Operating System Description for Commsignia V2X Devices

Document ID: OS-002
Issue no.: 2-1

info@commsignia.com
http://www.commsignia.com

Contents

1 Overview of the operating system

The device is running a Linux-based operating system and can be accessed by the console through a serial connection or SSH and also through a graphical user interface (GUI) from a web browser.

The operating system is a Linux distribution for embedded services. It provides a file system with package management utilized by the Commsignia Software Stack. This operating system features extensible configuration possibilities for network-related settings, such as:

- IPv4 and IPv6 support
- Wireless functionality
- Firewall, NAT, port forwarding and other security functions
- Dynamically-configured port forwarding protocols UPnP and NAT-PMP through upnpd, etc.
- Load balancing for use with multiple ISPs using source-specific routing
- A writable root file system, enabling users to add, remove or modify any file.
- An extensive web based graphical user interface

It also uses a command line interface for configuring the system through a serial or an SSH connection.

The system can also be configured using the GUI and it is recommended to use this as the primary method for all configuration steps described in this document.

2 Accessing the Operating System

The following chapters contain information about accessing the operating system.

2.1 Log in using the GUI

This chapters details the necessary steps required to log in to the Graphical User Interface (GUI) of the operating system on the device.

Before you begin

Before connecting, make sure that the device is connected to the network, all antennas are attached and powered up. The device must also have a previously configured IP address.

Procedure

1. Open a web browser and enter the IP address previously configured for the device. The default IP address is 192.168.0.54 and the default password is UK5BJLFZVBPZLIM55Y. We recommend changing the default values after the first login.
2. When prompted with the login screen, enter the password for `root` access. The default `root` password is shared separately and it can later be changed in the **System** > **Administration** menu.

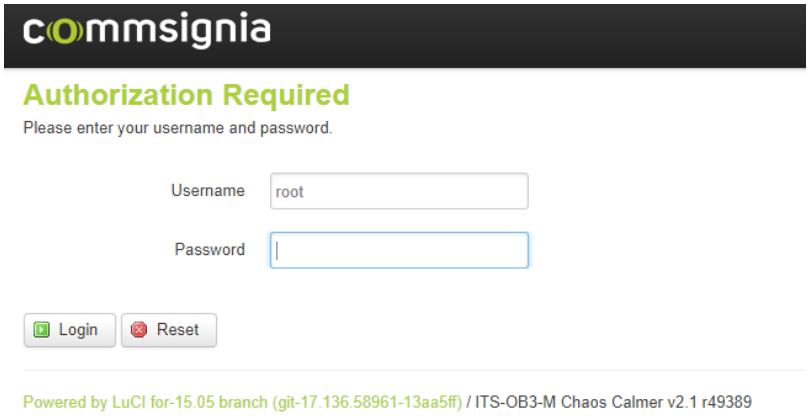


Figure 1: The GUI login screen

3. After successfully logging in, you will be prompted with the GUI overview page.

Figure 2: The GUI overview page after successfully logging in

Results

You are now successfully connected to the device, using the GUI.

What to do next

You can use this interface to configure settings and gather information from the device.

2.2 Log in using SSH

This chapter describes how to log in to the device using an SSH connection.

Before you begin

Before connecting to the device make sure it is connected to the network and the antennas and it is powered up. The device must also have a previously configured IP address for a successful SSH connection.

Procedure

1. Open an SCP connection with the following settings. Any SCP connection capable software can be used, in this example we have used `WinSCP`.

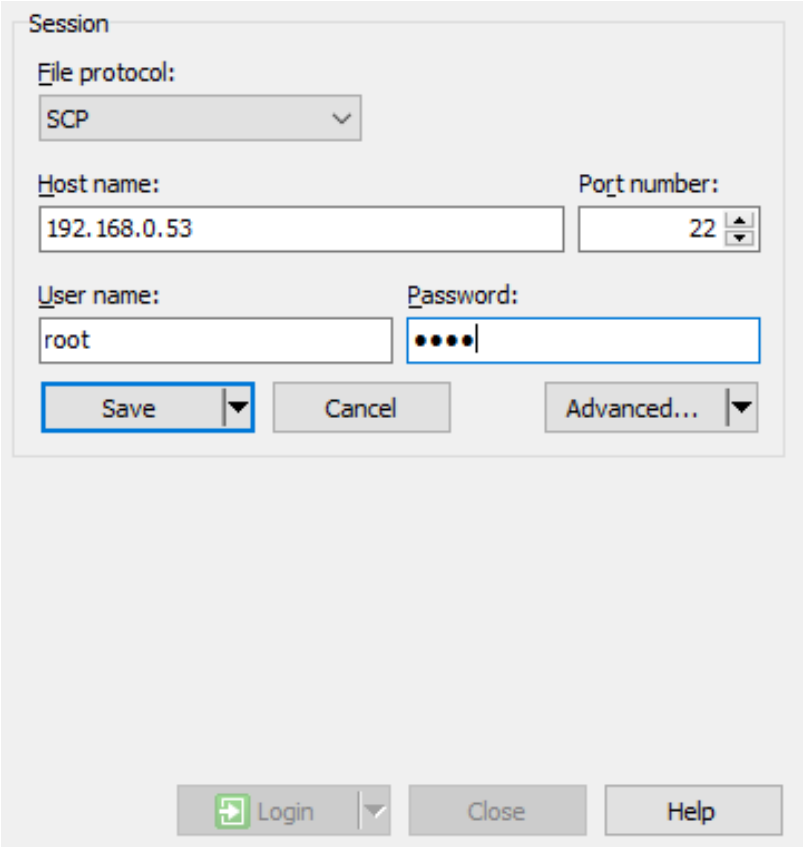


Figure 3: SCP client settings

File protocol	SCP
Host name	The IP address of the device.
Port number	22 - This is the default value. You can change this later using the **System** > **Administration** menu in the GUI.

2. Enter the `root` password to gain access. The default password for the device is shared separately. This can also be changed later, using the **System** > **Administration** menu in the GUI.

Results

You are successfully connected to the device with an SSH connection.

What to do next

SSH connection can be used for a remote terminal connection to the host system or you can use SCP for transferring and editing files on the file system of the device.

3 Security

3.1 Changing the password

This chapter describes the steps for changing the password using the GUI, as well as using an SSH connection.

Before you begin

To successfully complete these steps you must have previously completed the initial configuration steps to set up an IP address for the device.

Procedure

- You can change the password using the GUI in the **System** > **Administration** menu.

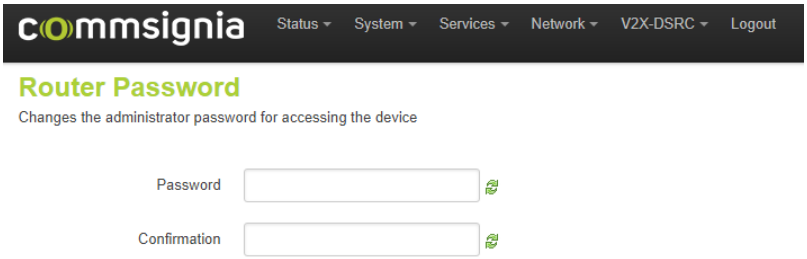


Figure 4: Changing the password in the GUI

  Please make sure to remember your password, because it is needed every time you want to access the device and its configuration options.
- Alternatively, after connecting to the device using a SSH connection, you can enter a new password using the `passwd` command in the console.

Results

After successfully completing one of the above mentioned steps your new password is configured for accessing the device.

3.2 Password reset

You can optionally set up an SMTP server with an administrator email address for the device to enable a password recovery link on the login page of the web GUI. For any further questions regarding password recovery, contact Commsignia support.

3.3 Firewall

You can check the status of the firewall under the **Status** > **Firewall** menu.

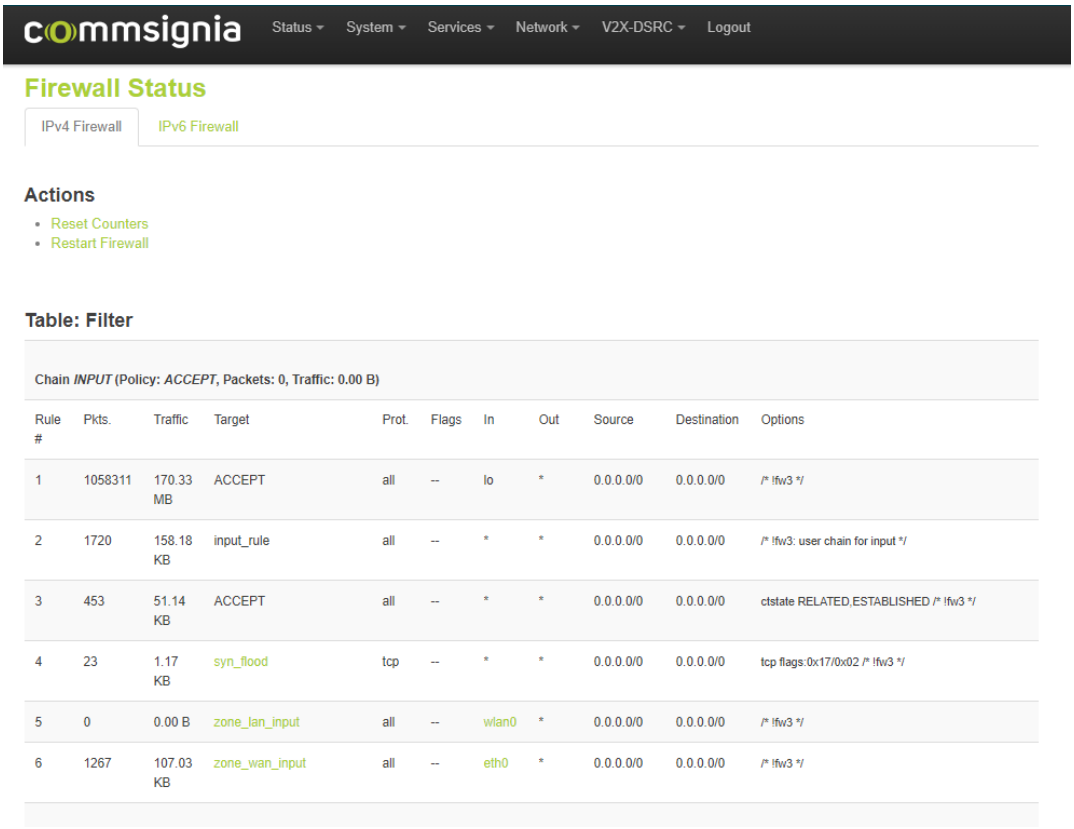


Figure 5: Firewall status

Firewall related settings can be configured under the **Network** > **Firewall** menu.

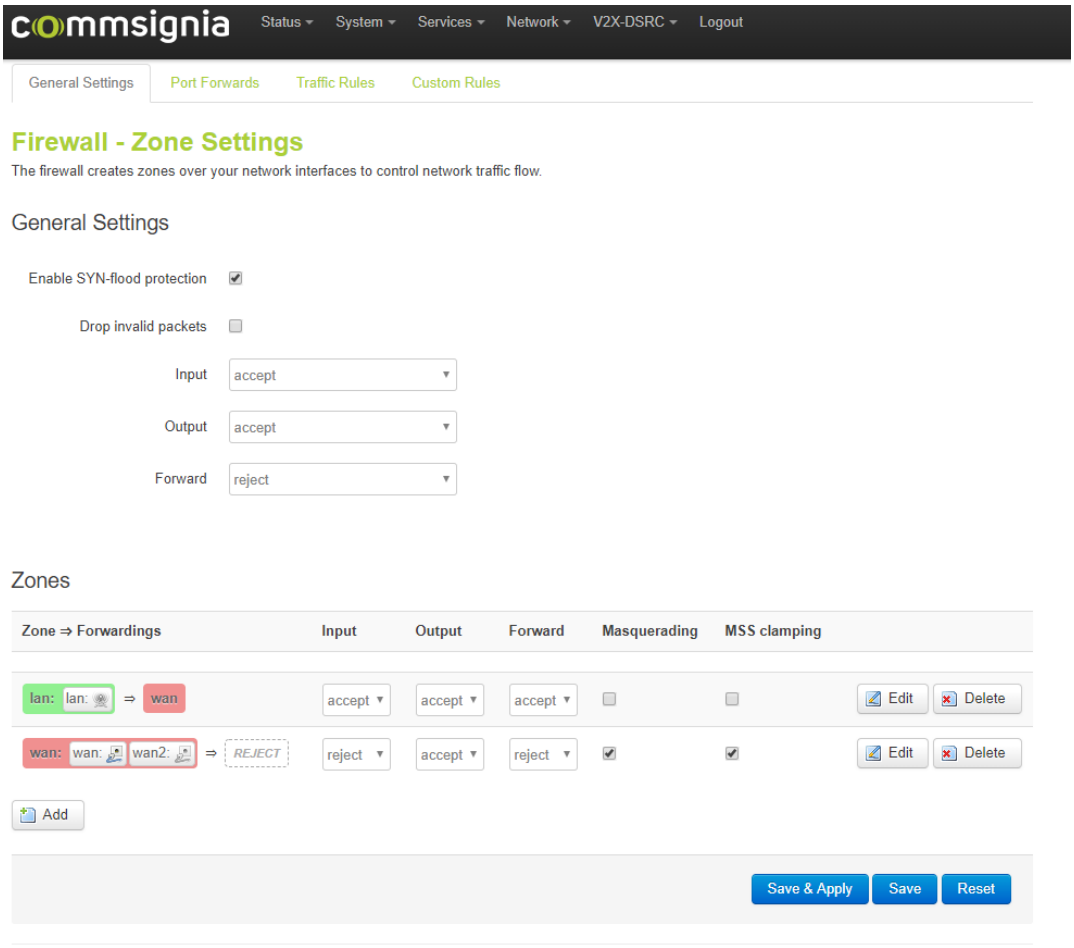


Figure 6: Firewall configuration menu

The firewall's default configuration keeps only the following specific ports open.

For TCP:

- HTTP
- HTTPS
- SSH
- SNMP

For UDP:

- SNMP
- mDNS (Avahi)

Other ports (such as NTCIP, EAS) must be opened manually in the firewall configuration menu described above.

Note: Upgrading the device's software to a newer version does NOT affect firewall configuration, even if it is not secure.

4 System information

4.1 Version information

This chapter provides an overview about the versions of the operating system and the individual software packages and where to find them in the GUI.

Operating system and GUI versions

The version numbers of the operating system and the GUI can be checked on the bottom of each page and in the **Status** > **Overview** menu. It is listed under the `System` headline.

Figure 7: The Overview page showing the system version

Package versions

The installed package versions can be checked under the **System** > **Software** menu.

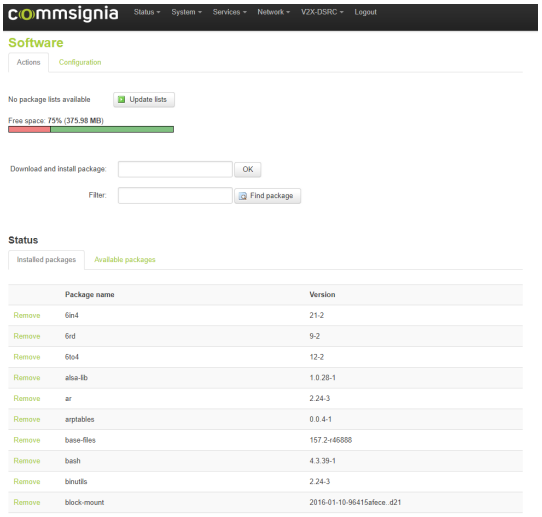


Figure 8: Package versions

Software stack versions

The version of the Commsignia Unplugged-RT software stack can be checked in the **V2X-DSRC** > **Stack** menu.

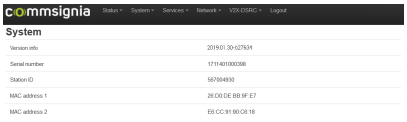


Figure 9: Unplugged-RT versions

4.2 System Uptime

The uptime of the operating system can be checked on the overview page in the **Status** > **System** menu in the GUI.

Figure 10: The overview page showing the uptime of the operating system

4.3 RAM and CPU usage of the running processes

Detailed information can be gathered about the resource usage of each running process in the **Status** > **Processes** menu in the GUI. This view shows the Process ID, the Owner and the Command name as well as the CPU and RAM usage. You also have the option to `Hang Up`, `Terminate`, or `Kill` each process.

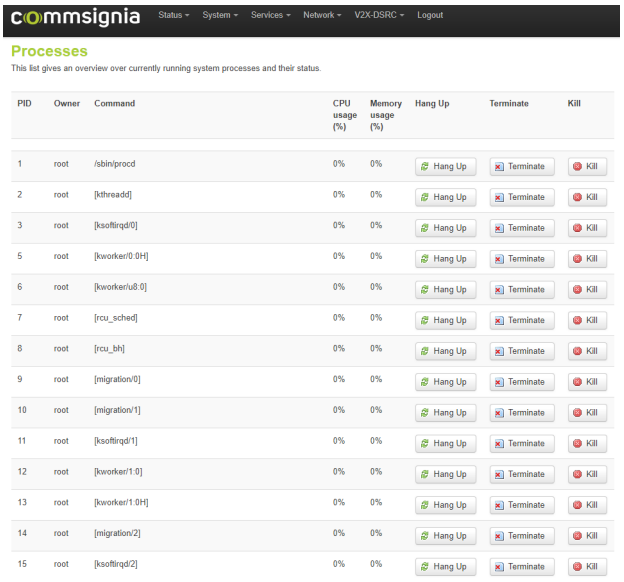


Figure 11: The Processes screen in the GUI

4.4 System log

The system logs can be accessed in the **Status** > **System log** menu. Configuration options related to logging - such as the address of an external logging server or the log output level - can be changed in the **System** > **System** menu, in the Logging tab.

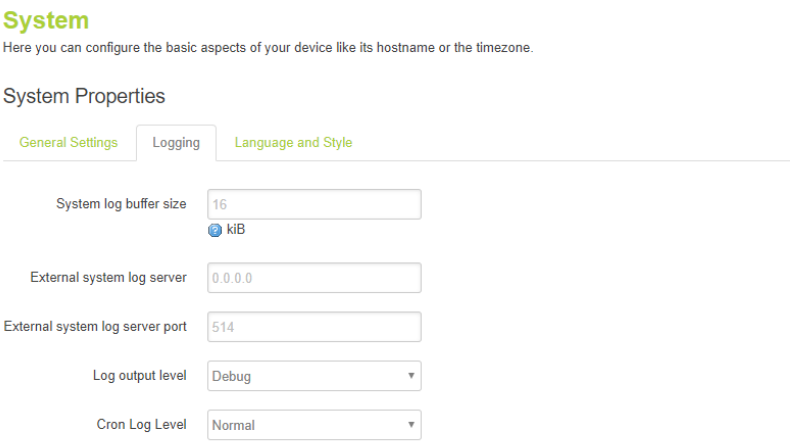


Figure 12: System properties - Logging tab

4.5 CAN interface

You can use the commands detailed in this section to communicate with a vehicle's CAN bus. For the physical CAN connection layout, refer to the hardware description of the device.

To receive information from a CAN interface:

```
candump can0
```

To send data to a CAN interface:

```
cansend can0 100#00000000
```

In this example can0 is the number of the CAN interface connection, 100 is the ID, and zeros represent the sent data.

5 Network configurations

The following chapters provide details about the various available network configurations for the device.

5.1 Configuring a static wired network

This chapters details the necessary steps required to configure a wired network connection with a static IP address for the device using the GUI.

Before you begin

Make sure the device is connected to the network, all antennas are attached and powered up. The device must also have a previously configured IP address.

Procedure

1. Open a web browser and enter the IP address previously configured for the device.
2. When prompted with the login screen, enter the password for `root` access. The default `root` password is shared separately and it can later be changed in the **System** > **Administartion** menu.

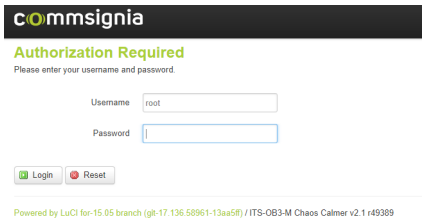


Figure 13: The login screen

3. Select the `Network Interfaces` menu option from the menu bar on the top of the page. On this page you can see a list of the already configured interfaces with their status and basic configurations. You can also `Connect`, `Stop`, `Edit`, or `Delete` each individual interface.

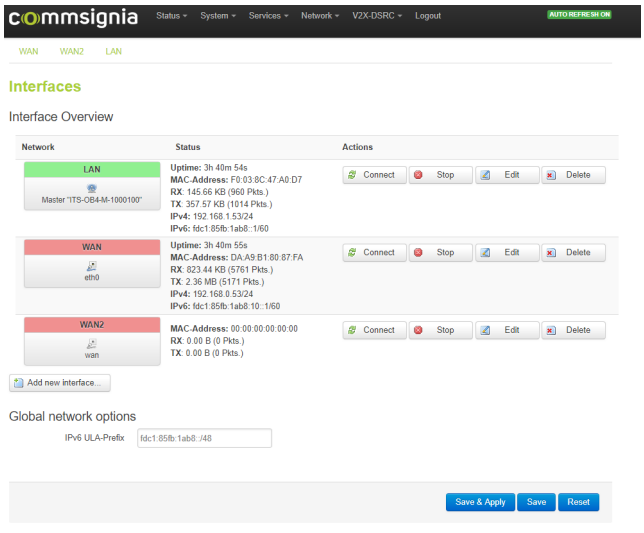


Figure 14: The Interfaces page

4. Select the `Edit` button of an already existing interface that you would like to configure.

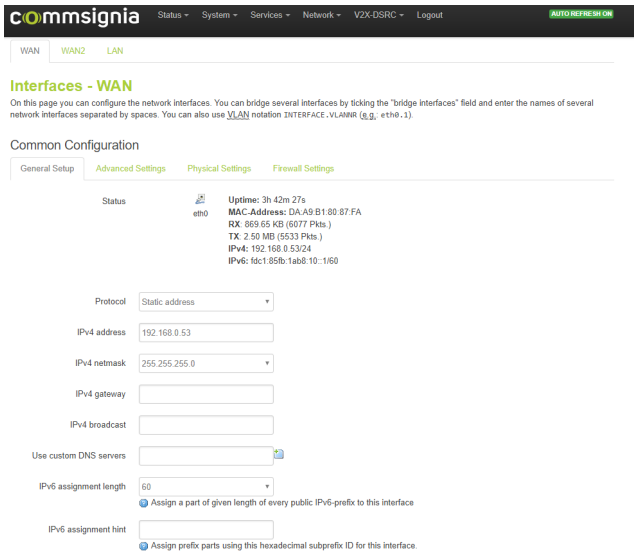


Figure 15: The general configuration page for the selected interface

The general setup page will let you configure the basic settings for the connection. Select Static address as the protocol and provide the IPv4 address, netmask, and gateway that you want to use for the device.

You can also select, the **`Add new interface...`** button if you want to create a new interface for the device.

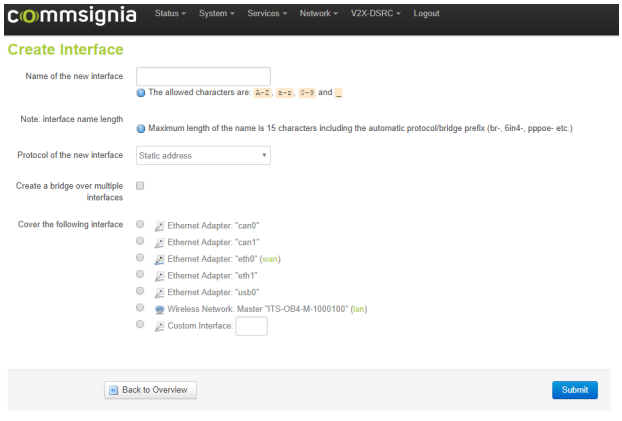


Figure 16: The Create Interface page

This option will let you create a new interface with a static address and the name of your choice. After providing all details, click the Submit button. This will take you to the general configuration page mentioned above, where you can provide the same basic IP settings for your newly created interface.

5. Select the **`Advanced Settings`** tab

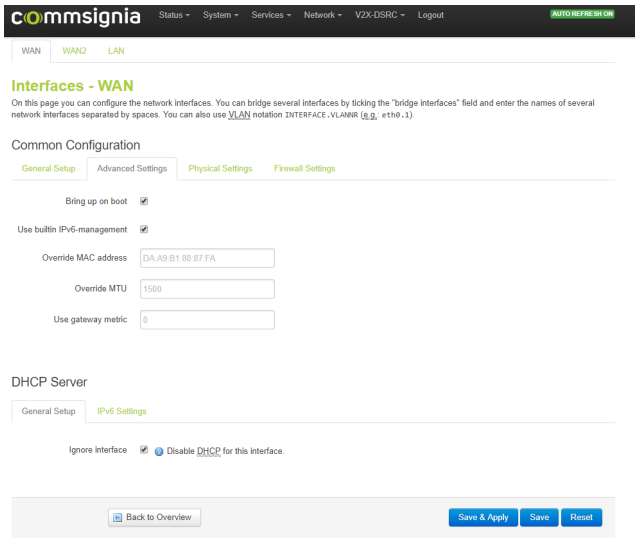


Figure 17: The Advanced settings page

Here you can specify the advanced network configurations if you have to. It is recommended to use the default settings.

6. Select the Physical Settings tab

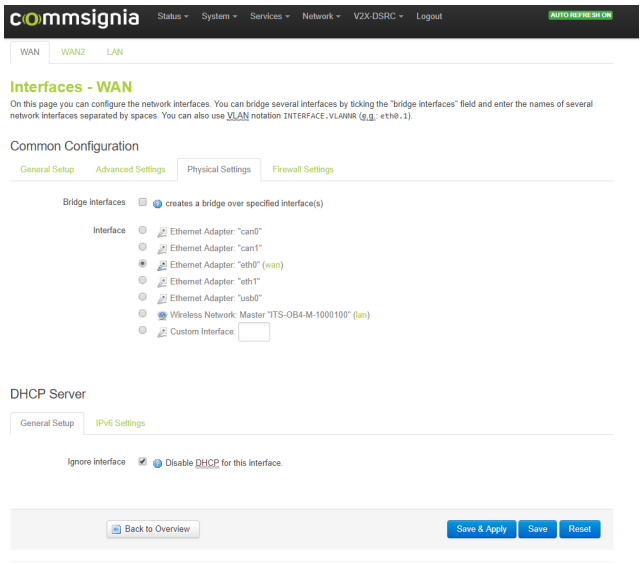


Figure 18: The Physical Settings tab

You can select the Ethernet Adapter for the interface or you can create a bridge over the specified interfaces.

7. Select the Firewall Settings tab

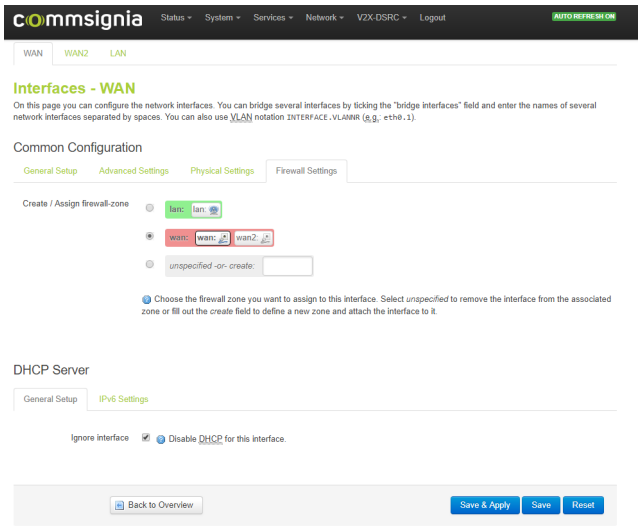


Figure 19: The Firewall Settings tab

You can create or assign a firewall zone for the interface on this page.

8. Click the Save and Apply button. The changes will be saved and will take immediate effect. No restart is necessary. You can reconnect to the GUI with the newly specified IP address if you want to make further changes.

Results

An Ethernet network connection is configured for the device with a static IP address.

5.2 Configuring a DHCP wired network

This chapters details the necessary steps required to configure a wired network connection with DHCP for the device using the GUI.

Before you begin

Make sure the device is connected to the network, all antennas are attached and powered up. The device must also have a previously configured IP address.

Procedure

1. Open a web browser and enter the IP address previously configured for the device.
2. When prompted with the login screen, enter the password for `root` access. The default `root` password is shared separately and it can later be changed in the **System** > **Administartion** menu.

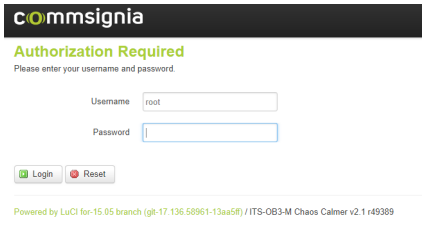
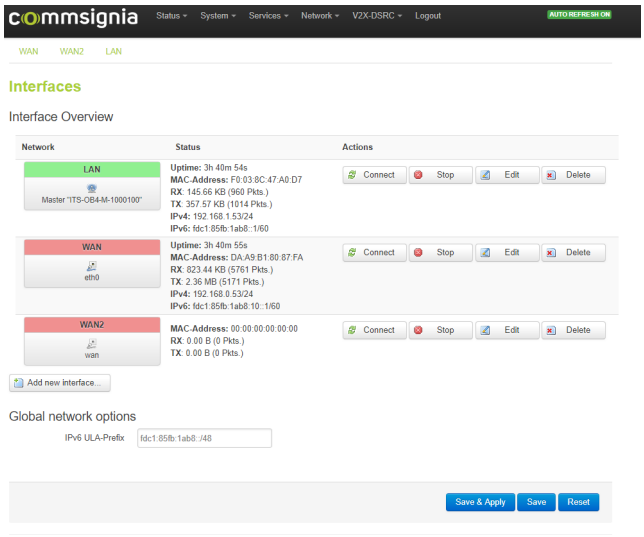


Figure 20: The login screen

3. Select the `Network Interfaces` menu option from the menu bar on the top of the page.



On this page you can see a list of the already configured interfaces with their status and basic configurations. Yo

Figure 21: The Interfaces page

4. Select the **`Edit`** button of an already existing interface that you would like to configure.

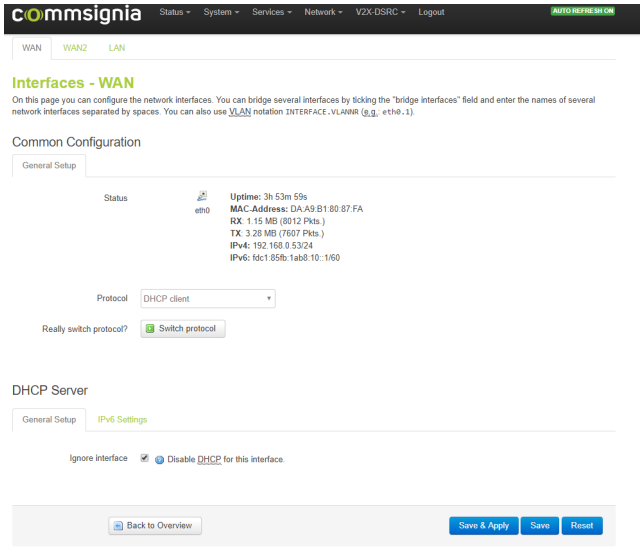


Figure 22: The general configuration page for the selected interface

The general setup page will let you configure the basic settings for the connection. Select DHCP as the protocol and when prompted confirm the changing of the protocol.

You can also select, the **`Add new interface...`** button if you want to create a new interface for the device.

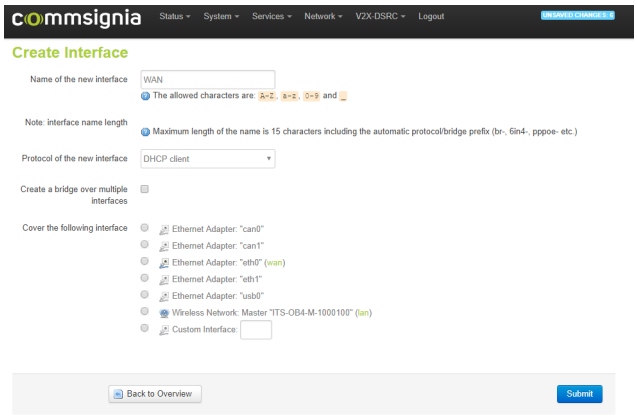


Figure 23: The Create Interface page

This option will let you create a new interface with DHCP and the name of your choice. After providing all details, click the Submit button. This will take you to the general configuration page mentioned above, where you can provide the same basic network settings for your newly created interface.

5. Select the `Advanced Settings` tab

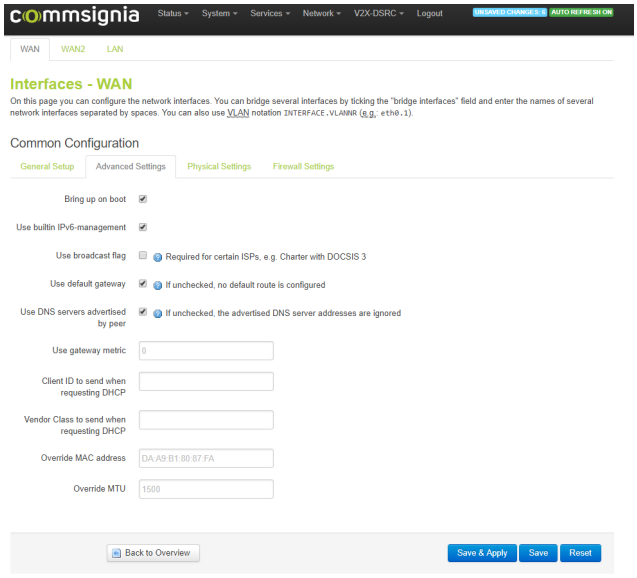


Figure 24: The Advanced settings page

Here you can specify the advanced network configurations if you have to. It is recommended to use the default settings.

6. Select the Physical Settings tab

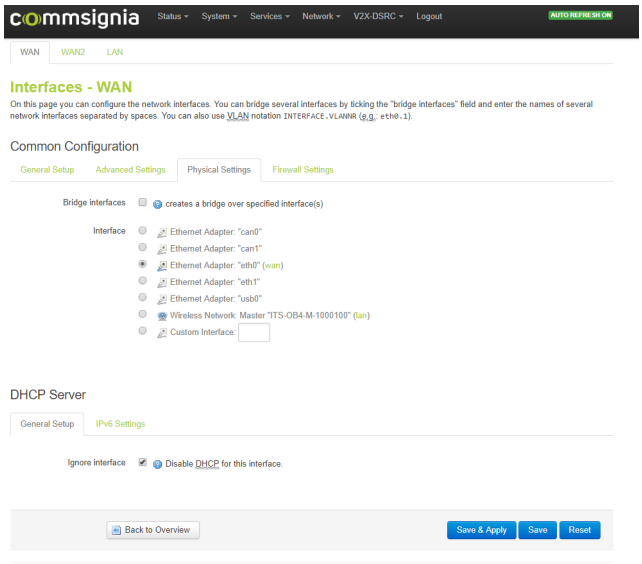


Figure 25: The Physical Settings tab

You can select the Ethernet Adapter for the interface or you can create a bridge over the specified interfaces.

7. Select the Firewall Settings tab

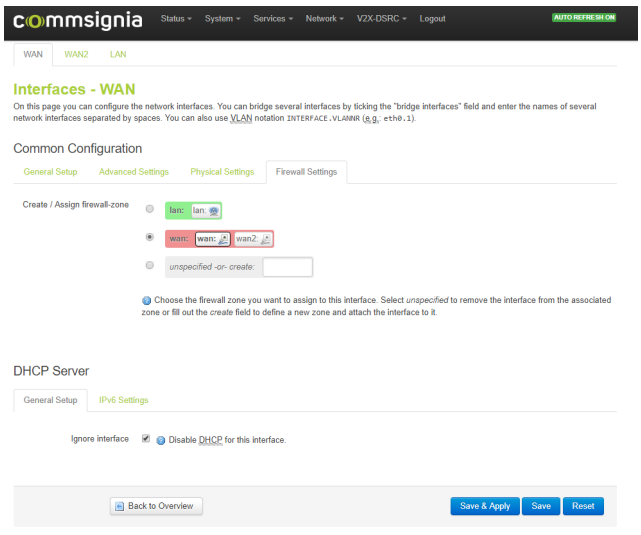


Figure 26: The Firewall Settings tab

You can create or assign a firewall zone for the interface on this page.

8. Click the Save and Apply button. The changes will be saved and will take immediate effect. No restart is necessary. You can reconnect to the GUI with the newly specified IP address if you want to make further changes.

Results

An Ethernet network connection is configured for the device with DHCP.

5.3 Configuring the device as a client for a wireless network with a

This chapters details the necessary steps required to configure a wireless network connection with a Static IP address for the device using the GUI.

Before you begin

Make sure the device is connected to the network, all antennas are attached and powered up. The device must also have a previously configured IP address.

Procedure

1. Open a web browser and enter the previously configured IP address for the device. When prompted, log in with `root` access.

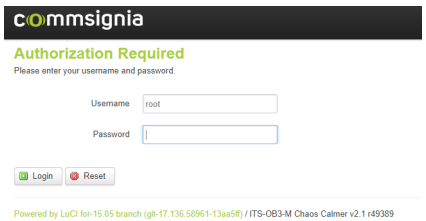


Figure 27: The login screen

2. Select the **Network** > **Interfaces** menu. This will show a list of the already configured interfaces available on the device.

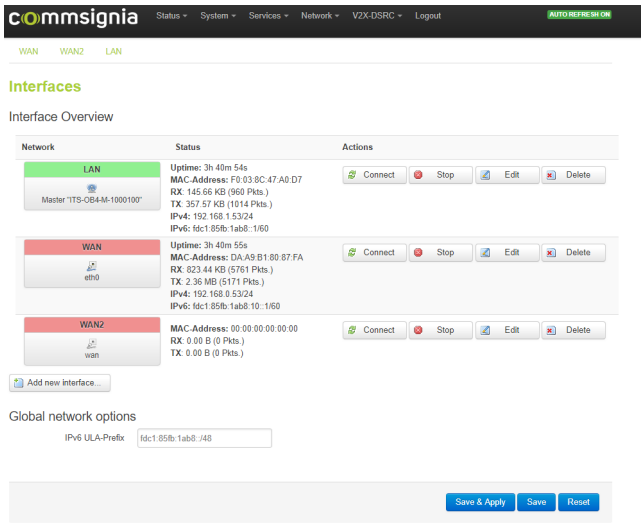


Figure 28: The Interfaces page

3. By default, the wireless connection is configured for the LAN interface. Click the `Edit` button to change the settings for an already existing interface or click the `Add new interface...` button if you want to configure a new interface for a wireless connection.

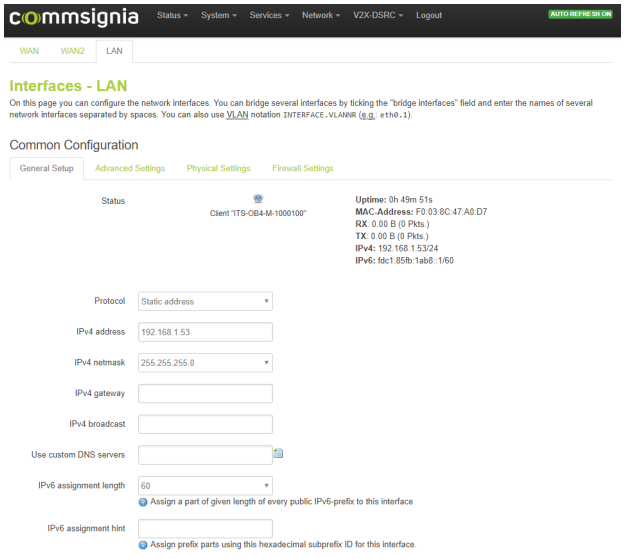


Figure 29: Static protocol selected for wireless access

Select `Static address` as the `Protocol` for the interface. Confirm this choice by clicking on the `Switch protocol` button if prompted.

4. You can select the `Advanced Settings`, `Physical Settings` and `Firewall Settings` tabs in case you have to make changes but it is recommended to leave the default settings.
5. Select the **Network** > **Wifi** menu from the menu bar on the top of the page. This will show you an overview of available wireless modules.

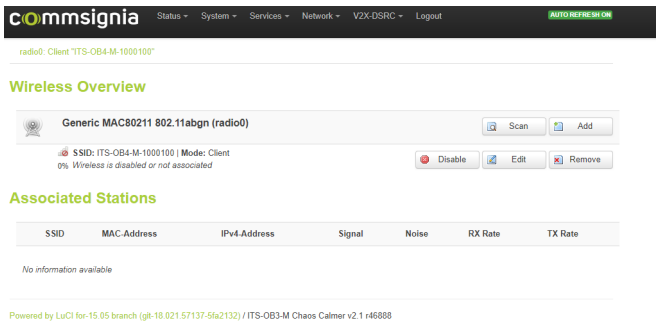


Figure 30: Wireless Overview

6. Click the `Edit` button. This will show you the page for `General Setup` for the `Device Configuration` and the `Interface Configuration` settings.

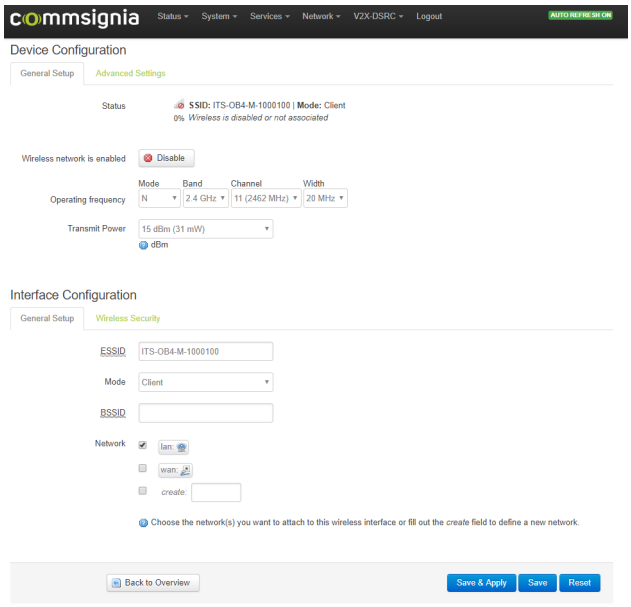


Figure 31: Configurations page

Here you can enable or disable the wireless connection, change the operating frequency settings, change the ESSID, or change the Mode for the interface (for example from Client to Access point). It is recommended to leave the default settings.

7. Select the `Advanced Settings` tab for further configuration options for the device.

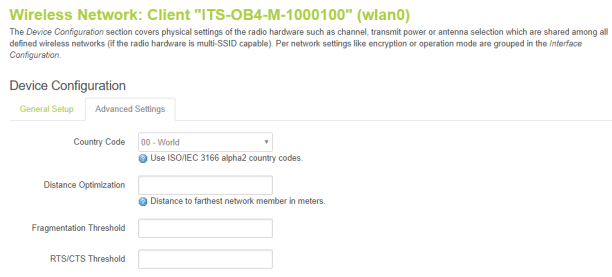


Figure 32: Advanced wireless settings for the device

8. Select the Wireless Security tab under Interface Configuration, to configure security options for the wireless interface (such as the Encryption method and the passkey for the connection).

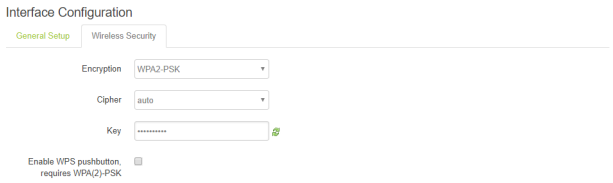


Figure 33: Wireless security settings

9. Click the `Save & Apply` button for the changes to take effect immediately. No reboot is required.

Results

You have successfully configured an interface for a wireless connection on the device with a Static IP address.

5.4 Configuring the device as a client for a wireless network with DI

This chapters details the necessary steps required to configure a wireless network connection with DHCP for the device using the GUI.

Before you begin

Make sure the device is connected to the network, all antennas are attached and powered up. The device must also have a previously configured IP address.

Procedure

1. Open a web browser and enter the previously configured IP address for the device. When prompted, log in with `root` access.

Figure 34: The login screen

2. Select the **Network** > **Interfaces** menu. This will show a list of the already configured interfaces available on the device.

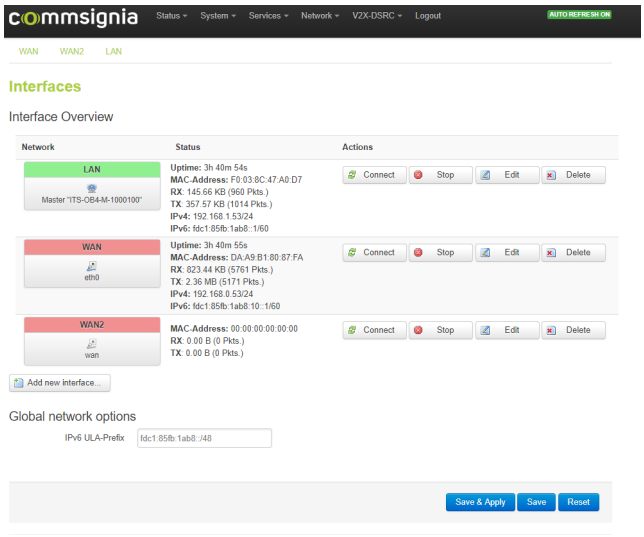


Figure 35: The Interfaces page

3. By default, the wireless connection is configured for the LAN interface. Click the `Edit` button to change the settings for an already existing interface or click the `Add new interface...` button if you want to configure a new interface for a wireless connection.

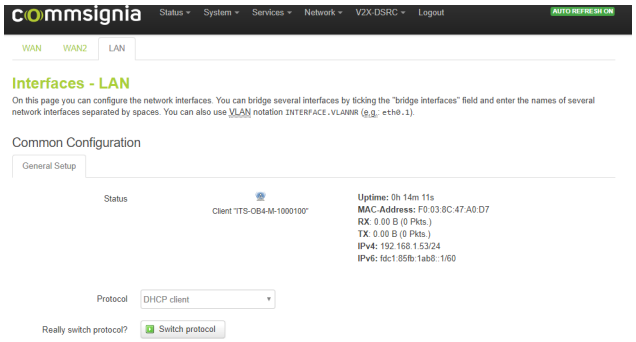


Figure 36: DHCP protocol selected for wireless access

Select `DHCP client` as the `Protocol` for the interface. Confirm this choice by clicking on the `Switch protocol` button.

4. You can select the `Advanced Settings`, `Physical Settings` and `Firewall Settings` tabs in case you have to make changes but it is recommended to leave the default settings.
5. Select the **Network** > **Wifi** menu from the menu bar on the top of the page. This will show you an overview of available wireless modules.

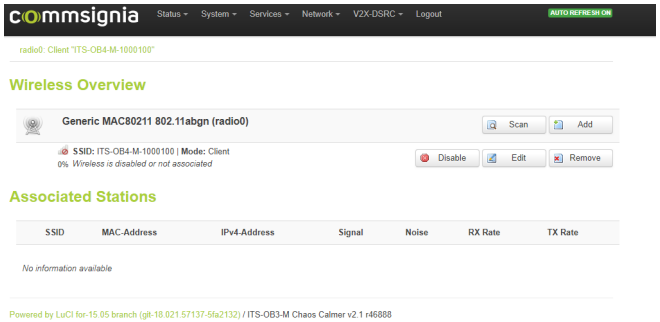


Figure 37: Wireless Overview

6. Click the `Edit` button. This will show you the page for `General Setup` for the `Device Configuration` and the `Interface Configuration` settings.

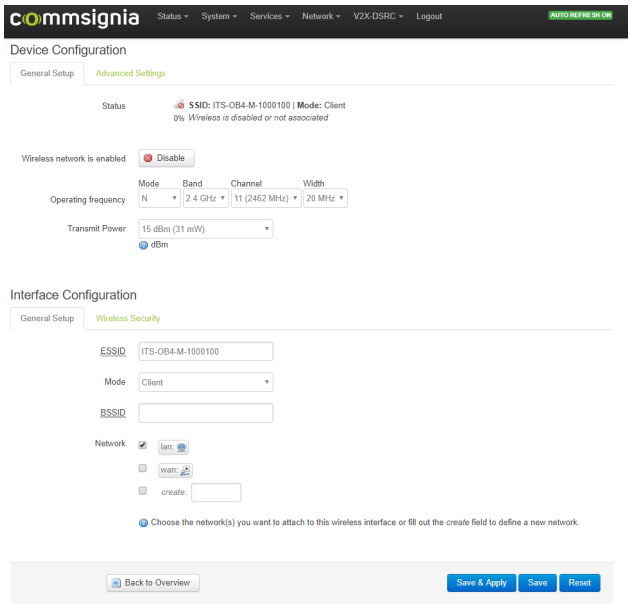


Figure 38: Configurations page

Here you can enable or disable the wireless connection, change the operating frequency settings, change the ESSID, or change the Mode for the interface (for example from Client to Access point). It is recommended to leave the default settings.

7. Select the `Advanced Settings` tab for further configuration options for the device.

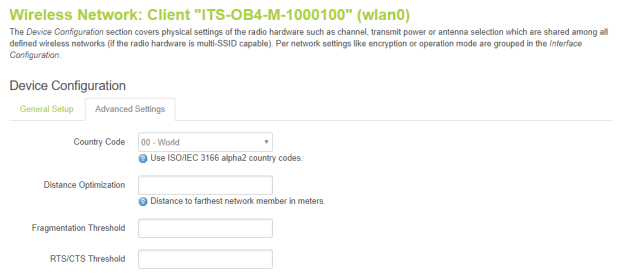


Figure 39: Advanced wireless settings for the device

8. Select the Wireless Security tab under Interface Configuration, to configure security options for the wireless interface (such as the Encryption method and the passkey for the connection).

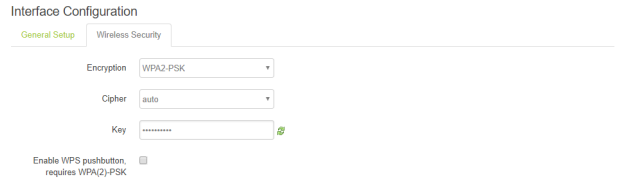


Figure 40:

9. Click the `Save & Apply` button for the changes to take effect immediately. No reboot is required.

Results

You have successfully configured an interface for a wireless connection on the device with DHCP.

5.5 Enabling or disabling IPv6 support for network connections

This section describes the steps required to enable or disable IPv6 support for the device.

Before you begin

The device must be powered on with all antennas and network cables connected and you must be signed in.

Procedure

1. Go to the **Network** > **Interfaces** menu and select the **General Setup** tab.
2. In the Global network options you can change the IPv6 unique local address prefix.This step is optional.
3. Select the interface you want to configure IPv6 connection for by clicking the **Edit** button.
4. In the **Common Configuration** section you will see the current status and configured addresses for the selected interface. You can configure the IPv6 assignment by selecting the length from the drop-down menu. You can also disable the feature by selecting **Disabled** from the drop down menu.

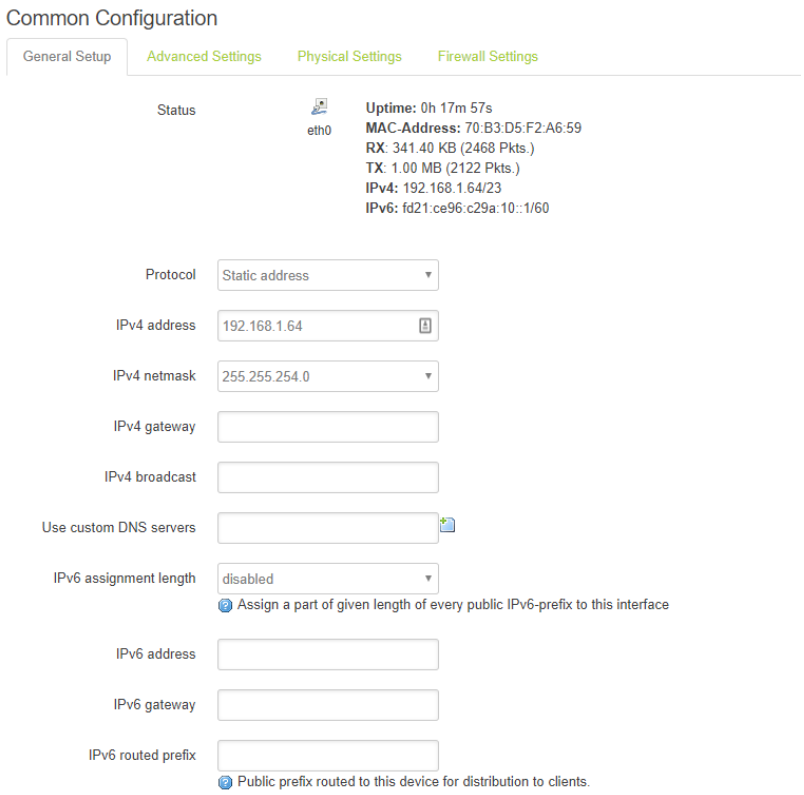


Figure 41: IPv6 settings

5.6 Cellular network configuration

This chapters details the necessary steps required to configure a wireless network connection for the device using the GUI.

Before you begin

Make sure the device is connected to the network, all antennas are attached and powered up. The device must also have a previously configured IP address. For a cellular configuration, the device must have an installed LTE module.

Procedure

1. Open a web browser and enter the IP address previously configured for the device.
2. When prompted with the login screen, enter the password for `root` access. The default `root` password is shared separately and it can later be changed in the **System** > **Administration** menu.

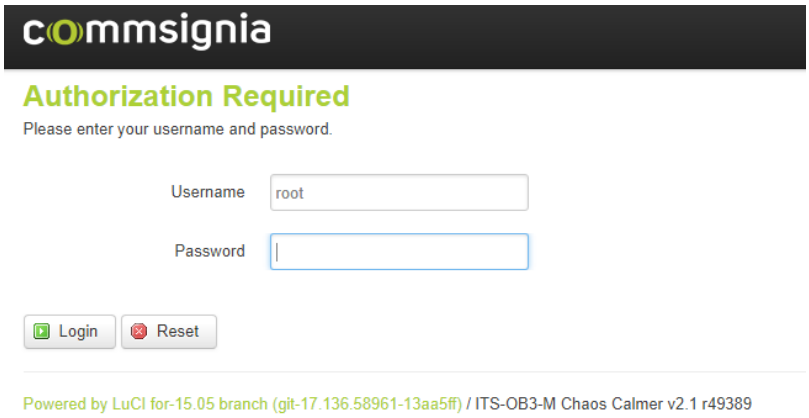


Figure 42: The login screen

3. Select the **Network** > **Interfaces** menu option from the menu bar on the top of the page.

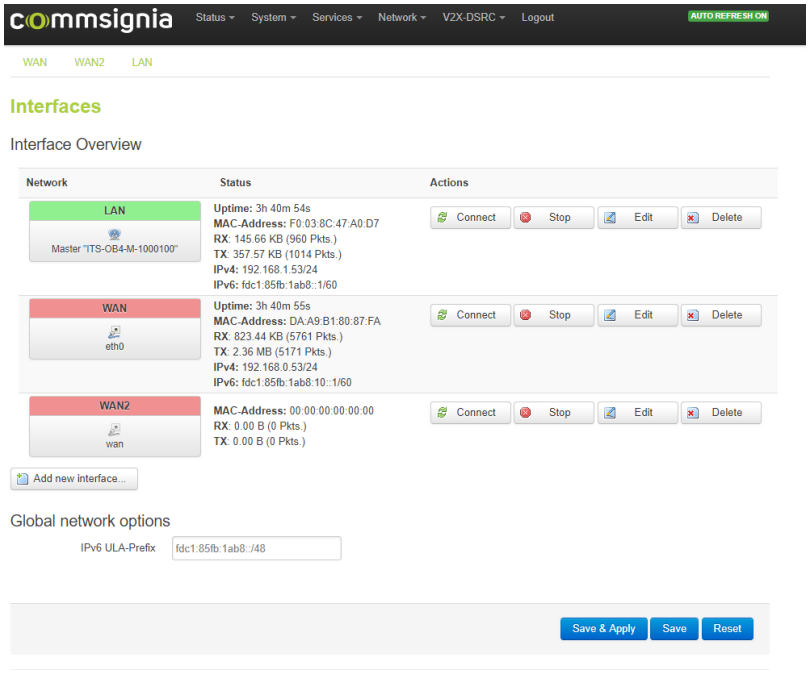


Figure 43: The Interfaces page

On this page you can see a list of the already configured interfaces with their status and basic configurations. You can also `Connect`, `Stop`, `Edit`, or `Delete` each individual interface.

4. Select the `Edit` button of an already existing interface or the `Add new interface...` button if you want to create a new interface for the cellular connection.
5. Select `QMI` as the `Protocol` for the interface. Enter `/dev/cdc-wdm0` into the `Modem device` field

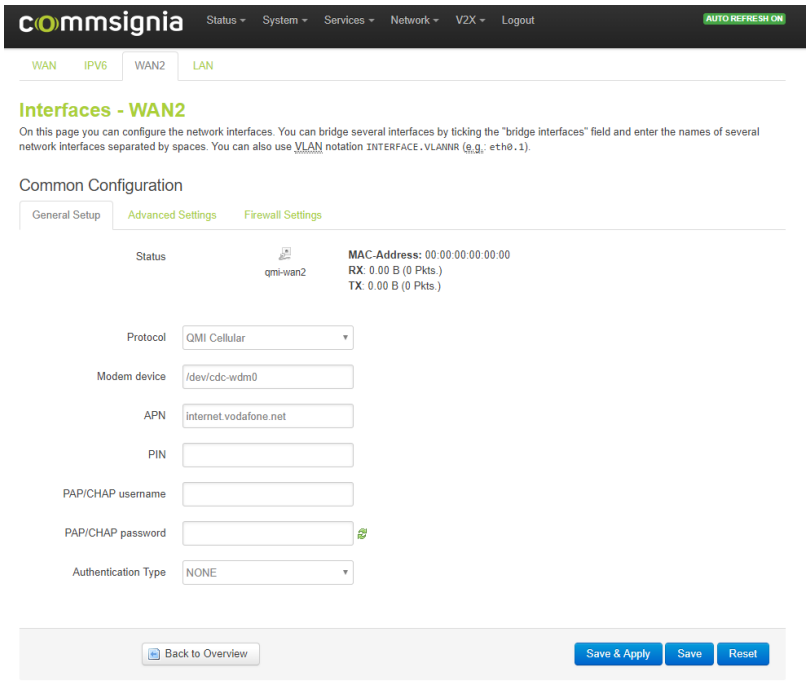


Figure 44: General settings for the cellular connection

6. Select the `Firewall Settings` tab. This is where you can create or assign a firewall zone for this interface.

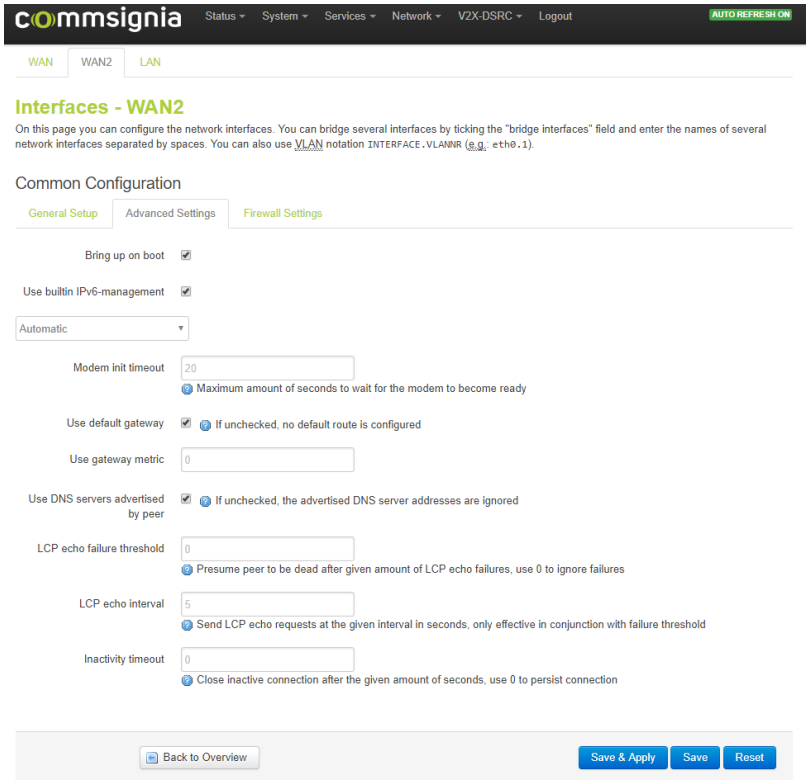


Figure 45: Firewall settings for the cellular connection

7. When you are finished with all configuration steps, click the `Save & Apply` button. This will apply the configured settings for the device and resynchronize the network settings. It is not necessary to reboot the device for the changes to take effect.

Results

You have successfully configured an interface with a wireless network connection for the device.

5.7 Disabling automatic cellular connections

In case you want to disable the automatic startup of cellular connections, when a SIM card is inserted, you can do that in the Advanced Settings.

Procedure

Select the `Advanced Settings` tab for further configuration options. It is recommended to leave the default settings at this time. If you want to disable automatically enabling a cellular connection, deselect the `Bring up on boot` check box.

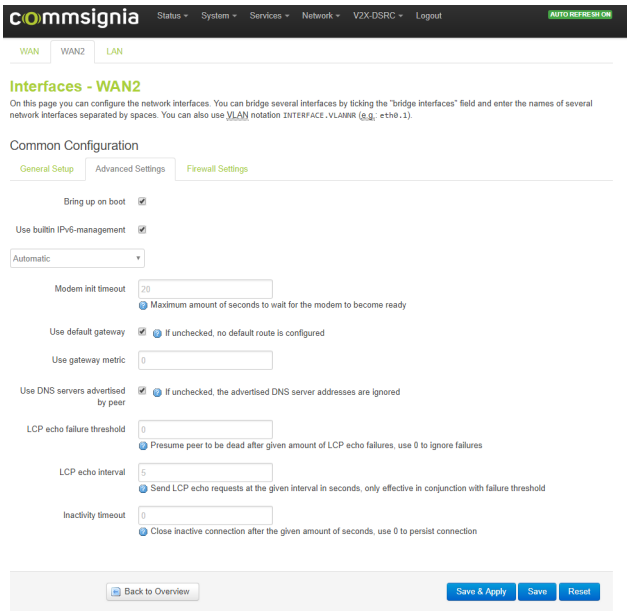


Figure 46: Advanced settings for the cellular connection

6 Configuring NTP as time reference

This chapter details the requirements and the necessary steps for configuring Network Time Protocol (NTP) as the time synchronization method for the system.

Before you begin

Make sure all antennas are connected and the device is powered up. The device must be connected to a computer with an Ethernet cable and have a previously configured IP address on the eth0 interface, available for connection. The device must already have a DNS-server and a default gateway configured.

Procedure

1. Connect to the device's main operating system using either using the GUI or an SSH connection.
2. Ensure that the device has a properly configured DNS-server and default gateway. For more information, refer to the ***Network configurations*** chapter of this document.
3. Set the navigation mode to manual and set the coordinates. This is part of the software stack configuration and it can be set from the GUI in the **V2X-DSRC** > **Stack** menu, on the **Advanced configuration** panel.

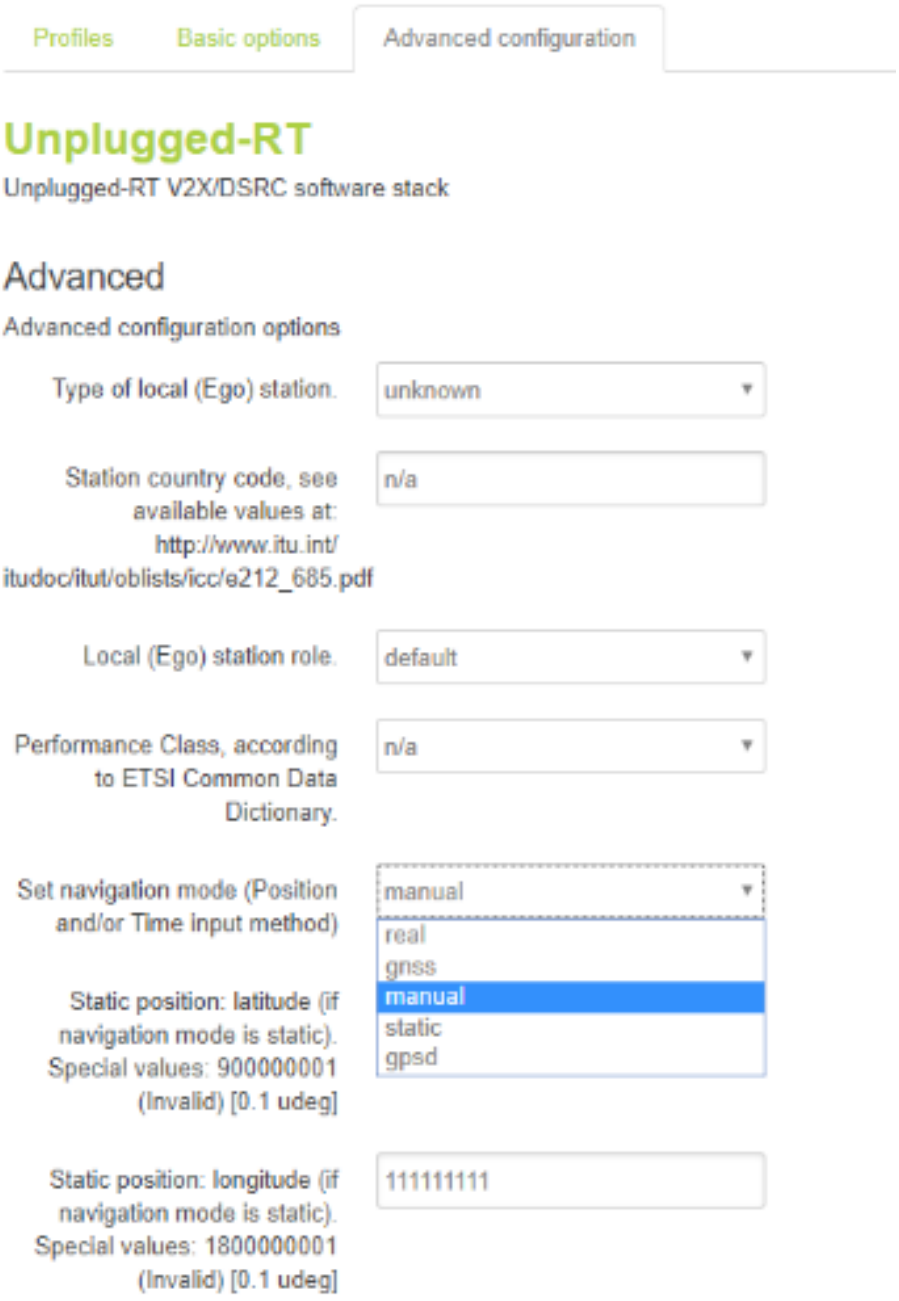


Figure 47: Navigation mode in the stack settings

Select the manual navigation mode, then set the `latitude`, `longitude`, and `altitude` values.

4. Enable the device to act as an NTP client in the System menu page, under Time Synchronization.

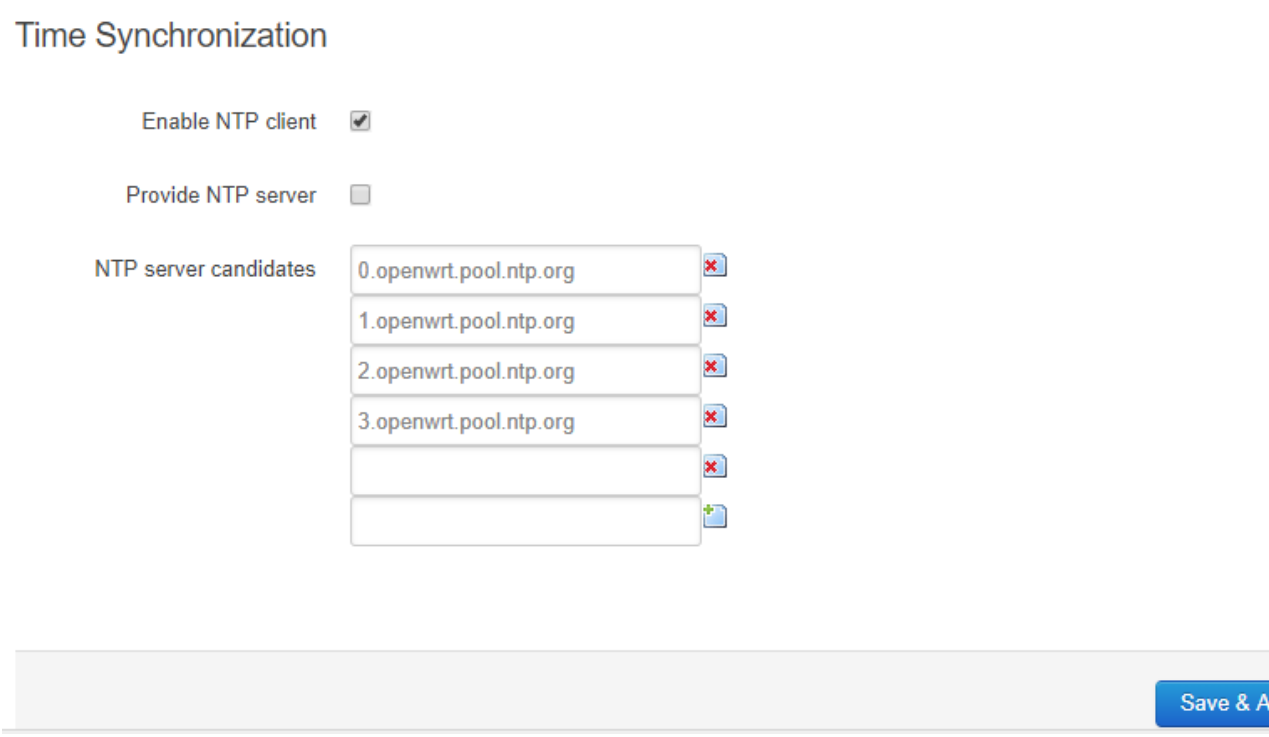


Figure 48: Time Synchronization set to NTP

5. To test the process using an SSH connection, check `/etc/config/system` for NTP servers and use one of them for measuring the difference between system time and the NTP service time. You can also test it by using the following command example:

```
ntpd -wqp 0.openwrt.pool.ntp.org
```

   Check the offset value, which is listed in seconds.

Results

You have successfully configured the device's system to use Network Time Protocol as the time synchronization service.

7 Updating the Operating System using an USB driv

You can automatically update the operating system of the device using an USB drive. This method is only applicable for Commsignia ITS-OB4-M units.

Before you begin

Before updating the system software, the device must be connected to the network and powered on. Make sure that all antennas are properly connected before powering on the device. The device must also have a previously configured IP address. You will need a USB drive formatted to the FAT32 file system and the upgrade image.

Procedure

1. Verify that you have the upgrade image file (upgrade.pack) on the USB drive and that the device operates normally. During normal operation the L1 and L3 LEDs are green and L2 blinks red.
2. Plug the USB drive into the device. Verify that the upgrade process is started by checking if the L3 LED is blinking red.
3. Wait about 1 minute.
4. When the L3 LED on the device is continuously red, the upgrade is ready.
5. Remove the USB drive.
6. Press the restart button on the device. This will initiate a power cycle and reboot the unit.
7. After the reboot, verify that the device is working normally. During normal operation the L1 and L3 LEDs are green and L2 blinks red.

Results

The system is successfully upgraded on the device.

8 Updating the system using an SSH connection

Before you begin

Before updating the system software, the device must be connected to the network and powered on. Make sure that all antennas are properly connected before powering on the device. The device must also have a previously configured IP address.

Note: It is recommended to handle the update using the GUI. Using an SSH connection for updating the system software should only be used as a backup procedure.

Procedure

1. Open an SCP connection to the device using the following settings:

File protocol	SCP
Host name	The IP address of the device.
Port number	22 - This is the default value. You can change this later using the **System** > **Administration** menu in the GUI.
User name and password	Use `root` access for the update. By default there is no separate password for the SSH connection so you can use the password for the device.

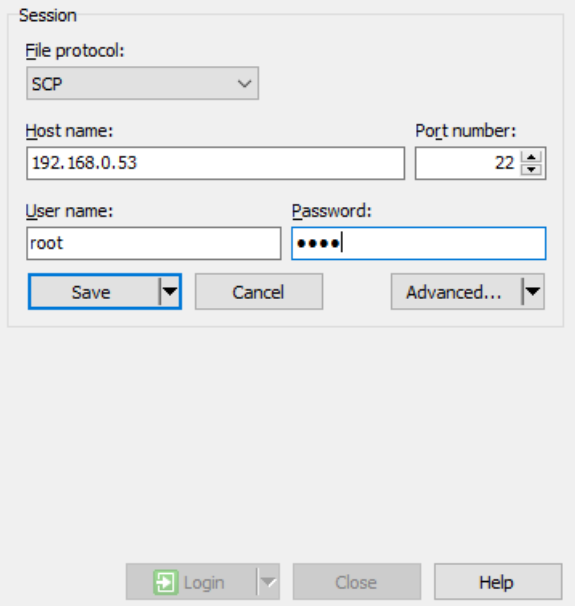


Figure 49: Example SCP settings

2. Upload the `.tar.sig` image file using the SCP connection. The file is a compressed image file that contains the update package for example `example-sysupgrade.tar`. It is recommended to upload this file to the `/tmp` folder.
3. After the upload is finished, use the following command to start the update procedure:

```
signedUpgrade.sh /tmp/example-sysupgrade.tar.sig
```

Note: If your current Unplugged-RT software version is below 1.16.0 then a backup of the `/etc/its.cfg` file must be made because the `license-key` parameter will reset in this file after the update. For instructions how to check the Unplugged-RT software stack version, see *Version information*.

4. After initiating the update process the console log will display the status. After a successful update, the last line in the console log will be `Rebooting device`. The device will reboot and the SSH connection will be lost.
5. Establish a new SSH connection to validate the success of the update.

Results

The system is successfully updated on the device.

9 Configuring an IP address for the device using the

Before you begin

Before logging in make sure the device is connected to a computer with a serial connection and powered up.

Note: Make sure all antennas are connected properly to the device before powering it up.

About this task

This chapter details the necessary steps to log in to the operating system on the device using the console through a serial connection and configure an IP address for the device so it can be accessed through the graphical user interface or through an SSH connection.

Procedure

1. Download and install the `CP210x USB to UART Bridge VCP Drivers` from https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers For installation instructions and driver related support, refer to the Silicon Labs website.
2. Open a console connection to the serial COM port using the following settings:

Parameter	Value
Serial line:	COM4
Speed (baud)	115200
Data bits	8
Stop bits	1
Flow control	XON/XOFF

Note: To find the appropriate COM port that the device is connected to, refer to the Device Manager of your operating system.

3. Log in as `root`. The default password is provided separately.
4. Modify the `ipaddr` field to match your network settings.

```
config interface 'wan'
        option ifname 'eth0'
        option macaddr '70:B3:D5:F2:A7:34'
        option proto 'static'
        option netmask '255.255.255.0'
        option ipaddr '192.168.0.54
```

You can also set it temporarily with the command below (example):

```
root@ITS-OB4-M-1000100:~# ifconfig eth0 192.168.0.54
```

Note: This will not save the IP configuration but will let you access the the GUI from a web browser.

5. You can now also change the password using the `passwd` command. You can also do this later using the GUI in the **System** > **Administration** menu.

Results

You have accessed the operating system running on the device through a serial connection and configured an IP address.

What to do next

You can now use the GUI or an SSH connection for further configuration steps.