commsignia

Operating System User Manual for Commsignia Products



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.	
Time sync	11 11
Available configuration options.	
Network configurations	15
Wired network configuration.	15
Configuring a static wired network	
Configuring a DHCP wired network	18 22
Configuring the device as a client in a wireless network with a Static IP address	
Configuring the device as a client for a wireless network with DHCP	
Cellular network configuration	27
Undeting the Operating System	20
opualing the Operating System	
Updating the system using the GUI.	
opuating the system using an oor connection.	
Troubleshooting.	
Configuring an IP address for the device using the console	

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.



2.1 Overview of the operating system

The device is 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.

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.

Authorization Re Please enter your username and	quired password	
Username Password	root	
🔟 Login 🛛 🙆 Reset		
D Login Reset	h (gil-17/136/58981-13#45#) / IT	5-083-M Chaos Calmer v2.1 r49389

Figure 1: The GUI login screen

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





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.

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.

Session Eile protocol: SCP Host name: 192.168.0.53 User name: Port number: 22 User name: Password:	
Save Cancel Advanced	
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 <i>Configuring an IP address for the device using the console.</i>
Port number	22 - This is the default value. You can change this later using the System > Administration menu in the GUI.
Enter the root password to gain access. The defa	ault password for the device is shared

 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.

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 configuration 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.

commsignia Status ~	System + Services + N	letwork * V2X-DSRC * I	ogout
Router Password			
Changes the administrator password for accessin	g the device		
Password	Ø		
Confirmation	8		

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.

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.

co mmsignia	Status + System + Services + Network + V2X-DSRC + Logeut	AUTO REFRESH ON	
Status			
System			
Hostname	ITS-OB4-M-1000100		
Model	Commsignia OB4 Edition		
Firmware Version	ITS-OB3-M Chaos Calmer v2.1 r49389 / LuCI for-15.05 branch (git-17.136.58961-13aa	58)	
Kernel Version	3.18.45		
Local Time	Thu Jan 1 00:30:53 2004		
lptime	0h 31m 4s		
Load Average	0.09, 0.15, 0.09	JK	
/lemory			
Total Available	1533848 KB / 1850488 KB (92%)		
Free	1532516 kB / 1650488 kB (92%)		*
Buffered	1332 kB / 1650486 kB (0%)		

Figure 5: The Overview page showing the system version

Package versions

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

com	nsignia Status -	System - Services - N	etwork + V2X-DSRC +	Logout	
Actions	Configuration			\sim	
No package lists Free space: 75%	available Update lists (375.98 MB)				
Download and i	Filter:	OK	package		
Status					
installed pack	Package name		Version		
Remove	6in4		21-2		
Remove	6rd		9-2		
Remove	6to4		12-2		
Remove	alsa-lib		1.0.28-1		
Remove	ar		2.24-3		
Remove	arptables		0.0.4-1		
Remove	base-files		157.2-1468	8	
Remove	bioutils.		2 24.3		
Remove	block-mount		2016-01-10	-96415afeced21	

Figure 6: Package versions

5.2 System Uptime

The uptime of the operating system can be checked on the overview page in the Status > Systemmenu 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.

C(O)	mm	Signia Status + System +	Services * Network * V.	2X-DSRC +	Logout		
Proc	Gesses	erview over currently running system proces	ses and their status.				
PID	Owner	Command	CPU usage (%)	Memory usage (%)	Hang Up	Terminate	Kill
t.	root	/sbin/procd	0%	0%	🥔 Hang Up	X Terminate	🙆 Кі
2	root	[kthreadd]	0%	0%	🖉 Hang Up	X Terminate	🥥 кі
3	root	[ksoftirqd/0]	0%	0%	🖉 Hang Up	Terminate	🔕 Ka
5	root	[kworker/0:0H]	0%	0%	🖉 Hang Up	Terminate	🔕 Ki
6	root	[kworker/u8:0]	0%	0%	🖉 Hang Up	Terminate	🙆 Кі
r.	root	[rcu_sched]	0%	0%	🦉 Hang Up	Terminate	🙆 Ка
8	root	[rcu_bh]	0%	0%	🖉 Hang Up	Terminate	🙆 Ка
9	root	[migration/0]	0%	0%	🏉 Hang Up	Terminate	🙆 ка
10	root	[migration/1]	0%	0%	🖉 Hang Up	Terminate	() Ki
11	root	[ksoffirqd/1]	0%	0%	🏉 Hang Up	Terminate	() KI
12	root	[kworker/1:0]	0%	0%	🖉 Hang Up	E Terminate	() Ki
13	root	[kworker/1:0H]	0%	0%	🏉 Hang Up	Terminate	🔘 кі
14	root	[migration/2]	0%	0%	🏉 Hang Up	Terminate	() KI
15	root	[ksoftirqd/2]	0%	0%	🖉 Hang Up	Terminate	O K

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 following 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
```

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

Firewall

Routes

System log

Kernel log

Processes

Realtime graphs

System

System

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.

Frewall settings - the default values are part of the basic software configuration.

Routing settings - the default values are part of the basic software configuration.

Prints the most recent log lines of the V2X software stack running on the device.

Prints the most recent log lines of the operating system.

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.

Shows a graphical output of the processors load, wired and wireless network statistics, and active connections.

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.

Administration This menu lets you change the password and the SSH connection settings. This menu lists the installed packages and their Software versions. The default values are included in the basic software configuration, and changes are not recommended. This is a list of scripts that start automatically Startup 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. This menu is used for backing up and updating **Backup / Flash firmware** 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

> Only available if a wireless module is connected to the device. This menu contains an overview of the Wifi settings.

with a static IP address.

You can change the DHCP and DNS handling settings for the system. It is recommended to use the default values.

This is where you can configure the host names. It is recommended to use the default values.

You can specify static routes per network configuration in this menu. It is recommended to keep default settings.

You can find the basic diagnostic tools supported by the OS in this menu: ping, traceroute, and nslookup.

Wifi

DHCP and **DNS**

Host names

Static routes

Firewall

V2x-DSRC

Status

Stack

Participant group Fusion-filtering

Applications

Legacy applications

Traffic Light Controller

Logout

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

This menu shows the V2X stack version, basic stack parameters, and statistics counter listing.

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 settings

Next generation Commsignia filtering and fusion logic, only available in certain software distributions.

Next generation Day 1 applications based on CFF, only available in certain software distributions.

Configuration parameters for Day 1 safety and traffic efficiency applications (licensed separately from the software stack).

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.

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.

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.

commsignia		
Authorization Required		
Please enter your username and password.		
Username root		
Pasword [
📴 Login 🔘 Reset		
Powered by LuCI for-15-05 wands (gb-17.136.50961-13aa54) / ITS-0834/ Chaos Calmer v2.1 r49389		
Figure 10: The login screen		
Select the Network Interfaces menu c	ption 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

WAN WANZ LAN						
Interfaces						
Interface Overview						
Network	Status	Actions				
LAN Master TTS-OB4-M-10	Uptime: 3h 40m 54s MAC-Address: F0 03 8C 47 A0 D7 TX 156 5K 8(960 Pkts.) TX: 357 57 KB (1014 Pkts.) IPv4: 152.166.15324 IPv6: 164: 35ft 1abe.160	Connect (Stop	Edit Edit	E Delete	
WAN etho	Uptime: 3h 40m 55s MAC-Address: DA.49 B1:80 87 FA RX: 823 44 KB (567 PMs.) IX: 2.36 MB (5177 PMs.) IPv4: 192.168.0.53/24 IPv6: 161:3656:1ab8.10::1/60	S Connect	Stop	Edit	Delete	
WAN2	MAC-Address: 00:00:00:00:00:00	🕫 Connect 📢	Stop	🔀 Edit	🔊 Delete	
wan	RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)					
Add new interface						
Global network optic	ons					
IPv6 ULA-Prefi	K Ede 1 85th 1ab8-/48					

Figure 11: The Interfaces page

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

: <mark>©</mark> mms	ignia	Status	- Syste	m = Ser	rvices + Network	+ V2X-DSRC	- Logout	AUTO RET RE SHOR
WAN WAN2	LAN							
nterfaces -	WAN							
this page you can twork interfaces sep	configure the parated by sp	network int aces. You c	erfaces. Yo an also us	ou can bridg e <u>VI,AN</u> not	ge several interface tation INTERFACE.V	s by ticking the "bi ILANNR (<u>e.g.</u> ; eth0	ridge interfaces" field a .1).	nd enter the names of several
ommon Confi	iguration							
General Setup	Advanced S	attings	Physical	Settings	Firewall Sattings			
	Status		ath0	Uptime: MAC-Adi RX: 869 (TX: 2.50 IPv4: 192 IPv6: fdc	3h 42m 27s dress: DA.A9.B18 65 KB (6077 Pkts.) MB (5533 Pkts.) 2.168.0.53/24 1.856b 1ab8 10::1/6	0.87.FA 0		
	Protocol	Static addr	855		*			
IPv4	address	192.168.0.	53					
IPv4	netmask	255.255.25	5.0		٠			
IPv4	gateway							
IPv4 t	proadcast							
Use custom DN	S servers							
IPv6 assignme	ent length	60 Assign a	part of giv	en length o	* of every public IPv6	prefix to this inter	ace	
IPv6 assign	ment hint	Assion r	voliv narte	using this k				

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.

C	Create Interface
	Name of the new interface The allowed charactery are, 2, 2, -1, -1, and
	Note: interface name length 👔 Maximum length of the name is 15 characters including the automatic protocol/bridge prefbx (br; 5n-l, pppde, etc.).
	Proped of the new interface Static address •
	Croate a bridge oper multiple in insteaders
	Cover the Network Starting Cover and
	As thermal Adapter "why? Zenemal Adapter "why? Werkens Netropyck Marster 'US OB4-M-M000F0/" (im) Wrekens Netropyck Marster 'US OB4-M-M000F0/" (im)
	Custon Intélicio
	R Backal Overview

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

: @ mm:	signia	B Stat	us + System + S	Services - Network -	V2X-DSRC -	Logout	AUTO REFILE SHOW
YUAN YUAN							
nterfaces	- WAN						
On this page you ca network interfaces s	n configure ti eparated by	ne network spaces. You	interfaces. You can b i can also use <u>VLAN</u>	ridge several interfaces b notation INTERFACE .VLA	iy ticking the "bridg NNR (<u>e, g</u> ,: eth0.1)	e interfaces" field and er	nter the names of several
Common Cor	nfiguratio	n					
General Setup	Advanced	Settings	Physical Settings	Firewall Settings			
Bring	up on boot						
Use builtin IPv6-m	anagement	2					
Override M	AC address		1 80 87.FA				
Ov	erride MTU						
Use gate	way metric	0					
DHCP Server							
General Setup	IPv6 Settl	ngs					
lano	re interface	ROD	vable DHCP for this is	nterface			
		- 00	and the second				
	R B	ack to Over	stass			Sma & Ann	hu Sawa Revel
		ack to over	THEY .			Save & App	y care read

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

Interfaces On this page you can network interfaces so	- WAN n configure the network i eparated by spaces. You	nterfaces. You can brid can also use <u>VLAN</u> not	ge several interfaces t tation INTERFACE.VLA	by ticking the "bridge ANR (e.g. eth0.1)	interfaces" field and en	er the names of several
Common Cor	figuration					
General Setup	Advanced Settings	Physical Settings	Firewall Settings			
Create / Assign fir	ewall-zone I an	to the frewall zone you to out the create field to c	want to assign to this idefine a new zone and	nterface. Select unsp l attach the interface f	recified to remove the in	terface from the associated
OHCP Server	10. A Desta					
Ignor	e interface 🖉 🥥 De	sable <u>DHCP</u> for this inte	inface.			

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 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.

Authorization Re	quired	
Please enter your username and	password,	
Username	root	
Password	[
Director Director		

Figure 17: The login screen

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

Network	Status	Actions				
LAN	Uptime: 3h 40m 54s	& Connect Stop				
Master "ITS-OB4-M-1000100"	MAC-Address: F0:03/8C.47/A0:D7 RX: 145.66 KB (960 Pkts.) TX: 357.57 KB (1014 Pkts.) IPv4: 192.168.1.53/24 IPv6: fdc1:85fb:1ab8::1/60					
WAN Etho	Uptime: 3h 40m 55s MAC-Address: DA:A9:B1:80:87:FA RX: 823.44 KB (5761 Pkts.) TX: 2.36 MB (5171 Pkts.) IPv4: 192.168.0.53/24 IPv6: fdc1:85fb:1ab8:10::1/60					
WAN2	MAC-Address: 00:00:00:00:00:00	🖉 Connect 🥘 Stop 🛃 Edit 💌 Delete				
Add new Interface	RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)					
obal network options						

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

Save & Apply Save Re:

Figure 18: The Interfaces page

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

	COmmisignia Status + System + Services + Network + V2X DISRC + Logout MINTERNETSING	
	Interfaces - WAN	
	webnoth interfaces separated by spaces. You can also use <u>VLAN</u> existing EXTERTACE, VLANNE (g.g. etto).1)	
	Common Configuration General Setup	
0	Stade Uptime: 10:50a; 64 MCA: 40/resp: DA(A) 01:00:37 FA Stade DR(PDP Pas); TX: T2:04 (0:700? Pas); UPK: 64:11:55b: 1:100; TX: 12:04 (0:700? Pas); TX: 12:04 (0:700? Pas);TX: 12:	
	Backs Overniege Save & Arguit Save Messel	

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.

Create Interface	
Name of the new interface	WAN
	The allowed characters are A-2, s-2, 0-9 and
Note: interface name length	Maximum length of the name is 15 characters including the automatic protocol/bridge prefix (br-, 6in4-, pppoe- etc.)
Protocol of the new interface	DHCP client
Create a bridge over multiple interfaces	8
Cover the following interface	C Alapter: "can0"
	Ethernet Adapter: "cant"
	Ethernet Adapter: "eth0" (wan)
	Ethernet Adapter: "eth1"
	Carl Ethernet Adapter: "usb0"
	wireless Network: Master 'ITS-OB4-M-1000100" (tan)
	Custom Interfaces

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

WAN WAN2	- WAN	te network	interfaces. You can bridg	e several interfaces by ticking t	he "bridge interfaces" field a eth0.1).	ind enter the names of several
Common Cor	figuratio	n				
General Setup	Advanced	Settings	Physical Settings	Firewall Settings		
Bridge	e interfaces	0 g a	eates a bridge over spec	ified interface(s)		
	Interface		Ethernet Adapter: "can0" Ethernet Adapter: "can1" Ethernet Adapter: "eth0" Ethernet Adapter: "eth1" Ethernet Adapter: "usb0" Wireless Network: Maste Custom Interface:	(wan) *'ITS-OB4-M-1000100" (lum)		
OHCP Server						
General Setup	IPv6 Settin	ngs				
Ignor	re interface	2 🕢 D	isable <u>DHCP</u> for this inte	flace.	Save 8	Keply Save Real

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

	COmmisignia Status - System - Services - Network - V2XDSRC - Logard AMTRIMPREMICER
	YON WINZ LAN
	Interfaces - WAN
	On this page you can contigure the network interfaces? You can bridge serveral interfaces by locking the finitige interfaces? field and enterther planes of several network interfaces separated by spaces. You can also use VLAN notation TVTERFACE. VLANK (e.g., etho.1)
	Common Configuration
	General Statig Ad-Band Stellings Physical Statiges Provided Statiges
	Create / Assign frewalk-zone Inter Line: (b)
	Charge the frexual zone you want to assign to this interface. Select unspected to remove the deterface from the associated zone or III out the create field to define a new zone and attach the interface to it
	DHCP Server
	General Setup IPv6 Settings
	Ignore interface 🛛 🖉 👔 Disable <u>DHCP</u> for this interface.
•	Back to Overview.
	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.

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 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.

Authorization Required fease enter your username and password.	
Username root	
Password	
Login Reset www.eduy(uc) for 5 65 branch (gb: 17 195 59901-13as57) / ITS-083-M Chaos Calmer v2 1;4598	9

Figure 24: The login screen

 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.

:omms	signia	Statu	s = System = S	ervices - Networ	k + V2X-DSRC + Logout	ALTO REFRESH ON
WAN WAN2	LAN					
this page you can twork interfaces so	- LAN configure the parated by t	e network i paces. You n	nterfaces. You can bri can also use <u>VLAN</u> n	dge several interfac otation INTERFACE .	es by ticking the "bridge interfaces" field an vLANNR (e.g., eth0.1).	d enter the names of several
General Setup	Advanced	Settings	Physical Settings	Firewall Setting	1	
	Status		Client TTS-O	9 34-M-1000100"	Uptime: 0h 49m 51s MAC-Address: F0:03.8C.47.A0.D7 RX: 0.00 8 (0 PMs.) TX: 0.00 8 (0 PMs.) IPv4: 192.168.153/24 IPv6: fdc1.85fb:1ab8.:160	
	Protocol	Static add	fress	*		
IP	/4 address	192,168,1	1.53			
IPv	4 netmask	255.255	255.0	*		
IPv	4 gateway					
IIPv4	broadcast					
Use custom DI	NS servers			1		
IPv6 assignn	nent length	60 () Assign	a part of given length	* of every public IPv6	-prefix to this interface	
IPv6 assig	nment hint					

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.

COmmsignia State - System - Service - Network - V2X-DSRC -	Logout (MITO P97HISH CM	
Wireless Overview		
Generic MAC80211 802.11abgn (radio0)	C Scan 🔝 Add	
SID: 1152-084-M-10001001 Mode: Chent ors: Wheeles is Basched or not associated	Disable Z Edit S Remove	
Associated Stations		
3.5U INAC-ADDRESS IPV4-ADDRESS Signal	NOISE NA HATE I A HATE	
Peyened by LuCl for-15 05 branch (gls-18 021 57137-5762 172) / RS-OB3-M Chaos Chemer v2.1 r46688		
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.

0.00000	icoli	Elizaria European Veneziaria VIV. DED Laurat Alternative
: <mark>o</mark> mms	signia	a satus - sytoom - services - heterook - v2A-USHC - Logicat - menomenation
evice Config	juration	
General Setup	Advanced	d Sattings
	Status	SSID: ITS-DB4-M-1001100 I Mode: Client My Wreless is disabled or not associated
Wireless network	is enabled	Disable
Operating	frequency	Mode Band Channel Widh N * 2.4 GHz * 11 (24/2 MHz *) 21 MHz *
Trans	smit Power	15 dBm (31 mil/) *
nterface Conf	figuratior	n
General Setup	Wireless S	Searthy
	ESSID	ITS-0B4-M-1000100
	Mode	Client
	BSSID	
	Network	
		Choose the network(s) you want to attach to this wireless interface or BI out the create field to define a new network
	📄 Ba	Jack to Overview Save & Apply Save Kesel

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.

	Wireless Network: Client (TS-OB4-M-1000100" (wlan0)
	The Device Configuration section covers physical sectings the radio hardware such as channel, transmit power or anterna selection wipth ger shared among all defined winders networks (if the radio hardware is multi-SSID dipable). Per network settings like encryption or operation mode are organized in the interface Configuration.
	Device Configuration
	General Setup Advanced Settings
	Country Code 00 - World Country Code 01 - World Country Code 04-Weil SO/IEC 3166 alpha2 country codes.
	Distance Optimization © Distance to farthest network member in meters. Fragmentation Transhold
	RTSCT97Trreshold
	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).

Encryption	WPA2-PSK	•	
Cipher	auto	*	
Key		8	

- 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.

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 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.

commsigni	а					
Authorization Re	quired					
Please enter your username and	password.					
Username	root					
Password						
1 83000						
🔲 Login 🧶 Reset						
Figure 31: 2. Select the Netwo	The login scree		is will show ;	a list of the a	Iready conf	ïgured
interfaces availa	ble on the devic	e.				
commsignia	Status + System + Services - Netw	ork + V2X-DSRC + Logou	AUTOREFE	RESH CON		
WAN WANZ LAN						
Interfaces						
Interface Overview						
Network	Status	Actions				
LAN Master 175-0643-100010	Uptime: 3h 40m 54s MAC-Address: F0.03.8C 47 A0 D7 RX: 145.66 KB (960 Pits.) TX: 357.57 KB (1014 Pits.) IPv4: 192.168.1.53/24 IPv6: 161.65b/t.169/	Connect Q	Stop Z Edt 🗷 Defet	10		
WAN Éo	Uptime: 3h 40m 55s MAC-Address: DA:A9:B1:80:87,FA RX: 823.44 K8 (5761 Ptr5) TX: 23:64 M8 (5171 Ftks) IPv4: 192.168.0 53224 IPv6: tds1.85tb,1ab8:10,7160	Connect C	itop 🖉 Edit 💌 Delet	to		
WANZ E wan	MAC-Address: 00:00:00:00:00:00 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	🛱 Connect 🥘	Stop 🔣 Edit 💉 Deter	te		
Add new interface						
Global network options						



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.

- Commission	Status + System + Services + Netwo	ik + VZA-USHG + Logout	PROTO HEARE SHI ON
WAN WAN2 LAN			
nterfaces - LAN			
n this page you can configure the	ie network interfaces. You can bridge several interfaces you can also use VI AN notation INTERFACE	es by ticking the "bridge interfaces" field and enter the r	names of several
	And a second second second	MUR	
Common Configuratio	n		
General Setup			
Status		Uptime: 0h 14m 11s	
	OF THE REPORT OF THE PROPERTY	MAC # July 50 03 00 17 40 07	
	Calent 11S-084-M-1000100	MAC-Address: F0.03.0C.47.A0.07	
	Calent 115-CB4-M-1000100	RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	
	Calent 115-084-W-1000100*	RX: 0.00 B (0 Pkts) TX: 0.00 B (0 Pkts) IPv4: 192 168.153/24	
	Caent 115-084-N-1000100	MAC.48001995 F0.05.30.47.40.07 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.) IPv4: 192.168.1.5.324 IPv6: fdc1.85fb.1ab8::1/60	
Protocol	Cleft: 115-05-44-1000107	ML 4.00 (0 PMs) TX 0.00 B (0 PMs) TX 0.00 B (0 PMs) IPv4: 192.168.1.53/24 IPv6: t6c1.85/b.1ab8.1/60	
Protocol	DHCP client *	MAC_A001698: F0/350-47-A0U1 RX 000 B (0 PMs) TX 000 B (0 PMs) IPv4: 526.15.5224 IPv6: 6c1 85fb 1ab8 1/60	

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.

radic0, Client "ITS-OB4-M-1000100"		
Wireless Overview		
Generic MAC80211 802.11abgn (radio0)	🗟 Scan 🔝 Add	
SSID: TIS: OBE MA 1900 1001 Mode Cherk os: Wreless is disabled or not associated Associated Stations	Disable Z Edt K Remove	
SSID MAC-Address IPv4-Address Sign No information evaluable	aal Noise RX,Rate TX Rate	
Powered by LuCI for-15 05 brench Left-16.021 57137-5fia21321 / 175-083-M Chaos Calmer v2	2.1 r46888	

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.

Coneral Setur	Advanced	Carton C
General Semp	Status	user (jo use SSID: [TS-OB#/M=1064:09 Mode: Client priv (Vroless is ditabled or not associabled
Wireless network	is enabled	Diable
Operating	frequency	Mode Band Chambel Width N * 2.4 GHz * 111(2452 MHz) * 20 MHz *
Trans	mit Power	15 dBm (31 mW)
Interface Conf	figuration	
General Setup	Wireless S	ecuity
General Setup	Wireless S	ms-084-M-1000100
General Setup	Wireless S ESSID Mode	0049y ITS-0844-100100 Client •
General Solup	Wireless S ESSID Mode BSSID	ITS-OB4-M-1000100 Client •
General Setus	Wireless S ESSID Mode BSSID Network	Ecology ITS-OB4-M-1000100 Client • 2 Inn. (a)
General Setup	Wireless S ESSED Mode BSSED Network	econfy ITS-OB4-M-1000100 Client
General Setue	Wireless S ESSID Mode <u>BSSID</u> Network	ITS-0844-100100 Client •
General Setue	Wireless S ESSID Mode BSSID Network	ITS-OB4-M-1000100 Client Immediate Immediate



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.

Wireless N The Device Configure defined wireless net Configuration.	letwor ration section works (if the	k: Client " o covers physical se radio hardware is n	ITS-OB4 ettings of the radio sulti-SSID capabl	-M-1000100" (Wian0) to hardware such as channel, transmit power or anterna selection which are shared among all le). Per network settings like encryption or operation mode are grouped in the <i>interface</i>
Device Config	guration			
General Setup	Advanced	l Settings		
Co	untry Code	00 - World	3166 alpha2 cour	v ntry codes.
Distance C	ptimization	Olistance to face and the second s	rthest network m	ember in meters.
Fragmentation	Threshold			
RTSICTS	Threshold			

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).

General Setup Wireless	Security		
Encryption	WPA2-PSK		
Cipher	auto	•	
Key		Ø	
Enable WPS pushbutton,	8		

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.

Authorization Re	auired	
Please enter your username and	password.	
Username	root	
Password	[

Figure 38: The login screen

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

WAN WANZ LAN									
nterfaces nterface Overview									
Network	Status	Actie	ons						
LAN	Uptime: 3h 40m 54s. MAC-Addross: F0.03.0C 47 A0.D7 RX: 145.66 KB (960 Pkts.) TX: 357.57 KB (1014 Pkts.) IPv4: 192.166.153/24 IPv6: 161: 35fb: 1ab8.1160	8	Connect	0	Stop	12	Edit	×	Delete
WAN La etho	Uptime: 3h 40m 55s MAC.Address: DA A9 B1:80:87:FA RX: 823.44 KB (5761 Pkts.) TX: 2,36 MB (5171 Pkts.) IPv4: 192.168.0.53/24 IPv6: idc1:85fb:1ab8:10=:1/60	8	Connect		Stop		Edit		Delete
WAN2	MAC-Address: 00:00:00:00:00:00	12	Connect		Stop		Edit		Delete
wan	RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)								
Add new interface									
Global network options									
IPv6 ULA-Prefix Idc1	85fb:1ab8::/48								
					Sa	we & Ap	ply S	Save	Reset

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

COmmsignia Status + System + Services + Wethaven + V2X-DSRC + Logout
WAN WANZ LAN
Interfaces - WAN2 On this page you can configure the network interfaces. You can bidge several interfaces by sicking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use <u>VLAN</u> instalsion INTERFACE.VLARR (e.g., etb).1).
Common Configuration
General Setup Advanced Settings
Status MAC. Address: 00 00 00 00 00 00 wan RX 000 B (0 Pts.) TX 0 00 B (0 Pts.)
Protocol NCM y
Modern device (dowthyUSB0
Service Type auto •
APN
PIN
PAPICHAP usemama
PAPICHAP password
Dial number Symmetry
Surve X Appy Same Resid
Powered by LuCI are 15.05 branch (gb-18.021.57137.61a2132) / ITS-083-M Cbass Calimere2 Tr46008
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.

On this page you can configure th	🔏 he network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several	
etwork interfaces separated by	spaces. You can also use <u>VLAN</u> notation INTERFACE.vLANNE (<u>e.g.</u> ; eth0.1).	
Common Configuratio	in the second	
General Setup Advanced	1 Settings Firewall Settings	
Bring up on boot	8	
Use builtin IPv6-management	*	
sutomatic		
Modem init timeout	23	
	Maximum amount of seconds to wait for the modern to become ready	
Use default gateway	I unchecked, no default route is configured	
Use gateway metric	0	
Use DNS servers advertised by peer	C I unchecked, the advertised DNS server addresses are ignored	
LCP echo failure threshold	0	
	Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures	
LCP echo interval	5	
	Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold	
Inactivity timeout		
	@ Close inactive connection after the given amount of seconds, use 0 to persist connection	

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.

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.

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:



- 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.

- 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.



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 Serial line: Speed (baud) Data bits Stop bits

Flow control

XON/XOFF

Value

COM4

115200

8

1

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.

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.

