

For more information, we kindly ask you to see the OpenWRT wiki (the linux distribution wiki), for example the pages on securing access:

<http://wiki.openwrt.org/doc/howto/secure.access>

Step 5 - Save changes

Press the *[Save and Apply]* button at the bottom of the page, to keep and apply your new settings.

WiFi Password

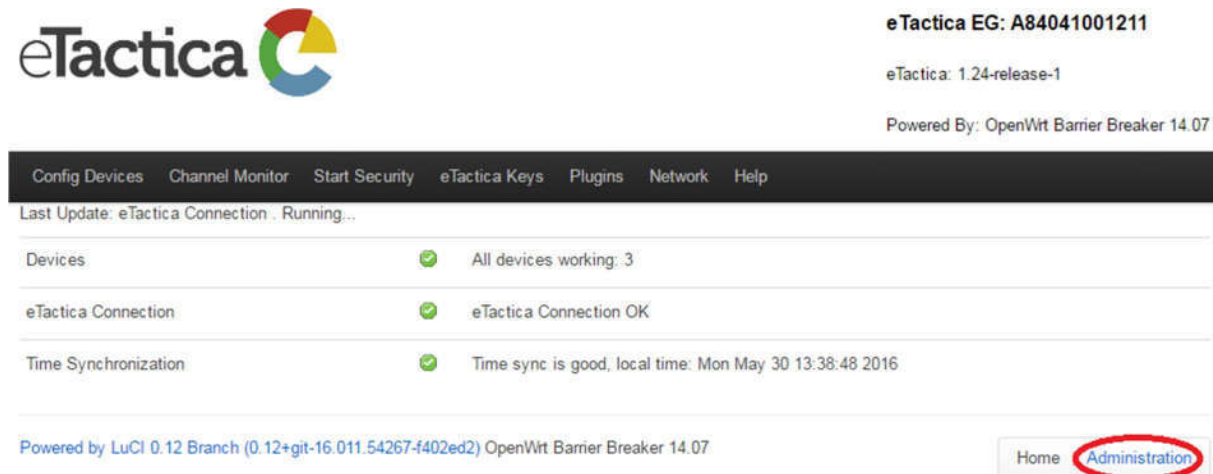
The following covers how to change the WiFi security password.

Step 1 - Connect to the Gateway

You need to be successfully connected to your gateway device. If not, see chapter 2, [Connecting to Gateway](#).

Step 2 - Go to Administration page

From the home page of the administration web console of your device, click on the *[Administration]* link.



eTactica EG: A84041001211

eTactica: 1.24-release-1

Powered By: OpenWrt Barrier Breaker 14.07

Config Devices Channel Monitor Start Security eTactica Keys Plugins Network Help

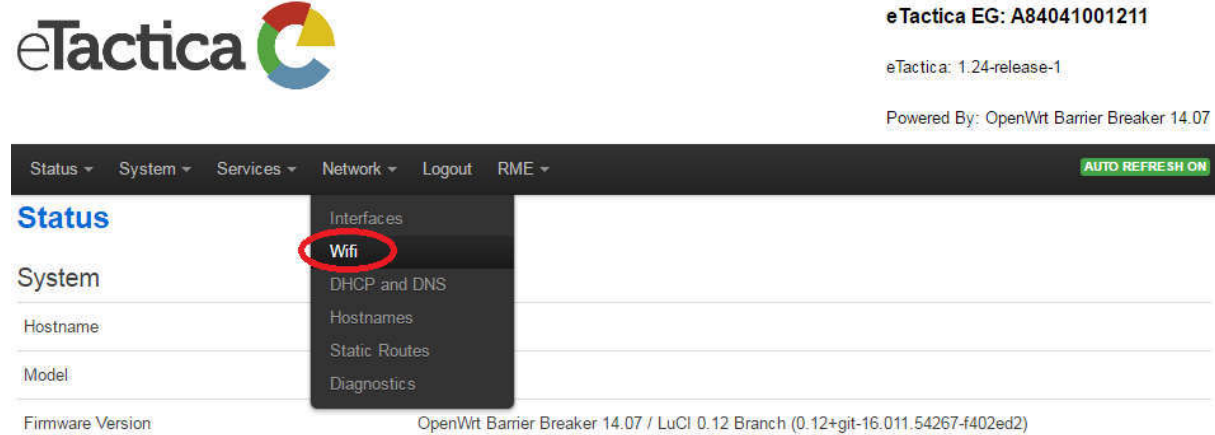
Last Update: eTactica Connection . Running...

Devices	✓	All devices working: 3
eTactica Connection	✓	eTactica Connection OK
Time Synchronization	✓	Time sync is good, local time: Mon May 30 13:38:48 2016

Powered by LuCI 0.12 Branch (0.12+git-16.011.54267-f402ed2) OpenWrt Barrier Breaker 14.07

Home **Administration**

Step 3 - Go to WiFi configuration page
From the top menu, choose Network->WiFi.



The screenshot shows the eTactica Gateway web interface. At the top, the eTactica logo is on the left, and the device ID 'eTactica EG: A84041001211' and version 'eTactica: 1.24-release-1' are on the right. Below the header, a navigation menu is visible with 'Network' selected, and a dropdown menu showing 'Wifi' circled in red. The main content area shows system information like 'Hostname', 'Model', and 'Firmware Version'.

You will be asked to login, if you haven't already done so.

Press the *[Edit]* button.

Wireless Overview



The screenshot shows the 'Wireless Overview' section. It displays details for a 'Generic MAC80211 802.11bg (radio0)' on channel 11. Below this, the SSID 'eTactica_EG_001211' and mode 'Master' are shown. At the bottom right, there are three buttons: 'Disable', 'Edit' (circled in red), and 'Remove'.

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
eTactica_EG_001211	AC:81:12:7A:82:E0	192.168.1.19	-90 dBm	-108 dBm	5.5 Mbit/s, MCS 0, 20MHz	36.0 Mbit/s, MCS 0, 20MHz

Powered by LuCI 0.12 Branch (0.12+git-16.011.54267-f402ed2) OpenWrt Barrier Breaker 14.07

[Home](#) | [Administration](#)

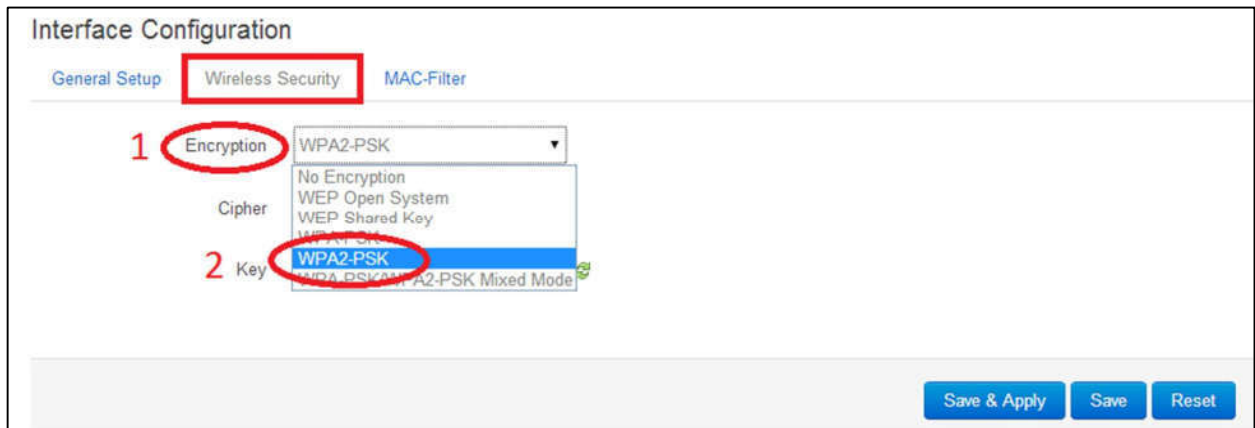
Step 4 - Change password

To change your WiFi password, scroll down to the part entitled:
Interface Configuration->Wireless Security .

Here you have to:

1. Choose Encryption
2. Choose WPA2/PSK

Unless you have any reason not to, choose *WPA2/PSK* (if you have some pre 2006 WiFi gear, you may need to choose *WPA-PSK/WPA2-PSK mixed mode*).



Interface Configuration

General Setup **Wireless Security** MAC-Filter

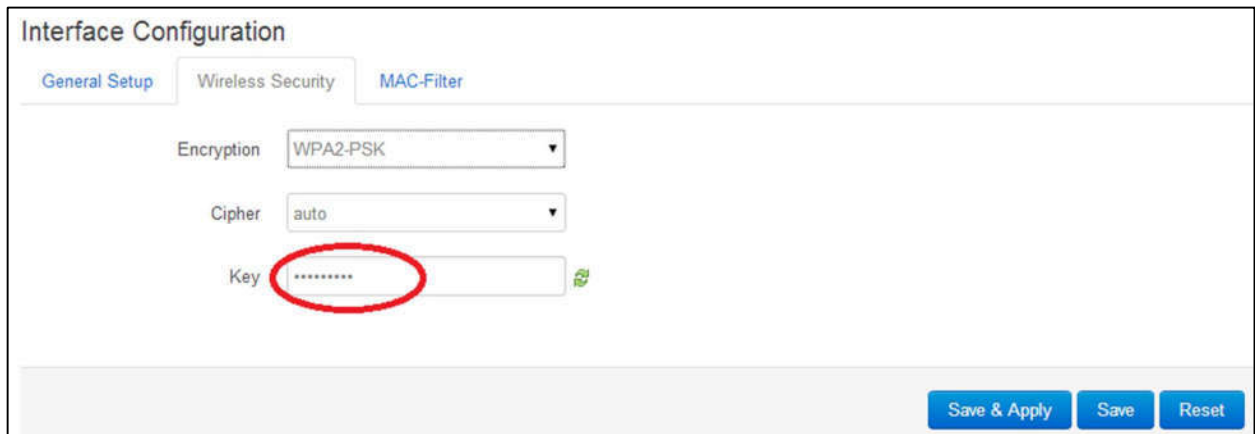
1 Encryption WPA2-PSK

Cipher

2 Key WPA2-PSK

Save & Apply Save Reset

Then, you can change your password in the *Key* field.



Interface Configuration

General Setup Wireless Security **MAC-Filter**

Encryption WPA2-PSK

Cipher auto

Key *****

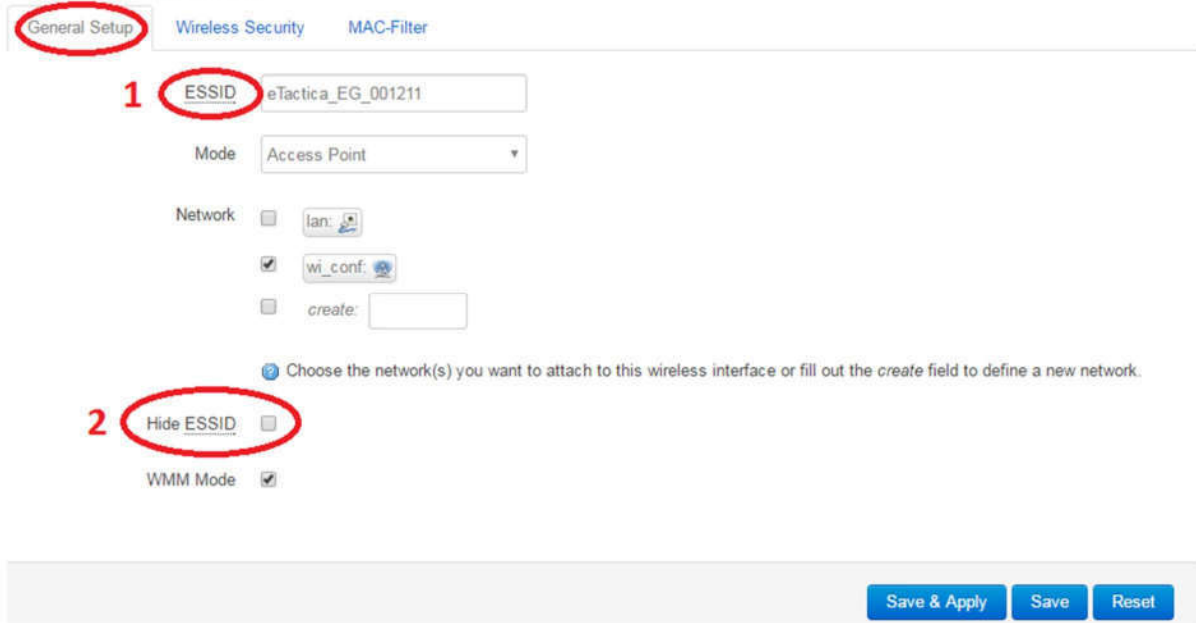
Save & Apply Save Reset

Step 5 - Additional SSID configuration

Additionally, if you select the General Setup tab, you can edit the following SSID settings:

1. Change the (E)SSID to make it discoverable under your desired name
2. Hide the (E)SSID so only those that actually know the (E)SSID can find the device on the wireless network

Interface Configuration



General Setup Wireless Security MAC-Filter

1 ESSID eTactica_EG_001211

Mode Access Point

Network ☐ lan: ☐ ☒ wi_conf: ☐ create:

[Choose the network\(s\) you want to attach to this wireless interface or fill out the create field to define a new network.](#)

2 Hide ESSID ☐

WMM Mode ☒

Save & Apply Save Reset

Step 6 - Save settings

When done, press the *[Save and Apply]* button at the bottom of the page, to keep and apply your new settings.

10. SNMP Support

The eTactica gateway supports queries via SNMP v2c, to get live measurement readings. In the following, the steps to enable this feature is described.

Enabling SNMP

The live measurement readings from all configured devices can be queried via SNMP v2c, on the standard UDP port 161, with the read-only community "public".

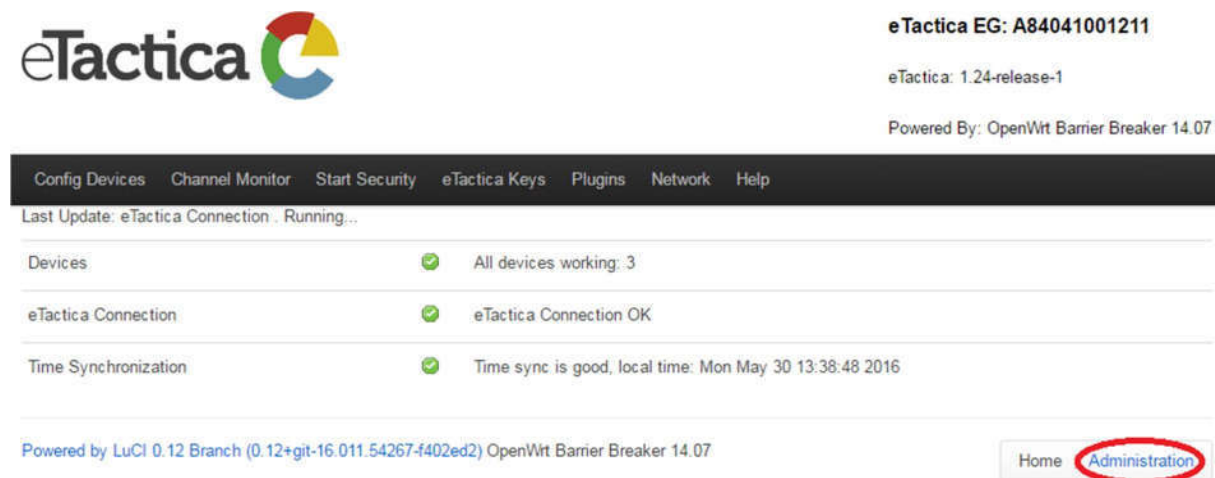
This service is disabled by default, but can be enabled as follows.

Step 1 - Connect to the Gateway

You need to be successfully connected to your gateway device. If not, see chapter 2, [Connecting to Gateway](#).

Step 2 - Go to Administration page

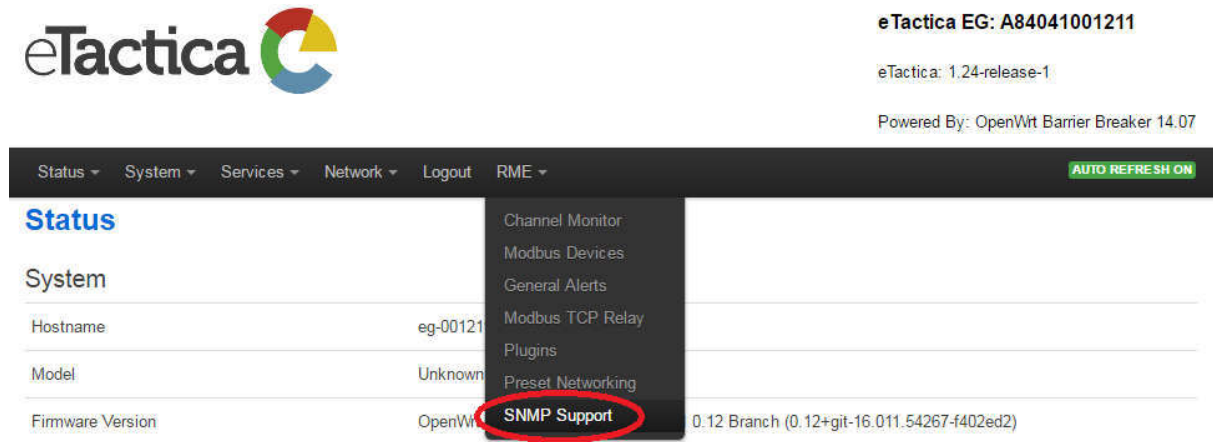
From the home page of the administration web console of your device, click on the [Administration](#) link.



This will require you to login, using the root password you have configured earlier. If not, please see chapter 9, [Password Settings](#).

Step 3 - Go to SNMP support

From the top menu, choose RME->SNMP Support.



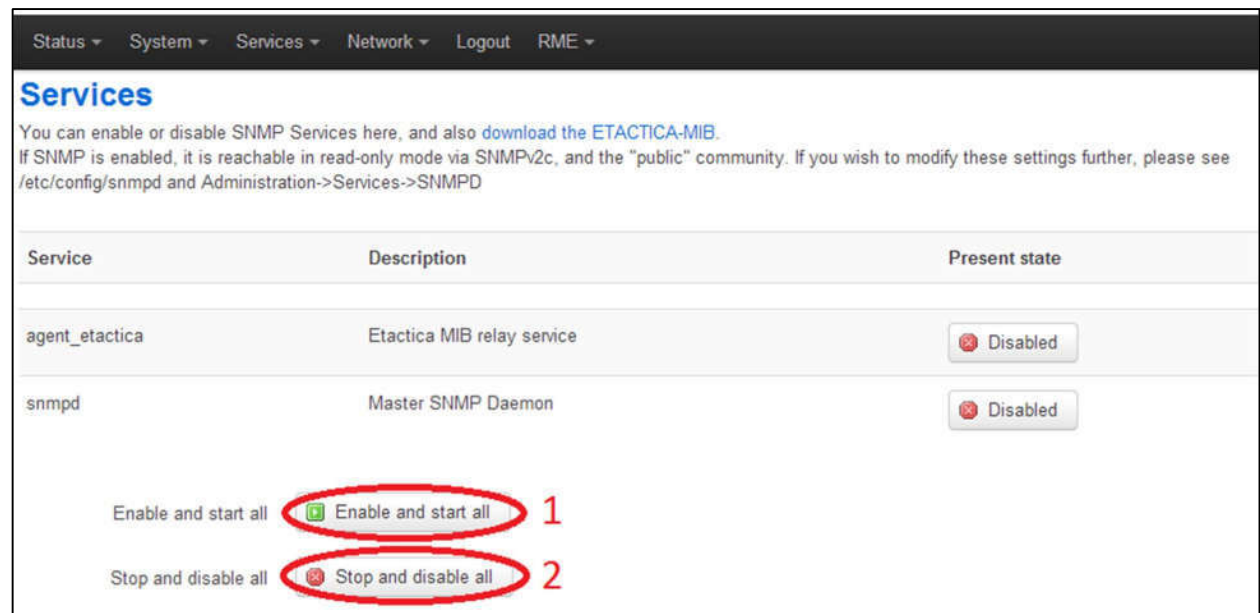
The screenshot shows the eTactica Gateway web interface. The top navigation bar includes 'Status', 'System', 'Services', 'Network', 'Logout', and 'RME'. The 'RME' dropdown menu is open, showing options: 'Channel Monitor', 'Modbus Devices', 'General Alerts', 'Modbus TCP Relay', 'Plugins', 'Preset Networking', and 'SNMP Support' (which is circled in red). The main content area shows the 'Status' page with system information: Hostname (eg-00121), Model (Unknown), and Firmware Version (OpenWrt 0.12 Branch (0.12+git-16.011.54267-f402ed2)).

The SNMP Support page contains links to the MIB file for use with third party SNMP tools such as *nagios*. The latest version of the MIB is always available at: <http://packages.etactica.com/snmp/ETACTICA-MIB.mib>.

The MIB file matching the running firmware can also be directly downloaded from the SNMP Support page itself. The support page also shows the status of the SNMP services and provides links to enable or disable them.

Step 4 - Enable SNMP

In most cases, you can simply press the *[Enable and start all]* button (1) to enable SNMP.



The screenshot shows the 'Services' page in the eTactica Gateway web interface. It lists two services: 'agent_etactica' (Etactica MIB relay service) and 'snmpd' (Master SNMP Daemon), both with a 'Disabled' status. At the bottom, there are two buttons: 'Enable and start all' (labeled 1) and 'Stop and disable all' (labeled 2). Both buttons are circled in red.

If you want disable SNMP you just follow the same procedure and use the *[Stop and disable all]* button.

Configuration (basic)

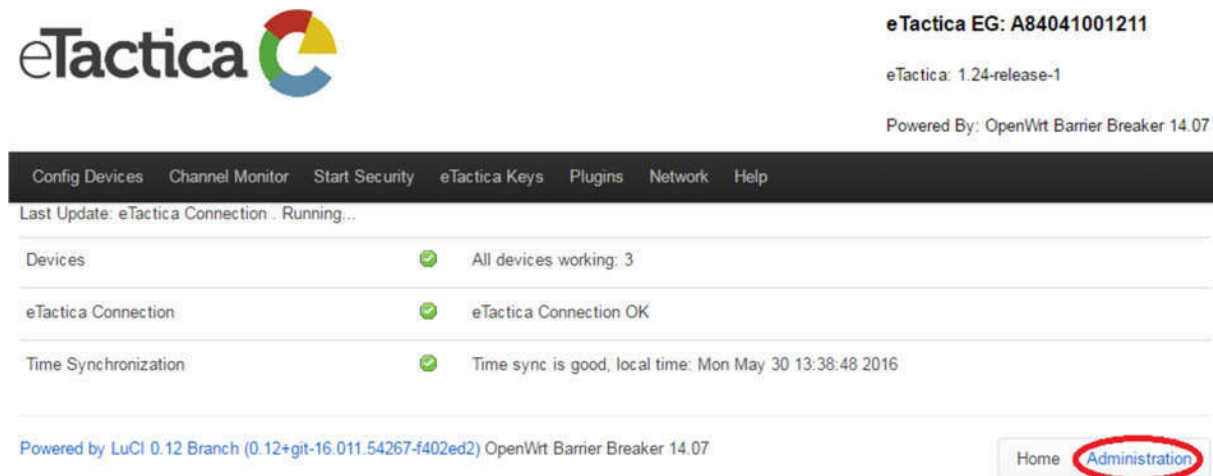
The SNMP daemon has *many* configuration settings, and they are all considered *advanced* topics. Some basic support is available via the administration web console, described in the following.

Step 1 - Connect to the Gateway

You need to be successfully connected to your gateway device. If not, see chapter 2, [Connecting to Gateway](#).

Step 2 - Go to Administration page

From the home page of the administration web console of your device, click on the [Administration](#) link.



This will require you to login, using the root password you have configured earlier. If not, please see chapter 9, [Password Settings](#).

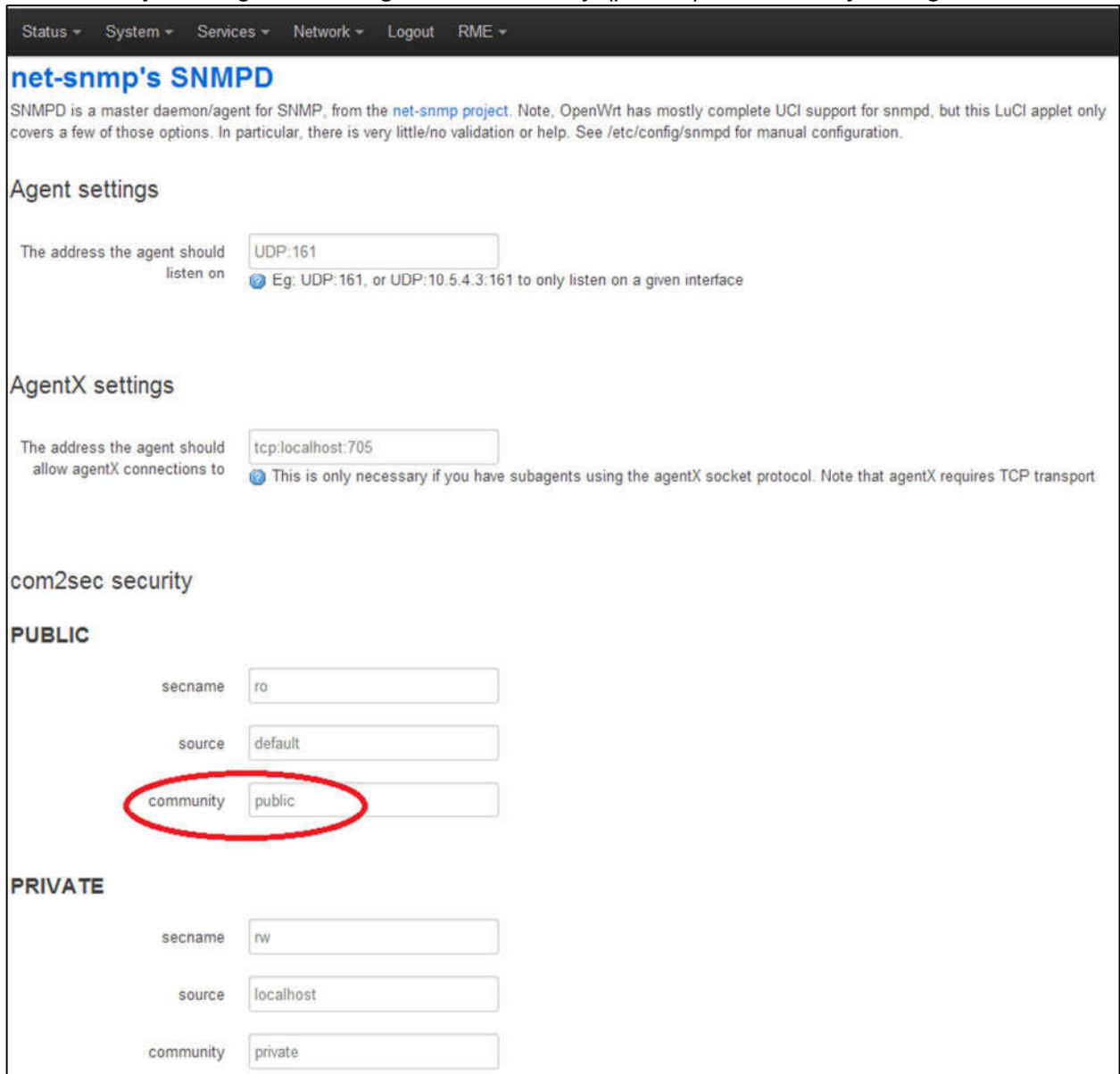
Step 3 - Access the SNMPD configuration page

From the top menu, choose [Services->SNMPD](#).



Step 4 - Change public/read-only community string

The only basic configuration value you may wish to change is the SNMP community setting - to change the read-only (public) community string.



If desired, you can change the Agent settings to listen for SNMP queries on a different port, or only a specific interface, but you should *NOT* change the AgentX address. This would prevent the eTactica MIB service from connecting and providing data.

In this section you can also modify the read-write community string (private by default) and where it can be accessed from (*localhost* only by default). You could enter a trusted network address here if desired, but consult the snmpd manual for full documentation at: <http://www.net-snmp.org/>.

Note that all the data in the eTactica MIB is read-only, regardless of which community string is used to access the MIB.

If you scroll down there is a basic UI for other settings. You could for instance delete the section for public_v1 to only allow SNMP v2c queries if desired.

Step 5 - Save Settings

When done, remember to press the *[Save and Apply]* button at the bottom of the page, to keep and apply your new settings.

Configuration (advanced)

If you want to make more detailed configuration changes to the snmp daemon, you need to edit the configuration files directly, or have a deeper understanding of the options available.

This requires familiarity with SSH and the command line environment of a Linux server, as well as familiarity with the Net-SNMP package.

The configuration file is `/etc/config/snmpd` (See <http://wiki.openwrt.org/doc/uci/snmpd> for more information).

Example usage

In the following, you find examples of SNMP queries.

To query each devices attributes

From a linux shell

```
$ snmptable -v 2c -c public 192.168.1.46 ETACTICA-MIB::etacticaDeviceAttributeTable -Cbi -OU
SNMP table: ETACTICA-MIB::etacticaDeviceAttributeTable
      index etacticaDevicePoints
"0004A3845A9B"          2
"0004A384E333"          12
"0004A39C541A"          12
"0004A39C62AE"          12
"0004A39C8187"          12
"FrerNaNo..H-04"        3
```

To query each devices readings

From a linux shell

```
$ snmptable -v 2c -c public 192.168.1.46 ETACTICA-MIB::etacticaDeviceReadingTable -Cbi -OU
SNMP table: ETACTICA-MIB::etacticaDeviceReadingTable
```

index	DataAge	Temperature	EnergyConsumed	EnergyConsumedReactive	Frequency
"0004A3845A9B"	0:0:00:01.07	?	?	?	?
"0004A384E333"	0:0:00:01.08	?	?	?	?
"0004A39C541A"	0:0:00:02.09	?	?	?	?
"0004A39C62AE"	0:0:00:01.10	?	?	?	?
"0004A39C8187"	0:0:00:02.10	?	?	?	?
"FrerNaNo..H-04"	0:0:00:01.11	?	8788470	171510	6000

Hint: double-click to select code

To query the readings of every point on each device

From a linux shell

```
$ snmptable -v 2c -c public 192.168.1.46 ETACTICA-MIB::etacticaDevicePointReadingTable -Cbi -OU
SNMP table: ETACTICA-MIB::etacticaDevicePointReadingTable
```

index	Current	Voltage	PowerFactor
"0004A3845A9B".1	93	?	?
"0004A3845A9B".2	44	?	?
"0004A384E333".1	45	?	?
"0004A384E333".2	44	?	?
"0004A384E333".3	40	?	?
"0004A384E333".4	45	?	?
"0004A384E333".5	49	?	?
"0004A384E333".6	68	?	?
"0004A384E333".7	41	?	?
"0004A384E333".8	42	?	?
"0004A384E333".9	0	?	?
"0004A384E333".10	40	?	?
"0004A384E333".11	0	?	?
"0004A384E333".12	41	?	?
"0004A39C541A".1	53	?	?
"0004A39C541A".2	199	?	?
"0004A39C541A".3	319	?	?
"0004A39C541A".4	52	?	?
"0004A39C541A".5	53	?	?
"0004A39C541A".6	53	?	?
"0004A39C541A".7	52	?	?
"0004A39C541A".8	50	?	?
"0004A39C541A".9	50	?	?
"0004A39C541A".10	52	?	?
"0004A39C541A".11	0	?	?
"0004A39C541A".12	50	?	?
"0004A39C62AE".1	45	?	?
"0004A39C62AE".2	40	?	?

Hint

11. Upgrade Firmware

The eTactica Gateway firmware can be upgraded via the administration web console.

All new releases of the gateway firmware, are provided and shared by eTactica at this location:

http://packages.etactica.com/barrier_breaker/

In the following, the firmware upgrade process is described.

Before you begin

Before you begin, we recommend that you locate and download the new firmware image to your computer:

1. Follow this link, in your web browser:
http://packages.etactica.com/barrier_breaker/
2. Follow the link with the highest version number xx.yy.zz:
`../barrier_breaker/gateway-xx.yy.zz-release-1`
3. Continue via atheros (for EG-100):
`../barrier_breaker/gateway-xx.yy.zz-release-1/atheros/` or `ax71xx` (for EG-200)
`- xx.yy.zz-release-1/ar71xx/`
4. Locate this file: "openwrt-atheros-combined.squashfs.img" (EG-100) or `openwrt-ar71xx-generic-rme-eg200-squashfs-sysupgrade.bin` (EG-200)
5. Press "md5sums" as well. This will download a file with checksums that you need to use later to verify the integrity of your firmware image.

Now move on to the upgrade process.

Step 1 - Connect to the Gateway

You need to be successfully connected to your gateway device. If not, see chapter 2, [Connecting to Gateway](#).

Step 2 - Go to Administration page

From the home page of the administration web console of your device, click on the [Administration](#) link.

[Config Devices](#)
[Channel Monitor](#)
[Start Security](#)
[eTactica Keys](#)
[Plugins](#)
[Network](#)
[Help](#)

Last Update: eTactica Connection . Running...

Devices	✓	All devices working: 3
eTactica Connection	✓	eTactica Connection OK
Time Synchronization	✓	Time sync is good, local time: Mon May 30 13:38:48 2016

Powered by LuCI 0.12 Branch (0.12+git-16.011.54267-f402ed2) OpenWrt Barrier Breaker 14.07

[Home](#)
[Administration](#)

This will require you to login, using the root password you have configured earlier. If not, please see chapter 9, [Password Settings](#).

Step 3 - Go to the upgrade page

From the top menu, choose System->Backup/Flash Firmware.

[Status](#)
[System](#)
[Services](#)
[Network](#)
[Logout](#)
[RME](#)
[AUTO REFRESH ON](#)

[Status](#)
[System](#)
[Software](#)
[Startup](#)
[Scheduled Tasks](#)
[LED Configuration](#)
[Backup / Flash Firmware](#)
[Custom Commands](#)
[Reboot](#)

Hostname	eg-001211
Model	Unknown
Firmware Version	OpenWrt Barrier Breaker 14.07 / LuCI 0.12 Branch (0.12+git-16.011.54267-f402ed2)
Kernel Version	3.10.49
Local Time	-

Step 4 - Get image file

Locate the *Flash new firmware image* section and follow this procedure:

1. Press the [Choose file] button (1), and locate your firmware image file you downloaded earlier.
2. By selecting **Keep settings** (2), all existing gateway settings and configuration will be left intact. This includes your list of measurement devices, any specific network arrangements, password settings, etc.
3. Finally, press the [Flash image] button (3). The gateway device will now download the new firmware image to its temporary location.

Flash operations

Actions Configuration

Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup:

Reset to defaults:

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: No file chosen

Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an OpenWrt compatible firmware image).

2 ☒ Keep settings:

Image: 1 3

Powered by LuCI 0.12 Branch (0.12+git-16.011.54267-f402ed2) OpenWrt Barrier Breaker 14.07

[Home](#) | [Administration](#)

Step 5 - Verify integrity and flash image

The gateway has now downloaded the new firmware image and will present you with this screen.

Flash Firmware - Verify

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity. Click "Proceed" below to start the flash procedure.

- Checksum: 75733408ed998405c2fec3a01134bac5
- Size: 6.19 MB
- Configuration files will be kept.

Powered by LuCI 0.12 Branch (0.12+git-16.011.54267-f402ed2) OpenWrt Barrier Breaker 14.07

[Home](#) | [Administration](#)

Confirm integrity

Before you proceed, please use the *md5sums* file you downloaded earlier to compare with the checksum presented.

Flash the new image

If the checksum matches, press the *[Proceed]* button and the gateway will install the new firmware image.

Step 6 - Wait for reboot

The installation process takes up to 4-5 minutes, so be patient. If you chose to keep your existing settings, in step 4, the gateway should reboot and become available again at the same URL as before.

You should see all the LEDs, except power, turn off and then start turning on and off again as it goes through the boot process.

Note

Please, do not power cycle the device. If you do so, you will need to do a manual recovery that cannot be done in the field.

12. Troubleshooting

The primary mission of the EG is to get your live energy data collected and sent to eTactica, so the home page of the administration console is your primary diagnostic console. If you want to check that everything is working properly, or to investigate why something isn't, the home page is the best place to start. You can always get to this page by clicking on the "eTactica" logo in the top banner.

The diagnostics run continuously, covering three main tests:

- **Devices**, that tells you whether your configured devices are connected and responding properly
- **eTactica Connection**, that tells you whether you are properly connected to the central eTactica servers
- **Time Synchronization**, that tells you if you have access to an NTP server and therefore provided with time synchronization

Devices

If you have not yet configured any devices, this test provides direct links to configure your devices. See chapter 4, [Device Configuration](#).

If all configured devices are responding correctly, this will be a green success mark.

If a device has been configured, but it is failing, this test will show a red failing mark and list the Modbus address that is failing.

If devices are responding correctly, but not providing the values you expected, you should use the [Channel Monitor](#) page to look at the live values. If a device is not mounted correctly, or not connected to the electrical panel correctly, it might be responding but generating invalid data.

Troubleshooting Modbus

All addresses fail to respond

Possible causes and fixes:

- Modbus cable has shorts or loose connections
- Modbus cable is not properly configured

Single address is failing

Possible causes and fixes:

- Modbus cable is not properly connected/configured for that specific device. Please note that manufacturers use different convention of labeling the RS485 data pins (A and B) so if you are using a non eTactica device you can try to switch the A and B wires
- Configured Modbus address is incorrect
- Modbus device has incorrect baud rate or parity settings

- Modbus device is not supported. Third party devices need plugins and your device may not be supported.

Multiple addresses fail to respond

Normally you should treat this as many single failures, but this can also be caused by the wiring not being properly connected beyond a certain point on the cable.

eTactica Connection

At the top level, we check whether the messaging bridge connection is active or not. If it's not active, further tests are done to try and help you work out what needs to be fixed.

Most of these tests depend on your Internet connection being properly configured and connected, see [Network Requirement](#) in chapter 1, [Introduction](#).

For Ethernet connection, first please check again that the network cable is plugged in at both ends (RJ45 LAN connector light should be on). For WiFi connection, please make sure that you have configured the gateway for WiFi properly. See chapter 8, [Network Settings](#).

If this is OK and still no connection, take a look at the tests below.

1) Testing DNSlookup of eTactica server

This is testing the configured DNS servers, whether names can be resolved. The server that is tested in the example below is the configured eTactica messaging server and will change if you switch security on for instance.

Config Devices
Channel Monitor
Start Security
eTactica Keys
Plugins
Network
Help

Last Update: eTactica Connection - Running...

Devices

Problems found:

- unit address: 41 (0x29) : has failed 750 times: Modbus protocol.
- unit address: 131 (0x83) : has failed 750 times: Modbus protocol.
- unit address: 150 (0x96) : has failed 751 times: Modbus protocol.

eTactica Connection

eTactica Connection down!

Testing DNS lookup of eTactica server: mq.dcc01.etactica.com

Check your network configuration
Test DNS manually

Testing remote TCP port access mq.dcc01.etactica.com:8883

Check your firewall settings allow access to mq.dcc01.etactica.com:8883

Testing message publishing

Check your security keys if security is enabled

Testing general web access (www.google.com)

Web access is required for software updates

Testing local message broker

Time Synchronization

Time not synchronized

Testing local NTP server

Testing DNS resolution

For further diagnosis press the link [\[Test DNS manually\]](#).

This will require you to login, using the root password you have configured earlier. If not, please see chapter 9, [Password Settings](#).

This screen appears, offering three different network diagnostic tools.

Diagnostics

Network Utilities

Install iputils-traceroute6 for IPv6 traceroute

Powered by LuCI 0.12 Branch (0.12+git-16.011.54267-f402ed2) OpenWrt Barrier Breaker 14.07

[Home](#) | [Administration](#)

To test DNS resolution, either press the [\[Nslookup\]](#) button, using the default name or enter any name that should exist, such as www.google.com or www.ibm.com.

If everything OK you will see this screen.

Diagnostics

Network Utilities

Install iputils-traceroute6 for IPv6 traceroute

```

Server: 127.0.0.1
Address 1: 127.0.0.1 localhost

Name: openwrt.org
Address 1: 78.24.191.177 openwrt.org
    
```

Powered by LuCI 0.12 Branch (0.12+git-16.011.54267-f402ed2) OpenWrt Barrier Breaker 14.07

[Home](#) | [Administration](#)

If this test fails (see picture below), speak to your network operator. They may ask you to run further tests with other tools on this page, i.e. *ping* and *traceroute*.

Note that this test can potentially also fail if eTactica services are having a major failure.

Diagnostics

Network Utilities

Install iputils-traceroute6 for IPv6 traceroute

```

Server: 127.0.0.1
Address 1: 127.0.0.1 localhost

nslookup: can't resolve 'openwrt.org': Name or service not known
    
```

Powered by LuCI 0.12 Branch (0.12+git-16.011.54267-f402ed2) OpenWrt Barrier Breaker 14.07

[Home](#) | [Administration](#)

2) Testing remote TCP port access

This test attempts to open an outbound TCP connection to the named server and port. As with the DNS test above, the specifics here will change depending on whether security is enabled or not and your particular account details. The reason is that we have multiple messaging servers located around the world. The port number is always 1883 for insecure systems and 8883 for secure systems.

If this test fails, it is probably due to network firewalls at your location that block access. Speak to your network operator. Please refer to [Network Requirement](#) in chapter 1, [Introduction](#).

Note that this test can also fail if eTactica services are having a problem with your assigned messaging server. This should not happen at installation time however, but it's important to note.

3) Testing general web access

This is an optional test, so if this fails it's not necessarily a major problem. It could indicate that things are not operating as you expect, but general web access is used for doing software updates and automatically turning on security.

4) Testing local message broker

This should never fail, but is included for completeness. The eTactica gateway runs a message broker for sharing information between applications running on the gateway itself. This broker is also what bridges data out to the central eTactica servers.

This test should only fail if you have manually edited the settings for the "*mosquitto*" service and inadvertently inserted some errors, or disabled the service completely.

Time Synchronization

To ensure reliable data logging, we require access to a NTP server for proper time synchronization. Measurement samples are time-stamped on the gateway itself, as we support network interruptions for up to several hours by buffering messages as needed. NTP is used for this.

This can take several minutes to synchronize, especially if it was running before the network connections were fixed. It can be faster to restart the gateway, but it's normally simpler to just finish testing other parts of the installation first.

So try at least one or both:

- Check if network connections are ok
- Restart and wait 5 minutes

If time is still not synchronizing after verifying the above, talk to your network operator about firewalls on UDP port 123, and review the [Network Requirement](#) in chapter 1, [Introduction](#).

You need to make sure that at least one of the NTP servers listed is valid and reachable from your gateway. You can manually edit the list of NTP servers available.

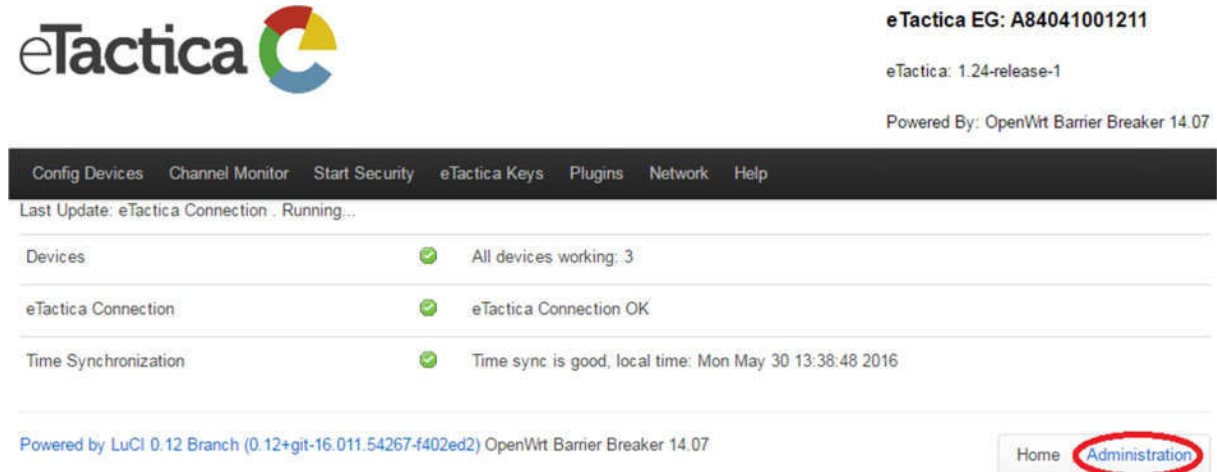
Please follow the steps below, to do that.

Step 1 - Connect to the Gateway

You need to be successfully connected to your gateway device. If not, see chapter 2, [Connecting to Gateway](#).

Step 2 - Go to Administration page

From the home page of the administration web console of your device, click on the [Administration](#) link.



The screenshot shows the eTactica Gateway Administration page. At the top, the eTactica logo is on the left, and the device ID "eTactica EG: A84041001211" is on the right. Below the device ID, it says "eTactica: 1.24-release-1" and "Powered By: OpenWrt Barrier Breaker 14.07". A navigation bar at the top contains links: Config Devices, Channel Monitor, Start Security, eTactica Keys, Plugins, Network, and Help. Below this bar, a status section shows "Last Update: eTactica Connection . Running...". A table below this shows the status of various components:

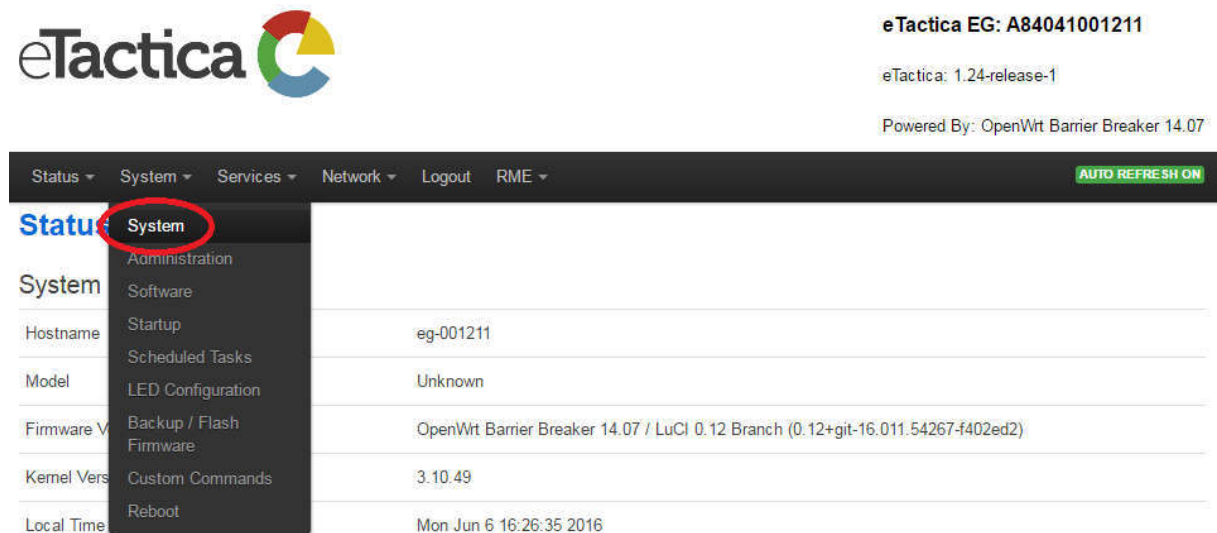
Devices	✓	All devices working: 3
eTactica Connection	✓	eTactica Connection OK
Time Synchronization	✓	Time sync is good, local time: Mon May 30 13:38:48 2016

 At the bottom, it says "Powered by LuCI 0.12 Branch (0.12+git-16.011.54267-f402ed2) OpenWrt Barrier Breaker 14.07". On the right, there are two buttons: "Home" and "Administration", with "Administration" circled in red.

This will require you to login, using the root password you have configured earlier. If not, please see chapter 9, [Password Settings](#).

Step 3 - Go to System setup

From the top menu, choose [System->System](#).



The screenshot shows the eTactica Gateway System setup page. At the top, the eTactica logo is on the left, and the device ID "eTactica EG: A84041001211" is on the right. Below the device ID, it says "eTactica: 1.24-release-1" and "Powered By: OpenWrt Barrier Breaker 14.07". A navigation bar at the top contains links: Status, System, Services, Network, Logout, and RME. The "System" link is circled in red. Below the navigation bar, a dropdown menu is open, showing options: Administration, Software, Startup, Scheduled Tasks, LED Configuration, Backup / Flash Firmware, Custom Commands, and Reboot. The "System" option is selected. The main content area shows a table with system information:

Hostname	eg-001211
Model	Unknown
Firmware Version	OpenWrt Barrier Breaker 14.07 / LuCI 0.12 Branch (0.12+git-16.011.54267-f402ed2)
Kernel Version	3.10.49
Local Time	Mon Jun 6 16:26:35 2016

 At the bottom right, there is a green button labeled "AUTO REFRESH ON".

Step 4 - Edit NTP Server list

You will see a screen like this, and you can add/remove/edit the list of NTP servers as you wish.

System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

General Settings
Logging
Language and Style

Local Time Mon Jun 6 16:28:44 2016

Hostname

Timezone

Time Synchronization

Enable NTP client ☒

Provide NTP server ☒

NTP server candidates

0.openwrt.pool.ntp.org	<input type="button" value="x"/>
1.openwrt.pool.ntp.org	<input type="button" value="x"/>
2.openwrt.pool.ntp.org	<input type="button" value="x"/>
3.openwrt.pool.ntp.org	<input type="button" value="x"/>
ntp.etactica.com	<input type="button" value="x"/>
79.171.98.82	<input type="button" value="+"/>

Important to note

Do NOT remove the two check marks on "*Enable NTP client*" and "*Provide NTP server*". They are used for the synchronization itself and testing the time synchronization.

Step 5 - Save settings

When done, press the *[Save & Apply]* button to keep and apply your new settings.

eTactica web: Loading hardware fails

When you are configuring your hardware setup on the eTactica web, one of the steps is to connect to the gateway to download the hardware profile (information about all connected devices). If some of the devices are missing from the profile, make sure that they have been configured on the gateway and that the gateway is communicating with that device (green tick in the devices line and live readings on the *Channel Monitor* page).