eTactica

User Manual

V4.1
15.06.2016

WE MAKE ENERGY
MONITORING SIMPLE

eTactica Gateway EG-100 and EG-200

Contents

This is the user manual for the eTactica Gateways, valid for the products marked as EG-100 and EG-200 and firmware release 1.24. In this document, you will find information about installing and configuring your eTactica Gateway device.

The intended reader is a person with electrical background and basic knowledge in TCP/IP networking.

1. Introduction

The eTactica Gateway (EG) is a part of the eTactica line of products, including the eTactica Power Meter (EM), the eTactica Current Bar (EB) and the eTactica Current Meter (ES).

The EG collects and analyses your energy data, measured by the EM, EB and ES. The EG reads live data from connected devices via its device bus, using Modbus/RTU protocol on RS485 network (default settings: 19200, 8, E, 1). This allows multiple eTactica devices to be connected, as well as other 3rd party measurement devices that support Modbus/RTU.

The EG is a 32 bit Linux platform with Ethernet and WiFi connectivity and acts as a secure gateway between the electrical panel and the Internet. Measurement data is securely pushed through any Internet gateway to the eTactica datastore, where the data is securely accessible from any Internet browser. No need to open ports, just plug and play. Easy. Secure.

The EG-100 includes a 12W power supply which provides 12VDC@1A, to supply the EG itself as well as all the eTactica devices connected to the device bus.

The EG-200 uses an external power supply 12VDC, minimum 1,1A to power the EG and connected devices.

Main characteristics

- Supports up to 32 eTactica devices or 3rd party Modbus devices
- 5 LEDs that indicate the status of the device
- Built in webserver for device configuration and live measurements
- Wired and wireless LAN connections
- Modbus/RTU via RS485
- Standard DIN rail mounting (EG-100 6 unit, EG-200 2 unit)

Network Requirements

The Gateway has some network requirements for proper operation. The notes below apply to the normal, centrally hosted eTactica system.

DNS access

We expect to have DNS access available. How you configure your network and the EG's network interfaces (WiFi and LAN) is up to you, but we expect DNS access to be available.

Port access

For secure messaging

Outbound access to TCP port 8883 is required.
(Note, for secure messaging, outbound http(s) is required, for the secure signup process)

For insecure messaging

Outbound TCP port 1883 is required.

NTP access

The eTactica system expects to have reliable timestamps on the data sent from the EG. If there is an outbound access on UDP port 123, this will happen automatically, but you can also edit the list of NTP servers used and provide one in your own network if you prefer. See *Time Synchronization* in chapter 12, *Troubleshooting*.

HTTP and HTTPS access

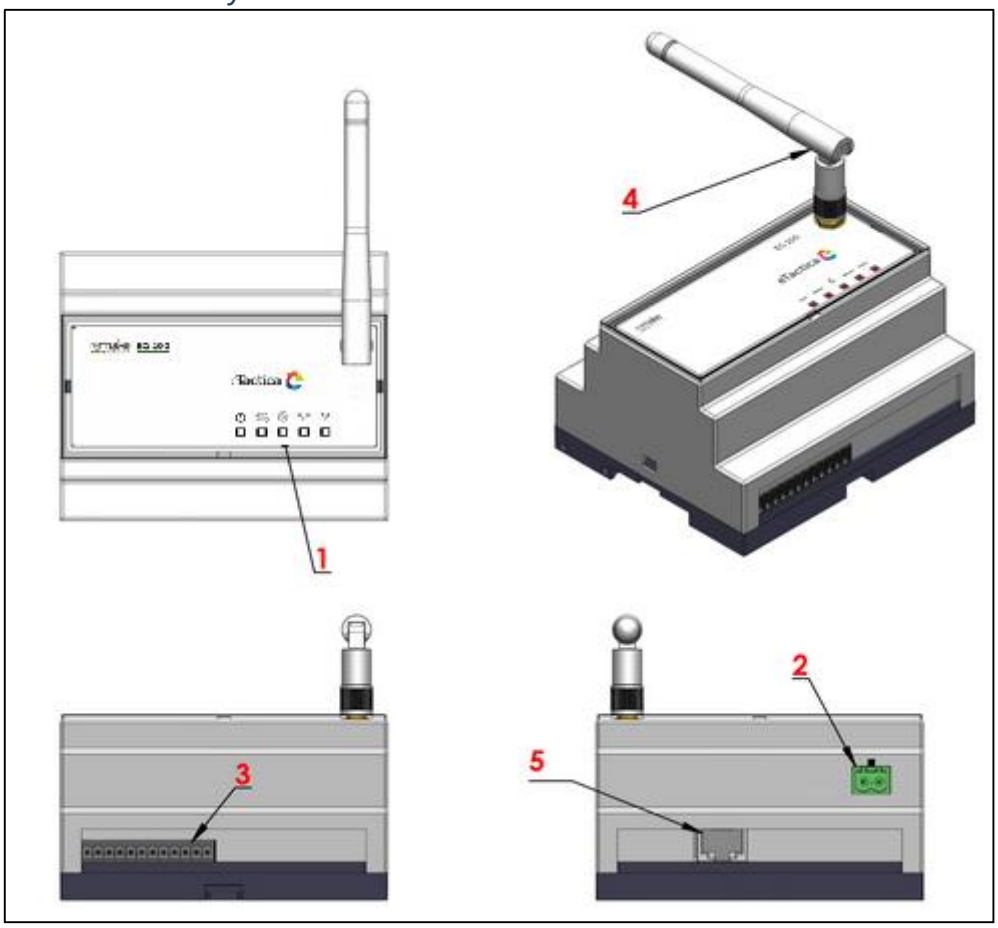
This is required for secure messaging, but optional for insecure messaging.

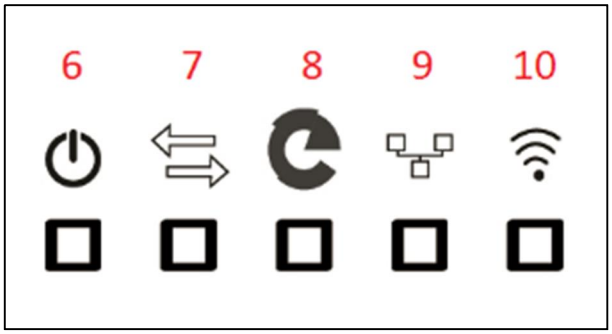
General web access on ports 80 and 443 are used for software updates and signing up for secure messaging. This is not required but it certainly makes things easier for everybody, and we highly recommend it.

Technical Specifications

EG-100	
OS	32-bit Linux
Network communication	Ethernet TCP/IP (10/100Mbit) WiFi (802.11b/g)
Device bus protocol	Modbus/RTU 19200, 8, E, 1 (default settings)
Device bus interface	RS485, 2-wire, shielded twisted pair, Multi stranded AWG22, Terminated
Device bus power source	12VDC@700mA
Max devices	32
Max cable length	60 m (Max cable length for the entire RS485 network, from the Gateway to the last slave-device)
Power Supply	90-260VAC@50/60 Hz
Power consumption	< 16W
Fastenings	DIN (EN 50022) 6 unit
Weight	180g
General Data	
Storage Temperature	-20° C to +70° C
Operating Temperature	0° C to +50° C
Safety	IEC/EN 60950-1 UL 60950-1 CSA C22.2 No. 60950-1-03, GB4943
EMC	EN 55022:2006 + A1:2007 EN 55024:1998 + A1:2001 +A2:2003 (class B) EN 61000-3-2:2006 + A1:2009+A2:2009 EN 61000-3-3:2008 FCC: Part 15 Subpart B, Subpart C EN 62311:2008 EN 300 328 V1.7.1:2006-05 EN 301 489-17 V2.1.1:2009-05

Connection Layout





1. Status LEDs
   (6 - Power, 7 - Modbus, 8 - eTactica online, 9 Ethernet link, 10 - WiFi)
2. Power input 90-260VAC@50/60 Hz
3. Device-bus connector
4. External Wifi antenna
5. RJ45 LAN connector (Ethernet)

Device bus connector

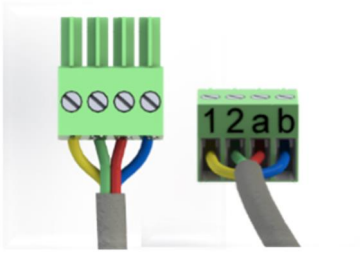
The device-bus connection layout, the communication bus that interconnects all eTactica devices.

[1] DC Power, 12VDC@700mA

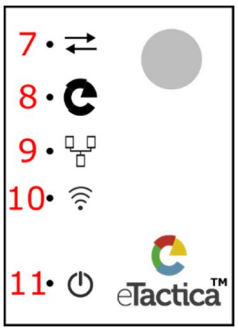
[2] GND

[a] RS485 A

[b] RS485 B



EG-200	
OS	32-bit Linux
Network communication	Ethernet TCP/IP (10/100Mbit) WiFi (802.11b/g/n)
Device bus protocol	Modbus/RTU 19200, 8, E, 1 (default settings)
Device bus interface	RS485, 2-wire, shielded twisted pair, Multi stranded AWG22, Terminated
Device bus power source	12VDC@700mA
Max devices	32
Max cable length	60 m (Max cable length for the entire RS485 network, from the Gateway to the last slave-device)
Power Supply	12VDC 1,1A
Power consumption	< 13W
Fastenings	DIN (EN 50022) 2 unit
Weight	87g
General Data	
External memory	Micro SD-card slot
Storage Temperature	-20° C to +70° C
Operating Temperature	-20° C to +50° C
Safety	IEC/EN 60950-1 UL 60950-1 CSA C22.2 No. 60950-1-03, GB4943
EMC	EN 55022:2006 + A1:2007 EN 55024:1998 + A1:2001 +A2:2003 (class B) EN 61000-3-2:2006 + A1:2009+A2:2009 EN 61000-3-3:2008 FCC: Part 15 Subpart B, Subpart C EN 62311:2008 EN 300 328 V1.7.1:2006-05 EN 301 489-17 V2.1.1:2009-05



1. RJ45 LAN connector (Ethernet)
2. Power input 12VDC
3. Device-bus connector
4. Status LEDs
   (7 - Modbus, 8 - eTactica online, 9 - Ethernet link, 10 WiFi, 11 - Power)
5. External Wifi antenna
6. Reset button (accessed through an opening on the enclosure)

Emission: Product family standard, Measurement, control and laboratory equipment
EN 61326-1:2013
EN 301-489-1-9-2:2011
Product standards:
EN 61000-3-2:2006 with Amd.1:2009 and Amd.2:2009, Harmonic current
EN 61000-3-3:2008, Flicker
Immunity: Product family standard Measurement, control and laboratory equipment
EN 61326-1:2013
EN 301-489-1-9-2:2011

2. Connecting to Gateway

In this chapter, you find a description of how to connect to the eTactica Gateway (EG) and how to do a simple setup, where a Wizard will guide you through all the steps.

Most commonly, this is done using the WiFi interface. By default, every Gateway comes with an open WiFi interface (wireless hotspot) for initial configuration.
The SSID for the wireless hotspot is always "eTactica eg_xxxxxx", where xxxxxx is a unique number for each Gateway.

Alternatively, you connect by using your Ethernet connection.

Connection via WiFi

Step 1 - Connect to WiFi hotspot

Use the normal operating system method for connecting to a new wireless hotspot.
On Windows it looks something like this:

Step 2 - Visit the administration web console

If you have connected via WiFi, the URL to the administration console is always http://192.168.49.1. Type this IP address into your web-browser to get access.

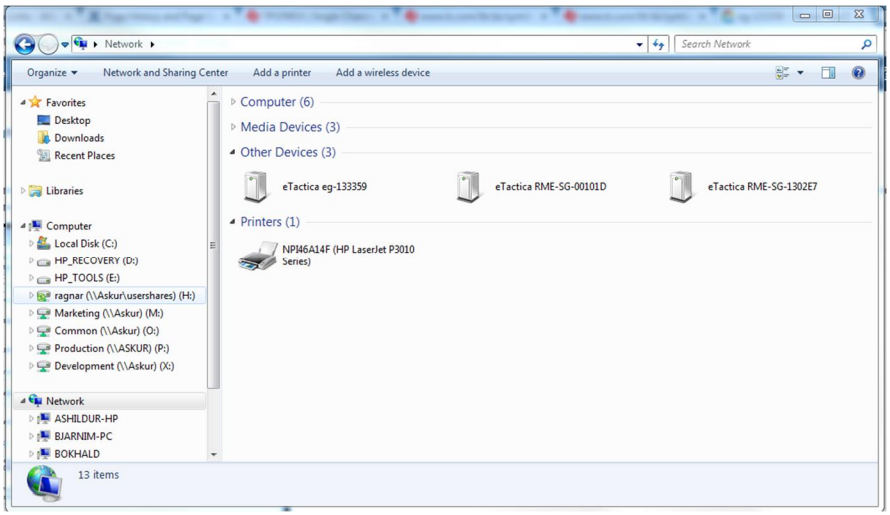
Connection via Ethernet

In our recommendation, the EG is connected to an existing managed IP network and receives an IP address via DHCP. If your computer/laptop is connected to the same network, you can also access the EG via this interface.

Windows

If the device has been connected to your existing Ethernet network, as we recommend, you can find the device in *Windows Explorer -> Network -> Other devices*, as shown below. Simply double click the name of the device you wish to connect to and you will automatically be directed to the administration web console page of the gateway, via your web-browser.

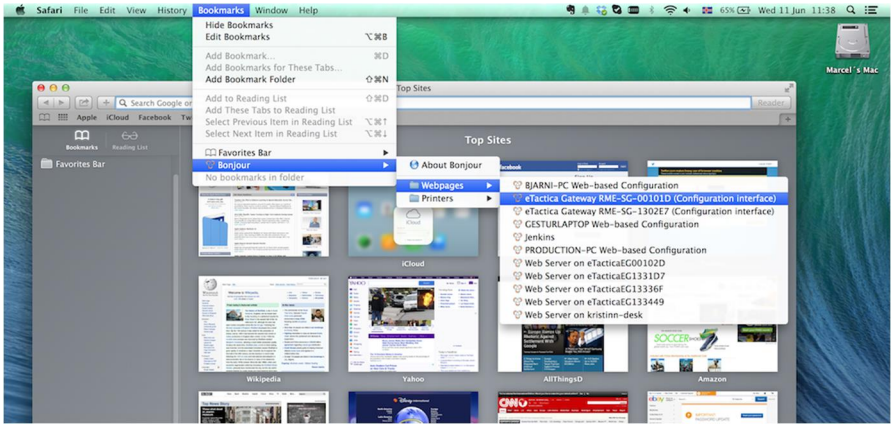
The name of the device shown here, will also match *"eTactica eg_xxxxxx",* where -xxxxxx is a unique number for each gateway device.



OSX

On OSX, using the Safari Browser, you can visit *Bookmarks -> Bonjour Bookmarks* and choose the entry for the matching device.

Note, you may need to enable browsing Bonjour Bookmarks first, see information at https://www.apple.com/support/bonjour/.



Linux

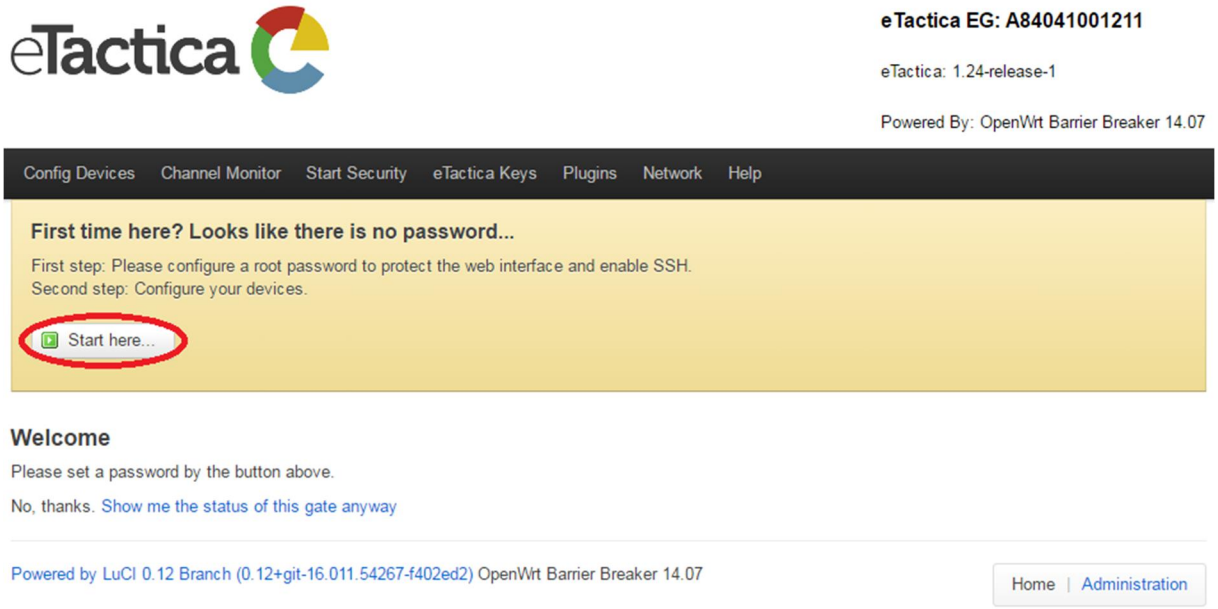
On Linux there are different tools available for this kind of discovery, i.e. *Avahi-discover*. You can use these tools to find your device and to the IP address (URL) it got assigned.

Once you have the IP address, you can enter it in your web-browser to access the admin console page of the gateway.

3. Simple Configuration Wizard

The following chapter describes the steps during configuration of your eTactica gateway, using the simple wizard and then setting up secure messaging.

Step 1 - Starting Wizard



The wizard process helps you configure the following items:

- The root password for your device
- Networking and WiFi passwords
- Configuring Modbus device list

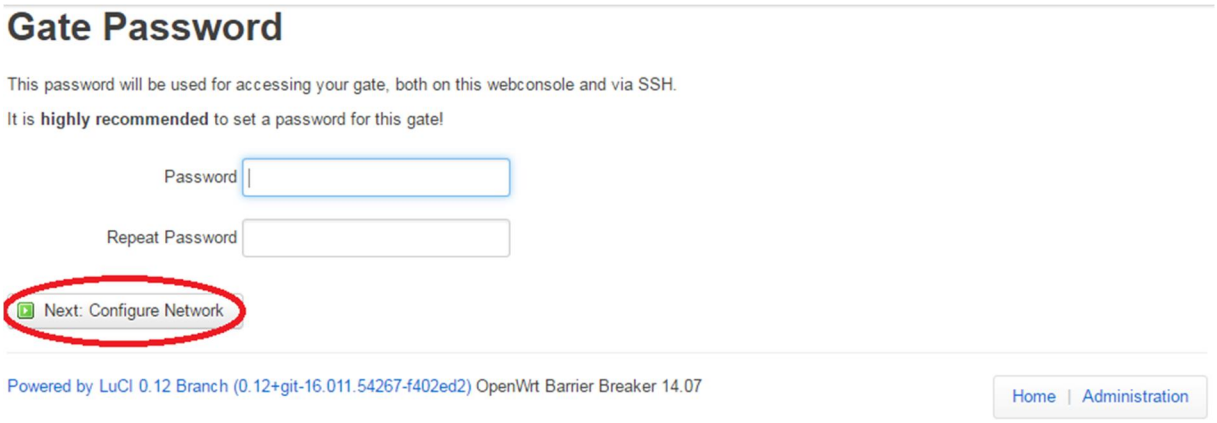
If you want to configure these items manually, you may simply proceed as documented in the rest of this manual. However, the vast majority of installations should be able to use the wizard.

Simply press the *[Start here]* button.

Step 2 - Setting Root Password

The root password is used to log in to the web administration console for modifying any important settings. The root password also provides SSH access to the device. As always, you should use a good password here.

When done, press the *[Next: Configure Network]* button for next step.

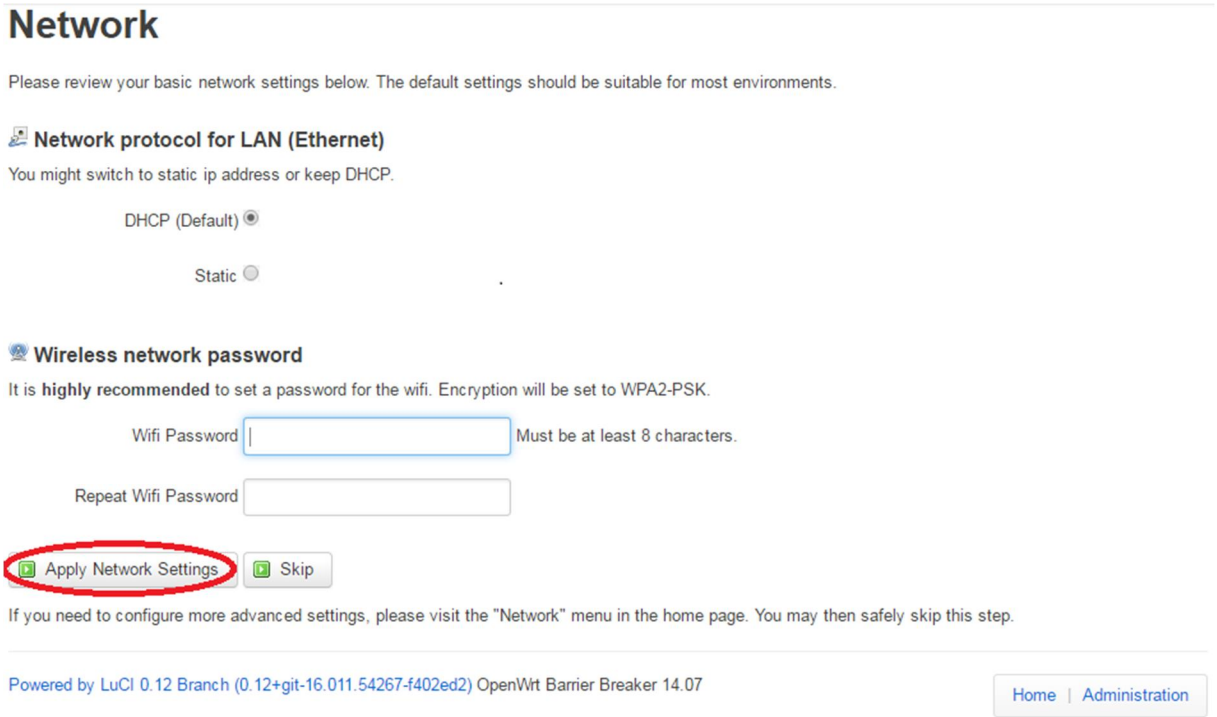


Step 3 - Configure Network

The recommended networking setup is to connect the Ethernet port to a regular DHCP network, as this requires the least configuration. Simply leave the mark on DHCP and move down to the WiFi password.

In either case, you should also enter a WiFi password here. This will use WPA2/WPA2-PSK, the best available wireless security at this time. This should be perfectly reasonable for most use cases.

When done, press the *[Apply Network Settings]* button to continue.

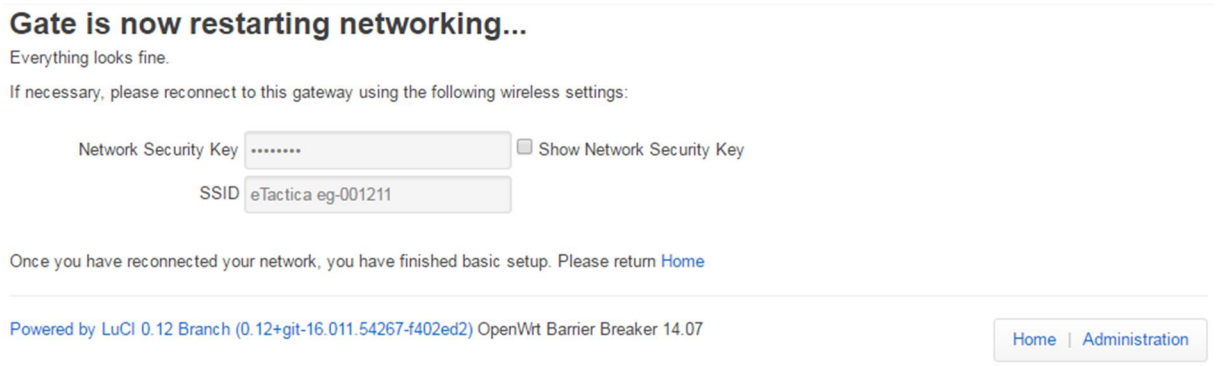


Note
If you wish to completely disable WiFi, that is of course possible, please see *Enable/Disable WiFi* in chapter 8, *Network Settings*, for instructions. Until you have reconnected with any updated networking settings, it's simply too unsafe to turn off the WiFi this early in the configuration process.

Step 4 - Reconnect

Once you have entered your desired networking setup and WiFi password, the device networking will restart.

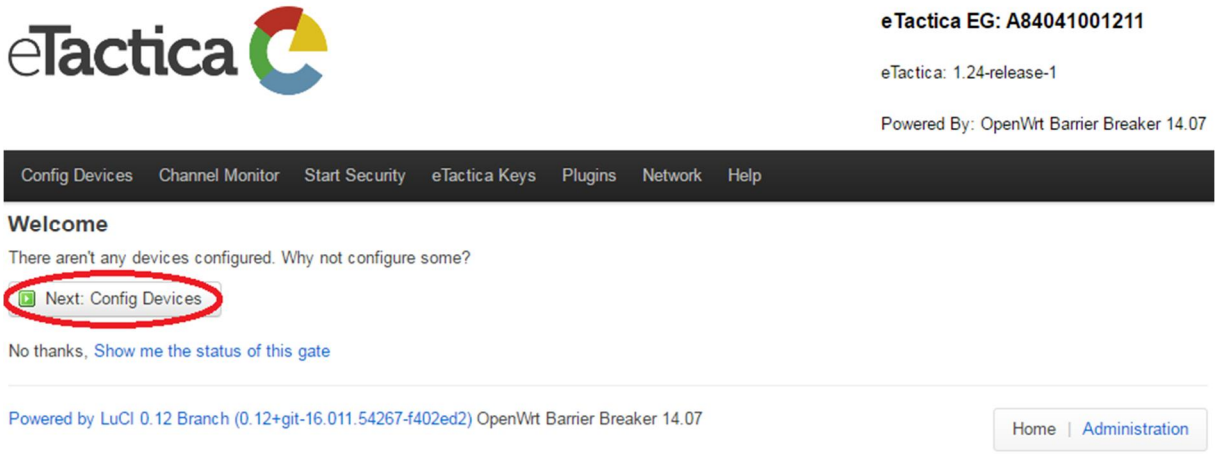
Depending on how you had originally connected to the device, you will most likely have to reconnect. The WiFi SSID will be shown, to help you reconnect via WiFi. This may take a minute or two to restart, so please be patient.



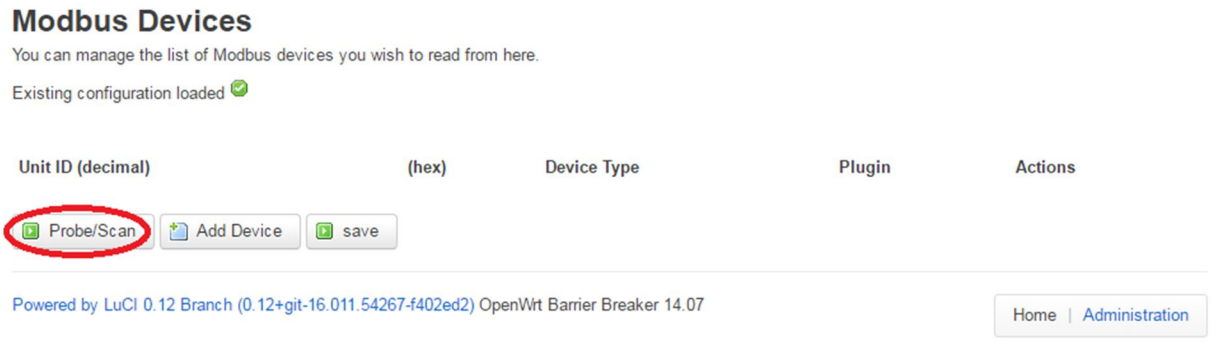
Once you have reconnected to the device, you should see a new home page.

Step 5 - Device Configuration

Now that your basic networking and security is setup, it's time to proceed to configure your measurement devices.



Please press the *[Next: Config Devices]* button to continue and you will see the following screen.



Step 6 - Scan for Devices

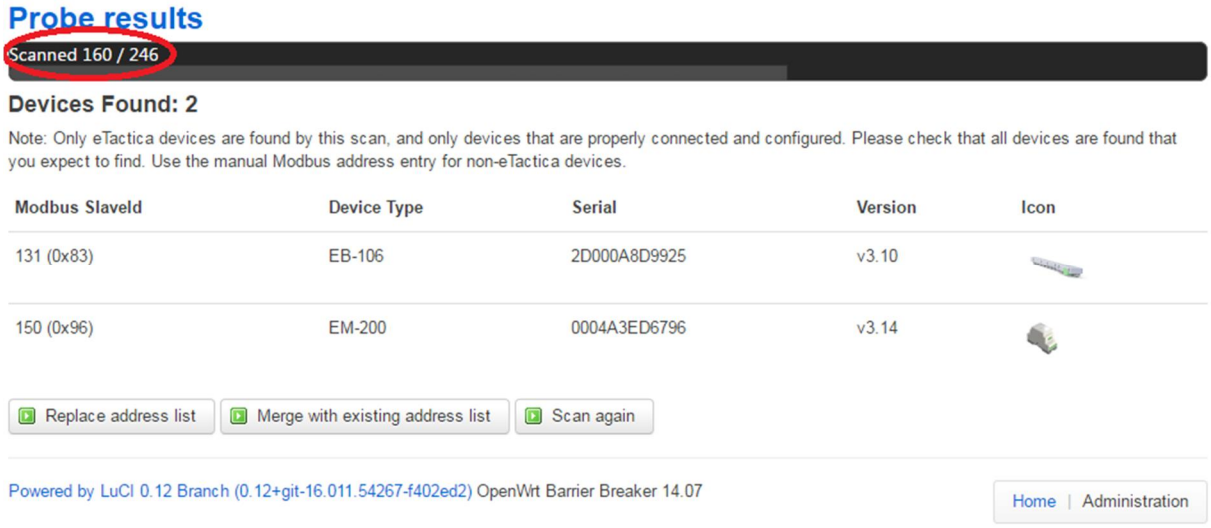
If you have many devices and they are all eTactica devices, you can attempt to scan for all connected devices. You should always review scan results to be sure they match the devices you expected to be found.

If you choose to scan, simply press the *[Probe/Scan]* button.

The process will take about 30 seconds, as it scans all possible Modbus addresses looking for eTactica devices.

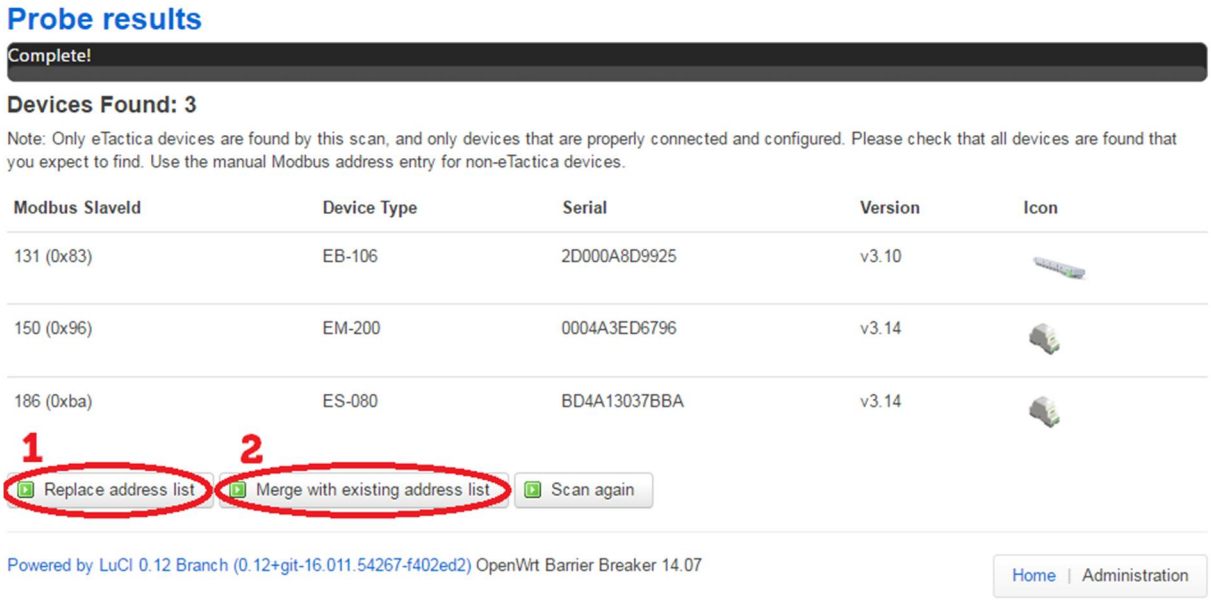
Note
This only works for eTactica devices and only for devices that are properly connected.

Here is a screenshot of the process about half complete.



Note that it shows the Modbus address (slave ID) of the detected device, its device type, the unique serial string and an icon for each device found to help you match against what you expected.

When the scan has finished you should see all connected eTactica devices.



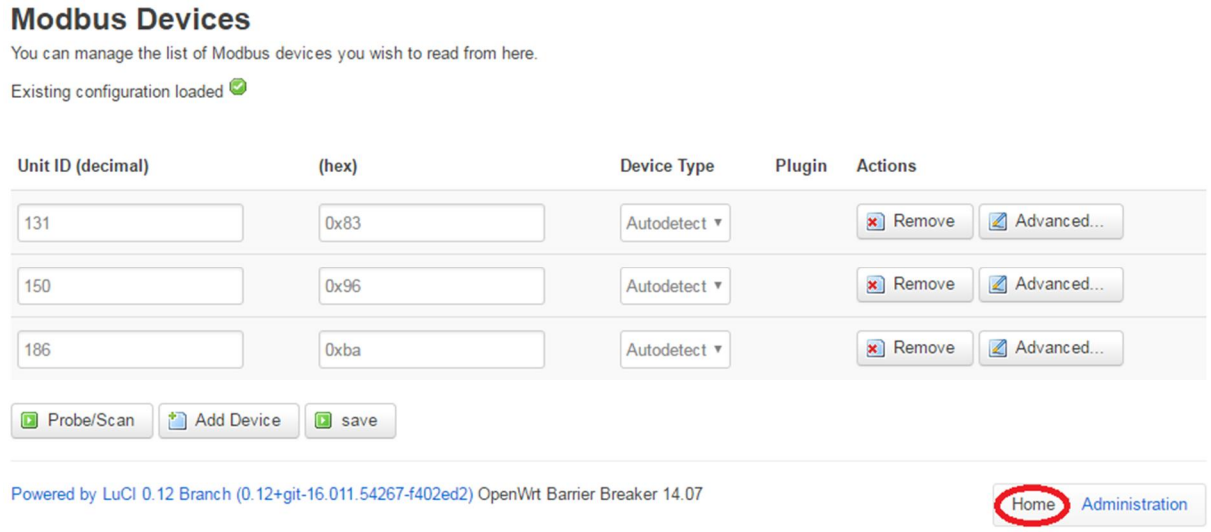
Step 7 - Saving Configuration

If you only care about the devices that were successfully scanned, you can press the *[Replace address list]* (1) button to replace any existing list with your scan results.

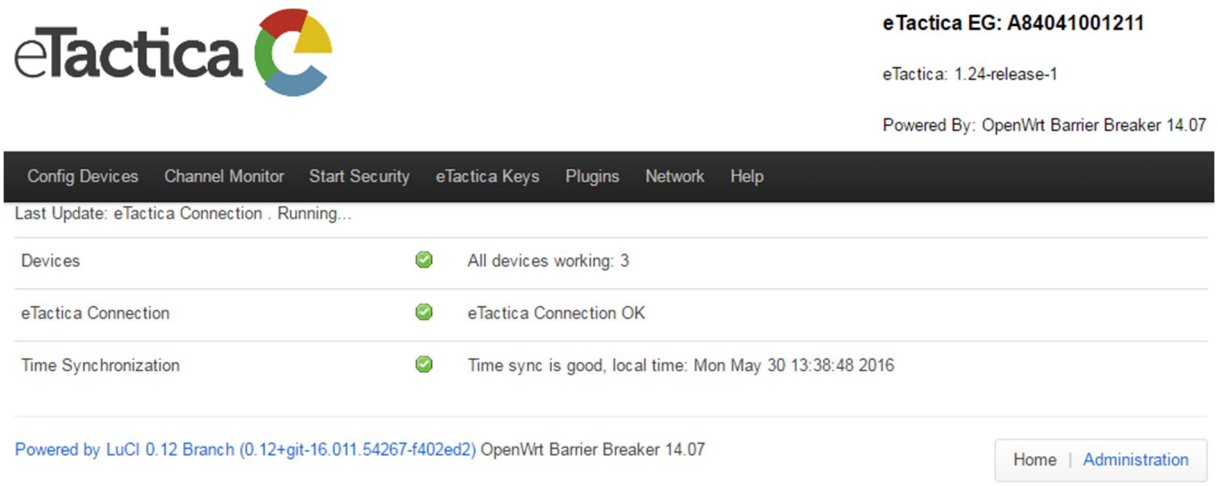
If you had third party devices already in your list, or if you have eTactica devices you plan on connecting later that you had manually entered in the previous step, then press the *[Merge with existing address list]* button (2) to merge a combined device list. See chapter 4 *Device Configuration* for further information about configuration.

If a device is not showing up in the scan list, please recheck its wiring and power supply, and feel free to scan again.

When choosing either *[Replace address list]* or *[Merge with existing address list]*, the configuration will be saved and applied.



For final diagnostics of your configuration go back to the home page of the administration web console by clicking on the *[Home]* button or the eTactica logo.



Hopefully you will see three green ticks that mean that everything is working correctly:

- Devices - All devices from your configuration list are connected and recognized
- eTactica Connection - Your network settings are correct and you are successfully connected to the eTactica web application
- Time Synchronization - You have access to a NTP server that will secure correct timestamp of your measurement data

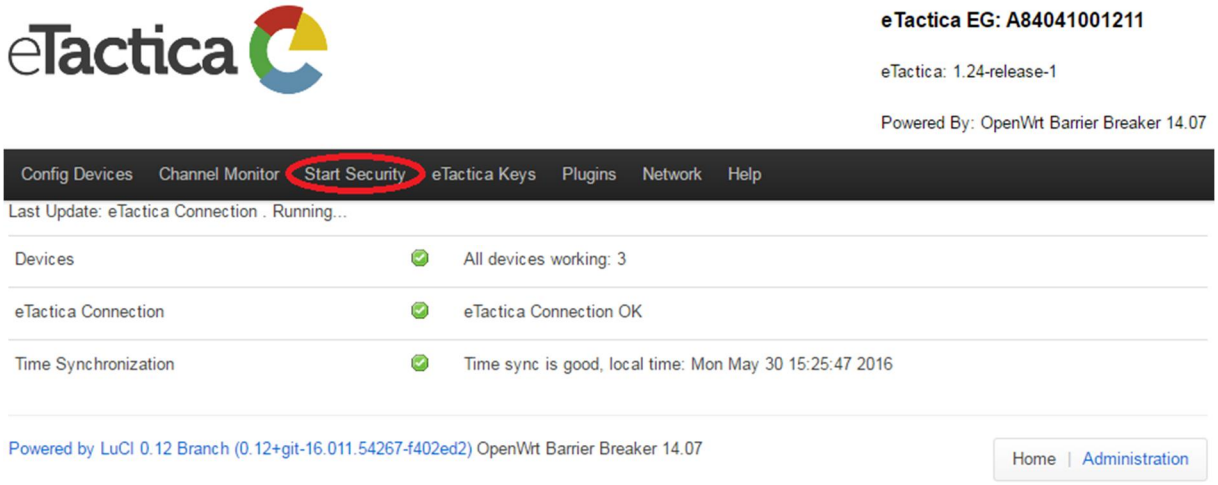
If you see red ticks on any of the above, please refer to chapter 12, *Troubleshooting*, to look for a solution to your problem.

Step 8 - Enter secure settings page

Here you find information to enable secure connection. This makes all communication between your eTactica gateway and the eTactica host securely encrypted.

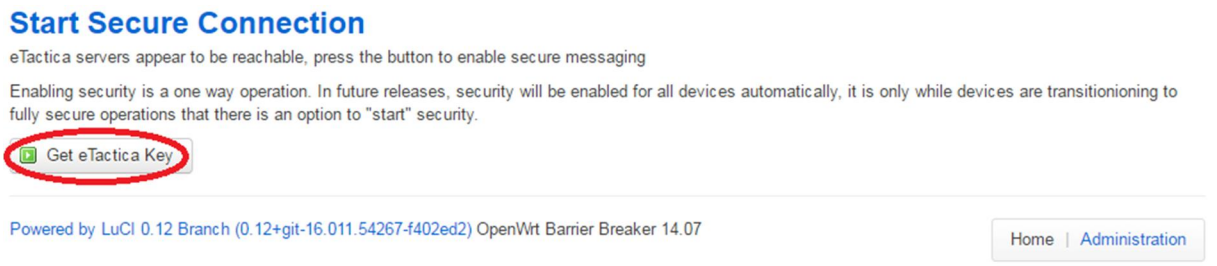
The encryption is not enabled by default, but can and SHOULD be enabled as shown in the following steps.

From the home page of the administration web console on your device, select *Start Security* from the top menu.

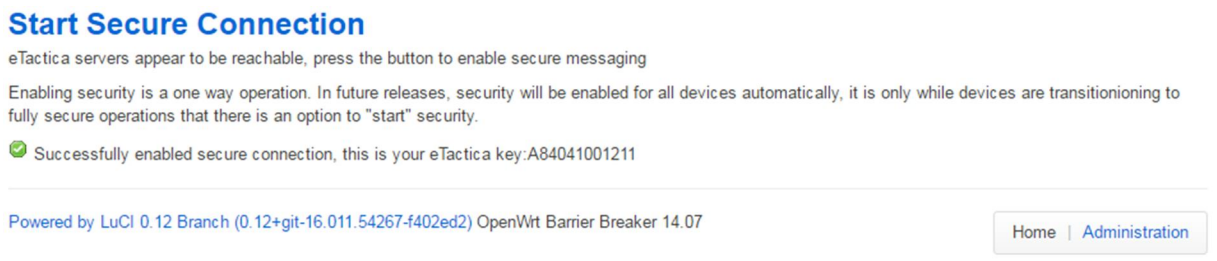


Step 9 - Start secure connection

Press the *[Get eTactica Key]* button.



Wait a few seconds while the key is retrieved.
If everything is working fine, you should see this.



Your gateway is now securely communicating with the eTactica host.

Step 10 - Completed

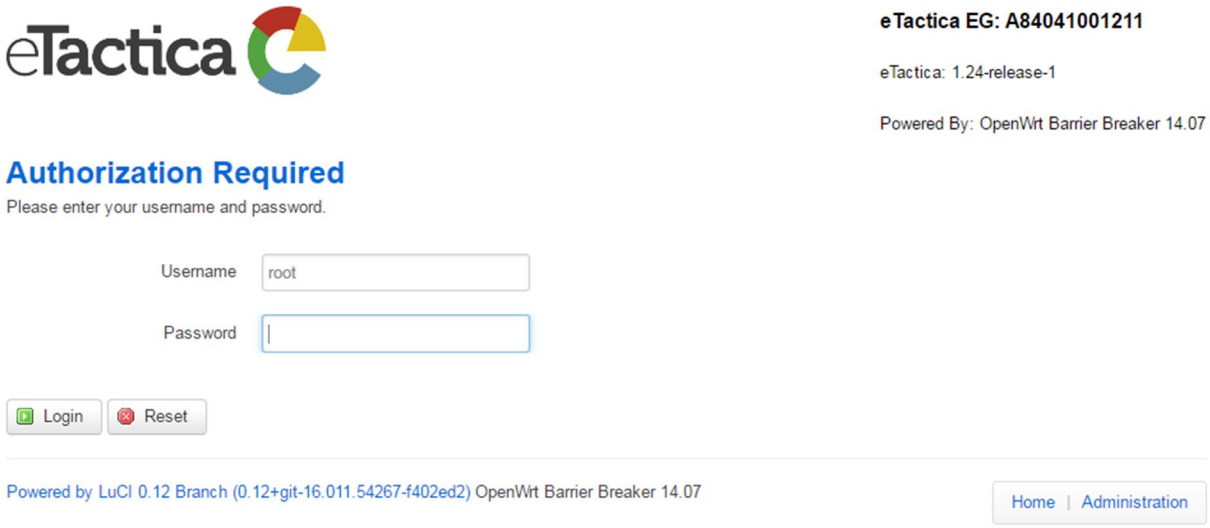
This completes your configuration, using the simple Wizard step by step guide.

Further Configuration

If you need to do some further configuration see the following chapters.

Login required

To edit most settings, you will need to be logged in and you will be presented with a screen like below.



The username is ALWAYS root and the password is the root password chosen by you during initial configuration.

4. Device Configuration

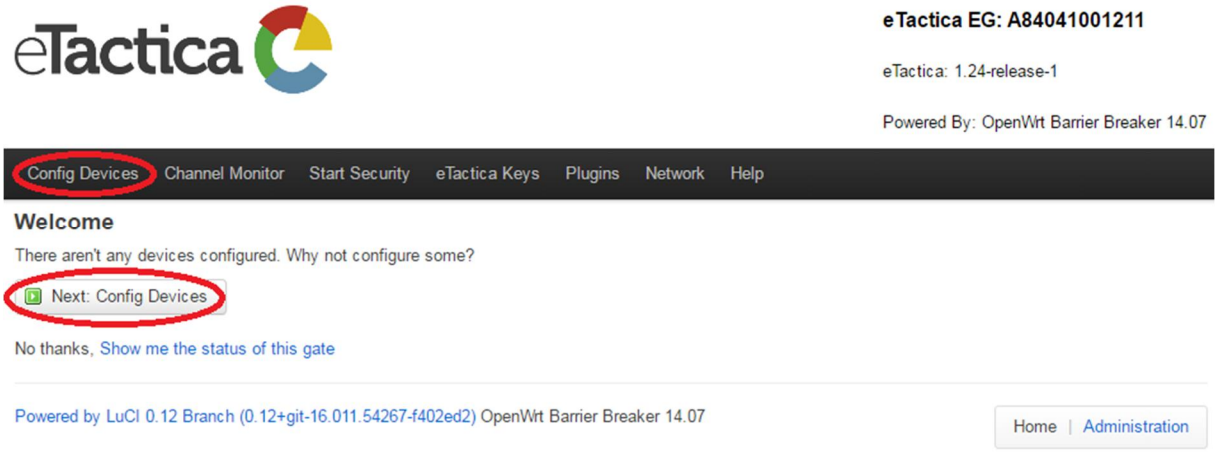
The following chapter describes how to add a Modbus device to the list of connected devices. This is done by entering the Modbus address of your device/s to the list, either manually or automatically by scanning.

Pre-requirements

You are successfully connected to your eTactica gateway, either via WiFi or Ethernet. If not, please see chapter 2 *Connecting to Gateway*.

Step 1 - Choose

From the menu at the home page for the administration web console, choose *Config Devices*.

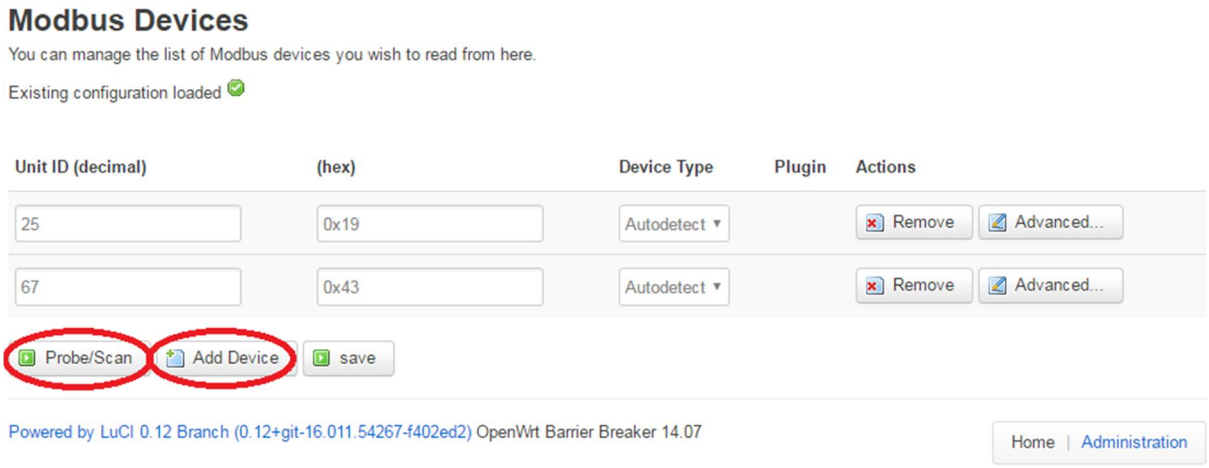


Note

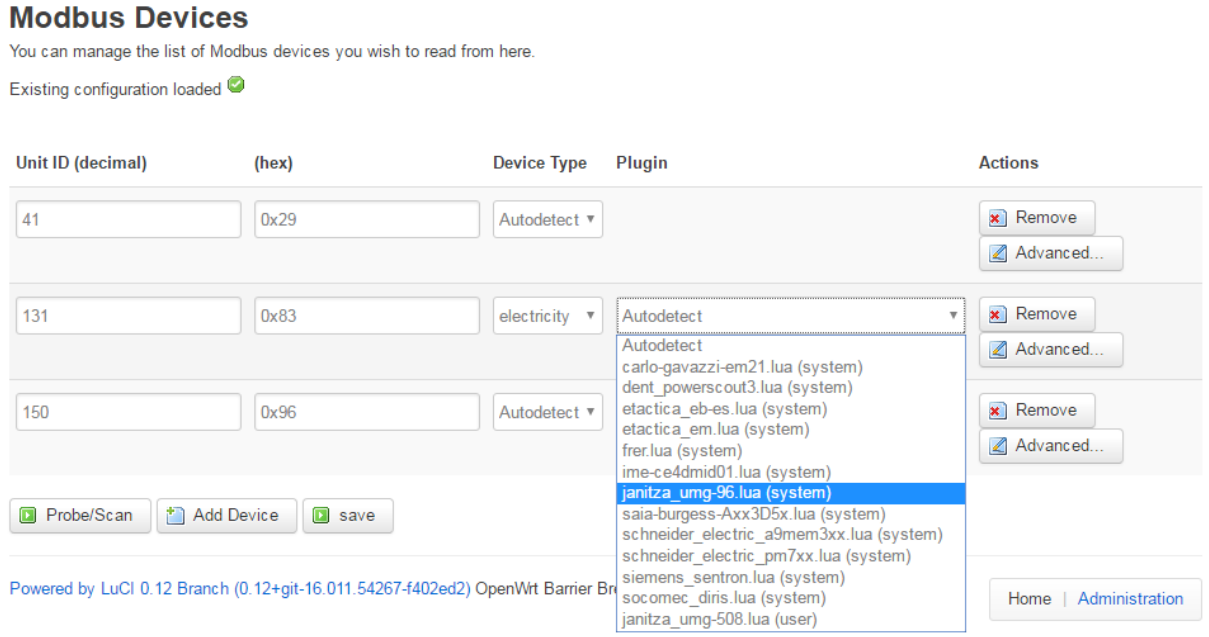
This will require you to login, using the root password you have configured earlier. If not, please see chapter 9, *Password Settings*.

Step 2a - Manually enter the device address

If you only have one or two devices, you can simply enter the Modbus slave addresses manually. (See A note on Modbus addresses below). Press the *[Add Device]* button as many times as you have devices to add. For each device fill in the Unit ID in either decimal or hex, the other will then be filled in automatically.



When Autodetect is chosen under Device Type the gateway should choose the right plugin for the device. If, for some reasons, Autodetect does not work, you can choose the plugin manually, choose the right category under device type and then choose the right plugin in the Plugin drop down list. By pressing the *[Advanced]* button you will find further configuration possibilities if they are available for that plugin. There will be a red frame around the *[Advanced]* button if the default value have been changed. There is more information about plugins in chapter 6, *Device Plugins.*



Press the *[save]* button to store settings.

Step 2b - Automatically scan for devices

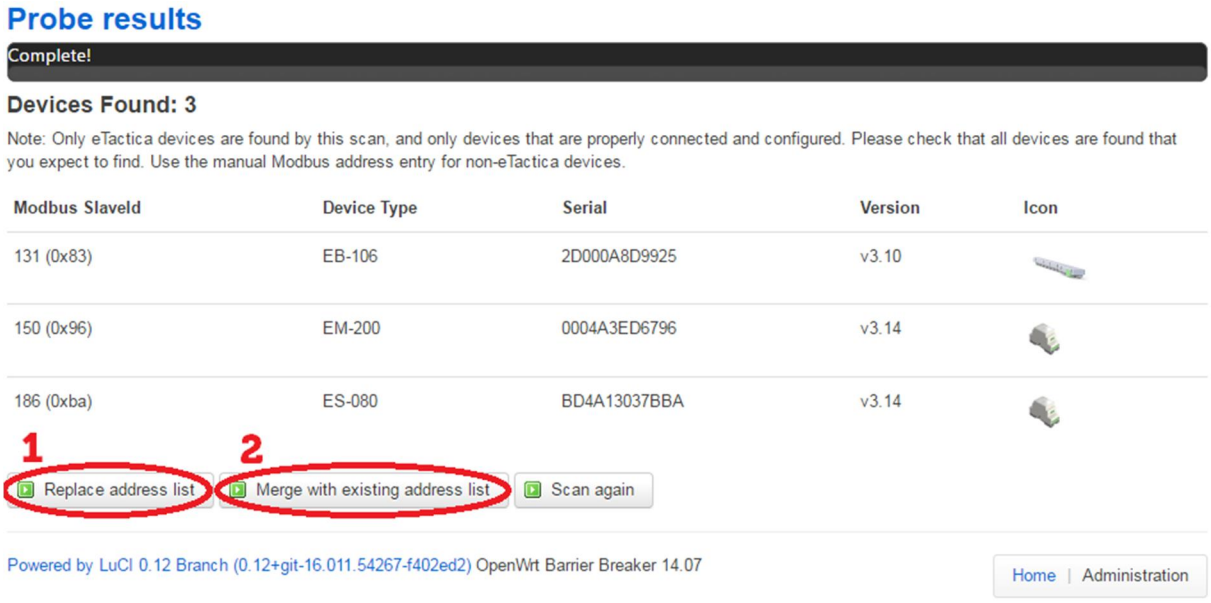
If you have many devices, you can attempt to scan for all connected devices. Please note that this only works for eTactica devices and only for devices that are properly connected.

You should always review the scan results to be sure they match the devices you expected to be found.

If you choose to scan, simply press the *[Probe/Scan]* button.

The process will take about 30 seconds, as it scans all possible Modbus addresses looking for eTactica devices.

Below is a screenshot of a completed scan process.



For each device that is detected, you can see the Modbus address found, the device type, the unique serial string and an icon for each device to help you match against what you expect.

If you had third party devices already in your list, or if you have eTactica devices you plan on connecting later that you had manually entered in the previous step, then press the *[Merge with existing address list]* button (2) to merge a combined device list.

If you only care about the devices that were successfully scanned, you can press the *[Replace address list]* (1) button to replace any existing list with your scan results.

If a device is not showing up in the scan list, please recheck its wiring and power supply, and feel free to scan again.

When choosing either *[Replace address list]* or *[Merge with existing address list]*, the configuration will be saved and applied.

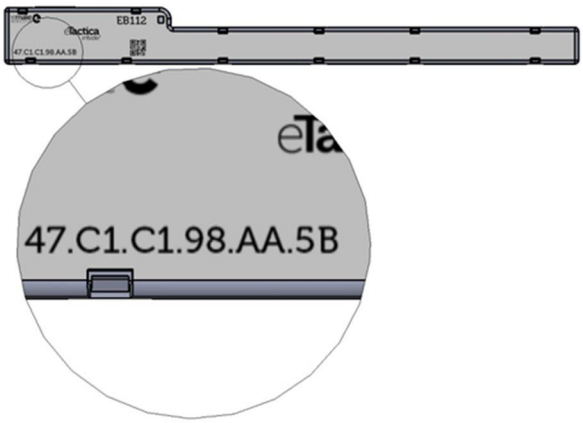
For 3rd party devices

For third party devices you need to find or change the Modbus address yourself. This might be via the LCD screen and buttons on the device, or in the device manuals. Once you have found/configured the address, enter it just like any other.

A note on Modbus addresses

The Modbus addresses are fixed for all eTactica devices and are based on the serial number (unique ID) of the device.

The unique ID is a 12-digit sequence of hexadecimal numbers that you find on the label of the device.



You need to read the last two letters/digits (hexadecimal) from the unique ID of each device that represent the Modbus address.

Example:
If the unique ID for your EB-112 device is , then the Modbus address is 5B.

Unauthorized Modbus addresses

According to the Modbus protocol specifications, some addresses are not allowed: 00, F8, F9, FA, FB, FC, FD, FE, FF.
Even so, these addresses can exist in the unique ID string.

For manual configuration of devices

For manual configuration of devices you need to be careful. If you have a device with an unauthorized Modbus address, then the address isn
the code but the two previous letters (and if they are also unauthorized the next two).

Example:
If your device ID is .43.4C.FD then you have to put 4C into the list.

For automatic scanning of devices

For automatic scanning of devices, this is not an issue. The unique serial string is already known by each device and therefore also if it contains unauthorized digits. The device itself works out a correct Modbus address, during boot-up, and will reply using the correct address.

5. Channel Monitor

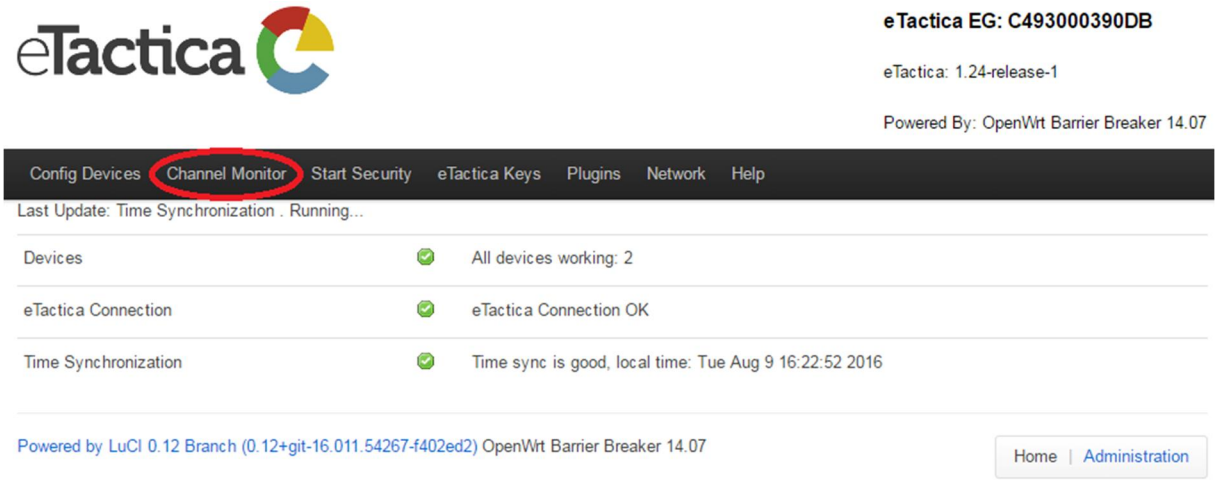
The Channel Monitor lists all connected devices and displays all measurements.

Step 1 - Connect to your Gateway

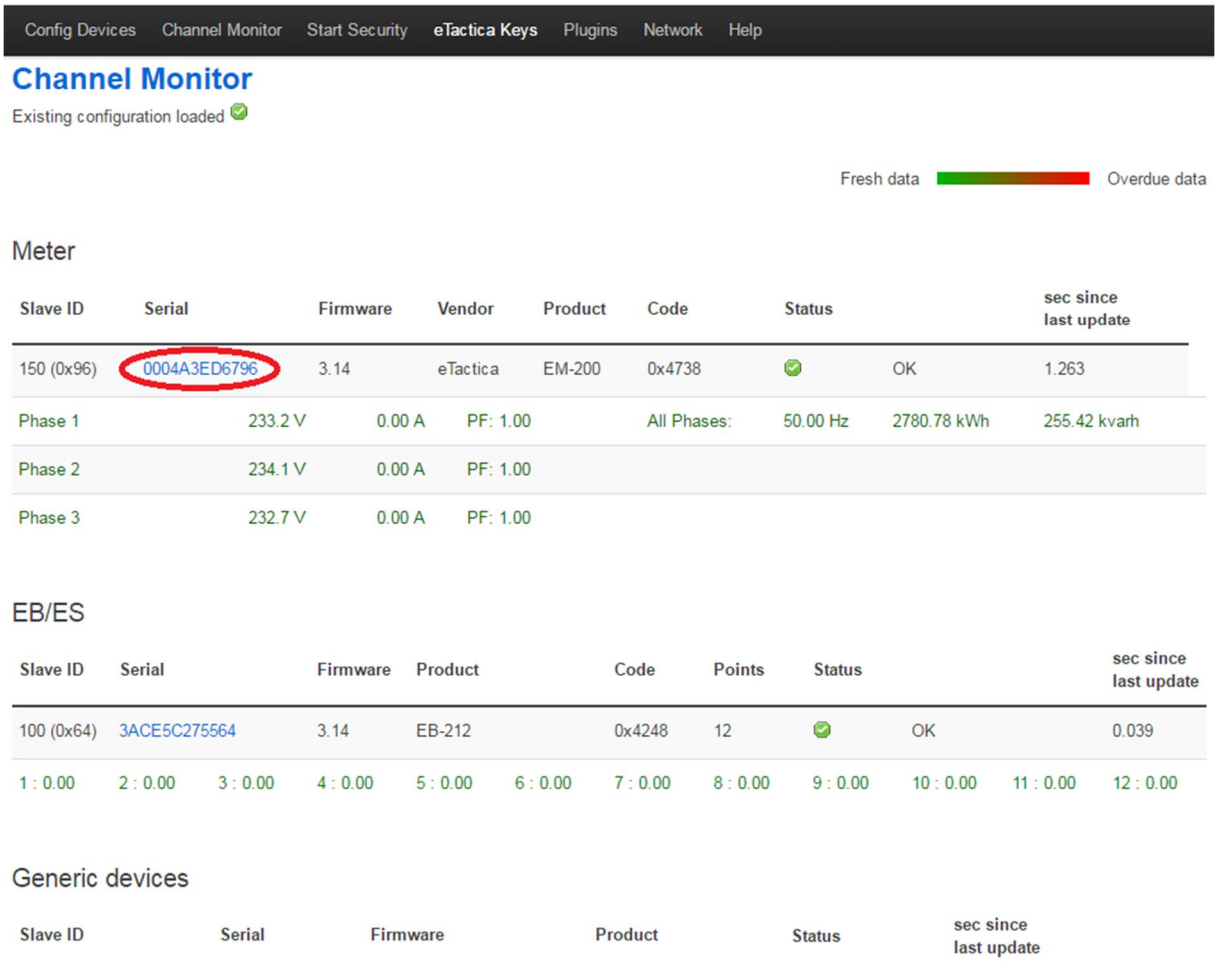
If you are not connected to your gateway device, please see chapter 2, *Connecting to Gateway*.

Step 2 - Enter Channel Monitor page

On the home page of your administration web console, select *Channel Monitor* from the top menu.

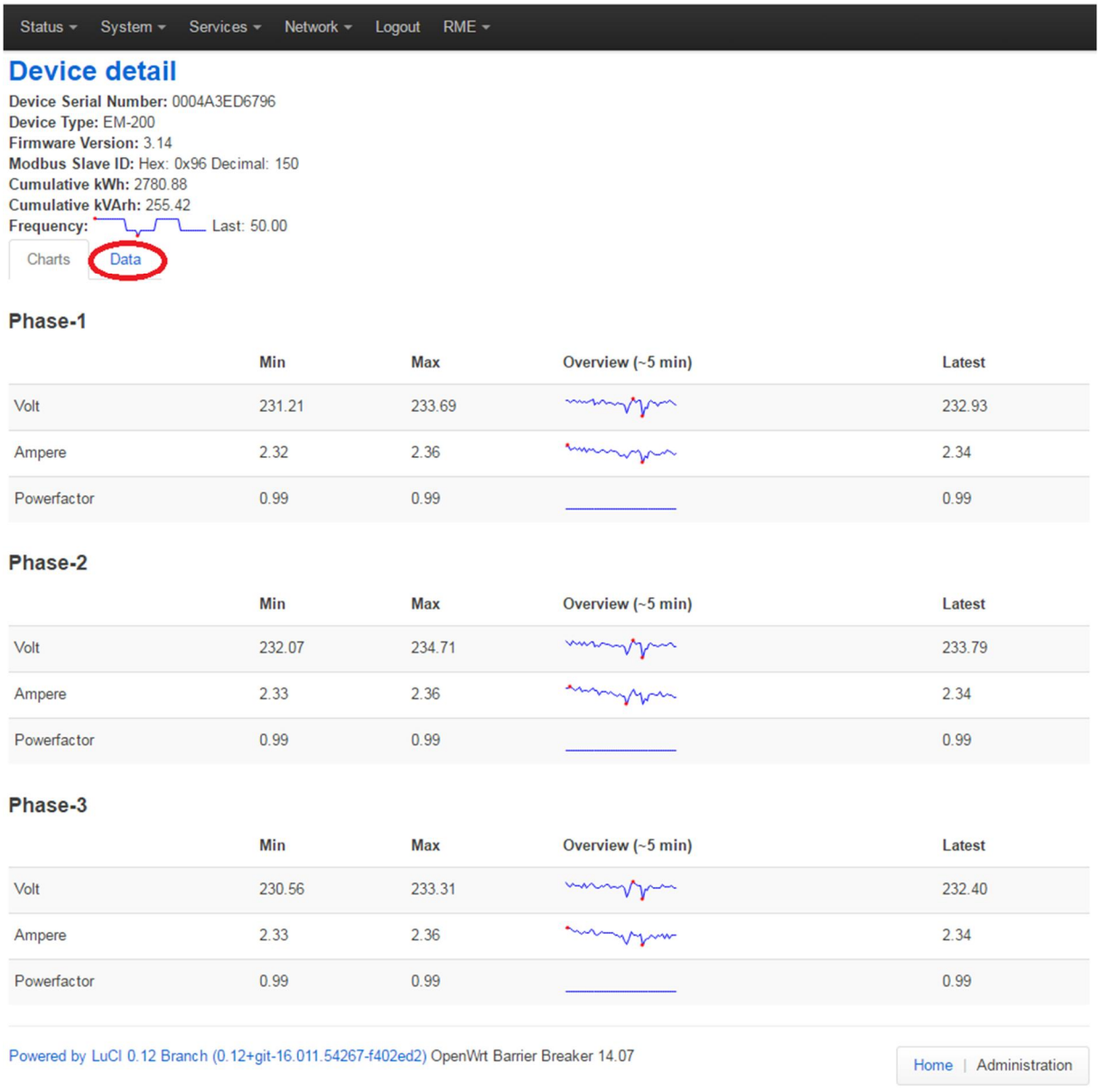


Here you can see a list of all connected devices, information about the type, serial number and firmware version. You can also see the latest readings.



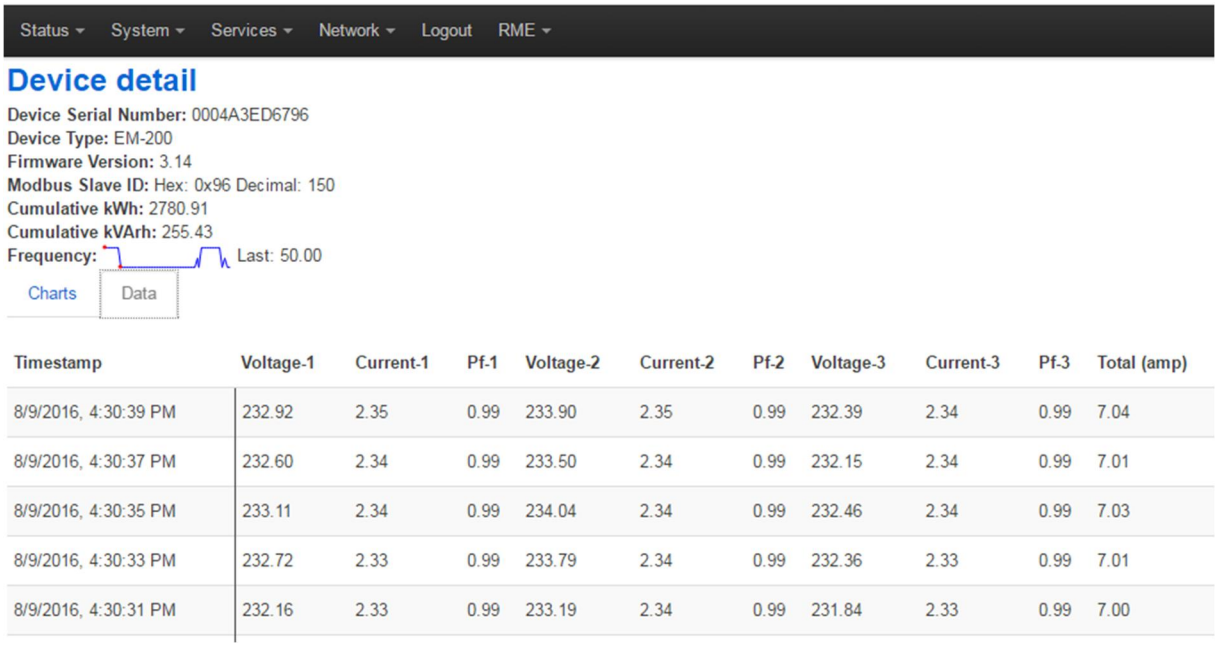
Step 2 - Go to the Device detail page

Click on the serial number of device of interest. Here you can see various information about that device, all measurements, both in numbers and also in small graph with up to 5 minutes of data (starting when the page is opened).



Step 3 Go To the tabulated data page

Click on the *[Data]* button to see all measurements in tabulated form.



Timestamp	Voltage-1	Current-1	Pf-1	Voltage-2	Current-2	Pf-2	Voltage-3	Current-3	Pf-3	Total (amp)
8/9/2016, 4:30:39 PM	232.92	2.35	0.99	233.90	2.35	0.99	232.39	2.34	0.99	7.04
8/9/2016, 4:30:37 PM	232.60	2.34	0.99	233.50	2.34	0.99	232.15	2.34	0.99	7.01
8/9/2016, 4:30:35 PM	233.11	2.34	0.99	234.04	2.34	0.99	232.46	2.34	0.99	7.03
8/9/2016, 4:30:33 PM	232.72	2.33	0.99	233.79	2.34	0.99	232.36	2.33	0.99	7.01
8/9/2016, 4:30:31 PM	232.16	2.33	0.99	233.19	2.34	0.99	231.84	2.33	0.99	7.00

The newest measurements are added to the top of the list.

6. Device Plugins

Add/Remove Device Plugins

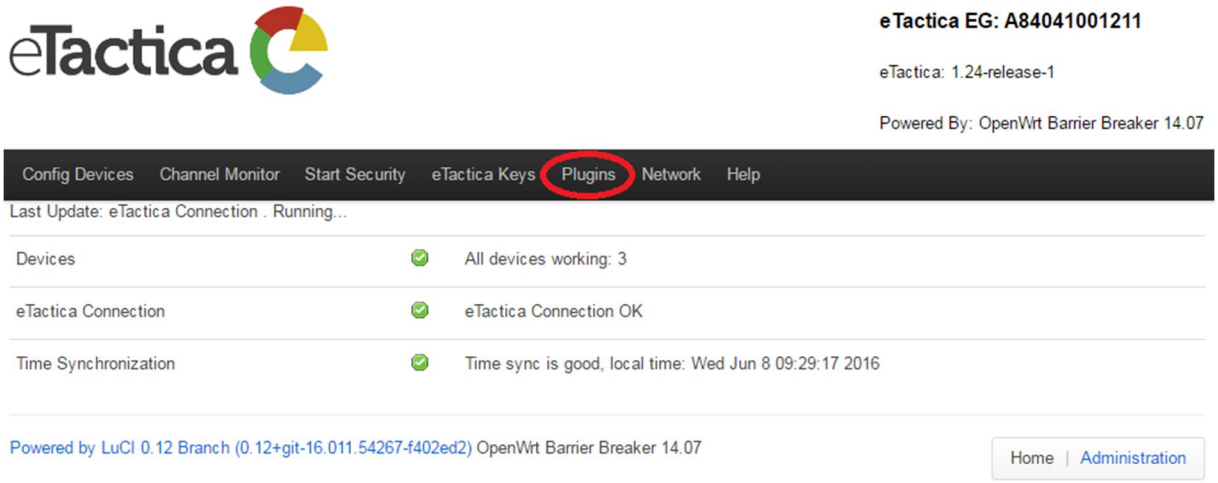
The eTactica gateway uses plugins to support all data collection devices, both 3rd party and our own eTactica devices. These plugin scripts tell the gateway how to access a particular device, and what values to read from that device. The administration console lists all the plugins, allows you to add new plugins to support new devices, create new plugins, edit plugins that are installed and delete plugins that might conflict.

Step 1 - Connect to your Gateway

You need to be successfully connected to your gateway device. If not, see chapter 2, *Connecting to Gateway*.

Step 2 - Go to the plugins page

From the home page of the administration web console of your device, select *Plugins*.

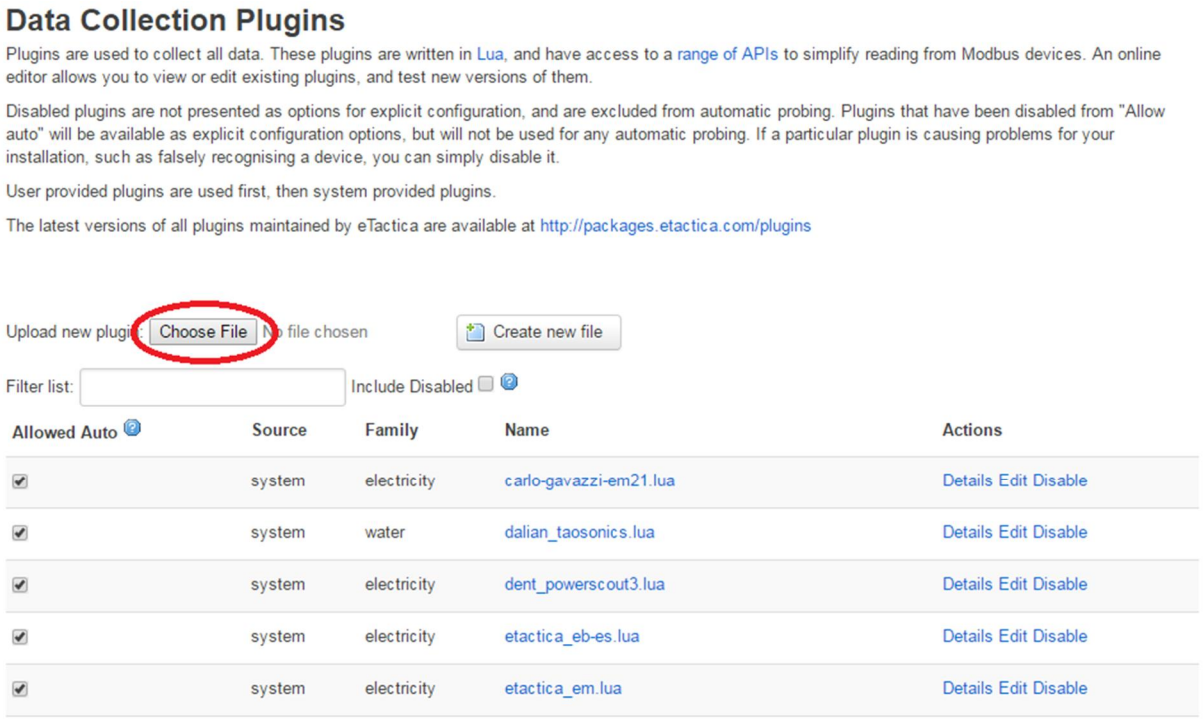


This will require you to login, using the root password you have configured earlier. If not, please see chapter 9, *Password Settings*.

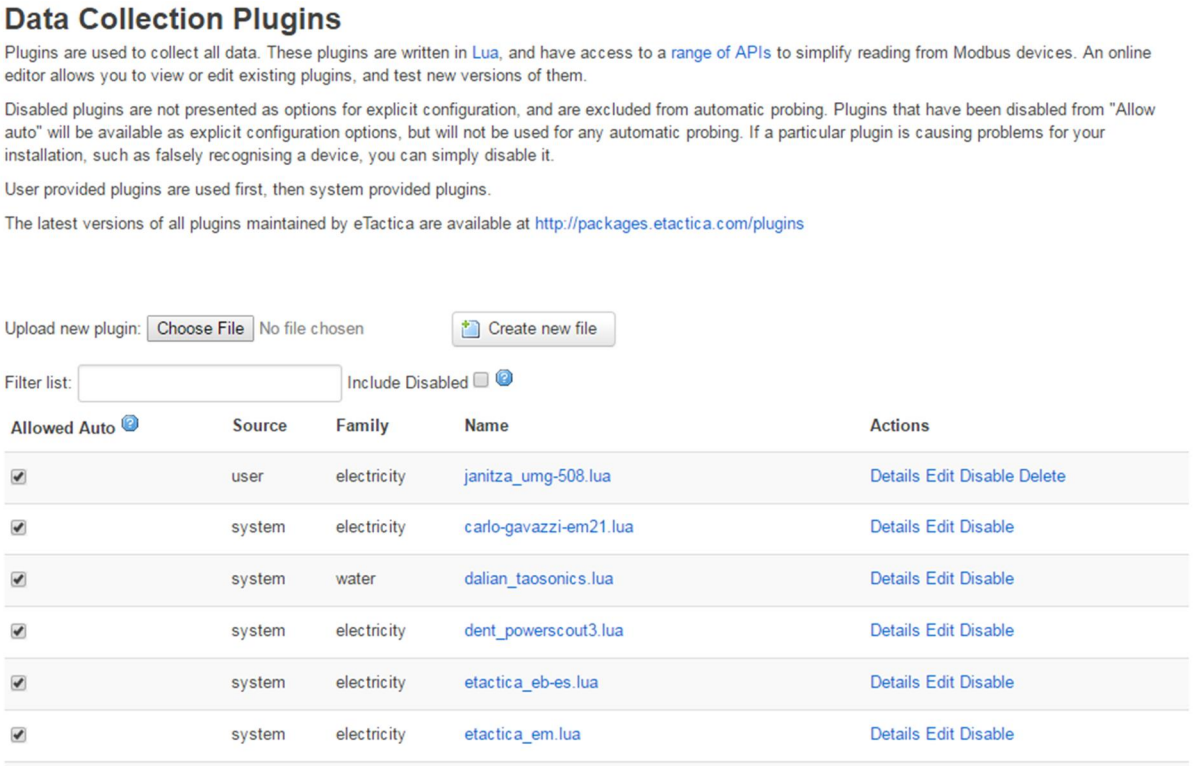
Step 3 - Add new plug-ins

On the Plugins configuration page, you can see the list of already installed plugins that the gateway is now able to use for a data collection device access.

To add more plugins to that list, press the *[Choose File]* button and select the script file from your computer to upload to your gateway.



In the following example, we have selected a Janitza UMG-508 meter plugin and it will be added to the list of plugins.



The latest versions of all plugins maintained by eTactica are available at http://packages.etactica.com/plugins

You can create your own plugin, either from scratch by pressing the *[Create new file]* button or by modifying an existing plugin by clicking *[Edit]* for the plugin you want to modify. Then you do the modifications you want and save the plugin under a new name. There is a link to further documentations on the plugin API on the plugin

Clicking the name of a plugin or will show you more information for that plugin. Disabled plugins are not presented as options for explicit configuration, and are excluded from automatic probing. Disabled plugins will disappear from the list unless the tick box is checked. Plugins that have been disabled from "Allowed auto" will be available as explicit configuration options, but will not be used for any automatic probing. If a particular plugin is causing problems for your installation, such as falsely recognizing a device, you can simply disable it.

7. Modbus Settings

The eTactica gateway, as a data collecting device, uses the Modbus/RTU protocol over an RS485 serial line to communicate with one or many connected measurement devices. Up to 32 devices can be connected at once.

Default configuration

By default, the eTactica gateway is configured to maintain a connection to eTactica servers, posting real time measurements from configured devices. All connected devices are listed up, using the administration web console on the gateway, where the user types in the Modbus address required to identify each connected device (For device configuration, see chapter 4, *Device Configuration*).

The gateway continuously makes Modbus/RTU requests to each device and forwards these readings to the eTactica server database.

The RS485 interface is by default configured with the following protocol settings, according to Modbus/RTU:

- 19200, baudrate
- 8, data bits
- Even, parity
- 1, stop bit

Furthermore, the eTactica gateway can also be used as a simple Modbus/TCP to Modbus/RTU bridge that is connected to a 3rd party management or data collecting software. All Modbus queries are then handled by the 3rd party software.

In the following, a step by step guide is provided for:

- Edit the serial protocol settings
- Configure the Modbus/TCP access

Edit RS485 serial settings

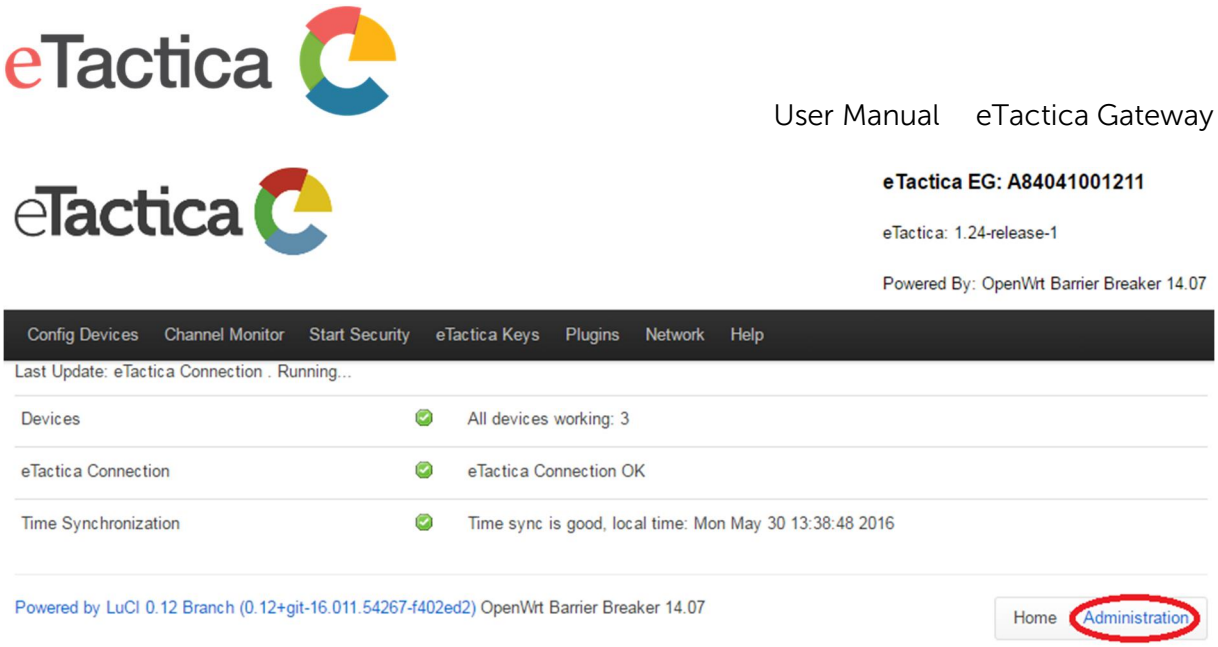
The user is able to change the default serial settings for the RS485 interface.

Step 1 - Connect to the Gateway

If you are not connected to your gateway device, please see chapter 2, *Connecting to Gateway*.

Step 2 - Go to Administration page

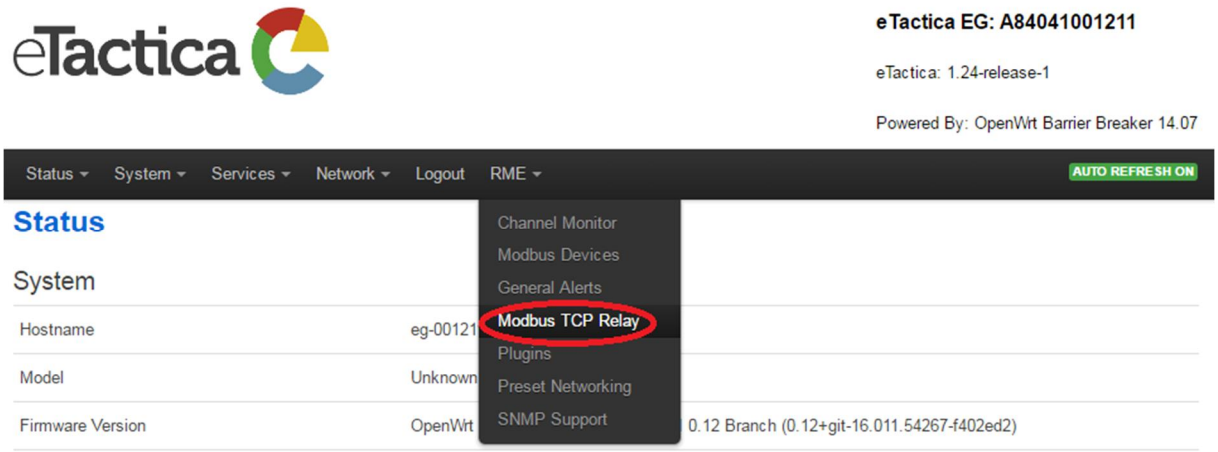
From the home page of the administration web console of your device, click the *[Administration]* link.



This will require you to login, using the root password you have configured earlier. If not, please see chapter 9, *Password Settings*.

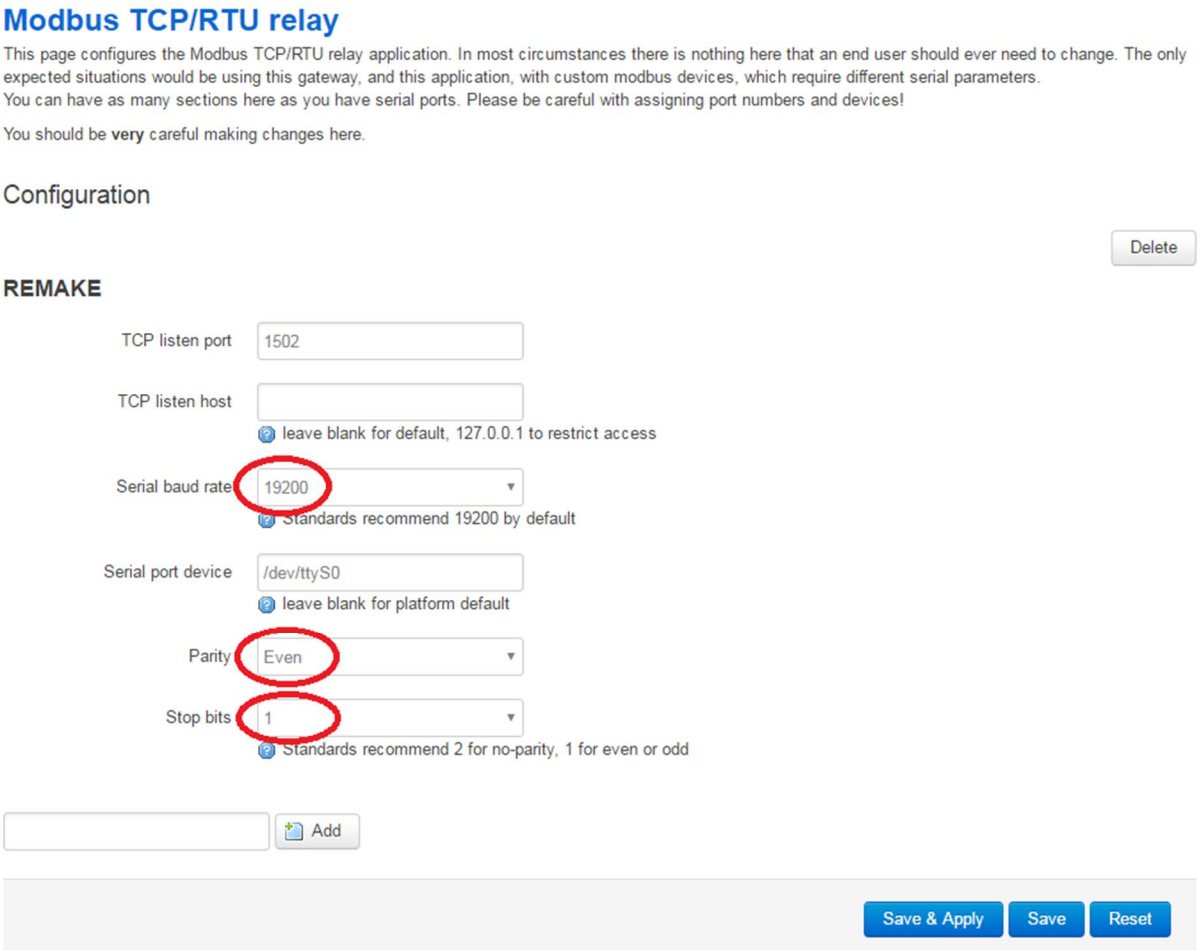
Step 3 - Go to the Modbus TCP/RTU relay page

From the top menu, choose *RME->Modbus TCP Relay*.



Step 4 - Change settings

You can now change the serial settings; baud rate, parity and stop bits.



Step 5 - Save settings

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

Modbus/TCP

By default, the eTactica gateway is pre-configured to communicate with eTactica servers. However, the gateway also provides a Modbus/TCP to Modbus/RTU bridge interface on TCP port 1502. This allows the use of any third party Modbus software to query devices connected to the Modbus/RTU port of the gateway from a remote network.

Note

Using this Modbus/TCP relay at the same time as the default eTactica service, requires some caution. The serial network has only a limited bandwidth and each Modbus request must be handled in sequence. Trying to operate the relay of requests at a high rate, when you also have multiple devices configured for eTactica, may result in intermittent timeouts and communication failures.

- The minimum polling interval of the Modbus/TCP Master must be set to 500 msec or longer.
  This is the timeout used on the serial side and if your TCP master waits for less than this time, you may timeout when the device is still sending a valid reply.

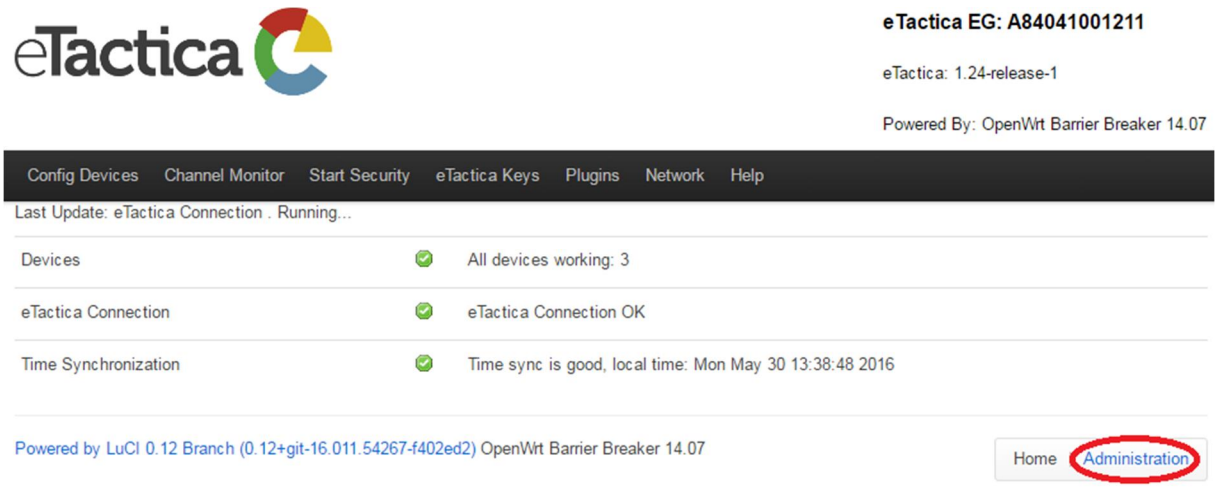
By default, this bridge/relay port listens on all interfaces. If you would like to disable remote access to this service, please change only the *listen_host* property in the configuration page, see below. Note that this bridge service is used internally, so it should not be completely disabled.

Step 1 - Connect to the Gateway

If you are not connected to your gateway device, please see chapter 2, *Connecting to Gateway*.

Step 2 - Go to Administration page

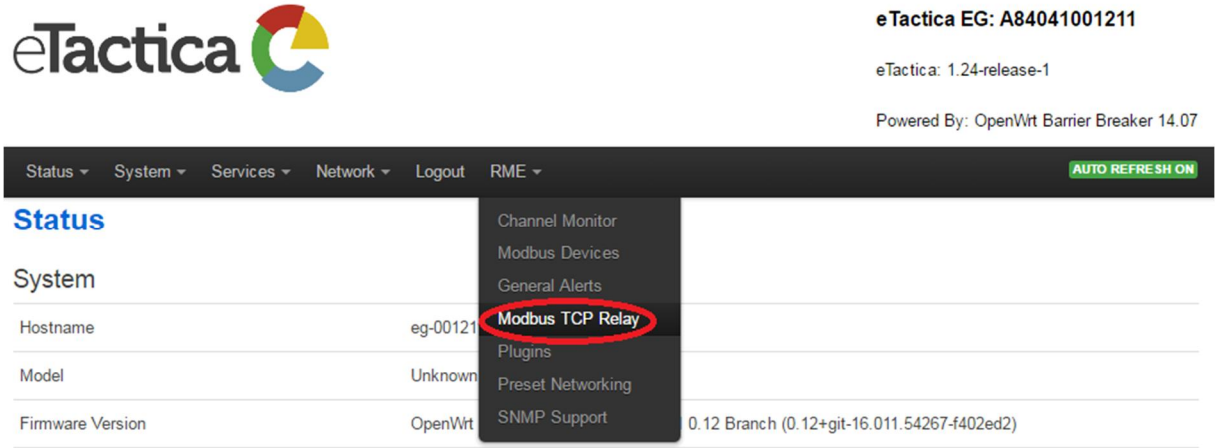
From the home page of the administration web console of your device, click the *[Administration]* link.



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 the Modbus TCP/RTU relay page

From the top menu, choose *Network->Modbus TCP Relay*.



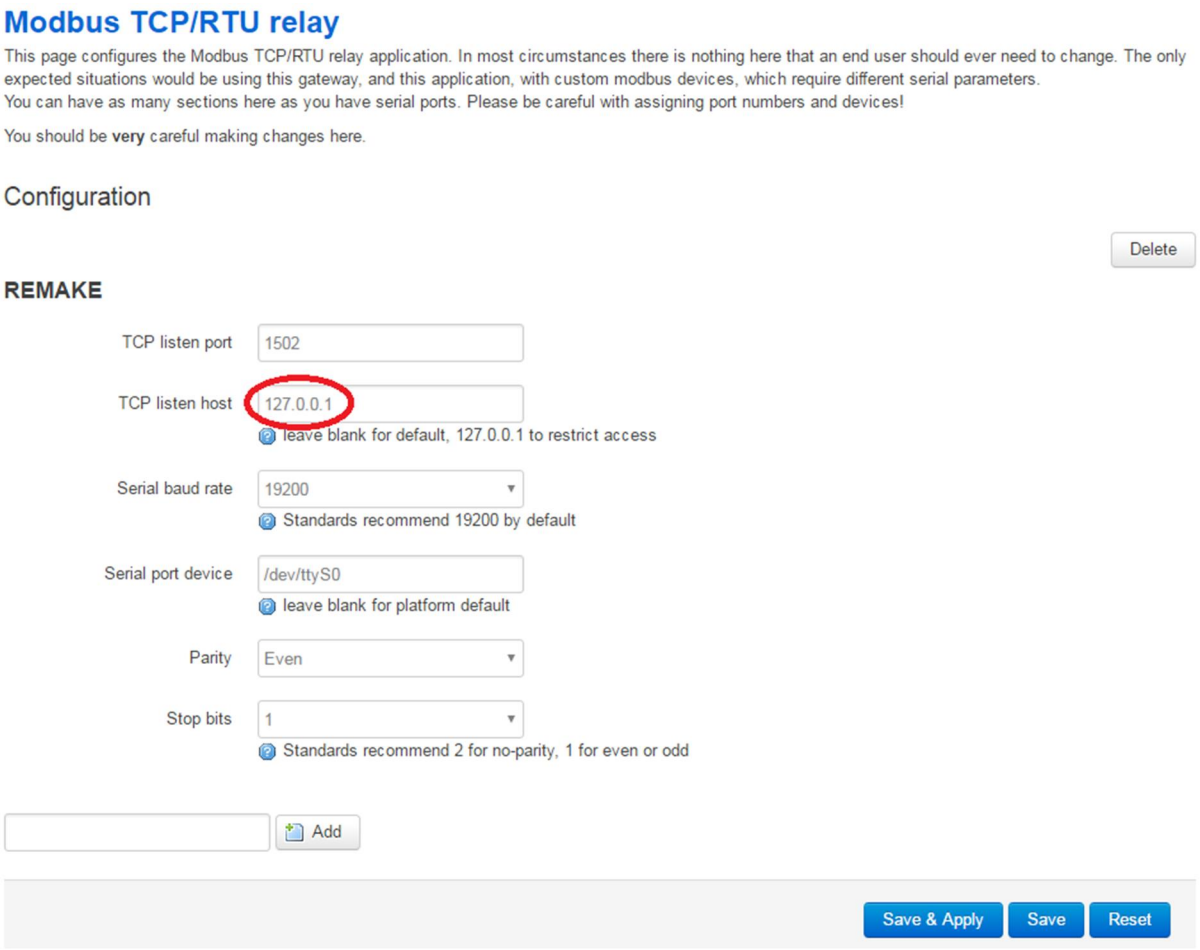
Step 4 - Restrict access

By default, the *TCP listen host* field is blank. This means that the TCP access is open for everyone, via port 1502.

To restrict any access or disable Modbus/TCP for 3rd party devices, insert 127.0.0.1 to the *CP listen host* field. This will only allow the localhost or the gateway itself, to use the internal TCP relay service.

Note

It is important to note that you can t restrict access to a single or several IP addresses on your network. Either Modbus/TCP is open to all devices on your network, or it is completely blocked. The only allowed IP address for this field is 127.0.0.1.



Step 5 - Save settings

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

8. Network Settings

In this chapter, you will find information related to the following network settings:

- Change to static IP address
- Enable/Disable WiFi interface
- Internet connection via WiFi (No Ethernet connection)
- Advanced WiFi parameters

Static IP address

In some installations, the network facilities require the use of statically configured networking. The eTactica gateway supports this, but it requires manual configuration.

Required Information

The following details are *required* from the network manager:

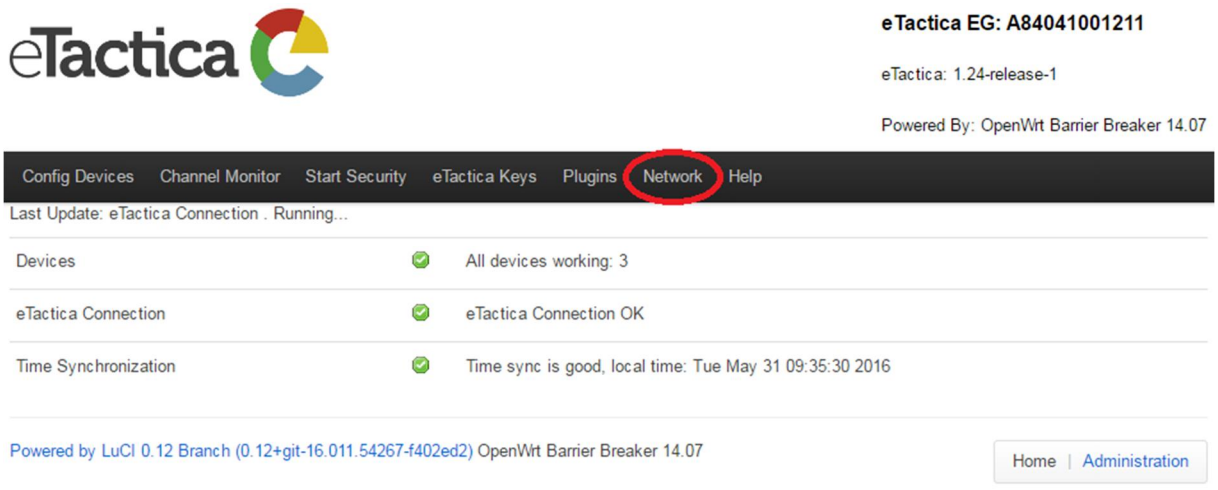
Required Information	Example Value
IP Address	10.0.42.141
Subnet Mask	255.255.255.0
Gateway	10.0.42.254
DNS Server	10.0.1.1

Step 1 - Connect to your Gateway

If you are not connected to your gateway device, please see chapter 2, *Connecting to Gateway*.

Step 2 - Enter Networking configuration page

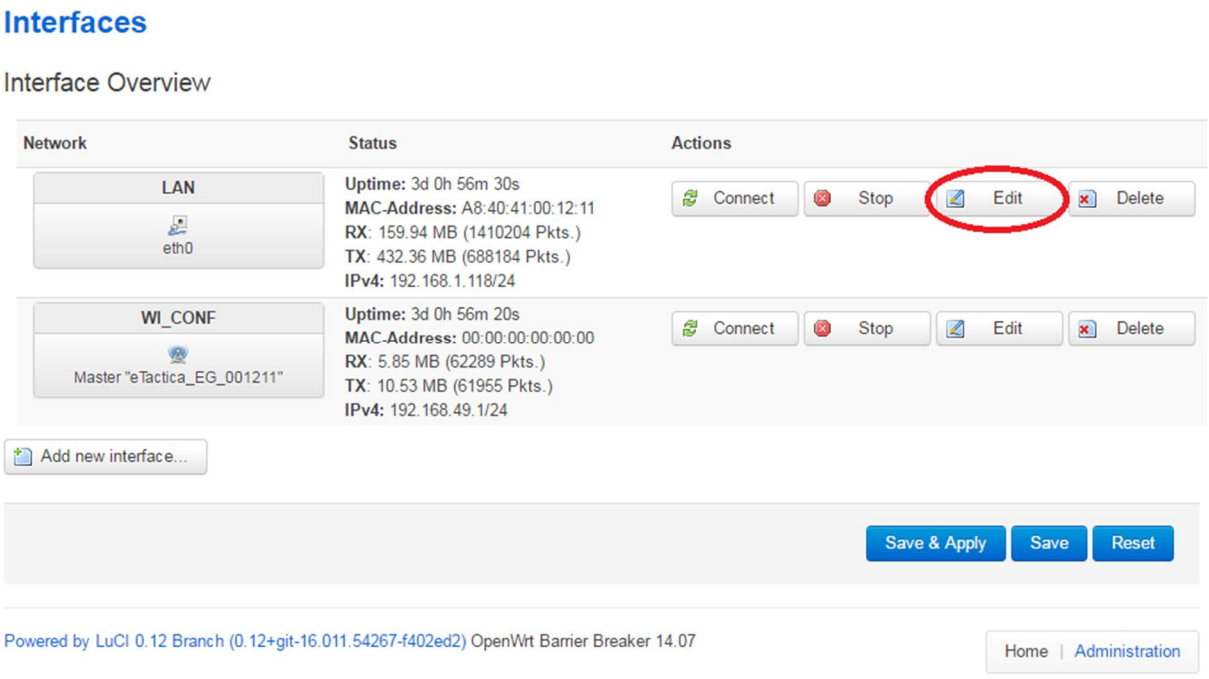
On the home page of your administration web console, select *Network* from the top menu.
Alternatively, to access network settings, you can use the *[Administration]* link and from there you select *Network->Interface* from the top menu.



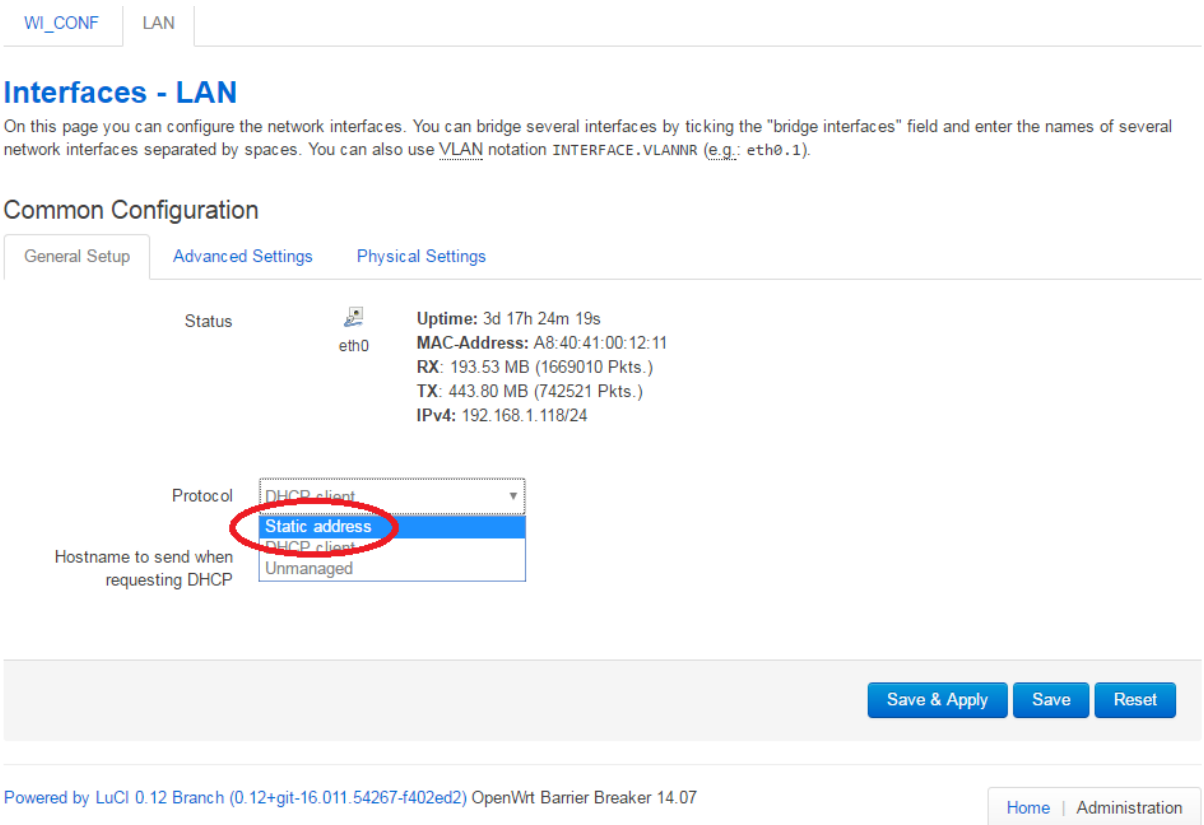
This will require you to login, using the root password you have configured earlier. If not, please see chapter 9, *Password Settings*.

Step 3 - Edit the network interface you wish to configure statically

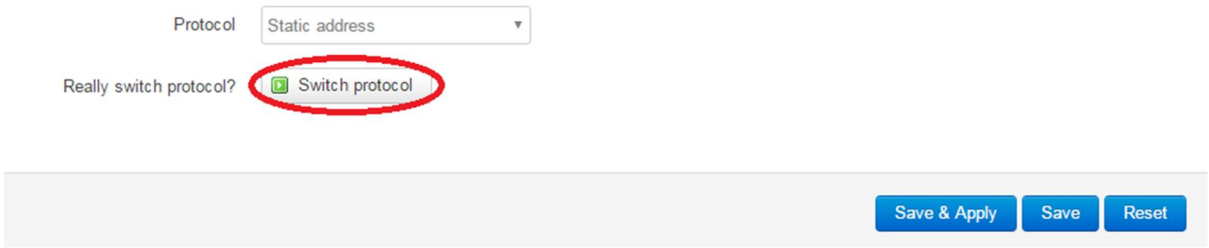
Press the *[Edit]* button, for your interface. This could be either the WiFi or the Ethernet interface, but will generally be the Ethernet interface (LAN).



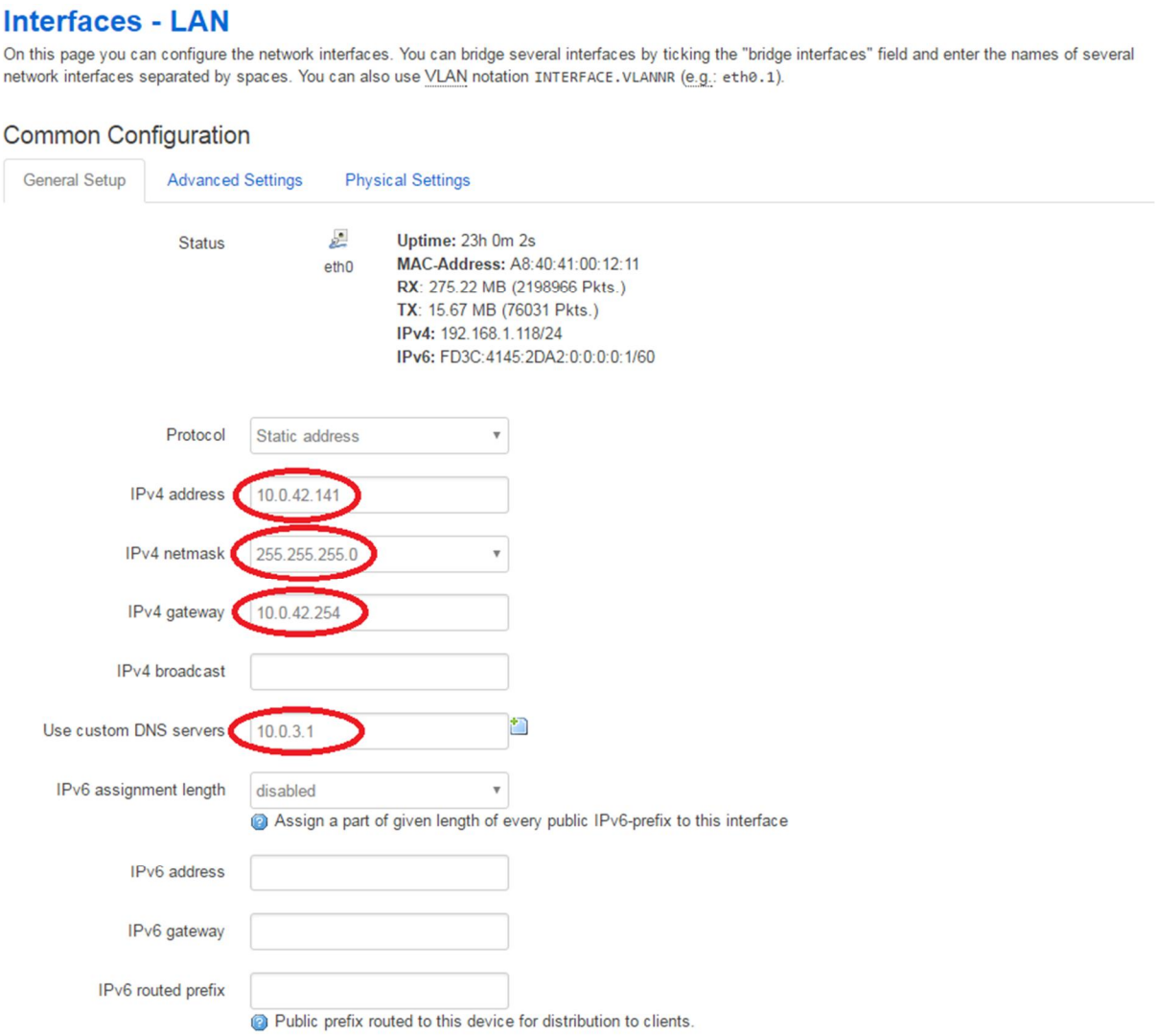
Switch the interface to *Static address* .



Confirm that you want to switch protocol by pressing *[Switch protocol]* button.

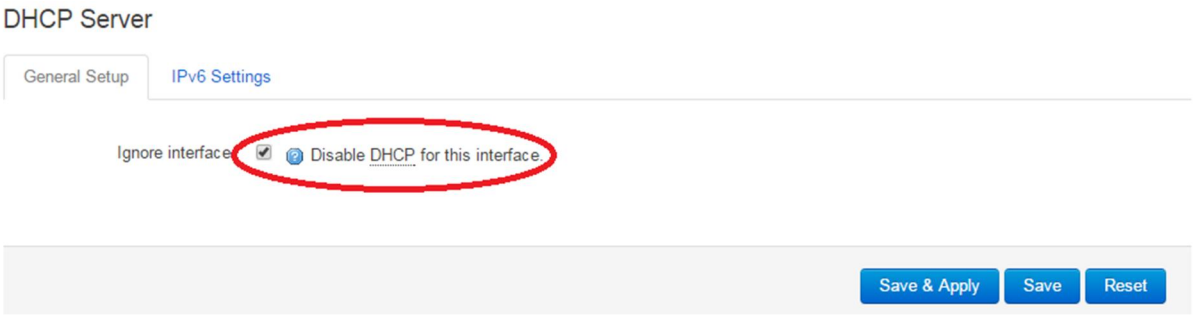


Fill in the form with the details you were provided.



You would also like to disable DHCP for the interface.

In almost all cases, if you are configuring a static IP for your Gateway, you will want to disable DHCP for the interface. This would normally only be used if you were configuring the Gateway as a router, rather than as a static client. If you do NOT disable DHCP, you may find that other devices on your statically configured network segment start receiving DHCP offers from your Gateway, which will rarely be what you were hoping to achieve.



Step 4 - Save settings

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

Enable/Disable WiFi

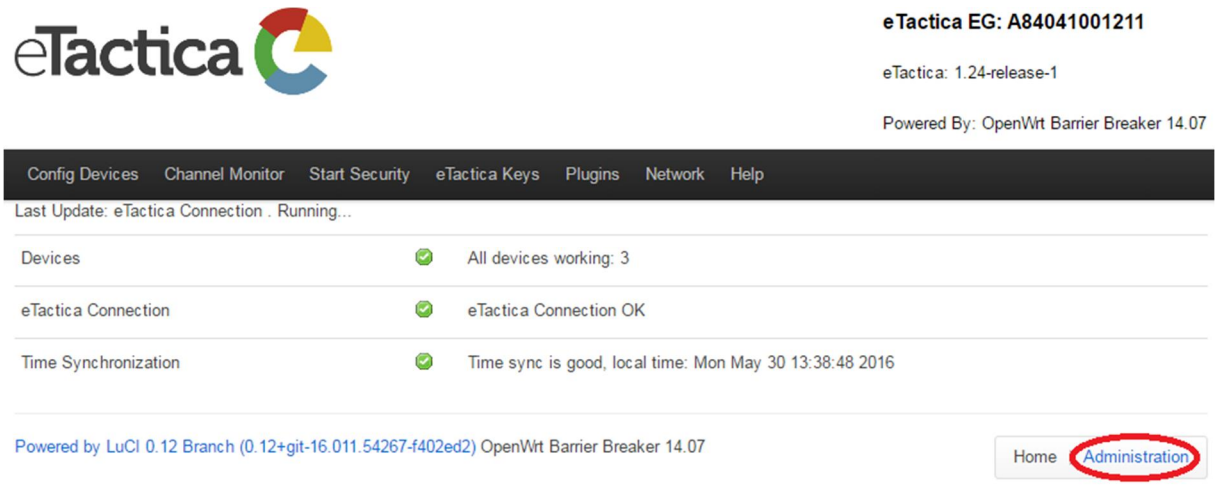
In some installations, once configuration has been completed, you want to completely disable WiFi access and do any future configuration via the Ethernet interface.

Step 1 - Connect to the Gateway

If you are not connected to your gateway device, please see chapter 9, *Connecting to Gateway*.

Step 2 - Go to Administration page

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



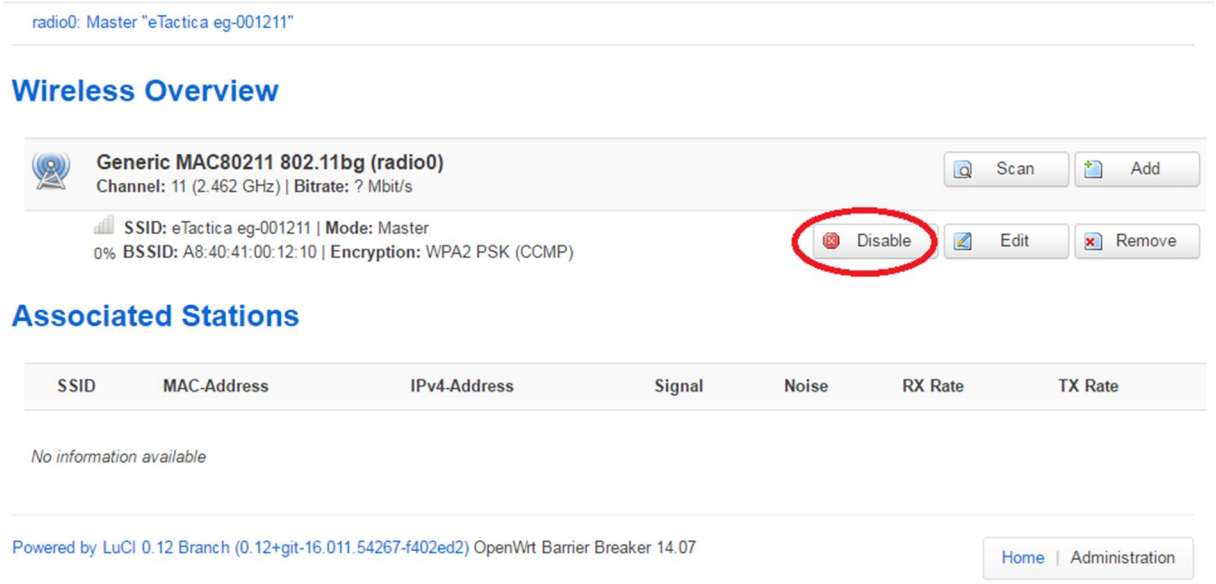
This will require you to login, using the root password you have configured earlier. If not, please see chapter 9, *Password Settings*.

Step 3 - Go to the WiFi configuration page

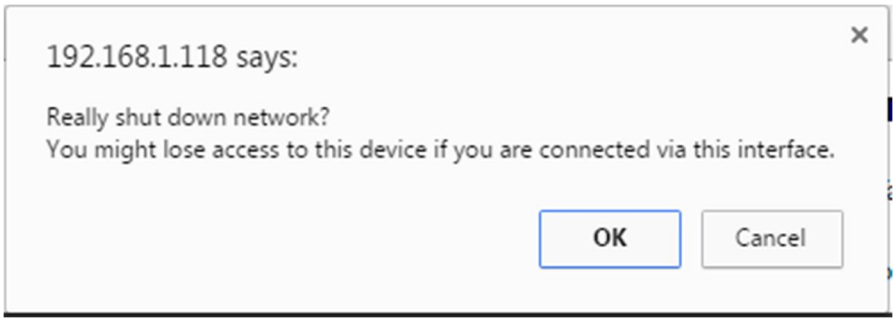
Choose *Network->WiFi* from the top menu.

Step 4 - Turn off WiFi

Press the *[Disable]* button.



Confirm that you want to shutdown network.



The WiFi should now be completely disabled.

Re-enable WiFi access to the Gateway

Since you have disabled the WiFi completely, the only option to access your Gateway is via your IP network. To do that see *Connection via Ethernet* in chapter 2, *Connecting to Gateway*.

Internet connection via WiFi (No Ethernet Connection)

By default, the eTactica gateway is configured as a wireless access point that you can use for configuration, with the Ethernet port preconfigured to be plugged into your existing network and receive address information via DHCP.

For most cabinet installations, Ethernet is available and desirable, and even if you need to make some changes to the networking (static IPs, etc.) you can do all that via the WiFi configuration network. However, you can also configure the Gateway

to use the WiFi link as the connection to network, if you don't have Ethernet access in your cabinet.
The EG-100 can only handle one WiFi connection at a time, so when the Internet connection is changed to the WiFi the access point has to be changed to the Ethernet port. On the EG-200 you can continue to use WiFi for the access point and then you can skip steps 1 to 4 in the instruction below.

Pre-requirements

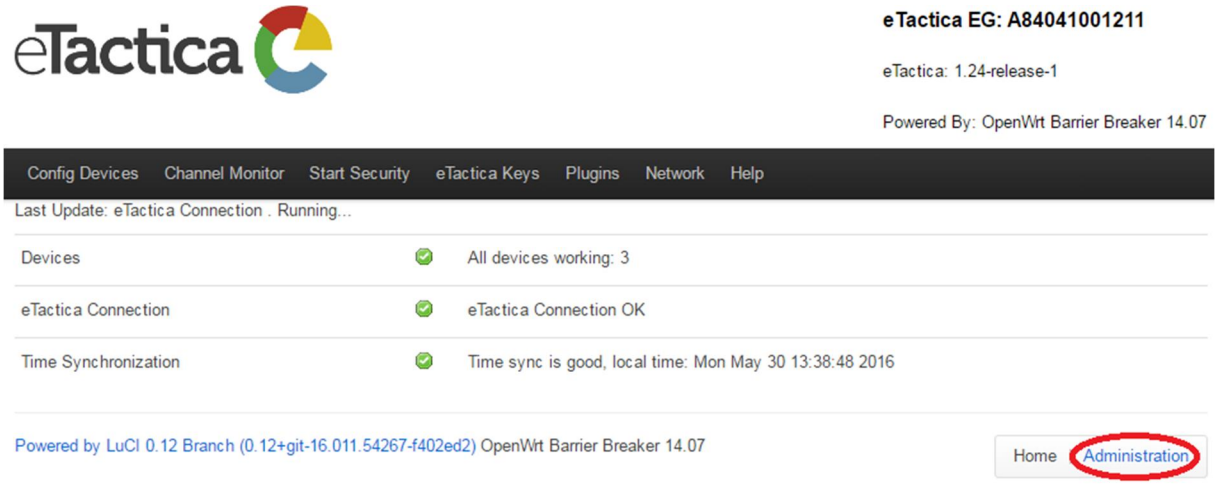
You are successfully connected to your gateway. If you are not connected yet, please see chapter 2, *Connecting to Gateway*.

Furthermore before you start, you'll need the following:

- Computer/Laptop with WiFi for initial switch-over to Ethernet
- Ethernet cable to connect your computer/laptop to the Gateway to continue configuration (not needed for EG-200)
- Wireless network keys and names for connection to your desired wireless network

Step 1 - Go to Administration page (for EG-200 go to step 5)

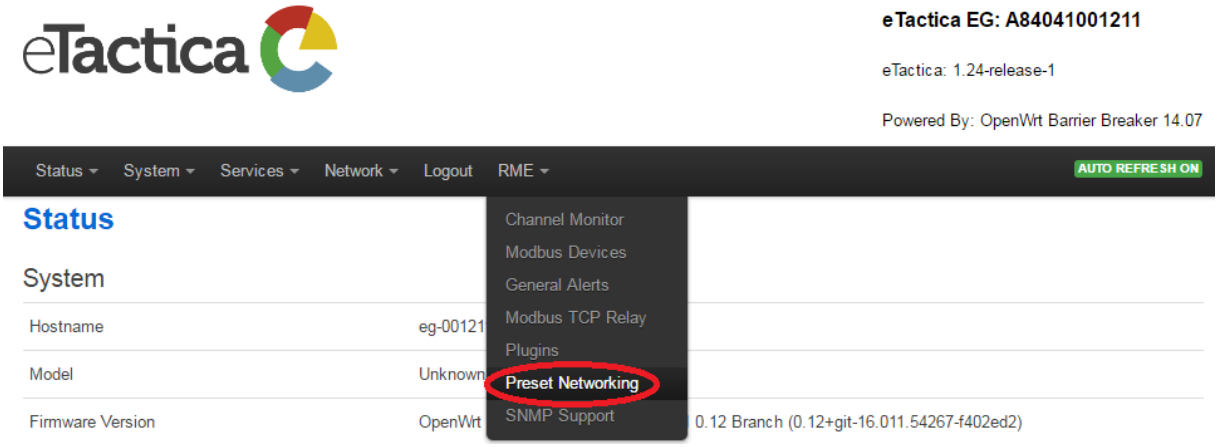
From the home page of the administration web console of your device, click the *[Administration]* link.



This will require you to login, using the root password you have configured earlier. If not, please see chapter 9, *Password Settings*.

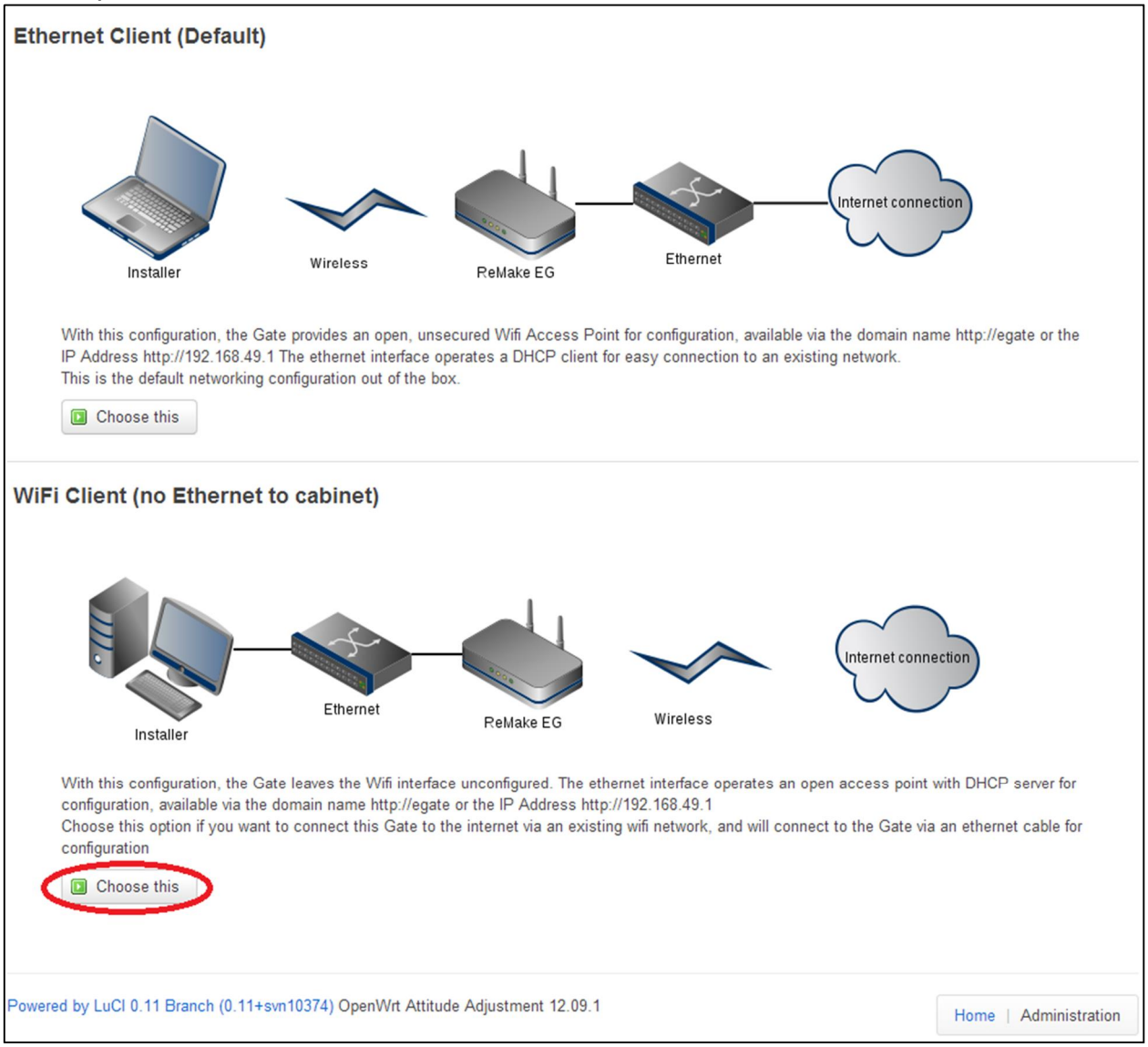
Step 2 - Go to "Preset networking"

Choose *RME->Preset Networking* from the top menu.

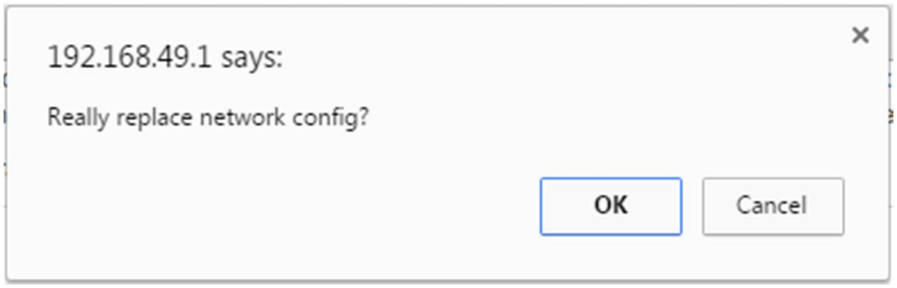


Step 3 - Switch network

You want to switch your network completely over to being an Access Point on the Ethernet port. Press the *[Choose this]* button, under "*WiFi Client (no Ethernet to cabinet)*".



Confirm that you want to switch network.



You will then connect your computer to the Gateway with a network cable and the WiFi interface will be free to reconfigure for your desired WiFi network.

Step 4 - Connect the Ethernet cable and reboot

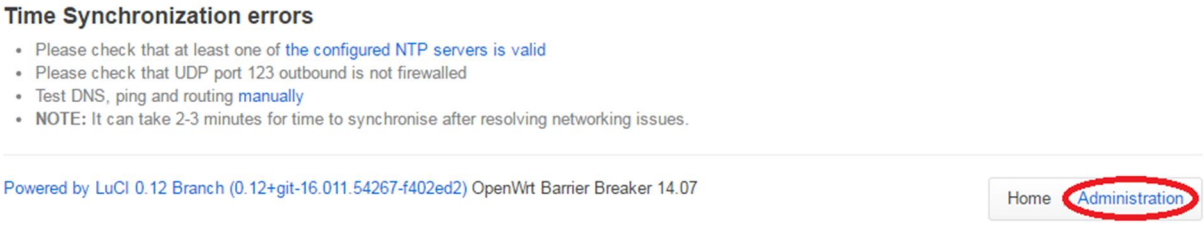
To make sure all the network comes up cleanly, the Gateway will replace its entire network configuration with clean templates and reboot. At this point you should connect the Ethernet cable from your computer directly to the gateway.

When the Gateway has come up again, re-enter in your web browser the URL for the home page of the administration web console: http://192.168.49.1

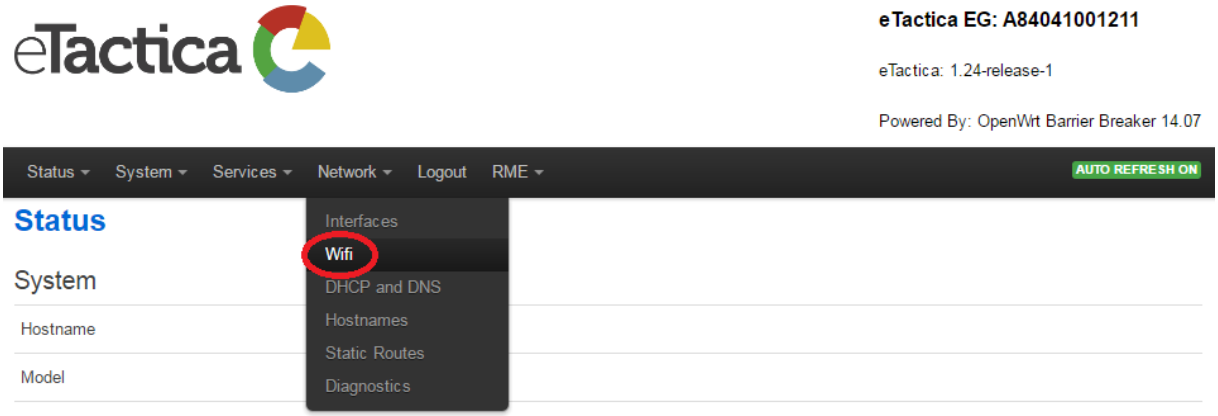
Step 5 - Configure Wireless Interface

In the following example, the Gateway is being configured to connect to a network named *Office-WiFi* .

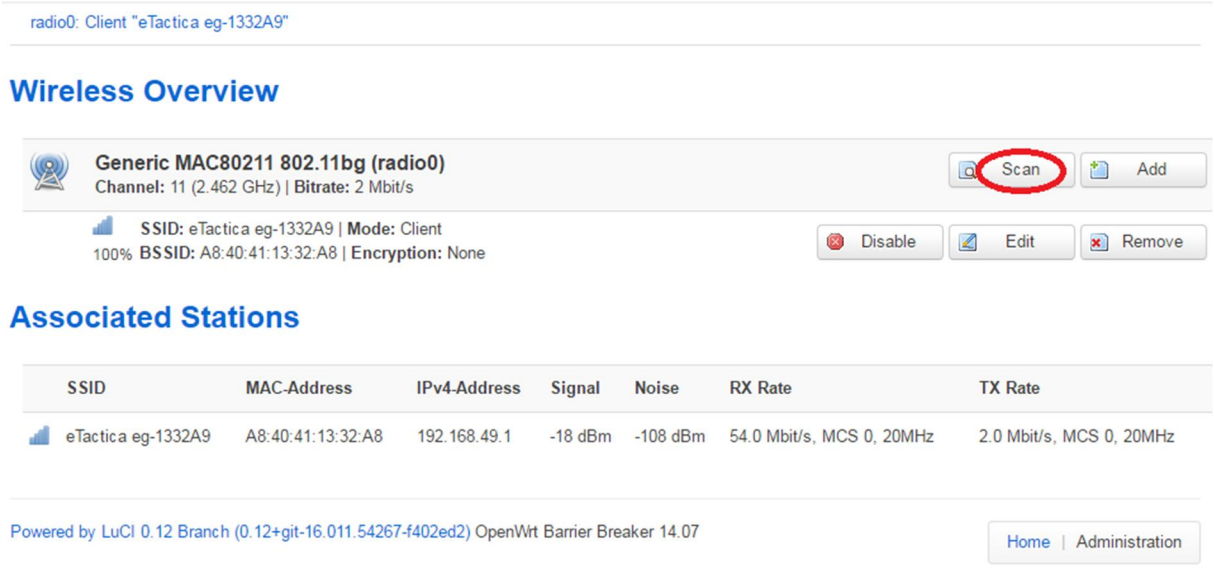
From the home page, click on the *[Administration]* link near the bottom of the page.



Choose *Network-> WiFi* from the top menu.

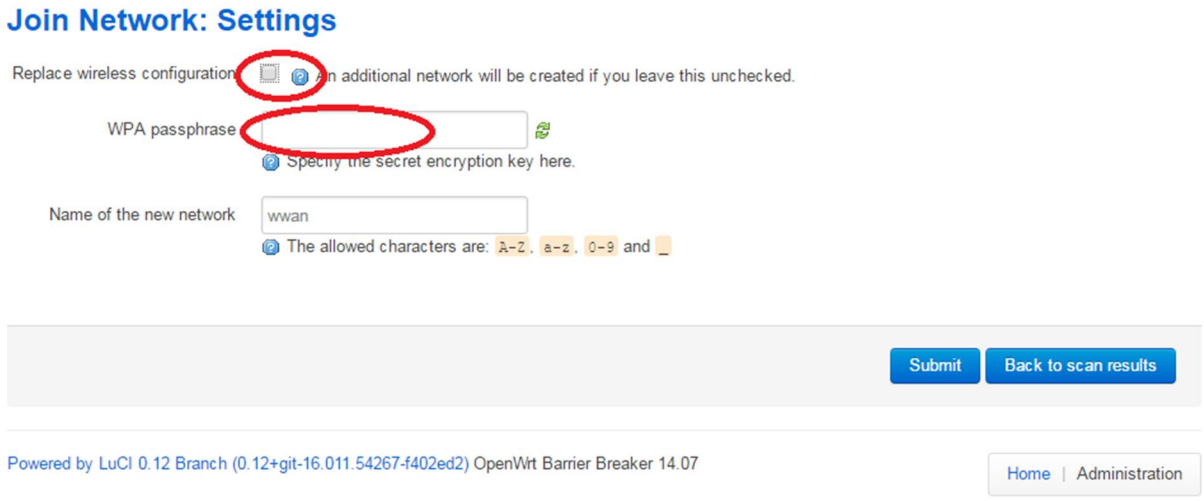


Press the *[Scan]* button.

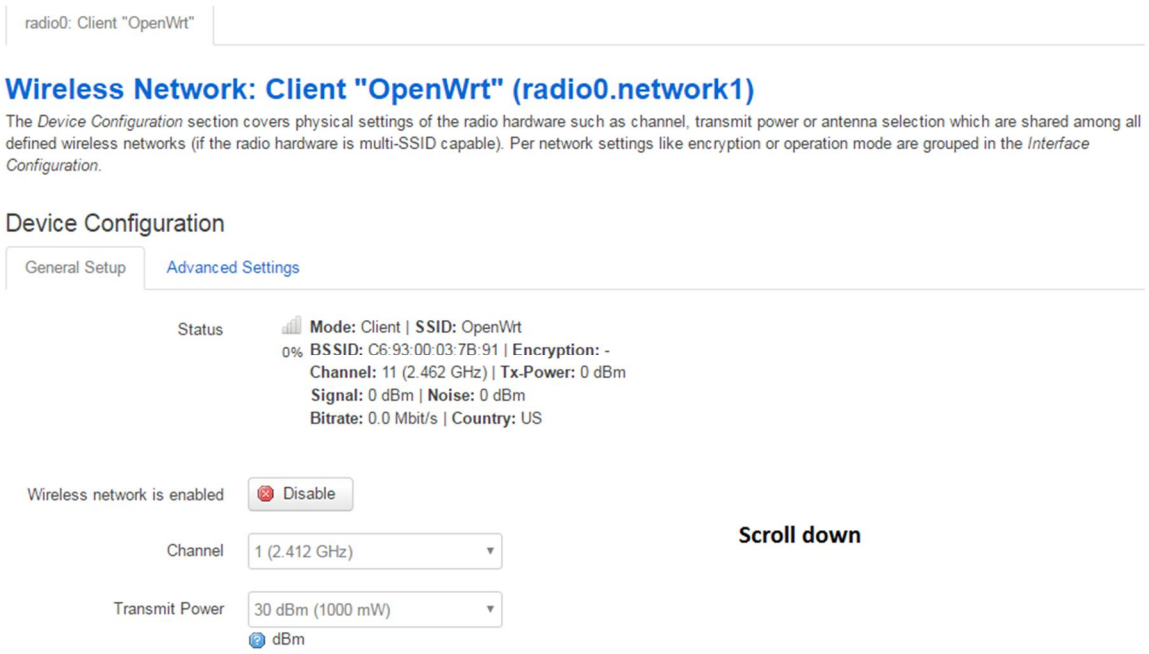


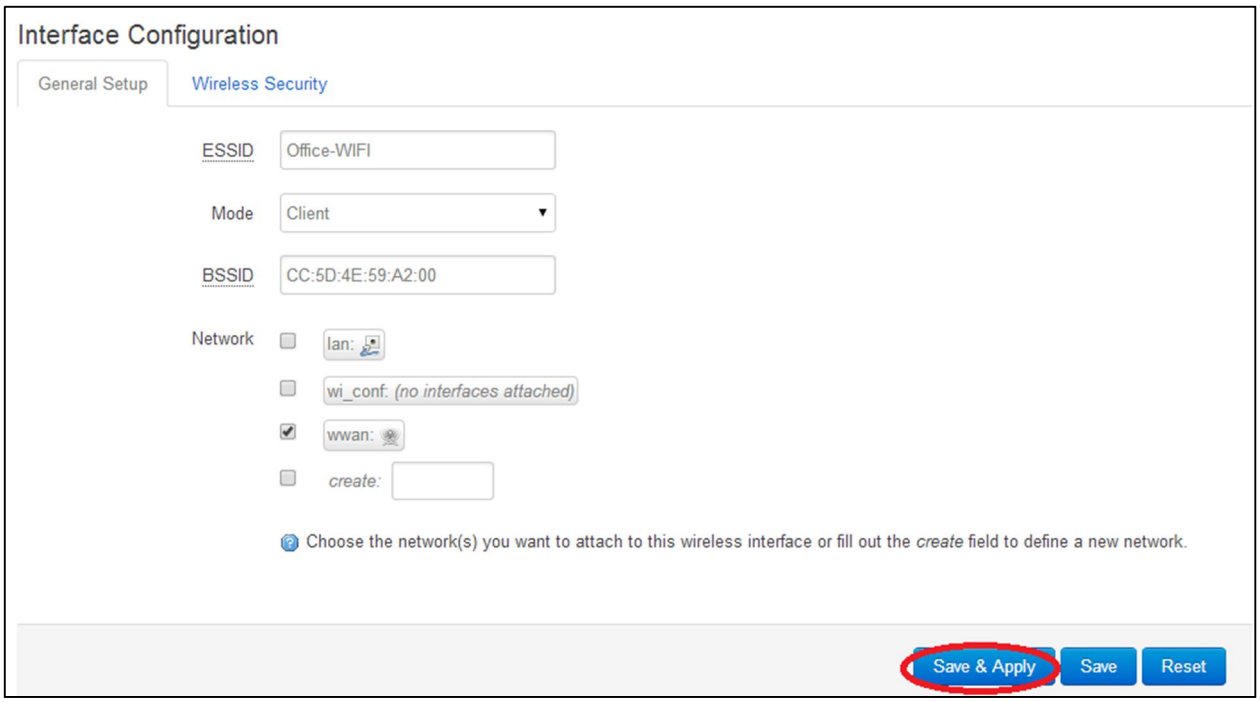
A list of all available wireless networks appears and you simply choose the one you wish to connect to.

Here you enter in your wireless network password/passphrase and on EG-200 remove the tick mark for



Now press the *[Submit]* button to continue and you will get some more options.





In most of the cases, this is all you need to do.

Step 6 - Save settings

Press the *[Save and Apply]* button to keep and apply your settings and you should be connected to your chosen WiFi network.
This can take a few minutes for all networking to restart, please be patient. If the page doesn't update properly, just choose *Network->WiFi* from the top menu bar again. You should see it now connected.

If you wish to return to the original configuration, you can go back to *RME->Preset Networking*, and choose the *"Ethernet Client"* model.

Editing WiFi Parameters

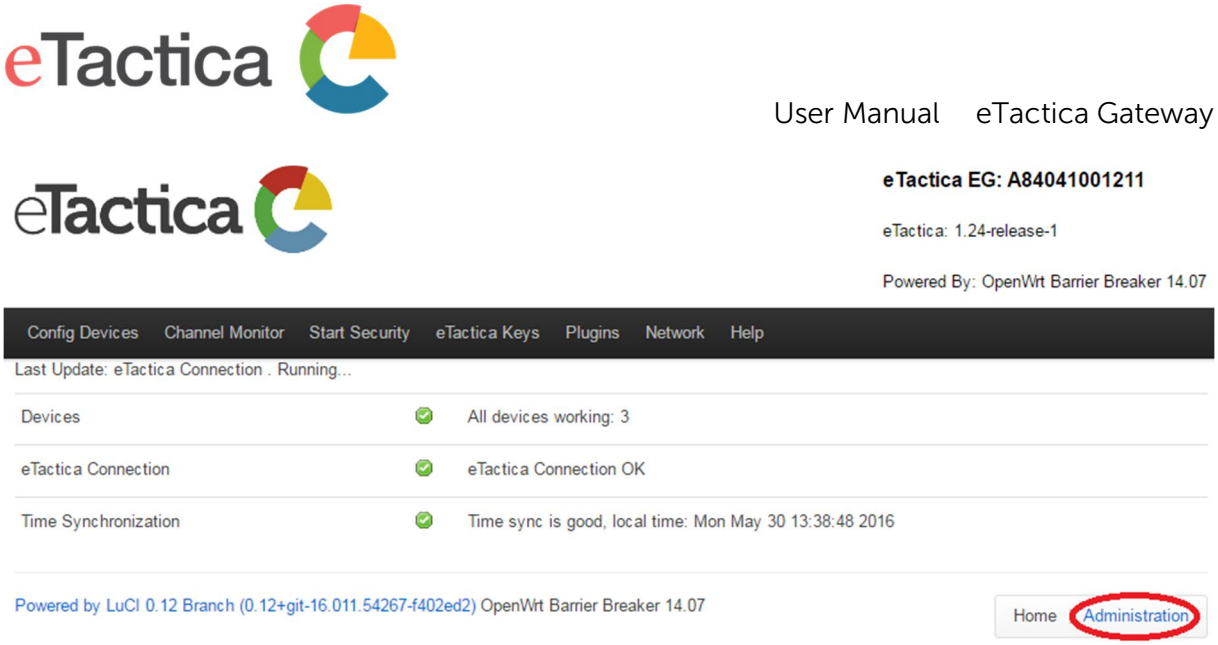
This section covers adjusting the SSID and TX power of your WiFi interface. These settings are rarely needed, but may be desired in high traffic locations to reduce interference and to reduce the range of allowed WiFi connections.

Pre-requirements

You are successfully connected to your gateway. If you are not connected yet, please see chapter 2, *Connecting to Gateway*.

Step 1 - Go to Administration page

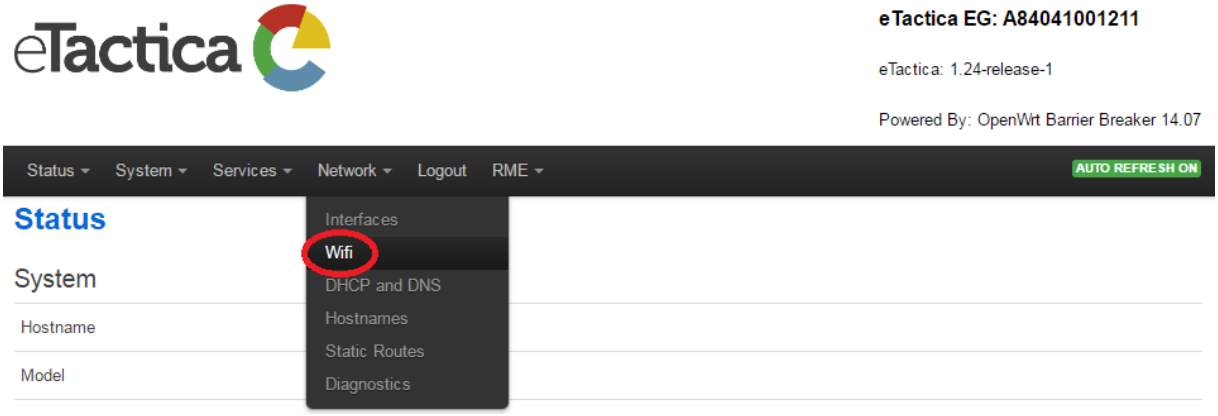
From the home page of the administration web console of your device, choose the *[Administration]* link.



This will require you to login, using the root password you have configured earlier. If not, please see chapter 9, *Password Settings*.

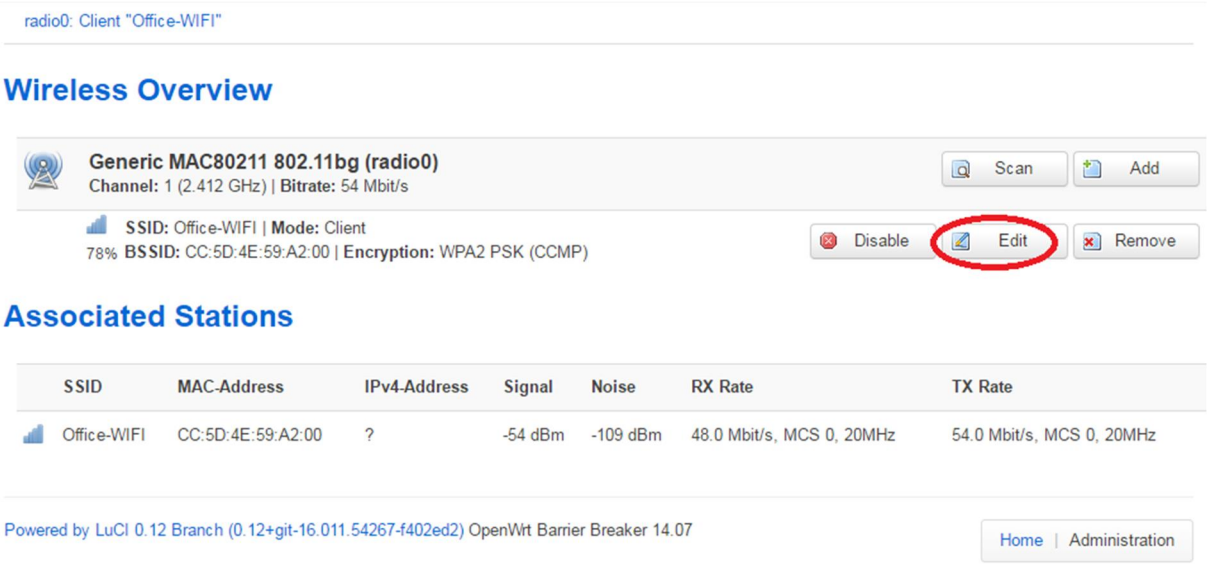
Step 2 - Go to the WiFi configuration page

From the top menu, choose *Network->WiFi*.



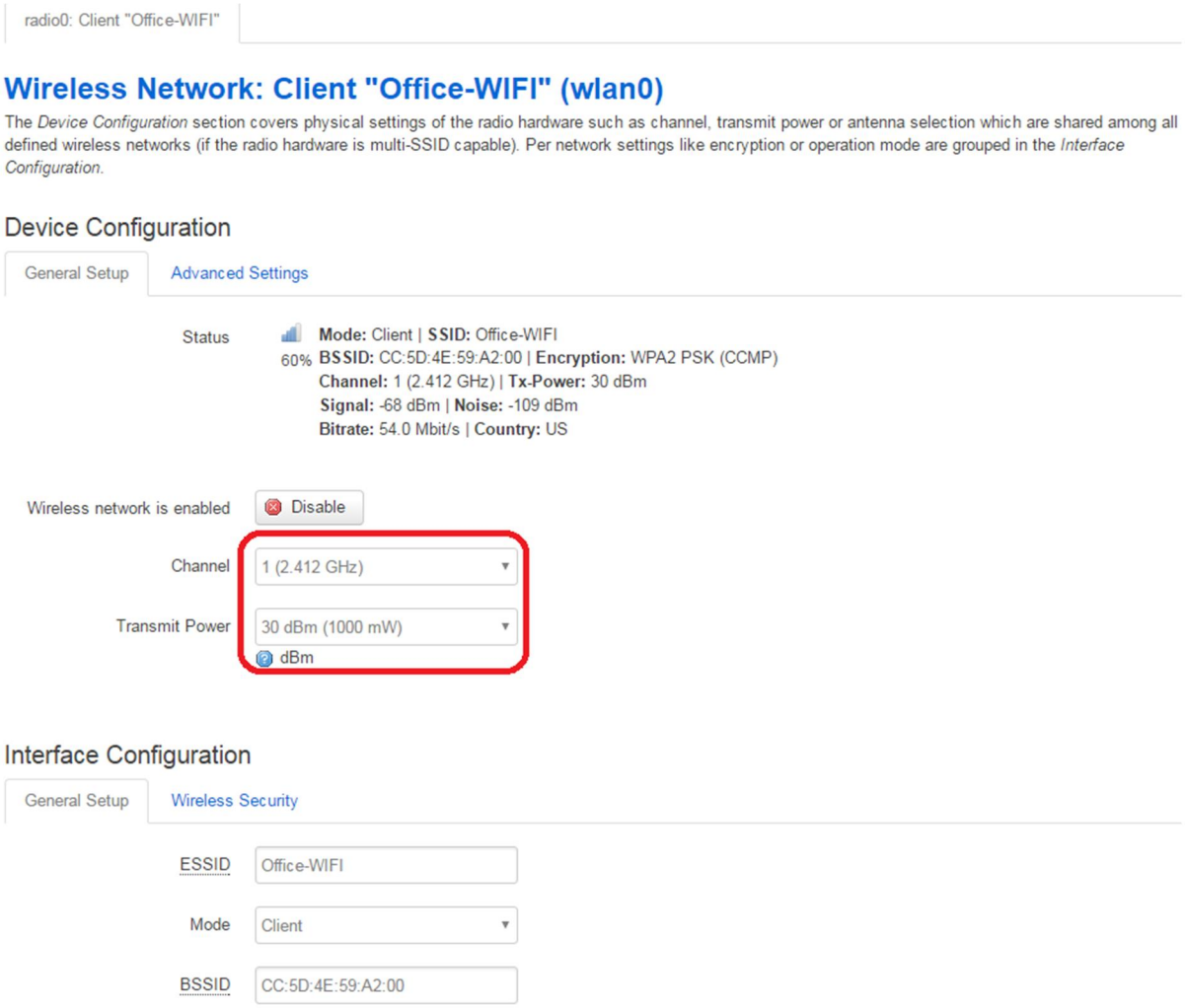
Step 3 - Edit the WiFi interface

Press the *[Edit]* button.



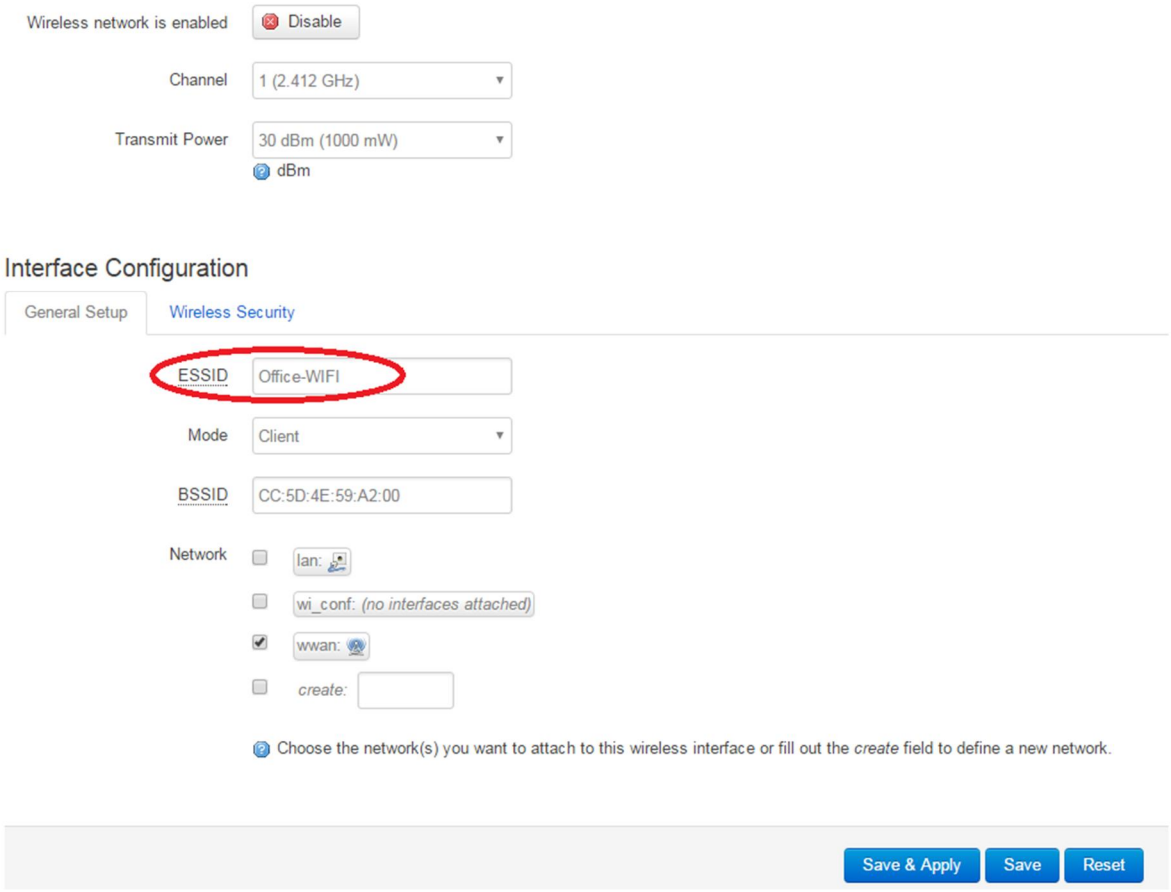
Step 4 - TX Power / WiFi Channel

The channel assignment and transmit power are set in the first section, but it is entirely site-specific configuration, so no advice or sensible defaults can be given here.



Step 5 - Change the (E)SSID

If you wish to change the SSID, to match a local naming policy, or simply to provide a helpful reminder of the location, (*Kitchen* , *Office 4B* or similar) the lower portion of the page allows this to be changed, along with other advanced WiFi settings.



Step 6 - Save settings

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

9. Password Settings

In this chapter, you find information on how to change password settings:

- Gateway root password
- WiFi secure access

Gateway Root Password

The default root username is on a new gateway there is no password set.

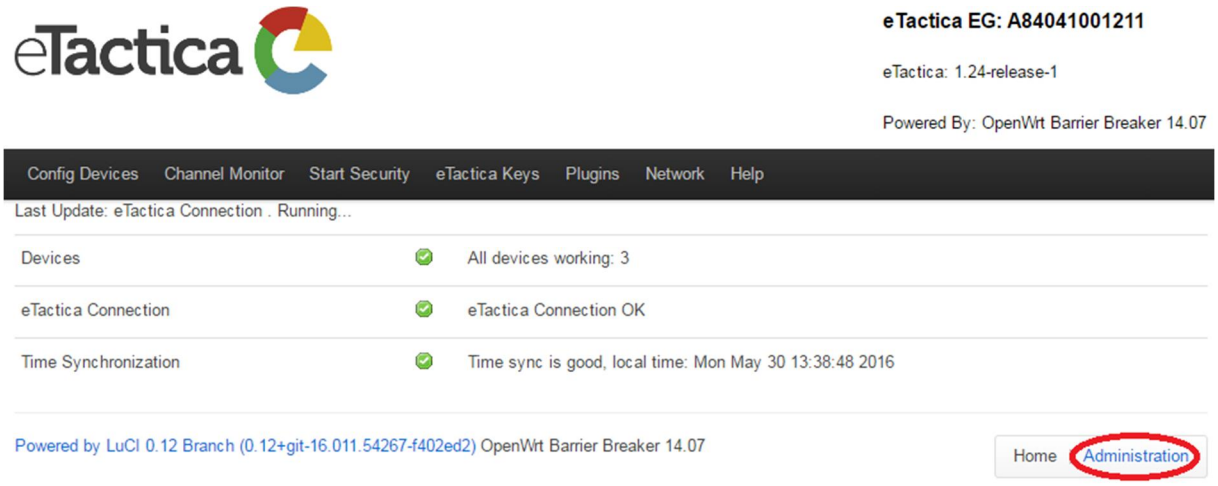
After you've logged in the first time, you SHOULD set the root password. In the following, you find a step-by-step guide, how to change it.

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

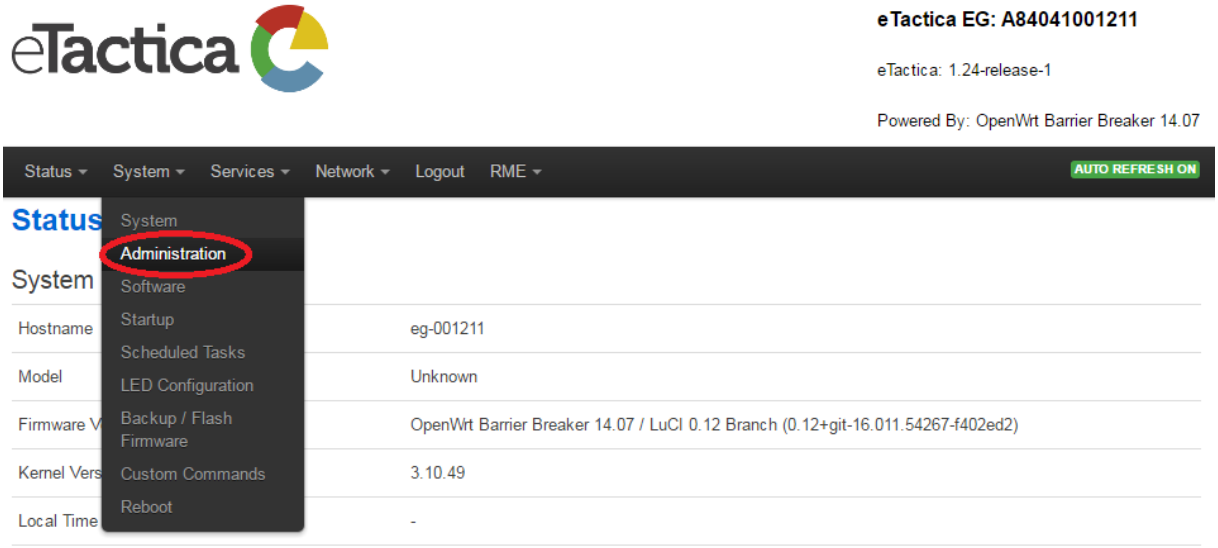
From the home page of the administration web console of your device, click on the *[Administration]* link.



You will be asked to login and if you haven't already set the password just press Return/Enter.

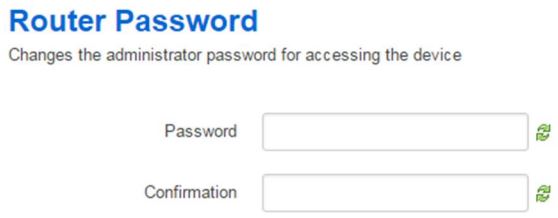
Step 3 - Go to Administration configuration page

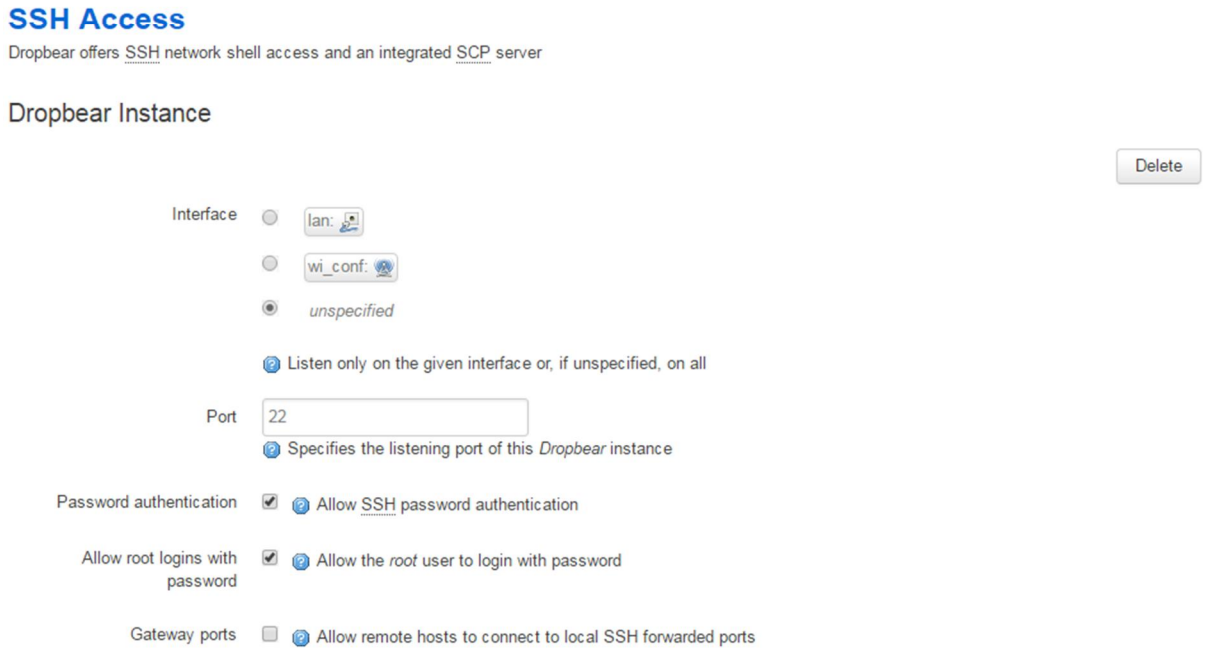
From the top menu, choose *System->Administration*.



Step 4 - Enter a new password

Enter new password. Note that the username is still "root".





You can also edit SSH settings here, for example to add a public key and disable password-based access altogether, or to ban SSH access from the internet.

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

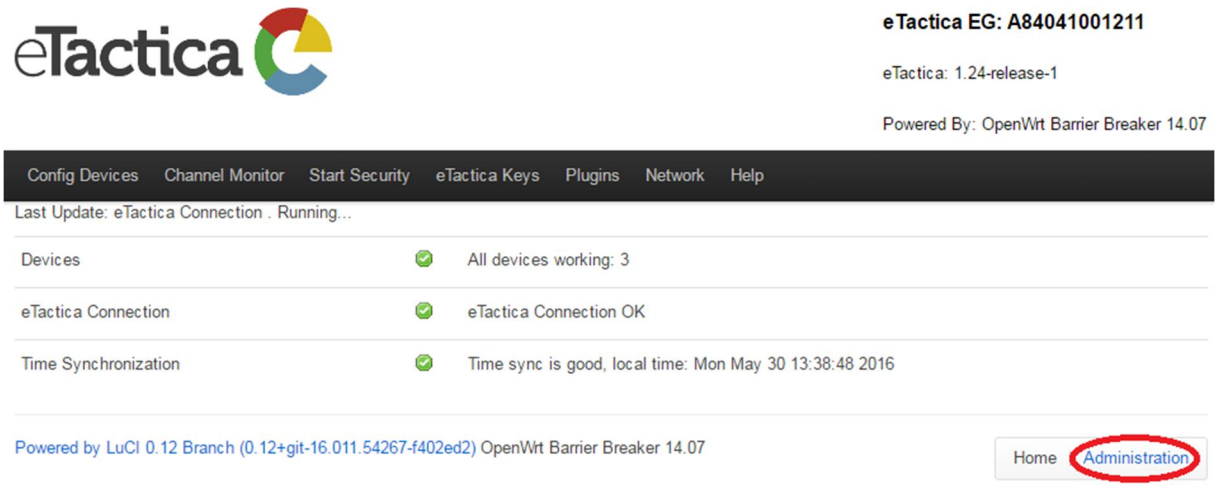
The following covers how to change the WiFi security password.

Step 1 - Connect to the Gateway

You need to be successfully connected to your gateway device. If not, see chapter 2, *Connecting to Gateway*.

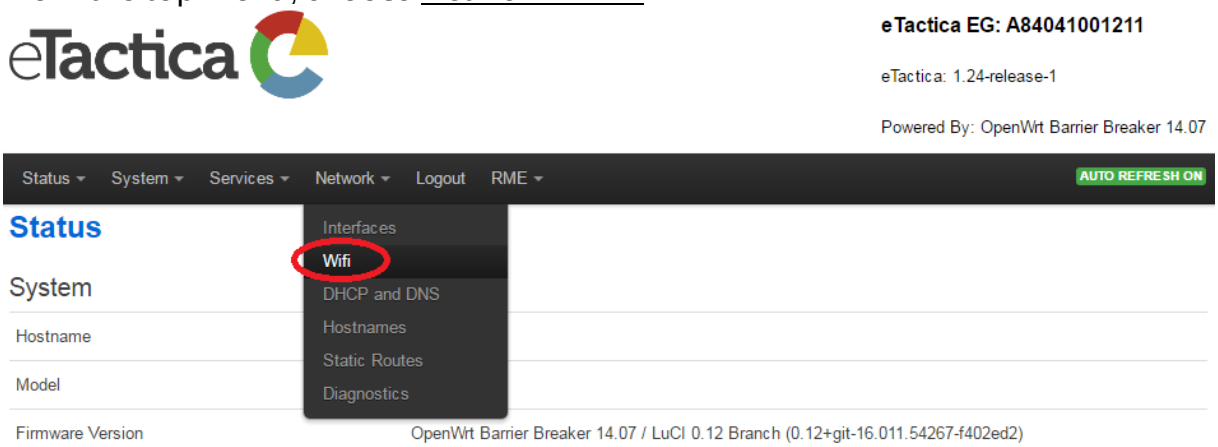
Step 2 - Go to Administration page

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



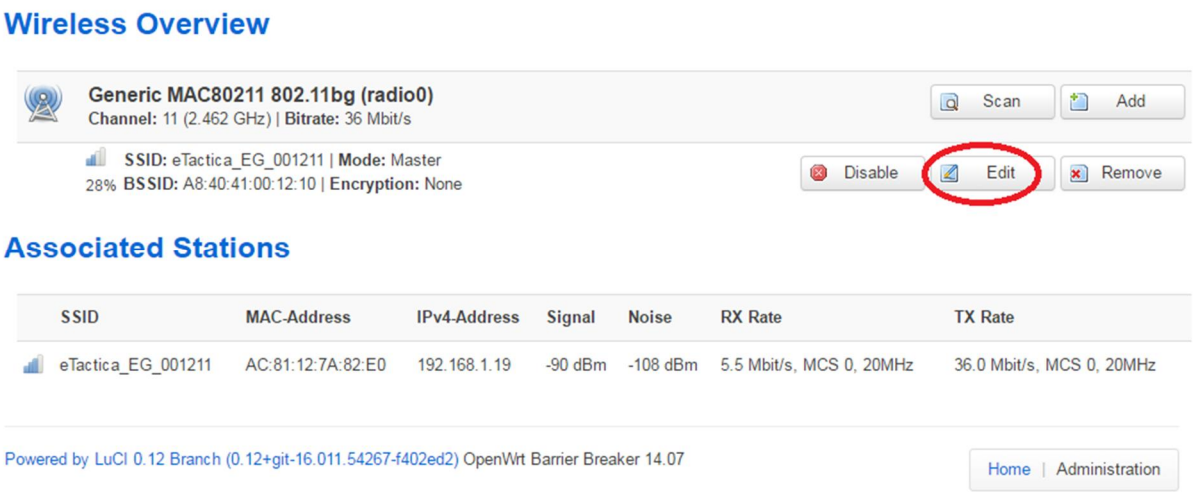
Step 3 - Go to WiFi configuration page

From the top menu, choose *Network->WiFi*.



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

Press the *[Edit]* button.



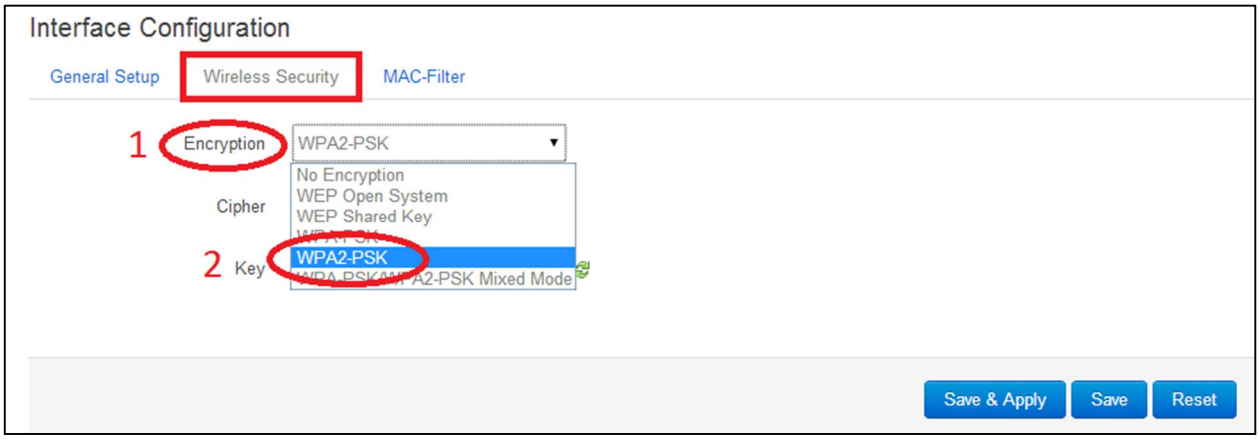
Step 4 - Change password

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

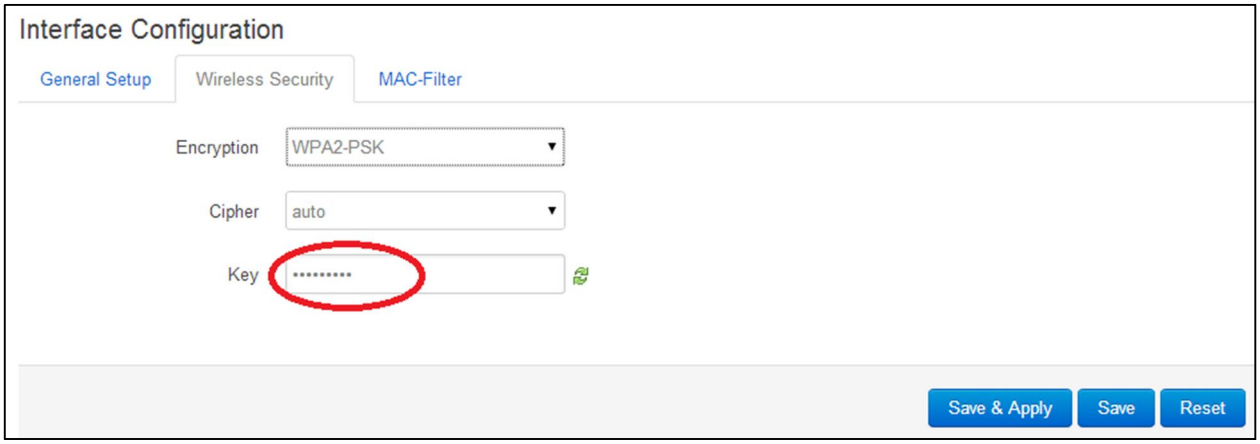
Here you have to:

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*).



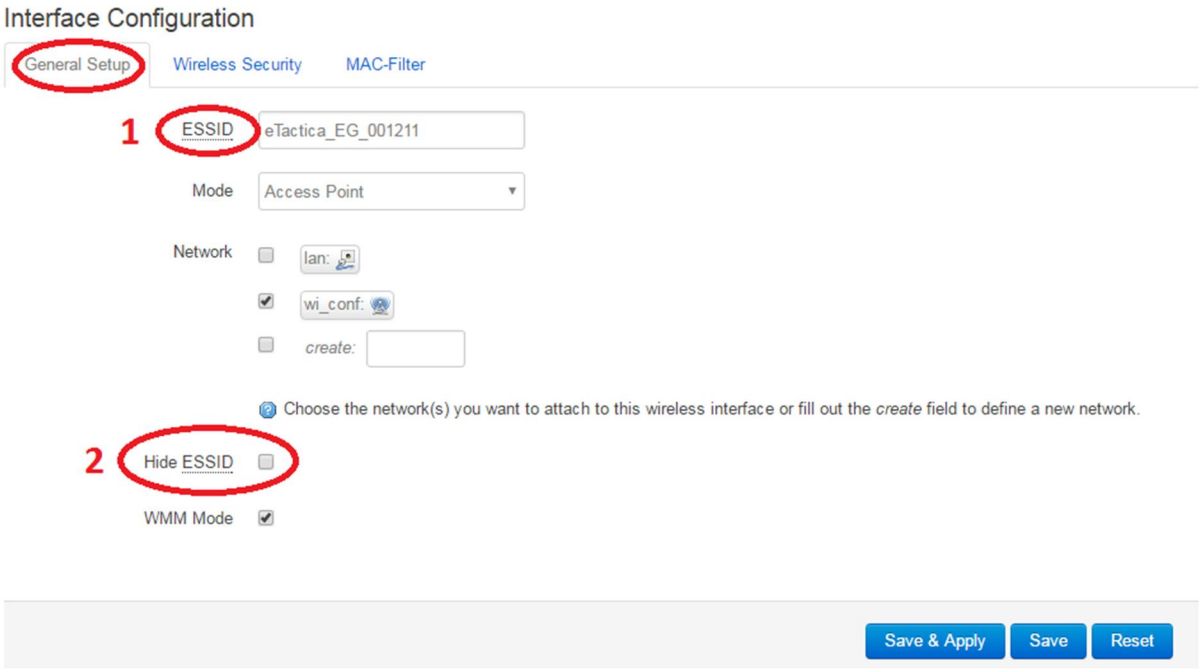
Then, you can change your password in the *Key* field.



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



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".

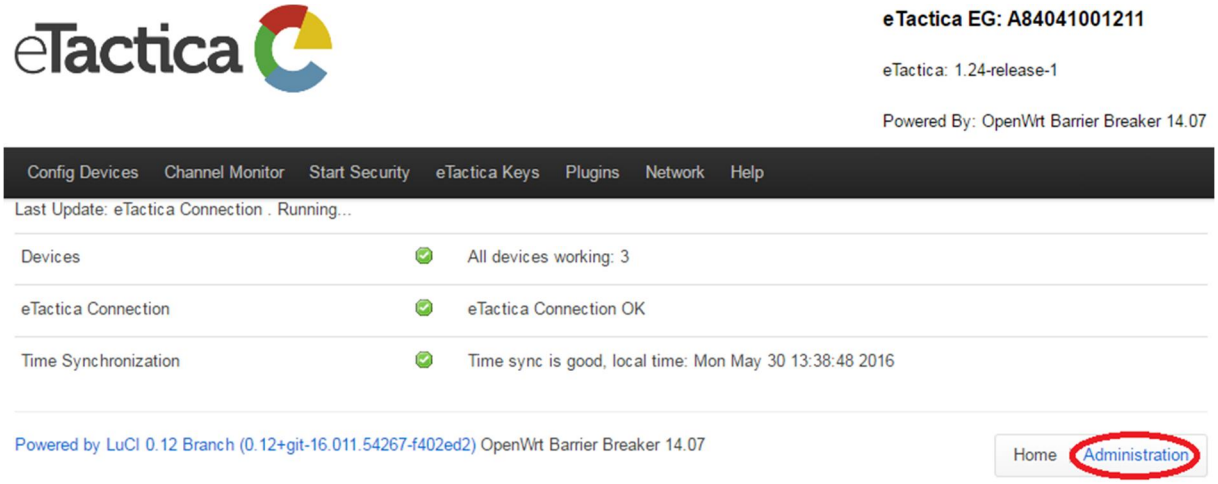
This service is disabled by default, but can be enabled as follows.

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

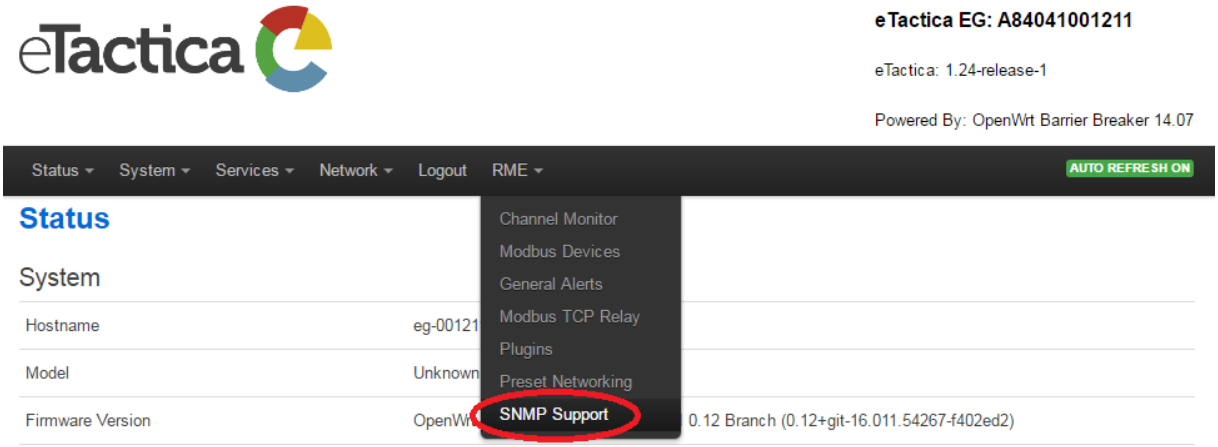
From the home page of the administration web console of your device, click on the *[Administration]* link.



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*.

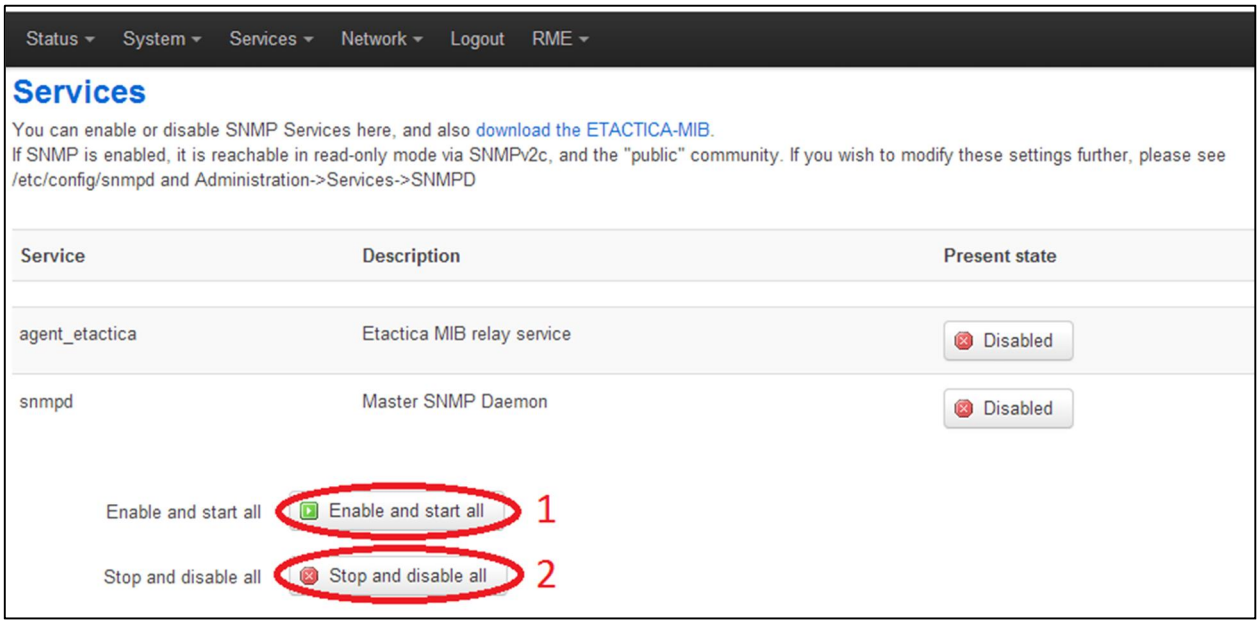


The SNMP Support page contains links to the MIB file for use with third party SNMP tools such as *nagios*. The latest version of the MIB is always available at: http://packages.etactica.com/snmp/ETACTICA-MIB.mib.

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.



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

Configuration (basic)

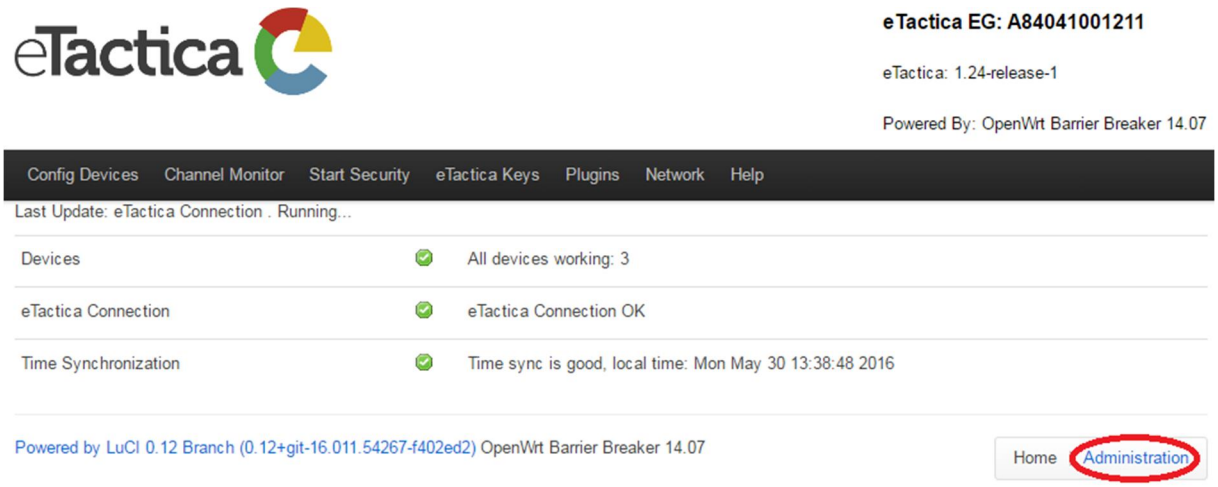
The SNMP daemon has *many* configuration settings, and they are all considered *advanced* topics. Some basic support is available via the administration web console, described in the following.

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

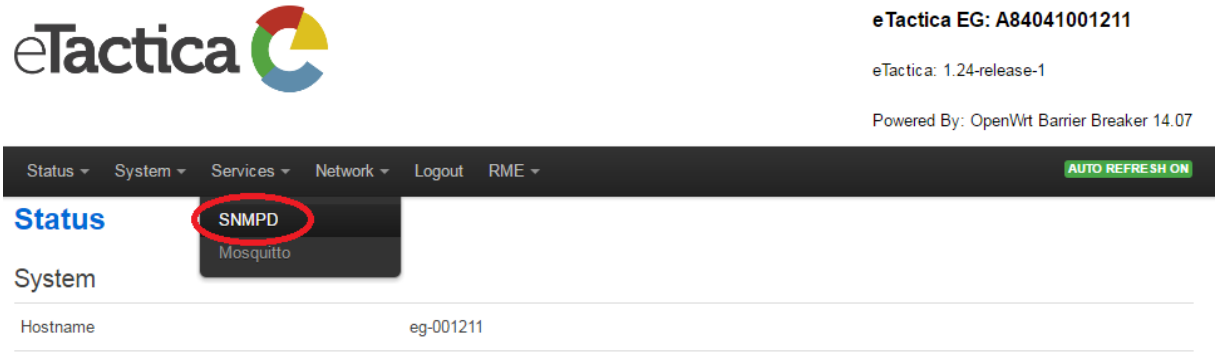
From the home page of the administration web console of your device, click on the *[Administration]* link.



This will require you to login, using the root password you have configured earlier. If not, please see chapter 9, *Password Settings*.

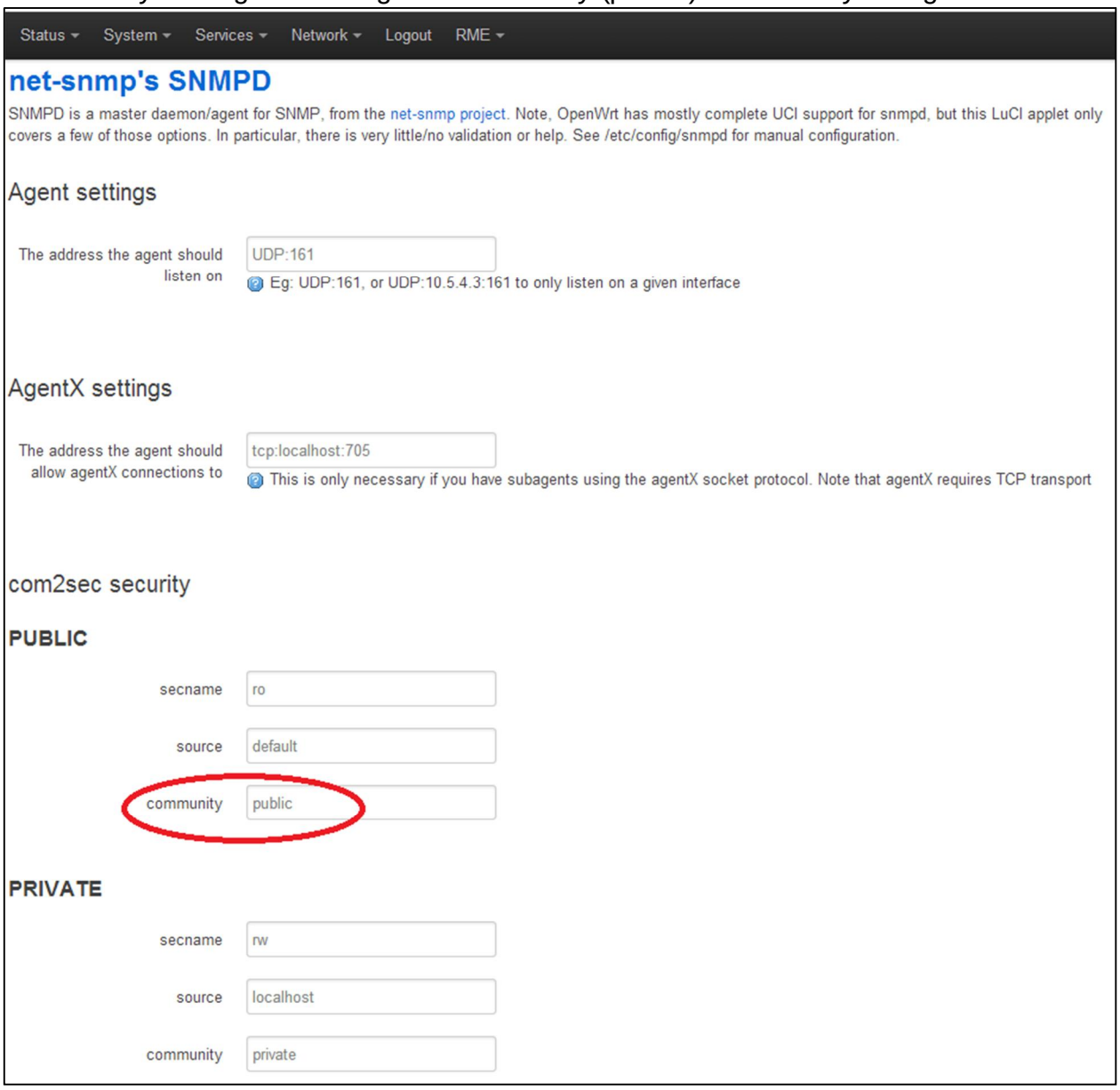
Step 3 - Access the SNMPD configuration page

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
```

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       ?           ?
```

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.

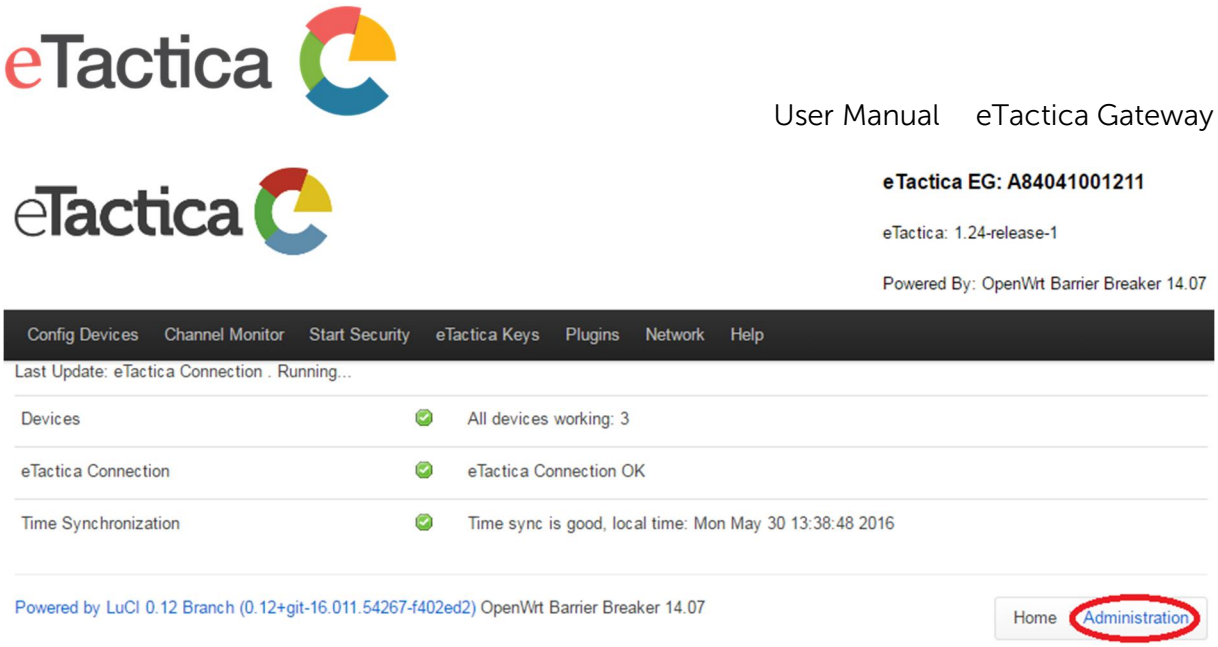
Now move on to the upgrade process.

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

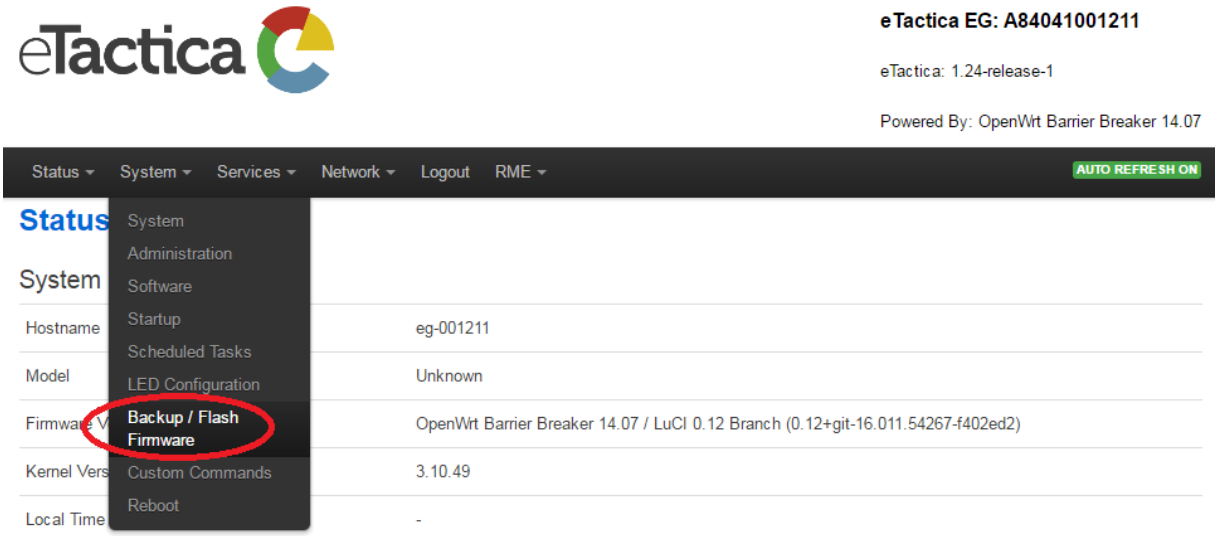
From the home page of the administration web console of your device, click on the *[Administration]* link.



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

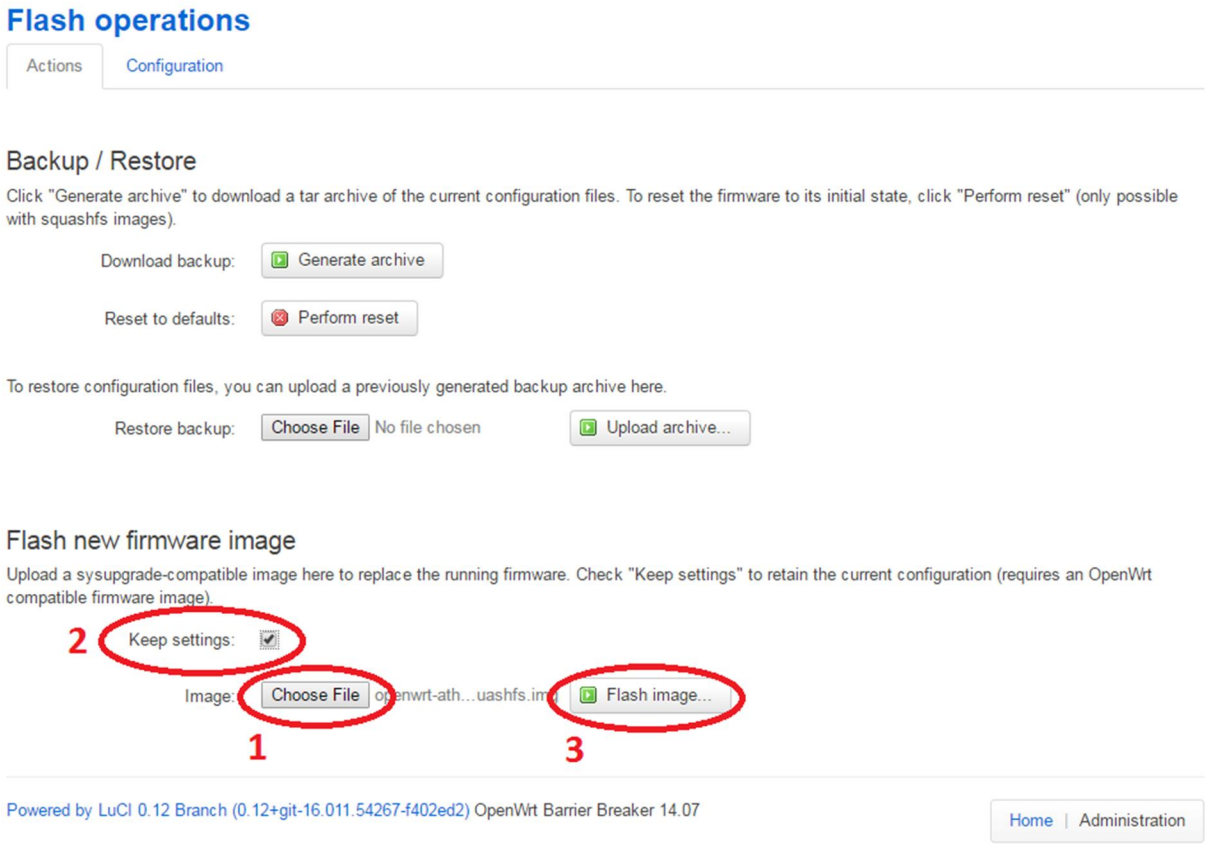
From the top menu, choose *System->Backup/Flash Firmware.*



Step 4 - Get image file

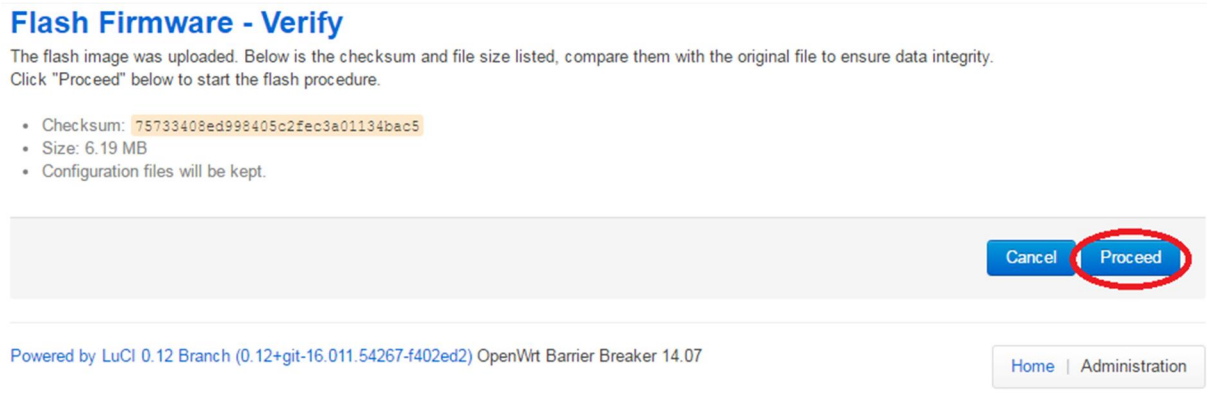
Locate the *Flash new firmware image* section and follow this procedure:

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.



Step 5 - Verify integrity and flash image

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



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.

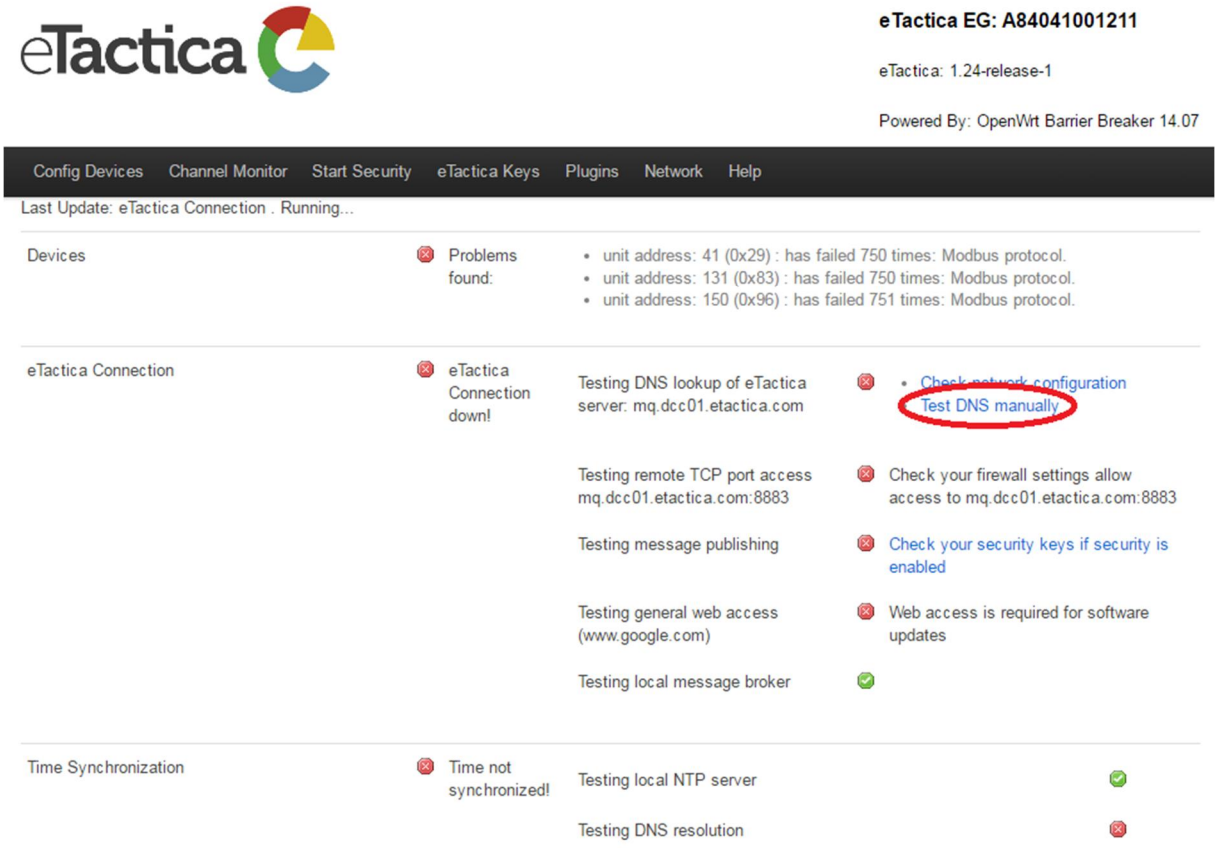
Most of these tests depend on your Internet connection being properly configured and connected, see *Network Requirement* in chapter 1, *Introduction*.

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.

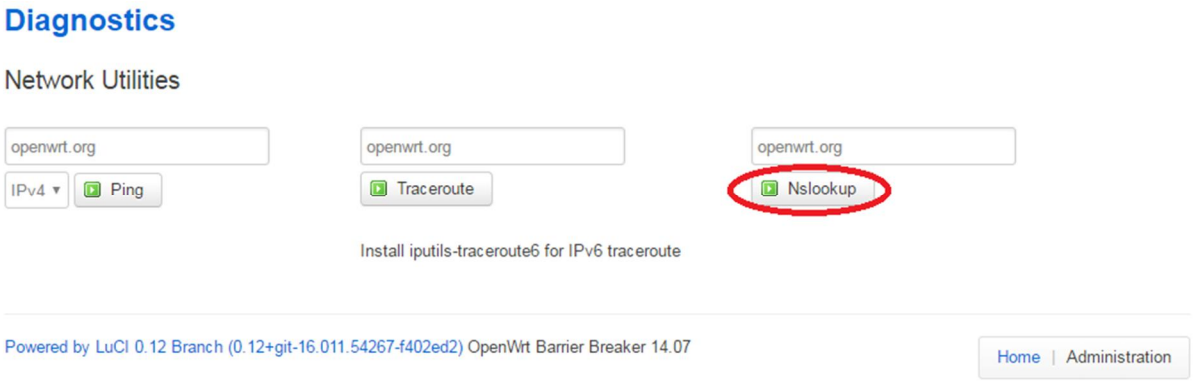
1) Testing DNS lookup of eTactica server

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.



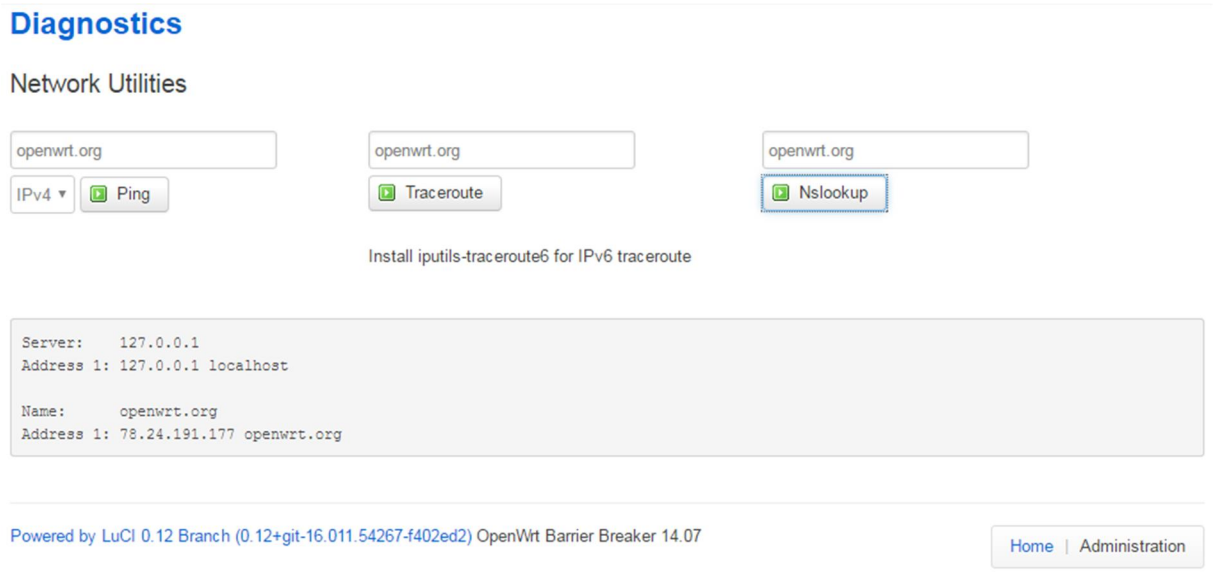
For further diagnosis press the link *[Test DNS manually]*.
This will require you to login, using the root password you have configured earlier. If not, please see chapter 9, *Password Settings*.

This screen appears, offering three different network diagnostic tools.



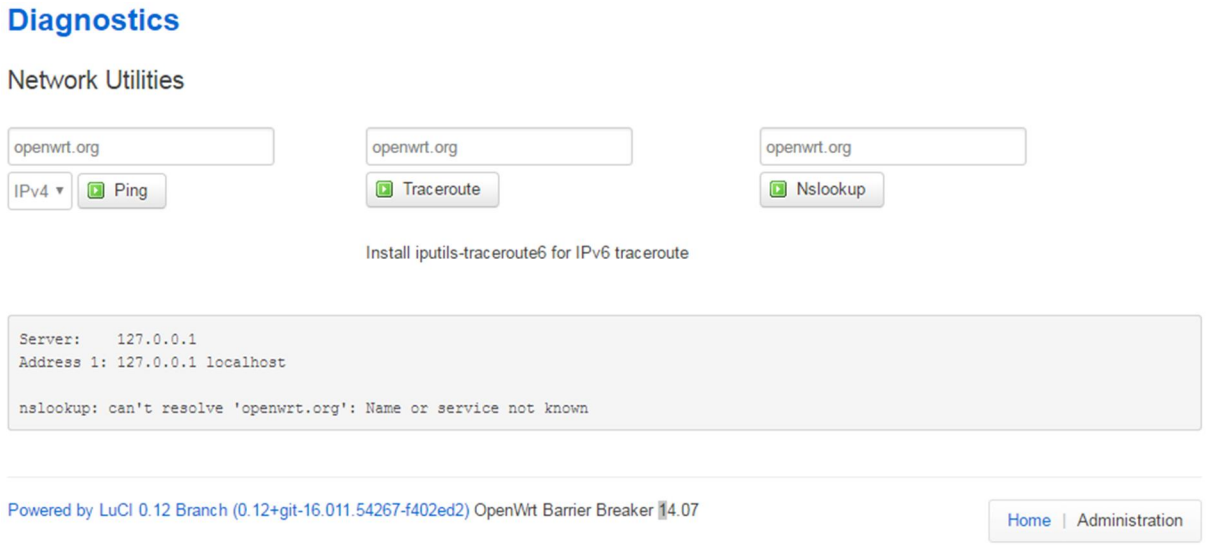
To test DNS resolution, either press the *[Nslookup]* button, using the default name or enter any name that should exist, such as www.google.com or www.ibm.com.

If everything OK you will see this screen.



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.



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.

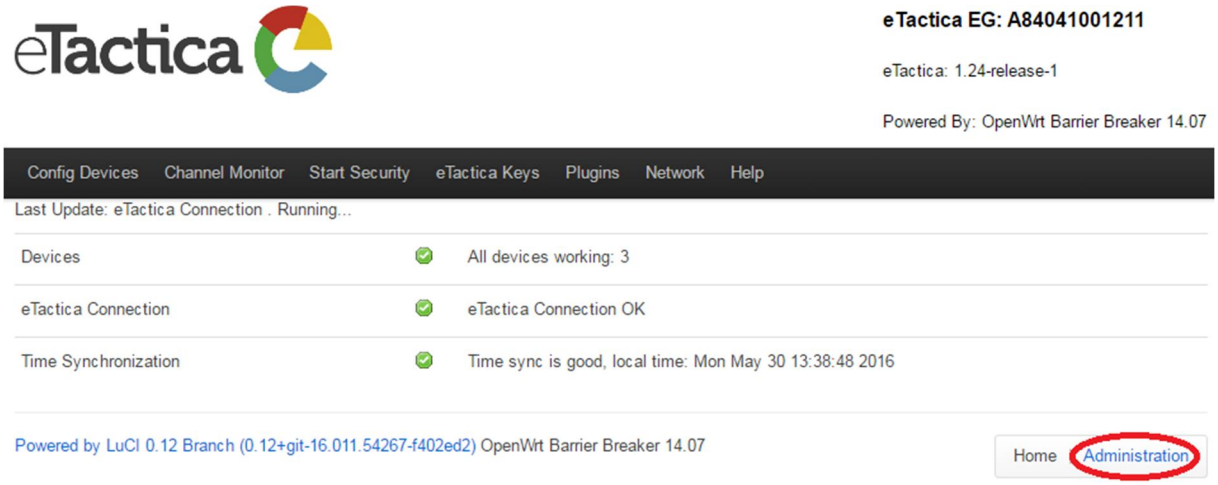
Please follow the steps below, to do that.

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

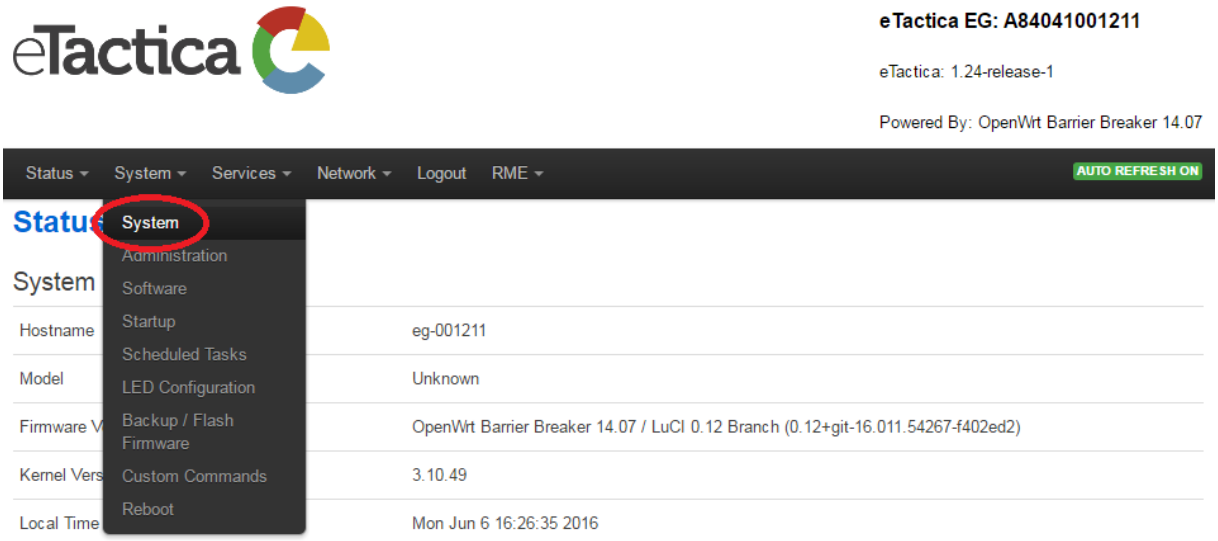
From the home page of the administration web console of your device, click on the *[Administration]* link.



This will require you to login, using the root password you have configured earlier. If not, please see chapter 9, *Password Settings*.

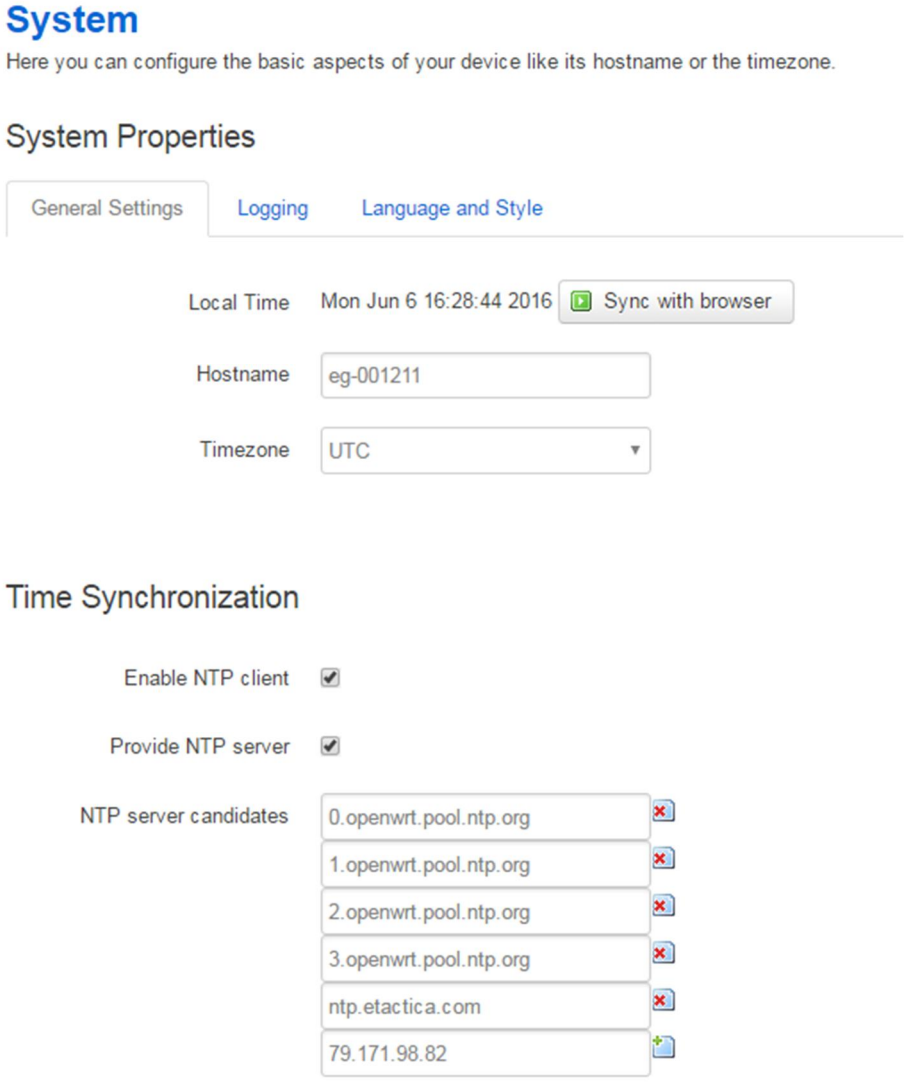
Step 3 - Go to System setup

From the top menu, choose *System->System.*



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.



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.

Reset

Soft reset

The reset button on the back of your gateway device, can be pressed once to simply reboot the gateway.

Factory reset

If you hold the button down for more than 5 seconds and less than 30 seconds, the gate will reboot and restore factory default settings.

13. Revision history

Revision	Date	Description	Responsible
1.0	2013	Initial Document	Fanny Mousseau Karl Palsson
2.0	---	Review editing	Karl Palsson
3.0	---	Layout editing	Fanny Mousseau
3.1	29.10.2013	Modbus TCP/RTU bridge support, disable Wi-Fi option	Gestur Palsson
3.2	19.12.2013	Remove the egate option, edit disable breaker feature, document review	Gestur Palsson
4.0	19.09.2014	Major review, layout and features according to firmware releases. Final document review.	Gestur Palsson Karl Palsson
4.1	11.08.2016	Various things updated, e.g. plugins Channel Monitor and troubleshooting, EG-200 added.	Ragnar Einarsson