USER MANUAL

Netbiter® Remote Access

Doc ID: HMSI-27-240
Version: 2.1

HALMSTAD • CHICAGO • KARLSRUHE • TOKYO • BEIJING • MILANO • MULHOUSE • COVENTRY • PUNE • COPENHAGEN • RAVENSBURG

HMS Industrial Networks
Mailing address: Box 4126, 300 04 Halmstad, Sweden
Visiting address: Stationsgatan 37, Halmstad, Sweden

E-mail: info@hms-networks.com
Web: www.netbiter.com

Important User Information

Liability

Every care has been taken in the preparation of this document. Please inform HMS Industrial Networks AB of any inaccuracies or omissions. The data and illustrations found in this document are not binding. We, HMS Industrial Networks AB, reserve the right to modify our products in line with our policy of continuous product development. The information in this document is subject to change without notice and should not be considered as a commitment by HMS Industrial Networks AB. HMS Industrial Networks AB assumes no responsibility for any errors that may appear in this document.

There are many applications of this product. Those responsible for the use of this device must ensure that all the necessary steps have been taken to verify that the applications meet all performance and safety requirements including any applicable laws, regulations, codes, and standards.

HMS Industrial Networks AB will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features, timing, or functional side effects found outside the documented scope of this product. The effects caused by any direct or indirect use of such aspects of the product are undefined, and may include e.g. compatibility issues and stability issues.

The examples and illustrations in this document are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular implementation, HMS Industrial Networks AB cannot assume responsibility for actual use based on these examples and illustrations.

Intellectual Property Rights

HMS Industrial Networks AB has intellectual property rights relating to technology embodied in the product described in this document. These intellectual property rights may include patents and pending patent applications in the USA and other countries.

Trademark Acknowledgements

Netbiter® is a registered trademark of HMS Industrial Networks AB. Java is a registered trademark of Oracle and/or its affiliates. All other trademarks are the property of their respective holders.

Netbiter® Remote Access User Manual
Doc ID: HMSI-27-240 Version: 2.1

Table of Contents

Page

This page intentionally left blank

1 Preface

1.1 About This Document

This document describes installation and configuration of the Netbiter Remote Access service. It does not describe how to physically install a Netbiter EasyConnect gateway or how to set up an account in Netbiter Argos, which is described in the documentation for these products.

For additional related documentation and file downloads, please visit the Netbiter support website at www.netbiter.com/support.

1.2 Related Documents

Related documents

Document	Author
Netbiter Argos Administration Manual	HMS
Netbiter EasyConnect Gateway Installation Guides	HMS
Netbiter EasyConnect User Manual	HMS

1.3 Document history

Summary of recent changes (version 2.00 to 2.10)

Change	Where (section)
Added preparations	*2.3*
Added proxy information	*2.3*, *4.1*
Added IP address range restrictions	*3.3*
Major rewrite of QuickConnect section + updated all screenshots	*4*

Revision list

Version	Date	Author	Description
1.00	March 2014	SDa	Initial release
1.10	Aug. 2014	SDa	Update for Netbiter Services
1.20	Nov. 2014	SDa	Updates for proxy server support, Netbiter Services. Added info on signal strength LED indication.
2.0	Aug. 2015	ThN	Major update
2.1	Dec. 2015	ThN	Update for December 2015 Remote Access release

1.4 Conventions

Unordered (bulleted) lists are used for:

- Itemized information
- Instructions that can be carried out in any order

Ordered (numbered or alphabetized) lists are used for instructions that must be carried out in sequence:

1. First do this,
2. Then open this dialog, and
   a. set this option...
   b. ...and then this one.

Bold typeface indicates interactive parts such as connectors and switches on the hardware, or menus and buttons in a graphical user interface.

```
Monospaced text is used to indicate program code and other
kinds of data input/output such as configuration scripts.
```

This is a cross-reference within this document: *Conventions, p. 4*

This is an external link (URL): www.hms-networks.com

This is additional information which may facilitate installation and/or operation.

This instruction must be followed to avoid a risk of reduced functionality and/or damage to the equipment, or to avoid a network security risk.

Caution
This instruction must be followed to avoid a risk of personal injury.

WARNING
This instruction must be followed to avoid a risk of death or serious injury.

2 Overview

2.1 General Description

Netbiter Remote Access provides a remote connection via Netbiter Argos to the serial and Ethernet ports on a Netbiter EC300 series gateway. This makes it possible to use personal computer software to remotely interact with industrial devices, just as if they were connected locally to the computer.

To establish the remote connection, a driver called *QuickConnect* is installed on the local computer. QuickConnect creates a secure “tunnel” via Netbiter Argos between the Netbiter gateway and the software application on the computer. A browser-based graphical user interface is used for configuration.

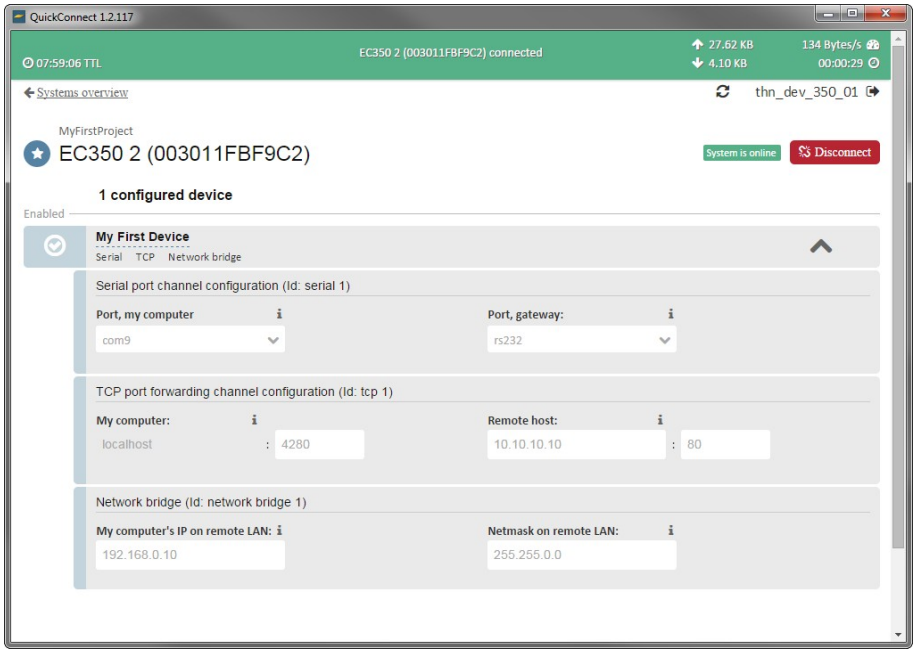

Fig. 1 The QuickConnect interface

Each tunnel can contain up to 50 individual “channels” for the actual connections to the remote devices. Three types of channel are supported:

Serial port channel	Creates a virtual serial port which is mapped to the RS-232 or RS-485 port on the Netbiter gateway.
Network bridge	Enables a remote connection to the Ethernet LAN port of the Netbiter gateway, allowing access to any device on the remote network.
TCP/UDP port forwarding	Maps the channel to a specific remote IP address and port for TCP/UDP messaging.

*Netbiter Remote Access is designed for connections that are open only for a limited time (8 hours maximum) while the user performs the required tasks. Permanent connections, for example between a SCADA application and equipment in the field, are **not** supported.*

2.2 Supported Equipment

Netbiter Remote Access can remotely connect with almost any industrial application with a serial or Ethernet port, and the list of tested and verified applications is constantly being revised and amended.

Please visit www.netbiter.com for up-to-date information about supported applications.

2.3 Requirements

Using the Netbiter Remote Access function requires:

- A Netbiter EC300 series gateway
- An active Netbiter Argos account
- The Netbiter QuickConnect driver installed on your computer
- General knowledge of TCP/IP networks
- Specific knowledge of the remote network setup

2.4 Preparations

Drawing a diagram of your network environment and making notes of local restrictions and features will help you when setting up Remote Access. Make sure that you have at least the following information about the local and remote networks:

- Network addressing mode (DHCP or static IP)
- IP address ranges, netmasks, and default gateways (if not using DHCP)
- Firewall restrictions and policies

> **!** *The described software should only be installed in a network that is protected by a firewall. Contact your network administrator if in doubt.*

2.5 Proxy Support

If the computer is connecting to the Internet via a proxy, you will be asked to enter proxy information before you can log in to QuickConnect. The system-wide proxy settings in Windows should normally be used.

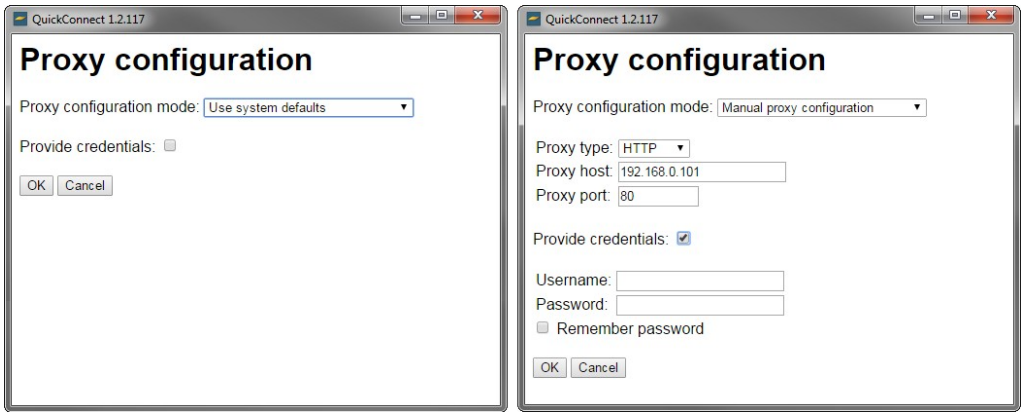

Fig. 2 Proxy configuration

QuickConnect currently supports the following proxy types:

Proxy type	Authentication
HTTP	none, basic, digest, NTLM
SOCKSv5	none

- If a HTTP proxy requires authentication you will be asked to provide user credentials twice on the first login attempt.
- Passwords used for proxy authentication must not contain spaces or special characters.
- If NTLM credentials are requested the username may need to be prefixed with the Windows domain (in the format *domain\username*), depending on how the proxy and computer are configured.
- If a Network Bridge configuration is used, a proxy exception for the corresponding network should be added to the system proxy configuration.

2.6 Installation overview

Setting up Netbiter Remote Access includes the following basic steps:

1. Installing a Netbiter EC300-series gateway at the location of the remote device
2. Activating the Netbiter gateway in a Netbiter Argos account
3. Configurating Remote Access functionality in Netbiter Argos
4. Installing QuickConnect on the local computer to use for Remote Access
5. Configurating one or more remote access channels to the device to be accessed
6. Initiation/opening of the connection to the remote device

This document does not describe how to physically install a Netbiter EasyConnect gateway or how to set up an account in Netbiter Argos. Please refer to the documentation available at the Netbiter support website, www.netbiter.com/support.

2.7 Connection Examples

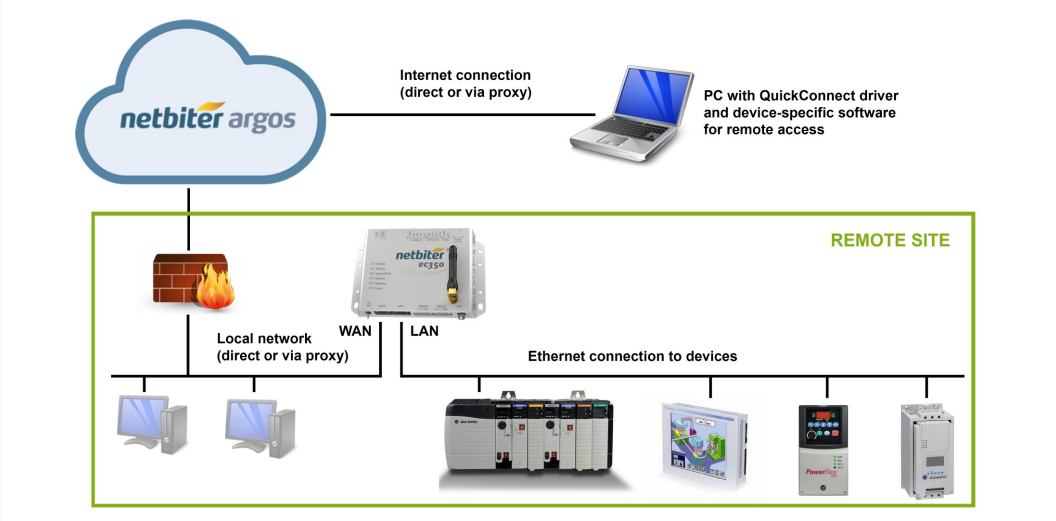

Fig. 3 WAN link to Ethernet LAN

Remote access to an Ethernet-based control network via a LAN network at the remote site, using an Ethernet-based connection over the Internet.

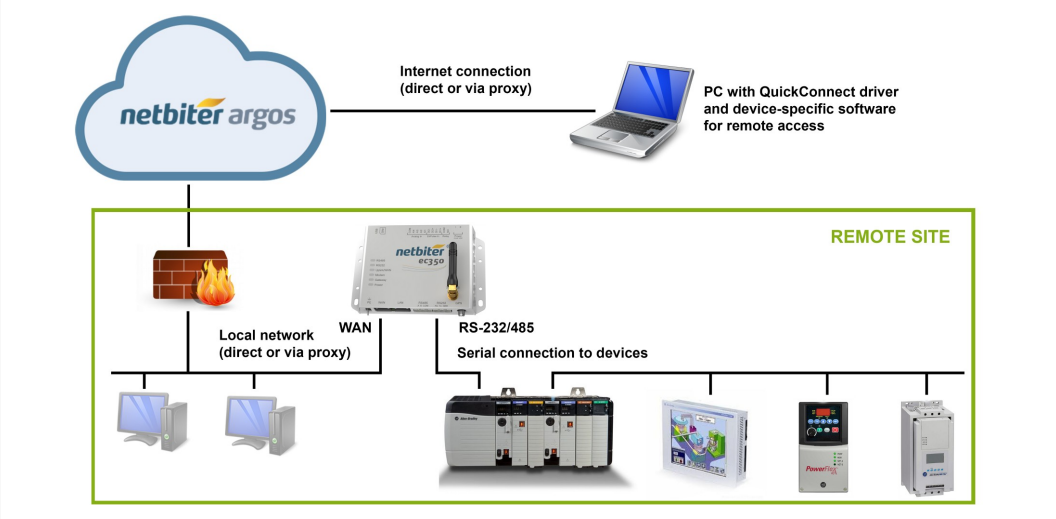

Fig. 4 WAN link to serial

Remote access to a serial control network via a LAN network at the remote site, using an Ethernet-based connection over the Internet.

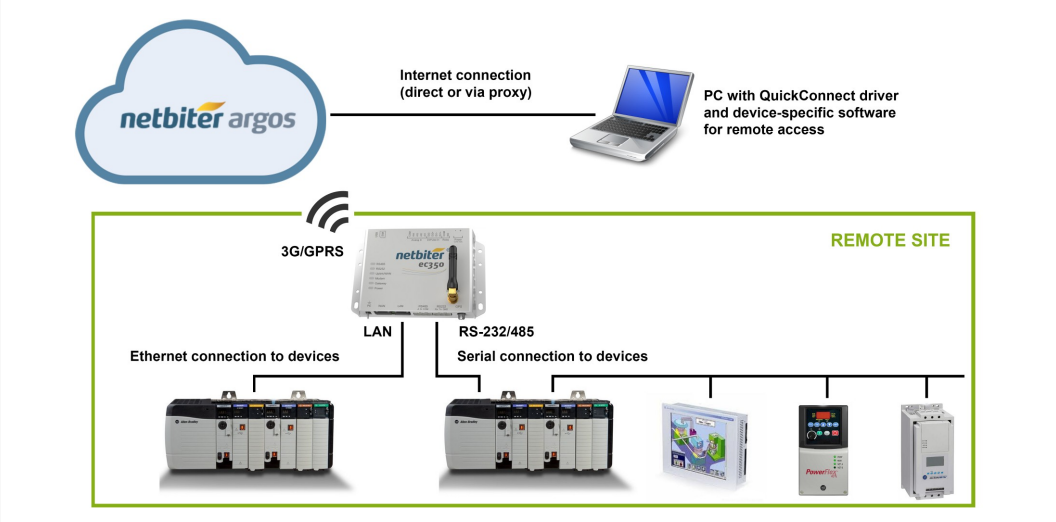

Fig. 5 Mobile link to serial and Ethernet

Remote access to both serial and Ethernet-based device networks using Netbiter Argos over a mobile connection (EC350 only).

3 Configuring Remote Access in Netbiter Argos

The following procedure requires a Netbiter EC300 series gateway activated in Netbiter Argos.

3.1 Activating Remote Access Mode

On the **Management** page, select **Configuration** (in *Manage and Analyze* accounts you also have to select a system) and enable **Use this system for remote access**.

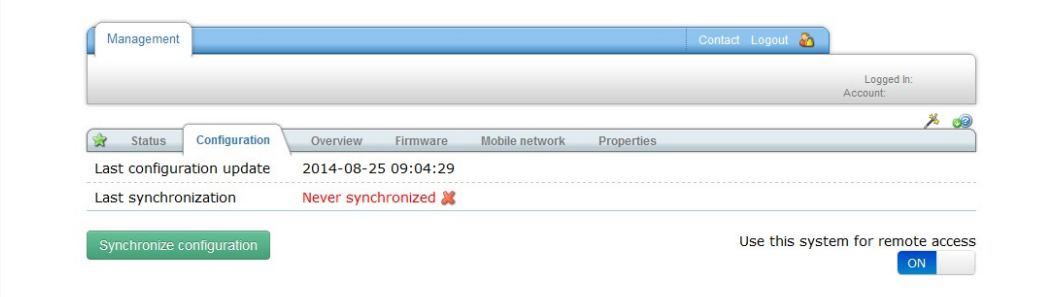

Fig. 6 Enabling Remote Access

The Configuration page will now only contain one tab, **Gateway settings**, which contains settings for the Remote Access service and for LAN configuration.

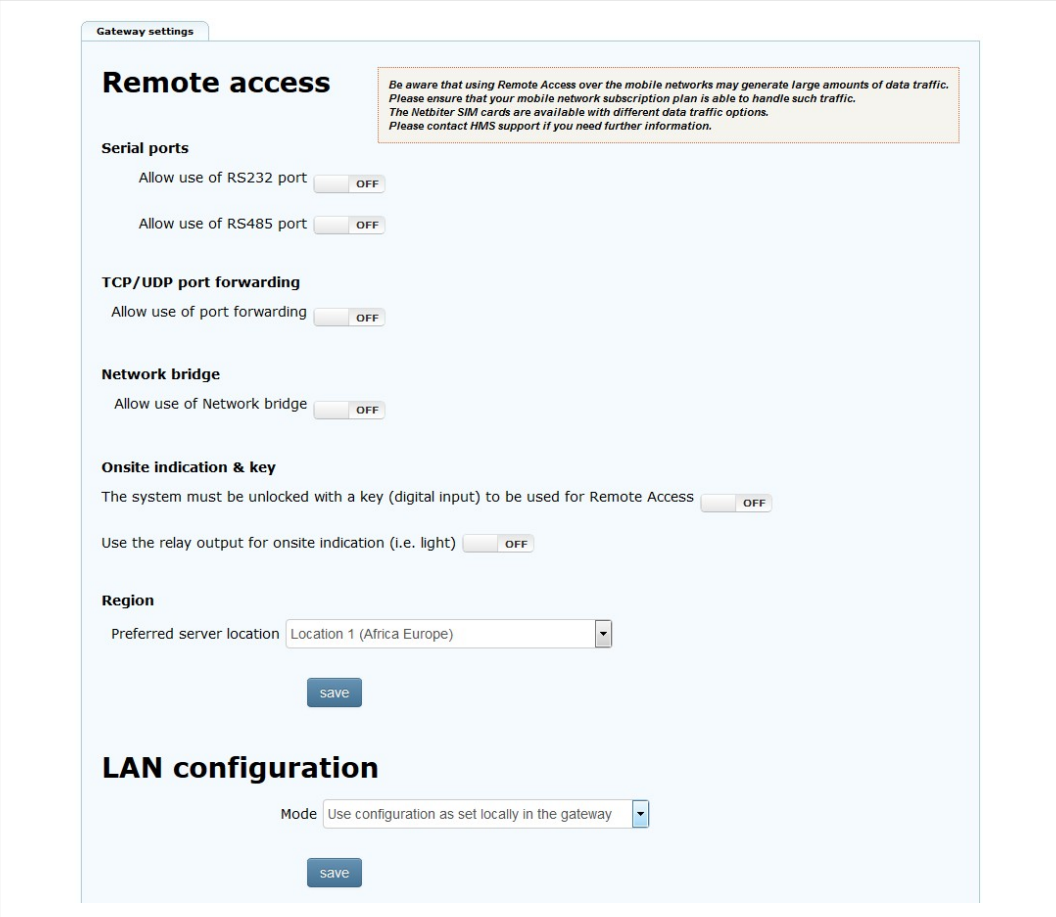

Fig. 7 Gateway settings tab

3.2 Remote Access Settings

After changing these settings, click on **Save** to apply the changes.

3.2.1 Serial Ports

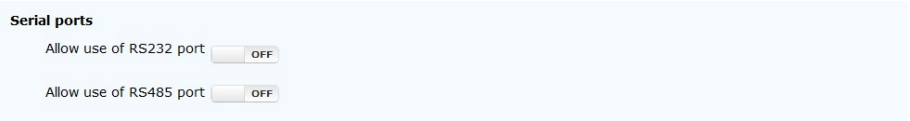

Fig. 8 Selecting serial ports

Enables/disables the required serial ports on the Netbiter EasyConnect gateway.

3.2.2 TCP/UDP Port Forwarding

Fig. 9 TCP/UDP port forwarding mode

Sets up a “whitelist” that restricts which IP addresses, ports and protocols (TCP, UDP, or both) are allowed for accessing remote devices. Wildcards (*) can be used.

Click on **Add new entry** to add to the list. To delete an entry, click on **remove**.

3.2.3 Network Bridge

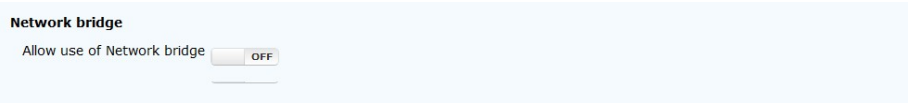

Fig. 10 Network bridge mode

If the remote device has no support for access via a specified network (TCP/UDP) port, the remote network can be set to bridged mode. This will enable a channel functioning as a VPN connection, meaning that the client accessing the device will have secure access to the entire network on the remote side.

> **!** *Enabling the Network Bridge setting will allow access to all IP addresses and ports on the remote network.*

3.2.4 Onsite Indication & Key

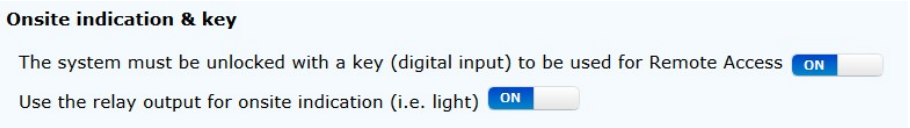

Fig. 11 Onsite indication & key

For greater physical security it is possible to locally enable/disable Remote Access directly from the hardware, and also to visually indicate whether the function is currently in use.

The operator of a machine could for example temporarily allow maintenance personnel to use Remote Access. The operator will be notified when the technician is connected. When maintenance has completed, the operator can disable Remote Access again.

Key

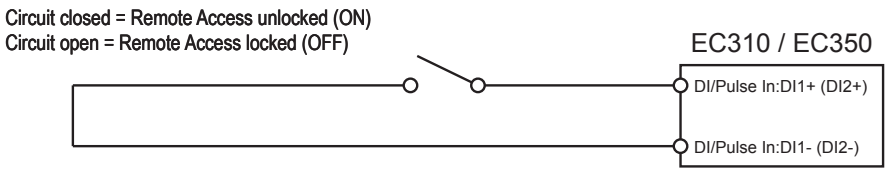

Fig. 12 Wiring diagram - digital input

Set **The system must be unlocked...** to **ON** and connect a switch or relay to the digital input on the Netbiter gateway as shown in the diagram.

Onsite Indication

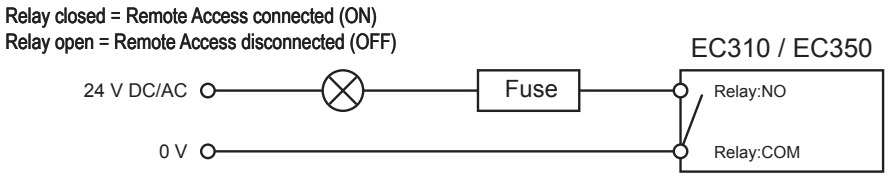

Fig. 13 Wiring diagram - relay output

Set **Use the relay output...** to **ON** and connect a lamp or other indication device to the relay output on the Netbiter gateway as shown in the diagram.

3.2.5 Region

This will be the tunnel server used for secure communication. To minimize latency, select a server location closest to where the Netbiter gateway is located.[1]

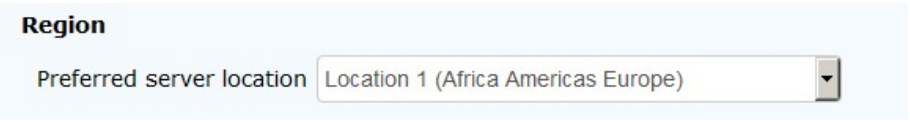

Fig. 14 Server location setting

1. When using a mobile connection, the optimal location can also depend on the country origin of the SIM card in combination with the location of the Netbiter gateway.

3.3 LAN Configuration

These settings affect the **LAN** port on the Netbiter EasyConnect gateway, which is the port used for connecting to the Ethernet network on the remote side of the tunnel.

Fig. 15 LAN configuration

Use configuration as set locally in the gateway	The LAN port will use the configuration set in the gateway. See the ***Netbiter EasyConnect User Manual***.
LAN interface not in use	Disables the LAN port.
Get IP address automatically from a DHCP server	Use a DHCP server on the remote network.
Manually set a fixed IP address and netmask	Set a static IP address and netmask.

To avoid potential address conflicts when setting a static IP address and netmask for the LAN port, use only the address spaces reserved for private networks:

- 10.0.0.1 – 10.255.255.254
- 172.16.0.1 – 172.31.255.254
- 192.168.0.1 – 192.168.255.254

After changing the settings, click on **Save** to apply the changes.

3.4 Synchronizing

The final step to perform is to *synchronize* the configuration — to upload the changes made in Netbiter Argos to the Netbiter EasyConnect gateway.

Save all settings, then click on **Synchronize configuration** to start the synchronization. The system may be shown as offline until synchronization has completed.

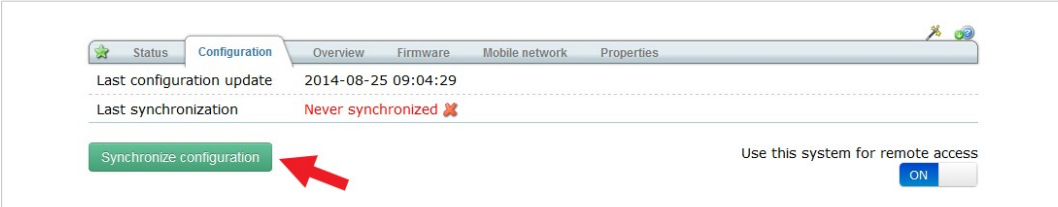

Fig. 16 Synchronizing the configuration

3.5 Configuring Users (Manage and Analyze)

Netbiter Argos *Manage and Analyze* accounts can have multiple users with different levels of access. To be able to use the Remote Access function, users must have this access level explicitly granted for each project by the administrator.

See the ***Netbiter Argos Administration Manual*** on how to manage user rights.

4 QuickConnect

4.1 Installing QuickConnect

QuickConnect is a driver and configuration tool required for a computer to be used for the Netbiter Argos Remote Access service.

QuickConnect can be downloaded from the Netbiter support website www.netbiter.com/support and also directly from within Netbiter Argos.

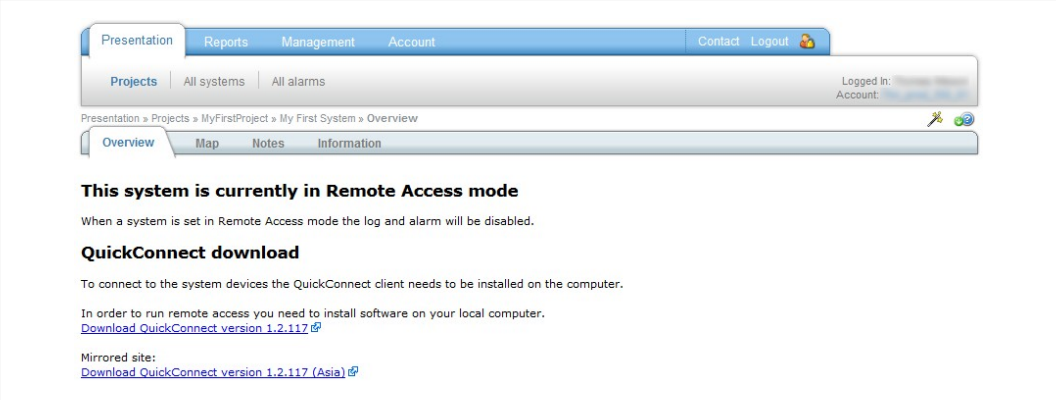

Fig. 17 QuickConnect download links

Save the file to the computer and unzip the contents to your desktop, then double-click on the executable file and follow the on-screen instructions to install QuickConnect.

The QuickConnect installer will also install 3 additional software components: *OpenVPN*, *Serial IP* and *Windows TAP*. These components do not need to be opened or run manually and normally do not require configuration.

You may have to restart your computer to complete the installation.

4.2 Starting QuickConnect

Start the configuration program from the shortcut in the start menu or on your desktop and log in using your Netbiter Argos username and password.

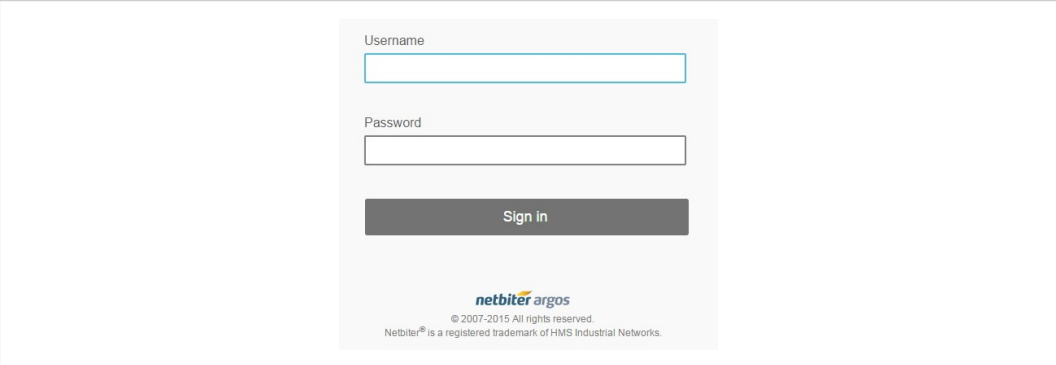

Fig. 18 QuickConnect login window

4.2.1 Proxy Support

If the computer is connecting to the Internet via a proxy, you will be asked to enter proxy information before you can log in to QuickConnect. The system-wide proxy settings in Windows should normally be used.

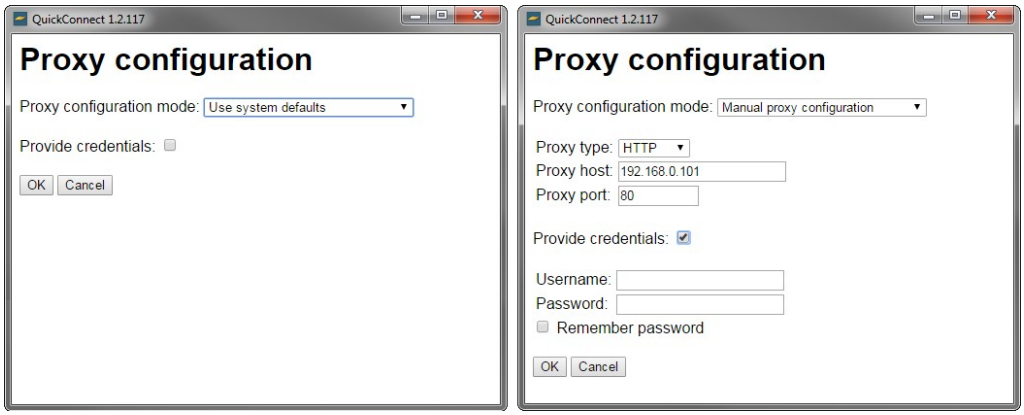

Fig. 19 Proxy configuration

QuickConnect currently supports the following proxy types:

Proxy type	Authentication
HTTP	none, basic, digest, NTLM
SOCKSv5	none

- If a HTTP proxy requires authentication you will be asked to provide user credentials twice on the first login attempt.
- Passwords used for proxy authentication must not contain spaces or special characters.
- If NTLM credentials are requested the username may need to be prefixed with the Windows domain (in the format *domain\username*), depending on how the proxy and computer are configured.
- If a Network Bridge configuration is used, a proxy exception for the corresponding network should be added to the system proxy configuration.

4.3 Configuring a System for Remote Access

4.3.1 Systems Overview

After logging in to QuickConnect the **Systems overview** page will be displayed, listing all the available systems for the account.

Fig. 20 QuickConnect Systems overview

Clicking on a system will open its configuration page. (If the system has an active connection the settings cannot be edited and will be greyed out.)

Field systems marked as **Favorites** will be listed at the top. To mark/unmark a system as a favorite, click on the star icon ☆ .

If the system administrator has made changes to the configuration while you are logged in, you may need to reload the page by clicking on the refresh icon ↻.

4.3.2 Adding a New Device

1. Click on a system to open its configuration page then click on **Add device**. A list of predefined device configurations will be displayed.

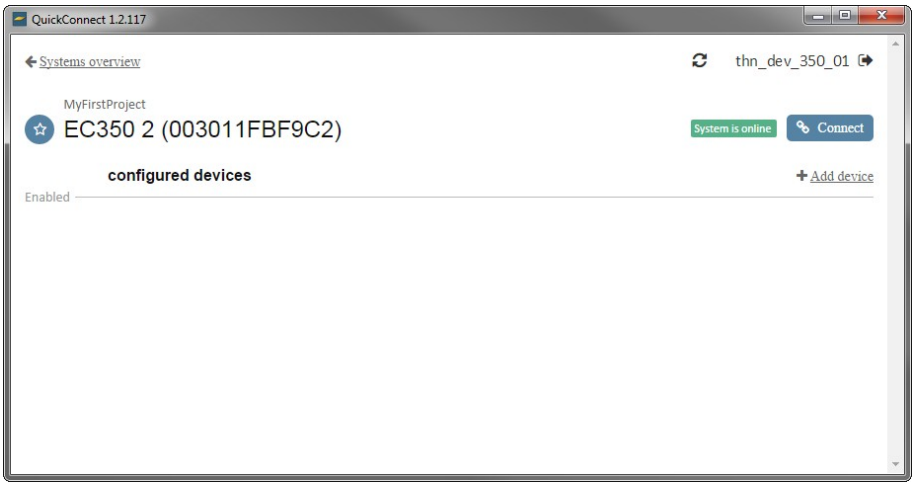

Fig. 21 System configuration page (with no configured devices)

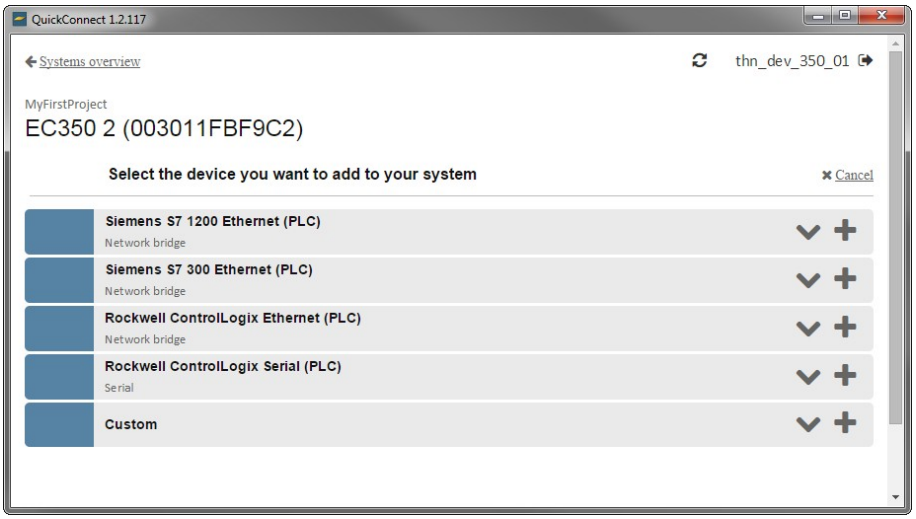

Fig. 22 Device list

2. Click on the plus icon ➕ to start configuring a connection based on the associated preconfigured device. If the device to be used is not in the list, select **Custom**.

4.3.3 Renaming a Device

Devices can be renamed for easier identification. To edit the name of a device, just click on the name and start typing.

> ℹ *Adding the IP address or port to the device name can be helpful when you have multiple devices in the same tunnel. This will not affect the actual IP address or port settings for the device.*

4.3.4 Adding Channels

A new device will have an initial (unconfigured) channel configuration based on the predefined device. You can add multiple channels of any type to a device.

The channels will get an individual ID based on their type and the order they were added to the device, e.g. serial 1, serial 2, network bridge 1, etc. The IDs are also used in error messages.

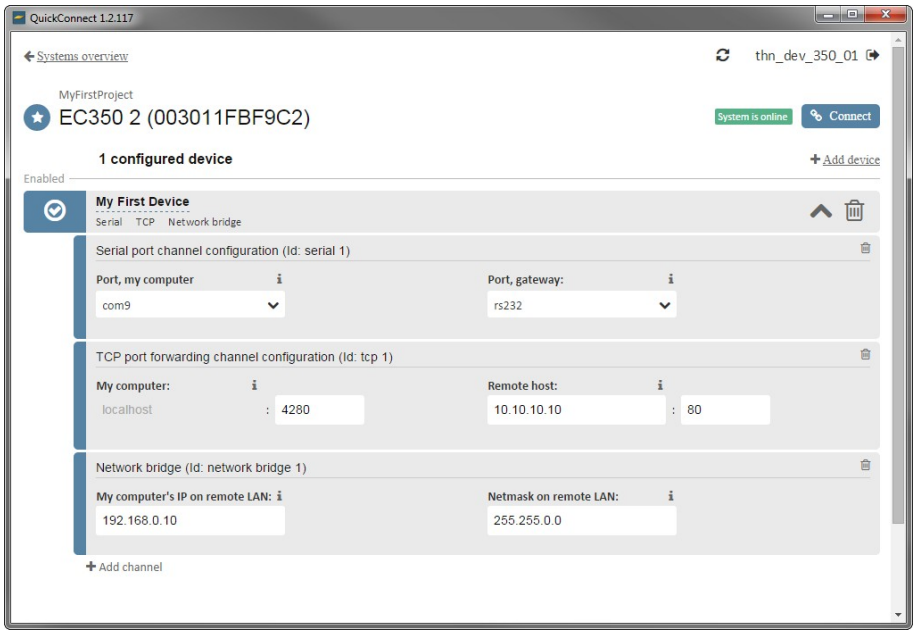

Fig. 23 One TCP port forwarding channel and two serial channels in the same tunnel

Adding a Serial Channel

A serial channel configuration connects a virtual serial port on the computer (COM port) with a physical serial port (RS-232 or RS-485) on a Netbiter EasyConnect gateway. The serial ports to use must also be enabled in Netbiter Argos. See *Remote Access Settings, p. 11*.

1. Click on **Add channel** and select **Serial**.
2. Select a free virtual serial port on your computer.
3. Select a physical serial port on the Netbiter gateway.

Fig. 24 Serial channel configuration

Adding a Network Bridge

A Network Bridge configuration creates a virtual private network (VPN) which will have access to the remote network. A virtual network adapter (Windows-TAP) is created automatically for this purpose when you install QuickConnect.

Network Bridge must also be enabled in Netbiter Argos. See *Remote Access Settings, p. 11*.

1. Click on **Add channel** and select **Network bridge**.
2. Enter the IP address and subnet mask to assign to the virtual network adapter on the remote network.

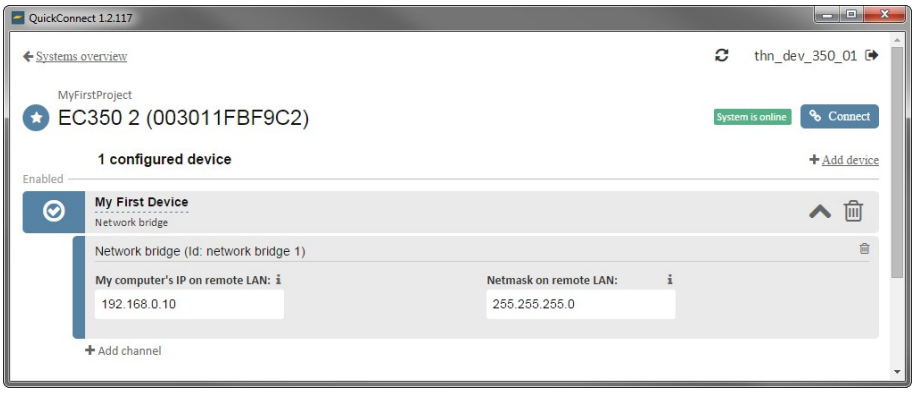

Fig. 25 Network bridge configuration

> ! *Check that the IP addresses are valid and not already in use, and that you have entered the correct subnet mask. Contact your network administrator if in doubt.*

Adding TCP/UDP Port Forwarding

Port forwarding allows you to specify an IP address, network protocol and remote port to connect to. Which IP addresses and ports are allowed must first be specified in the “whitelist” in Netbiter Argos. See *Remote Access Settings, p. 11*.

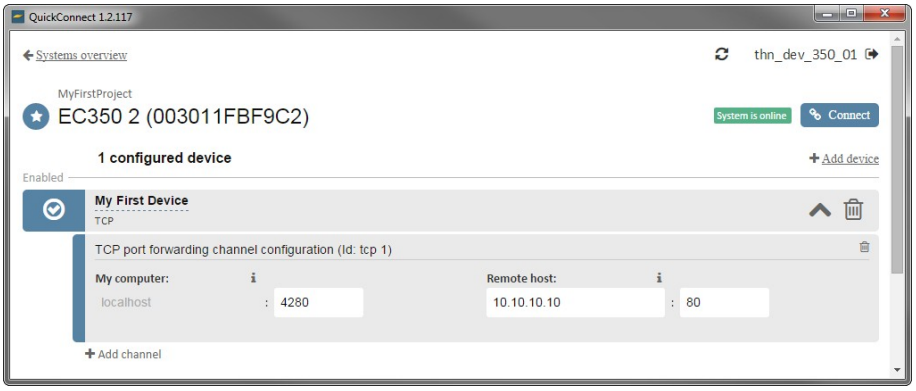

Fig. 26 TCP/UDP port forwarding

1. Click on **Add channel** and select **TCP** or **UDP**.
2. Enter the TCP or UDP port number to use on the local computer (localhost), and the port number and IP address to use on the remote device.

4.4 Connecting to a Remote Device

When the configuration is complete in QuickConnect as well as in Netbiter Argos, click on **Connect** to open the tunnel to the remote device.

When the connection has been established the elapsed time (TTL) and the amount of data traffic up/down will be displayed in the green bar at the top of the client window.

The configurations cannot be modified while the tunnel connection is open. To close the connection. click on **Disconnect**.

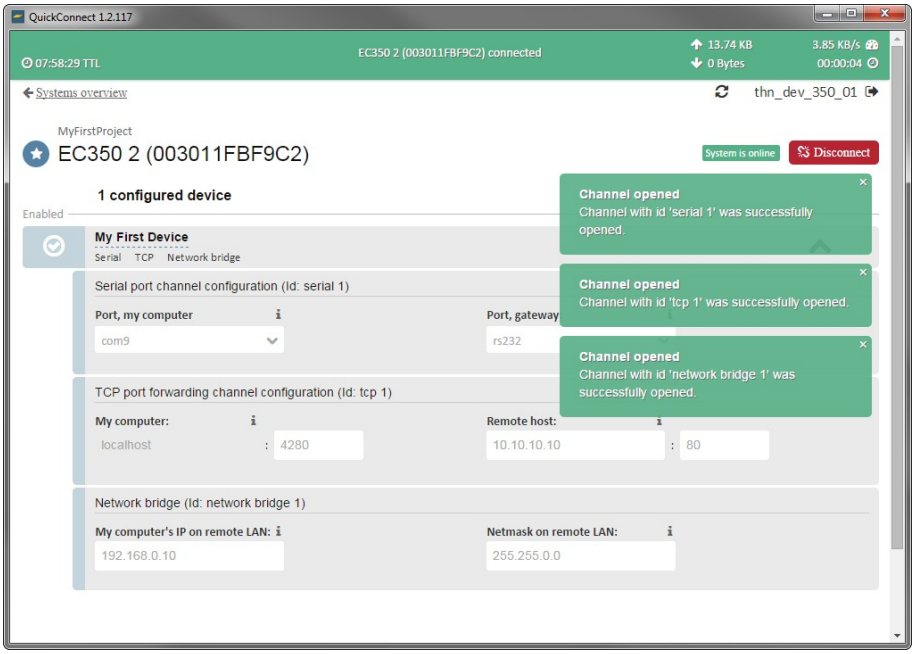

Fig. 27 System connected

For information on how to remotely control a device, see the manufacturer's documentation for the specific software tools.

4.5 Logging Out and Exiting QuickConnect

The QuickConnect application and the communication tunnels can be exited or terminated manually or automatically in a number of ways:

- Closing the QuickConnect window will minimize the application to the system tray and logout the user. Any open tunnels will stay open.
- Clicking on the “logout” icon will logout the user and close all open tunnels.
- Clicking on **Disconnect** will close the currently displayed tunnel connection.
- Opening a new communication tunnel to a system will automatically close any existing tunnel to that system.
- Right-clicking on the QuickConnect icon in the Windows system tray and selecting **Exit** will terminate the application and close any open tunnels.

Timeout

- An open tunnel will automatically close after 8 hours. All ongoing communication will be terminated.
- After 60 minutes of inactivity, the user will be automatically logged out. Any open tunnels will stay open for a maximum of 8 hours.