commsignia

Operating System User Manual
for
Commsignia Products

BACL Corp.
CONFIDENTIAL
04/20/2018

Copyright © 8, Commsignia Ltd. Lónyay utca 31. Budapest 1093 Hungary | info@commsignia.com | http://www.commsignia.com

BACL Corp.
CONFIDENTIAL
04/20/2018

Contents

Preface 3
Disclaimer 3
Document Changelog 3
Related documentation. 4

Introduction. 5
Overview of the operating system. 5

Accessing the Operating System 6
Log in using the GUI. 6
Log in using SSH. 7

Security 8
Changing the password. 8

System information 9
Version information 9
System Uptime. 10
RAM and CPU usage of the running processes. 10
Time sync 11
Configuring time sync for NTP 11
Available configuration options. 12

Network configurations 15
Wired network configuration. 15
Configuring a static wired network 15
Configuring a DHCP wired network 18
Wireless network configuration. 22
Configuring the device as a client in a wireless network with a Static IP address 22
Configuring the device as a client for a wireless network with DHCP 25
Cellular network configuration 27

Updating the Operating System 30
Updating the system using the GUI. 30
Updating the system using an SSH connection. 31

Troubleshooting. 33
Configuring an IP address for the device using the console 33

BACL Corp. CONFIDENTIAL 04/20/2018

1 Preface

1.1 Disclaimer

This document may be revised without prior notice. For most recent releases, visit our website or contact support. Please send any comments or remarks about this document to support@commsignia.com (including the document title in the subject). Commsignia Inc. reserves all rights to this document and the information contained herein. Products, names, logos and designs described may in whole or in part be subject to intellectual property rights.

Note: Any changes or modifications made to this device that are not expressly approved by Commsignia Inc. may void the user's authority to operate the equipment.

Note: Confidential - This document is provided in confidence and may not be used for any purpose other than that for which it is supplied. All content within may not be disclosed to any third party or used for other purpose without the written permission of Commsignia Ltd.

FCC compliance statement

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in
a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

RF exposure warning

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must be at least 20 cm from the user and must not be co#located or operating in conjunction with any other antenna or transmitter.

1.2 Document Changelog

This section is a reference to the iterative changes in the document listed by issue number.

Table 1: Changes in the document

Issue number	Changes
1-1	Added information about the NTP configuration.
1-0	This is the first issue of the document.

BACL Corp.
CONFIDENTIAL
04/20/2018

BACL Corp.
CONFIDENTIAL
04/20/2018

2 Introduction

2.1 Overview of the operating system

The device iis running an open source operating system and can be accessed by the console through a serial connection or SSH and also through a graphical user interface from a web browser.

Commsignia is using an open source Linux distribution for embedded services. It provides a fully writable filesystem 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

The system can be configured using a command line interface, through a serial or an SSH connection.

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

BACL CORP:
CONFIDENTIAL
04/20/2018

3 Accessing the Operating System

The following chapters contain information about accessing the operating system.

3.1 Log in using the GUI

This chapters details the necessary steps required to log in to the Graphical User Interface 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. For more information about configuring an IP address for the device, see *Configuring an IP address for the device using the console.*

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 or with the `passwd` command in the console.

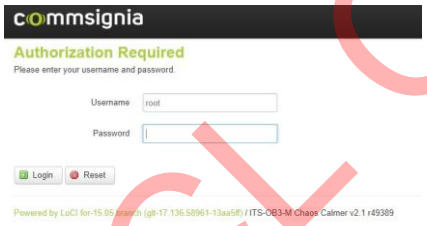


Figure 1: The GUI login screen

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.

BACL Corp. CONFIDENTIAL 04/20/2018

3.2 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. For more information about configuring an IP address for the device, see *Configuring an IP address for the device using the console.*

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`.

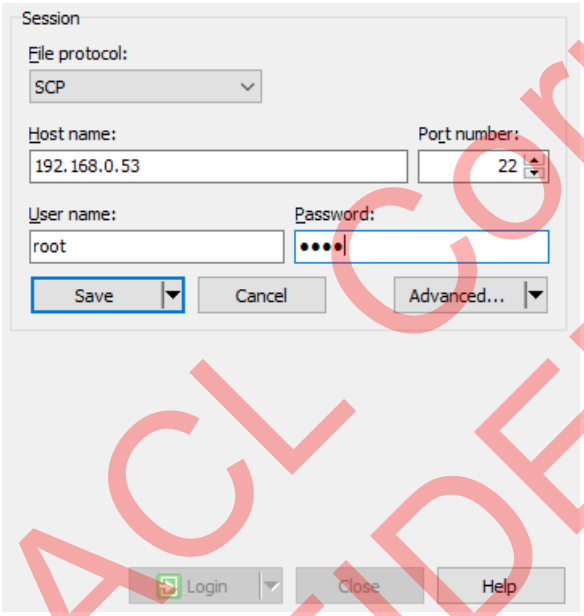


Figure 3: SCP client settings

File protocol	SCP
Host name	The IP address of the device. For more information about configuring an IP address for the device, see *Configuring an IP address for the device using the console.*
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 or with the `passwd` command in the console.

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.

BACL Corp. CONFIDENTIAL 04/20/2018

4 Security

4.1 Changing the password

This chapter describes the steps for changing the password using the command line as well as the GUI.

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. For more information, see the *Initial access configuraiton using the console* chapter.

Procedure

- After connecting to the device using a serial connection or an SSH connection, you can enter a new password using the `passwd` command in the console.
- You can change the password using the GUI in the **System** > **Administration** menu.

Figure 4: Changing the password in the GUI

Results

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

BACL CORP.
CONFIDENTIAL
04/20/2018

5 System information

5.1 Version information

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

OS 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.

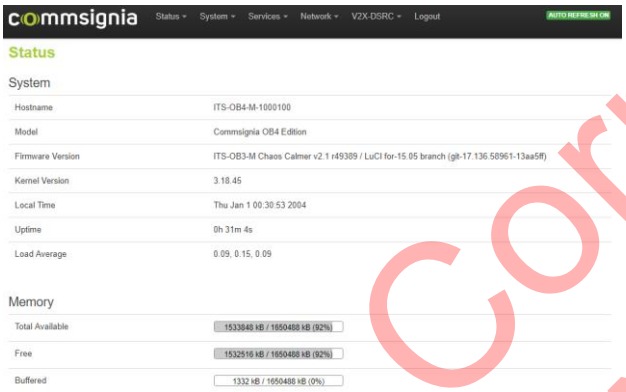


Figure 5: The Overview page showing the system version

Package versions

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

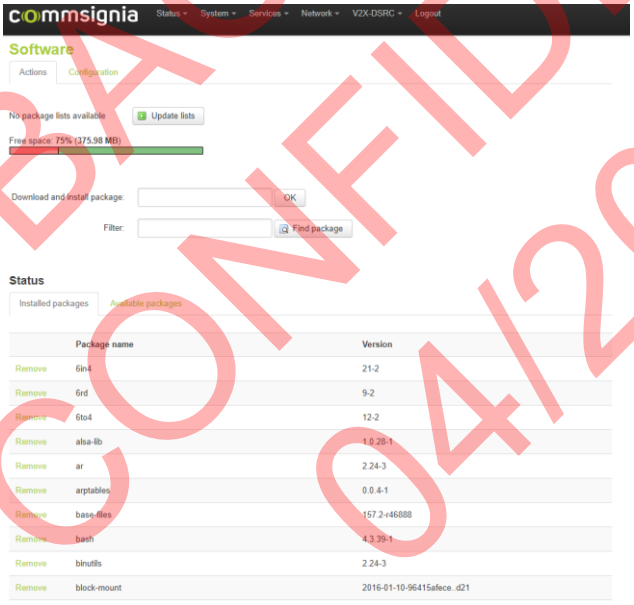


Figure 6: Package versions

BACL Corp.
CONFIDENTIAL
04/20/2018

5.2 System Uptime

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

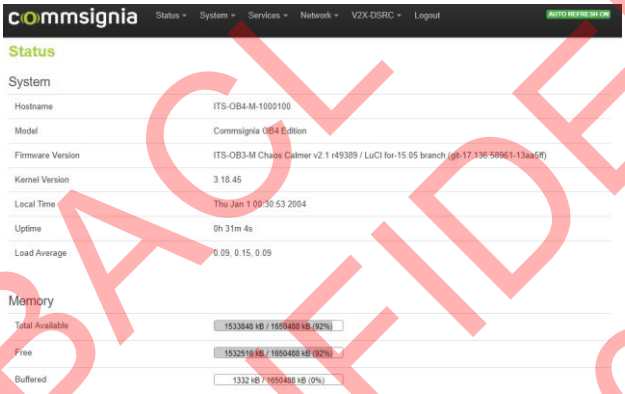


Figure 8: The overview page showing the uptime of the operating system

5.3 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.

BACL Corp.
CONFIDENTIAL
04/20/2018

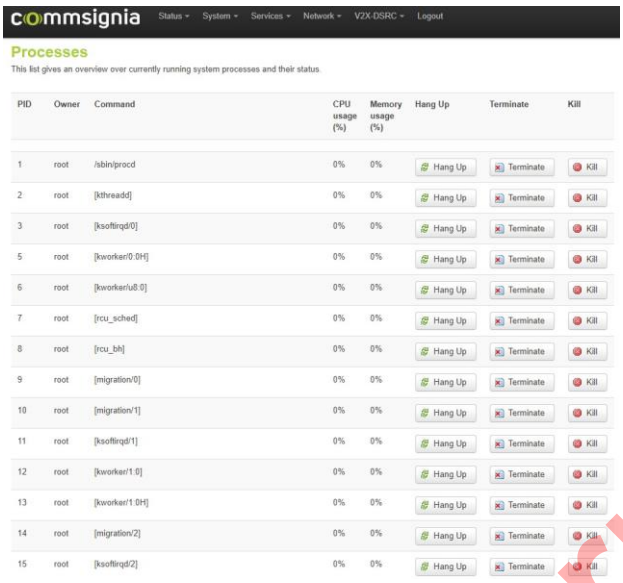


Figure 9: The Processes screen in the GUI

5.4 Time sync

The system uses GNSS as a source of accurate time for synchronization purposes by default. It is also possible to configure the system to use Network Time Protocol (NTP) in case manual navigation is used (for example if a GPS signal is not available) or for testing.

5.4.1 Configuring time sync for NTP

This chapter details the requirements and the necessary steps for configuring Network Time Protocol (NTP) as the time sync 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 either a USB or an Ethernet cable and have a previously configured IP address on the eth0 interface, available for connection.

Procedure

1. Connect to the device's main operating system using either a serial or an SSH connection.
2. Check the default gateway. You can set it using the following command:

```
route add default gw 192.168.0.1
```

3. Set the DNS-server if you have to. Edit the namespace in resolv.conf, using the follwing command:

```
vi /etc/resolv.conf
```

4. Set the navigation mode to manual and set the coordinates:

```
uc  se  upladv.upladv.navigation_mode='manual
i   t   '
uc  se  upladv.upladv.manual_latitude='10'
i   t   upladv.upladv.manual_longitude='20'
uc  commi
```

BACL Corp. CONFIDENTIAL 04/20/2018

5. Start the NTPD service to synchronize system time with the NTP service.

```
/etc/init.d/sysntpd start
```

The system may require a restart for the NTP service to fully initialize. In this case, use the following command:

```
/etc/init.d/sysntpd restart
```

6. To test the process, measure the difference between the system time and the NTP service time using the following command:

```
ntpd -wqp 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 sync service.

5.5 Available configuration options

The following options can be configured in the GUI menus

Status

Overview	Provides an overview of high level system parameters and version information for the operating system, as well as basic usage information such as the uptime.
Firewall	Frewall settings - the default values are part of the basic software configuration.
Routes	Routing settings - the default values are part of the basic software configuration.
System log	Prints the most recent log lines of the V2X software stack running on the device.
Kernel log	Prints the most recent log lines of the operating system.
Processes	Lists the currently running processes and their resource usage, with options to `Hang up`, `Terminate`, or `Kill` each process. You can get the same list with the `ps` command in the console.
Realtime graphs	Shows a graphical output of the processors load, wired and wireless network statistics, and active connections.

System

System	This menu contains basic system properties. This is where the host name can be configured. For time synchronization settings, see the software stack manual. The synchronization can be handled through an NTP server, the GPS antenna, or through the API. The default time synchronization mode is through the GPS antenna - this is recommended because this is the most reliable and accurate option.

BACL Corp.
CONFIDENTIAL
04/20/2018

Administration	This menu lets you change the password and the SSH connection settings.
Software	This menu lists the installed packages and their versions. The default values are included in the basic software configuration, and changes are not recommended.
Startup	This is a list of scripts that start automatically after the device is powered on.
Scheduled tasks	You can schedule the execution of user defined scripts in this menu.
Mount points	This menu shows a default list of mounted devices and file systems. In case you want to attach a USB drive or another external peripheral (that is supported by the system) you can do that here.
LED configuration	It is recommended to keep the default settings. This is where you can change the LED lights configuration in special cases.
Backup / Flash firmware	This menu is used for backing up and updating the firmware. For more information, see the *Updating the Operating System* chapter.
Custom commands	You can define custom shell commands in this menu, that can be executed from the GUI.
Reboot	Reboots the device. All connections will be terminated by this process and you must log in again after the reboot is completed.

Services

OpenVPN	By default, there is no VPN connection used by the system.

Network

Interfaces	This menu lists the available interfaces. By default a wired connection is configured for the device with a static IP address.
Wifi	Only available if a wireless module is connected to the device. This menu contains an overview of the Wifi settings.
DHCP and DNS	You can change the DHCP and DNS handling settings for the system. It is recommended to use the default values.
Host names	This is where you can configure the host names. It is recommended to use the default values.
Static routes	You can specify static routes per network configuration in this menu. It is recommended to keep default settings.
Diagnostics	You can find the basic diagnostic tools supported by the OS in this menu: `ping`, `traceroute`, and `nslookup`.

BACL CONFIDENTIAL 04/20/2018

Firewall	This is where you can configure the Firewall settings for the device: `General settings`, `Port Forwards`, `Traffic Rules`, and `Custom Rules`.

V2x-DSRC

Status	This menu shows the V2X stack version, basic stack parameters, and statistics counter listing.
Stack	This menu contains the basic configuration presets for the EU and US stack versions. Commsignia pre- configures the devices for each delivery. The basic configuration lists user defined parameters.
Participant group	Participant group settings
Fusion-filtering	Next generation Commsignia filtering and fusion logic, only available in certain software distributions.
Applications	Next generation Day 1 applications based on CFF, only available in certain software distributions.
Legacy applications	Configuration parameters for Day 1 safety and traffic efficiency applications (licensed separately from the software stack).
Traffic Light Controller	This feature enables the device to act as a test traffic light controller for field tests. This can be separately licensed for RSU variants only.

Logout

Log out of the device. Selecting this will take you back to the authorization screen, where you can log in again after providing a user name and a password.

BACL Corp
CONFIDENTIAL
04/20/2018

6 Network configurations

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

6.1 Wired network configuration

6.1.1 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. For more information about configuring an IP address for the device, see *Configuring an IP address for the device using the console*.

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 or with the `passwd` command in the console.

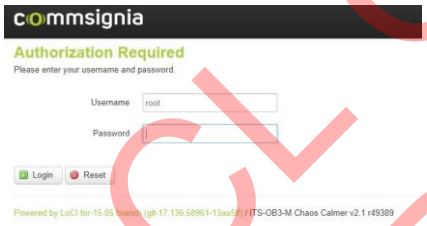


Figure 10: The login screen

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.

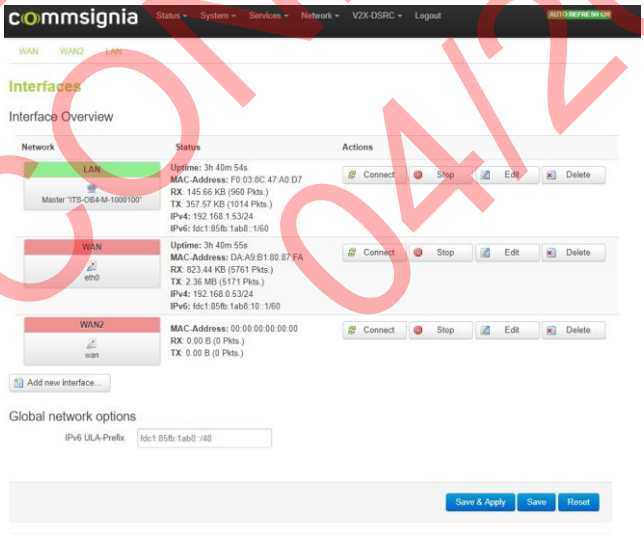


Figure 11: The Interfaces page

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

BACL Corp. CONFIDENTIAL 04/20/2018

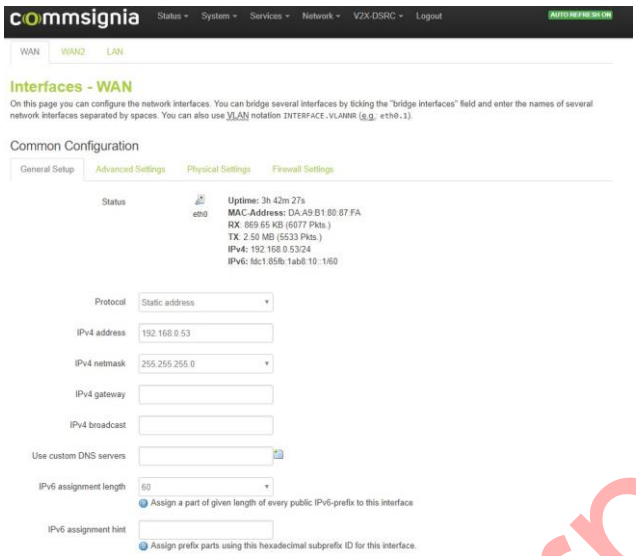


Figure 12: The general configuration page for the selected interface

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.

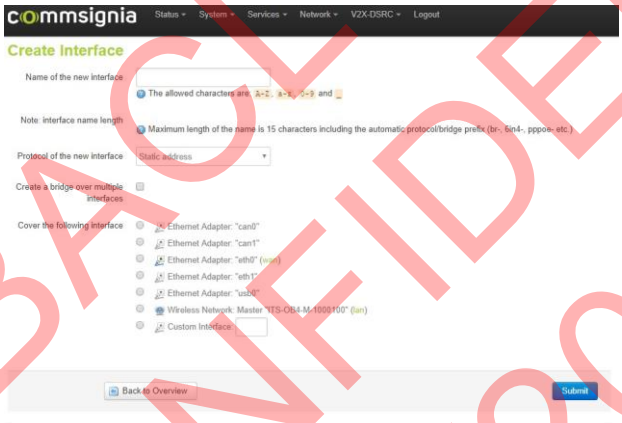


Figure 13: The Create Interface page

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

BASF Corp. CONFIDENTIAL 04/20/2018

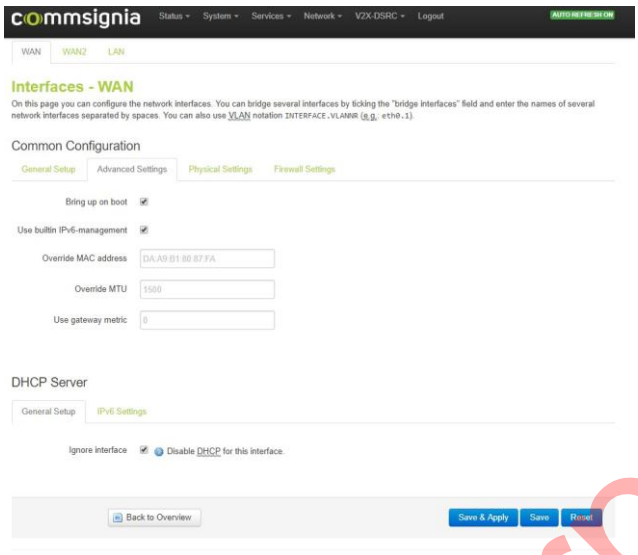


Figure 14: The Advanced settings page

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

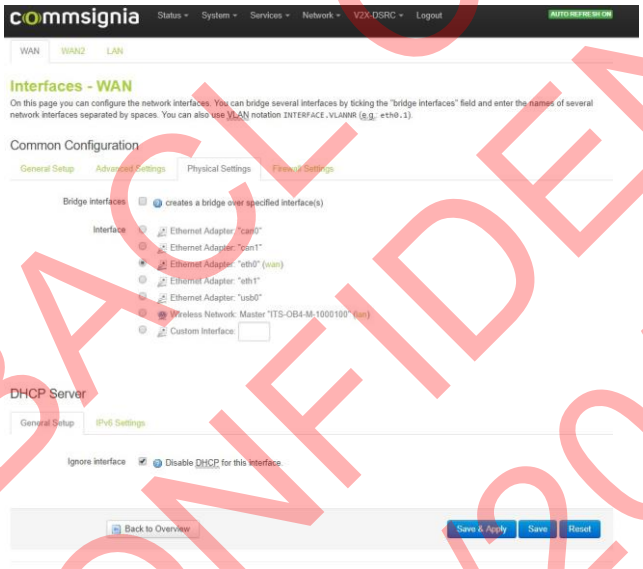


Figure 15: The Physical Settings tab

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

BASL Corp. CONFIDENTIAL 04/20/2018

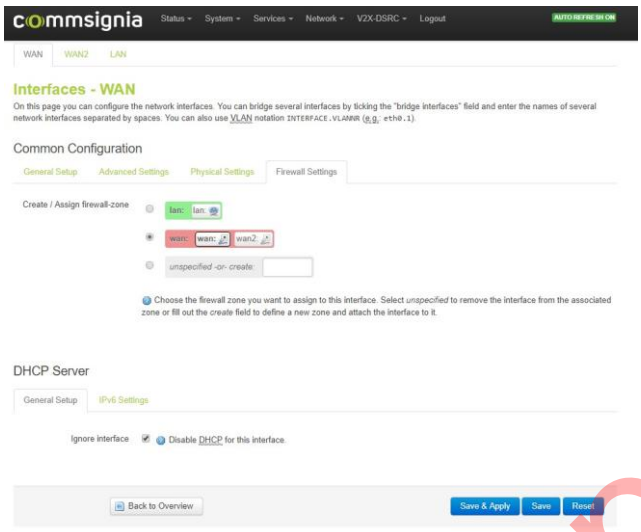


Figure 16: The Firewall Settings tab

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 interface 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. For troubleshooting purposes you can configure an IP address also using the console. For more information, see the *Configuring an IP address for the device using the console* chapter.

6.1.2 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. For more information about configuring an IP address for the device, see *Configuring an IP address for the device using the console*.

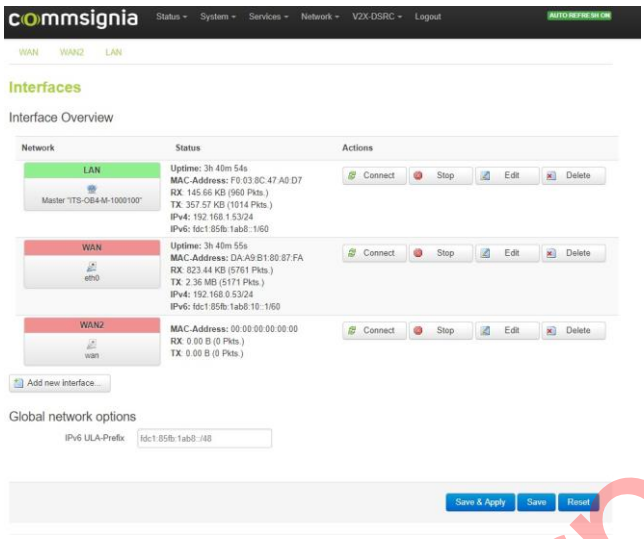
Procedure

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 or with the `passwd` command in the console.

Figure 17: The login screen

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

BACH Corp. CONFIDENTIAL 04/20/2018



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

Figure 18: The Interfaces page

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

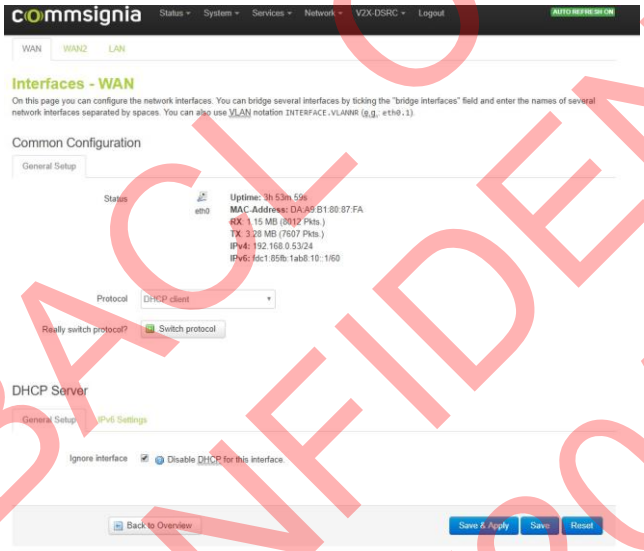


Figure 19: The general configuration page for the selected interface

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.

BACL Corp. CONFIDENTIAL 04/20/2018

Figure 20: 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

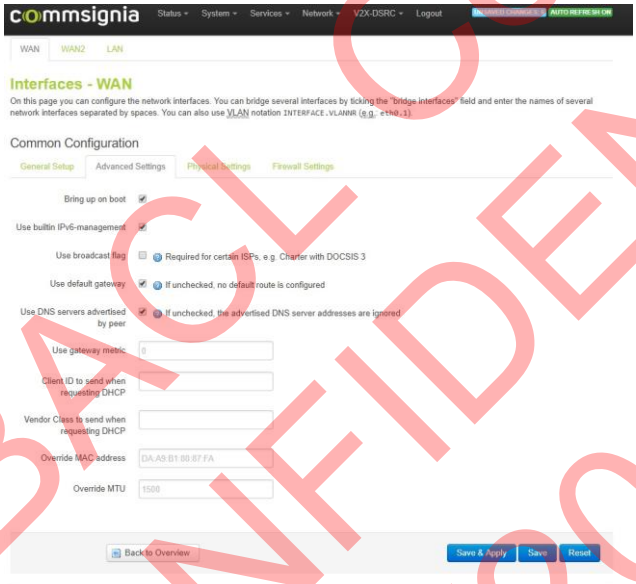


Figure 21: The Advanced settings page

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

BACL CONFIDENTIAL 04/20/2018

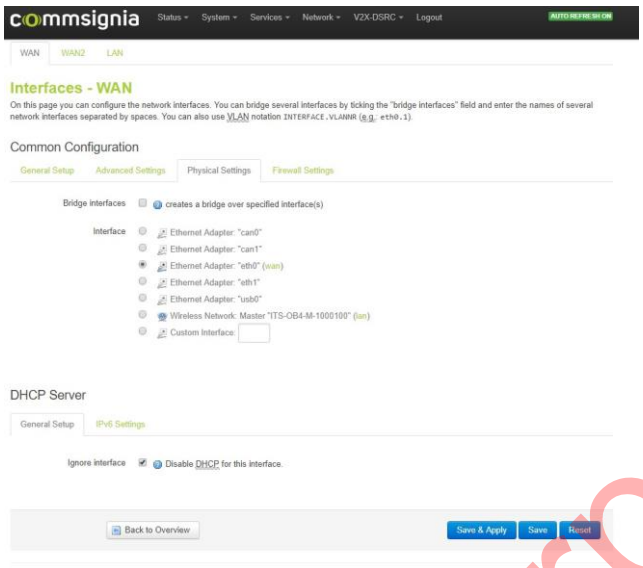


Figure 22: The Physical Settings tab

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

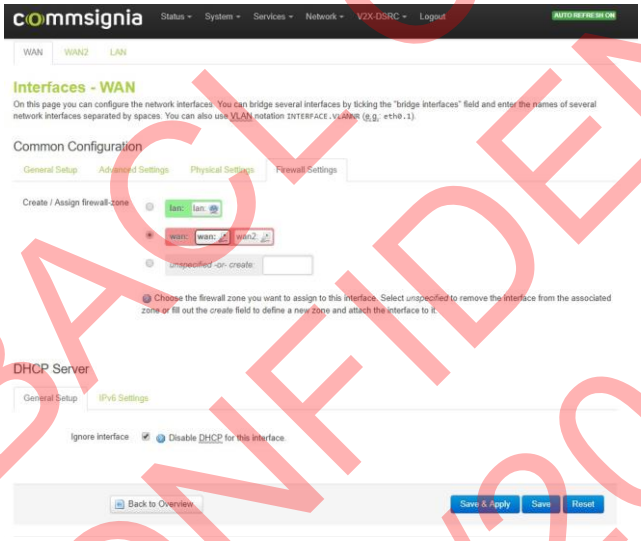


Figure 23: The Firewall Settings tab

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 interface 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. For troubleshooting purposes you can configure the network also using the console. For more information, see the *Configuring a DHCP network connection for the device using the console* chapter.

BASL Corp. - CONFIDENTIAL 04/20/2018

6.2 Wireless network configuration

6.2.1 Configuring the device as a client in a wireless network with a Static IP address

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. For more information about configuring an IP address for the device, see *Configuring an IP address for the device using the console*.

Procedure

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

Figure 24: The login screen

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

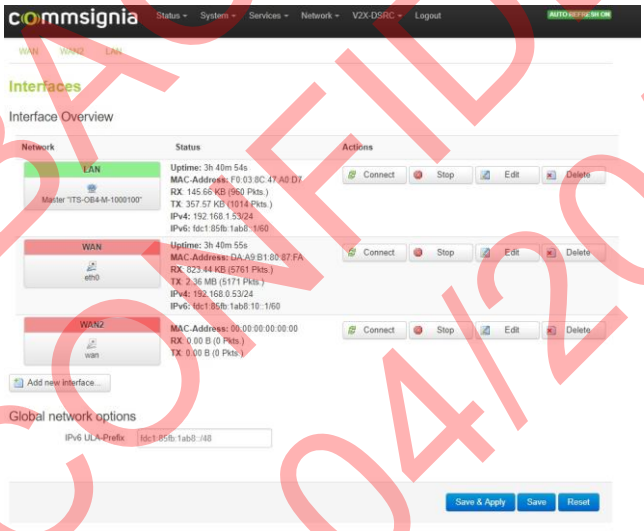


Figure 25: The Interfaces page

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.

BOSCH Corp.
CONFIDENTIAL
04/20/2018

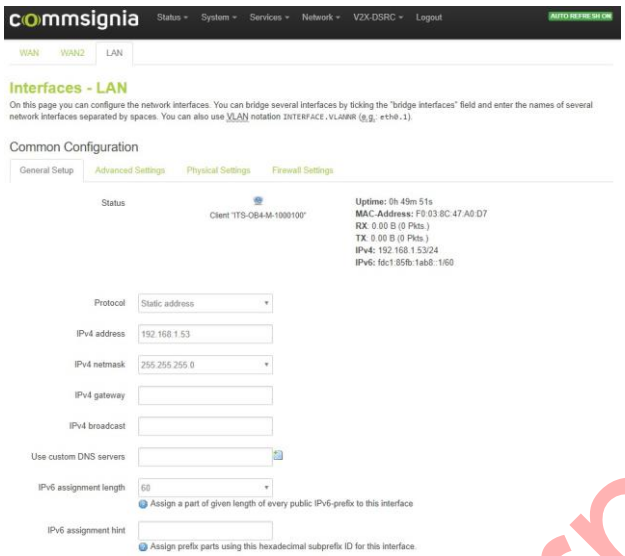


Figure 26: Static protocol selected for wireless access

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.

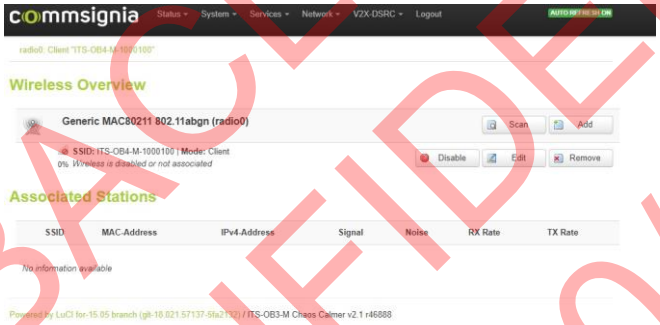


Figure 27: Wireless Overview

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

BACL Corp. CONFIDENTIAL 04/20/2018

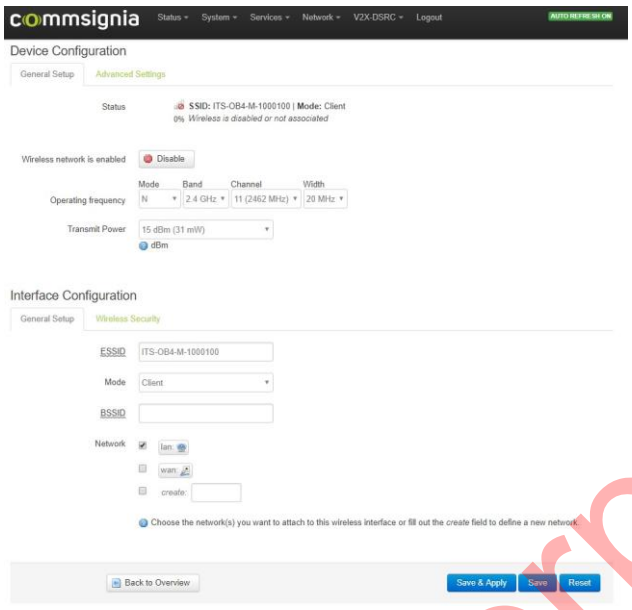


Figure 28:

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.

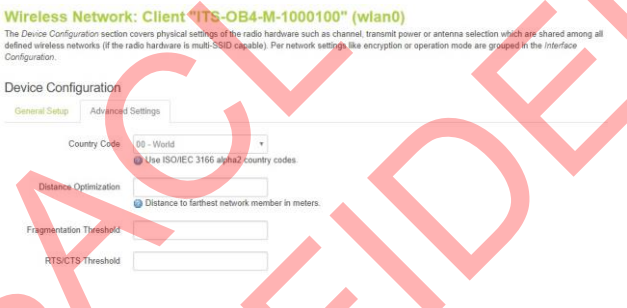


Figure 29: Advanced wireless settings for the device

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).

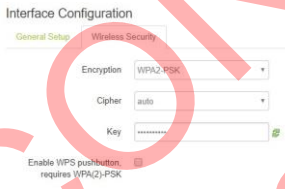


Figure 30: Wireless security settings

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.

BACL Corp. CONFIDENTIAL 04/20/2018

6.2.2 Configuring the device as a client for a wireless network with DHCP

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. For more information about configuring an IP address for the device, see *Configuring an IP address for the device using the console*.

Procedure

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

Figure 31: The login screen

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

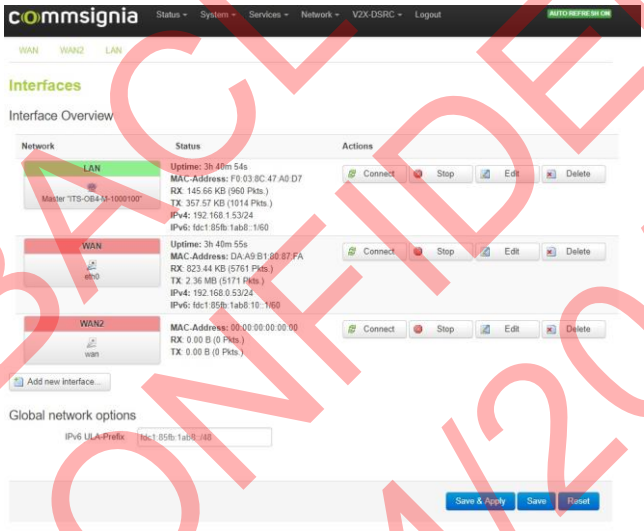


Figure 32: The Interfaces page

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.

BACL Corp. CONFIDENTIAL 04/20/2018

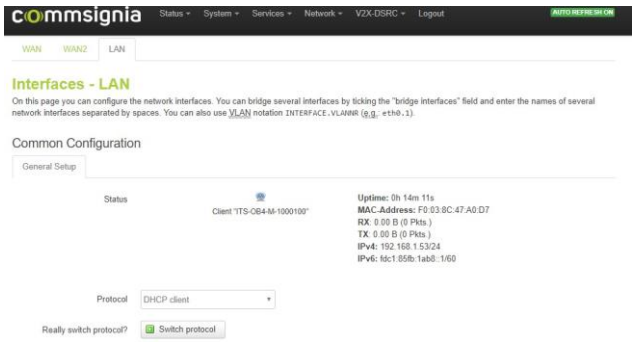


Figure 33: DHCP protocol selected for wireless access

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.

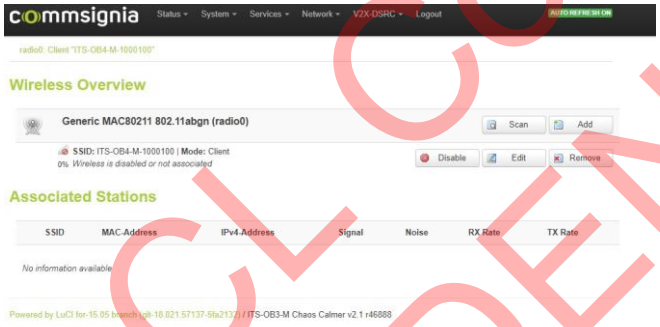


Figure 34: Wireless Overview

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

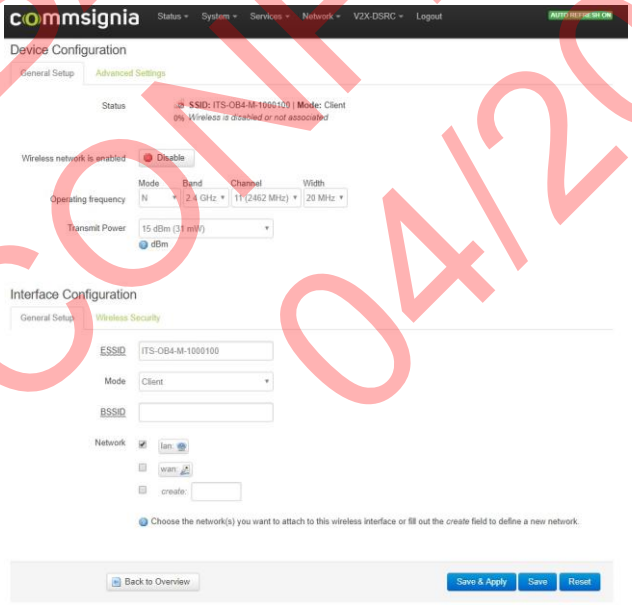


Figure 35:

BACL Corp.
CONFIDENTIAL
04/20/2018

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 36: 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 37:

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.

6.3 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. For more information about configuring an IP address for the device, see *Configuring an IP address for the device using the console*.

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 or with the `passwd` command in the console.

Figure 38: The login screen

BACL Corp. CONFIDENTIAL 04/20/2018

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

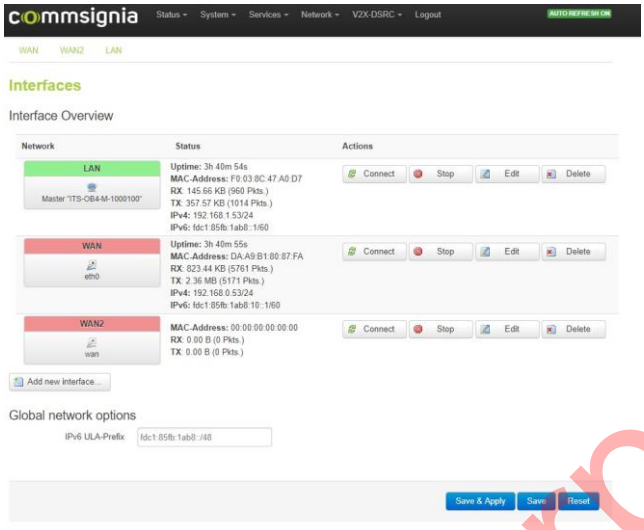


Figure 39: The Interfaces page

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 `NCM` as the `Protocol` for the interface. Enter `/dev/ttyUSB0` into the `Modem device` field

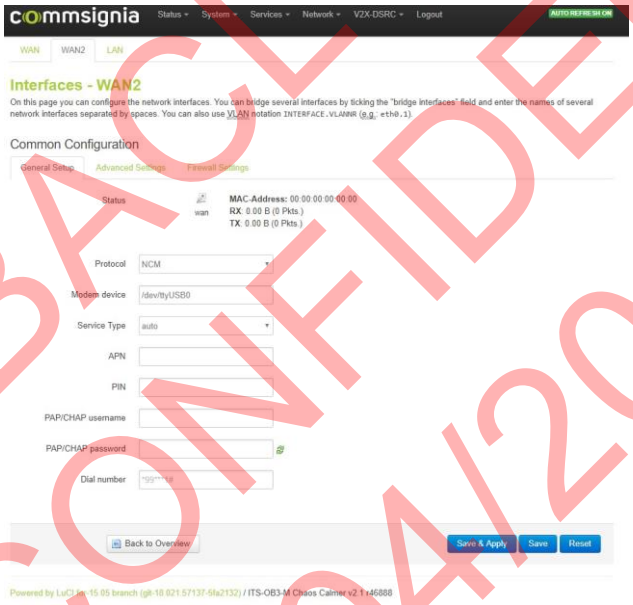


Figure 40: General settings for the cellular connection

6. Select the `Advanced Settings` tab for further configuration options. It is recommended to leave the default settings at this time.

BACL Corp. CONFIDENTIAL 04/20/2018

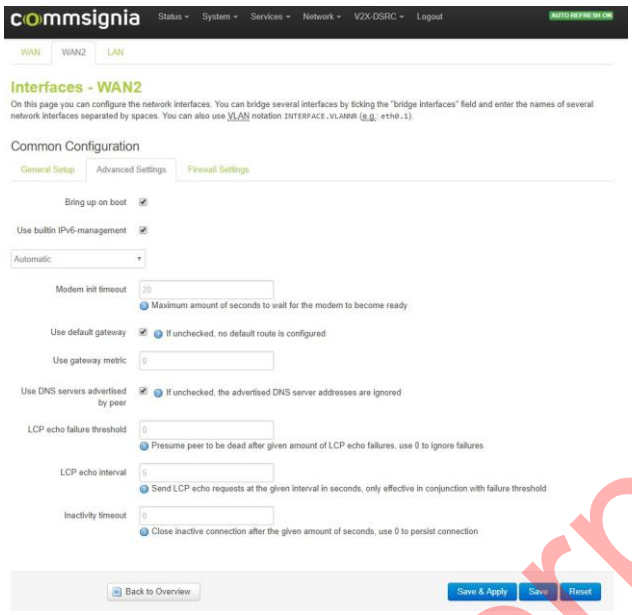


Figure 41: Advanced settings for the cellular connection

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

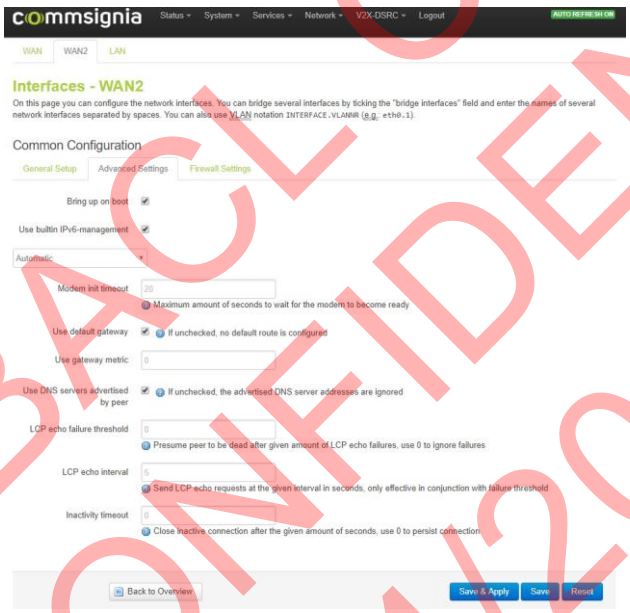


Figure 42: Firewall settings for the cellular connection

8. When you are finished with all configuration steps, click the `Save & Apply` button. This will apply the configured settings for the device and resync 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.

BACL Corp. CONFIDENTIAL 04/20/2018

7 Updating the Operating System

The system software, including the operating system and the software stack can be upgraded using either the GUI or through an SSH connection.

7.1 Updating the system using the GUI

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. For more information, see *Configuring initial access using the console*.

Procedure

1. Log in to the GUI by opening a browser and entering the IP address of the device. Log in with `root` access.
2. Select the **System** > **Backup / Flash firmware** menu.
3. Under `Flash new firmware image` select the image file. The image file is a `.tar` file that contains the update package, for example `example-sysupgrade.tar`.

   Note: It is recommended to keep the `Keep settings` box checked in to avoid an unnecessary loss of configuration during the update.

Figure 43: The Backup / Flash firmware menu

   Note: A backup of the `/etc/its.cfg` file must be made because the `license-key` parameter will reset in this file after the update.

4. Click the `Flash image...` button to upload the selected image file. The upload progress can be tracked in the browser and after it is finished, the MD5 hash will be displayed to validate that the uploaded file was not corrupted during the transfer. The update process takes approximately 2 minutes.
5. After the update process is finished, the device is accessible again from the web interface.

   Note: After the update, the default password is reset for `root` access.

Results

You have successfully updated the system software of the device.

BACL Corp.
CONFIDENTIAL
04/20/2018

7.2 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. For more information, see Configuring initial access using the console.

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. For more information about configuring an IP address for the device, see *Initial access configuration using the console*.
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.

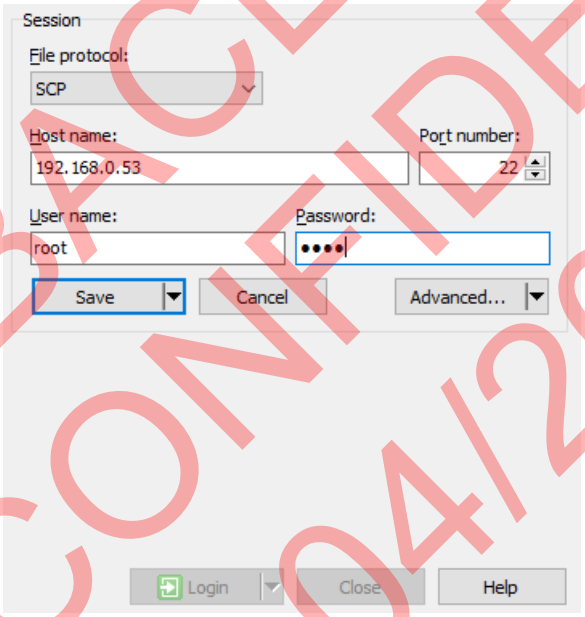


Figure 44: Example SCP settings

2. Upload the `.tar` 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
```

Note: A backup of the `/etc/its.cfg` file must be made because the `license-key` parameter will reset in this file after the update.

BACL CORP. CONFIDENTIAL 04/20/2018

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. Estabilish a new SSH connection to validate the success of the update.

Results

The system is successfully updated on the device.

BACL Corp.
CONFIDENTIAL
04/20/2018

8 Troubleshooting

8.1 Configuring an IP address for the device using the console

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. Open the network configuration file using the following command:

```
root@ITS-OB4-M-1000100:~# vi /etc/config/network
```

5. 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.
6. 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.

BACL CORP.
CONFIDENTIAL
04/20/2018

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.

BACL Corp.
CONFIDENTIAL
04/20/2018