Application Note

Functions of the Integrated WebServer

Hilscher Gesellschaft für Systemautomation mbH
www.hilscher.com

DOC091203AN06EN | Revision 6 | English | 2017-09 | Released | Public

Table of contents

1 Introduction

1.1 About this document

1.1.1 Description of the contents

This document describes the HTTP functions of the WebServer, which is integrated in the firmware of several communication modules with flash memory for Real-Time Ethernet networks by Hilscher.
Here you can learn how to call up functional web pages with your browser, e. g. in order to update a firmware.
This document also provides information on how to add your own content to the WebServer.

Please note that the description of the WebServer in netIC DIL-32 Communication IC Devices is not part of this document. The WebServer functions in netIC devices are described in the Application Note *Functions of the Integrated WebServer in netIC DIL-32 Communication IC Devices*, DOC140201ANxxEN.

1.1.2 List of revisions

Index	Date	Revision
1	2009-12-21	Document created
2	2010-07-19	Document completely revised
3	2012-02-06	Document completely revised
4	2012-02-28	Section *Examples for adding own content* [▷ page 24] added
5	2013-10-15	Section *Devices and firmware with integrated WebServer* [▷ page 6] updated.
6	2017-09-19	Structure and layout of document revised. netRAPID **NRP 51-RE** in section *Devices and firmware with integrated WebServer* [▷ page 6] added. *netHOST Device Test Application* added as download tool. Chapter *Uploading WebServer content to netRAPID* [▷ page 29] added.

Table 1: List of revisions

1.1.3 Abbreviations

Abbreviation	Description
HTTP	Hypertext Transfer Protocol
TCP	Transmission Control Protocol
IP	Internet Protocol
SSI	Server Side Includes
iframe	Inline Frame

Table 2: Abbreviations

1.1.4 Conventions in this document

Notes, operation instructions and results of operation steps are marked as follows:

Notes

Note:
<important note>

Note:
<simple note>

<note, where to find further information>

Operation instructions

1. <operational step>
   - ➢ <instruction>
   - ➢ <instruction>
2. <operational step>
   - ➢ <instruction>
   - ➢ <instruction>

Results

<intermediate result>

<final result>

1.2 Description WebServer

The WebServer, integrated in the firmware of Hilscher communication modules for Real-Time Ethernet systems, allows you to read device parameters, to update firmware and to reset the device by HTTP commands. Thus, you can use a standard web browser and the Ethernet interface of the device to perform these tasks.

You can also upload your own web pages and graphics (e. g. your company logo) to the WebServer and thus customize the pages hosted by the WebServer. This does not affect the HTTP functions of the WebServer.

The WebServer also supports user and password administration with MD5 coding. A configuration file (`security.cfg`) which contains the definitions of users, groups and passwords can be uploaded to the WebServer by using the Hilscher *cifX Test Application* or the *netHOST Device Test Application*.

Note:
The **comX**, **netIC** and **netJACK** communication modules are delivered with pre-loaded WebServer content (Security.cfg, HTML pages, graphics, style sheets etc.), which means that you can open the WebServer pages of these modules immediately after having commissioned them.
The **netRAPID NRP 51-RE** module, in contrast to the above mentioned modules, is shipped with its WebServer content not yet installed – which means that you have to download these WebServer files to the netRAPID after having commissioned the netRAPID (i.e. after having downloaded its firmware and device configuration).
So, if you are a user of the netRAPID, please read the instructions in the *Uploading WebServer content to netRAPID* [page 29] chapter first.

1.3 Devices and firmware with integrated WebServer

The WebServer is available in Hilscher devices for Real-Time Ethernet systems running on the following firmware versions:

Product line	Device type name	Protocol	Firmware	Supported since firmware version
comX	COMX 100CA-RE COMX 100CN-RE	EtherNet/IP Scanner	comXeim.nxf	2.4.9.2
		EtherNet/IP Adapter	comXeis.nxf	2.5.16.3
		Open Modbus/TCP	comXomb.nxf	2.5.4.0
		PROFINET IO Device	comXpns.nxf	3.4.33.0
		Sercos Slave	comXs3s.nxf	3.0.8.0
	COMX 51CA-RE COMX 51CN-RE	EtherNet/IP Adapter	M060H000.nxf	2.7.12.0
		Open Modbus/TCP	M060L000.nxf	2.5.10.0
		PROFINET IO Device	cx51pns.nxf	3.5.22.0
		Sercos Slave	M060J000.nxf	3.1.18.0
netIC	See Application Note *Functions of the Integrated WebServer in netIC DIL-32 Communication IC Devices*, DOC140201ANxxEN			
netJACK	NJ 50D-RE	EtherNet/IP Adapter	J030H000.nxf	2.5.16.3
		Open Modbus/TCP	J030L000.nxf	2.5.4.0
		PROFINET IO Device	J030D000.nxf	3.4.33.0
		Sercos Slave	J030J000.nxf	3.0.32.0
	NJ 51D-RE	EtherNet/IP Adapter	J060H000.nxf	2.7.12.0
		Open Modbus/TCP	J060L000.nxf	2.5.10.0
		PROFINET IO Device	J060D000.nxf	3.5.22.0
		Sercos Slave	J060J000.nxf	3.1.18.0
	NJ 100EN-RE NJ 100DN-RE	EtherNet/IP Scanner	J020G000.nxf	2.4.9.2
		EtherNet/IP Adapter	J020H000.nxf	2.5.16.3
		Open Modbus/TCP	J020L000.nxf	2.5.4.0
		PROFINET IO Device	J020D000.nxf	3.4.33.0
		Sercos Slave	J020J000.nxf	3.0.32.0
netRAPID	NRP 51-RE	EtherNet/IP Adapter	R060H000.nxf	2.13.x.x
		PROFINET IO Device	R060D000.nxf	3.12.x.x
		Open Modbus/TCP	R060L000.nxf	2.6.x.x
		Sercos Slave	R060J000.nxf	3.5.x.x
		POWERLINK Controlled Node	R060K000.nxf	3.3.x.x

Table 3: List of devices and firmware with integrated WebServer

2 Accessing the WebServer

2.1 Prerequisites

- The firmware of the communication module must be equipped with the WebServer functionality. You will find a List of Devices and Firmware with Integrated WebServer in the *Devices and firmware with integrated WebServer* [page 6] section.
- The communication module is ready for operation.
- The communication module is connected to a network via its Ethernet interface.
- PC with connection to the network and a web browser.
  The WebServer was tested with the following browser versions:

Browser	Version
Internet Explorer	8.0 (Windows XP)
	9.0 (Windows 7)
Firefox	10.0
Chrome	17.0
Opera	11.61
Safari	5.1.2

Table 4: Browser tested for WebServer

- You must know the IP address of the communication module and a valid user name and a password. For information on user names and passwords, see chapter *User authentication* [page 16].
- If you want to customize your user authentication, you need to upload an authentication file to the WebServer. For this purpose, you need a PC which has the cifX Test Application installed on it, and an Evaluation Board to connect your module to the PC. For more information, see *Customized user authentication* [page 16] section.

2.2 Connecting to WebServer

You connect to the WebServer by entering the IP address of the communication module in the address bar of your web browser.

Note:
The IP address of the communication module is usually defined during configuration of the device by SYCON.net or by the netX Configuration Tool. For further information on how to configure your device and how to set the IP address, please refer to the Operating Instruction Manual for the DTM of the concerned protocol.

Entering the IP address of the device will direct you to the home page/start page of the WebServer. From there you can navigate by hyperlinks to the other pages. You can also open a page by entering the corresponding URL into the address bar of your browser.

Web page	Function	URL in browser
Home	Displays device parameters	`http://<IP-Address>`
Firmware Update	Displays version of currently loaded firmware and loads new firmware.	`http://<IP-Address>/fwupdate.sht`
File Upload	Uploads files to the public folder of the WebServer. Files can also be deleted here.	`http://<IP-Address>/upload.sht`
Reset	Resets device.	`http://<IP-Address>/reset.sht`

Table 5: URLs of WebServer pages

Alternatively, you can call up the merely functional pages of the WebServer, i. e. those HTML pages, which contain only the HTTP functions and no navigation pane or graphics, by entering the following URL into the address bar of your browser.

Function	URL in browser
Displays version of currently loaded firmware and loads new firmware.	`http://<IP-Address>/fwupdate`
Uploads files to the public folder of the WebServer. Files can also be deleted here.	`http://<IP-Address>/upload`
Resets device.	`http://<IP-Address>/reset`

Table 6: Open HTTP functions directly

3 Functions via HTTP

3.1 Displaying device information

The home page of the WebServer displays basic identification parameters of your device. The home page opens after entering the URL `http://<IP-Address>` in the address bar of your web browser.
After having navigated to other pages of the WebServer, you can use the **Home** button in the navigation pane to return to the home page.

netX50/100 Configuration

Welcome to the administration interface of your netX device.

Here you can set different operating parameters and execute remote functions.

Device Information

Property	Value
Product Name:	netJACK 100
Device Number:	1625100
Serial Number:	20008
MAC Address:	00:02:a2:23:6c:81

Figure 1: Homepage WebServer (as depicted in Internet Explorer, might differ in other browser)

3.2 Displaying and updating firmware

The **Firmware Update** page displays the version of the currently loaded firmware and provides a function for uploading new firmware.

To open the firmware page, click **Firmware Update** button in the navigation pane or enter URL `http://<IP-Address>/fwupdate.sht` in the address bar of your web browser.

Note:
This page is protected by a password. For further information on password protection, please see *User authentication* [page 16] chapter.

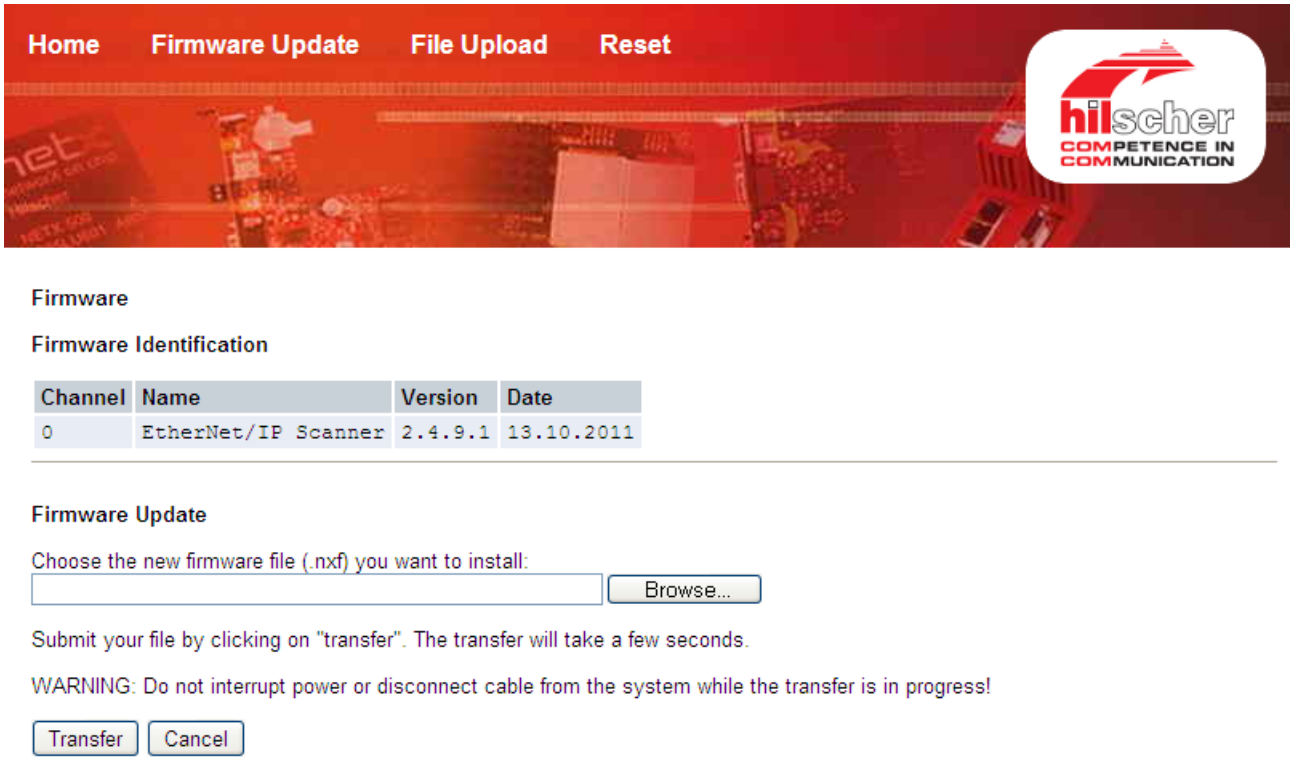

Figure 2: Firmware Update (as depicted in Internet Explorer, might differ in other browser)

Note:
Firmware can only be updated if the chosen firmware and the device are compatible with each other. This means that you cannot load, for instance, an EtherNet/IP Scanner (master) firmware to a netJACK 50 running with a netX 50 controller. Before the update takes place, the system automatically performs a compatibility check, in which e.g. device class and hardware properties are being checked.

Firmware Identification

The **Firmware Identification** section displays the following information about the firmware currently loaded in the device:

- **Channel**: Channel number (Port number)
- **Name**: Name of loaded firmware
- **Version**: Firmware version
- **Date**: Date of firmware

Firmware Update

In the **Firmware Update** section, you can select a new firmware file in order to replace the old firmware, and start the update.

Click **Browse…** button to open a dialog to select the firmware you want to upload. Path and name of the selected file are displayed in the adjacent field.

Note:
The filename extension of firmware files is `.nxf`.

Control element	Function
Selection field	Shows selected file and its location.
Browse…	Opens the file selection dialog.
Transfer	Uploads selected firmware file to device.
Cancel	Cancels firmware update and clears selection field.

Table 7: Controls in Firmware Update

Please observe the following property damage message:

NOTICE

Hazard of device damage by power failure!

Do not interrupt the power supply or disconnect the network cable during transfer of the firmware file.
A power failure while switching from the old to the already stored new firmware can cause severe malfunction of the device.

After you have started the upload by clicking the **Transfer** button, the validity of the firmware file is being checked by the system. If the file fails the validity check, the file will not be stored in the device and an error message will be displayed on the web page. If the file passes, a **Transfer succeeded** message will be displayed.

After successful transfer, you need to reset the device in order to start up the new firmware (see *Reset* [page 15] section).

3.3 File upload

On the **File Upload** page, you can upload files to the accessible directory of the WebServer. Here you can also check which folders and files are currently stored there, and delete items.

To open the file upload, click **File Upload** button in the navigation pane or enter URL `http://<IP-Address>/upload.sht` in the address bar of your web browser.

Note:
This page is protected by a password. For further information on password protection, please see *User authentication* [page 16] section.

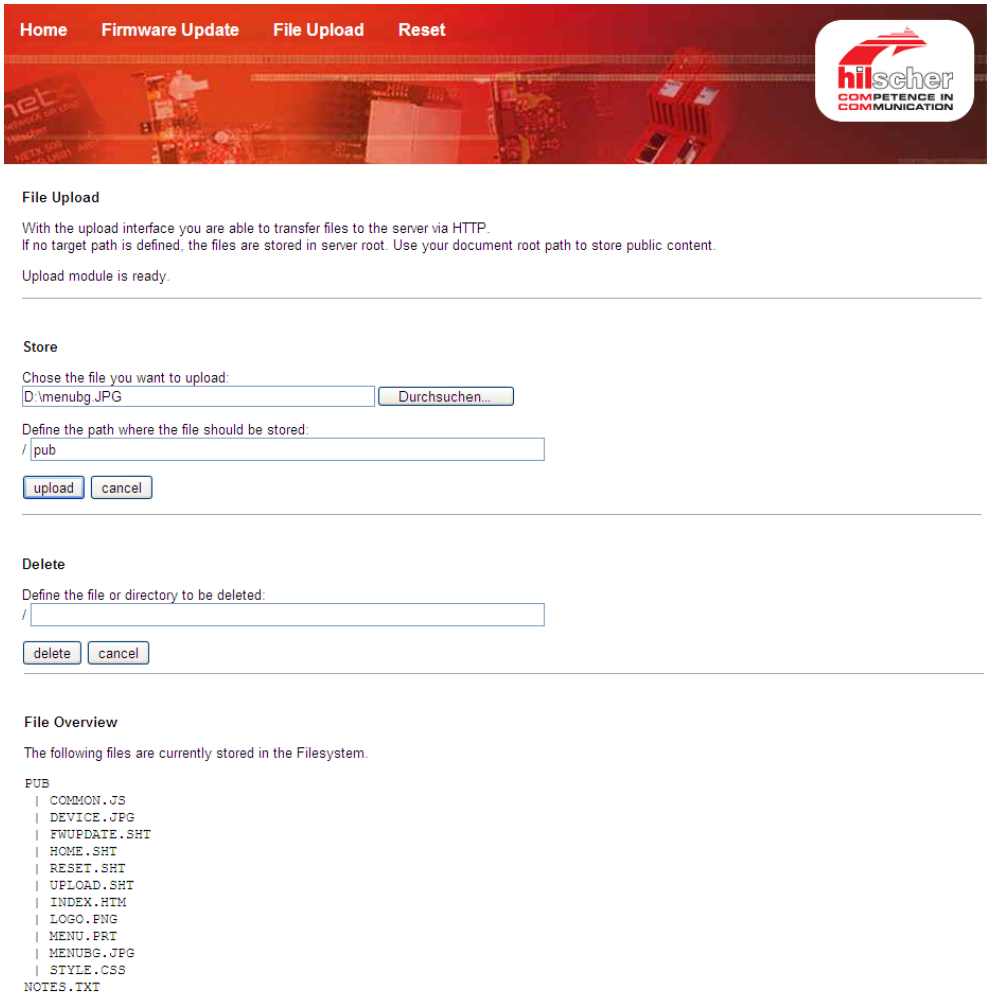

Figure 3: File Upload (as depicted in Internet Explorer, might differ in other browser)

Store

In the **Store** area, you can select the file that you want to upload to the WebServer, and start the upload. Note the following:

- You can upload only one file at a time.
- Filenames must not be longer than eight characters (8.3 filename convention), otherwise the file will not be stored on the WebServer.
- Total size of upload should not exceed one megabyte.
- Files with identical names already stored on the WebServer will be overwritten without a warning message.

Click **Browse…** button to open a dialog to select the file you want to upload. Path and name of the selected file are displayed in the adjacent field.

In the field below **Define the path…**, enter the directory of the public folder `pub` and click **Upload** to start the upload. You can create a new subfolder by entering it as part of the target path, e.g. `pub/myfolder`.

Note:
The File Upload can only access the `Port_1/sx` directory and its subfolders. The `Port_1/sx` path is preset in the File Upload. All web pages and graphics which can be displayed by the WebServer are stored in this directory in a “public” `pub` folder (path: `Port_1/sx/pub`). If you want to add your own content to the WebServer and also want to have it displayed, you need to store it in this public folder. Because the `Port_1/sx` path is preset in the File Upload, you have to enter only the pub folder in the **Define the path…** field of the upload dialog. If you do not enter `pub` and leave the field empty, the uploaded files will be stored in the higher-level directory `Port_1/sx` (and therefore can later not be displayed).
Thus, by uploading files to the `Port_1/sx` directory, you can practically deposit “hidden” files on the WebServer, if you want to do so.

For a graphic depiction of the relevant directories and how to access them, see *Access to the directories* [page 39] chapter.

Control element	Function
Selection field	Shows selected file and its location.
Browse…	Opens the file selection dialog.
Entry field	Enter target directory for the upload.
Upload	Uploads selected file to WebServer.
Cancel	Cancels upload and clears selection field.

Table 8: Controls in Store section of File Upload

Note:

You cannot use the File Upload for updating firmware, because it can only access `Port_1/sx` directory and its subfolders, whereas firmware is stored in `Port_0`. To upload a firmware file, you must use the **Firmware Update** function described in section *Displaying and Updating Firmware* [page 10].

Neither can you use the File Upload to upload the `security.cfg` authentication file, because this file is stored in the root directory of `Port_1`, which cannot be accessed by the **File Upload** function. You must use the *cifX Test Application* or the *netHOST Device Test Application* to upload the `security.cfg` file to the WebServer (see sections *Uploading authentication file* [page 19] respectively *Uploading authentication file to the netRAPID via netHOST and USB* [page 29]).

Delete

In the **Delete** area, you can delete a file or a folder from the WebServer.

Enter the path of the file or folder that you want to delete. You can only delete elements that are stored in the `Port_1/sx` directory or its subfolders.

Control element	Function
Entry field	Enter path of the elements to be deleted.
Delete	Deletes specified elements from the WebServer.
Cancel	Cancels action and clears entry field.

Table 9: Controls in Delete section of File Upload

File Overview

The **File Overview** displays all folders and files which are stored in the `Port_1/sx` directory (i. e. in the directory accessible by the **File Upload** function).

Note:

All characters are displayed in upper-case. If a file name contains a blank, only the part of the file name that lies **before** the blank will be displayed. Example: The file `my notes.txt` will be displayed as `MY.TXT`.

3.4 Reset

On the **Reset** page, you can reset your communication module.

To open the **Reset** page, click **Reset** button in the navigation pane or enter URL `http://<IP-Address>/reset.sht` in the address bar of your web browser.

Note:
This page is protected by a password. For further information on password protection, please see *User authentication* [page 16] section.

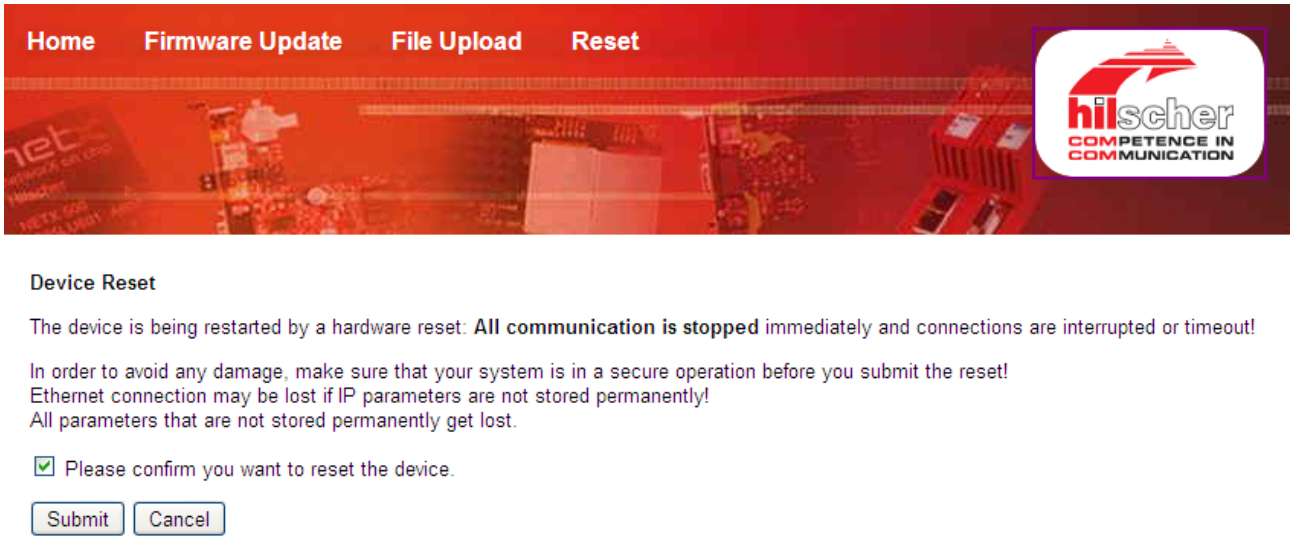

Figure 4: Device Reset (as depicted in Internet Explorer, might differ in other browser)

A reset has to be made after every firmware or configuration update.
It has the following consequences:

- The firmware is being restarted and connections will be interrupted or timed out.
- I/O bus communication is being stopped.
- The IP connection may be lost if the IP parameters have not been defined and stored in the device permanently by SYCON.net or the netX Configuration Tool.

Note:
If you reset the device and the IP parameters have not been stored permanently, or if you have switched the device to a different Ethernet protocol, you may have to reassign the IP address (by using a suitable tool like e. g. SYCON.net) before you can reconnect to the WebServer.

Activate the checkbox in front of **Please confirm...** to acknowledge that you want to reset the device.
To start the reset, click **Submit** button.
Click **Cancel** button to uncheck the checkbox in front of **Please confirm...**

4 User authentication

4.1 Default user authentication

Access to the **Firmware Update**, **File Upload** and **Reset** functions is protected by a default user authentication.

On calling up one of these functions, a password dialog appears. Default authentication parameters for all functions are:

User Name: `admin`
Password: `admin`

These default authentication parameters remain valid until you have stored a `security.cfg` authentication file containing a new password for the `admin` user in the root directory of `Port_1` on the WebServer.

4.2 Customized user authentication

You can establish a customized user authentication for your WebServer. For this purpose, you need to define users with their rights and passwords in a simple text file and store it as `security.cfg` authentication file on the WebServer in the root directory of `Port_1`.
Passwords must be stored as MD5 code/hash in the `security.cfg` file. You can use any MD5 generator (available as freeware or online tool) to create the MD5 code.

Use the *cifX Test Application* or the *netHOST Device Test Application* to upload or delete the `security.cfg` authentication file.

Once you have uploaded the security.cfg authentication file to the WebServer, the parameters contained in this file are binding, and the parameters of the default user authentication are no longer valid.

Important:
Take care to define an `admin` user with a new password in the authentication file, in order to abrogate the default user authentication parameters (`admin` / `admin`) and to protect access to the WebServer effectively. If the authentication file contains no `admin` user, the old default user authentication parameters for the `admin` stay valid, in addition to the new parameters contained in the authentication file for other new users, which you may have defined.

Deleting the `security.cfg` file reinstates the parameters of the default user authentication.

4.2.1 Groups and rights

The right to access a certain function of the WebServer is linked to the membership of the user in the corresponding functional group.

The following functional groups are currently implemented on the WebServer:

Group	Function
reset	allows to reset the device
firmware	allows to update the firmware of the device
upload	allows to store or delete files in the `Port_1/sx` directory

Table 10: Functional groups

A functional group is assigned to an individual user in the authentication file by stating the functional group in the same line behind the user name and the MD5 password hash. To each user name, several functional groups can be assigned.

Note:
The **admin** user is always automatically member of all three functional groups **reset**, **firmware** and **upload**; even if these groups have not been explicitly assigned to the **admin** user.

4.2.2 security.cfg authentication file

In the `security.cfg` authentication file, you can use a simple text editor to edit users and assign functional groups and MD5 password hashes.

The ASCII text file starts with the specification of the realm, followed by the lines containing the parameters of each user. Each line contains the parameters of a single user in the following syntax:

```
<user name>;<MD5 hash generated from user
name:realm:password>;<functional group1>,<functional
group2>, (…);
```

On your product DVD, in the `Examples & API > [x]. WebServer pages > Common > Port_1` directory, you will find an example of a `security.cfg` file which you can use as template for creating your own authentication file. This file contains three predefined users, named `user`, `manager` and `admin`, endowed with the following passwords and rights:

User name	Password	Functional group
user	user	reset
manager	manager	reset, firmware
admin	admin	firmware, reset, upload

Table 11: Assignment of users, passwords and rights in security.cfg example file

These assignments are coded in the `security.cfg` file by using the following strings:

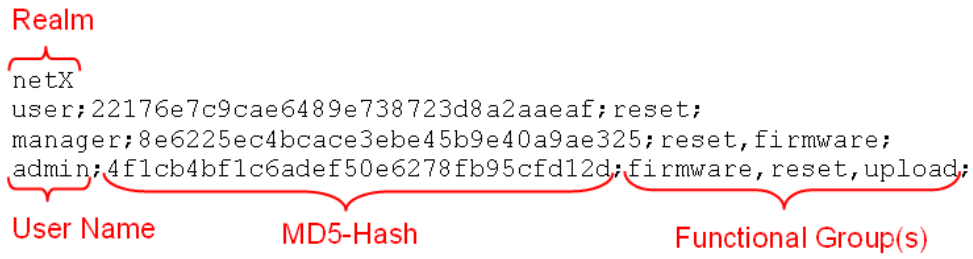

Figure 5: Strings in security.cfg

4.2.3 Generating password hash with MD5

Passwords must be stored in the `security.cfg` authentication file as MD5 hash. You can use any MD5 generator to create the password hash and then paste the generated string into the corresponding line in the authentication file.

The MD5 hash must be generated with the following parameters in the following syntax:

```
<User Name>:<Realm>:<Password>
```

This means, that e. g. for a user John Doe with his password “summertime” you would have to enter the following parameter string into the MD5 generator:

```
John Doe:netX:summertime
```

The MD5 generator will turn this input into the hash `9764e291537f2017a065c63c56968800`.

Note the following about user names and passwords:

- You can use all printable ASCII characters and a blank space (ASCII code 32 [dec] to 126 [dec]) in user names and passwords, but no semicolon (;) in a user name, because the semicolon serves as separator in the authentication file.
- All entries are case sensitive.
- The spelling of the user name in the MD5 generator and in the login dialog of the WebServer must be identical to the spelling in the authentication file (e. g. in regard to blanks between first names and surnames).
- The spelling of the password in the MD5 generator must be identical to the spelling in the login dialog of the WebServer.

4.2.4 Uploading authentication file

The `security.cfg` authentication file must be stored in the root directory of `Port_1` of the system.

Because the **File Upload** of the WebServer can only access the `Port_1/sx` directory, but not the `Port_1` root directory, you have to use the *cifX Test Application* or the *netHOST Device Test Application* to upload the `security.cfg` file to the WebServer.
This section describes how to use the *cifX Test Application* for this.

The cifX Test Application, which is part of the cifX Device Driver installation for Windows, allows you to access your communication module via its host interface. For this purpose, you have to connect your module via Evaluation Board with a PC which has the cifX Test Application installed on it. For further information on how to use an Evaluation Board, please refer to the User Manual of your communication module.

Step by step instructions for uploading authentication file

1. Start the cifX Test Application.
   - ➢ Open the **Control Panel** of Windows and double click **cifX Test** entry.
   - ↬ The cifX Test Application opens.
2. In the cifX Test Application, open Channel1 of the device.
   - ➢ In the menu, choose **Device > Open**.
   - ↬ The **Channel Selection** dialog opens.
   - ➢ In the left area, select **Channel1**, then click **Open** button.

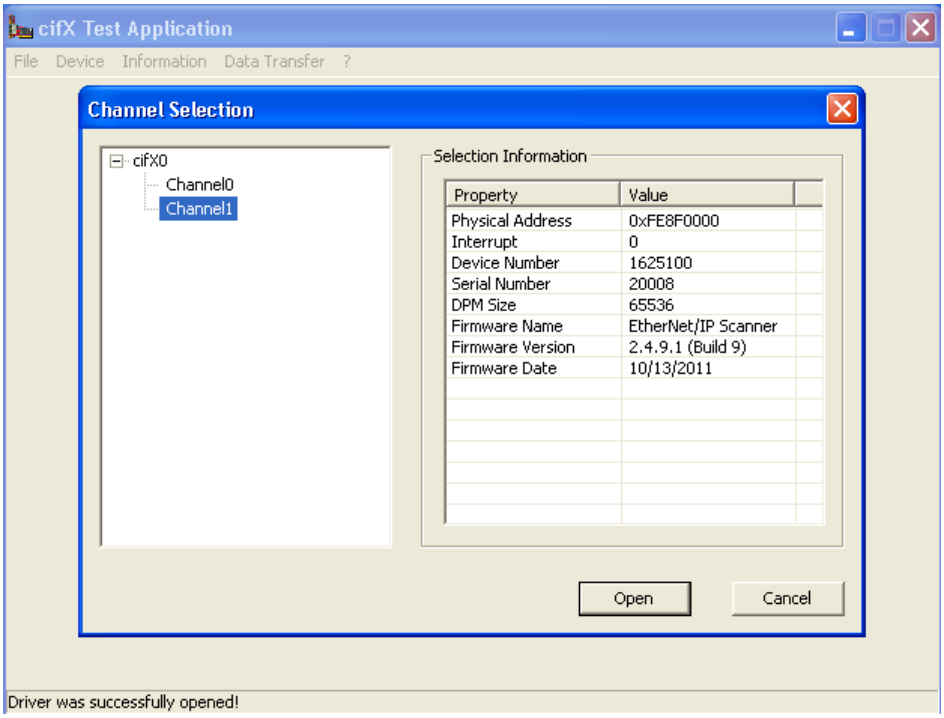

Figure 6: Select channel in cifX Test Application

   - ↬ The channel is opened and the **Channel Selection** dialog window closes.

3. Upload authentication file to the device.
   - ➢ In the menu, choose **Device > Download.**
   - ⇘ The **Download Test** window opens.
   - ➢ In the **Download Mode** dropdown list, choose **File Download** entry.
   - ➢ In the **Filename** field, click … button to open a file selection dialog.
   - ➢ In the file selection dialog, choose `security.cfg` on your file system and click **Open** dialog.
   - ⇘ The file selection dialog closes.
4. Transfer authentication file.

Note:
Keep in mind, that the old security.cfg file, which might have already existed in the root directory, will be overwritten by the downloaded new file without a warning message.
In the CifX Test Application, you can use the **File Explorer** to check which files are currently stored in the root directories of the device, and download these files to your own local system for backup, if necessary. First open the channels (ports) you want to check, then choose **Device** > **File Explorer** in the menu.

- ➢ Click **Download** button to transfer the authentication file to the device.

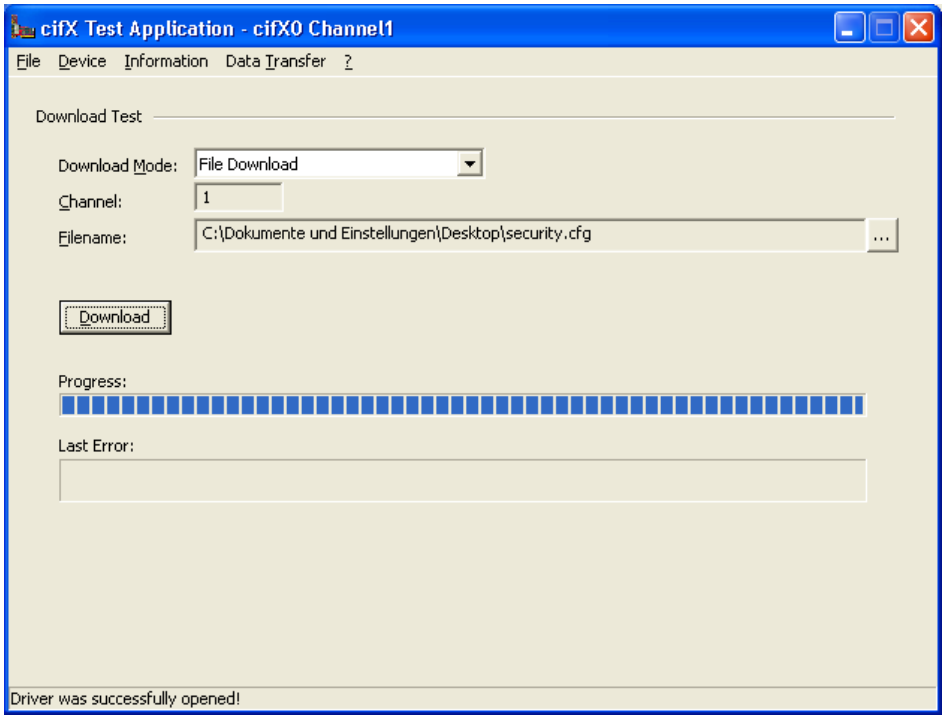

Figure 7: Download authentication file

- ⇨ You have transferred the authentication file to the device.

Note:
You must reset the device to activate the new authentication file.
In the cifX Test Application, choose **Device** > **Reset**.

4.2.5 Deleting authentication file

With the *cifX Test Application* or the *netHOST Device Test Application*, you can delete the `security.cfg` from the WebServer and thereby reinstate the default user authentication.
This section describes how to use the *cifX Test Application* for this.

Step by step instructions for deleting authentication file

➢ Start the cifX Test Application and open Channel1 as described in steps 1 and 2 in the *Uploading Authentication File* [page 19] section.

➢ Choose **Device** > **File Explorer** and select the security.cfg file listed under **Filename**.

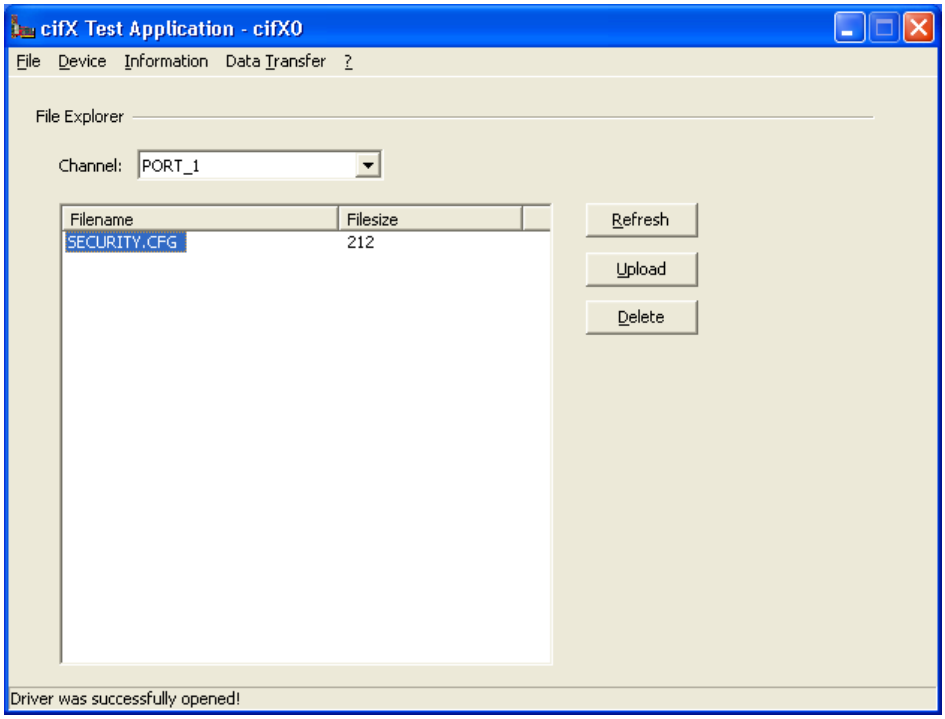

Figure 8: Display and delete files in File Explorer

Note:
If necessary, you can save the file to your local system by clicking the **Upload** button before deleting it from the WebServer.

➢ To delete the file, click **Delete** button.

➢ Choose **Device** > **Reset** to reset the device.

⇨ You have deleted the security.cfg authentication file. The default user authentication is active again (see *Default User Authentication* [page 16]).

5 Adding own content

5.1 Overview

You can store your own web pages and images (e.g. your company logo) on the WebServer or revise the pages provided by Hilscher, in order to customize structure and design of the website hosted on the WebServer.

Use the **File Upload** to upload new files or web pages to the `Port_1/sx/pub` public directory of the WebServer as described in the *File upload* [page 12] section.
Please note the following:

- Only 8.3 filenames are supported, i.e. filenames must consist of no more than eight characters, filename extensions of no more than three characters.
- Total size of files in public directory should not exceed two megabytes.

The HTTP functions **Firmware Update**, **File Upload** and **Reset** will not be affected by any changes you make in the public directory, because the actual HTML pages containing the code for these functions are stored in a place which is not accessible by the user. Even if you deleted from the public directory all pages containing links to these functions, you still would be able to call up these functions by entering the corresponding URL in your browser. The URLs of these functions are listed in the *Connecting to WebServer* [page 8] section.

Example files on product DVD

On your product DVD, in the `Examples & API > [x]. WebServer pages > Common > Port_1 > sx > pub` directory, you will find the very same files which are also stored in the public directory of the WebServer within the device, when the device is being shipped to the customer. (Note the exception of the netRAPID: in its state of delivery, the netRAPID comes with its web files not yet loaded on the device – this needs to be done by the user.)
These files are the web pages and graphics which are displayed by default when you first connect to the WebServer. You can use these files as templates and change them locally according to your needs – e.g. by inserting new HTML code, customizing the style sheet or replacing graphics with your own company logo – and upload them to the WebServer afterwards.

Note:
The `device.jpg` graphic file in the `Examples & API > [x]. WebServer pages > Common > Port_1 > sx > pub` directory on the DVD is a proxy file.
You will find a graphic file containing an actual picture of your device on the DVD in the `Examples & API > [x]. WebServer pages > Product` directory, in a subfolder named after your device (e.g. `comX`, `netJACK` or `netRAPID`).

Server Side Includes and Inlineframes

Most of the default web pages of the WebServer use Server Side Includes (SSI) und Inlineframes (iframe). With SSI and iframe commands, you can embed HTML code or other pages dynamically in your web page. An HTML file containing SSI commands must carry the file name extensions `.sht` or `.stm` for the WebServer to be able to process it.

For Example, in the `fwupdate.sht`, `reset.sht` and `upload.sht` files the navigation (menu) pane is embedded as SSI command `<!--#include file="menu.prt" -->`, and the HTML pages containing the actual code for the **Firmware Update**, **File Upload** and **Reset** functions are embedded as iframes (e. g. `<iframe src="fwupdate"…>`).

5.2 Examples for adding own content

The following sections provide step-by-step instructions for typical tasks which you might want to perform in order to customize the web pages of the WebServer. Note that these are only exemplary descriptions and that there are – depending on your skills in web design – other possible ways of proceeding.

5.2.1 Example 1: Substituting company logo in the navigation pane

The navigation pane on top of each WebServer page carries the Hilscher logo. The logo is hyperlinked, so that if you click on it, it will direct your browser to the Hilscher Website. If you want to exchange the Hilscher logo with your own company logo and if you want the hyperlink to lead to your own company's website, proceed as follows:

1. Exchange graphic file (for this, you don't need to edit HTML code).
   - ➢ Simply overwrite the `logo.png` file on the WebServer, which contains the Hilscher logo. For this, you only need to upload a PNG graphic file which contains your own logo and which is also named "logo.png" to the `pub` folder on the WebServer. (See *File upload* [page 12] section.)

   

   Note:
   A pixel size of 150 (width) x 100 (height) for the logo is recommended.

   - ⇨ As soon as your browser reloads a page of the WebServer, the new logo.png file with your company logo will be shown instead of the Hilscher logo.
2. Adapt hyperlink (for this, you need to edit the HTML code in the `menu.prt` file, which defines the contents of the navigation pane).
   - ➢ Copy the `menu.prt` file from the product DVD to your local PC. The `menu.prt` file is stored on the DVD in the directory `Examples & API > [x]. WebServer pages > Common > Port_1 > sx > pub`.
   - ➢ Open the file in Windows Notepad.

You see the HTML code in the `menu.prt` file:

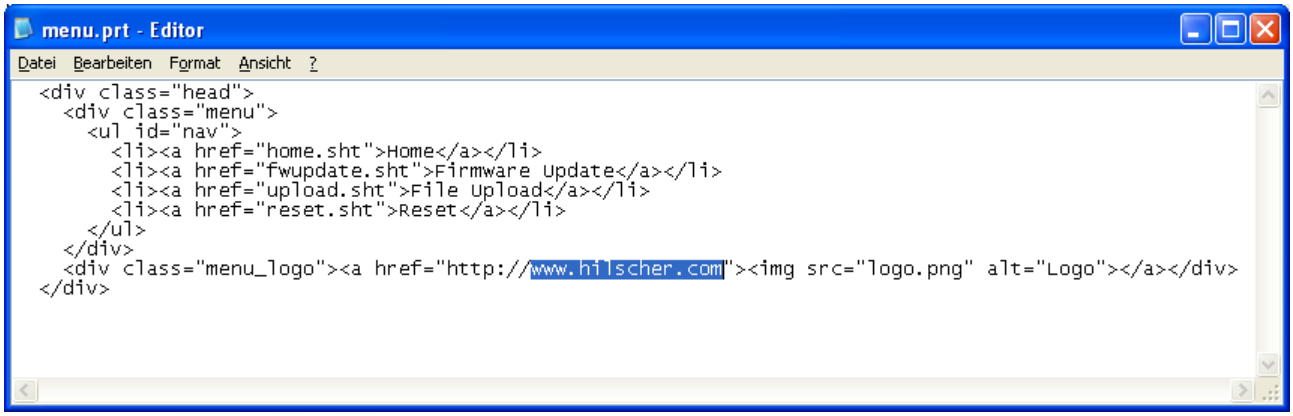

Figure 9: Editing hyperlink in menu.prt

- Substitute the `www.hilscher.com` web address with your own web address, e.g. `www.doe-automation.com`.
- Save and close the file.
- Upload the altered `menu.prt` file to the `pub` folder on the WebServer (see *File upload* [page 12] section), thereby overwriting the old `menu.prt` file.
- As soon as you click on the logo after your browser has reloaded a page of the WebServer, you will be directed to your own company's website.

5.2.2 Example 2: Changing background design in the navigation pane

If you want to change the background image in the navigation pane, you can simply overwrite the `menubg.jpg` graphic file on the WebServer, which contains the current background image. For this, you only need to upload a JPEG graphic file which contains your preferred background image and which is also named `menubg.jpg` to the `pub` folder on the WebServer. (See *File upload* [page 12] section.)
A pixel size of 932 (width) x 152 (height) for the background picture is recommended.

Layout and design of the WebServer pages are defined in a cascading style sheet named `style.css`. If, for example, you want a simple blue space instead of an image for background design in the navigation pane, you need to edit the style sheet:

- Copy the `style.css` file from the product DVD to your local PC. The `style.css` is stored on the DVD in the directory `Examples & API > [x]. WebServer pages > Common > Port_1 > sx > pub.`
- Open the file in a suitable editing tool.

You see the declarations contained in the `style.css` file:

```
* {
        font-family:Arial;
}

body {
  text-align:left;
  background-color:#E9E9EA;
}

/*** NAVIGATION MENU ***/
.head {
  margin:0; border:0; padding:0;
  height: 152px;
  max-width: 932px;
  background-color:#e01010;
  background-image:url(menubg.jpg);
  background-repeat:no-repeat;
  background-position:left top;
}

.menu {
  margin: 0; padding: 0;
  min-width: 28em;
  float: left;
}
```

Figure 10: Style.css file

- Navigate to the `.head` selector in the `*** NAVIGATION MENU ***` section and remove the background image by deleting the string `background-image:url(menubg.jpg);`.
  Then change the background color by substituting the value #e01010 (the value for the currently used red color) behind the background-color property with a value for blue, e. g. #0000FF.
- Save and close the file.
- Upload the altered `style.css` file to the `pub` folder on the WebServer (see *File upload* [page 12] section), thereby overwriting the old `style.css` file.

⇨ As soon as you reload a WebServer page in your browser, the background of the navigation pane will be depicted in blue color.

5.2.3 Example 3: Integrating new web page

You can upload new web pages to the WebServer and link them in the navigation pane. If, for example, you want to add a web page featuring notes or working instructions, proceed as follows:

1. Create a new web page. You can use an existing web page as template and fill it with your own content.
   - ➢ Copy the `reset.sht` file from the product DVD to your local PC. The `reset.sht` is stored on the DVD in the directory `Examples & API > [x]. WebServer pages > Common > Port_1 > sx > pub`
   - ➢ Open the file in a suitable editing tool.
   - ↬ You see the HTML code in the `reset.sht` file (for clarity, the following figure features line folding):

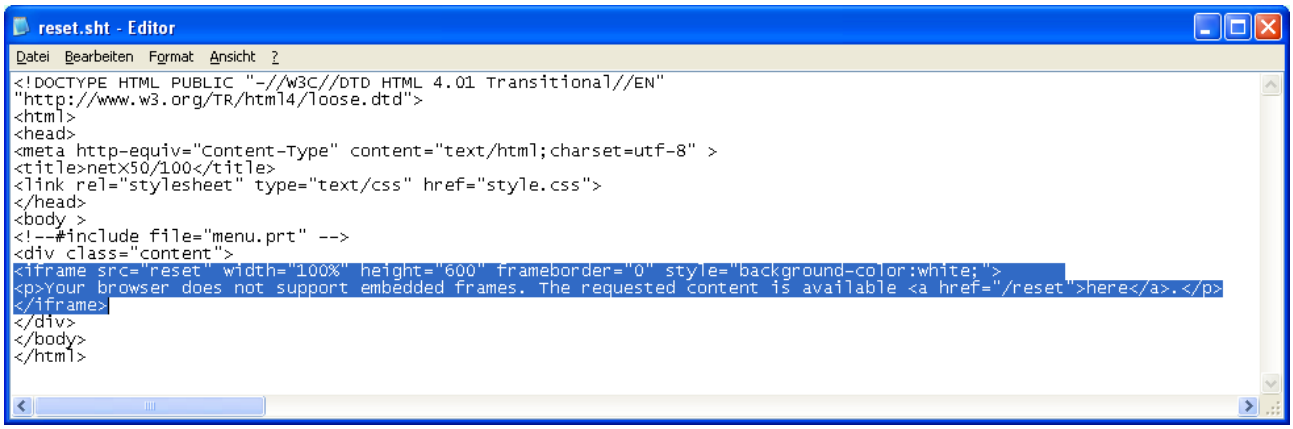

Figure 11: HTML code in the `reset.sht` file

- ➢ Delete the iframe element from the HTML code (i. e. the string from the opening tag `<iframe src="reset"[…]>` to the closing tag `</iframe>`). Then insert your notes or working instructions as HTML text at the same position, replacing the deleted iframe element:

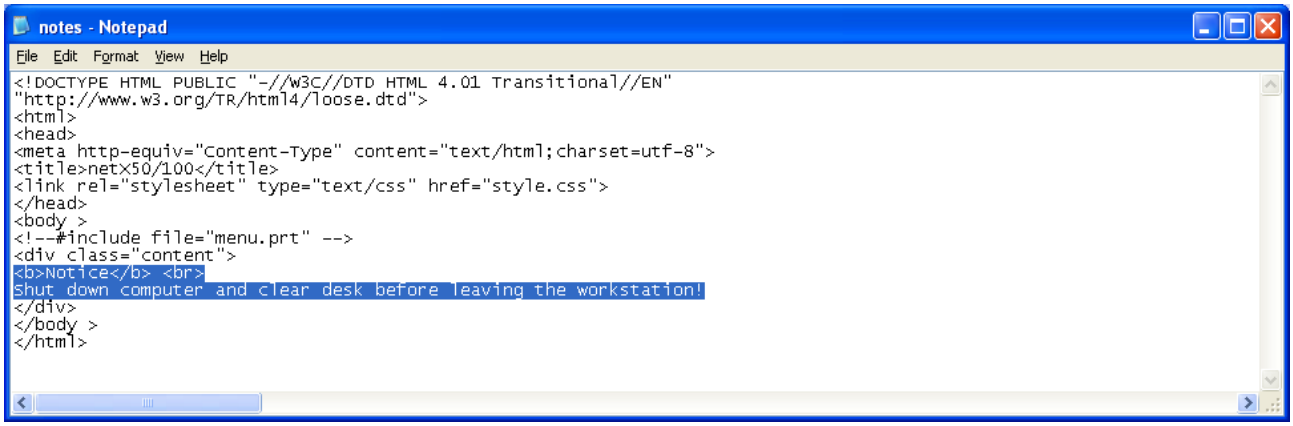

Figure 12: Insert own text

- ➢ Save the file e. g. as `notes.sht`. Take care that the file name consists of no more than eight characters and that the extension is `.sht`.

➢ Upload the `notes.sht` file to the `pub` folder on the WebServer (see *File upload* [▷ page 12] section).

2. Add in the navigation pane a link to the new web page. For this, you need to insert a hyperlink in the `menu.prt` file, which defines the contents of the navigation pane.

➢ Copy the `menu.prt` file from the product DVD to your local PC. The `menu.prt` file is stored on the DVD in the directory `Examples & API > [x]. WebServer pages > Common > Port_1 > sx > pub`.

➢ Open the file in Windows Notepad.

➢ You see the HTML code in the `menu.prt` file:

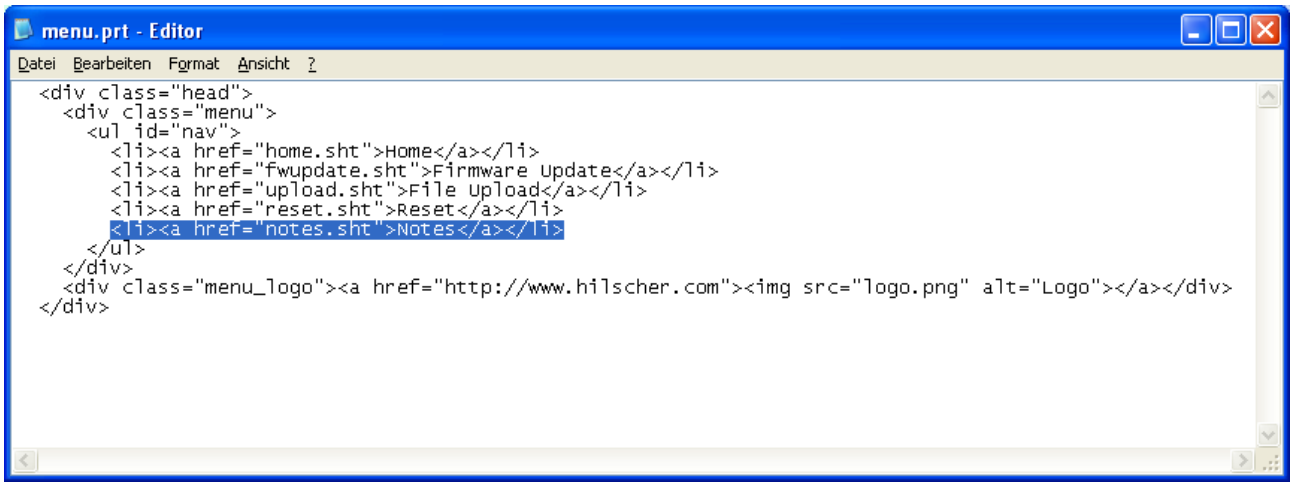

Figure 13: Adding hyperlink for new web page

➢ Enter the code for the hyperlink:
`<li><a href="notes.sht">Notes</a></li>`

➢ Save and close the file.

➢ Upload the altered `menu.prt` file to the `pub` folder on the WebServer (see *File upload* [▷ page 12] section), thereby overwriting the old `menu.prt` file.

⇨ As soon as your browser has reloaded a page of the WebServer, you will see the new hyperlink in the navigation pane. You can open your new page by clicking on the hyperlink or by entering the IP address followed by the filename `(http://<IP-Address>/notes.sht)` in the address bar of your web browser.

6 Uploading WebServer content to netRAPID

6.1 Overview

The **netRAPID NRP 51-RE** is shipped with its WebServer content not yet installed – which means that you have to download these WebServer files to the netRAPID after having commissioned the netRAPID (i.e. after having downloaded its firmware and device configuration).

For loading the “public” content files to the WebServer (the i.e. HTML pages, graphics, and style sheets, which are to be stored in the `pub` folder), you can use the **File Upload** function of the WebServer. The HTTP functions **Firmware Update**, **File Upload** and **Reset** are implemented in the device firmware independently from the “loadable” public web content.

However, for loading the `security.cfg` authentication file to the WebServer, you need the *netHOST Device Test Application*, which allows you to access the “non-public” `Port_1` root directory of the netRAPID via USB (the authentication file must be stored in this `Port_1` root directory for protection).

6.2 Uploading authentication file to the netRAPID via netHOST and USB

Prerequisites

- You have downloaded the firmware to the netRAPID.
- If you are not using the netRAPID Evaluation Board: The netRAPID host device is equipped with a USB interface.
- You have access to the netRAPID product DVD.
- You have installed the Hilscher USB device drivers on your PC. (To install the USB drivers, open the `Driver and Toolkit\USB Diagnostic Driver` directory, then double-click `setup.exe` file. Follow the instructions of the installation wizard)
- The netRAPID Evaluation Board (respectively the host device of the netRAPID) is connected to a voltage supply.
- The netRAPID Evaluation Board (respectively the host device of the netRAPID) is connected to your PC via USB.

Step-by-step instructions

1. Open the **netHOST Device Test Application** on your PC.
   - ➢ On the netRAPID product DVD, open the `Tools\netHOST\x64` folder.
   - ➢ Double-click the `netHOST.exe` file.
   - ➪ The **netHOST Device Test Application** opens:

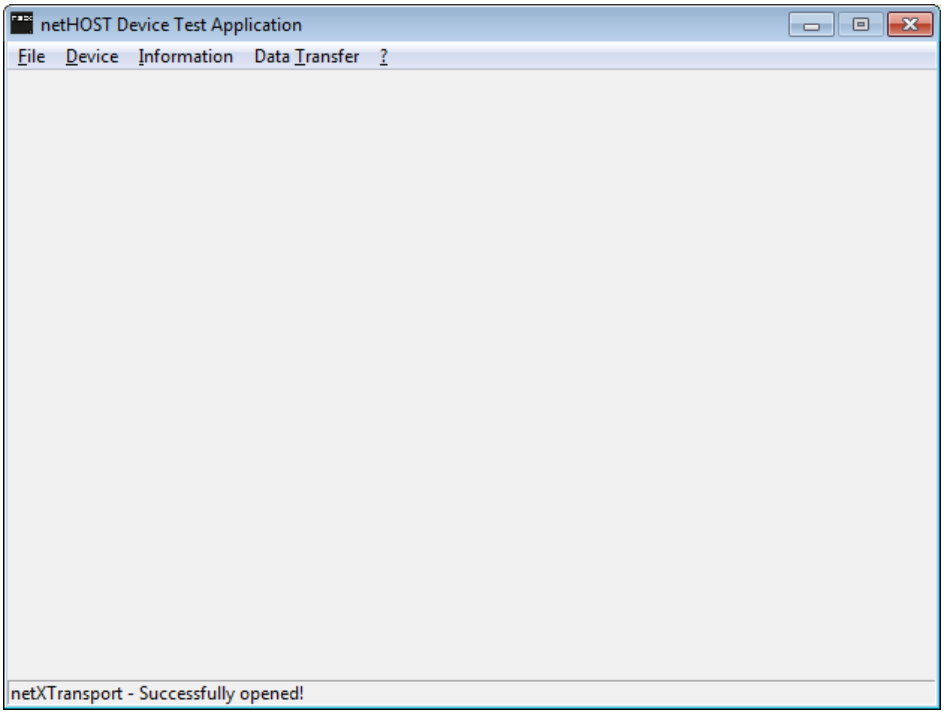

Figure 14: netHOST Device Test Application start screen

2. Open connection to `Channel 1` (`port 1`) of the netRAPID.

   ➢ Open the **Device** menu and make sure that the **Select netX Driver** option is selected:

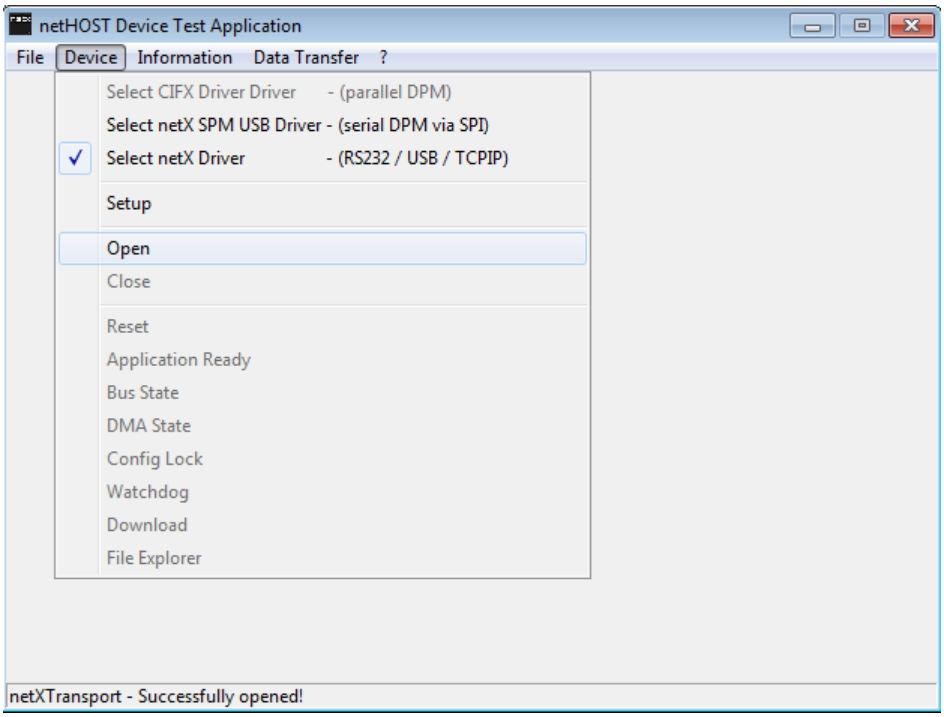

Figure 15: Select netX Driver in netHOST

   ➢ Then choose **Open** from the **Device** menu and wait for a few seconds.

   ↯ The **Channel Selection** dialog window opens.

   ➢ In the left part of the window, select **Channel1**, then click **Open** button.

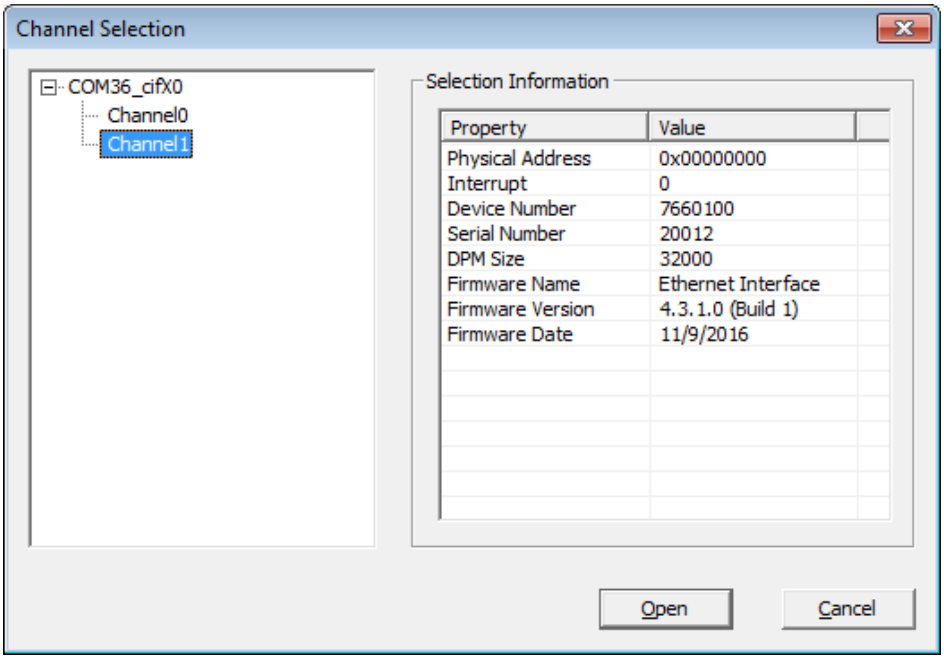

Figure 16: Channel Selection in netHOST

The **Channel Selection** dialog box closes, and back in the netHOST Application window, the header displays the selected channel:

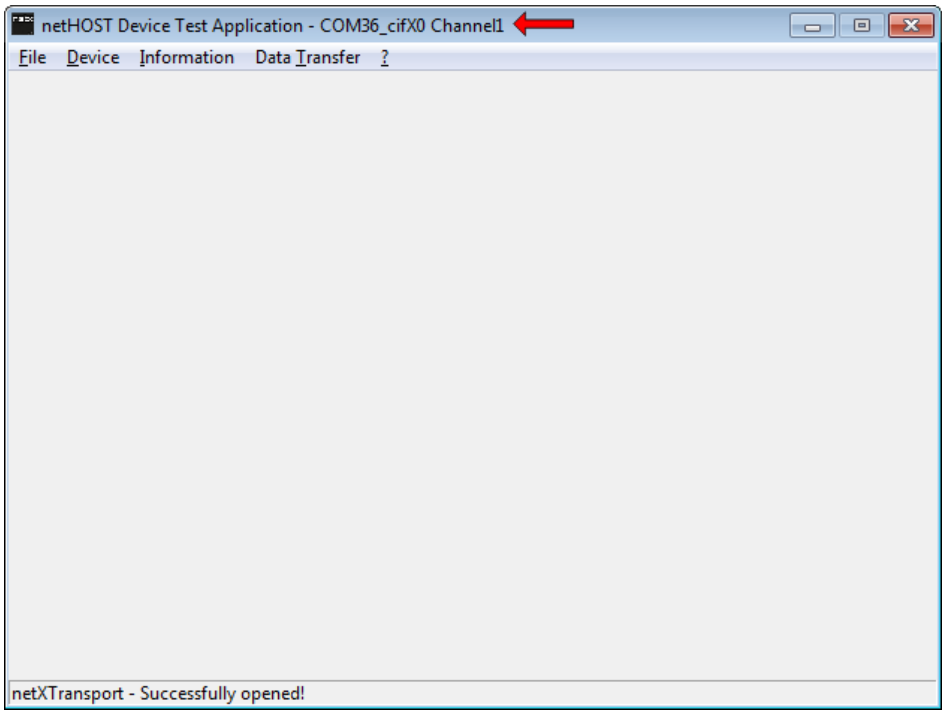

Figure 17: Selected channel in netHOST

3. Download authentication file to the netRAPID.
   - In the menu, choose **Device > Download.**
   - The **Download Test** window opens.

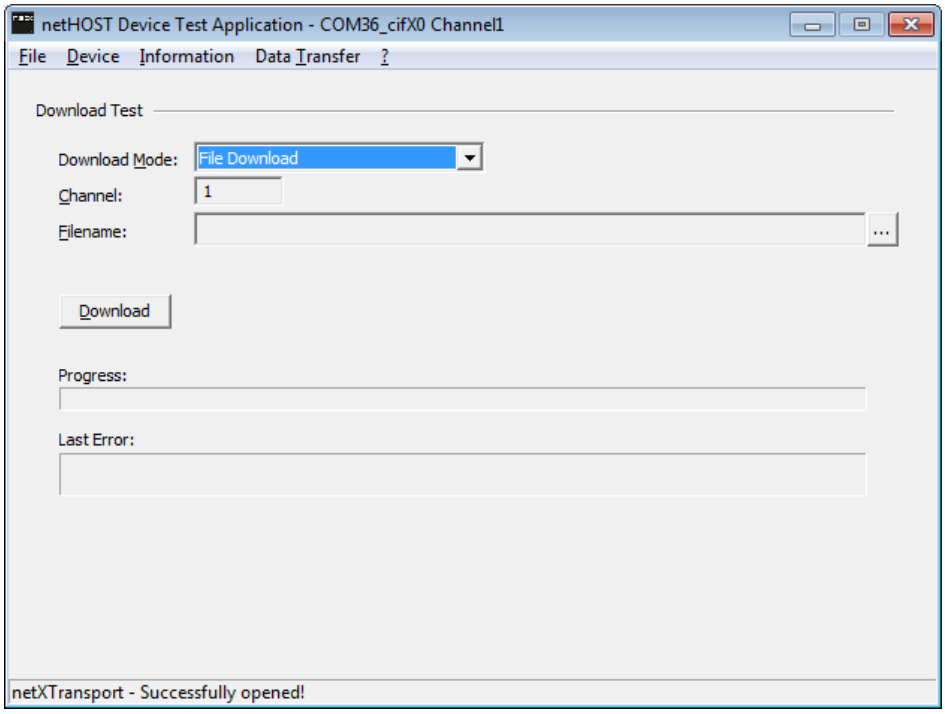

Figure 18: File Download in netHOST

   - In the **Download Mode** dropdown list, choose **File Download** entry.
   - In the **Filename** field, click ... button to open a file selection dialog.

↬ The Windows file selection dialog opens.

➢ On the netRAPID product DVD, open the `Examples and API\[x]. WebServer pages\Common\PORT_1` folder.

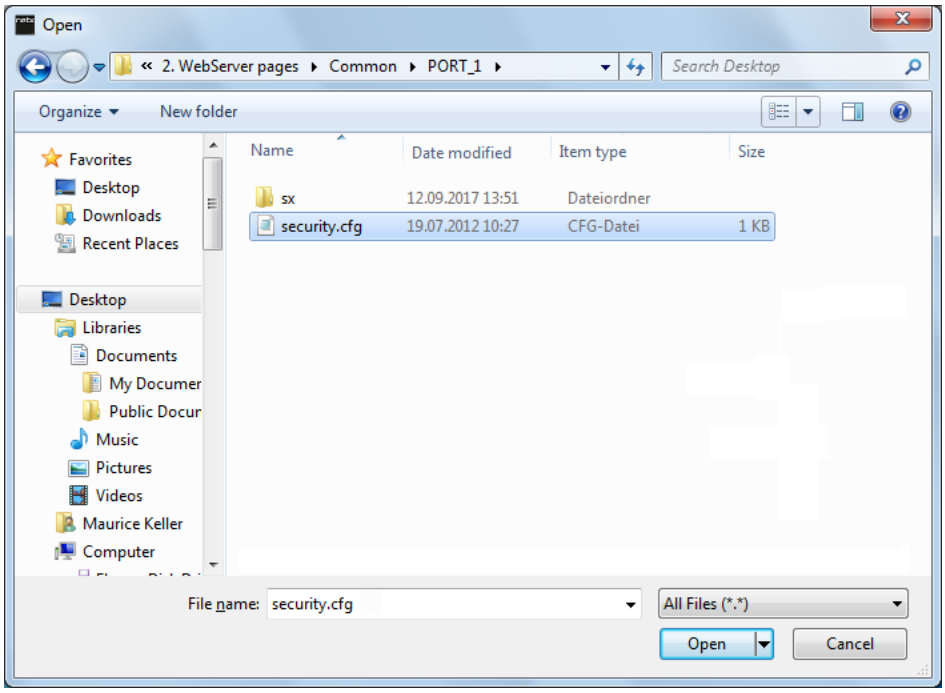

Figure 19: security.cfg in Windows file selection dialog

➢ Choose the `security.cfg` file and click **Open**.

↬ The file selection dialog closes and the path of the selected file is displayed in the **Filename** field.

➢ Click **Download** button.

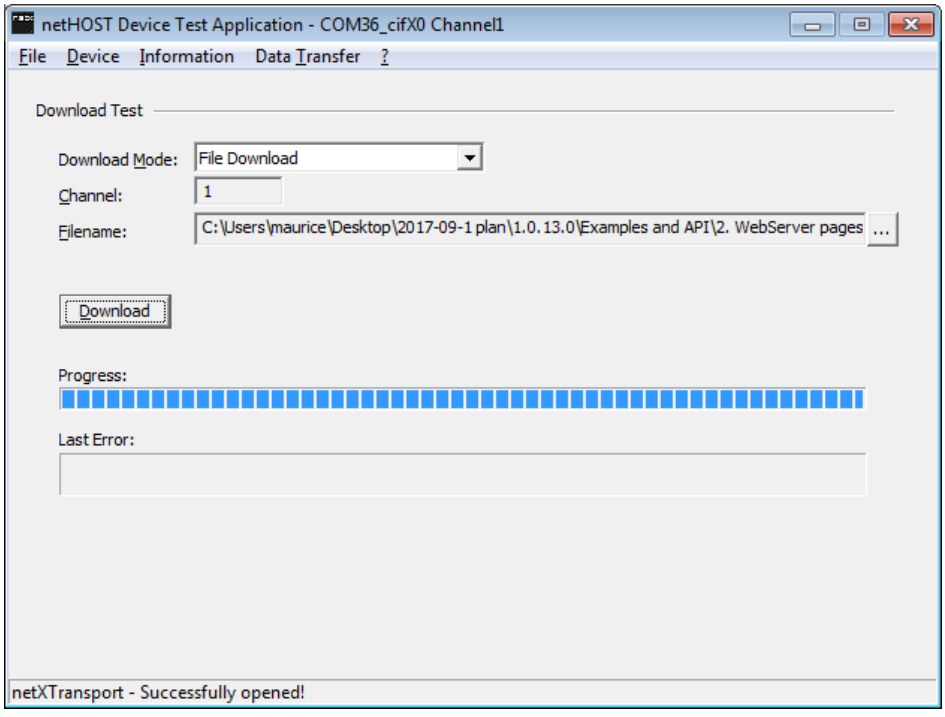

Figure 20: Download authentication file in netHOST

While the file is being downloaded to the netRAPID, a progress bar is displayed.

Note:
A completed download is indicated only by the full progress bar; there will be no extra message box popping up in order to inform you about the completion of the download.

4. Check Download.
   - In the **Device** menu, choose **File Explorer**.
   - The `security.cfg` , which you have downloaded to the device, should now be displayed in the **File Explorer**:

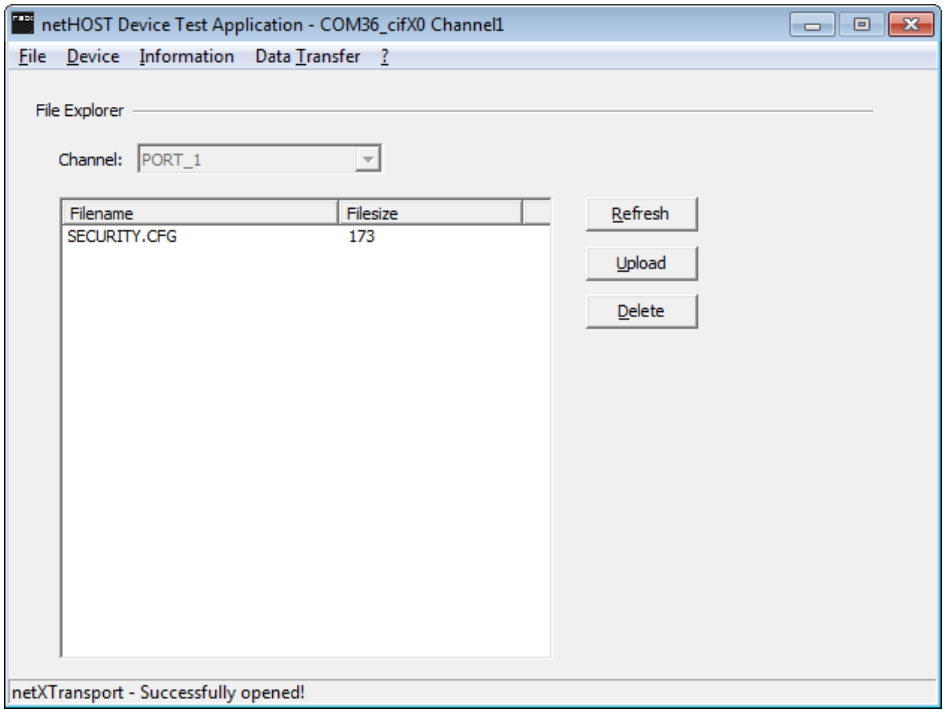

Figure 21: File Explorer in netHOST

Note:
The `sx` folder, which is also located in `PORT_1` (and in which the public content of the WebServer is stored) cannot be displayed by the netHOST Device Test Application.

- In the menu, choose **Device** > **Close** and then **File** > **Quit** to close the netHOST Device Test Application.
- You have transferred the authentication file into the netRAPID. You can now proceed to transfer the WebServer content files into the netRAPID by using the **File Upload** function (you cannot use the netHOST Device Test Application for this).

6.3 Uploading Web-Content to the netRAPID via File Upload

Prerequisites

- You have downloaded the firmware to the netRAPID.
- An IP address has been configured for the netRAPID.
- You know the IP address of the netRAPID.
- You have access to the netRAPID product DVD.
- The netRAPID Evaluation Board (respectively the host device of the netRAPID) is connected to a voltage supply.
- The netRAPID Evaluation Board (respectively the host device of the netRAPID) is connected to an IP network via its Ethernet interface.
- PC with web browser connected to the same IP network.

Step-by-step instructions

➢ Enter the IP address of your netRAPID in the address bar of your web browser, followed by `upload`. Use the following syntax:
`http://<IP address>/upload`

↬ A password dialog opens.

➢ Enter user name `admin` and password `admin` (default, if not defined otherwise in the `security.cfg` file)

↬ The **File Upload** module of the WebServer opens in your browser:

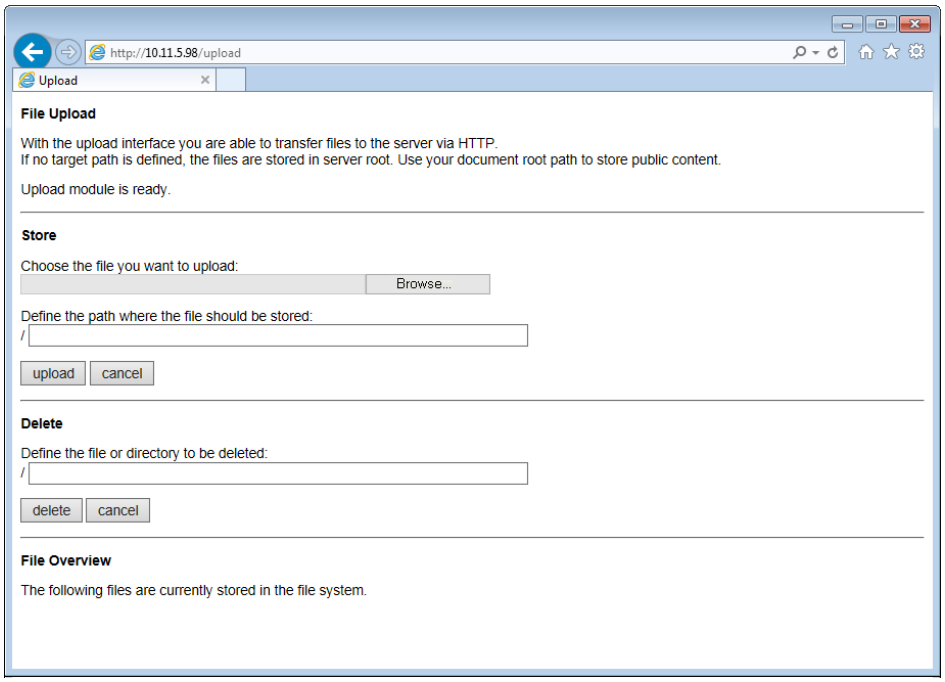

Figure 22: File Upload module of WebServer (as depicted in Internet Explorer, might differ in other browser)

➢ In the field **Define the path where the file should be stored** enter `pub`.

➢ Click **Browse...** button.

↬ The File selection dialog opens.

➢ On the netRAPID product DVD, open the `Examples and API\[x]. WebServer pages\Common\PORT_1\sx\pub` folder.

➢ Select the `common.js` file and click **Open** button.

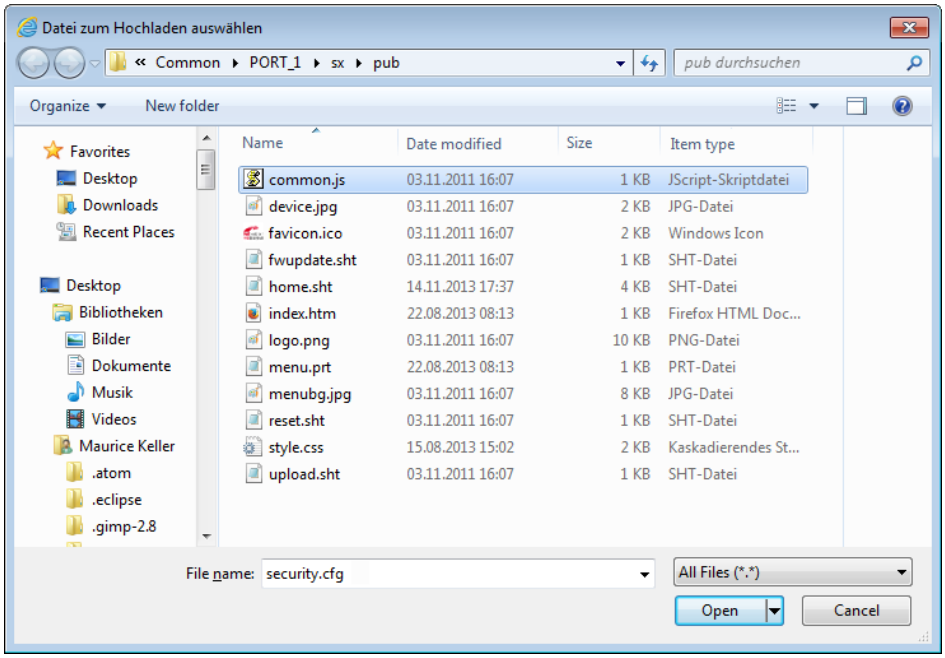

Figure 23: File selection dialog

➢ The file selection dialog closes and the path of the selected file is displayed in the **Choose the file you want to upload** field:

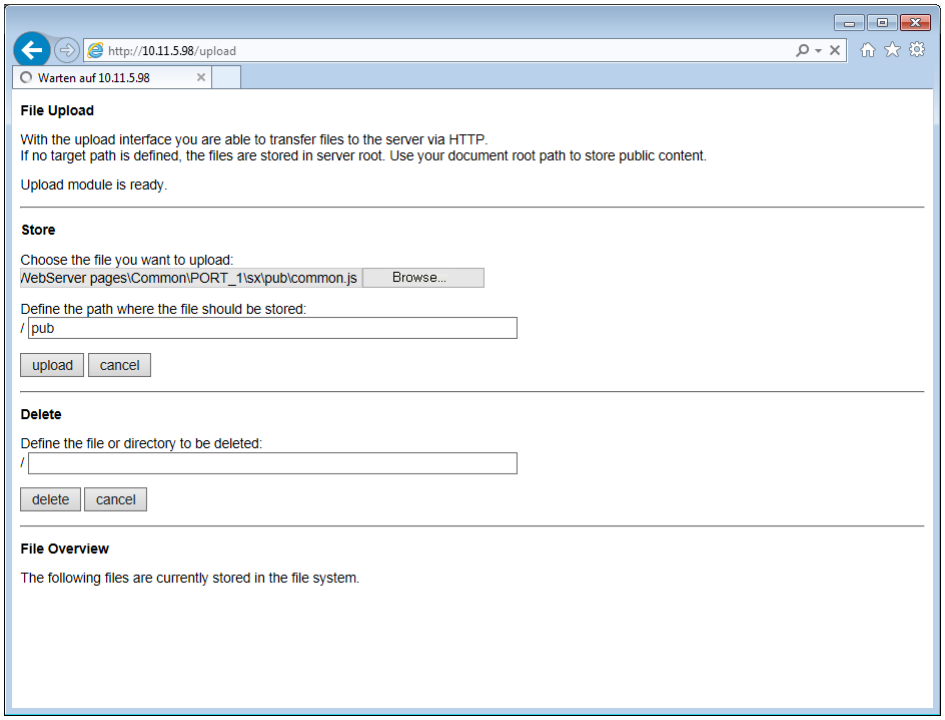

Figure 24: File upload

➢ Click **upload** button.

The WebServer automatically creates the `pub` folder in the `Port_1/sx` directory and uploads and stores the selected file in it.
The **File Overview** shows the uploaded items:

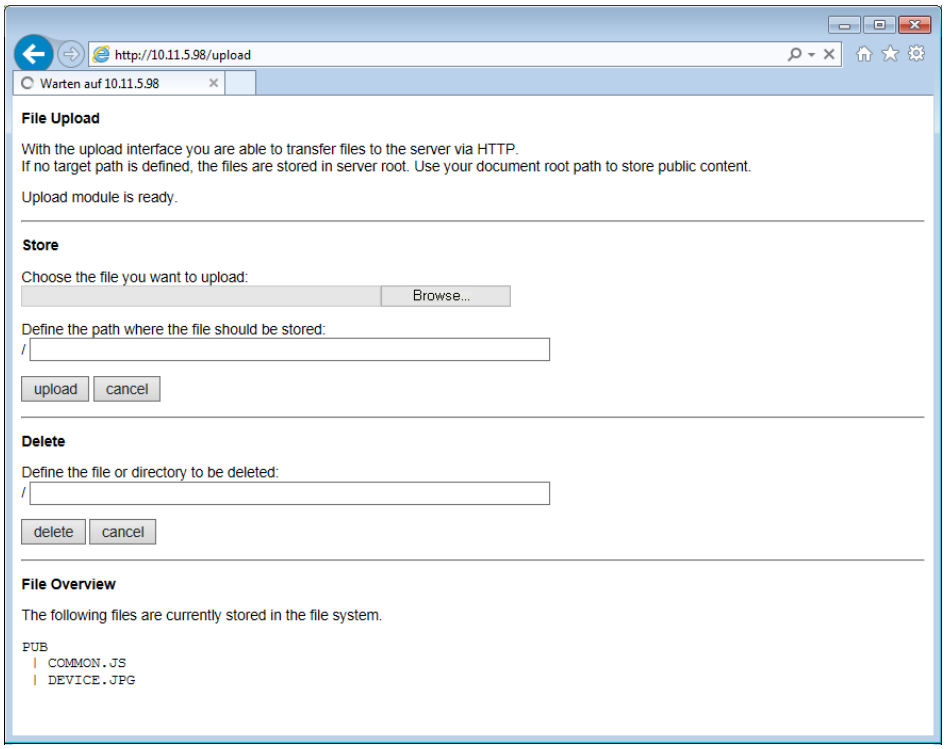

Figure 25: File Overview

➢ Upload all other files from the `Examples and API\[x]. WebServer pages\Common\PORT_1\sx\pub` folder of the netRAPID product DVD to the device. (You must upload each file separately, because the module can upload only one file at a time.)

Note:
The `device.jpg` file is only a proxy. Use the real netRAPID image instead (also called `device.jpg`), which you will find in the `Examples and API\2. WebServer pages\Product \netRAPID\PORT_1\sx\pub` folder on the product DVD.

⇨ After having uploaded all files, you can display the WebServer content by simply entering the IP address of the netRAPID:

Figure 26: Default netRAPID WebServer pages

7 Access to the directories

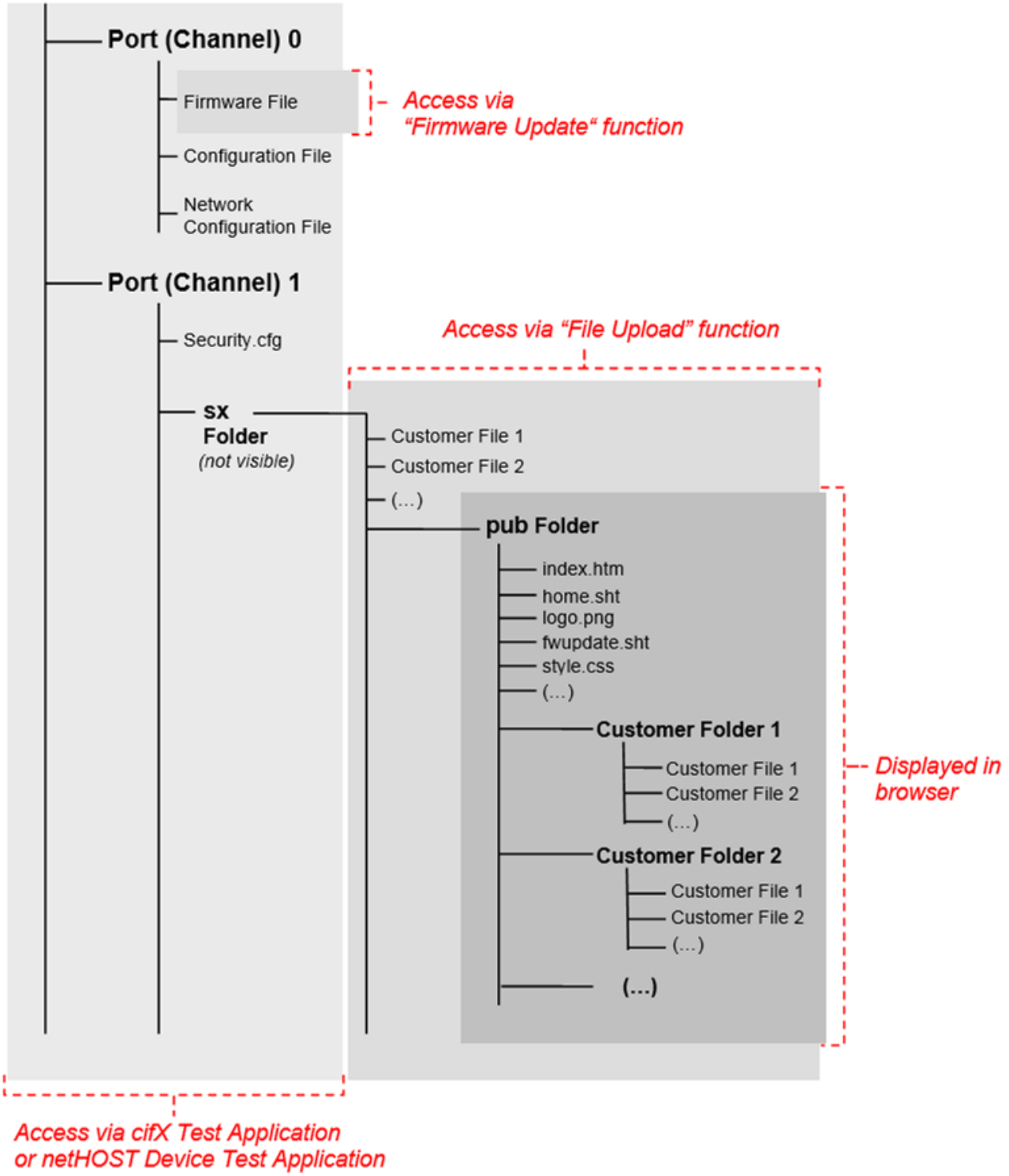

Figure 27: Access to directories

List of figures

List of tables

Contacts

HEADQUARTERS

Germany

Hilscher Gesellschaft für
Systemautomation mbH
Rheinstrasse 15
65795 Hattersheim
Phone: +49 (0) 6190 9907-0
Fax: +49 (0) 6190 9907-50
E-mail: info@hilscher.com

Support

Phone: +49 (0) 6190 9907-99
E-mail: de.support@hilscher.com

SUBSIDIARIES

China

Hilscher Systemautomation (Shanghai) Co. Ltd.
200010 Shanghai
Phone: +86 (0) 21-6355-5161
E-mail: info@hilscher.cn

Support

Phone: +86 (0) 21-6355-5161
E-mail: cn.support@hilscher.com

France

Hilscher France S.a.r.l.
69500 Bron
Phone: +33 (0) 4 72 37 98 40
E-mail: info@hilscher.fr

Support

Phone: +33 (0) 4 72 37 98 40
E-mail: fr.support@hilscher.com

India

Hilscher India Pvt. Ltd.
Pune, Delhi, Mumbai
Phone: +91 8888 750 777
E-mail: info@hilscher.in

Italy

Hilscher Italia S.r.l.
20090 Vimodrone (MI)
Phone: +39 02 25007068
E-mail: info@hilscher.it

Support

Phone: +39 02 25007068
E-mail: it.support@hilscher.com

Japan

Hilscher Japan KK
Tokyo, 160-0022
Phone: +81 (0) 3-5362-0521
E-mail: info@hilscher.jp

Support

Phone: +81 (0) 3-5362-0521
E-mail: jp.support@hilscher.com

Korea

Hilscher Korea Inc.
Seongnam, Gyeonggi, 463-400
Phone: +82 (0) 31-789-3715
E-mail: info@hilscher.kr

Switzerland

Hilscher Swiss GmbH
4500 Solothurn
Phone: +41 (0) 32 623 6633
E-mail: info@hilscher.ch

Support

Phone: +49 (0) 6190 9907-99
E-mail: ch.support@hilscher.com

USA

Hilscher North America, Inc.
Lisle, IL 60532
Phone: +1 630-505-5301
E-mail: info@hilscher.us

Support

Phone: +1 630-505-5301
E-mail: us.support@hilscher.com