA LOGIC Connectivity Service

Make sure that the DELTA LOGIC Connectivity Service update server is activated in the router. This is done in the router's "Administration" menu on the "Update" page. If this is activated, the certificate is automatically updated during operation.

4.1.8.2 INSYS router that can no longer be reached in the DELTA LOGIC Connectivity

In this case, the certificate must be exchanged via local access on the router.
See the "Manual Configuration" sections.

4.1.8.3 Third-party device (PC, controller, tablet, etc.)

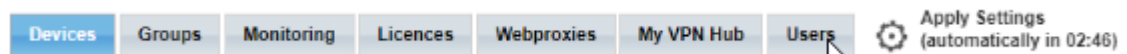
With a third-party device, the OpenVPN configuration must be exchanged manually on the third-party device. See "Configuring a Third-Party Device".

4.2 Groups

The groups to which the devices are assigned can be added and managed on the Groups tab (group management). Groups are used to group devices with similar functions in order to assign them common communication rules.



Following the modification of a group, a timer will appear in the menu bar, which indicates the time until the settings are applied. A click on the gear symbol triggers an immediate restart. Since each modification of the Groups configuration requires a restart of the OpenVPN server instance, this shortens the configuration processes by combining all changes that require a restart and executing them at the same time. An active timer will continue its countdown after logout from the Management Portal and restart the OpenVPN server instance upon expiration.



4.2.1 Creating a group

It is recommended to think about a reasonable arrangement of the devices into groups before adding the groups.

To do this, select the "Groups" tab in the DELTA LOGIC Connectivity Service.

Configuration ("Groups" tab, "Add group" button)

The **group name** is a name that uniquely describes the group so that it can be distinguished from other groups.

The **Allow connections among group members** checkbox can be used to specify whether the devices within this group can connect to each other.

Save your settings by clicking "OK".

4.2.2 Manage the groups

The "Groups" tab shows a list of the created groups. The groups can be managed here. Communication within a group and between different groups is also defined here.

Configuration ("Groups" tab)

Another group can be added with the **Add group** button.

Another group can be added with the **Copy** button, whereby the parameters of the window are already preassigned with those of the copied group. Adjusting these parameters allows for quick creation of similar groups.

This group can be deleted with the **Delete** button.

The name of this group is displayed in the **Group name** column.

The button in the **Internal Connections** column can be used to specify whether connections between the devices in this group are allowed or forbidden.

The button in the **Connection from** column can be used to specify the groups from which incoming connections are accepted, i.e., devices in the marked groups can establish connections to the devices in this group. Furthermore, these connections can be restricted to specific protocols, target stations and target ports (group management advanced). The names of the groups allowed for these connections are displayed on the button. The addition [LIMITED] indicates that additional restrictions have been set for these connections.

The button in the **Connection to** column can be used to specify the groups to which outgoing connections can be established, i.e., devices in this group can establish connections to the devices in the marked groups. Furthermore, these connections can be restricted to specific protocols, target stations and target ports (group management advanced). The names of the

groups allowed for these connections are displayed on the button. The addition [LIMITED] indicates that additional restrictions have been set for these connections.



Note: If a connection is set with one of the "Connect from" or "Connect to" buttons, it is automatically set for the other direction as well.

4.2.3 Rules of Communication

4.2.3.1 Establishing the rules of communication

After the groups have been created, the communication rules can be created within the individual groups and between the groups. These rules are subject to change at any time.

The communication rules determine whether PCs, VPN routers and locally connected devices can connect to each other.

4.2.3.2 Communication within a group

The DELTA LOGIC Connectivity Service allows all devices in a group to allow or deny communication with each other. A ban on internal connections makes sense, for example, if devices from different customers are in a group. The rules for internal communication are defined when the group is created and can be changed at any time on the "Groups" tab in the "Internal Connections" column.

4.2.3.3 Communication between groups

The DELTA LOGIC Connectivity Service makes it possible to define rules for communication between devices that are in one group and devices that are in another group. The rules for communication between the groups are defined on the "Groups" tab in the "Connection from" (incoming) or "Connection to" (outgoing) columns for the respective group. For example, if a group (A) is allowed incoming connections from another group (B), outgoing connections to group (A) are automatically allowed for group (B).

4.2.3.4 Restrictions for the communication between groups

If connections between the devices of individual groups are permitted, access to the entire network behind this router is enabled for connections to a router. It is therefore possible to restrict these connections to specific protocols, destination stations and destination ports. This is done when specifying the permitted connections by checking the "Additional restrictions for the connection destinations" checkbox.

Protocol

It is possible to restrict the protocol used for the connection to "TCP+UDP", "TCP", "UDP" or "ICMP". If a specific protocol is selected here, only connections via this protocol can be established between the devices in the relevant groups. User connections usually use TCP or UDP; the ping command to check reachability uses ICMP.

Destination station

By specifying a destination station, it is possible to limit the connections to specific devices in the network behind the router. For the destination station, only the part of the address that specifies the designation within the respective network is specified. This information is "added" to the network address to obtain the IP address of the target device. A target station that defines an entire IP address range can also be specified with the help of a network mask in CIDR notation.

Destination port

By specifying a target port, it is possible to restrict TCP and UDP connections to specific ports. Multiple ports can be specified, separated by commas, or entire port ranges. For example, the destination port specification "80, 443, 1194-1199" allows connections via ports 80, 443, 1194, 1195, 1196, 1197, 1198 and 1199.

4.3 Monitoring

The monitoring function is used to monitor and ensure that all participants in the VPN network can be reached (network monitoring). There are various options for checking the connection. The checks and hosts can be created and managed on the Monitoring tab. Hosts are all network devices that can be addressed via an IP address in the VPN network. These are the VPN participants (routers, PCs, tablets, etc.) themselves and the devices in the network (Control Network, OT) behind the routers (controllers, panel PCs, HMIs, data loggers, measuring devices, condition monitoring or edge -Computing devices, etc.).

If verification of a connection fails, an error report is sent to a registered email address. As soon as this check is successful again, another e-mail will be sent informing you that the connection has been restored.

Examinations are not affected by any communication rules.

Five checks can be created per valid VPN license, whereby these tests can be distributed across all devices and are not limited to the device assigned to the respective license. The number of hosts is not limited.

The PING, HTTP, and HTTPS types of checks generate traffic over the VPN connection. The VPN-type check does not cause any additional data volume, as the continuous tunnel monitoring is evaluated on the VPN server.

See also the FAQ on network monitoring.

4.3.1 Adding a Check

When adding a device, a check will be added if the checkbox “Default monitoring” is checked. In this case, this device will automatically be added as a host together with a ping check with an interval of 60 minutes. Further checks can be added on the Monitoring/Checks tab.

Configuration (“Monitoring/Checks” tab, “Add new check” button)

The **Name** is a name that describes the check such clearly that it can be distinguished from other checks. The proposed name is composed of the type of the check and the specified host.

The **Description** field can be used for a detailed description of the check. The content of this field will also be transmitted in the failure report. It can thus be used to transmit further information in the failure report.

The **Host** for which the check is to be performed can be selected from the respective drop-down list. All already added hosts are listed here. If the check is to be performed for a host that has not yet been added, this can be added using the “add new host” button.

The **Type** of the check can be selected from the respective drop-down list. The following types are available for this:

- **HTTP:** An HTTP request to the web server of the specified host will be performed. If the web server responds with OK, the check is considered as successful.
- **HTTPS:** An HTTPS request to the web server of the specified host will be performed. If the web server responds with OK, the check is considered as successful.
- **PING:** A ping request to the specified host will be performed. The check is considered as successful if the host responds to 3 of 5 ping requests within 5 seconds positively.
- **VPN:** The OpenVPN client status in the VPN server is used here. If it is still registered, the check is considered as successful.

The **Check interval** specifies the interval in which the checks are performed.

The **Retry interval** specifies the interval in which the checks are performed if a check has failed. This interval is usually shorter than the check interval.

The **Max. check attempts** specify the number of checks before the regular check interval is used again.

The **Alarm e-mail** is the address to which the failure reports will be sent. Several recipient addresses can be entered separated by commas or blanks. If no address is entered, no failure report will be sent.

The **Http(s) port** specifies the port that is used for receiving the HTTP(S) requests to the web server of the host (only for type HTTP(S)).

The **Http(s) username** is used for HTTP(S) requests to the web server if this requires an authentication (only for type HTTP(S)).

The **Http(s) password** is used for HTTP(S) requests to the web server if this requires an authentication (only for type HTTP(S)).

Save your settings by clicking "OK".

4.3.2 Managing the Checks

The “Monitoring/Checks” tab shows a list of the added checks. The checks can be managed here. Moreover, the status of the checks is indicated here. The checks are listed in host groups. The checks under the respective hosts can be expanded or collapsed using the “+” or “-” button in front of the host. If the checkbox “Collapse groups without disturbances” is checked, only the groups that have disturbances are expanded.

The **Add new check** button can be used to add another check.

The **Copy** button can be used to add another check in which the parameters in the window are already preset with those of the copied check. Adjusting these parameters allows a quick adding of similar checks.






The **Delete** button can be used to delete this check.

The **Manage** button can be used to edit the settings of this check.

The name of this check is indicated in the **Name** column.

The last state of this check is indicated in the **State** column.

The following states are possible:

-  **OK:** The last check was successful.
-  **warning:** The last check was successful, but the request has only been responded with delays (packet turnaround time ≥ 2500 ms) or not completely.
 -  unstable: Frequent state changes have been detected with activated stability recognition.
-  **pending:** No check has been performed so far.
-  **error:** The last check was not successful.

The **Since** column indicates since when this check is in this state.

The configured type of this check is indicated in the **Type** column.

The configured interval of this check is indicated in the **Interval** column.

The e-mail address to which the failure reports of this check are sent is indicated in the **E-mail** column.

4.3.3 Adding a Host

A host must be added to add a check. This can be made when adding a check or separately on the Monitoring/Hosts tab. When adding a host, a ping check with an interval of 60 minutes will automatically be added for this host. If a host is added that is not VPN client, the associated VPN client will also be added as host if it has not already been added.

Configuration (“Monitoring/Hosts” tab, “Add new host” button)

The **Name** is a name that describes the host such clearly that it can be distinguished from other hosts.

The **Accessible IP address** is the IP address under which the device, which is to be added as host, is accessible in the VPN network. The accessible IP address of a device can also be taken from the respective column on the Devices tab. If no accessible IP address has been specified for a device, the fix VPN IP address can also be used. This is indicated if you select on the Devices tab the "More information" button of the respective device.

4.3.4 Managing the Hosts

The “Monitoring/Hosts” tab shows a list of the added hosts. The hosts can be managed here. Moreover, the status of the hosts is indicated here. The hosts are listed in device groups. The hosts under the respective devices can be expanded or collapsed using the “+” or “-” button in front of the device. The group starts with the VPN host followed by further hosts in the local network of the VPN client. The network structure will be visualised by the indentation. If the checkbox “Collapse groups without disturbances” is checked, only the groups that have disturbances are expanded.

Configuration (“Monitoring/Hosts” tab)

The **Add new host** button can be used to add another host.

The **Copy** button can be used to add another host in which the parameters in the window are already preset with those of the copied host. Adjusting these parameters allows a quick adding of similar hosts.

The **Delete** button can be used to delete this host.





The **Manage** button can be used to edit the settings of this host.

The name of this host is indicated in the Name column.

The **Accessible IP** column indicates the IP address under which this host can be accessed.

The last state of this host is indicated in the **State** column.

The following states are possible:

-  **up:** The last check of this host was successful.
-  **warning:** The last check of this host was successful, but the request has only been responded with delays (packet turnaround time ≥ 2500 ms) or not completely.
unstable: Frequent state changes have been detected with activated stability recognition.
-  **unknown:** The host is unknown.
unreachable: The host could not be reached.
-  **down:** The last check of this host was not successful.

The **Since** column indicates since when this host is in this state.

4.3.5 Configuring the check options

The “Options” tab provides a series of settings for view and notification regarding the checks.

Configuration (“Monitoring/Options” tab)

If the option **Collapse groups without disturbances** is activated, only the groups with disturbances are displayed on the “Checks” and “Hosts” tabs. The groups can always be expanded manually using the “+” symbol in front of the device name.

The setting **Suppress messages at instance restart** specifies how long monitoring will be suspended upon a restart. This can be used to avoid sending the e-mails upon loss and restoration of the connection following a restart.

If the option **Detect and report unstable VPN connections** is activated, the stability of the connection will be determined in addition to the connection status check. A connection is classified as “unstable” if more than 4 state changes have occurred in the last 21 checks. The

connection is classified as "stable" again if not more than one state change has occurred during the last 21 tests. A state change is when the device connection changes from "connected" to "disconnected" or the connection quality becomes too poor (packet turnaround time ≥ 2500 ms) and vice versa.

If the option **Send mail at stability issues** is activated, notifications will also be sent if the connection is detected as "unstable".

If the option **Disable all monitoring notifications** is activated, no notifications regarding the checks will be sent. Temporarily disabling notifications can be helpful to prevent repeated sending of notifications in case of extensive configuration changes.

4.4 Licenses

The use of the DELTA LOGIC Connectivity Service is linked to the purchase of licenses. Further details on the licenses can be found on our website and in the product description.

4.4.1 Ordering a Licence

Four time-limited licences are available in the **free test phase**. Further licences can be ordered on the Licences tab.

Configuration (“Licences” tab, “Order licences” button)

The status of all licenses is listed again at the top of the window. The currently valid price list can also be called up. To place an order, you must also accept the General Terms and Conditions here.

The number of **licenses** indicates how many licenses of the respective license model you want to order with this order.

The **Order Reference Number** should be entered in the Order reference number field. This information facilitates processing and can prevent delays.

The customer's **company data** is taken from the data stored in the DELTA LOGIC Connectivity Service and cannot be edited. Sales tax ID and customer number must still be specified.

The **contact person** is taken from the data stored in the DELTA LOGIC Connectivity Service and can still be edited.

The **customer's name** for the input in the quick start wizard of INSYS routers is given here again but cannot be edited.

Place the order by clicking on "Order".



An e-mail with a confirmation of the order will be sent to the e-mail address stored in your account.

4.4.2 Managing the Licenses

The “Licences” tab shows a list of the existing licences. The licences can be managed here. Moreover, the scope and the validity period of the licences is indicated as well as the device to which they are assigned to.

Configuration (“Licences” tab)

The **Order licences** button can be used to order further licences.

The **Manage** button can be used to assign or release the license to another device. With Flex licenses, a license can be canceled at the end of the current month.

A license log for this license can be displayed with the **More Info** button. The log contains all events related to this license.

The name of this license is displayed in the **Name** column. The name assigned by the DELTA LOGIC Connectivity Service can also be edited here.

The scope of this license is displayed in the **Scope** column.

The **Valid until** column shows how long this license is still valid.

The **Device** column shows which device this license is assigned to.

The **Renewal** column shows how many years after expiration this license will be renewed.

The **Receipt** column shows the order with which this license was ordered.

The **Free** column shows whether this license was made available free of charge.



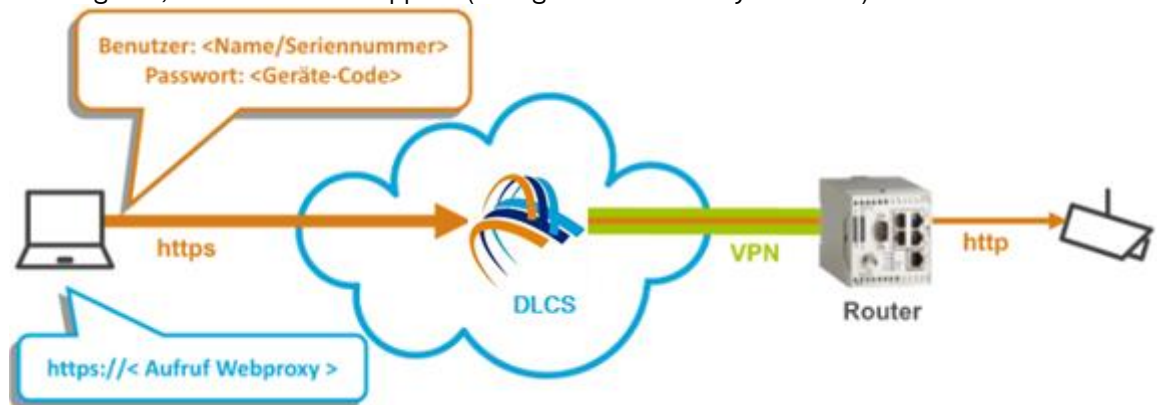
For each change, an email will be sent to the email address stored in your account.

4.5

Web Proxies

The DELTA LOGIC Connectivity Service enables web proxies to be set up.

Web proxies provide access to a web service that can be reached in the VPN using the HTTP or HTTPS protocol. This means that many http(S)-enabled devices (e.g. IP cameras) can be accessed from almost any PC or smartphone with Internet access. The data is transmitted encrypted via https. The device can be accessed using the address shown in the "Call Web Proxy" column. Authentication is via a combination of username and password. The username is either the name of the web proxy or the serial number of the VPN router to which the device to be accessed is connected. The password is the device code of the VPN router. If no device code is configured, the default code applies (configurable in the "My VPN" tab).



Password authentication can be optionally deactivated. This may be necessary, if a camera requires an HTTP authentication since a two-stage authentication is not possible in one browser session.

It is also possible to establish a persistent connection for full-duplex communication through a WebSocket using the port specified.

Note



Security risk!

The application concerned is accessible via the Internet when using a web proxy.

The encrypted connection is only protected against access from the Internet by a password. Choose a password that is as secure as possible and change the password regularly. We do not recommend this feature for safety-critical applications.

4.5.1 Setting Up a Web Proxy

Proceed as follows to add a new web proxy.

Configuration ("Webproxies" tab, "Add new webproxy" button)

The **device** for which the web proxy is set up can be selected from all INSYS routers registered at the DELTA LOGIC Connectivity Service.

The **name** is a name that uniquely describes the web proxy so that it can be distinguished from other web proxies.

The **IP address in the VPN** is the IP address under which the device can be reached in the VPN.

If the **Destination uses HTTPS protocol** checkbox is selected, the web proxy supports TLS-enabled connections between the VPN service and the edge device or application, if supported.

The **port** is the port through which the device can be accessed.

If the **No authentication by web proxy** checkbox is selected, the device can be accessed without a password.

The following **advanced settings** are available for special use cases. We recommend using the default settings if you are unsure of the impact of changes:

If the checkbox **Additional independent authentication on target device (only "Form-based-Auth")** is selected, "Form-based authentication" can take place on the target device in addition to authentication by the web proxy.

If the **Proxy WebSocket protocol** checkbox is activated, a WebSocket connection (ws: or wss:) is enabled between the VPN service and the application. For example, we recommend allowing a WebSocket connection if a web proxy is used to access INSYS routers with icom OS 5.5 or higher.

The HTTP protocol for the web proxy can be specified under **Select protocol version**. HTTP/1.1 is recommended for new web proxies. If required, HTTP/1.0 can be used to support communication with legacy web proxies.

If the **CORS enabled** checkbox is activated, cross-origin resource sharing is allowed, i.e. the client may also make script requests to a server in a different domain, which is normally prohibited by the same-origin policy (SOP).

If the **Accept-Encoding: without compression** checkbox is activated, no further compression of the transmitted content takes place.

Save your settings by clicking "OK".

Note



Security risk!

The application concerned is accessible via the Internet without protection by the DELTA LOGIC Connectivity Service upon deactivation of the authentication.

Security can only be provided by the application itself. A regular check of the application for security vulnerabilities is strictly recommended therefore. We do not recommend this function for applications that are relevant to security.

4.5.2 Managing the Web Proxies

The “Webproxies” tab shows a list of the existing web proxies. The web proxies can be managed here. Moreover, the scope and the validity period of the licences is indicated as well as the device to which they are assigned to.

Configuration (“Webproxies” tab)

Another web proxy can be added with the **Add web proxy** button.

Another web proxy can be added with the **Copy** button, whereby the parameters of the window are already preassigned with those of the copied web proxy. Adjusting these parameters enables quick creation of similar web proxies.

This web proxy can be deleted with the **Delete** button.

With the **Manage** button, the settings of this web proxy can be edited.

The name of this web proxy is displayed in the **Name** column.

The **web proxy call** column shows the address with which the application behind the device can be accessed without VPN access.

The IP address under which the device can be reached in the VPN is displayed in the **IP in VPN** column.

The **Port** column shows the port through which the device can be accessed.

The Device column shows the device on the VPN through which the application can be accessed.

An **open lock** appears in the last column if this web proxy is configured for access without a password.

4.6 My VPN

The "My VPN Hub" tab shows important information about this account. This data can also be important for the manual configuration of third-party devices, for example.

DELTA LOGIC Connectivity Service Settings

Devices Groups Monitoring Webproxies **My VPN Hub** Users M2M SIM Activities Licences

Set Default Code VPN Log Restart VPN Instance Custom information Activate grouping for devices and licences ☒

Setup two-factor authentication for this user

Feature	Status
Instance ID	271 - premium
Customer Name	DELTA LOGIC GmbH
Default Code	<div>XXXXXXXXXX</div> <i>The default code is used for Quick installation of INSYS routers if no individual device code is set</i>
Status Page	https://status.ics-vpn.de/ <i>The password is the default code</i>
VPN Server	271.dlcs-vpn.de
VPN Port	1149 / udp
VPN Range (reserved)	198.18.0.0 / 255.255.0.0
Licences	15 Unrestricted Licences (5 used) 0 Classic Licences (0 used) 0 Flexible Licences (0 used) 0 Flexible (non INSYS device) Licences (0 used)
Certificate Renewal Interval	90 days <i>Certificates are renewed on the server after this period automatically. Old certificates are cancelled only when a newer certificate has been used successfully. INSYS routers can download and install new certificates automatically from the server.</i>
Allow Webproxy without authentication	not permitted <i>Access through the webproxy is secured by http authentication. If your application requires http authentication as well then the webproxy authentication can be deactivated.</i>
Your user name is	deltalogic
Your user role is	Customer Administrator
Two-factor authentication required	No
Two-factor authentication status	No
Delete this account	Delete this account

The instance number is a unique number used to identify an account. The account type, which defines the scope of services of this account, is specified after the instance number.

The customer's name is required for the quick start wizard of INSYS routers.

The default code is always used as the device code if no separate device code is specified for a device. The device code is required for the quick start wizard of INSYS routers and for access via a web proxy.

The information for VPN server, VPN port and VPN area is important for the manual VPN configuration of third-party devices (PCs). The VPN port specifies on which UDP port the DELTA LOGIC Connectivity Service accepts OpenVPN tunnels. The user must ensure that outgoing UDP traffic for the router is allowed on this port and responses are allowed (e.g., open this port in the firewall).

The Licences section provides an overview of the number and type of licenses available and how they are used.

In addition to displaying the username and user role of the logged-in user, it is also shown whether two-factor authentication is required due to the setting in the user administration (Users tab) and the status of the two-factor authentication for the currently logged-in user (Tab My VPN Hub) now is.

The standard code can also be changed here, additional licenses ordered, the VPN log downloaded, and the two-factor authentication activated, deactivated, and renewed for this user.

4.6.1 Changing the Default Code

Proceed as follows to change the default code.

Configuration ("My VPN Hub" tab, "Set Default Code" button)

The **Default Code** is indicated and can be changed accordingly.

Save your settings by clicking "OK".

4.6.2 Downloading the VPN-Log

The VPN log records all events of the VPN server.

Configuration ("My VPN Hub" tab, "VPN-Log" button)

The drop-down list **Days** determines the number of days included in the log.

Download the log by clicking "OK".

4.6.3 Restarting the VPN instance

The VPN instance can be restarted manually if necessary.

Configuration ("My VPN Hub" tab, "Restart VPN instance" button)

Restart the VPN instance by clicking "Restart VPN instance".

4.6.4 Ordering licences

See the license ordering section.

4.6.5 Managing the two-factor authentication

Two-factor authentication adds another level of security to username and password login by requiring the additional entry of a one-time password. The password is generated using the TOTP (Time-based One-time Password) process with the help of an app on a separate device (e.g., smartphone). To do this, the user account of the DELTA LOGIC Connectivity Service must be registered once in the app. TOTP is an open standard and a variety of apps are available for different platforms such as the open-source software FreeOTP (<https://freeotp.github.io/>). Since the one-time passwords are generated based on time and are only valid for a limited time, it is necessary for the time on the separate device to be accurate and synchronized regularly.



Note:

If two-factor authentication is enforced in the user management (see section "User management"), the logged-in user cannot deactivate it here. It can only be activated and deactivated here if it is not activated in the user management.

4.6.5.1 Setting up the two-factor authentication for the user logged in

- You have logged on to the DELTA LOGIC Connectivity Service
- You have opened the "My VPN" tab
 - a. Click the Set up two-factor authentication for this user button.
 - b. Scan the displayed QR code with the TOTP app.
 - c. Generate the one-time password in the app and enter it in the DELTA LOGIC Connectivity Service.
 - d. Click Configure One-Time Password.

You have now set up two-factor authentication for this user and you will be asked for a one-time password each time you log in again.

4.6.5.2 Disabling two-factor authentication for the logged-in user

- You have logged on to the DELTA LOGIC Connectivity Service
- The two-factor authentication is active for the logged in user
- You have opened the "My VPN" tab
 - a. Click the Disable two-factor authentication for this user button.

You have now deactivated two-factor authentication for this user and will no longer be asked for a one-time password the next time you log in.



Note:

If two-factor authentication is deactivated for a user, it should also be deleted from the app. If it is activated again, it must be set up again in the app.

4.6.5.3 Renew two-factor authentication for the logged-in user

- You have logged on to the DELTA LOGIC Connectivity Service
- The two-factor authentication is active for the logged in user
- You have opened the "My VPN" tab
 - a. Click the Renew Two-Factor Authentication button.
 - b. Scan the displayed QR code with the TOTP app.
 - c. Generate the one-time password in the app and enter it in the DELTA LOGIC Connectivity Service.
 - d. Click Configure One-Time Password.

You have now renewed two-factor authentication for this user.

5 Configuration of the VPN participants

The configuration of the VPN participants depends on the respective device. Routers and fault monitors of DELTA LOGIC can be configured quick and easy for the DELTA LOGIC Connectivity Service using the startup wizard. Alternatively, it is possible to configure this manually. A configuration file and a container with all necessary certificates and keys can be downloaded from the DELTA LOGIC Connectivity Service for this.

Third-party devices like PCs, tablets or controls are configured manually. An Open-VPN configuration file and a container with all necessary certificates and keys can be downloaded from the DELTA LOGIC Connectivity Service for this.

5.1 Configuration of an icom OS router

A VPN router with icom OS can be configured either using the quick start wizard or manually.



Important Note:

The quick start to the DLCS only works with devices with newer firmware from icom OS 5.3

5.1.1 Configuration using the Quick Start Wizard

The quick start wizard in the web interface is used to quickly start up the router for the DELTA LOGIC Connectivity Service.

The router gets the entire VPN configuration from the DELTA LOGIC Connectivity Service. To do this, the router must first have been created as a device in the DELTA LOGIC Connectivity Service.

To put a router into operation with the quick start wizard for the DELTA LOGIC Connectivity Service, it is recommended to first reset it to the basic settings. Information on this can be found in the Quick Installation Guide as well as in the inline and online help of the router. Click the question mark in the header for inline help.

The customer's name and device code required here can be found on the "My VPN" tab.

The Quick Start Wizard configures the router. This then establishes a WAN connection and establishes a secure connection to the init server of the VPN service (the init server is accessed via UDP port 1194). Then the router gets the VPN configuration from the server and applies it. The local network of the router is configured according to the information that was set when creating the device in the DELTA LOGIC Connectivity Service. After completing the quick start wizard, the router appears with a slight delay in the DELTA LOGIC Connectivity Service with the status online.

5.1.2 Manual configuration

The manual configuration is useful when a router has already been configured and put into operation and is also to participate in the VPN service.

The configuration file, which can be downloaded in the DELTA LOGIC Connectivity Service on the "Devices" tab for the respective device using the "Download" button (arrow down) ("INSYS Router Configuration" link), contains all the configuration settings required for this. These can be loaded into the open profile in the router's web interface in the "Administration" menu on the "Profiles" page. However, a secure configuration for the DELTA LOGIC Connectivity Service is not yet guaranteed, as this depends on the router settings that have already been made. If, for example, more than one WAN chain or VPN tunnel has already been defined, this can lead to conflicts with the configuration file. Further manual post-processing of the configuration is then required. Refer to the router's inline and online help for instructions. Click the question mark in the header for inline help.

5.2 Configuration of an INSYS OS router

This section applies to VPN routers with INSYS OS. Again, the configuration can be done via the quick start wizard or manually.



Important Note:

The quick start to the DLCS only works with devices with newer firmware from INSYS OS 2.12.21.

5.2.1 Configuration using the Quick Start Wizard

The quick start wizard in the web interface is used to quickly start up the router for the DELTA LOGIC Connectivity Service. The router must have firmware from 2.12.21 for this.

The router gets the entire VPN configuration from the DELTA LOGIC Connectivity Service. To do this, the router must first have been created as a device in the DELTA LOGIC Connectivity Service.

To put a router into operation with the quick start assistant for the DELTA LOGIC Connectivity Service, it must first be reset to the basic settings. Information on this can be found in the Quick Installation Guide and in the user manual of the router. The quick start wizard is only displayed in the web interface when the router is started for the first time or after a factory reset.

The customer's name and device code required here can be found on the "My VPN" tab.

The Quick Start Wizard configures the router. This then establishes a WAN connection and establishes a secure connection to the init server of the VPN service (the init server is accessed via UDP port 1194). Then the router gets the VPN configuration from the server and applies it. The local network of the router is configured according to the information that was set when creating the device in the DELTA LOGIC Connectivity Service. After completing the quick start wizard, the router appears with a slight delay in the DELTA LOGIC Connectivity Service with the status online.



Please note that the router is already addressed via the new IP address, if such has been entered under "Accessible local IP address" when creating the device in the DELTA LOGIC Connectivity Service.

5.2.2 Manual configuration

The manual configuration is useful when a router has already been configured and put into operation and is also to participate in the VPN service.

The router must have firmware 2.4.0 or higher for this.

The configuration file, which can be downloaded in the DELTA LOGIC Connectivity Service on the "Devices" tab for the respective device using the "Download" button (arrow down) ("INSYS Router Configuration" link), contains all the configuration settings required for this. These can be loaded onto the router in the router's web interface in the "System" menu on the "Update" page. However, a secure configuration for the DELTA LOGIC Connectivity Service is not yet guaranteed, as this depends on the router settings that have already been made. For example, if it was previously configured as a VPN server, it may conflict with the configuration file. Further manual post-processing of the configuration is then required. Information on this can be found in the user manual for the router.



Please note that the router can already be reached via the new IP address after the restart if one was available when creating the device in the DELTA LOGIC Connectivity Service under "Accessible local IP-Adress".

5.3 Configuration of a PC/third-party device

If you have created a third-party device (PC, controller, etc.) in the DELTA LOGIC Connectivity Service, you can download the configuration for the VPN network from the DELTA LOGIC Connectivity Service. If possible, the current OpenVPN version from the following page should be installed on the third-party device <https://openvpn.net/community-downloads/> must be installed.

The configuration file that can be downloaded in the DELTA LOGIC Connectivity Service on the "Devices" tab for the respective device using the "Download" button (down arrow) contains the OpenVPN configuration settings.

The OpenVPN configuration file must be stored in the "Config" directory of the OpenVPN installation (e.g., Windows: C:\Programs\OpenVPN\config).

With this you can start the OpenVPN GUI and connect to the VPN.



Note:

Under Windows and older OpenVPN versions, the GUI must be started as an administrator, otherwise the routes will not be set. The PC appears as "online" in the DELTA LOGIC Connectivity Service but cannot communicate.

The VPN connection can be checked, for example, by "pinging" the IP address of a VPN participant from the third-party device or by entering it in a browser (e.g., to access its web interface).

6 VPN Activity Log

The DELTA LOGIC Connectivity Service logs various activities in the portal, such as logging on and off of users or adding and deleting devices.

A click on the "Activity Log" tab opens the new portal of the DELTA LOGIC Connectivity Service. All operations regarding the DELTA LOGIC Connectivity Service are shown there in the "Activities" menu. Refer to the online help for further information.

7 User management

User administration is also available for the DELTA LOGIC Connectivity Service Portal.

The "Users" tab shows all users assigned to this account. Additional users with different rights can be created.

7.1.1 Creating a user

When creating a user, different user roles with different rights are available:

- **Account Admin:** Has all rights including user administration. An account administrator can be designated as a contact person. He then receives the system messages by e-mail. Existing users are classified as account administrators. The user to whom the account was registered will be used as the contact person.
- **Read only:** Can view all list views in the menus and download the device list and VPN log files, but cannot make any settings or download certificates or configurations.

Configuration ("Users" tab, "Add user" button)

With the **role**, you choose which rights the newly created user should have.

The **Form of address** determines whether the user is addressed as Mr. or Ms. in automatically generated e-mails.

Surname and **first name** are also used in correspondence.

E-mail defines the e-mail address used for correspondence with the user.

The newly created user can log in to the DELTA LOGIC Connectivity Service with the **username** and **password**. It is recommended that a new user changes their password to a password known only to them after the first login.

Save your settings by clicking "OK".

7.1.2 Managing users

The "Users" tab shows a list of the created users. Here the users can be managed and adjusted.

Configuration ("Devices" tab)

Another user can be added with the **Add new user** button.

A list of the created users can be downloaded with the **Download user list** button.

The data of this user can be edited with the button **Manage**.

Two-factor authentication can also be enforced for this user here.

This user can be deleted with the **Delete** button.

The contact person for this account can be specified in the **Contact person** column. Users who only have read rights cannot be specified as contact persons. Users who are set as contacts cannot be deleted.

The user role assigned to this user is displayed in the **Role** column.

The salutation configured for this user is displayed in the **Salutation** column.

The last name configured for this user is displayed in the **Last Name** column.

The first name configured for this user is displayed in the **First Name** column.

The email address configured for this user is displayed in the **Contact email** column. All correspondence with this user will be sent to this address.

The username configured for this user is displayed in the **Username** column.

The column **Created by** shows which user created this user.

The **Created-on** column shows when this user was created.

The **Last Password Change** column shows when this user's password was last changed.

The **2FA Required** column shows whether two-factor authentication is enforced for this user.

7.1.3 Enforce two-factor authentication for a user

Two-factor authentication adds another level of security to username and password login by requiring the additional entry of a one-time password. The password is generated using the TOTP (Time-based One-time Password) process with the help of an app on a separate device (e.g., smartphone). To do this, the user account of the DELTA LOGIC Connectivity Service must be registered once in the app. TOTP is an open standard and a variety of apps are available for different platforms such as the open-source software FreeOTP (<https://freeotp.github.io/>). Since the one-time passwords are generated based on time and are only valid for a limited time, it is necessary for the time on the separate device to be accurate and synchronized regularly.

A user with administrator rights can enforce two-factor authentication for each set up user. This setting takes precedence over setting up two-factor authentication for a logged-in user on the "My VPN Hub" tab.

Configuration ("Users" tab, "Manage" button)

Enabling **Require two-factor authentication** will enforce two-factor authentication for that user. The next time that user logs in, a QR code will appear that the user must scan with the TOTP app to set it up for two-factor authentication.

7.1.4 Downloading the User List

The "Users" tab shows a list of the created users. This list can be downloaded as a CSV file. The CSV file contains the columns analogous to the user list, separated by an "=" (equals sign).

Configuration ("Users" tab, "Download customer list" button)

Clicking on **Download customer list** downloads the user list in the download window.