



**Application Note**  
**Funktionen des integrierten WebServers**

**Hilscher Gesellschaft für Systemautomation mbH**  
**[www.hilscher.com](http://www.hilscher.com)**

DOC091203AN06DE | Revision 6 | Deutsch | 2017-09 | Freigegeben | Öffentlich

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung.....</b>	<b>3</b>
1.1	Über dieses Dokument .....	3
1.1.1	Inhaltsbeschreibung .....	3
1.1.2	Änderungsübersicht .....	3
1.1.3	Abkürzungen .....	3
1.1.4	Konventionen in diesem Dokument .....	4
1.2	Kurzbeschreibung WebServer .....	5
1.3	Geräte und Firmware mit integriertem WebServer .....	6
<b>2</b>	<b>Zugang zum WebServer .....</b>	<b>7</b>
2.1	Voraussetzungen .....	7
2.2	Seiten des WebServers aufrufen .....	8
<b>3</b>	<b>Funktionen über HTTP .....</b>	<b>9</b>
3.1	Geräte-Parameter anzeigen.....	9
3.2	Firmware-Version anzeigen und Firmware aktualisieren .....	10
3.3	File Upload .....	12
3.4	Reset.....	16
<b>4</b>	<b>Zugangsverwaltung .....</b>	<b>18</b>
4.1	Default-Zugangsverwaltung .....	18
4.2	Eigene Zugangsverwaltung.....	18
4.2.1	Gruppen und Rechte .....	19
4.2.2	Zugangsverwaltungsdatei security.cfg .....	19
4.2.3	Generierung eines Passwort-Hashs mit MD5 .....	20
4.2.4	Zugangsverwaltungsdatei hochladen .....	21
4.2.5	Zugangsverwaltungsdatei löschen.....	23
<b>5</b>	<b>Eigene Inhalte einbinden.....</b>	<b>24</b>
5.1	Übersicht .....	24
5.2	Beispiele für das Einbinden eigener Inhalte .....	26
5.2.1	Beispiel 1: Firmenlogo in der Navigationsleiste austauschen.....	26
5.2.2	Beispiel 2: Design der Navigationsleiste ändern.....	27
5.2.3	Beispiel 3: Neue Webseite einbinden .....	29
<b>6</b>	<b>WebServer-Content auf netRAPID hochladen .....</b>	<b>31</b>
6.1	Übersicht .....	31
6.2	Zugangsverwaltungsdatei per netHOST und USB auf netRAPID hochladen .....	31
6.3	Web-Content per File Upload auf netRAPID hochladen .....	37
<b>7</b>	<b>Zugriff auf Verzeichnisse .....</b>	<b>41</b>
	<b>Abbildungsverzeichnis.....</b>	<b>42</b>
	<b>Tabellenverzeichnis.....</b>	<b>43</b>
	<b>Kontakte.....</b>	<b>44</b>

# 1 Einleitung

## 1.1 Über dieses Dokument

### 1.1.1 Inhaltsbeschreibung

Dieses Dokument beschreibt die HTTP-Funktionen des WebServers für Flash-basierte Real-Time-Ethernet-Kommunikationsmodule von Hilscher. Hier erfahren Sie, wie Sie mit einem Browser funktionale Webseiten aufrufen können, z. B. um eine Firmware zu aktualisieren. Außerdem finden Sie hier Informationen, wie Sie eigene Inhalte in den WebServer einbinden können.

Beachten Sie, dass die Beschreibung der Funktionen des WebServers im netIC DIL-32 Kommunikations-IC nicht Bestandteil dieser Application Note ist. Für den WebServer in netIC-Geräten existiert ein separates Dokument, die Application Note *Funktionen des integrierten WebServers in netIC DIL-32 Kommunikations-IC-Geräten*, DOC140201ANxxDE.

### 1.1.2 Änderungsübersicht

Index	Datum	Änderungen
1	2009-12-21	Dokument erstellt.
2	2010-07-19	Beschreibung der Funktionen erweitert und aktualisiert.
3	2012-02-06	Dokument komplett überarbeitet.
4	2012-02-28	Abschnitt <i>Beispiele für das Einbinden eigener Inhalte</i> [► Seite 26]ergänzt.
5	2013-10-15	Abschnitt <i>Geräte und Firmware mit integriertem WebServer</i> [► Seite 6] aktualisiert.
6	2017-09-19	Dokumentstruktur und Layout überarbeitet. netRAPID NRP 51-RE in Abschnitt <i>Geräte und Firmware mit integriertem WebServer</i> [► Seite 6] aktualisiert. <i>netHOST Device Test Application</i> als Download-Tool ergänzt. Kapitel <i>WebServer-Content auf netRAPID hochladen</i> [► Seite 31] ergänzt.

Tabelle 1: Änderungsübersicht

### 1.1.3 Abkürzungen

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

Tabelle 2: Abkürzungen

## 1.1.4 Konventionen in diesem Dokument

Hinweise, Handlungsanweisungen und Ergebnisse von Handlungen sind wie folgt gekennzeichnet:

### Hinweise



---

**Wichtig:**

<Wichtiger Hinweis>

---



---

**Hinweis:**

<Einfacher Hinweis>

---



---

<Hinweis, wo Sie weitere Informationen finden können>

---

### Handlungsanweisungen

1. <Arbeitsschritt>

➤ <Handlungsanweisung>

➤ <Handlungsanweisung>

2. <Arbeitsschritt>

➤ <Handlungsanweisung>

➤ <Handlungsanweisung>

### Handlungsergebnisse

↷ <Zwischenergebnis>

⇒ <Endergebnis>

## 1.2 Kurzbeschreibung WebServer

Der in die Firmware von Hilscher-Kommunikationsmodulen für Real-Time-Ethernet-Systeme integrierte WebServer ermöglicht es, Statusparameter abzurufen sowie ein Firmware-Update oder ein Reset des Geräts über HTTP durchzuführen. Somit können Sie auf diese Funktionen mittels Standard-Webbrowser und Ethernet-Schnittstelle zugreifen.

Außerdem können Sie mittels File-Upload eigene Webseiten und Grafiken (z. B. Ihr Firmenlogo) auf dem WebServer hinterlegen und dadurch das Design der vom WebServer angezeigten Seiten nach Ihren Wünschen gestalten. Die HTTP-Funktionen des WebServers bleiben davon unberührt.

Der WebServer unterstützt ferner eine Benutzer- und Passwort-Verwaltung mit MD5-Kodierung. Eine Konfigurationsdatei (`security.cfg`), welche die Benutzer, Gruppen und Passwort-Definitionen enthält, kann mit der *cifX Test Applikation* oder der *netHOST Device Test Application* auf den WebServer geladen werden.



---

### Hinweis:

Die Kommunikationsmodule **comX**, **netIC** und **netJACK** werden mit vorinstalliertem WebServer-Content (`Security.cfg`, HTML-Seiten, Grafiken, Stylesheet etc.) ausgeliefert; d. h. Sie können sich deren WebServer-Seiten sofort nach der Inbetriebnahme der Module anzeigen lassen.

Der **netRAPID NRP 51-RE** hingegen wird ohne vorinstallierten WebServer-Content ausgeliefert, daher müssen Sie nach der Inbetriebnahme des netRAPIDs (nach dem Firmware-Download und der Konfiguration) die Dateien für den WebServer zunächst selber in das Gerät übertragen. Als netRAPID-Nutzer lesen Sie daher bitte zuerst das Kapitel *WebServer-Content auf netRAPID hochladen* [► Seite 31].

---

## 1.3 Geräte und Firmware mit integriertem WebServer

Der WebServer steht in folgenden Hilscher-Geräten für Real-Time-Ethernet-Systeme und folgender Firmware zur Verfügung:

Produktfamilie	Artikelbezeichnung	Protokoll	Firmware	Unterstützt ab 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	Siehe Application Note <i>Funktionen des integrierten WebServers in netIC DIL-32 Kommunikations-IC-Geräten</i> , DOC140201ANxxDE			
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

Tabelle 3: Liste der Geräte und Firmware mit integriertem WebServer

## 2 Zugang zum WebServer

### 2.1 Voraussetzungen

- Die Firmware des Kommunikationsmoduls muss mit der WebServer-Funktionalität ausgestattet sein. Die entsprechenden Module und Firmware finden Sie im Abschnitt *Geräte und Firmware mit integriertem WebServer* [► Seite 6].
- Das Kommunikationsmodul ist betriebsbereit.
- Das Kommunikationsmodul ist über seine Ethernet-Schnittstelle mit einem Netzwerk verbunden.
- Sie verfügen über einen PC mit Verbindung zum Netzwerk und einen Webbrowser. Der WebServer wurde mit folgenden Browser-Versionen getestet:

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

Tabelle 4: Getestete Browser-Versionen für WebServer

- Sie müssen die Adresse Ihres Kommunikationsmoduls sowie einen gültigen Benutzernamen mit Passwort kennen. Informationen zu Benutzernamen und Passwörtern finden Sie im Kapitel *Zugangsverwaltung* [► Seite 18].
- Falls Sie eine eigene Zugangsverwaltung betreiben möchten, benötigen Sie zum Hochladen der Zugangsverwaltungsdatei einen PC mit installierter cifX Test Applikation sowie ein passendes Evaluation Board, mit dem Sie Ihr Kommunikationsmodul mit dem PC verbinden können. Weitere Informationen hierzu finden Sie im Abschnitt *Eigene Zugangsverwaltung* [► Seite 18].



#### Hinweis:

Die Kommunikationsmodule **comX**, **netIC** und **netJACK** werden mit vorinstalliertem WebServer-Content (Security.cfg, HTML-Seiten, Grafiken, Stylesheet etc.) ausgeliefert; d. h. Sie können sich deren WebServer-Seiten sofort nach der Inbetriebnahme der Module anzeigen lassen.

Der **netRAPID NRP 51-RE** hingegen wird ohne vorinstallierten WebServer-Content ausgeliefert, daher müssen Sie nach der Inbetriebnahme des netRAPIDs (nach dem Firmware-Download und der Konfiguration) die Dateien für den WebServer zunächst selber in das Gerät übertragen. Als netRAPID-Nutzer lesen Sie daher bitte zuerst das Kapitel *WebServer-Content auf netRAPID hochladen* [► Seite 31].

## 2.2 Seiten des WebServers aufrufen

Sie rufen den WebServer auf, indem Sie die IP-Adresse des Kommunikationsmoduls in die Adresszeile Ihres Webbrowsers eingeben.

**Hinweis:**

Die IP-Adresse wird dem Kommunikationsmodul i. d. R. bei seiner Konfiguration mittels SYCON.net oder netX Configuration Tool zugewiesen. Nähere Informationen hierzu finden Sie im Bediener Manual des DTM für das entsprechende Protokoll.

Nach Eingabe der IP-Adresse gelangen Sie zunächst auf die Startseite (Homepage) des WebServers. Von dort können Sie über Links die anderen Seiten aufrufen.

Sie können die Webseiten auch aufrufen, indem Sie deren URL in der Adresszeile Ihres Browsers eingeben:

Webseite	Funktion	URL in Browser
Home	Geräte-Parameter anzeigen	http://<IP-Adresse>
Firmware Update	Firmware-Version anzeigen / Firmware aktualisieren	http://<IP-Adresse>/fwupdate.sht
File Upload	Datei hochladen oder löschen	http://<IP-Adresse>/upload.sht
Reset	Geräte-Reset	http://<IP-Adresse>/reset.sht

Tabelle 5: Übersicht der Webseiten und deren URLs

Alternativ können Sie die rein funktionalen Webseiten des WebServers, d. h. diejenigen HTML-Seiten, die lediglich die HTTP-Funktionen und keine Navigationsleiste oder Grafiken enthalten, direkt aufrufen, indem Sie folgende URL in der Adresszeile Ihres Browsers eingeben:

Funktion	URL in Browser
Firmware-Version anzeigen / Firmware aktualisieren	http://<IP-Adresse>/fwupdate
Datei hochladen oder löschen	http://<IP-Adresse>/upload
Geräte-Reset	http://<IP-Adresse>/reset

Tabelle 6: HTTP-Funktionen direkt aufrufen



## 3 Funktionen über HTTP

### 3.1 Geräte-Parameter anzeigen

Die Startseite des WebServers zeigt Ihnen Parameter zur Identifikation Ihres Gerätes.

Sie gelangen auf die Startseite, indem Sie die URL `http://<IP-Adresse>` in die Adresszeile Ihres Browsers eingeben.

Nach dem Wechsel auf andere Seiten des WebServers gelangen Sie in der Navigationsleiste durch Anklicken der Schaltfläche **Home** wieder auf die Startseite zurück.



#### 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

Abbildung 1: Startseite WebServer (Darstellung im Internet Explorer, kann in anderen Browsern abweichen)

## 3.2 Firmware-Version anzeigen und Firmware aktualisieren

Auf der Seite **Firmware Update** sehen Sie die aktuell geladene Firmware-Version und können eine neue Firmware-Datei in Ihr Gerät laden.

Sie gelangen auf die Firmware-Seite, indem Sie die Schaltfläche **Firmware Update** in der Navigationsleiste anklicken oder die URL `http://<IP-Adresse>/fwupdate.sht` in die Adresszeile Ihres Browsers eingeben.



### Hinweis:

Diese Seite wird standardmäßig durch eine Passwort-Abfrage geschützt. Näheres hierzu finden Sie im Abschnitt *Zugangsverwaltung* [► Seite 18].

Channel	Name	Version	Date
0	EtherNet/IP Scanner	2.4.9.1	13.10.2011

Abbildung 2: Firmware Update (Darstellung im Internet Explorer, kann in anderen Browsern abweichen)



### Hinweis:

Bei einem Firmware-Update müssen die gewählte Firmware und das Gerät zueinander passen; d. h. Sie können z. B. keine EtherNet/IP Scanner (Master) Firmware auf einen netJACK 50 mit netX 50 Chip laden. Vor einem Update findet eine automatische Kompatibilitätsprüfung statt. Dabei werden z. B. Geräteklasse und Hardware-Eigenschaften geprüft.

## Firmware Identification

Im Bereich **Firmware Identification** werden folgende Parameter der aktuell im Gerät vorhandenen Firmware angezeigt:

- **Channel:** Kanalnummer (Channel bzw. Port)
- **Name:** Name der geladenen Firmware
- **Version:** Firmware-Version
- **Date:** Datum der Firmware

## Firmware Update

Im Bereich **Firmware Update** können Sie eine Firmware-Datei zum Upload in das Gerät auswählen und den Upload starten.

Klicken Sie die Schaltfläche **Durchsuchen**, um einen Dialog zur Auswahl der Datei zu öffnen. Pfad und Name der gewählten Datei werden im nebenstehenden Feld angezeigt.



### Hinweis:

Firmware-Dateien haben immer die Dateinamenserweiterung `.nxf`.

Bedienelement	Funktion
Anzeigefeld	Zeigt ausgewählte Datei mit Pfad.
Durchsuchen	Öffnet den Dateiauswahl-Dialog.
Transfer	Überträgt die ausgewählte Firmware-Datei zum Gerät.
Cancel	Bricht das Firmware-Update ab und löscht Inhalt des Anzeigefelds.

Tabelle 7: Bedienelemente Firmware-Update

## ACHTUNG

### Geräteschaden durch Unterbrechung des Datei-Transfers

Unterbrechen Sie keinesfalls die Spannungsversorgung und ziehen Sie nicht das Netzkabel während des Transfers der Firmware-Datei. Wenn der Strom zum Zeitpunkt des Umschaltens von der alten zur schon gespeicherten neuen Firmware ausfällt, kann dies schwere Fehlfunktionen des Geräts zur Folge haben.

Nach dem Start des Uploads mit der Schaltfläche **Transfer** wird die Validität der Datei geprüft. Wird die Datei abgelehnt, erscheint eine Fehlermeldung, wird die Datei akzeptiert, erscheint die Meldung **Transfer succeeded**.

Nach erfolgreichem Transfer müssen Sie einen Reset ausführen, um die neue Firmware zu starten. Sehen Sie hierzu den Abschnitt **Reset** [► Seite 16].

### 3.3 File Upload

Auf der Seite **File Upload** können Sie Dateien in das per HTTP zugängliche Verzeichnis des WebServers laden sowie Dateien löschen. Außerdem können Sie hier sehen, welche Ordner und Dateien sich in dem Verzeichnis befinden.

Sie gelangen auf die Upload-Seite, indem Sie die Schaltfläche **File Upload** in der Navigationsleiste anklicken oder die URL `http://<IP-Adresse>/upload.sht` in die Adresszeile Ihres Browsers eingeben.

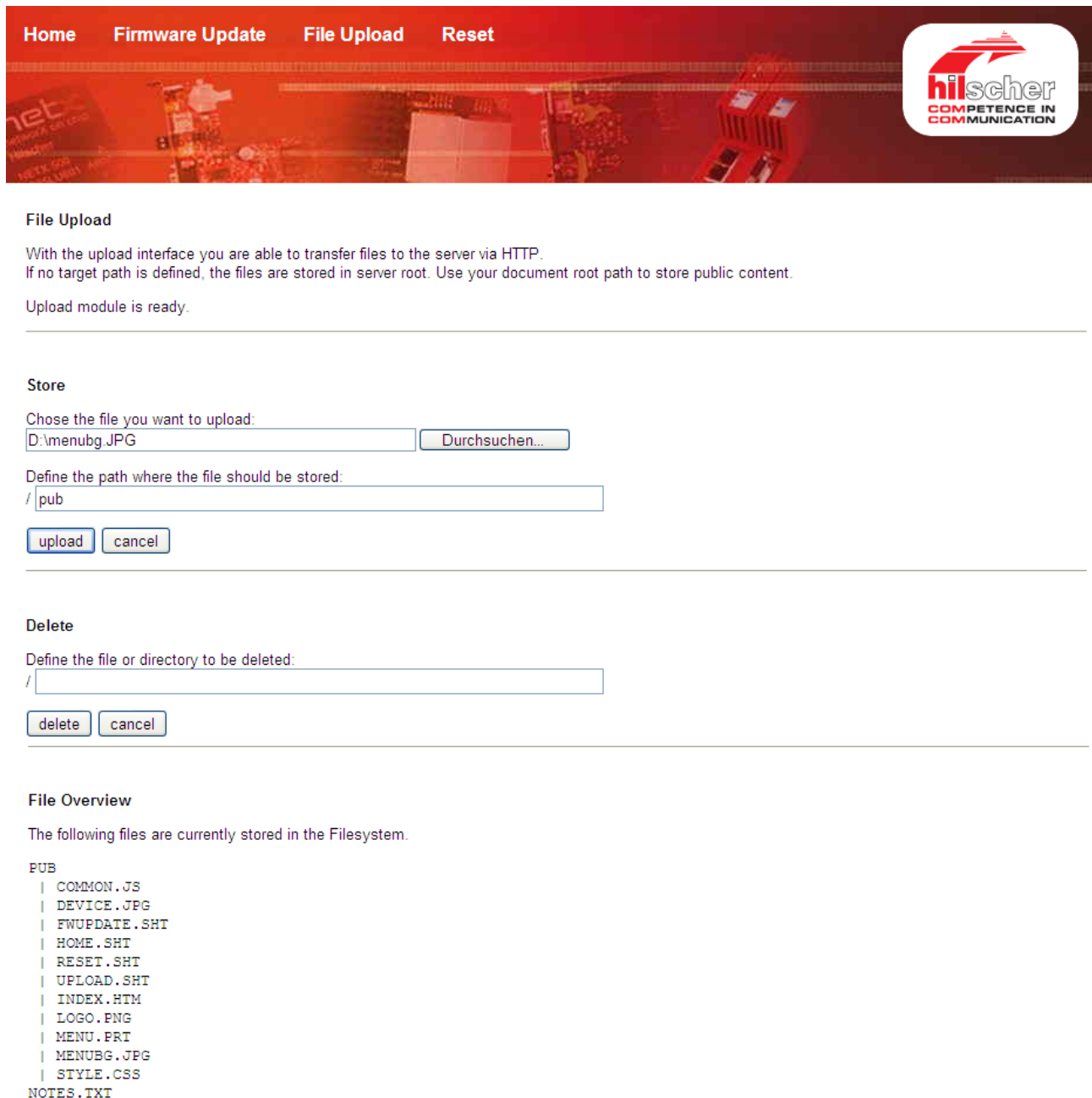


---

**Hinweis:**

Diese Seite wird standardmäßig durch eine Passwort-Abfrage geschützt. Näheres hierzu finden Sie im Abschnitt *Zugangsverwaltung* [► Seite 18].

---



**Home**   **Firmware Update**   **File Upload**   **Reset**

**hilscher**  
COMPETENCE IN  
COMMUNICATION

---

### File Upload

With the upload interface you are able to transfer files to the server via HTTP.  
If no target path is defined, the files are stored in server root. Use your document root path to store public content.

Upload module is ready.

---

#### Store

Chose the file you want to upload:

Define the path where the file should be stored:

---

#### Delete

Define the file or directory to be deleted:

---

#### File Overview

The following files are currently stored in the Filesystem.

PUB

- | COMMON.JS
- | DEVICE.JPG
- | FWUPDATE.SHT
- | HOME.SHT
- | RESET.SHT
- | UPLOAD.SHT
- | INDEX.HTM
- | LOGO.PNG
- | MENU.PRT
- | MENUBG.JPG
- | STYLE.CSS

NOTES.TXT

Abbildung 3: File Upload (Darstellung im Internet Explorer, kann in anderen Browsern abweichen)

### Store

Im Bereich **Store** können Sie eine Datei zum Upload auf den WebServer auswählen und den Upload starten. Beachten Sie dabei folgendes:

- Es kann immer nur eine Datei, nicht mehrere gleichzeitig übertragen werden.
- Der Name der Datei darf nicht länger als acht Zeichen sein (8.3 Namenskonvention), ansonsten wird die Datei nicht gespeichert.
- Die Gesamtgröße des Uploads sollte ein Megabyte nicht überschreiten.
- Wenn eine Datei gleichen Namens auf dem WebServer bereits vorhanden ist, wird diese ohne Warnhinweis überschrieben.

Klicken Sie die Schaltfläche **Durchsuchen**, um einen Dialog zur Auswahl der Datei zu öffnen. Pfad und Name der gewählten Datei werden im nebenstehenden Feld angezeigt.

Geben Sie in das Feld **Define the path...** das Verzeichnis des öffentlichen Ordners `pub` ein und klicken Sie anschließend die Schaltfläche **Upload**. Sie können einen neuen Unterordner anlegen, indem Sie ihn als Teil des Zielpfades eingeben, z. B. `pub/myfolder`.

**Hinweis:**

Der File Upload kann nur auf das Verzeichnis `Port_1/sx` und die darunter liegenden Ordner zugreifen. Der Pfad `Port_1/sx` ist im File Upload bereits voreingestellt. Die Webseiten und Grafiken, die der WebServer anzeigen kann, liegen in diesem Verzeichnis im „öffentlichen“ Ordner `pub` (Pfad: `Port_1/sx/pub`). Wenn Sie eigene Webseiten oder Grafiken in den WebServer einbinden und anzeigen lassen möchten, müssen Sie diese in diesem öffentlichen Ordner ablegen. Da der Pfad `Port_1/sx` im File Upload bereits voreingestellt ist, brauchen Sie hierzu im Feld **Define the path...** nur den Namen des öffentlichen Ordners `pub` einzugeben. Wenn Sie den öffentlichen Ordner `pub` nicht angeben und das Feld leer lassen, werden die hochgeladenen Dateien eine Ebene höher im Verzeichnis `Port_1/sx` abgelegt und können somit später auch nicht im Browser angezeigt werden.

Wenn Sie dies wünschen, können Sie Dateien auf dem WebServer also quasi „verstecken“, indem Sie diese im Verzeichnis `Port_1/sx` ablegen.

Eine Grafik mit den relevanten Verzeichnissen des WebServers und den Zugriffsmöglichkeiten finden Sie im Kapitel *Zugriff auf Verzeichnisse* [► Seite 41].

Bedienelement	Funktion
Anzeigefeld	Zeigt ausgewählte Datei mit Pfad.
Durchsuchen	Öffnet den Dateiauswahl-Dialog.
Eingabefeld	Manuelle Eingabe des Ziel-Verzeichnisses.
Upload	Überträgt die ausgewählte Datei zum WebServer.
Cancel	Bricht den Transfer ab und löscht Inhalt des Anzeige-Felds.

Tabelle 8: Bedienelemente Datei-Upload

**Hinweis:**

Sie können den File Upload nicht für ein Firmware Update verwenden, da der File Upload nur auf das Verzeichnis `Port_1/sx` und die darunter liegenden Ordner zugreifen kann, Firmware aber im `Port_0` gespeichert wird. Zum Upload einer Firmware-Datei müssen Sie die Funktion **Firmware Update** verwenden, wie im Abschnitt *Firmware-Version anzeigen und Firmware aktualisieren* [► Seite 10] beschrieben.

Ebenso wenig können Sie den File Upload zum Upload der Benutzer- und Passwort-Datei `security.cfg` verwenden, da diese Datei direkt im Root-Verzeichnis von `Port_1` gespeichert werden muss, auf das der File Upload keinen Zugriff hat. Zum Upload der Datei `security.cfg` müssen Sie die *cifX Test Applikation* oder die *netHOST Device Test Application* verwenden. Sehen Sie hierzu auch die Abschnitte *Zugangsverwaltungsdatei hochladen* [► Seite 21] bzw. *Zugangsverwaltungsdatei per netHOST und USB auf netRAPID hochladen* [► Seite 31].

**Delete**

Im Bereich **Delete** können Sie eine Datei oder einen Ordner vom WebServer löschen.

Geben Sie in das Feld den Pfad der Datei oder des Ordners ein, den Sie löschen möchten. Sie können nur Elemente löschen, die sich im Verzeichnis `Port_1/sx/` oder darunter befinden.

Bedienelement	Funktion
Eingabefeld	Manuelle Eingabe des Pfads der zu löschenden Elemente.
Delete	Löscht die ausgewählten Elemente vom WebServer.
Cancel	Bricht die Aktion ab und löscht Inhalt des Eingabefelds.

Tabelle 9: Bedienelemente Dateien löschen

**File Overview**

Im Bereich **File Overview** sehen Sie die Ordner und Dateien, die sich im Verzeichnis `Port_1/sx` (also im für den **File Upload** zugänglichen Verzeichnis des WebServers) befinden.

**Hinweis:**

Alle Buchstaben werden als Großbuchstaben angezeigt. Falls ein Dateiname ein Leerzeichen enthält, wird nur der Teil des Dateinamens angezeigt, der sich **vor** dem Leerzeichen befindet. Beispiel: Die Datei `my file.txt` wird als `MY.TXT` angezeigt.

## 3.4 Reset

Auf der Seite **Reset** können Sie ein Reset für Ihr Kommunikationsmodul durchführen.

Sie gelangen auf die Reset-Seite, indem Sie die Schaltfläche **Reset** in der Navigationsleiste anklicken oder die URL `http://<IP-Adresse>/reset.sht` in die Adresszeile des Browsers eingeben.

**Hinweis:**

Diese Seite wird standardmäßig durch eine Passwort-Abfrage geschützt. Näheres hierzu finden Sie im Abschnitt *Zugangsverwaltung* [► Seite 18].

Home Firmware Update File Upload Reset

**Device Reset**

The device is being restarted by a hardware reset: **All communication is stopped** immediately and connections are interrupted or timeout!

In order to avoid any damage, make sure that your system is in a secure operation before you submit the reset!  
Ethernet connection may be lost if IP parameters are not stored permanently!  
All parameters that are not stored permanently get lost.

☒ Please confirm you want to reset the device.

Submit Cancel

Abbildung 4: Reset (Darstellung im Internet Explorer, kann in anderen Browsern abweichen)

Ein Reset muss nach einem Firmware-Update oder einer Neukonfigurierung des Geräts durchgeführt werden und hat folgende Auswirkungen:

- Die Firmware wird neu gestartet und alle bestehenden Verbindungen werden unterbrochen oder führen zu einem Timeout.
- Die E/A-Kommunikation am Bus wird unterbrochen.
- Die IP-Verbindung kann verloren gehen, wenn die IP-Parameter nicht mittels SYCON.net oder dem netX Configuration Tool definiert und permanent im Gerät abgespeichert wurden.

**Hinweis:**

Wenn Sie einen Reset ausführen und die IP-Parameter nicht permanent gespeichert waren oder wenn Sie das Gerät auf ein anderes Ethernet-Protokoll umgestellt haben, müssen Sie dem Gerät seine IP-Adresse mit Hilfe eines geeigneten Tools neu zuordnen, bevor Sie wieder auf den WebServer zugreifen können.



Aktivieren Sie die Checkbox vor **Please confirm...**, um zu bestätigen, dass Sie ein Reset durchführen möchten. Um den Reset zu starten, klicken Sie anschließend die Schaltfläche **Submit**.  
Die Schaltfläche **Cancel** entfernt das Häkchen aus der Checkbox vor **Please confirm...** wieder.

## 4 Zugangsverwaltung

### 4.1 Default-Zugangsverwaltung

Der Zugriff auf die Funktionen **Firmware Update**, **File Upload** und **Reset** ist standardmäßig durch eine Nutzer-Authentifizierung geschützt.

Wenn Sie eine der oben genannten Funktionen aufrufen, erscheint ein Passwort-Dialog. Die Default-Zugangsparameter für sämtliche Funktionen sind:

**Benutzername:** admin

**Kennwort:** admin

Diese Default-Zugangsparameter gelten solange, bis Sie eine Zugangsverwaltungsdatei `security.cfg` mit einem neuen Kennwort für den Benutzer `admin` auf dem WebServer im Root-Verzeichnis von `Port_1` hinterlegt haben.

### 4.2 Eigene Zugangsverwaltung

Sie können eine eigene Zugangsverwaltung für den WebServer einrichten. Hierzu können Sie Benutzer und deren Rechte-Gruppen sowie Passwörter in einer Textdatei definieren und als Zugangsverwaltungsdatei `security.cfg` im Root-Verzeichnis von `Port_1` auf dem WebServer hinterlegen. Dabei müssen Passwörter als MD5-Code/Hash eingetragen werden. Zur Erzeugung des MD5-Codes können Sie einen beliebigen, als Freeware oder Online-Tool erhältlichen, externen MD5 Generator verwenden.

Zum Hochladen oder Löschen der Zugangsverwaltungsdatei müssen Sie die *cifX Test Applikation* oder die *netHOST Device Test Application* verwenden.

Sobald Sie eine Zugangsverwaltungsdatei `security.cfg` auf den WebServer geladen haben, gelten die darin enthaltenen Zugangsberechtigungen, und die Parameter der Default-Zugangsverwaltung sind außer Kraft gesetzt.



---

**Wichtig:**

Achten Sie darauf, dass Sie in der Zugangsverwaltungsdatei einen Benutzer `admin` mit einem neuen Kennwort anlegen, um die alten Default-Zugangsparameter (`admin / admin`) außer Kraft zu setzen und den Zugang zum WebServer wirkungsvoll zu schützen. Ist kein Benutzer `admin` in der Zugangsverwaltungsdatei enthalten, gelten zusätzlich zu den anderen in der Zugangsverwaltungsdatei enthaltenen Zugangsberechtigungen weiterhin die alten Default-Zugangsparameter für den `admin`.

---

Das Löschen der `security.cfg` setzt die Zugangsverwaltung wieder auf die Default-Zugangsparameter zurück.

## 4.2.1 Gruppen und Rechte

Zugriffsrechte auf Funktionen des WebServers sind an Rechte-Gruppen gekoppelt.

Folgende Rechte-Gruppen sind zur Zeit auf dem WebServer eingerichtet:

Rechte-Gruppe	Funktion
reset	erlaubt ein Reset des Geräts
firmware	erlaubt die Aktualisierung der Firmware des Geräts
upload	erlaubt Speichern und Löschen von Dateien im Verzeichnis <code>Port_1/sx</code>

Tabelle 10: Gruppen und deren Rechte

Die Zuordnung der Rechte-Gruppe zu einem Benutzernamen erfolgt dadurch, dass in der Zugangsverwaltungsdatei die Rechte-Gruppen in der gleichen Zeile hinter dem Benutzernamen und dem MD5 Passwort-Hash aufgelistet werden. Einem Nutzer können mehrere Rechte-Gruppen zugewiesen sein.



### Hinweis:

Der User `admin` ist immer automatisch Mitglied in allen drei Rechte-Gruppen `reset`, `firmware` und `upload`; auch wenn dem `admin` diese Rechte-Gruppen nicht explizit zugewiesen wurden.

## 4.2.2 Zugangsverwaltungsdatei `security.cfg`

In der Zugangsverwaltungsdatei `security.cfg` können Sie mit Hilfe eines einfachen Text-Editors neue Benutzer eintragen, einem Benutzer Rechte-Gruppen zuweisen, sowie ein Passwort in Form eines MD5-Hash eintragen.

Die ASCII-Textdatei beginnt mit der Angabe des Realm, danach folgen die Zeilen mit den Parametern der Benutzer. Eine Zeile enthält jeweils die Parameter eines einzelnen Benutzers. Dabei ist folgende Syntax zu beachten:

```
<Benutzername>;<MD5-Hash aus
Benutzername:Realm:Passwort>;<Rechte-Gruppe1>,<Rechte-
Gruppe2>;
```

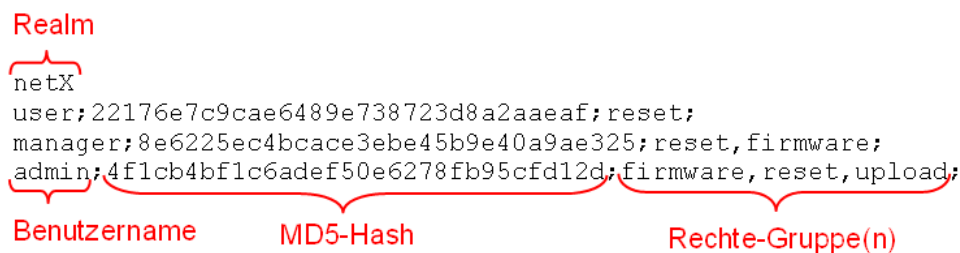
Auf der Produkt-DVD finden Sie unter

Examples & API > [x]. WebServer pages > Common > Port\_1 die Beispieldatei `security.cfg`, die Sie als Vorlage für ihre eigene Zugangsverwaltungsdatei verwenden und abändern können. Die Datei enthält bereits die drei vordefinierten Benutzer `user`, `manager` und `admin` mit folgenden Passwörtern und Rechten:

Benutzername	Passwort	Rechte-Gruppe
user	user	reset
manager	manager	reset, firmware
admin	admin	firmware, reset, upload

Tabelle 11: Benutzer-Passwort-Rechte-Matrix der Beispieldatei `security.cfg`

Diese Zuordnungen werden in der `security.cfg` mit den folgenden Zeichenketten realisiert:



The diagram shows a sample entry from a `security.cfg` file:
 

```
netX
user;22176e7c9cae6489e738723d8a2aaeaf;reset;
manager;8e6225ec4bcace3ebe45b9e40a9ae325;reset,firmware;
admin;4f1cb4bf1c6adef50e6278fb95cfd12d;firmware,reset,upload;
```

 Red curly brackets are used to group parts of the entry:
 

- A bracket above `netX` is labeled **Realm**.
- A bracket below `admin` is labeled **Benutzername**.
- A bracket below the long alphanumeric string `4f1cb4bf1c6adef50e6278fb95cfd12d` is labeled **MD5-Hash**.
- A bracket below `firmware,reset,upload` is labeled **Rechte-Gruppe(n)**.

Abbildung 5: Zeichenketten in Beispieldatei `security.cfg`

### 4.2.3 Generierung eines Passwort-Hashs mit MD5

Passwörter müssen in der Zugangsverwaltungsdatei als MD5-Hash hinterlegt werden. Sie können den Passwort-Hash mit jedem beliebigen MD5-Generator erzeugen und anschließend die erzeugte Zeichenkette in die entsprechende Zeile der Zugangsverwaltungsdatei `security.cfg` hineinkopieren.

Der MD5-Hash muss mit folgenden Parametern in folgender Syntax erzeugt werden:

```
<Benutzername>:<Realm>:<Passwort>
```

Für eine Nutzerin Hildegard Mustermann mit dem Passwort „Sommertag“ müssten Sie somit folgende Zeichenkette in den MD5-Generator eingeben:

```
Hildegard Mustermann:netX:Sommertag
```

Aus dieser Zeichenkette erzeugt der Generator den Hash  
`dc45c059135e49461f90bcc08bcb266d`.

Beachten Sie folgende Hinweise zu Benutzernamen und Passwörtern:

- Sie dürfen alle druckbaren ASCII-Zeichen und das Leerzeichen verwenden (ASCII-Zeichen 32 [dec] bis 126 [dec]), für den Benutzernamen jedoch kein Semikolon (;), da das Semikolon in der Zugangsverwaltungsdatei als Trennzeichen fungiert.
- Sie dürfen keine diakritischen Zeichen wie Umlaute (ä, ü, ö) oder Akzente (é, è, ê) und kein Eszett (ß) verwenden.
- Groß- und Kleinschreibung werden unterschieden.
- Die Schreibweise des Benutzernamens, die Sie im MD5-Generator und später im Anmelde-Dialog des WebServers verwenden, muss mit der Schreibweise in der Zugangsverwaltungsdatei übereinstimmen (z. B. in Hinblick auf Leerzeichen zwischen Vor- und Nachnamen).
- Die Schreibweise des Passworts, die Sie im MD5-Generator verwenden, muss mit der Schreibweise übereinstimmen, die Sie im Anmelde-Dialog des WebServers verwenden.

## 4.2.4 Zugangsverwaltungsdatei hochladen

Die Zugangsverwaltungsdatei `security.cfg` muss im Root-Verzeichnis von `Port_1` des Systems gespeichert werden.

Da der **File Upload** des WebServers nur auf das Verzeichnis `Port_1/sx` zugreifen kann, nicht aber auf das Root-Verzeichnis von `Port_1`, müssen Sie zum Hochladen der Zugangsverwaltungsdatei die Hilscher *cifX Test Applikation* oder die *netHOST Device Test Application* verwenden. Nachfolgend ist die Verfahrensweise mit der *cifX Test Applikation* beschrieben.

Die *cifX Test Applikation*, die Bestandteil des cifX Device Drivers für Windows ist, ermöglicht einen Zugriff auf das Kommunikationsmodul über dessen Host-Schnittstelle. Dazu müssen Sie das Kommunikationsmodul mit Hilfe eines Evaluation Boards in einen PC einbauen, bzw. mit einem PC verbinden, auf dem die cifX Test Applikation installiert ist. Nähere Informationen zum Einsatz von Evaluation Boards finden Sie in dem Benutzerhandbuch zu Ihrem Kommunikationsmodul.

### Schrittanleitung Zugangsverwaltungsdatei hochladen

1. cifX Test Applikation starten.
  - Doppelklicken Sie im Startmenü von Windows® den Eintrag **Systemsteuerung > cifX Test**.
  - Die cifX Test Applikation öffnet sich.
2. Channel1 des Geräts in der cifX Test Applikation öffnen.
  - Wählen Sie in der Menüleiste **Device > Open**
  - Der Dialog **Channel Selection** öffnet sich.
  - Markieren Sie im linken Fenster den Eintrag **Channel1** und klicken Sie anschließend die Schaltfläche **Open**.

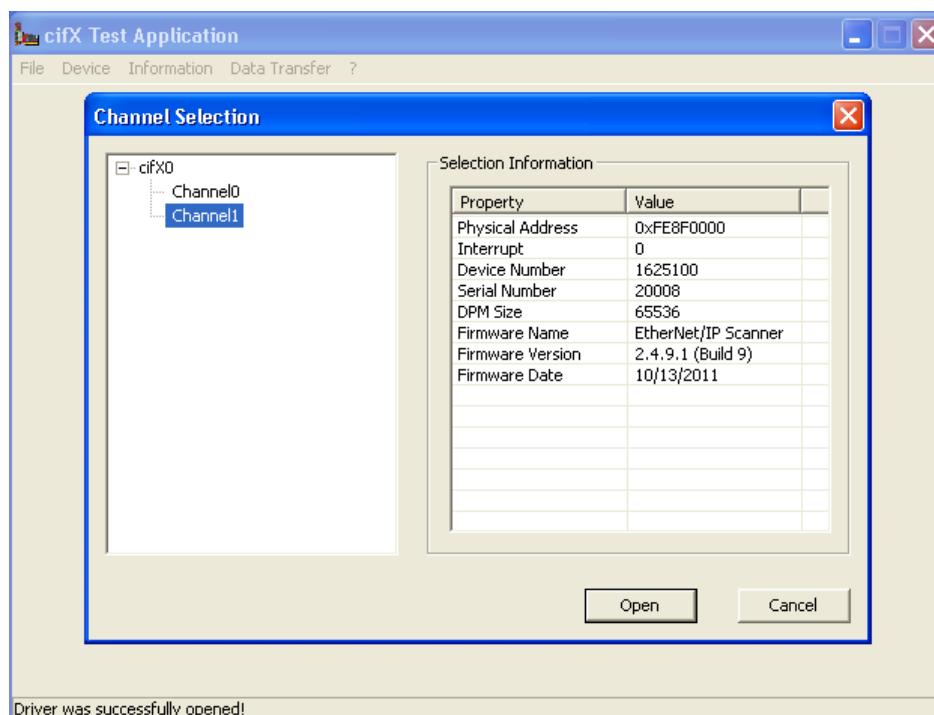



Abbildung 6: Auswahl des Channel in cifX Test Applikation

- ⇒ Der Port ist geöffnet und der Dialog **Channel Selection** schließt sich wieder.
- 3. Zugangsverwaltungsdatei auswählen.
  - Wählen Sie in der Menüleiste **Device > Download**.
  - ⇒ Das Fenster **Download Test** öffnet sich.
  - Wählen Sie in der Dropdown-Liste **Download Mode** den Eintrag **File Download**.
  - Klicken Sie in der Zeile **Filename** auf die Schaltfläche , um den Dateiauswahl-Dialog zu öffnen.
  - Wählen Sie im Dateiauswahl-Dialog die Datei `security.cfg` auf Ihrem Dateisystem und klicken Sie anschließend die Schaltfläche **Öffnen**.
  - ⇒ Der Dateiauswahl-Dialog schließt sich wieder.
- 4. Zugangsverwaltungsdatei übertragen.

**Hinweis:**

Beachten Sie, dass eine bereits auf dem Gerät vorhandene `security.cfg` beim Download überschrieben wird, ohne dass Sie eine Warnmeldung erhalten.

Die in den Root-Verzeichnissen des Geräts gespeicherten Dateien können Sie sich in der cifX Test Applikation unter **Device > File Explorer** anzeigen lassen und gegebenenfalls auf Ihr lokales System herunterladen (öffnen Sie vorher den entsprechenden Port bzw. Channel).

- Klicken Sie die Schaltfläche **Download**, um die Zugangsverwaltungsdatei in das Gerät zu übertragen.

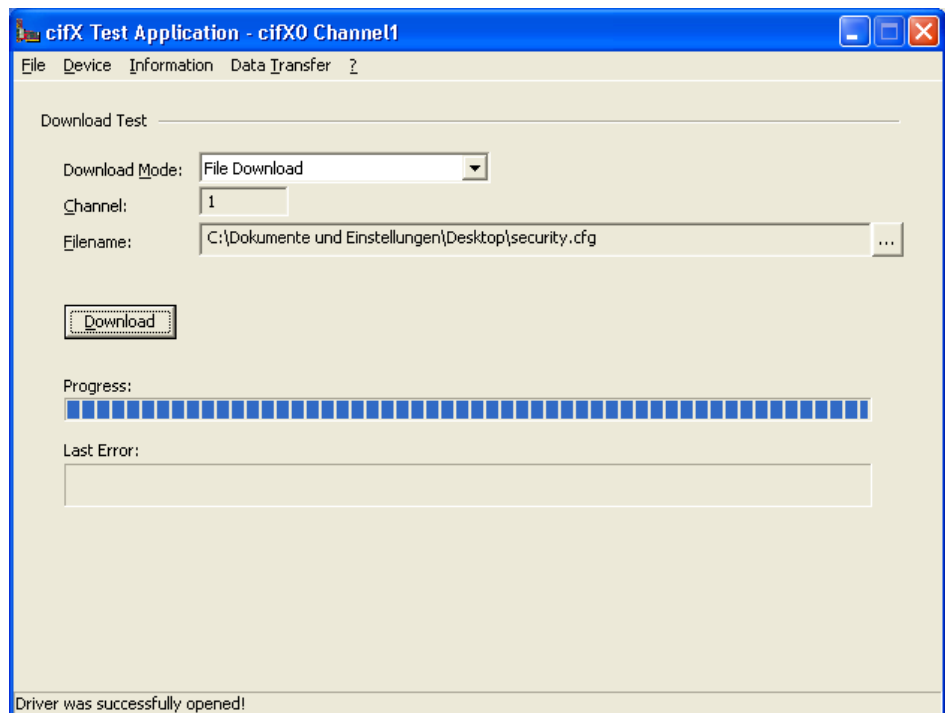


Abbildung 7: Zugangsverwaltungsdatei übertragen

- ⇒ Sie haben die Zugangsverwaltungsdatei in das Gerät übertragen.

**Hinweis:**

Um die neue Zugangsverwaltungsdatei zu aktivieren, müssen Sie ein Reset auf dem Gerät ausführen. In der *cifX Test Applikation* können Sie dies unter **Device > Reset** tun.

## 4.2.5 Zugangsverwaltungsdatei löschen

Sie können die Zugangsverwaltungsdatei `security.cfg` mit der *cifX Test Applikation* oder der *netHOST Device Test Application* vom WebServer löschen und somit die Default-Zugangsparameter wieder in Kraft setzen. Nachfolgend ist die Verfahrensweise mit der *cifX Test Applikation* beschrieben.

### Schrittanleitung Zugangsverwaltungsdatei löschen

- Starten Sie die *cifX Test Applikation* und öffnen Sie Channel1 wie in den Schritten 1 und 2 im Abschnitt *Zugangsverwaltungsdatei hochladen* [▶ Seite 21] beschrieben.
- Wählen Sie **Device > File Explorer** und markieren Sie die unter **Filename** aufgeführte `security.cfg`.

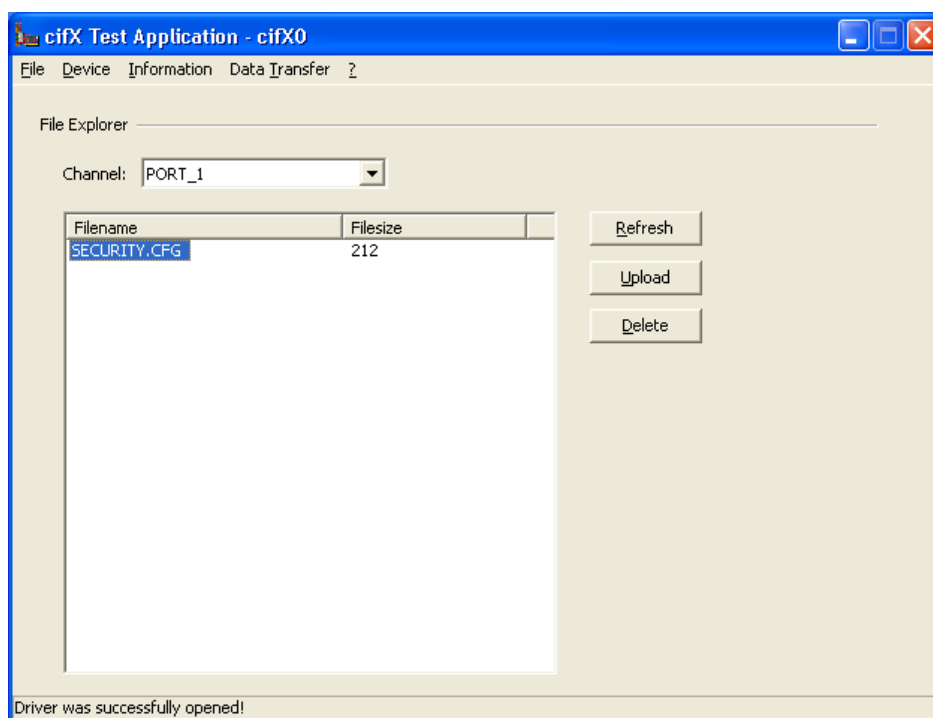


Abbildung 8: Dateien in File Explorer anzeigen und löschen

**Hinweis:**

Sie können die Datei bei Bedarf vor dem Löschen sichern, indem Sie sie mit der Schaltfläche **Upload** vom WebServer auf Ihren PC hochladen und dort speichern.

- Klicken Sie die Schaltfläche **Delete**, um die Datei zu löschen.
- Führen Sie unter **Device > Reset** ein Reset aus.
- ⇒ Sie haben die Zugangsverwaltungsdatei `security.cfg` gelöscht. Es gelten wieder die Default-Zugangsparameter (siehe Abschnitt *Default-Zugangsverwaltung* [▶ Seite 18]).

## 5 Eigene Inhalte einbinden

### 5.1 Übersicht

Sie können eigene Webseiten und Grafiken (z. B. Ihr Firmenlogo) auf dem WebServer hinterlegen oder die vorhandenen Webseiten ändern, um das Design der vom WebServer angezeigten Seiten nach Ihren Wünschen zu gestalten.

Neue Dateien können Sie mit dem **File Upload** in das öffentliche Verzeichnis des WebServers `Port_1/sx/pub` hochladen, wie im Abschnitt *File Upload* [► Seite 12] beschrieben.

Beachten Sie dabei folgendes:

- Es werden nur „8.3 Namen“ unterstützt, d. h. ein Dateiname darf nicht mehr als acht Zeichen umfassen, die Namensweiterung nicht mehr als drei Zeichen.
- Der Speicherbedarf der Dateien im öffentlichen Verzeichnis sollte insgesamt zwei Megabyte nicht überschreiten.

Die HTTP-Funktionen **Firmware Update**, **File Upload** und **Reset** bleiben von Änderungen, die Sie im öffentlichen Verzeichnis vornehmen, unberührt, da die eigentlichen HTML-Seiten, die den Code für diese Funktionen enthalten, für den Nutzer unzugänglich abgelegt sind. Selbst wenn Sie sämtliche Seiten, die Links auf diese Funktionen enthalten, im öffentlichen Ordner löschen, können Sie diese Funktionen immer noch direkt über deren URL aufrufen. Die entsprechenden URLs finden Sie in der Tabelle *HTTP-Funktionen direkt aufrufen* [► Seite 8].

#### Beispieldateien auf der Produkt-DVD

Auf Ihrer Produkt-DVD finden Sie im Ordner

`Examples & API > [x]. WebServer pages > Common > Port_1 > sx > pub` die gleichen Dateien, die sich nach Auslieferung Ihres Gerätes auch im öffentlichen Verzeichnis des WebServers befinden und die bei Aufruf des WebServers angezeigt werden (beim netRAPID sind diese Dateien im Auslieferungszustand des Gerätes noch nicht geladen, und müssen daher erst noch vom Nutzer in das Gerät transferiert werden). Diese Dateien können Sie lokal als Templates verwenden und nach Ihren Wünschen abändern – indem Sie z. B. neuen HTML-Code einfügen, das Stylesheet ändern oder Grafiken durch eigene Logos ersetzen – und anschließend auf den WebServer hochladen.



#### Hinweis:

Bei der Bilddatei `device.jpg` im Verzeichnis `Examples & API > [x]. WebServer pages > Common > Port_1 > sx > pub` auf der DVD handelt es sich um eine Platzhalter-Datei. Sie finden ein Bild von Ihrem Gerät auf der DVD im Verzeichnis `Examples & API > [x]. WebServer pages > Product` in einem Unterordner, der nach Ihrem Gerät benannt ist (z.B. `comX`, `netJACK` oder `netRAPID`).



## Server Side Includes und Inlineframes

Die meisten Seiten des WebServers arbeiten mit Server Side Includes (SSI) und Inlineframes (iframe), mit deren Hilfe man HTML-Code oder andere Webseiten dynamisch einbinden kann. Eine HTML-Datei, die SSI-Anweisungen enthält, muss die Dateierweiterung `.sht` oder `.stm` aufweisen, um vom WebServer verarbeitet werden zu können.

In den Dateien `fwupdate.sht`, `reset.sht` und `upload.sht` beispielsweise ist die Menüleiste als SSI Anweisung `<!--#include file="menu.prt" -->` eingebunden, und die HTML-Seiten, die den eigentlichen Code für die Funktionen **Firmware Update**, **File Upload** und **Reset** enthalten, sind als iframes (z. B. `<iframe src="fwupdate"...>`) eingebettet.

## 5.2 Beispiele für das Einbinden eigener Inhalte

Nachfolgend finden Sie Schrittanleitungen für typische Anpassungen, die Sie als Nutzer an den Webseiten des WebServers vornehmen können. Beachten Sie, dass dies beispielhafte Beschreibungen sind, und – abhängig von Ihren Kenntnissen in Webdesign – auch andere Vorgehensweisen möglich sind.

### 5.2.1 Beispiel 1: Firmenlogo in der Navigationsleiste austauschen

In der Navigationsleiste der WebServer-Seiten befindet sich oben rechts das Hilscher-Logo. Weil hinter diesem Logo ein Hyperlink hinterlegt ist, gelangen Sie durch Anklicken des Logos mit Ihrem Browser auf die Firmenwebseite der Hilscher GmbH. Wenn Sie das Hilscher-Logo durch Ihr eigenes Firmenlogo ersetzen möchten, und der Hyperlink auf Ihre eigene Firmenwebseite führen soll, gehen Sie folgendermaßen vor:

1. Bilddatei austauschen. Hierfür müssen Sie keinen HTML-Code ändern.
  - Überschreiben Sie einfach die auf dem WebServer vorhandene Bilddatei `logo.png`, die das Hilscher-Logo enthält. Dazu müssen Sie lediglich eine PNG-Datei gleichen Namens mit Ihrem Firmenlogo per File Upload auf den WebServer in den Ordner `pub` hochladen. (Siehe Abschnitt *File Upload* [▶ Seite 12].)



#### Hinweis:

Für das Logo sind Abmessungen von etwa 150 (Breite) x 100 (Höhe) in Pixeln empfehlenswert.

- ⇒ Sobald Sie eine Seite des WebServers erneut aufrufen, wird statt des Hilscher-Logos die neue Bilddatei mit Ihrem Firmenlogo angezeigt.
2. Hyperlink anpassen. Hierfür müssen Sie in der Datei `menu.prt` den HTML-Code ändern, der die Inhalte des Navigationsmenüs definiert.
    - Kopieren Sie die Datei `menu.prt`, die sich auf der Produkt-DVD im Ordner `Examples & API > [x]. WebServer pages > Common > Port_1 > sx > pub` befindet, auf Ihren PC.
    - Öffnen Sie die Datei mit dem Windows-Editor.
    - ⇒ Sie sehen den HTML-Code der Datei `menu.prt`:

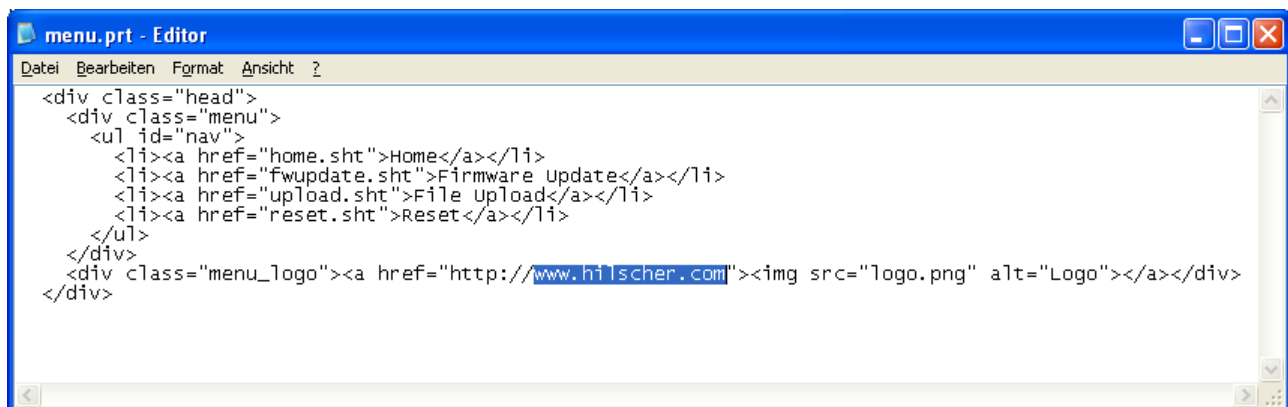


Abbildung 9: Hyperlink in `menu.prt` editieren

- Ersetzen Sie die Webadresse `www.hilscher.com` durch Ihre eigene Webadresse, z. B. `www.mustermann-automation.com`.
- Speichern und schließen Sie die Datei.
- Transferieren Sie die geänderte Datei `menu.prt` mittels File Upload auf den WebServer in den Ordner `pub` (siehe Abschnitt *File Upload* [► Seite 12]). Dabei überschreiben Sie die alte `menu.prt` Datei.
- ⇒ Sobald Sie eine Seite des WebServers erneut aufrufen und auf das Logo klicken, wird Ihr Browser auf Ihre Firmenwebseite weitergeleitet.

## 5.2.2 Beispiel 2: Design der Navigationsleiste ändern

Wenn Sie z. B. das Hintergrundbild der Navigationsleiste austauschen möchten, können Sie einfach die auf dem WebServer vorhandene Bilddatei `menubg.jpg`, die das Hintergrundbild enthält, durch eine gleichnamige Bilddatei ersetzen, die Sie per File Upload in den Ordner `pub` des WebServers hochladen. (Siehe Abschnitt *File Upload* [► Seite 12].) Für das Hintergrundbild sind Abmessungen von 932 (Breite) x 152 (Höhe) in Pixeln empfehlenswert.

Layout und Design der Seiten, die der WebServer anzeigt, werden im Cascading Style Sheet `style.css` definiert. Wenn Sie in der Navigationsleiste statt eines Bildes z. B. nur eine blaue Fläche als Hintergrund haben möchten, müssen Sie Änderungen im Style Sheet vornehmen. Gehen Sie hierzu wie folgt vor:

- Kopieren Sie die Datei `style.css`, die sich auf der Produkt-DVD im Ordner `Examples & API > [x]. WebServer pages > Common > Port_1 > sx > pub` befindet, auf Ihren PC.
- Öffnen Sie die Datei mit einem geeigneten Editor-Programm.

➤ Sie sehen die in der Datei `style.css` enthaltenen Deklarationen:

```
* {
    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;
}
```

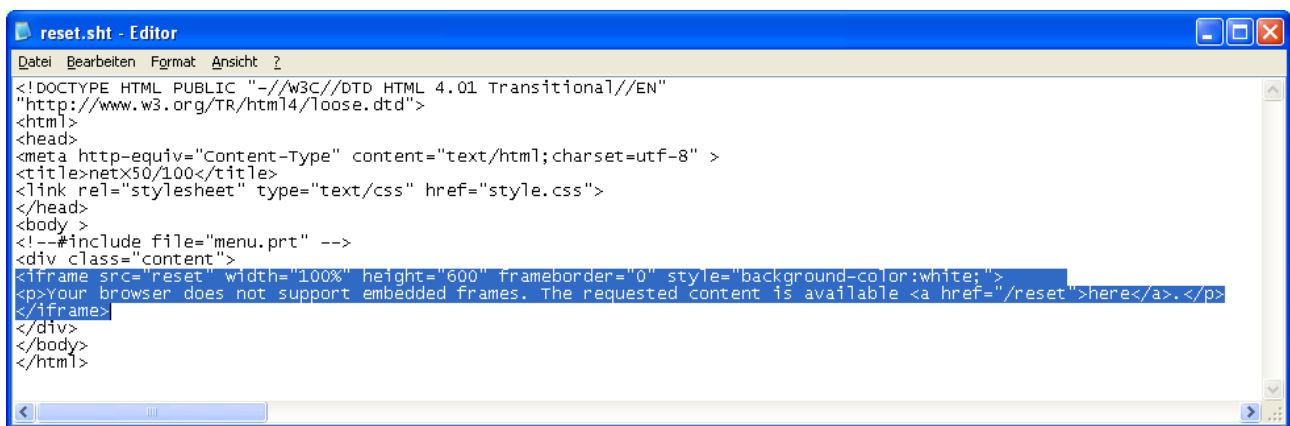
Abbildung 10: Ausschnitt aus `style.css`

- Navigieren Sie zu dem Selektor `.head` im Abschnitt `*** NAVIGATION MENU ***` und entfernen Sie das Hintergrundbild, indem Sie den Zeichenstring `background-image:url(menubg.jpg);` löschen. Ändern Sie anschließend die Hintergrundfarbe, indem Sie hinter dem Parameter `background-color` den Zeichenstring `#e01010` (steht für Rot) durch einen Wert für Blau ersetzen, z. B. `#0000FF`.
- Speichern und schließen Sie die Datei.
- Transferieren Sie die geänderte Datei `style.css` mittels File Upload auf den WebServer in den Ordner `pub` (siehe Abschnitt *File Upload* [▶ Seite 12]). Dabei überschreiben Sie die alte `style.css` Datei.
- ⇒ Sobald Sie eine Seite des WebServers erneut aufrufen, wird die Navigationsleiste mit blauem Hintergrund angezeigt.

### 5.2.3 Beispiel 3: Neue Webseite einbinden

Sie können eigene Webseiten auf den WebServer hochladen und Links auf diese Seiten in die Navigationsleiste einfügen. Wenn Sie z. B. eine Webseite einbinden möchten, die eine Arbeitsanweisung enthält, gehen Sie folgendermaßen vor:

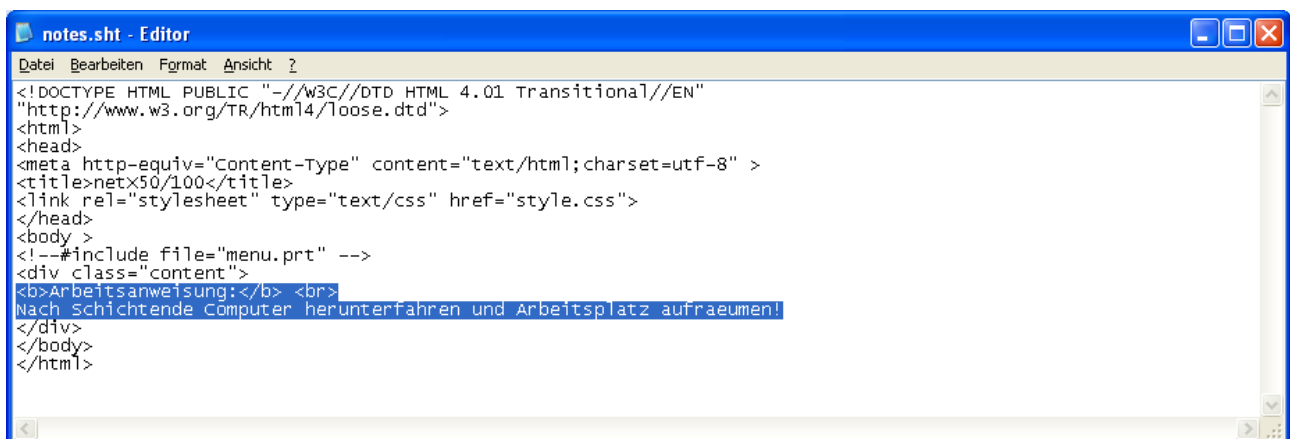
1. Erstellen Sie die Webseite, die die Arbeitsanweisung enthält. Sie können hierfür eine bereits vorhandene Webseite als Template verwenden.
  - Kopieren Sie die Datei `reset.sht`, die sich auf der Produkt-DVD im Ordner `Examples & API > [x]. WebServer pages > Common > Port_1 > sx > pub` befindet, auf Ihren PC.
  - Öffnen Sie die Datei mit einem geeigneten Editor-Programm.
  - Sie sehen den HTML-Code der Datei `reset.sht` (zur besseren Übersichtlichkeit wurden in der nachfolgenden Abbildung Zeilenumbrüche eingefügt):



```
reset.sht - Editor
Datei Bearbeiten Format Ansicht ?
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" >
<title>netx50/100</title>
<link rel="stylesheet" type="text/css" href="style.css">
</head>
<body>
<!--#include file="menu.prt" -->
<div class="content">
<iframe src="reset" width="100%" height="600" frameborder="0" style="background-color:white;">
<p>Your browser does not support embedded frames. The requested content is available <a href="/reset">here</a>.</p>
</iframe>
</div>
</body>
</html>
```

Abbildung 11: `reset.sht` als Template für eigene Webseite verwenden – `iframe` Element löschen

- Löschen Sie das `iframe`-Element aus dem HTML-Code (d. h. den Zeichenstring von einschließlich `<iframe src="reset"...>` bis `</iframe>`) und fügen Sie an gleicher Stelle den Text Ihrer Arbeitsanweisung ein.



```
notes.sht - Editor
Datei Bearbeiten Format Ansicht ?
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" >
<title>netx50/100</title>
<link rel="stylesheet" type="text/css" href="style.css">
</head>
<body>
<!--#include file="menu.prt" -->
<div class="content">
<b>Arbeitsanweisung:</b><br>
Nach Schichtende Computer herunterfahren und Arbeitsplatz aufräumen!
</div>
</body>
</html>
```

Abbildung 12: `reset.sht` als Template für eigene Webseite verwenden – eigenen Text einfügen

- Speichern Sie die Datei z. B. als `notes.sht`. Achten Sie darauf, dass der Dateiname nicht mehr als acht Zeichen aufweist und die Dateinamenerweiterung `.sht` lautet.

- Transferieren Sie die Datei `notes.sht` mittels File Upload auf den WebServer in den Ordner `pub` (siehe Abschnitt *File Upload* ► Seite 12)).
- 2. Link auf neue Webseite in die Navigationsleiste einfügen. Hierfür müssen Sie in der Datei `menu.prt`, die die Inhalte des Navigationsmenüs definiert, den Hyperlink ergänzen.
  - Kopieren Sie die Datei `menu.prt`, die sich auf der Produkt-DVD im Ordner `Examples & API > [x]. WebServer pages > Common > Port_1 > sx > pub` befindet, auf Ihren PC.
  - Öffnen Sie die Datei mit dem Windows-Editor.
  - ⇒ Sie sehen den HTML-Code der Datei `menu.prt`:

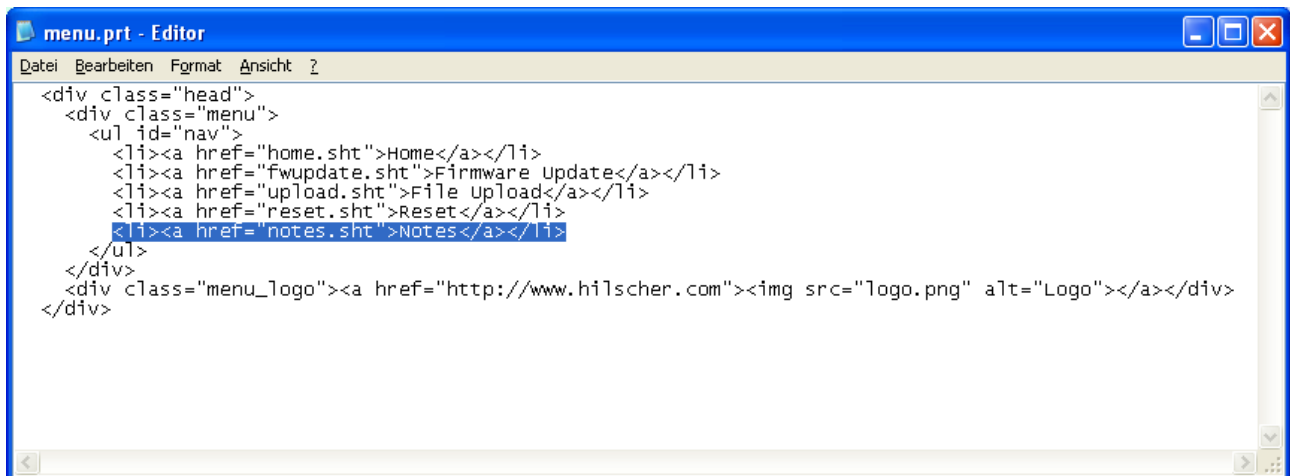


Abbildung 13: Hyperlink auf neue Webseite einfügen

- Fügen Sie den Hyperlink `<li><a href="notes.sht">Notes</a></li>` ein.
- Speichern und schließen Sie die Datei.
- Transferieren Sie die geänderte Datei `menu.prt` mittels File Upload auf den WebServer in den Ordner `pub` (siehe Abschnitt *File Upload* ► Seite 12)). Dabei überschreiben Sie die alte `menu.prt` Datei.
- ⇒ Sobald Sie eine Seite des WebServers erneut aufrufen, sehen Sie den neuen Hyperlink in der Navigationsleiste und können Ihre neue Webseite aufrufen, indem Sie auf den Link klicken oder die IP-Adresse samt Dateinamen (`http://<IP-Adresse>/notes.sht`) in die Adresszeile des Browsers eingeben.

## 6 WebServer-Content auf netRAPID hochladen

### 6.1 Übersicht

Der **netRAPID NRP 51-RE** wird ohne vorinstallierten WebServer-Content ausgeliefert, daher müssen Sie nach der Inbetriebnahme des netRAPIDs (nach dem Firmware-Download und der Konfiguration) die Inhalte des WebServers zunächst selber in das Gerät übertragen.

Für das Übertragen der „öffentlichen“ Inhalte bzw. Dateien, die im Ordner `pub` abgelegt werden (HTML-Seiten, Grafiken, Stylesheet etc.), können Sie die **File Upload**-Funktion des WebServers verwenden (die HTTP-Funktionen des WebServers **Firmware Update**, **File Upload** und **Reset** sind unabhängig vom ladbaren Web-Content bereits fest in der Geräte-Firmware enthalten).

Für das Übertragen der Zugangsverwaltungsdatei `security.cfg` hingegen benötigen Sie die *netHOST Device Test Application*, die den Zugriff auf das „nicht-öffentliche“ `Port_1` Root-Verzeichnis des netRAPIDs über USB ermöglicht, wo die Zugangsverwaltungsdatei abgelegt werden muss.

### 6.2 Zugangsverwaltungsdatei per netHOST und USB auf netRAPID hochladen

#### Voraussetzungen

- Sie haben die Firmware in den netRAPID geladen
- Auf dem netRAPID Host-Gerät ist eine USB-Schnittstelle implementiert (falls Sie nicht das Evaluation Board verwenden)
- Sie haben Zugriff auf die netRAPID Produkt-DVD
- Sie haben die Hilscher USB-Treiber auf Ihrem PC installiert (die Treiber befinden sich auf der netRAPID Produkt-DVD im Ordner `Driver and Toolkit\USB Diagnostic Driver` und können mit einem Doppelklick auf die Datei `setup.exe` installiert werden)
- Das netRAPID Evaluation Board bzw. das netRAPID Host-Gerät wird mit Spannung versorgt
- Das netRAPID Host-Gerät bzw. das Evaluation Board sind per USB mit Ihrem PC verbunden

### Schrittanleitung

1. Starten Sie die **netHOST Device Test Application** auf Ihrem PC.
  - Öffnen Sie auf der netRAPID Produkt-DVD den Ordner `Tools\netHOST\x64`.
  - Doppelklicken Sie die Datei `netHOST.exe`.
  - Die **netHOST Device Test Application** öffnet sich:

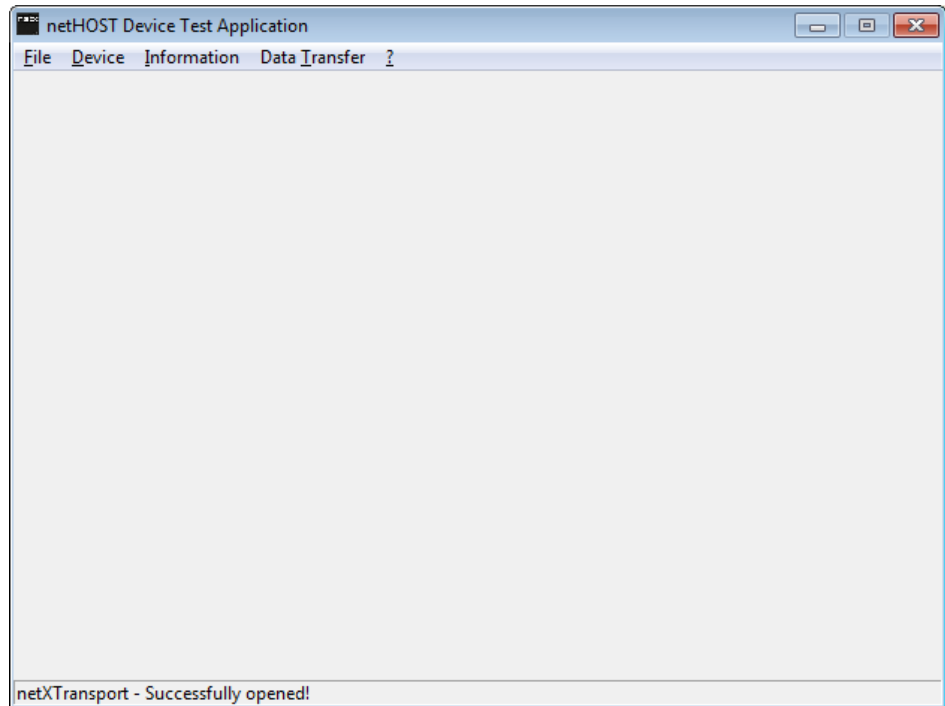


Abbildung 14: Geöffnete netHOST Device Test Application



2. Verbindung mit Channel 1 (port 1) im netRAPID herstellen.
  - Öffnen Sie das Menü **Device** und prüfen Sie, ob der Eintrag **Select netX Driver** angehakt ist:

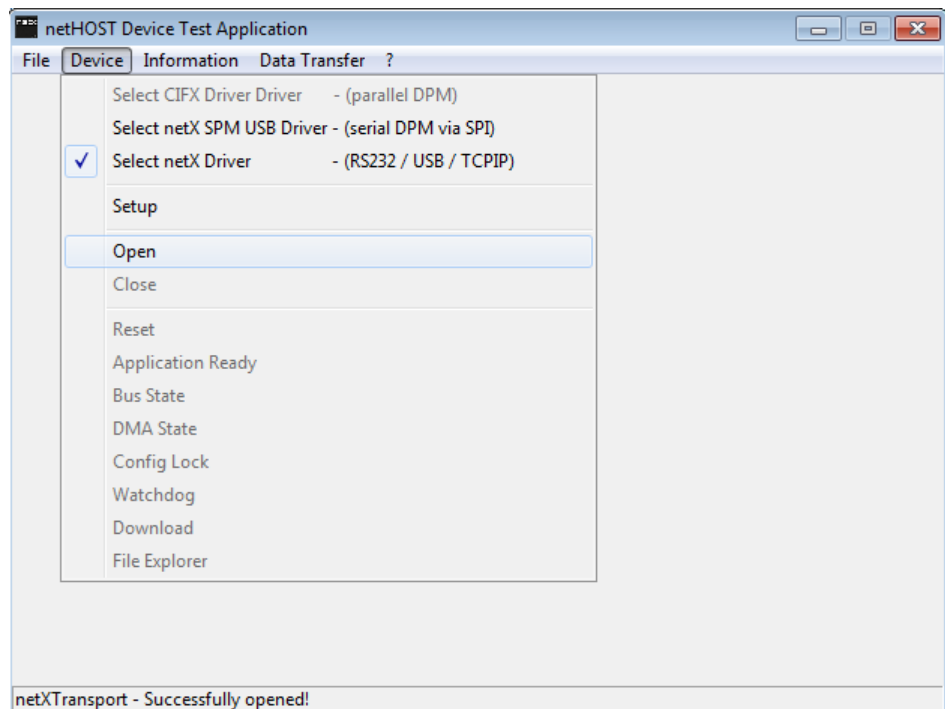


Abbildung 15: Select netX Driver in netHOST

- Wählen Sie dann im Menü **Device** den Eintrag **Open** und warten Sie einen kurzen Moment.
- Das Dialogfenster **Channel Selection** erscheint.
- Wählen Sie im linken Fenster den Eintrag **Channel1** und klicken Sie dann die Schaltfläche **Open**.

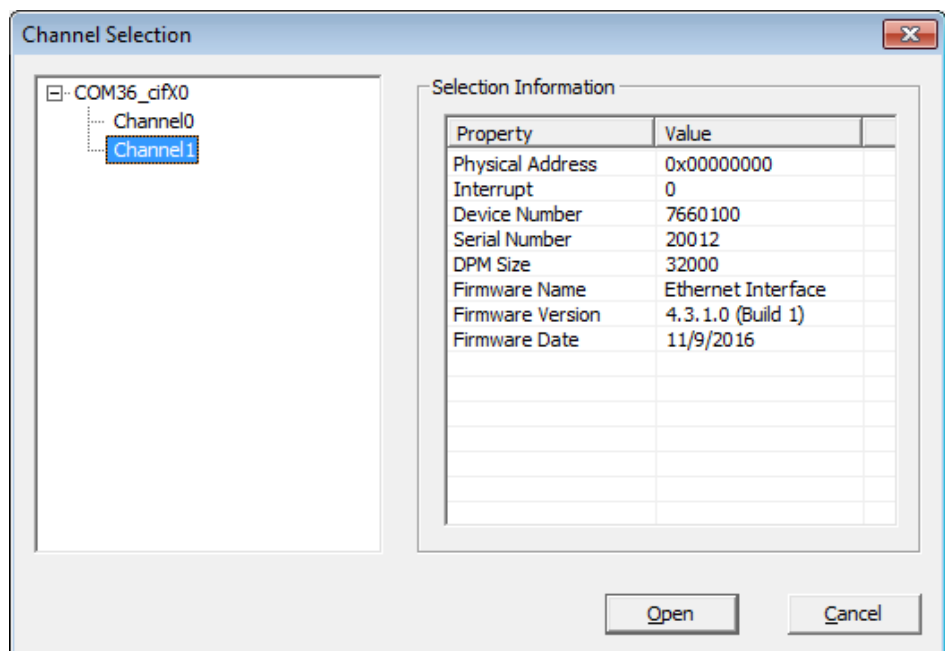


Abbildung 16: Channel Selection in netHOST

- Das Dialogfenster **Channel Selection** schließt sich und der gewählte Kanal wird in der Titelleiste angezeigt:

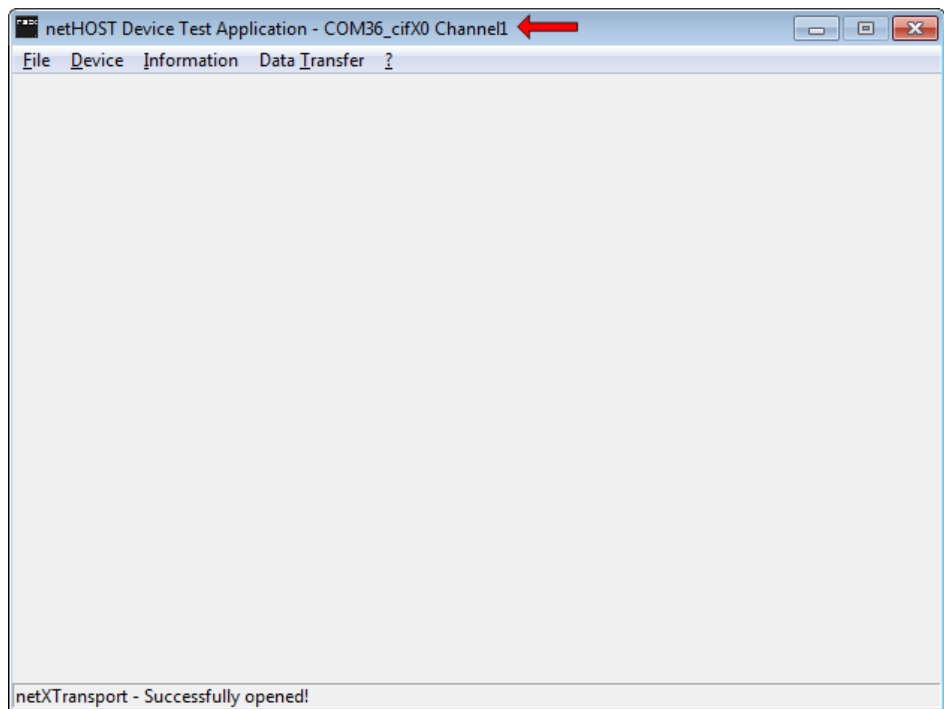


Abbildung 17: Gewählter Kanal in netHOST

3. Zugangsverwaltungsdatei in den netRAPID laden.
- Wählen Sie im Menü **Device** den Eintrag **Download**.
  - Das Dialogfenster **Download** erscheint.

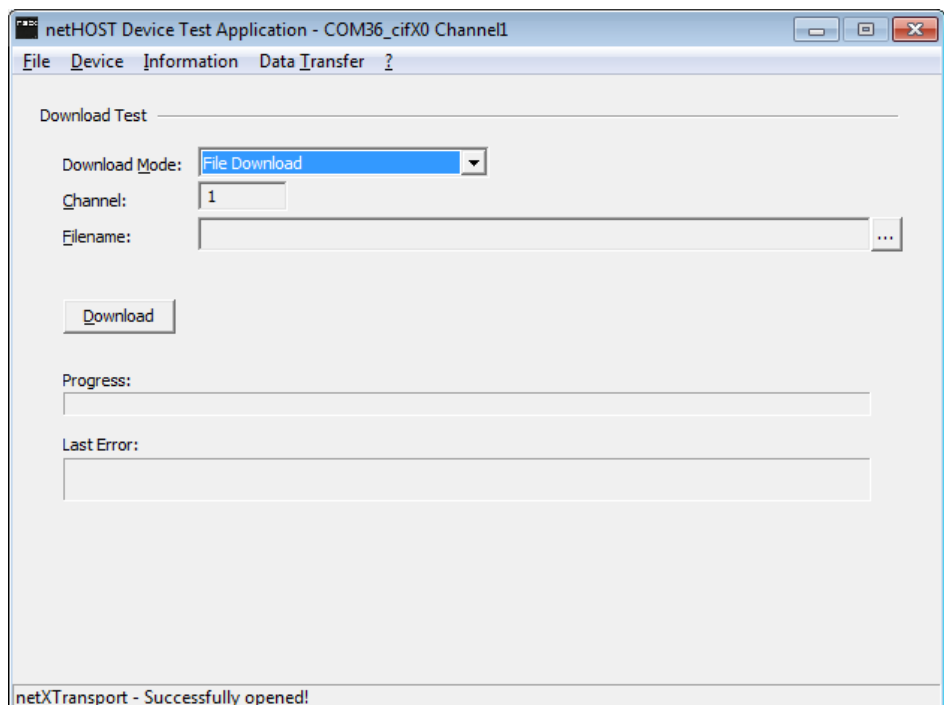


Abbildung 18: File Download in netHOST

- Wählen Sie in der Dropdown-Liste **Download Mode** den Modus **File Download**.
- Klicken Sie rechts neben dem Feld **Filename** auf die Schaltfläche .

- Der Windows-Dateiauswahl-Dialog öffnet sich.
- Öffnen Sie auf der netRAPID Produkt-DVD den Ordner `Examples and API\[x]. WebServer pages\Common\PORT_1`.

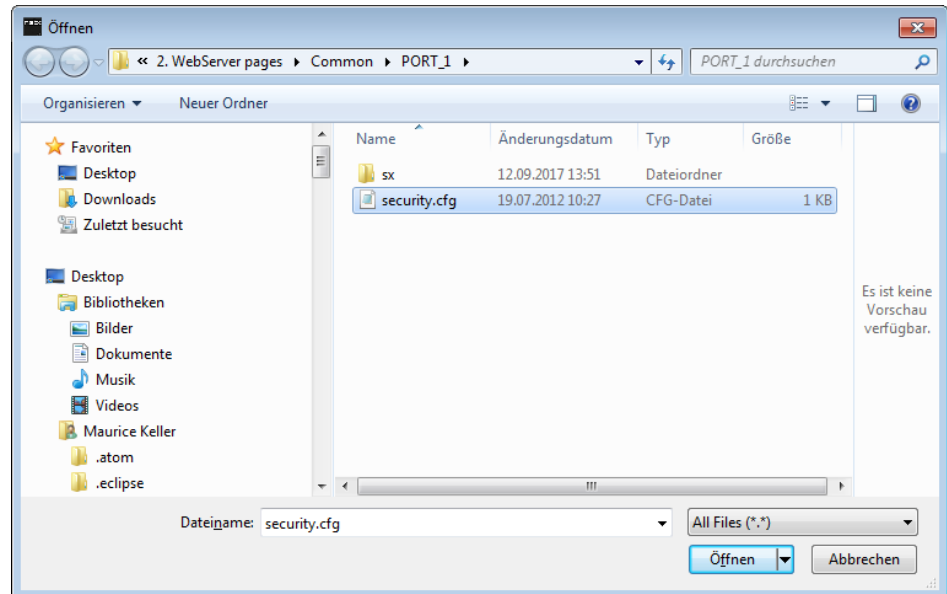


Abbildung 19: `security.cfg` in Windows-Dateiauswahl-Dialog

- Wählen Sie die Datei `security.cfg` und klicken Sie anschließend **Öffnen**.
- Der Windows-Dateiauswahl-Dialog schließt sich und der Pfad zu der gewählten Datei wird im Feld **Filename** angezeigt.
- Klicken Sie die Schaltfläche **Download**.

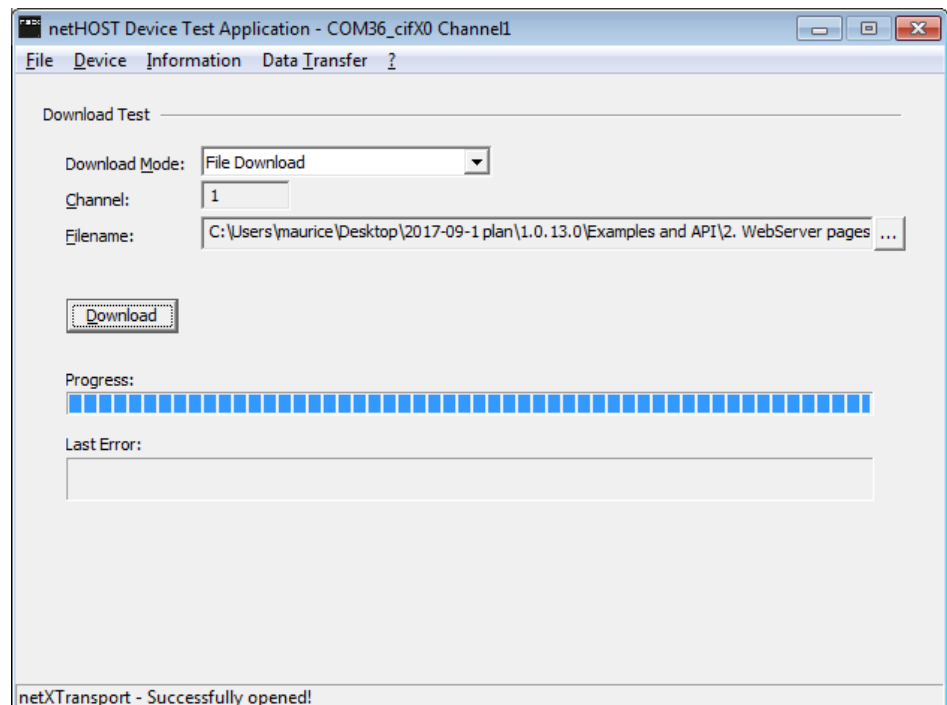


Abbildung 20: Download Fortschrittsbalken in netHOST

- Die Zugangsverwaltungsdatei wird in den netRAPID geladen. Der Fortschritt des Downloads wird im Feld **Progress** angezeigt.

**Hinweis:**

Ein erfolgreich abgeschlossener Download wird lediglich als voller Balken im Feld **Progress** angezeigt; es gibt kein separates Meldungsfenster.

## 4. Download prüfen.

- Wählen Sie im Menü **Device** den Eintrag **File Explorer**.
- ⇒ Die in das Gerät geladene Datei `security.cfg` sollte nun im **File Explorer** angezeigt werden:

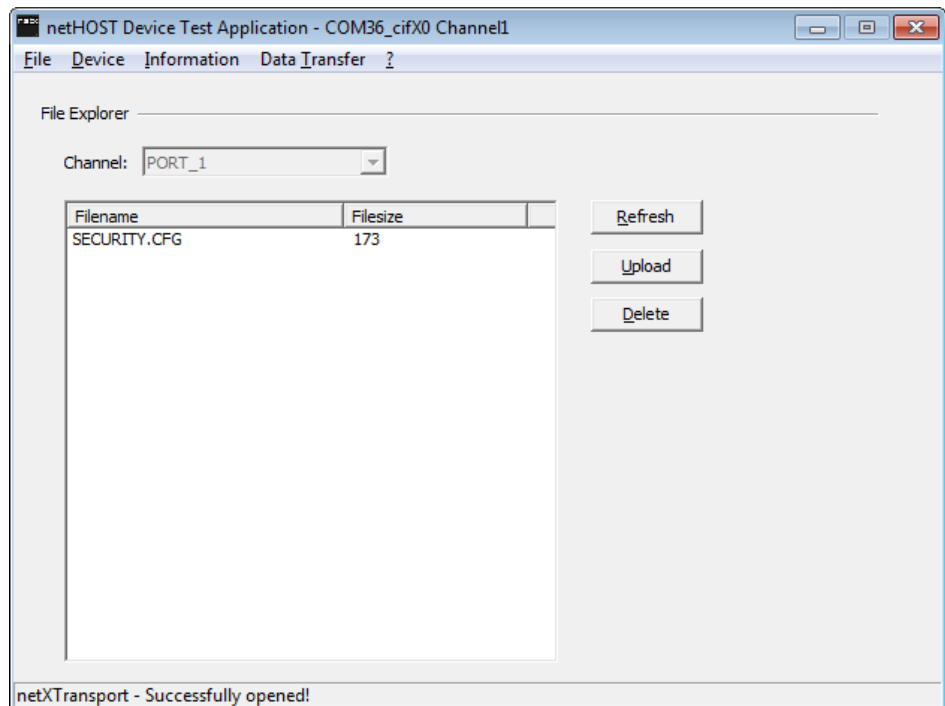


Abbildung 21: File Explorer in netHOST

**Hinweis:**

Das Verzeichnis `sx` in `PORT_1`, in dem die Inhalte des WebServers gespeichert werden, wird vom **File Explorer** der netHOST Device Test Application nicht angezeigt.

- ⇒ Wählen Sie im Menü **Device > Close** und anschließend **File > Quit** um die netHOST Device Test Application zu schließen.
- ⇒ Sie haben die Zugangsverwaltungsdatei in den netRAPID geladen. Sie können nun die übrigen WebServer-Dateien mithilfe der **File Upload**-Funktion in den netRAPID laden (die netHOST Device Test Application können Sie hierzu nicht verwenden).

## 6.3 Web-Content per File Upload auf netRAPID hochladen

### Voraussetzungen

- Sie haben die Firmware in den netRAPID geladen
- Dem netRAPID wurde im Rahmen der Geräte-Konfiguration eine IP-Adresse zugewiesen
- Sie kennen die IP-Adresse des netRAPIDs
- Sie haben Zugriff auf die netRAPID Produkt-DVD
- Das netRAPID Evaluation Board bzw. das netRAPID Host-Gerät wird mit Spannung versorgt
- Das netRAPID Evaluation Board bzw. das netRAPID Host-Gerät ist über seine Ethernet-Schnittstelle mit einem IP-Netzwerk verbunden
- Sie verfügen über einen PC mit Verbindung zum IP-Netzwerk des netRAPIDs und einen Webbrowser

### Schrittanleitung

- Geben Sie die IP-Adresse des netRAPID gefolgt von `upload` in die Adresszeile Ihres Browsers ein. Verwenden Sie folgende Syntax:  
`http://<IP-Adresse>/upload`
- Eine Passwort-Abfrage erscheint.
- Geben als Benutzername `admin` und als Kennwort ebenfalls `admin` ein.
- Die **File Upload**-Funktion des WebServers öffnet sich im Browser:

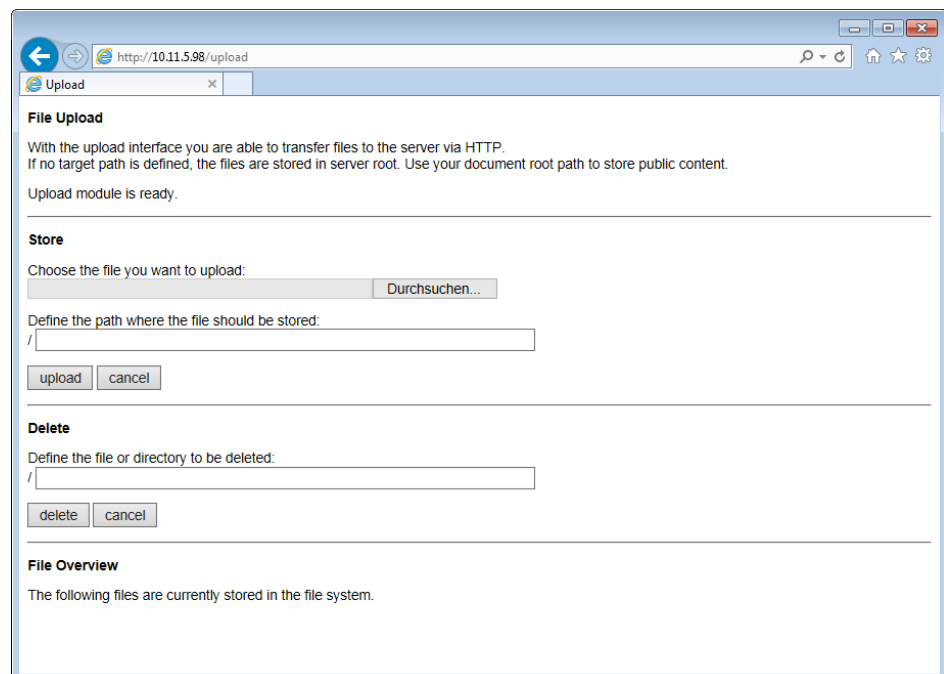


Abbildung 22: File Upload-Modul des WebServers (Darstellung im Internet Explorer, kann in anderen Browsern abweichen)

- Geben Sie in das Feld **Define the path where the file should be stored** den Ordernamen `pub` ein.
- Klicken Sie die Schaltfläche **Durchsuchen...**

- Der Windows-Dateiauswahl-Dialog öffnet sich.
- Öffnen Sie auf der netRAPID Produkt-DVD den Ordner `Examples and API\[x]. WebServer pages\Common\PORT_1\sx\pub`
- Wählen Sie die Datei `common.js` und klicken Sie anschließend **Öffnen**.

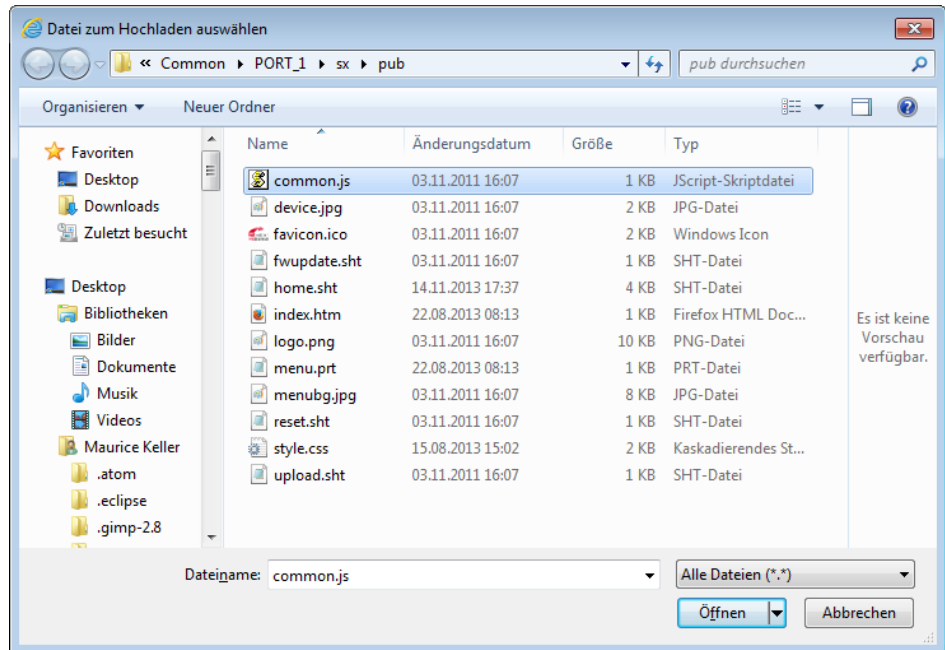


Abbildung 23: Windows-Dateiauswahl-Dialog

- Der Windows-Dateiauswahl-Dialog schließt sich und der Pfad zu der gewählten Datei wird im Feld **Choose the file you want to upload** angezeigt.

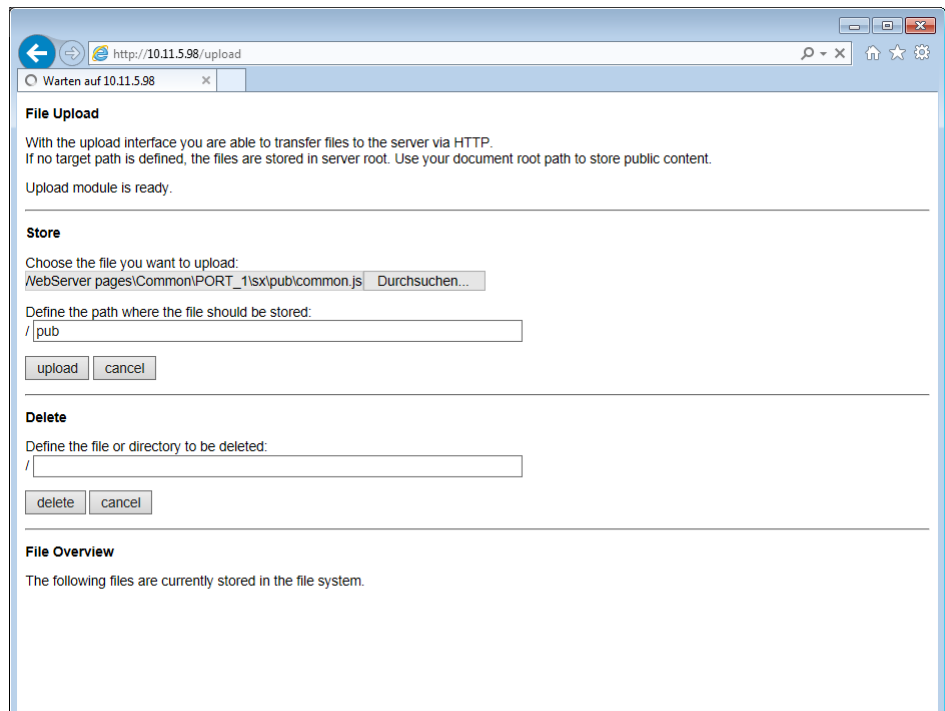


Abbildung 24: File upload

- Klicken Sie die Schaltfläche **upload**.

- Der WebServer legt automatisch den Ordner `pub` im Verzeichnis `Port_1/sx` an und lädt anschließend die gewählte Datei dorthin hoch. Im Bereich **File Overview** sehen Sie die hochgeladenen Ordner und Dateien:

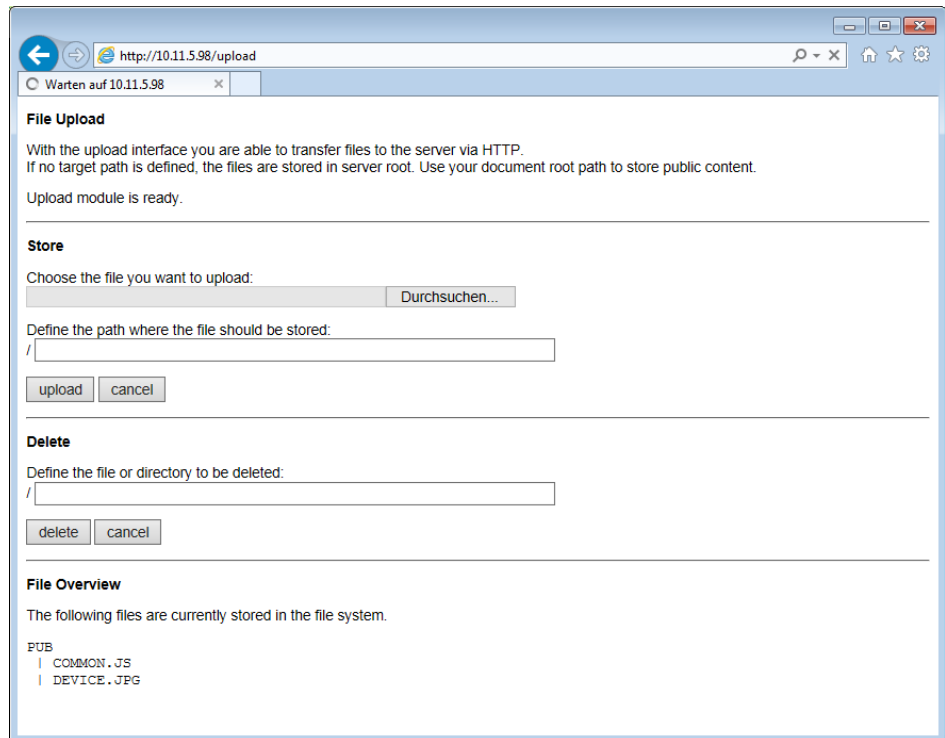


Abbildung 25: File Overview

- Laden Sie die übrigen Dateien, die sich auf der netRAPID Produkt-DVD im Ordner `Examples and API\[x]. WebServer pages\Common\PORT_1\sx\pub` befinden, ebenfalls in das Gerät. Sie müssen die Dateien einzeln hochladen.



#### Hinweis:

Die Bilddatei `device.jpg` ist nur eine Platzhalterdatei. Laden Sie stattdessen das netRAPID-Motiv auf das Gerät, das Sie auf der netRAPID Produkt-DVD im Ordner `Examples and API\2. WebServer pages\Product\netRAPID\PORT_1\sx\pub` finden.

- ⇒ Wenn Sie alle Dateien hochgeladen haben, können Sie die hochgeladenen WebServer-Seiten durch Eingabe der IP-Adresse aufrufen:



Abbildung 26: WebServer-Seiten des netRAPID



## 7 Zugriff auf Verzeichnisse

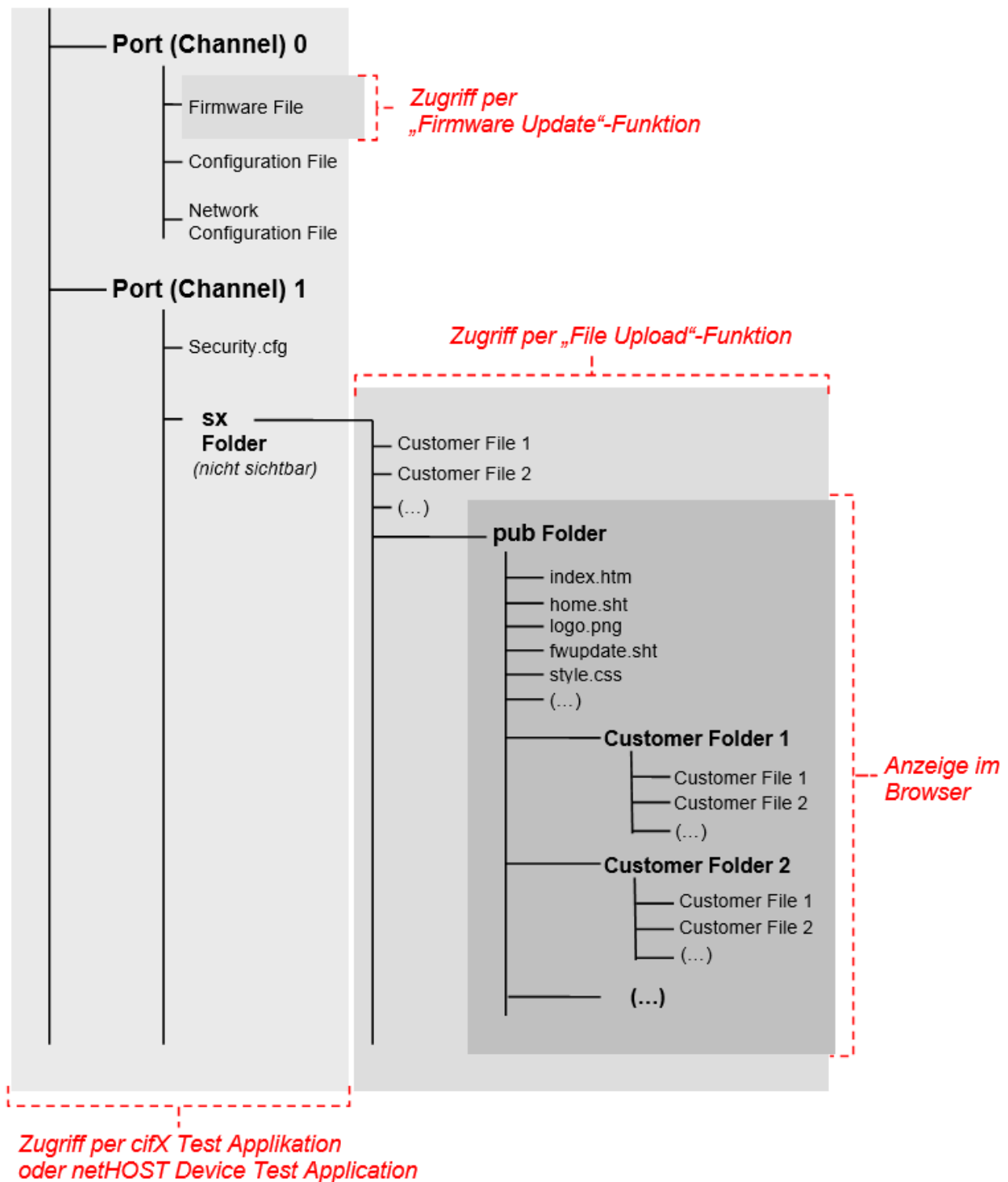


Abbildung 27: Zugriff auf Verzeichnisse des Systems

## Abbildungsverzeichnis

Abbildung 1:	Startseite WebServer (Darstellung im Internet Explorer, kann in anderen Browsern abweichen) .....	9
Abbildung 2:	Firmware Update (Darstellung im Internet Explorer, kann in anderen Browsern abweichen) .....	10
Abbildung 3:	File Upload (Darstellung im Internet Explorer, kann in anderen Browsern abweichen) .....	13
Abbildung 4:	Reset (Darstellung im Internet Explorer, kann in anderen Browsern abweichen) .....	16
Abbildung 5:	Zeichenketten in Beispieldatei security.cfg.....	20
Abbildung 6:	Auswahl des Channel in cifX Test Applikation .....	21
Abbildung 7:	Zugangsverwaltungsdatei übertragen .....	22
Abbildung 8:	Dateien in File Explorer anzeigen und löschen .....	23
Abbildung 9:	Hyperlink in menu.prt editieren .....	26
Abbildung 10:	Ausschnitt aus style.css .....	28
Abbildung 11:	reset.sht als Template für eigene Webseite verwenden – iframe Element löschen .....	29
Abbildung 12:	reset.sht als Template für eigene Webseite verwenden – eigenen Text einfügen.....	29
Abbildung 13:	Hyperlink auf neue Webseite einfügen.....	30
Abbildung 14:	Geöffnete netHOST Device Test Application .....	32
Abbildung 15:	Select netX Driver in netHOST .....	33
Abbildung 16:	Channel Selection in netHOST.....	33
Abbildung 17:	Gewählter Kanal in netHOST .....	34
Abbildung 18:	File Download in netHOST .....	34
Abbildung 19:	security.cfg in Windows-Dateiauswahl-Dialog.....	35
Abbildung 20:	Download Fortschrittsbalken in netHOST .....	35
Abbildung 21:	File Explorer in netHOST.....	36
Abbildung 22:	File Upload-Modul des WebServers (Darstellung im Internet Explorer, kann in anderen Browsern abweichen).....	37
Abbildung 23:	Windows-Dateiauswahl-Dialog.....	38
Abbildung 24:	File upload .....	38
Abbildung 25:	File Overview .....	39
Abbildung 26:	WebServer-Seiten des netRAPID .....	40
Abbildung 27:	Zugriff auf Verzeichnisse des Systems .....	41

## Tabellenverzeichnis

Tabelle 1:	Änderungsübersicht.....	3
Tabelle 2:	Abkürzungen.....	3
Tabelle 3:	Liste der Geräte und Firmware mit integriertem WebServer .....	6
Tabelle 4:	Getestete Browser-Versionen für WebServer .....	7
Tabelle 5:	Übersicht der Webseiten und deren URLs .....	8
Tabelle 6:	HTTP-Funktionen direkt aufrufen .....	8
Tabelle 7:	Bedienelemente Firmware-Update .....	11
Tabelle 8:	Bedienelemente Datei-Upload .....	14
Tabelle 9:	Bedienelemente Dateien löschen .....	15
Tabelle 10:	Gruppen und deren Rechte .....	19
Tabelle 11:	Benutzer-Passwort-Rechte-Matrix der Beispieldatei security.cfg .....	19

# Kontakte

## HAUPTSITZ

### Deutschland

Hilscher Gesellschaft für  
Systemautomation mbH  
Rheinstrasse 15  
65795 Hattersheim  
Telefon: +49 (0) 6190 9907-0  
Fax: +49 (0) 6190 9907-50  
E-Mail: [info@hilscher.com](mailto:info@hilscher.com)

### Support

Telefon: +49 (0) 6190 9907-99  
E-Mail: [de.support@hilscher.com](mailto:de.support@hilscher.com)

## NIEDERLASSUNGEN

### China

Hilscher Systemautomation (Shanghai) Co. Ltd.  
200010 Shanghai  
Telefon: +86 (0) 21-6355-5161  
E-Mail: [info@hilscher.cn](mailto:info@hilscher.cn)

### Support

Telefon: +86 (0) 21-6355-5161  
E-Mail: [cn.support@hilscher.com](mailto:cn.support@hilscher.com)

### Frankreich

Hilscher France S.a.r.l.  
69500 Bron  
Telefon: +33 (0) 4 72 37 98 40  
E-Mail: [info@hilscher.fr](mailto:info@hilscher.fr)

### Support

Telefon: +33 (0) 4 72 37 98 40  
E-Mail: [fr.support@hilscher.com](mailto:fr.support@hilscher.com)

### Indien

Hilscher India Pvt. Ltd.  
Pune, Delhi, Mumbai  
Telefon: +91 8888 750 777  
E-Mail: [info@hilscher.in](mailto:info@hilscher.in)

### Italien

Hilscher Italia S.r.l.  
20090 Vimodrone (MI)  
Telefon: +39 02 25007068  
E-Mail: [info@hilscher.it](mailto:info@hilscher.it)

### Support

Telefon: +39 02 25007068  
E-Mail: [it.support@hilscher.com](mailto:it.support@hilscher.com)

### Japan

Hilscher Japan KK  
Tokyo, 160-0022  
Telefon: +81 (0) 3-5362-0521  
E-Mail: [info@hilscher.jp](mailto:info@hilscher.jp)

### Support

Telefon: +81 (0) 3-5362-0521  
E-Mail: [jp.support@hilscher.com](mailto:jp.support@hilscher.com)

### Korea

Hilscher Korea Inc.  
Seongnam, Gyeonggi, 463-400  
Telefon: +82 (0) 31-789-3715  
E-Mail: [info@hilscher.kr](mailto:info@hilscher.kr)

### Schweiz

Hilscher Swiss GmbH  
4500 Solothurn  
Telefon: +41 (0) 32 623 6633  
E-Mail: [info@hilscher.ch](mailto:info@hilscher.ch)

### Support

Telefon: +49 (0) 6190 9907-99  
E-Mail: [ch.support@hilscher.com](mailto:ch.support@hilscher.com)

### USA

Hilscher North America, Inc.  
Lisle, IL 60532  
Telefon: +1 630-505-5301  
E-Mail: [info@hilscher.us](mailto:info@hilscher.us)

### Support

Telefon: +1 630-505-5301  
E-Mail: [us.support@hilscher.com](mailto:us.support@hilscher.com)