Can't sleep, hackers will eat me!

Search

About Me | Disclaimer | Tools

The Mobile Network Iceberg

November 5, 2015 08:28 | 9 Comments | Xavier

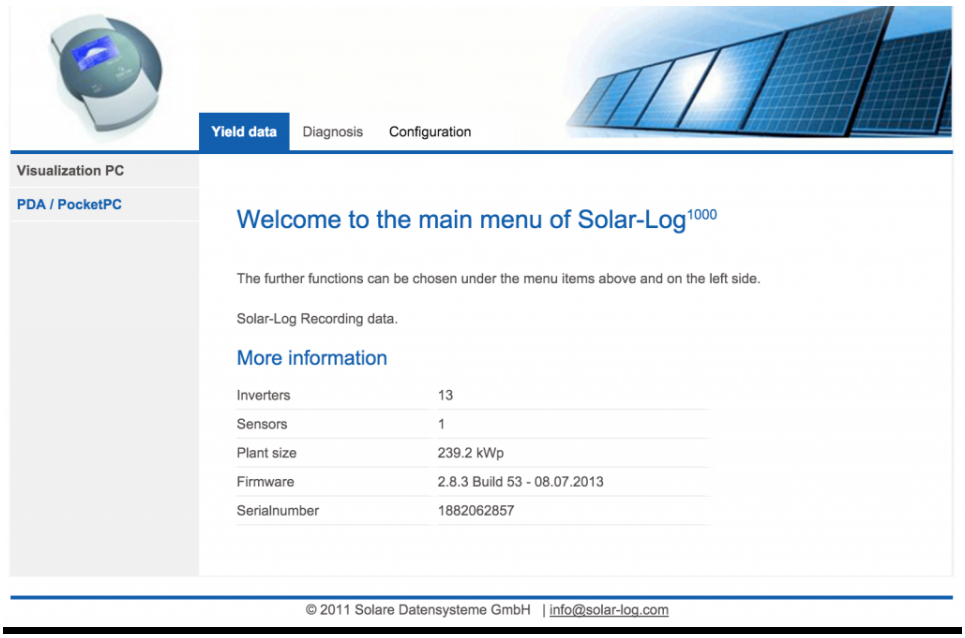
This is not a breaking news: The "*Internet of Things*" or connected objects is growing at the speed of the light. To convince the skeptics, just have a look at shodan.io to easily find plenty of devices that are (or should not be!) online.

A few days ago, I was discussing with a customer about an incident he faced: A corporate laptop was compromized via its 3G connectivity. Today, the IPv4 address space being full, mobile operators implement CGN ("*Carrier Grade NAT*") for most of their mobile customers. Even if NAT is not a firewall, it prevents incoming connections to reach the mobile device.

But, for some professional or high level services, public IP addresses can be assigned to mobile devices through their SIM card. This is particularly useful in M2M ("*Machine to Machine*") communications where devices must be sometimes reachable! While discussing about the incident with my customer, I got the IP address assigned to the 3G dongle. The IP address being part of a /16 network, it was too tempting to see what could be reached from the Internet. I searched for interesting open port and took some screenshots of discovered websites.

The pictures below are just a short resume of the findings: industrial systems, routers, exotic devices, etc. So many devices are publicly available… just being a mobile network connection. I also found MySQL, Remote Desktop and many other juicy services!

Note: no device was harmed during the scan 🙂



Powered by TRUESEC

Follow Me

Upcoming Events

Here is a list of events that I will attend and cover via Twitter and wrap-ups. Ping me if you want to meet! The list is regularly updated.

Recent Posts

The Truth is in Your Logs!

Physical Access == Pwn3d!

[SANS ISC Diary] Unity Makes Strength

Managing Palo Alto Firewalls Custom URL Categories

[SANS ISC Diary] Enforcing USB Storage Policy with PowerShell

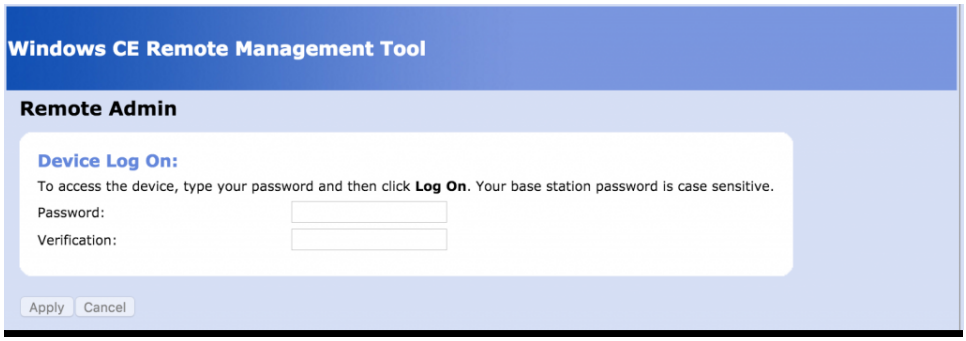
Popular Posts

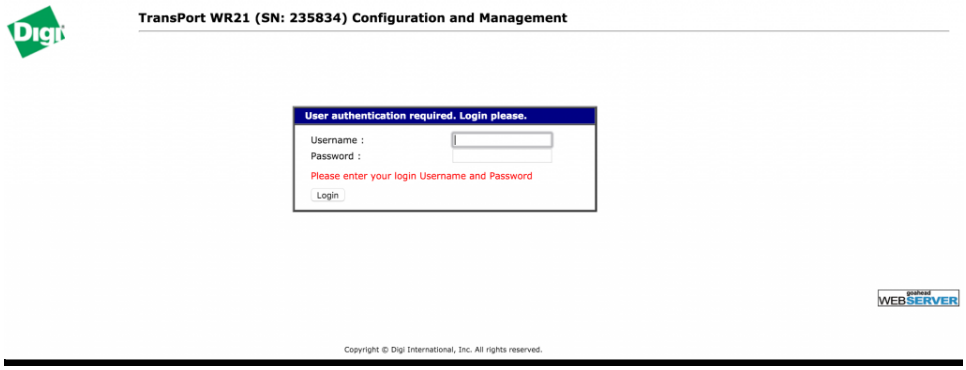
The Truth is in Your Logs!
2,049 views

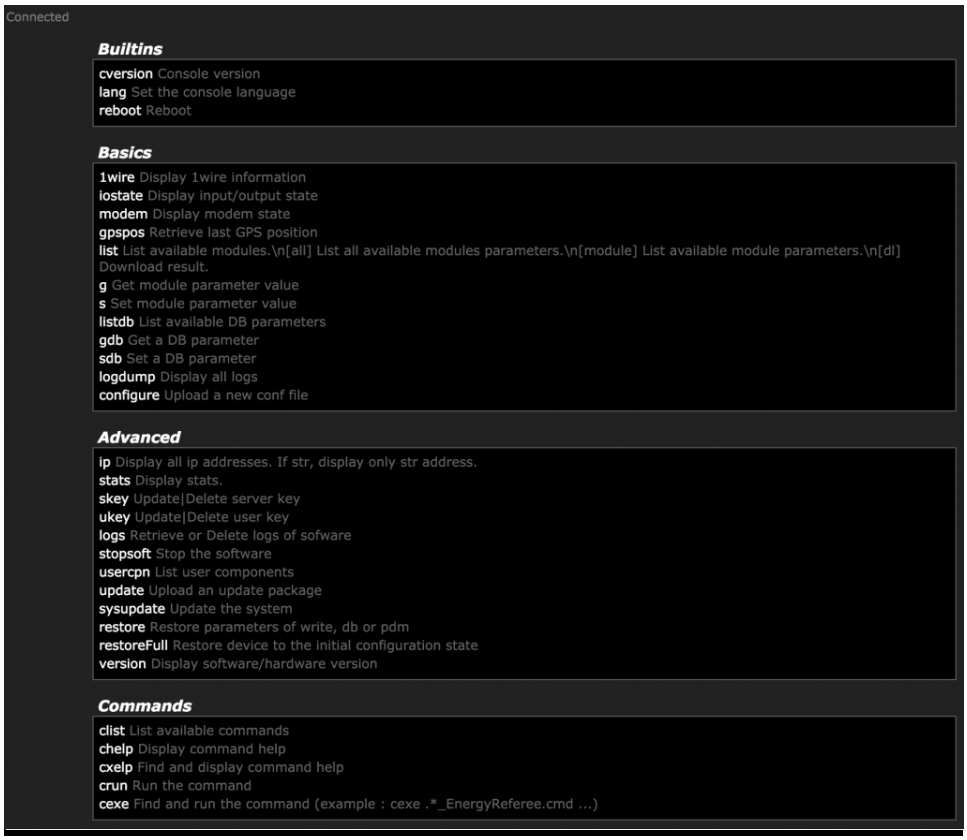
Physical Access == Pwn3d!
361 views

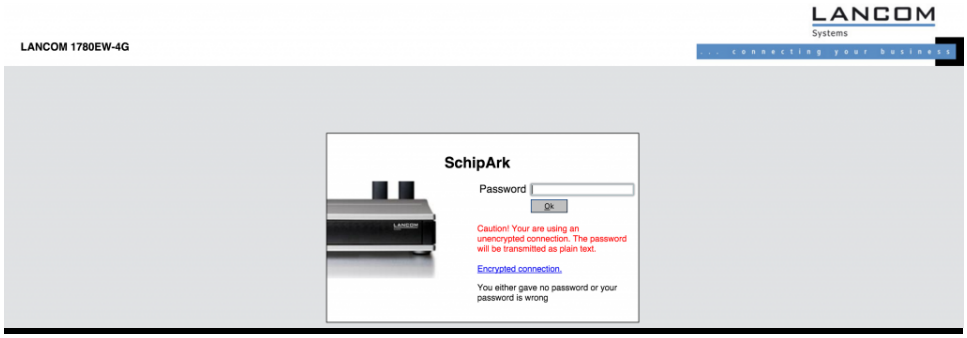
Managing Palo Alto Firewalls Custom URL Categories
206 views

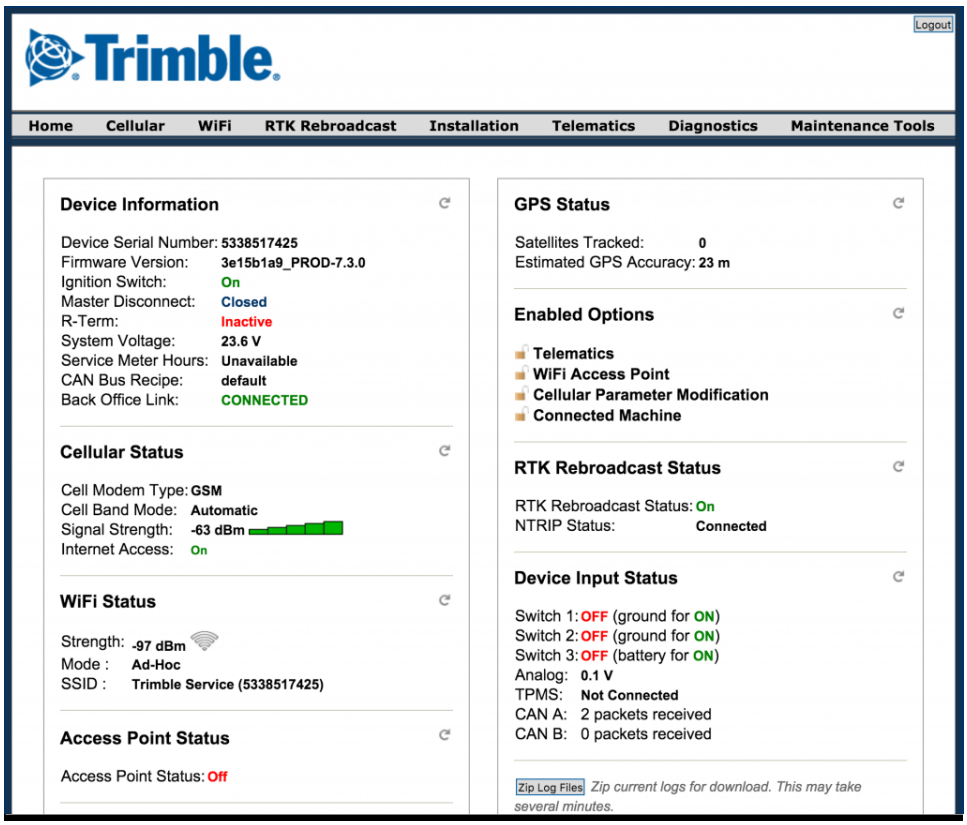
Show me your SSID's, I'll Tell Who You Are!

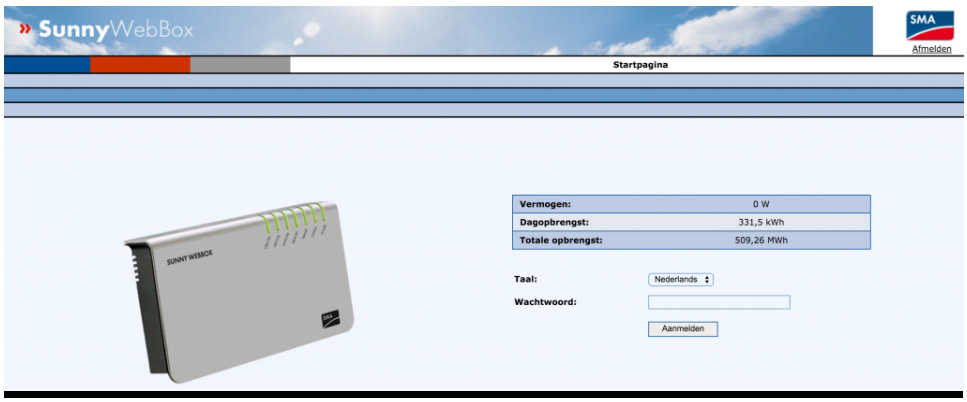


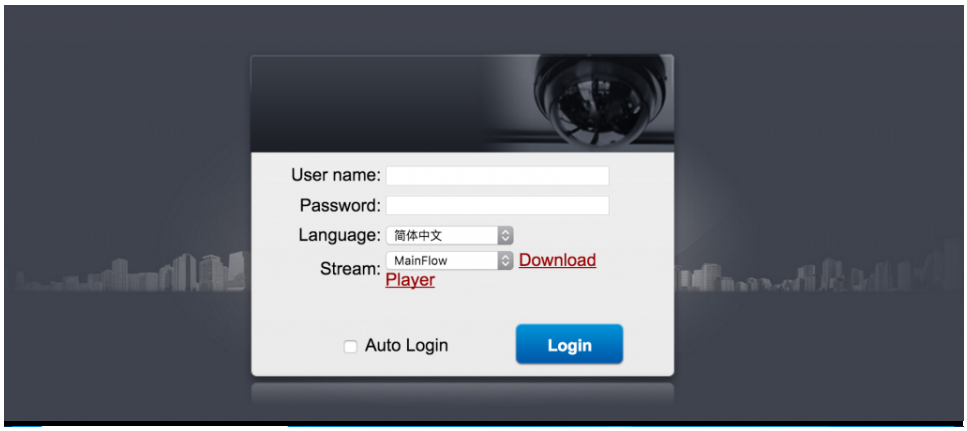












Vuln: Libxml2 'xmlParseConditionalSections()' Function Denial of Service Vulnerability

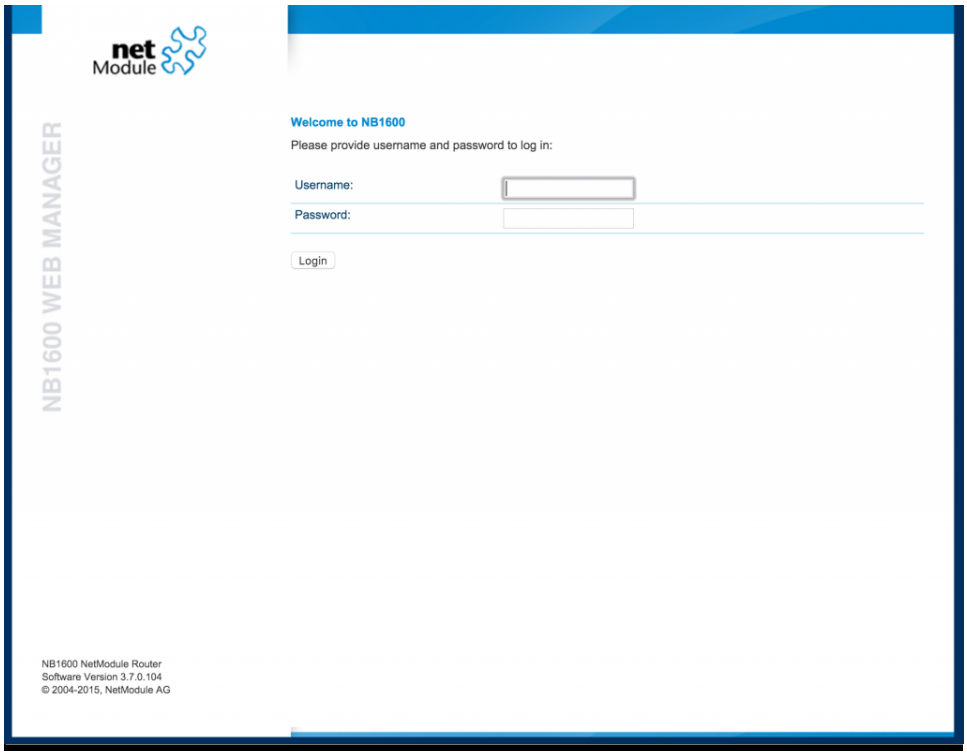
Bugtraq: [oCERT 2015-012] Ganeti multiple issues

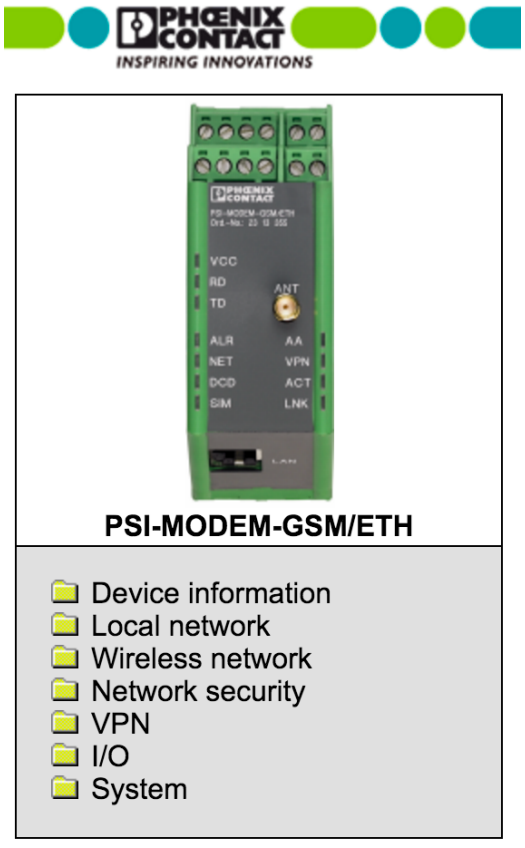
Bugtraq: WebKitGTK+ Security Advisory WSA-2015-0002

Bugtraq: libtiff bmp file Heap Overflow (CVE-2015-8668)

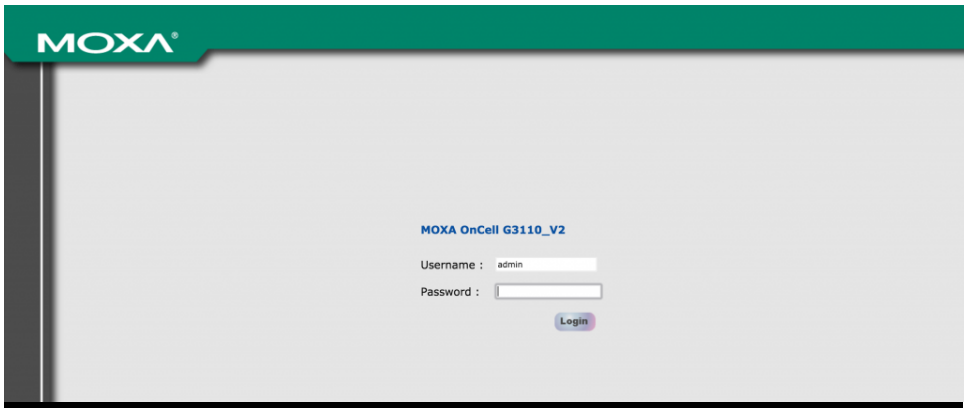
Bugtraq: libtiff: invalid write (CVE-2015-7554)

More rss feeds from SecurityFocus

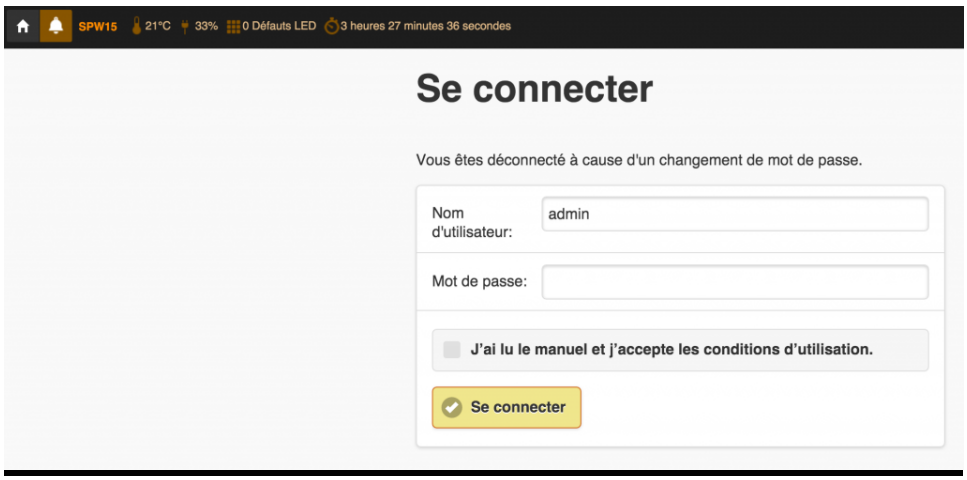




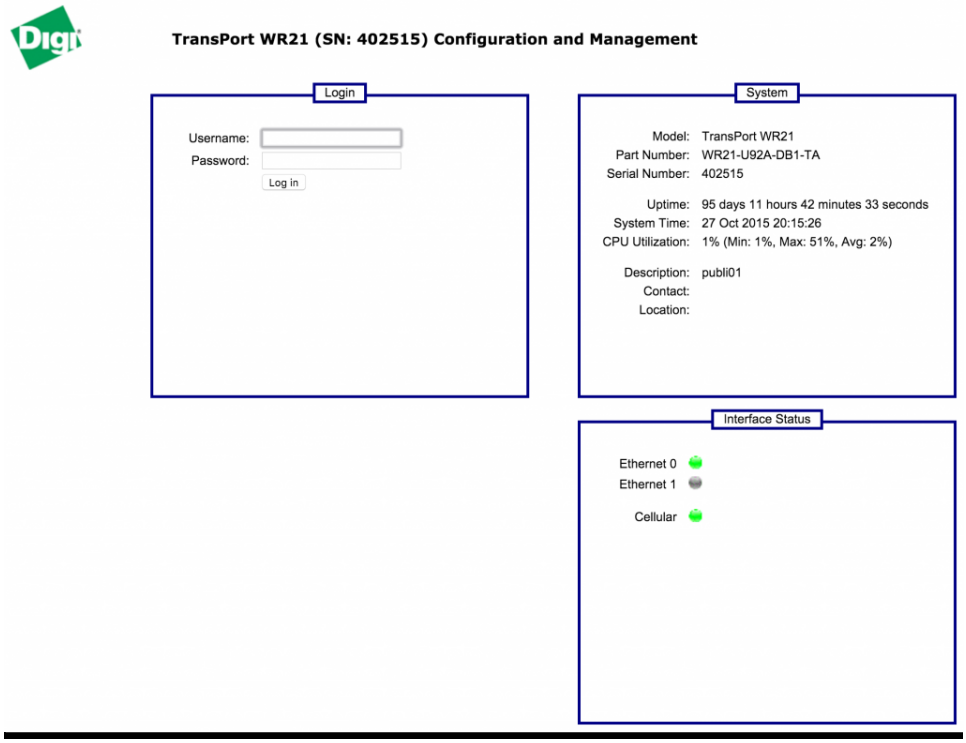
<%@ Language=VBScript %>
Welcome to BECKHOFF CE device

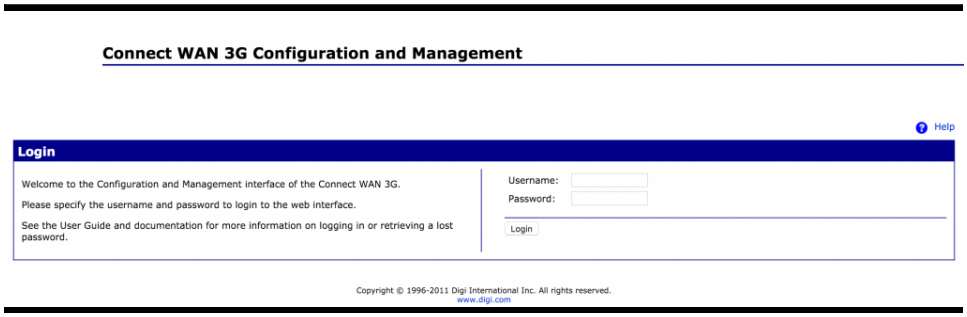

MOXA
MOXA OnCell G3110_V2
Username : admin
Password :
Login

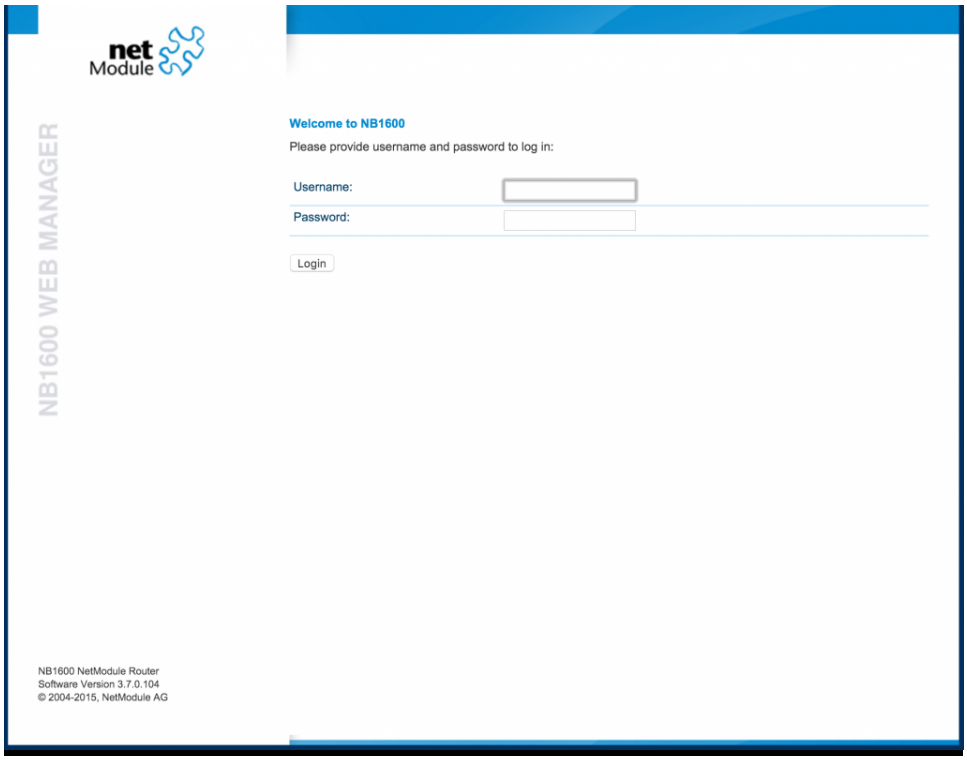

Login
Account
Password
Language
English
Login
D-Link


SPW15 21°C 33% 0 Défauts LED 3 heures 27 minutes 36 secondes
Se connecter
Vous êtes déconnecté à cause d'un changement de mot de passe.
Nom d'utilisateur: admin
Mot de passe:
J'ai lu le manuel et j'accepte les conditions d'utilisation.
Se connecter

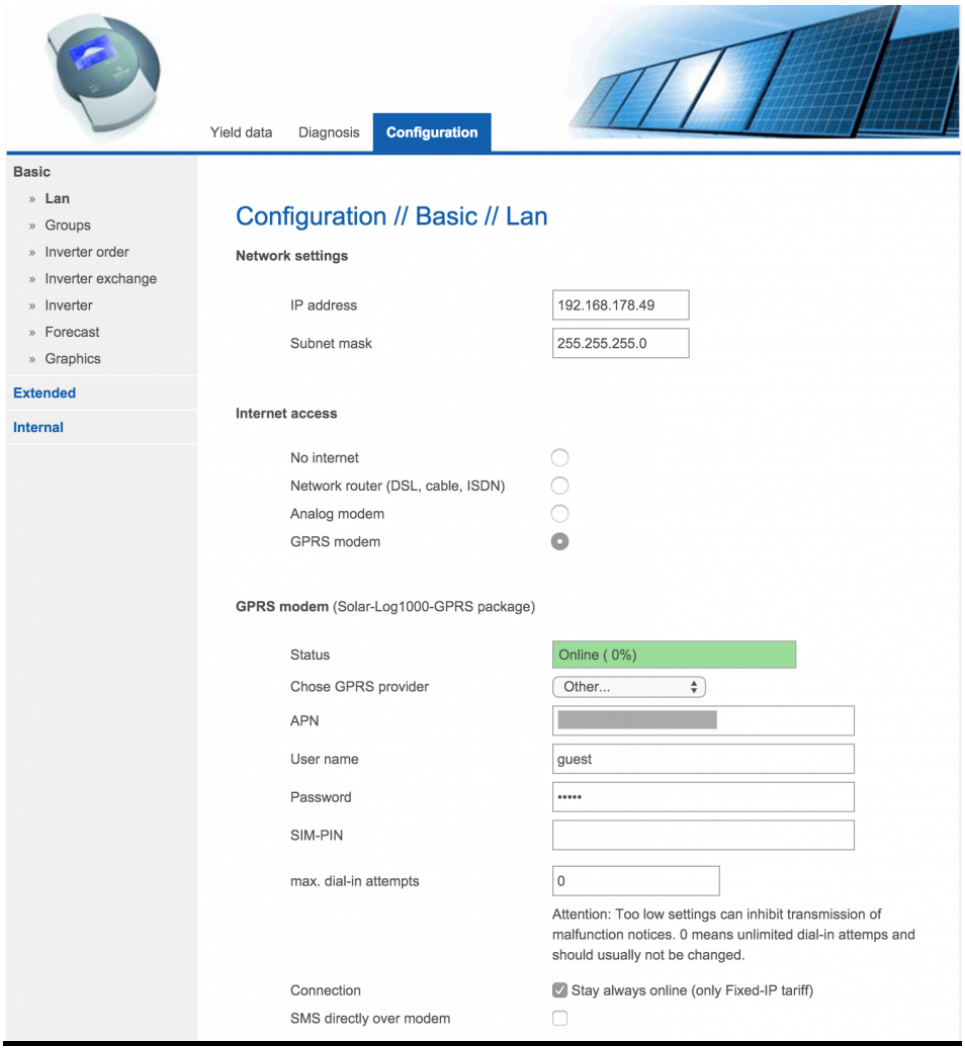

Intelligent Digital
Security System
PC
Web viewer
Mobile
Web viewer

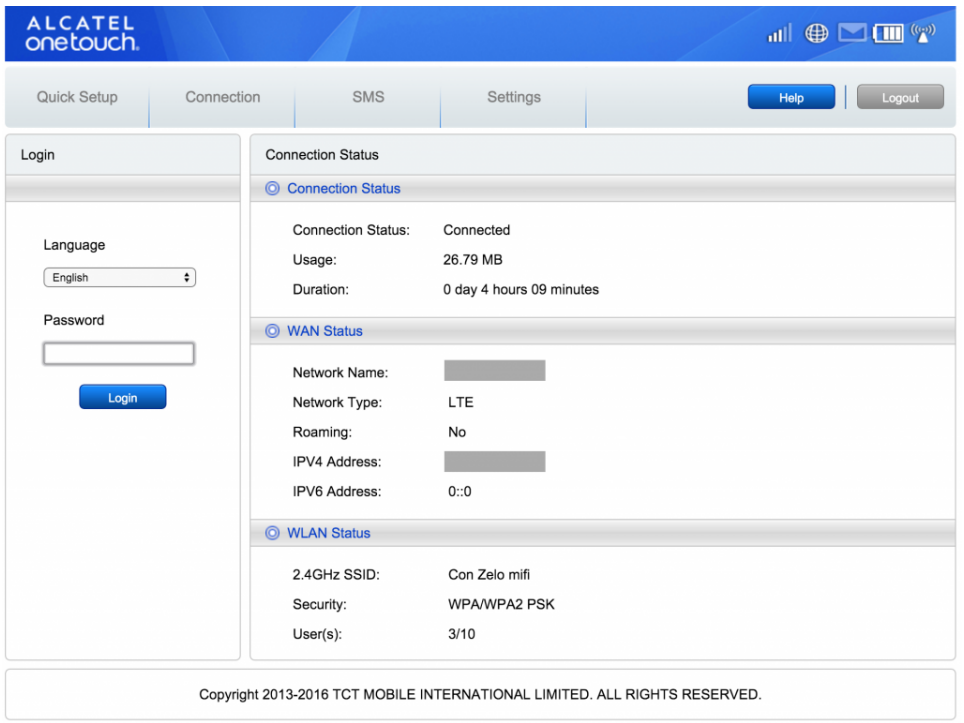

TransPort WR21 (SN: 402515) Configuration and Management
Login
Username:
Password:
Log in
System
Model: TransPort WR21
Part Number: WR21-U92A-DB1-TA
Serial Number: 402515
Uptime: 95 days 11 hours 42 minutes 33 seconds
System Time: 27 Oct 2015 20:15:26
CPU Utilization: 1% (Min: 1%, Max: 51%, Avg: 2%)
Description: publi01
Contact:
Location:
Interface Status
Ethernet 0
Ethernet 1
Cellular

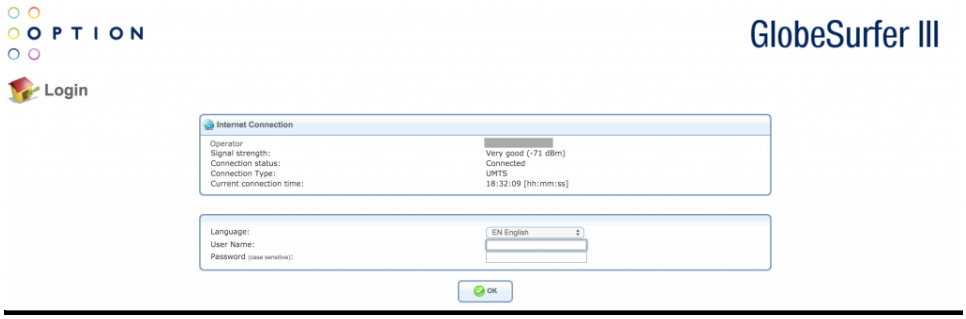

Connect WAN 3G Configuration and Management
Help
Login
Welcome to the Configuration and Management interface of the Connect WAN 3G.
Please specify the username and password to login to the web interface.
See the User Guide and documentation for more information on logging in or retrieving a lost password.
Username:
Password:
Login
Copyright © 1996-2011 Digi International Inc. All rights reserved.
www.digi.com


net Module
NB1600 WEB MANAGER
Welcome to NB1600
Please provide username and password to log in:
Username:
Password:
Login
NB1600 NetModule Router
Software Version 3.7.0.104
© 2004-2015, NetModule AG


Fronius
Fronius Datalogger Web
Realtime total view
en
Realtime total view
Realtime comparison view
Settings
11 °C
0 IG
12 °C
CO2 savings today ---
CO2 savings total ---
Earnings Today ---
Earnings Total ---
Digital 1
0 km/h
v2.0.1-1 / 1.4A
Update of version 2.0.1-1 to 2.0.5-4 available. :: Display changelog
Fronius International GmbH


Yield data
Diagnosis
Configuration
Basic
Lan
Groups
Inverter order
Inverter exchange
Inverter
Forecast
Graphics
Extended
Internal
Configuration // Basic // Lan
Network settings
IP address
192.168.178.49
Subnet mask
255.255.255.0
Internet access
No internet
Network router (DSL, cable, ISDN)
Analog modem
GPRS modem
GPRS modem (Solar-Log1000-GPRS package)
Status
Online (0%)
Chose GPRS provider
Other...
APN
User name
guest
Password
SIM-PIN
max. dial-in attempts
0
Attention: Too low settings can inhibit transmission of malfunction notices. 0 means unlimited dial-in attemps and should usually not be changed.
Connection
Stay always online (only Fixed-IP tariff)
SMS directly over modem


ALCATEL onetouch
Quick Setup
Connection
SMS
Settings
Help
Logout
Login
Language
English
Password
Login
Connection Status
Connection Status
Connection Status: Connected
Usage: 26.79 MB
Duration: 0 day 4 hours 09 minutes
WAN Status
Network Name:
Network Type: LTE
Roaming: No
IPV4 Address:
IPV6 Address: 0::0
WLAN Status
2.4GHz SSID: Con Zelo mifi
Security: WPA/WPA2 PSK
User(s): 3/10
Copyright 2013-2016 TCT MOBILE INTERNATIONAL LIMITED. ALL RIGHTS RESERVED.



Posted in: Uncategorized

Profile

Sign in with Twitter Sign in with Facebook
or

Comment

Name

Email

Not published

Website

Post It

- 9 Replies
- 0 Comments
- 9 Tweets
- 0 Facebook
- 0 Pingbacks

Last reply was 1 month ago

1. *@imifos*
   View 1 month ago
   @xme Please do not scan the internet. You can go to jail for doing this!! Scanning is allowed only to criminals!!

← Previous Post Next Post →