eTactica

MODERN ENERGY MONITORING

User Manual

eTactica Gateway – EG-200

V4.2

5.12.2018

WE MAKE ENERGY MONITORING SIMPLE

eTactica
Hlidasmari 14, 201 Kopavogur, Iceland
+354 535 3000

eTactica Gateway – EG-200

Table of Contents

This is the user manual for the eTactica Gateways, valid for the products marked as EG-200 and firmware release 2.8.1. 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) and the eTactica Power Bar (EB).

The EG collects and analyses your energy data, measured by the EM and the EB. 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 Wi-Fi 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-200 uses an external power supply 12-24VDC, minimum 1,1A to power itself 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 (2 unit)

Network Requirements

The Gateway has some network requirements for proper operation. We recommend that you talk to your IT department before installation, so they can have their part ready.

DNS access

We expect to have DNS access available. How you configure your network and the EG's network interfaces (Wi-Fi 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

To send data with reliable time stamps an NTP server is needed. 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 13, Troubleshooting.

HTTP and HTTPS access

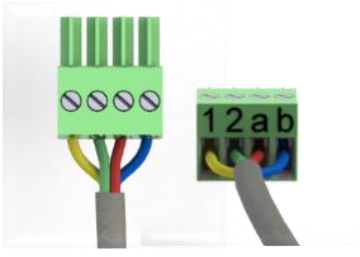
This is required for secure messaging, but optional for insecure messaging.

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.

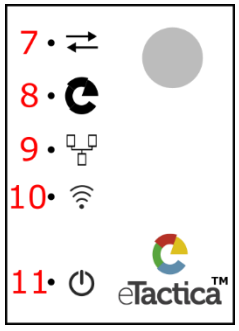
Device bus connector

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

[1]	DC Power, 12-24VDC@700mA
[2]	GND
[a]	RS485 A
[b]	RS485 B



EG-200	
OS	32-bit Linux
Network communication	Ethernet TCP/IP (10/100Mbit) Wi-Fi (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	12-24VDC@700mA, same as input voltage
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	12-24VDC 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
Standards	EN 61326-1 EN301-489-1-9-2 EN 61000-3-2 EN 61000-3-3



1. RJ45 LAN connector (Ethernet)
2. Power input 12-24VDC
3. Device-bus connector
4. Status LEDs (7 - Modbus, 8 - eTactica online, 9 - Ethernet link, 10 – Wi-Fi, 11 - Power)
5. External Wi-Fi antenna
6. Reset button (accessed through an opening on the enclosure)

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 basic setup.

Most commonly, this is done using the Wi-Fi interface. By default, every Gateway comes with an open Wi-Fi 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 Wi-Fi

Step 1 - Connect to Wi-Fi hotspot

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

You will be asked for a password as the gateway comes preconfigured with one. It is on a label on the right side of the gateway.

Step 2 - Visit the administration web console

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

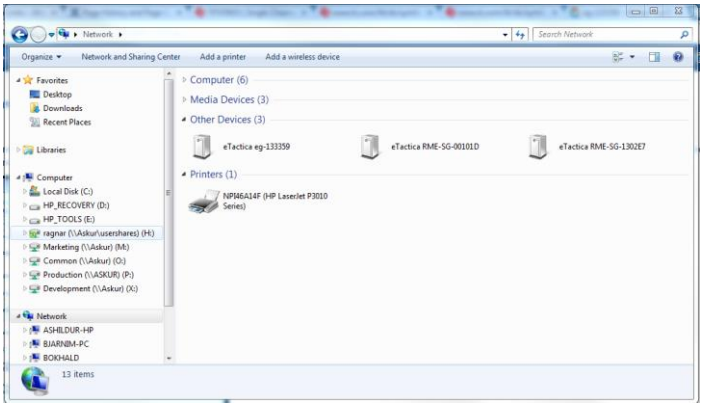
Connection via Ethernet

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.

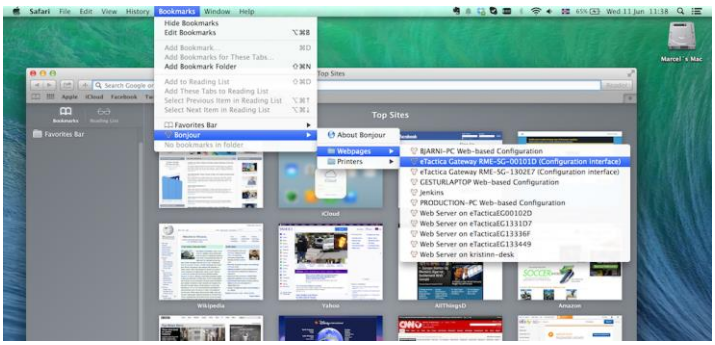
The name of the device shown here, will also match *'eTactica eg_xxxxxx'*, where -xxxxxx is a unique number for each gateway device.



OS X

On OS X, 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/.



This feature has been removed in Safari 11 and later version, but there are other tools available to find IP addresses of devices on network, e.g. by using the Terminal or some apps.

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

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. Basic Configuration

The following chapter describes the steps needed for a basic configuration of your eTactica gateway. If you need to do some further configuration, you may simply proceed as documented in the rest of this manual. However, for the vast majority of installations it should be enough to go through the steps in this chapter.

There is a wizard that will guide you through the first steps:

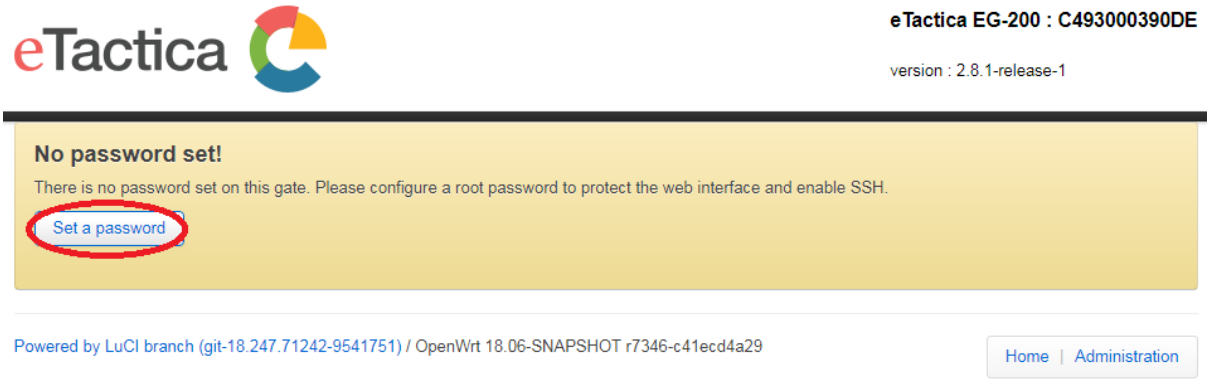
- The root password for your device
- Networking password
- Configuring Modbus device list (if you have third party devices)

If you have only eTactica devices, the "Scan-on-start" feature will automatically search for and configure them all in the first few minutes after starting a gateway that has no configuration.

Further steps needed for eTactica devices:

- Set up cabinet model
- Set CT sizes
- Start secure connection

Step 1 - Starting Wizard

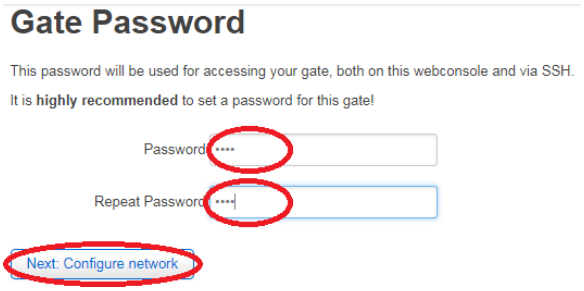


This is what will appear when you have connected to a gateway with no configuration. Simply press the *[Set a password]* button.

Step 2 - Setting Root Password

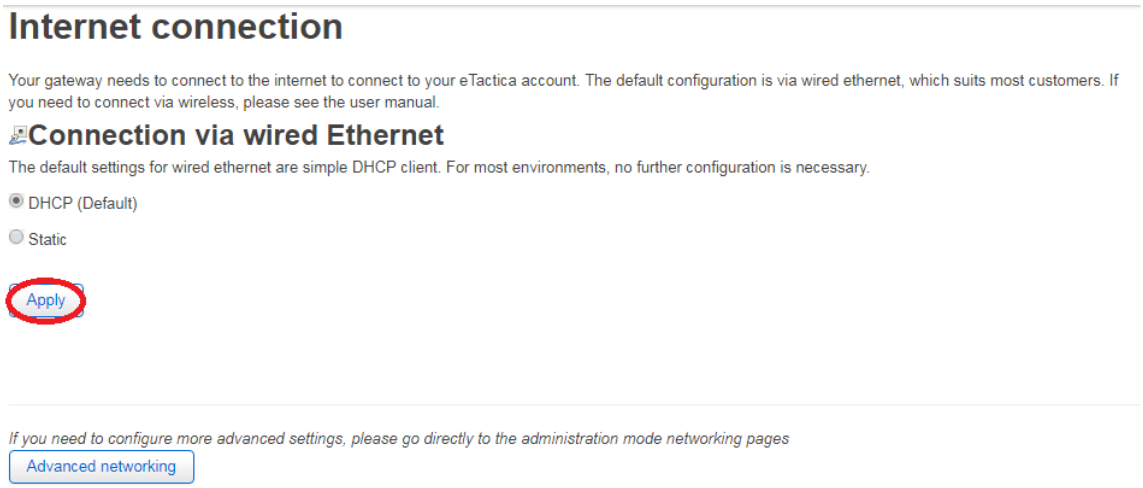
The root password is used to log in to the gateway. The root password also provides SSH access to the device. As always, you should use a good password here.

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



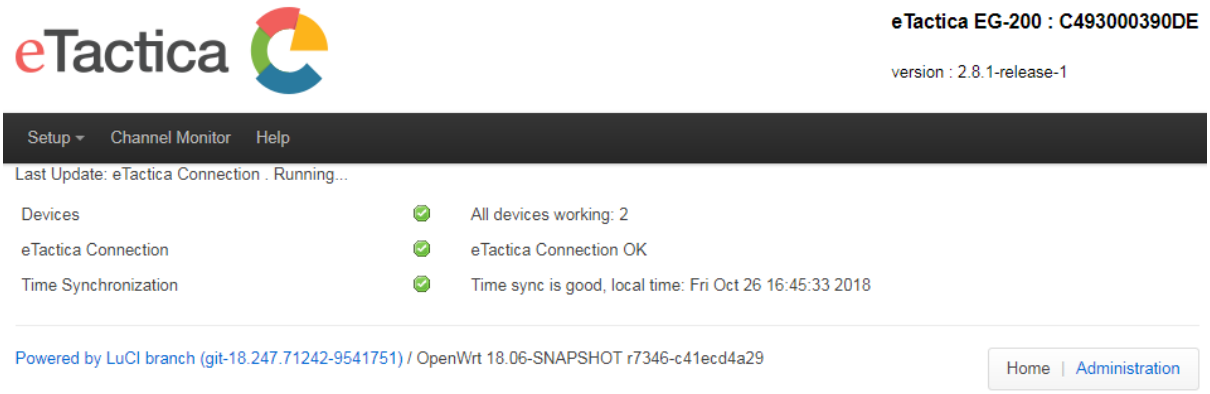
Step 3 - Configure Network

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, press *[Apply]* and then *[Continue]* when settings have been saved.



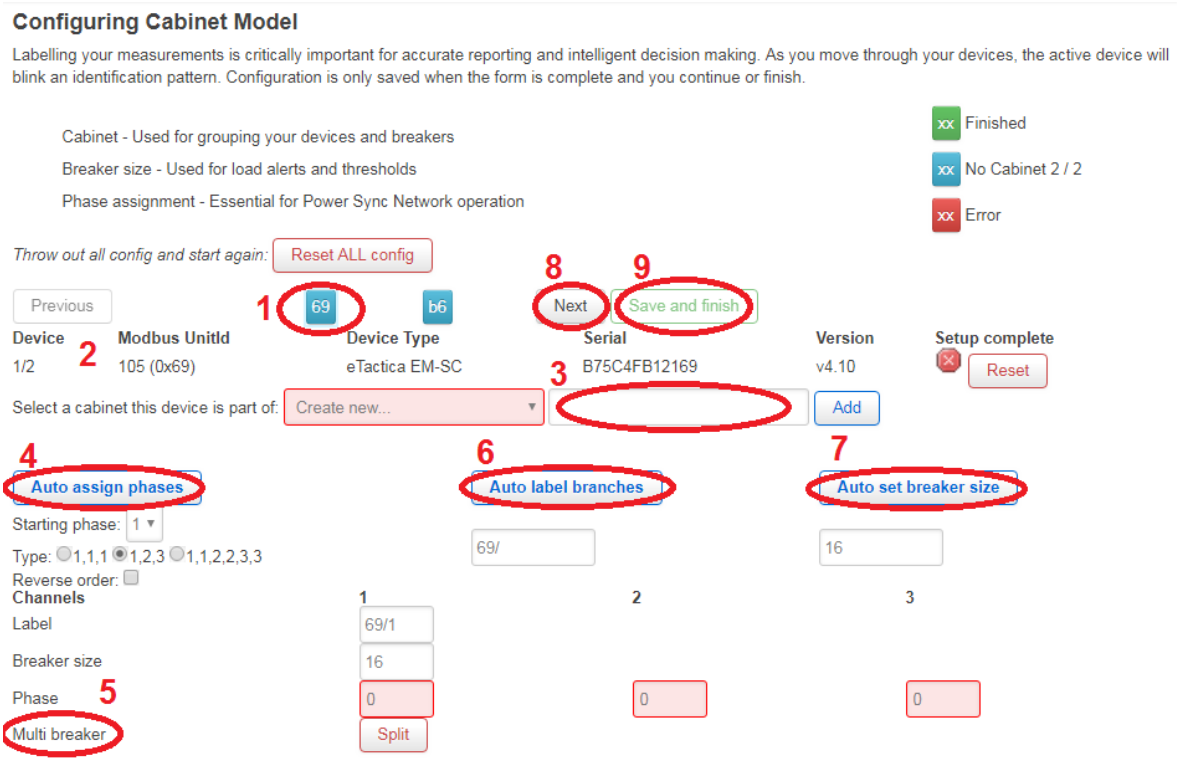
Step 4 – Home Page (Diagnostic page)

You will be transferred to the home page (the diagnostic page). Here you should see three green tick marks that show that device reading, connection to eTactica web server and time sync is ok. Check that the number of working devices is corresponds to the number of devices you have installed. If there are red "X" instead of green ticks, go to the troubleshooting section in this manual.



Step 5 – Configure Cabinet Model

The cabinet model specifies the properties of the devices, what cabinet they are in, name and size of the branches and phase assignment. This is needed for the Power sync network and it will also be used at the receiving end of the measurement data to get some meaningful information from the data.



From the top menu choose *Setup->Cabinet Model.* There is a list of configured devices, ordered by their Modbus addresses (*Unitd*), the first one will be flashing, showing that it is the one being worked on (1). Below the list is information about the active device (2). They will all be in blue, which means they are not in any cabinet. Start by naming a cabinet (3)

and click *"Add"* and the active device will be put in that cabinet. It is possible to have more than one cabinet on a gateway, just select *"Create new.."* and add another name.

Next job is to assign phases. You can use *[Auto assign phases]* if one of the options fits your setup (1, 1, 1; 1, 2, 3; 1, 1, 2, 2, 3, 3). You can also change the starting phase, e.g. 2, 3, 1, 2, 3, 1. Then click on the *[Auto assign phases]* button (4) to assign phases. If you have an unusual setup, just fill in the phase number for each channel in the table at the bottom.

If there are three phase breakers on an EB, it is possible to merge the channels for that breaker in the model. Click on the *[Merge]* button (5) for the first channel of the breaker and the three channels will be treated as one, except for phase assignment. You can split them up again if needed. EMs are merged as default but can also be split up.

Next is labeling of channels, the default option the Modbus address and then the channel number. Instead of the Modbus address, you can type in your own label and click on the *[Auto label branches]* button (6) and all branches will be labeled with your label and channel number. It is also possible to label each branch manually.

Then set breaker sizes. You can set all at once by typing in the amperage in the field below the *[Auto set breaker size]* button (7) and then click the button. To set individual breaker sizes, fill in the table at the bottom.

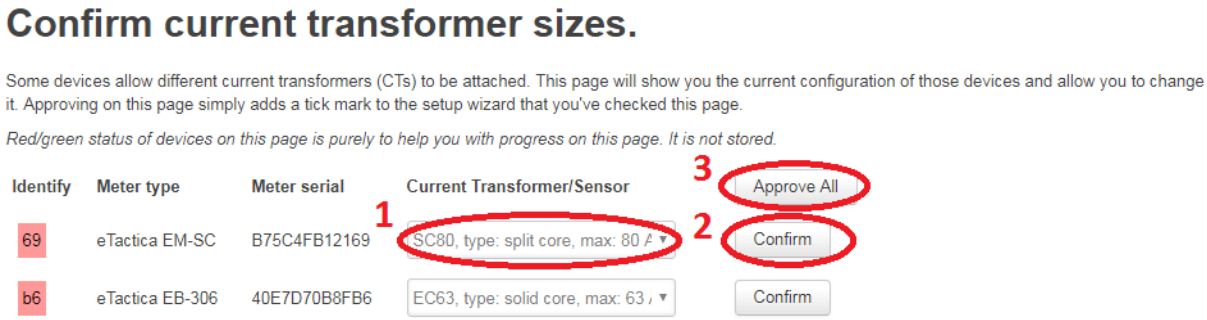
When you have configured everything for one device, click the *"Next"* button (8) and repeat for the next device and so on until you finished the last one, then click on *[Save and finish]* button (9) to save the cabinet model. All the Modbus addresses should now be green, indicating that everything is ok.

If you need to change something you can click the *[Reset]* to clear the active device or click *[Reset ALL config]* to start from the beginning.

Step 6 – Confirm Current Transformer Sizes

Here you see what current transformers are set up on your eTactica devices and change if necessary. The standard CTs for EBs are 63A solid core CTs, type EC-63, but it is also possible to use eTactica 80A, 200A and 500A split core CTs. EM-SC can use the same split core CTs. EM-FC can use eTactica 1000A, 2000A and 3000A flexible coil CTs.

From the top menu choose *Setup->Confirm CT sizes.* Check what CTs are configured for each device and if needed change by clicking on the drop-down menu (1) and select the correct one. Then either confirm for each device (2) or approve for all devices (3).



Step 7 – Secure Connection

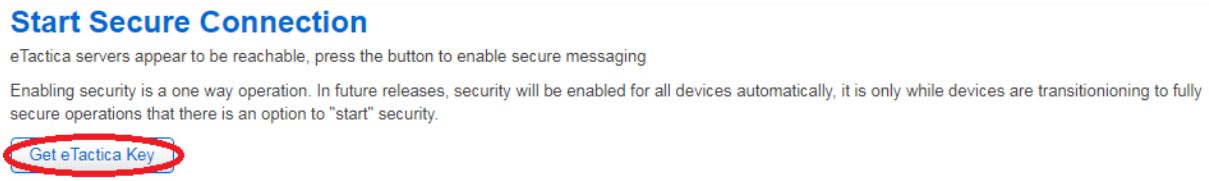
Here you find information to enable secure connection. This makes all communication between your eTactica gateway and the eTactica host securely encrypted.

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

From the home page on your device, select *Setup->Start Security* from the top menu.

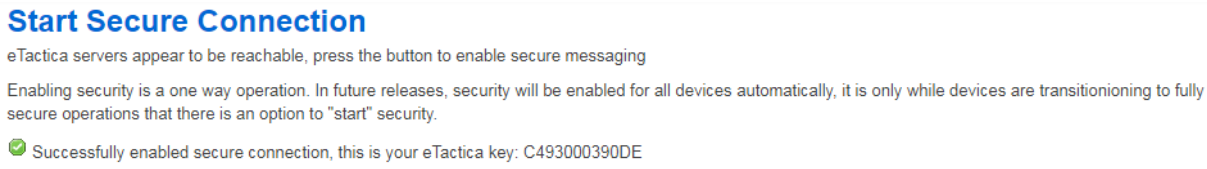
Step 8 - Start Secure Connection

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 9 - Completed

This completes your basic configuration.

4. Device Configuration

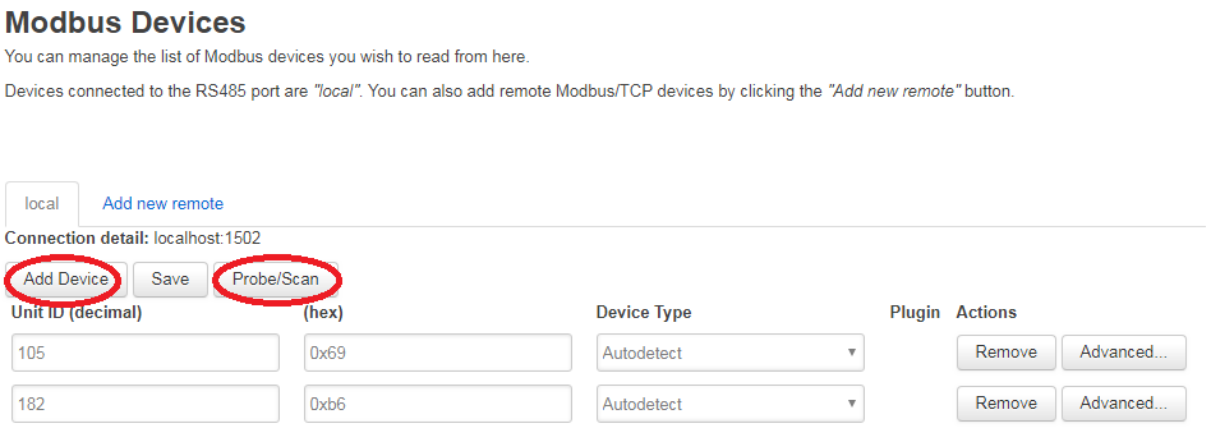
The following chapter describes how to add a Modbus device to the list of connected devices. This is done by entering the Modbus address of your device/s to the list, either manually or automatically by scanning. The *"Scan on start"* feature should find all connected eTactica devices when a gateway with no configuration is started. If you have some third party measuring devices or are adding eTactica devices at a later time, go through the steps in this chapter.

Pre-requirements

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

Step 1 - Choose "Config Devices"

Please choose *Setup->Config Devices* from the menu on the home page and you will see the following screen.

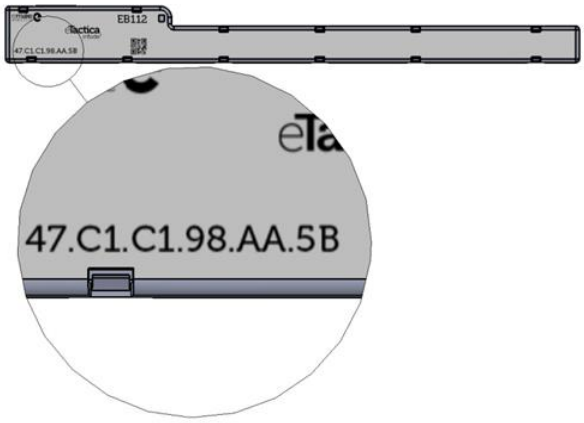


Step 2a - Manually enter the device address

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

The Modbus addresses are fixed for all eTactica devices and are based on the Device ID (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.

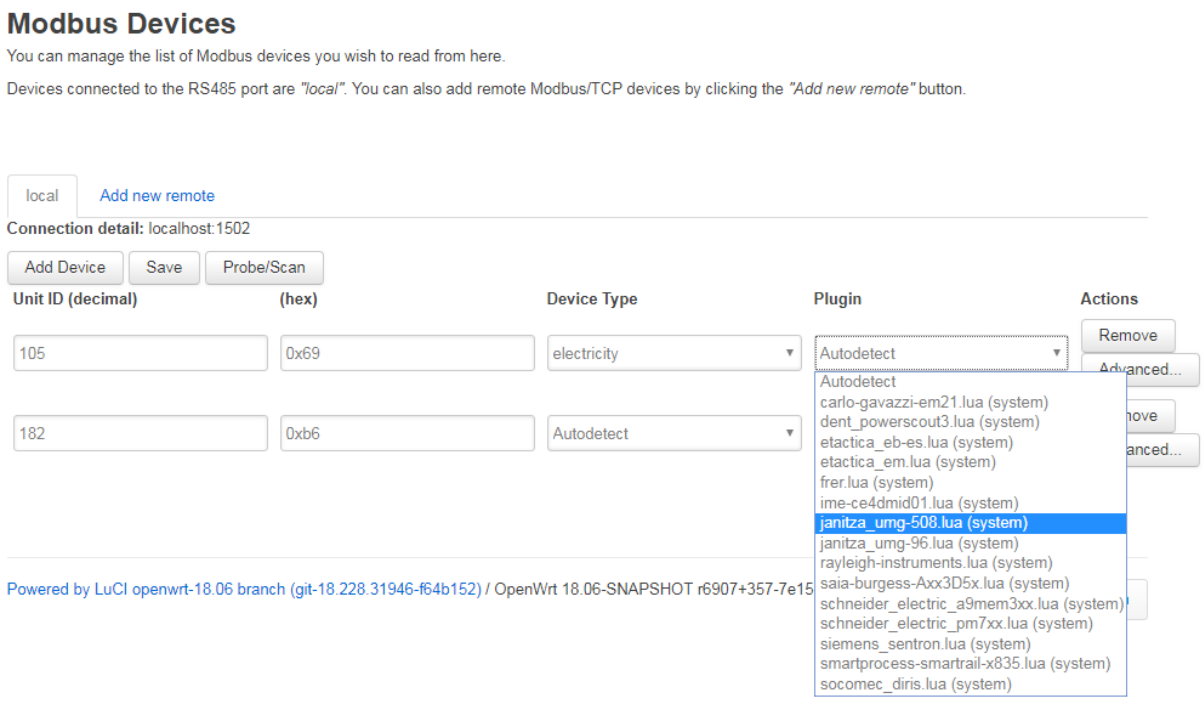
Example:

If the unique ID for your EB-312 device is "47.C1.C1.98.AA.5B", then the Modbus address is 5B.

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.

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 values 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

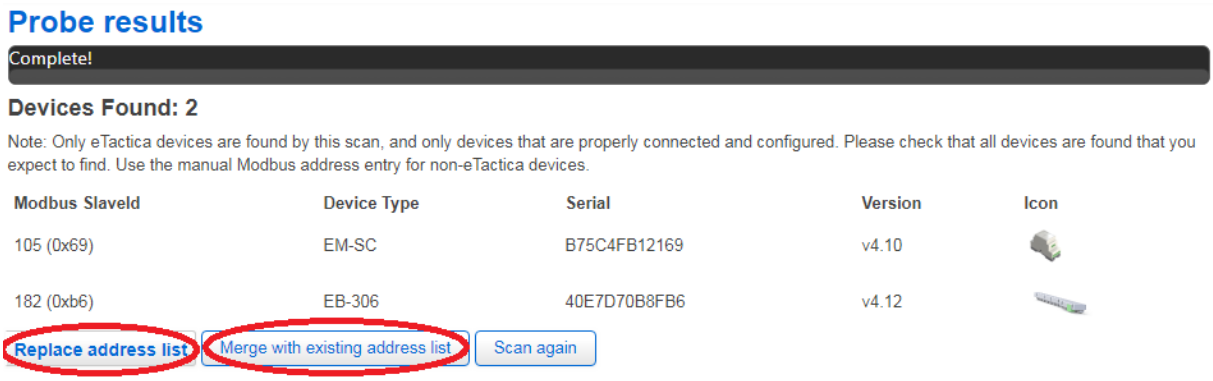
If you have many devices, you can attempt to scan for all connected devices. Please note that this only works for eTactica devices and only for devices that are properly connected.

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 to merge a combined device list.

If you only care about the devices that were successfully scanned, you can press the *[Replace address list]* 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.

5. Channel Monitor

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

Step 1 - Connect to your Gateway

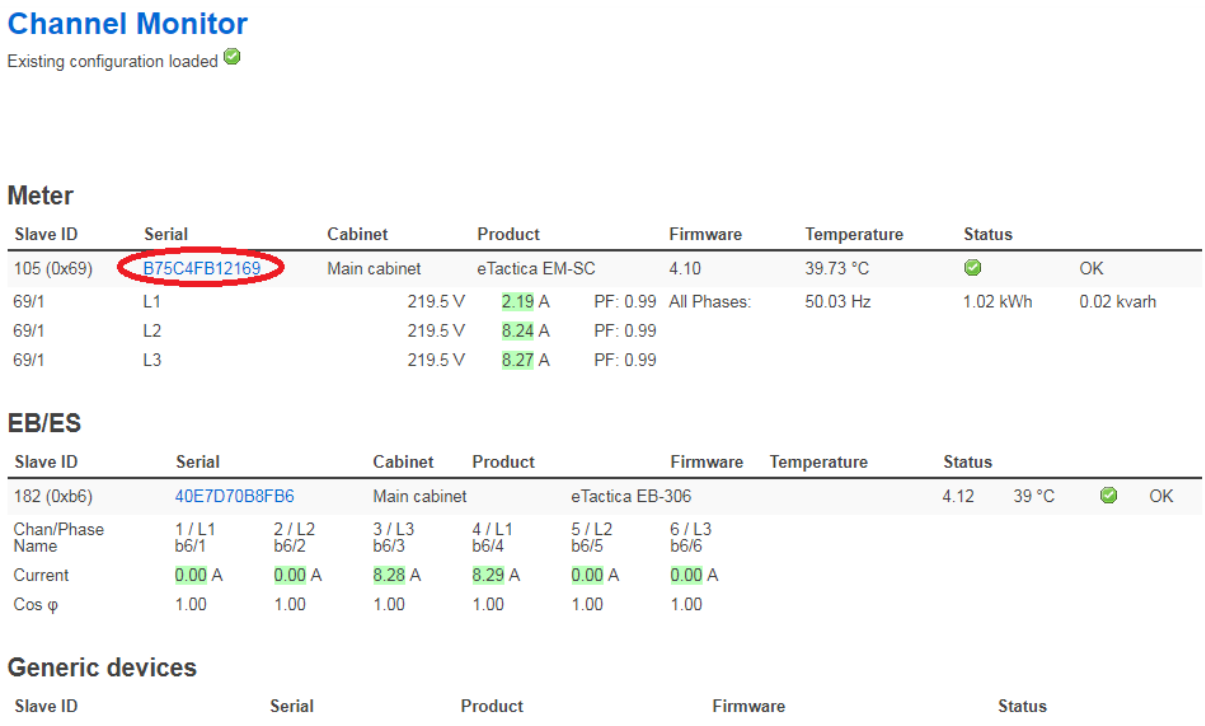
If you are not connected to your gateway device, please see chapter 2, *Connecting to Gateway*.

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.

If you have set up the Cabinet Model, the current readings will be colored relative to the breaker size, green for up to 90% of rated amperage, yellow for 90-100% and red for over 100%.



Step 3 - Go to the Device detail page

Click on the Device ID (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 that show the last 50 readings (starting when the page is opened).

Device detail

Device is operating normally.

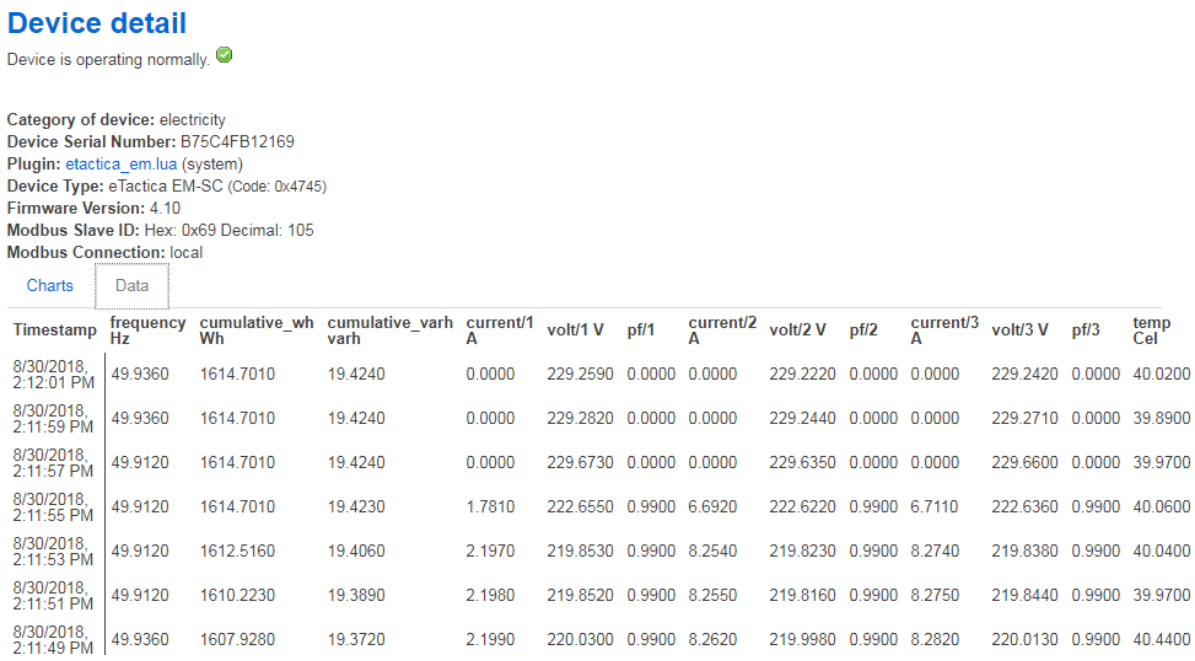
Category of device: electricity
Device Serial Number: B75C4FB12169
Plugin: etactica_em.lua (system)
Device Type: eTactica EM-SC (Code: 0x4745)
Firmware Version: 4.10
Modbus Slave ID: Hex: 0x69 Decimal: 105
Modbus Connection: local

Charts | Data

ID	Name	Nominal Size	Unit	Min	Max	Mean	Stddev	Overview (last 50 vals)	Latest
frequency			Hz	49.86	50.03	49.97	0.04		50.03
cumulative_wh			Wh	1306.27	1420.12	1363.20	33.62		1420.12
cumulative_varh			varh	17.15	17.99	17.57	0.25		17.99
current/1	69/1	16	A	2.18	2.21	2.21	0.01		2.21
volt/1			V	218.13	221.29	220.54	0.53		220.69
pf/1				0.98	0.99	0.99	0.00		0.99
current/2	69/1	16	A	8.19	8.31	8.28	0.02		8.29
volt/2			V	218.09	221.26	220.51	0.53		220.65
pf/2				0.98	0.99	0.99	0.00		0.99
current/3	69/1	16	A	8.21	8.33	8.30	0.02		8.31
volt/3			V	218.10	221.28	220.53	0.54		220.68
pf/3				0.98	0.99	0.99	0.00		0.99
temp			Cel	39.65	40.44	39.99	0.15		39.98

Step 4 Go To the tabulated data page

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



Device detail

Device is operating normally.

Category of device: electricity
Device Serial Number: B75C4FB12169
Plugin: etactica_em.lua (system)
Device Type: eTactica EM-SC (Code: 0x4745)
Firmware Version: 4.10
Modbus Slave ID: Hex: 0x69 Decimal: 105
Modbus Connection: local

Charts | Data

Timestamp	frequency Hz	cumulative_wh Wh	cumulative_varh varh	current/1 A	volt/1 V	pf/1	current/2 A	volt/2 V	pf/2	current/3 A	volt/3 V	pf/3	temp Cel
8/30/2018, 2:12:01 PM	49.9360	1614.7010	19.4240	0.0000	229.2590	0.0000	0.0000	229.2220	0.0000	0.0000	229.2420	0.0000	40.0200
8/30/2018, 2:11:59 PM	49.9360	1614.7010	19.4240	0.0000	229.2820	0.0000	0.0000	229.2440	0.0000	0.0000	229.2710	0.0000	39.8900
8/30/2018, 2:11:57 PM	49.9120	1614.7010	19.4240	0.0000	229.6730	0.0000	0.0000	229.6350	0.0000	0.0000	229.6600	0.0000	39.9700
8/30/2018, 2:11:55 PM	49.9120	1614.7010	19.4230	1.7810	222.6550	0.9900	6.6920	222.6220	0.9900	6.7110	222.6360	0.9900	40.0600
8/30/2018, 2:11:53 PM	49.9120	1612.5160	19.4060	2.1970	219.8530	0.9900	8.2540	219.8230	0.9900	8.2740	219.8380	0.9900	40.0400
8/30/2018, 2:11:51 PM	49.9120	1610.2230	19.3890	2.1980	219.8520	0.9900	8.2550	219.8160	0.9900	8.2750	219.8440	0.9900	39.9700
8/30/2018, 2:11:49 PM	49.9360	1607.9280	19.3720	2.1990	220.0300	0.9900	8.2620	219.9980	0.9900	8.2820	220.0130	0.9900	40.4400

The newest measurements are added to the top of the list, with the last 50 readings (starting when the page is opened).

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*.

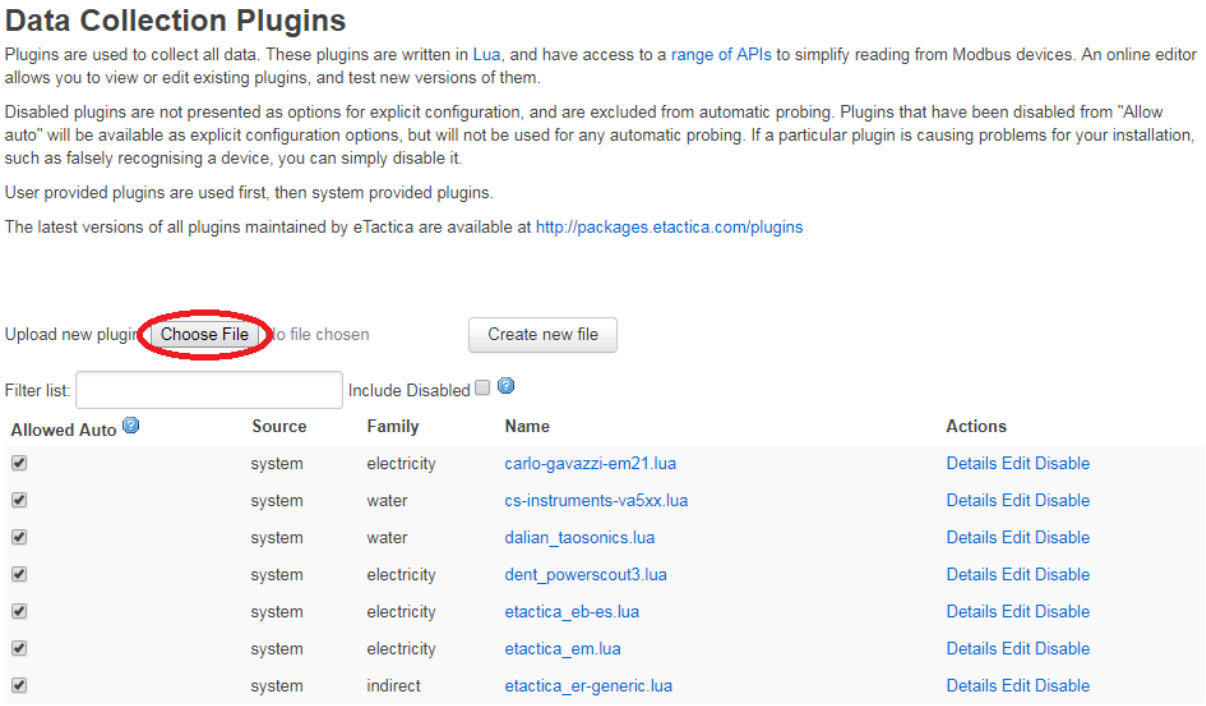
Step 2 - Go to the plugins page

From the home page of the administration web console of your device, select *Setup->Plugins* from the top menu.

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.



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 "Details", "Edit" and overview pages.

Clicking the name of a plugin or *[Details]* 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 *"Include Disabled"* 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 can change the default serial settings for the RS485 interface.

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

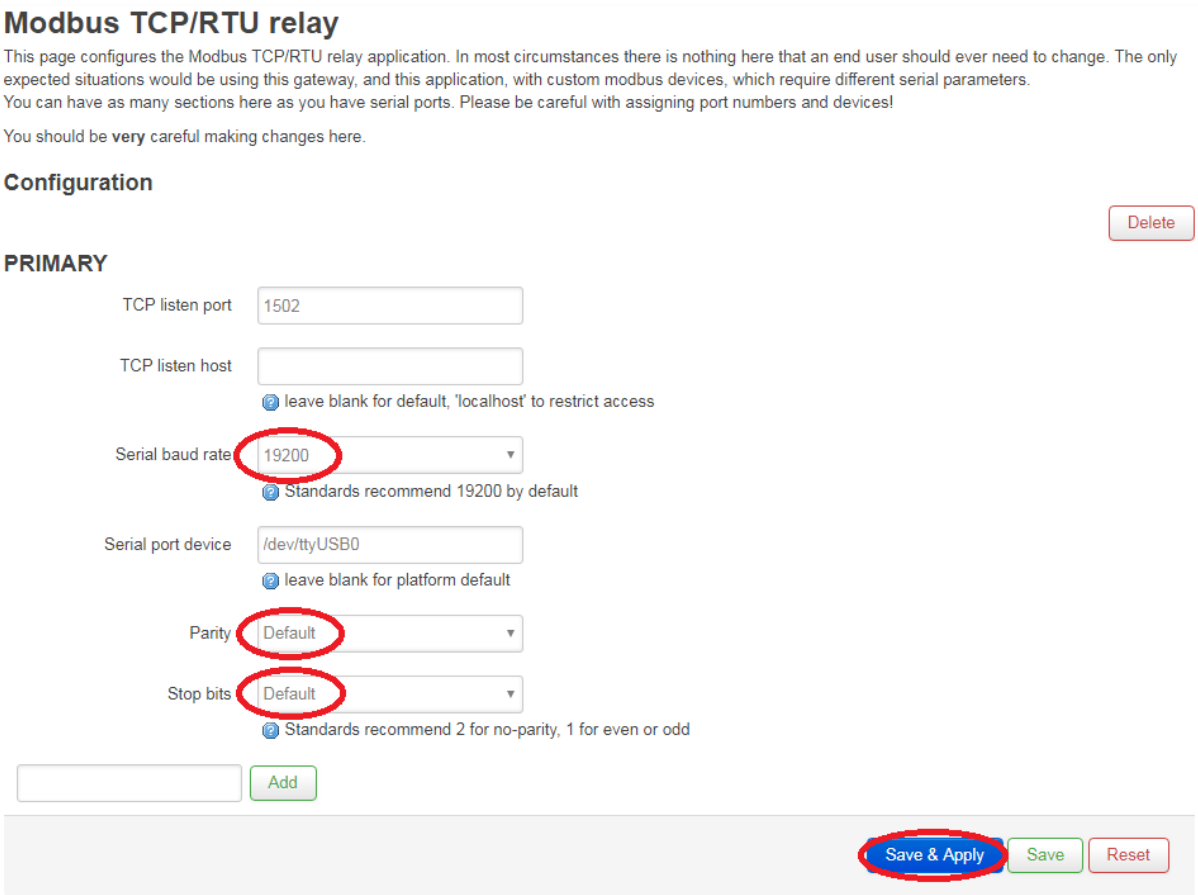
Click on the *[Administration]* link near the bottom of the page.

Step 2 - Go to the Modbus TCP/RTU relay page

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

Step 3 - Change settings

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



Step 4 - 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.

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

Click on the *[Administration]* link near the bottom of the page.

Step 2 - Go to the Modbus TCP/RTU relay page

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

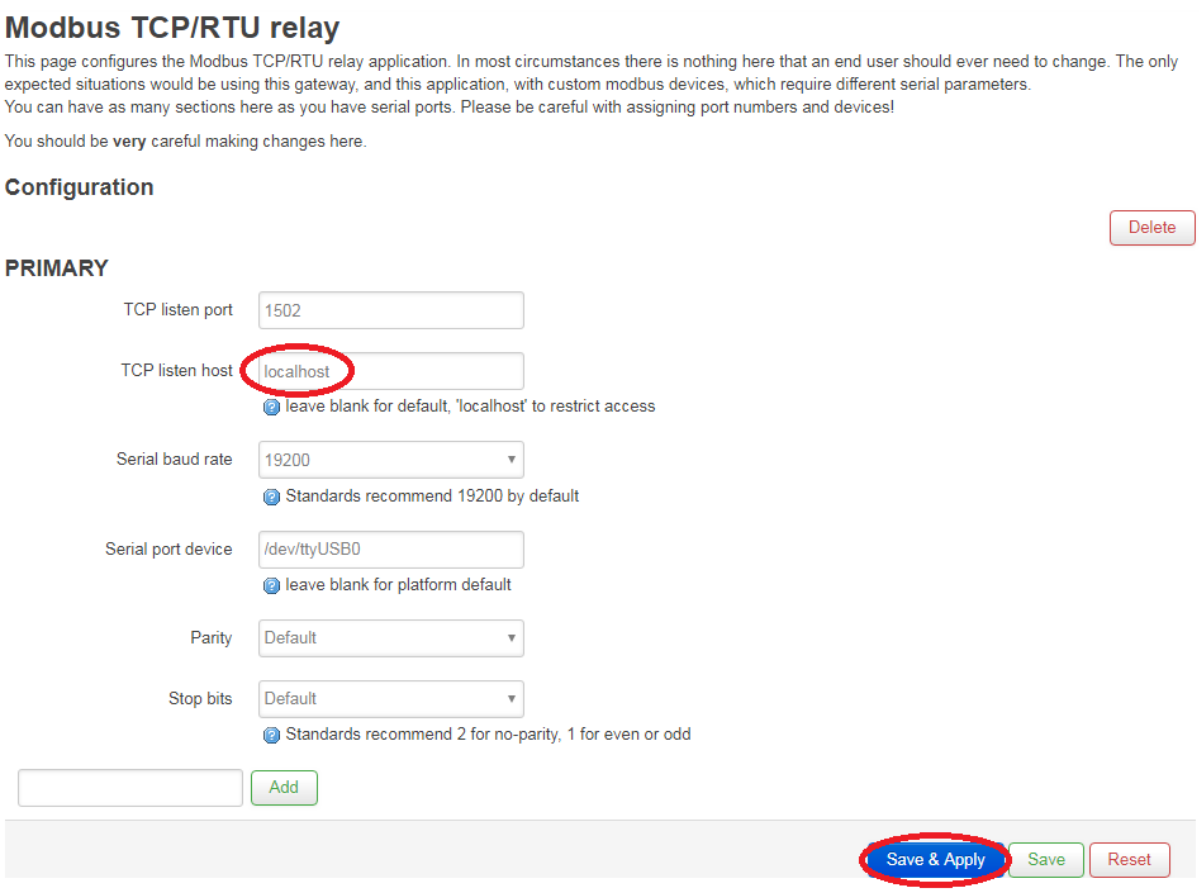
Step 3 - Restrict access

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 'localhost' in to the *"TCP 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 localhost.



Step 4 - 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 Wi-Fi interface
- Internet connection via Wi-Fi (No Ethernet connection)
- Advanced Wi-Fi 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:

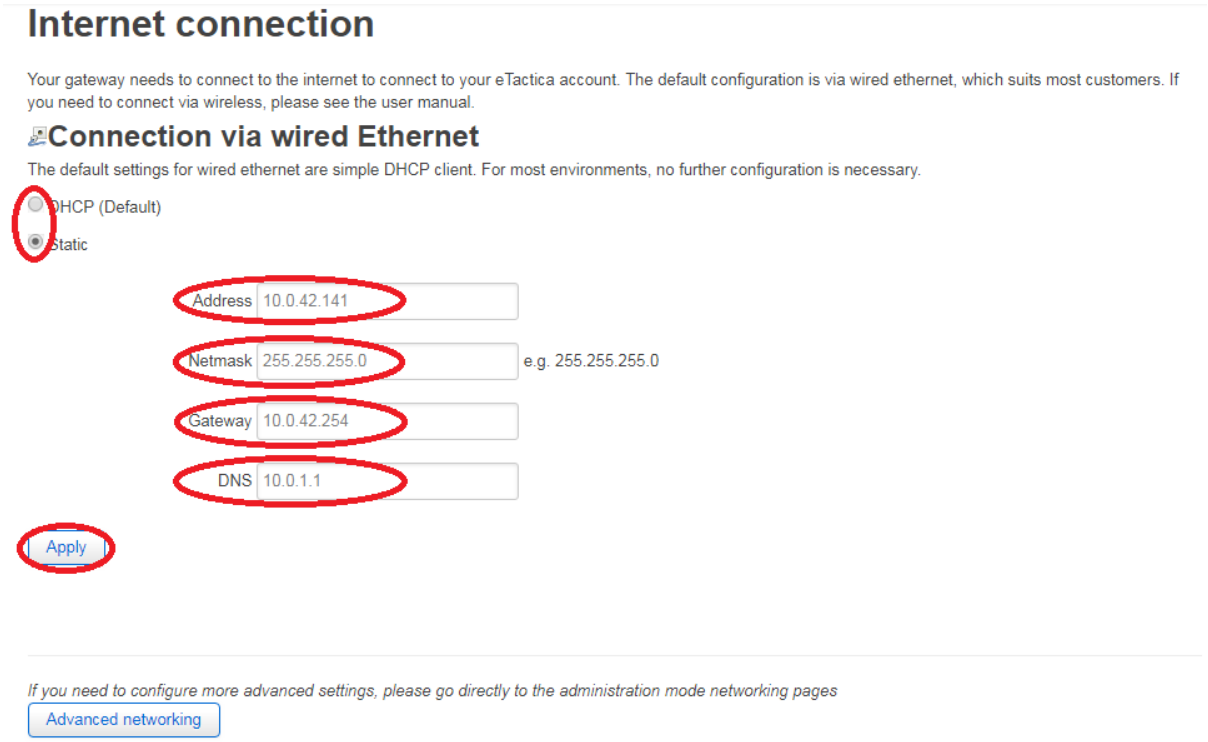
Required Information	Example Value
IP Address	10.0.42.141
Subnet Mask	255.255.255.0
Gateway	10.0.42.254
DNS Server	10.0.1.1

Step 1 - Connect to your Gateway

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

Step 2a - Enter the basic networking configuration page

On the home page of your administration web console, select *Setup->Network* from the top menu. This will take you to the page where you can set up your LAN (Ethernet) protocol.



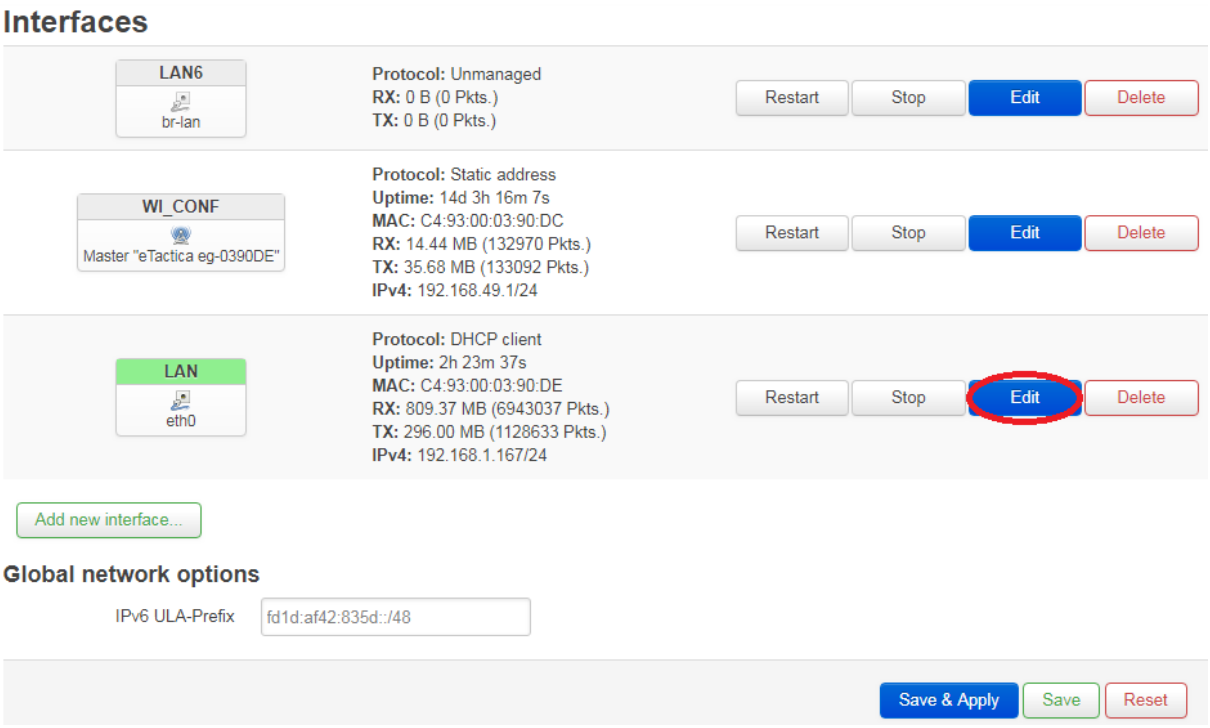
DHCP will be on by default, click on the Static button and you will get all the fields needed to set up the static IP address. Fill in all the fields as instructed by your network manager and click *[Apply]* to save the settings.

Step 2b - Enter the main network page

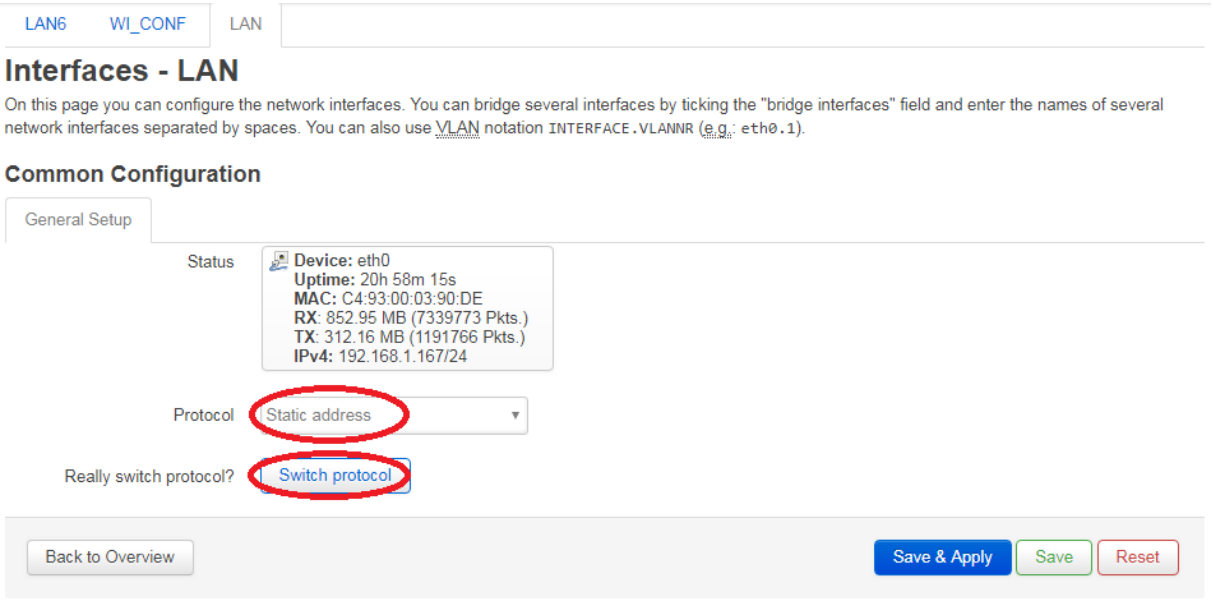
Alternatively, to access further network settings, you can click on the *[Advanced networking]* button on this page or use the *[Administration]* link near the bottom of the page and from there select *Network->Interface* from the top menu.

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

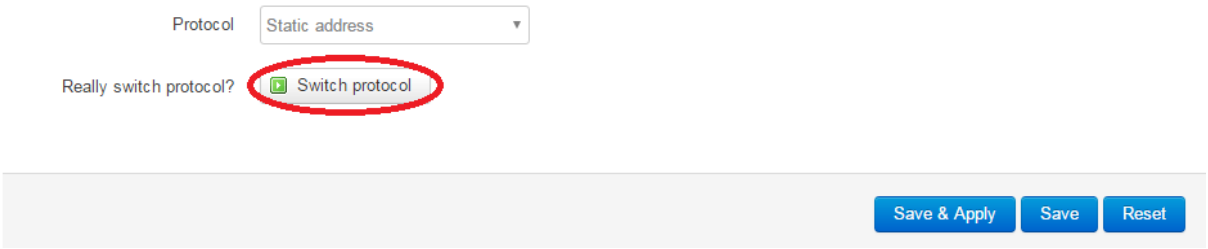
Press the *[Edit]* button, for your interface. This could be either the Wi-Fi or the Ethernet interface, but will generally be the Ethernet interface (LAN).



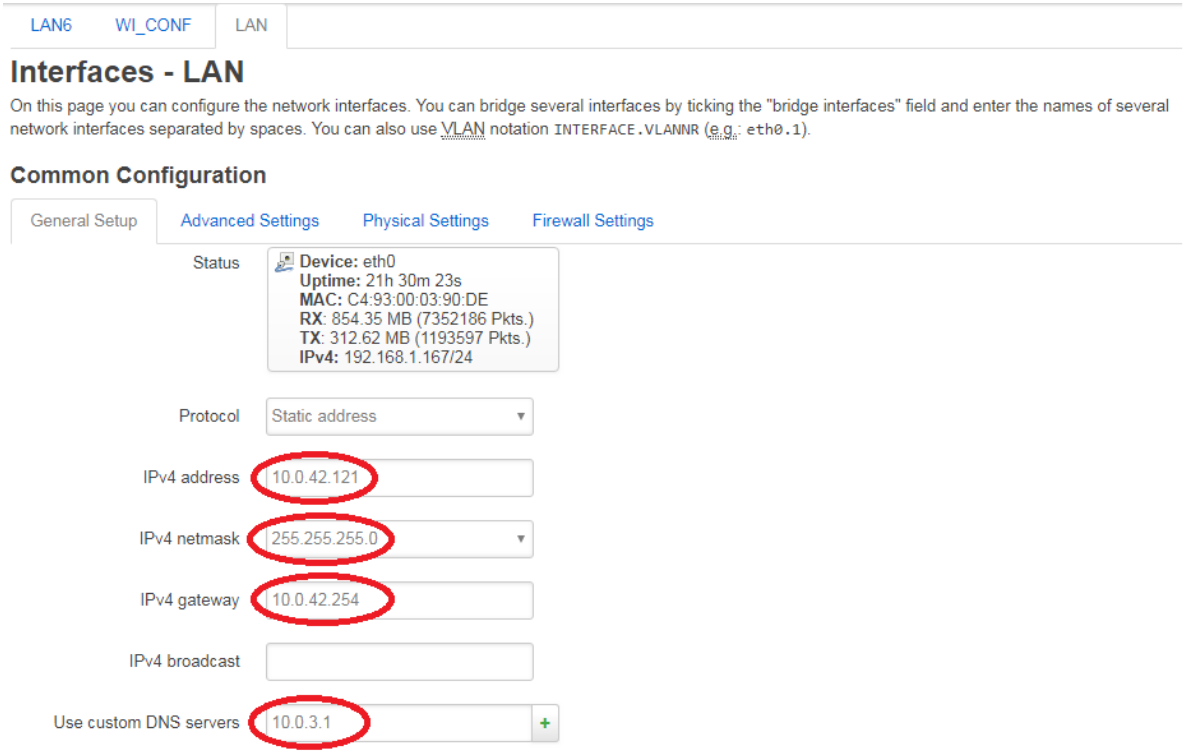
Switch the interface protocol from DHCP to *"Static address"*.



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

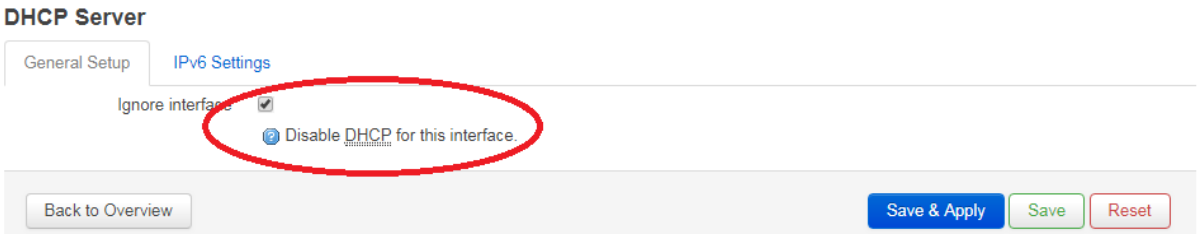


Fill in the form with the details you were provided.



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 Wi-Fi

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

Pre-requirements

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

Step 1 - Go to Administration page

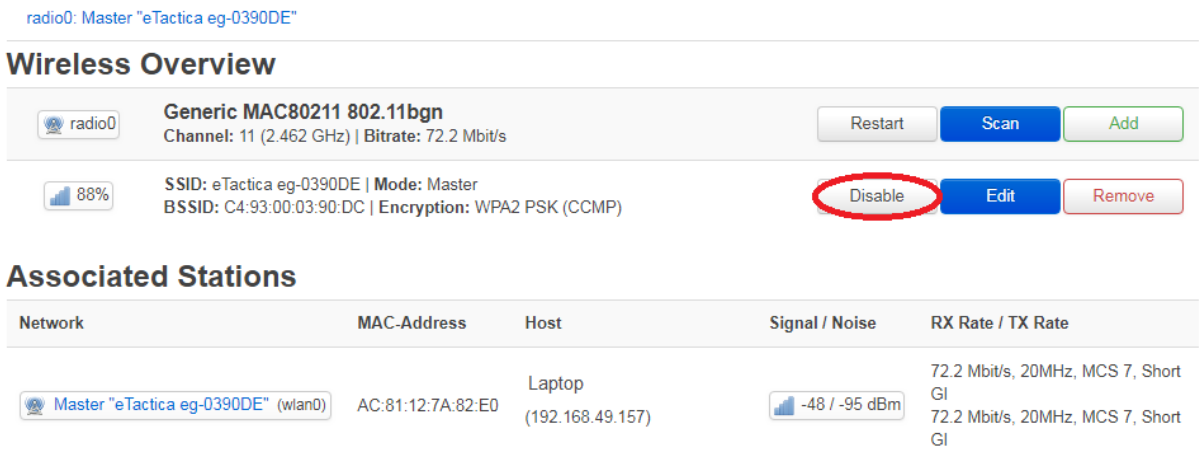
Click on the *[Administration]* link near the bottom of the page.

Step 2 - Go to the Wi-Fi configuration page

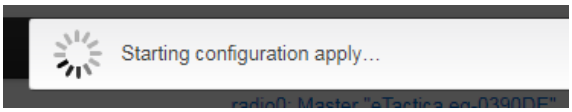
Choose *Network->Wireless* from the top menu.

Step 3 - Turn off Wi-Fi

Press the *[Disable]* button.



You will see this message:



And a few seconds later a message appears that says that configuration has been applied. The Wi-Fi should now be completely disabled.

Re-enable Wi-Fi access to the Gateway

Since you have disabled the Wi-Fi completely, the only option to access your Gateway is via your IP network. To re-enable the Wi-Fi, do as when you disabled the Wi-Fi, the only difference is that *[Disable]* button is now an *[Enable]* button.

Internet connection via Wi-Fi (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 Wi-Fi configuration network. However, you can also configure the Gateway to use the Wi-Fi link as the connection to network if you don't have Ethernet access in your cabinet.

There are two ways this can be set up:

- One is switching the roles of Wi-Fi and Ethernet ports; Internet connection will be through Wi-Fi and the Ethernet interface operates as an open access point with DHCP server for configuration. For this start with step one below.
- The other way is to keep the Access Point on Wi-Fi but change the network connection to Wi-Fi. For this start with step 5 below. In most cases this is the preferred way, your computer just stays connected through Wi-Fi and no need for Ethernet cable.

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 Wireless network keys and names for connection to your desired wireless network.

Step 1 - Go to Administration page

(Go to step 5 if you only want to change network connection to Wi-Fi)

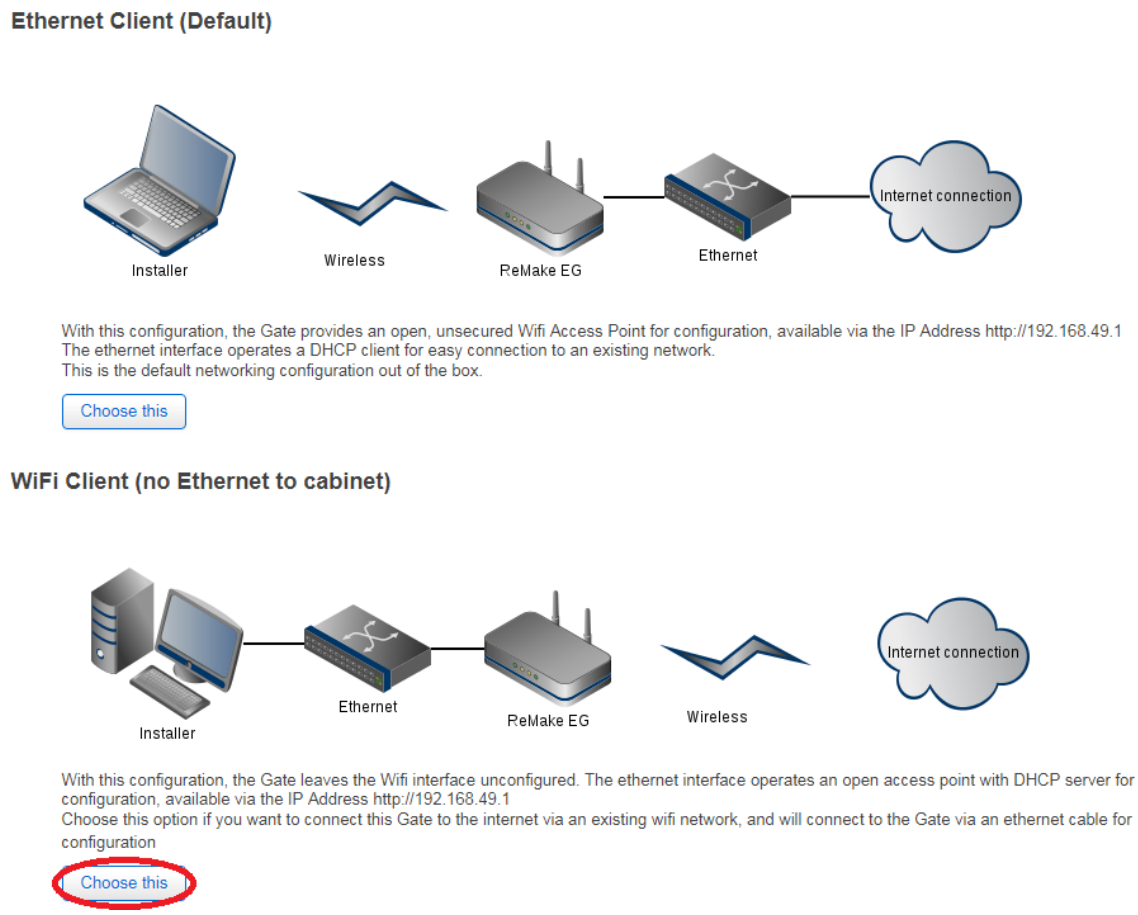
Click on the *[Administration]* link near the bottom of the page.

Step 2 - Go to "Preset networking"

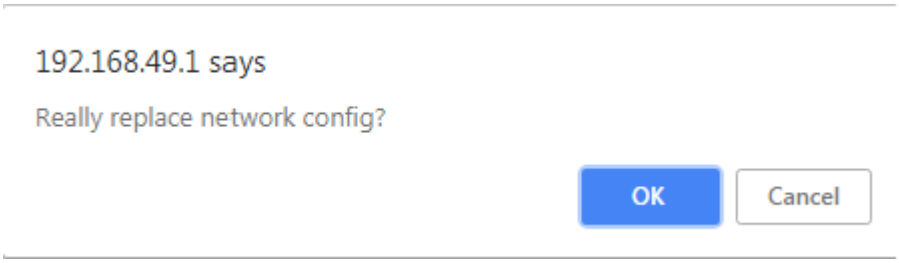
Choose *RME->Preset Networking* from the top menu.

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 "*Wi-Fi 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 Wi-Fi interface will be free to reconfigure for your desired Wi-Fi network.

Step 4 - Connect the Ethernet cable and reboot

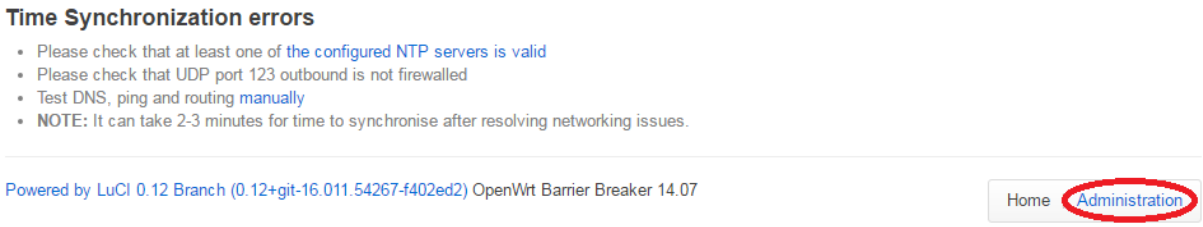
To make sure all the network comes up cleanly, the Gateway will replace its entire network configuration with clean templates and reboot. At this point you should connect the Ethernet cable from your computer directly to the gateway.

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 *"Etactica Staff"*.

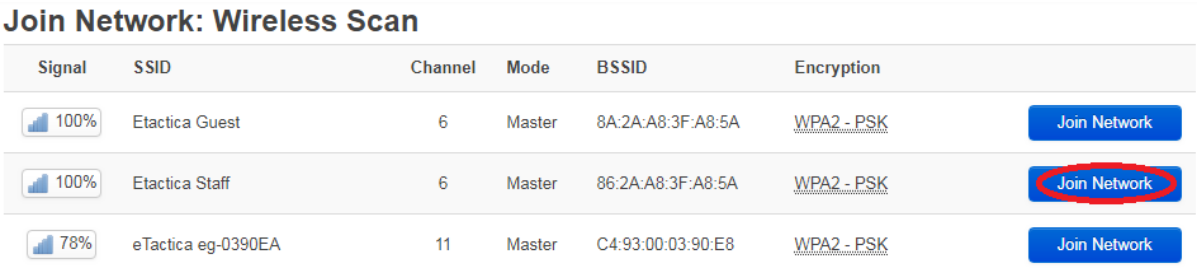
From the home page, click on the *[Administration]* link near the bottom of the page.



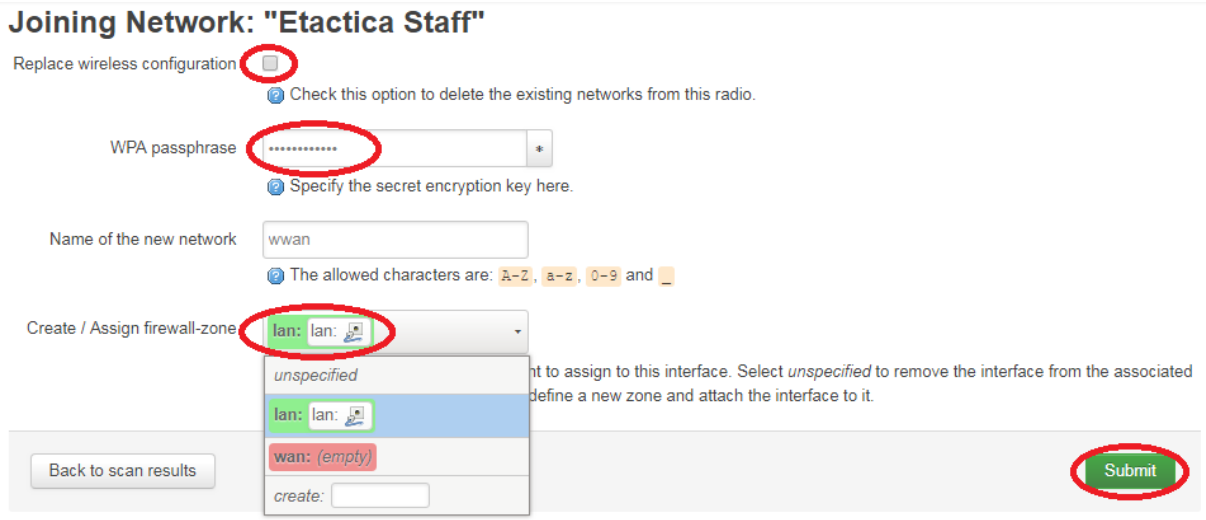
Choose *Network-> Wireless* from the top menu.

Press the *[Scan]* button.

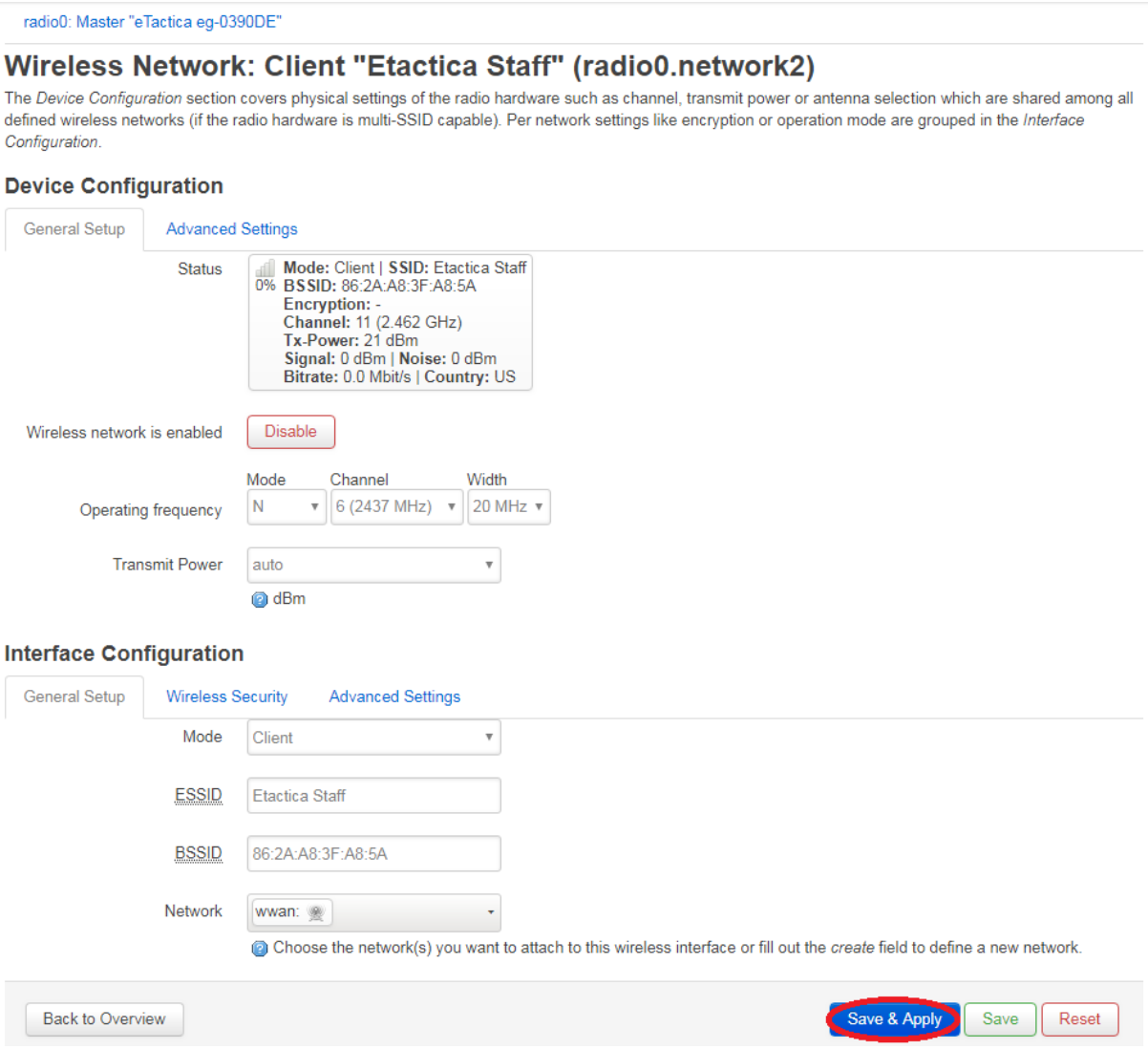
A list of all available wireless networks appears, and you simply choose the one you wish to connect to.



Here you enter your wireless network password/passphrase, change firewall zone to *'lan'* instead of *'wan'.* If you add a tick mark for "Replace wireless configuration" you will lose your connection to the gateway.



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



In most of the cases, there is no need to change anything here.

Step 6 - Save settings

Press the *[Save and Apply]* button to keep and apply your settings and you should be connected to your chosen Wi-Fi 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->Wireless* 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.

If you have only added a new network (from step 5) choose *Network->Wireless* and click on *[Remove]* button for that network to delete it.

Editing Wi-Fi Parameters

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

Click on the *[Administration]* link near the bottom of the page.

Step 2 - Go to the Wi-Fi configuration page

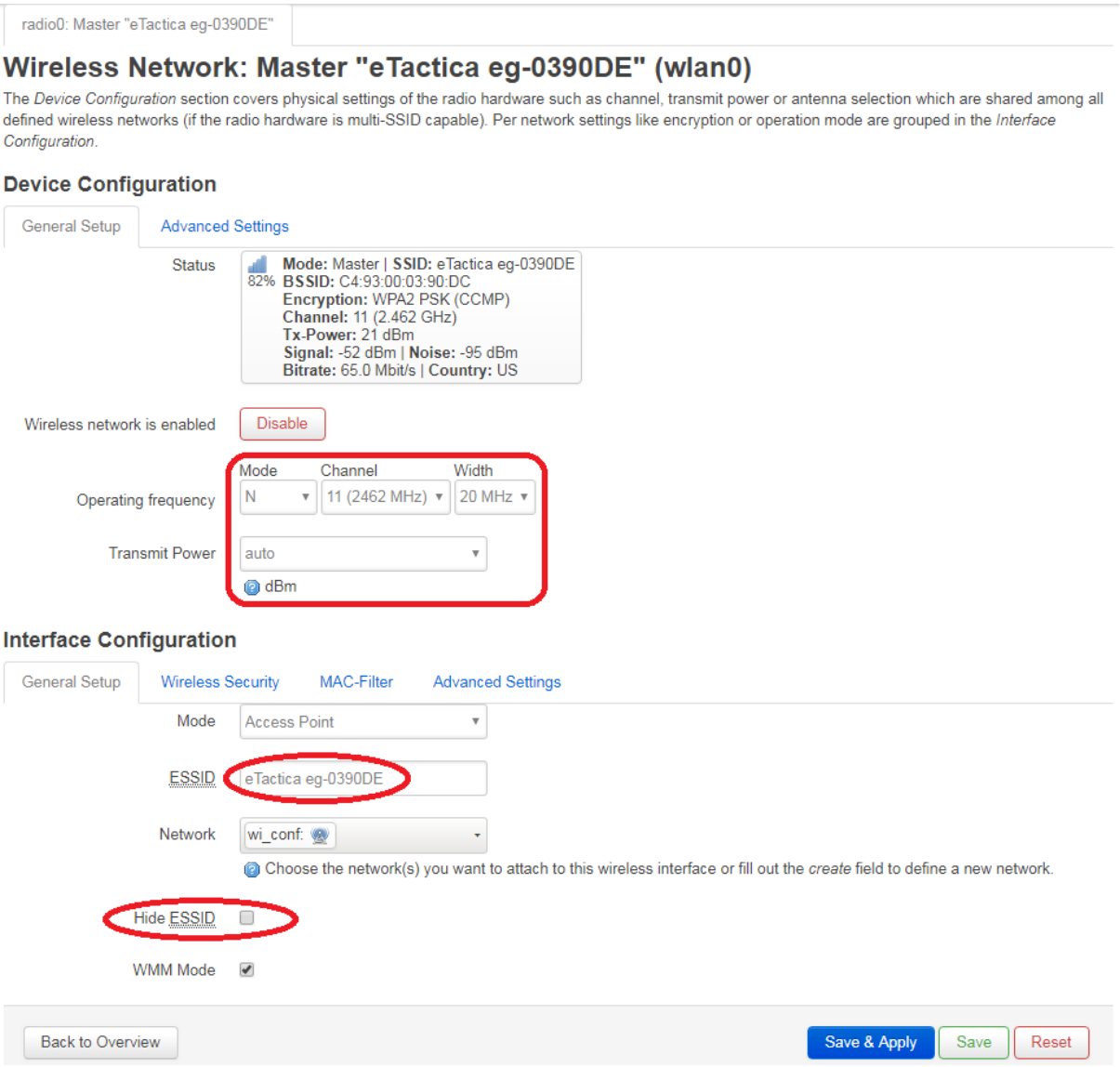
From the top menu, choose *Network->Wireless*.

Step 3 - Edit the Wi-Fi interface

Press the *[Edit]* button.

Step 4 - TX Power / Wi-Fi 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 4 - 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 5 - 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
- Wi-Fi secure access

Gateway Root Password

The default root username is *"root"* and 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.

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

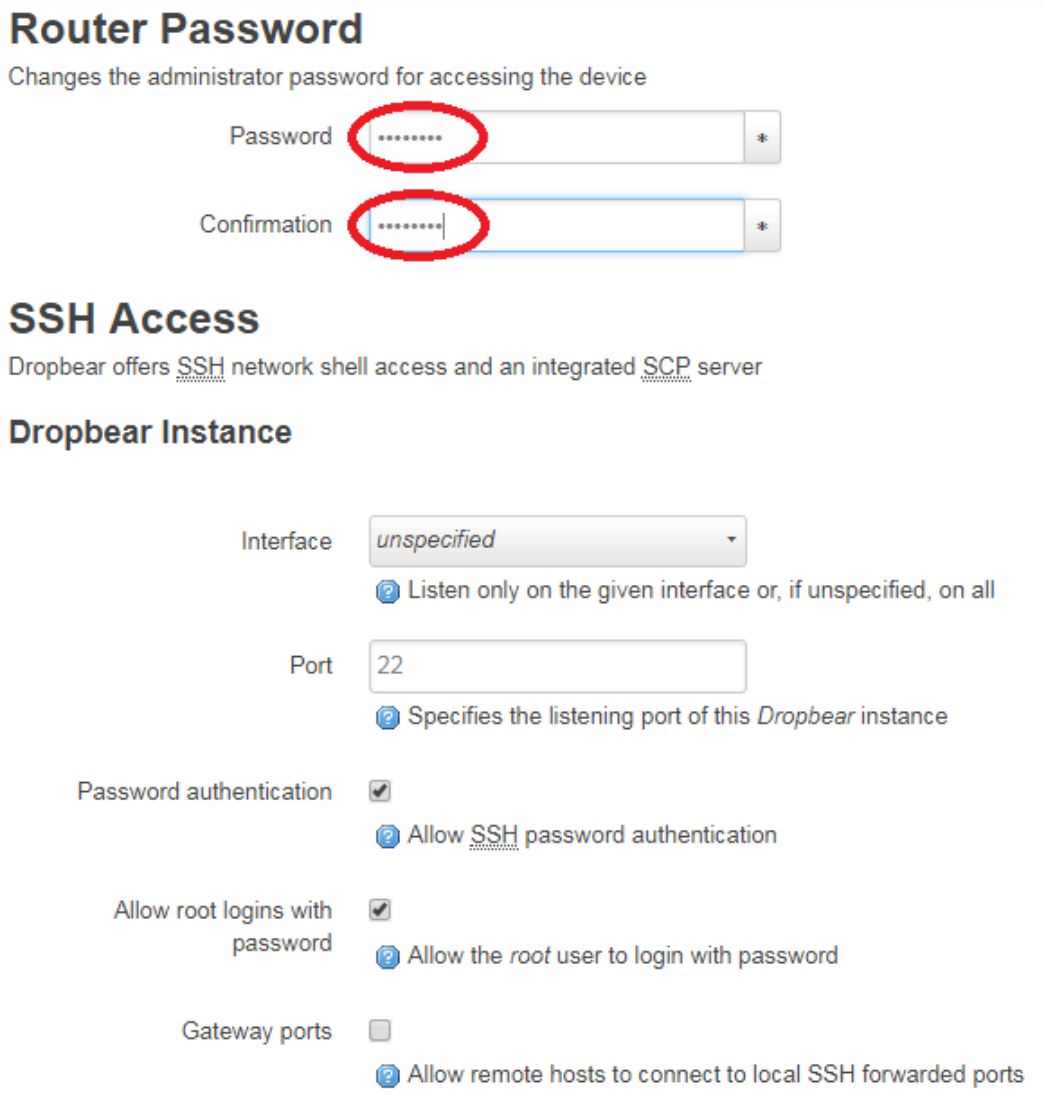
Click on the *[Administration]* link near the bottom of the page.

Step 2 - Go to Administration configuration page

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

Step 3 - 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:

https://openwrt.org/docs/guide-user/security/secure.access

Step 4 - Save changes

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

Wi-Fi Password

The gateway comes with a preconfigured Wi-Fi password that is on a label on the side of the gateway. The following covers how to change the Wi-Fi security password.

Pre-requirements

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

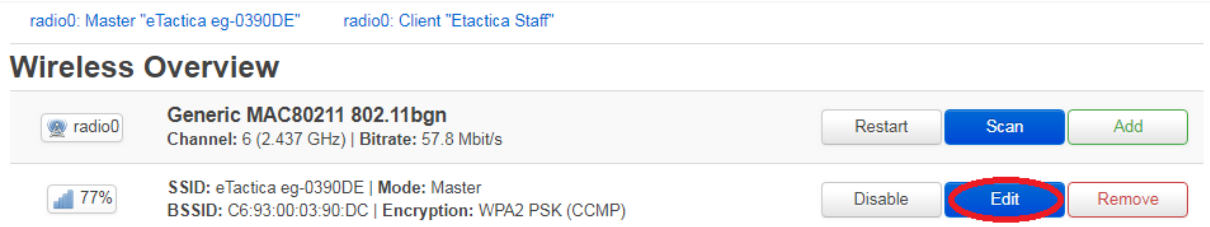
Step 1 - Go to Administration page

Click on the *[Administration]* link near the bottom of the page.

Step 2 - Go to Wi-Fi configuration page

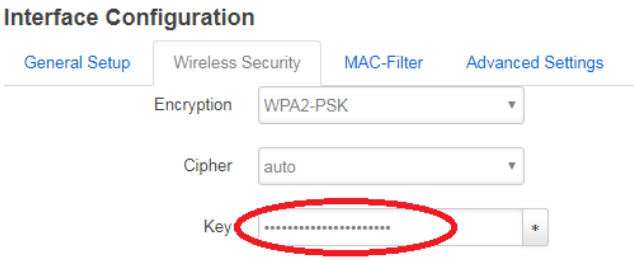
From the top menu, choose *Network->Wireless*.

Press the *[Edit]* button.

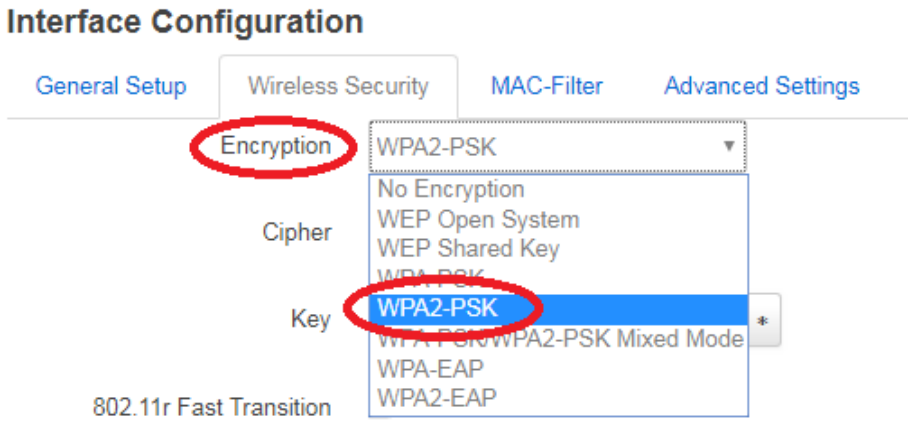


Step 3 - Change password

To change your Wi-Fi password, scroll down to the part entitled:
"Interface Configuration->Wireless Security".
Then, you can change your password in the "*Key*" field.



The default encryption type is "*WPA2/PSK*". Unless you have any reason not to, keep that setting (if you have some pre 2006 Wi-Fi gear, you may need to choose "*WPA-PSK/WPA2-PSK mixed mode"*).



Step 4 - Save settings

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

10. Configure remote MQTT bridges

The onboard MQTT message broker, mosquitto, allows configuring multiple remote bridges to send/receive topic trees to an external broker. The UI provides some limited support for configuring these. For full details and more information, you are strongly advised to consult the mosquitto man pages. This mechanism is how data is sent to eTactica for instance.

Step 1 - Go to Administration page

Click on the *[Administration]* link near the bottom of the page.

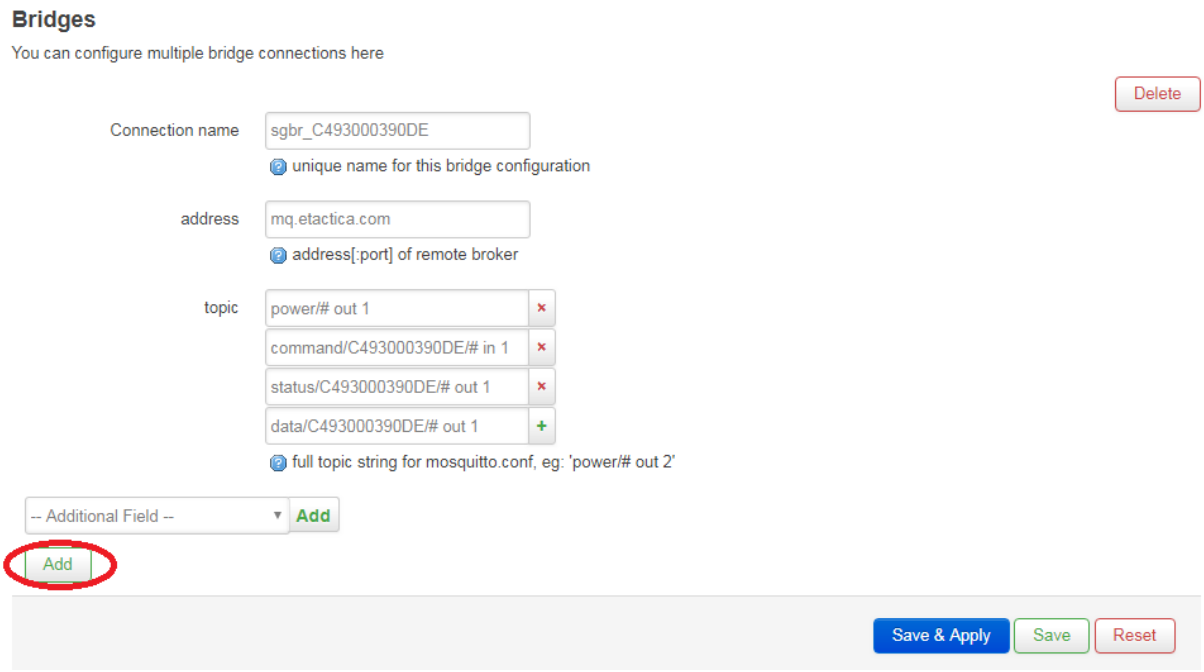
Step 2 - Go to the mosquitto page

Choose Services->Mosquitto

Step 3 - Edit/Add/Remove bridges

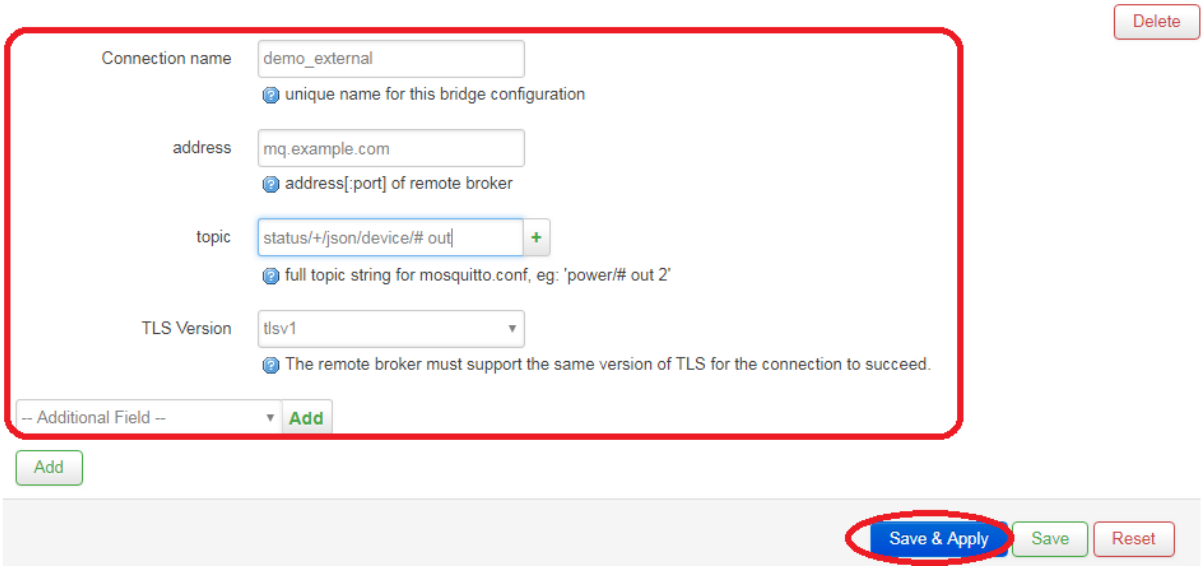
Scroll down to the section labelled "Bridges". Each bridge section can be quite large. The "delete" button will remove an entire bridge section, use caution! Click on "Add" near the bottom to create a new bridge.

Please do not modify the existing bridge configuration, it is used for sending data to eTactica. It is normally recreated on every reboot if it has been modified, but to avoid confusion, we recommend simply leaving it alone.



You can add as many extra bridges here as you like (you only need one bridge per remote server, the bridge configuration can map as many topic trees as you like). The options here are a subset of those described in the mosquitto.conf man pages. Please consult that manual for advice. This configuration can be very open ended, including topic remapping and we cannot provide any concrete guidance here without more information on a given client's particular needs. If a particular configuration file option is not exposed in the UI, please file a ticket with us and we can get it added.

A simple example of sending the live readings stream to a third-party broker is shown below.



Step 4 - Save settings

When you are happy with your settings, choose "Save and Apply", and the broker will restart with the new settings.

11. SNMP Support

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

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

Click on the *[Administration]* link near the bottom of the page.

Step 2 - Go to SNMP support

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

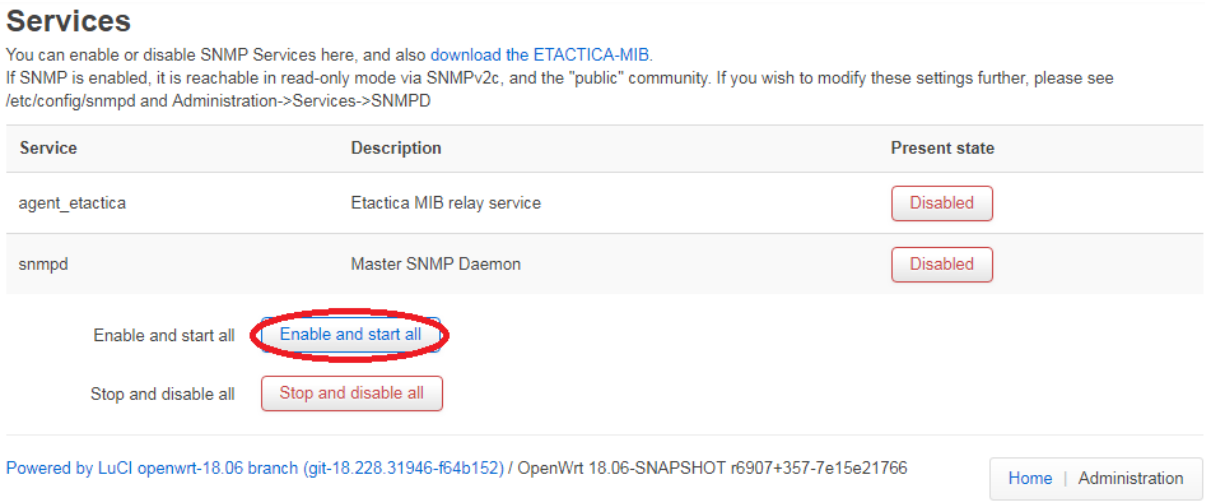
The SNMP Support page contains links to the MIB file for use with third party SNMP tools such as *Nagios* and *zabbix*. The latest version of the MIB is always available at:

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 3 - Enable SNMP

In most cases, you can simply press the *[Enable and start all]* button 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.

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

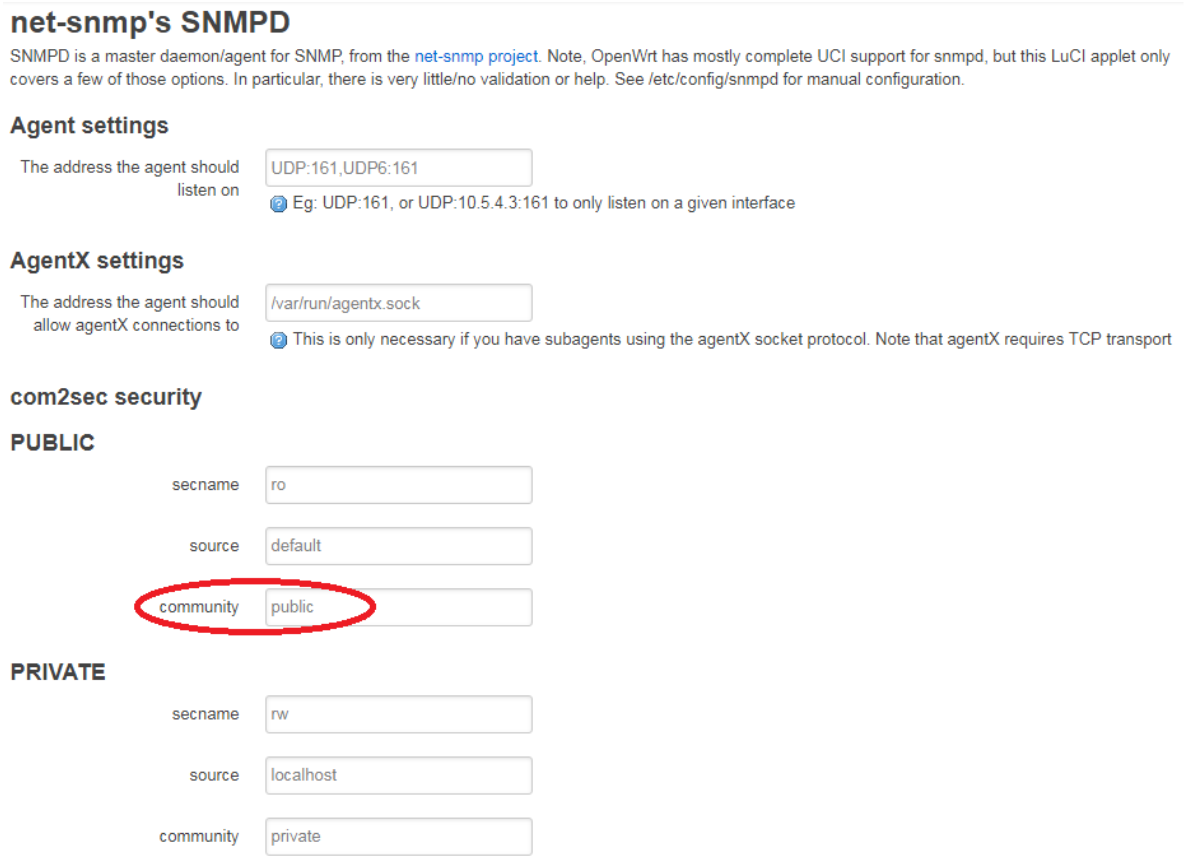
Click on the *[Administration]* link near the bottom of the page.

Step 2 - Access the SNMPD configuration page

From the top menu, choose *Services->SNMPD*.

Step 3 - 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 4 - 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 https://openwrt.org/docs/guide-user/services/snmp/snmpd for more information).

Example usage

In the following, you find examples of SNMP queries.

To query each device's 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 device's 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       ?           ?
```

12. Update Firmware

The eTactica Gateway firmware and the firmware on connected eTactica devices (version 4.0 and later, Powersync devices) can be updated via the administration web console. The gateway firmware is in general compatible with older devices, so there shouldn't be any issues with upgrading to the latest version with new features and security updates. The Powersync network is dependent on hardware features on the newest version of our devices (EB-3xx and EM-SC/EM-FC) and it will not work on older devices, they will just function as before.

All new releases of the firmware are provided and shared by eTactica at this location: http://packages.etactica.com/releases/

The update procedure has been mostly automated, so only a few clicks are needed but there Is also a manual way.

In the following, the firmware update process is described.

Gateway firmware update, the automated way

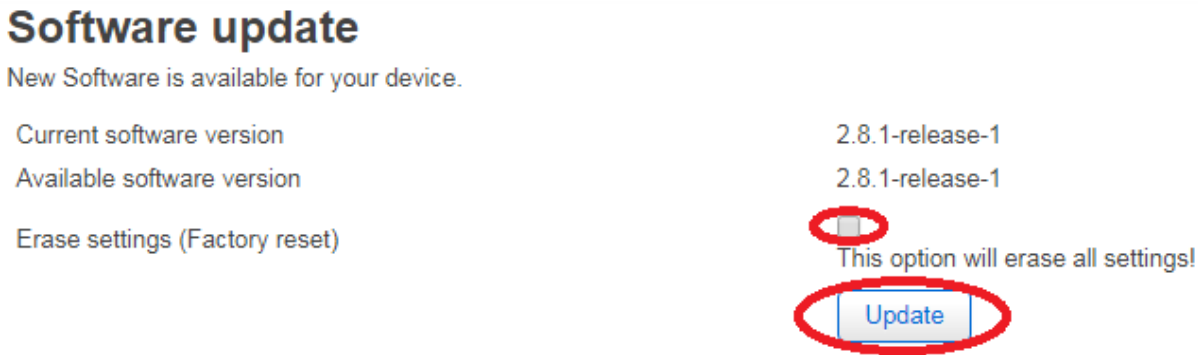
The gateway will check if a new version is available. For this the Internet connection must be active.

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 - Choose "Updates"

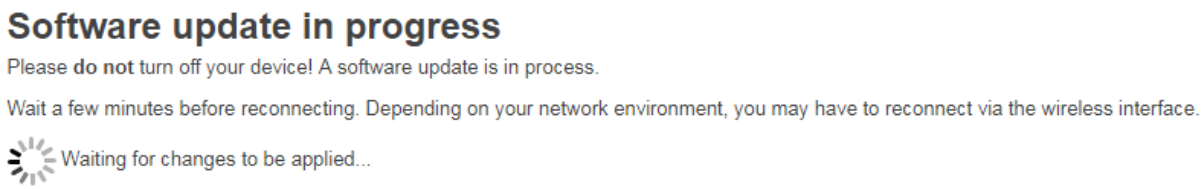
From the menu at the home page for the administration web console, choose *Setup->Updates*.



You will see the current version of firmware on the gateway and the newest version that is available. By selecting *"Erase settings"*, all existing gateway settings and configuration will be erased. This includes your list of measurement devices, any specific network

arrangements, password settings, etc. This should only be done if you're setting the gateway up in a new installation or the configuration has become corrupted for some reasons.

Click on *[Update],* and a message will appear informing you the update is in progress. The installation process takes up to 4-5 minutes, so be patient. 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.



Gateway firmware update, the manual way.

This should normally not be needed, but if you, for some reasons, want to go back to earlier version of firmware or have a special version, you can use this way

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/releases/
2. Follow the link with the highest version number gateway-xx.yy.zz:

- *"../releases/gateway-xx.yy.zz-release-1"*

3. Continue via targets and then ar71xx and generic:

- *"../releases/gateway-2.6.2-release-1/targets/ar71xx/generic/"*

4. Locate this file: *"rme-eg200-sysupgrade.bin"*
5. Press " *sha256sums*" 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 update process.

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

Click on the *[Administration]* link near the bottom of the page.

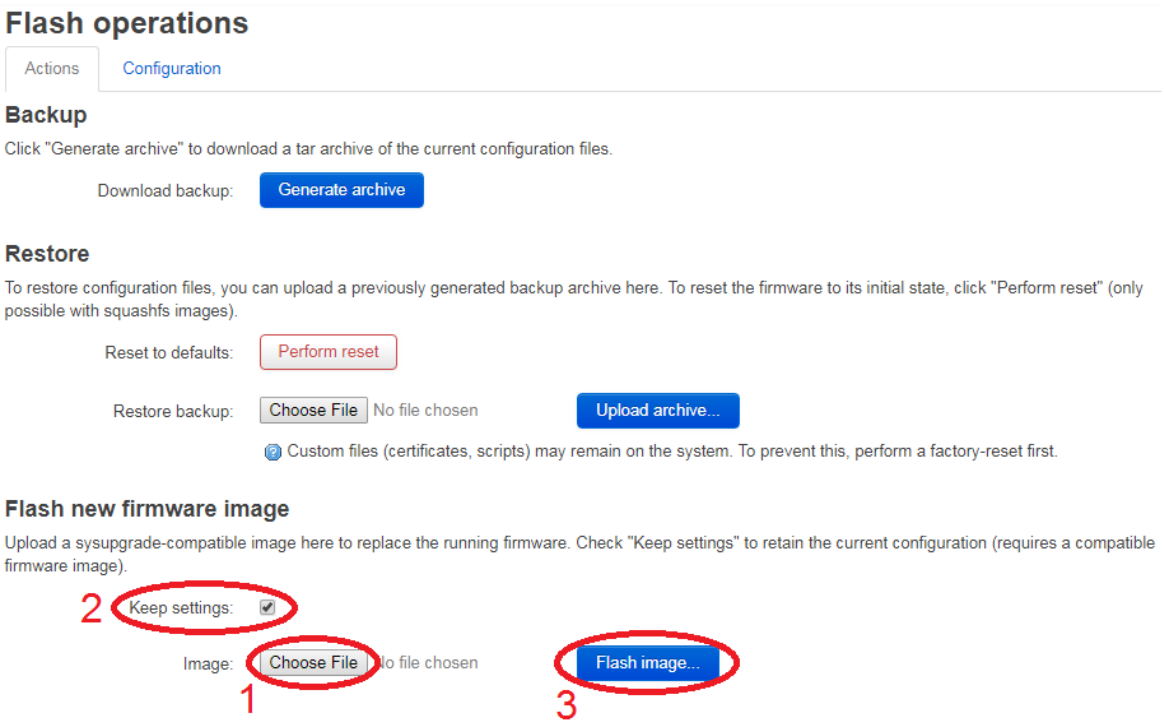
Step 2 - Go to the update page

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

Step 3 - Get image file

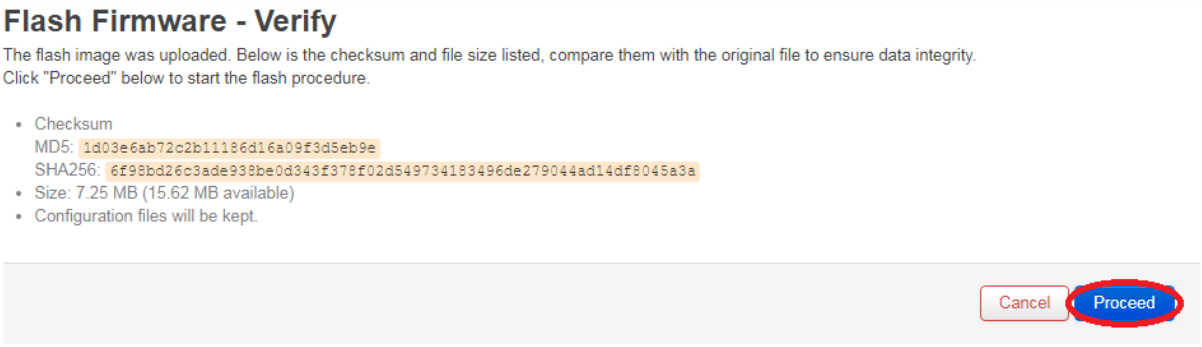
Locate the *"Flash new firmware image"* section and follow this procedure:

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 4 - 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 *"sha256sums"* 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 5 - 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.

Device firmware update, the automated way

Pre-requirements

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

Gateway connected to the Internet.

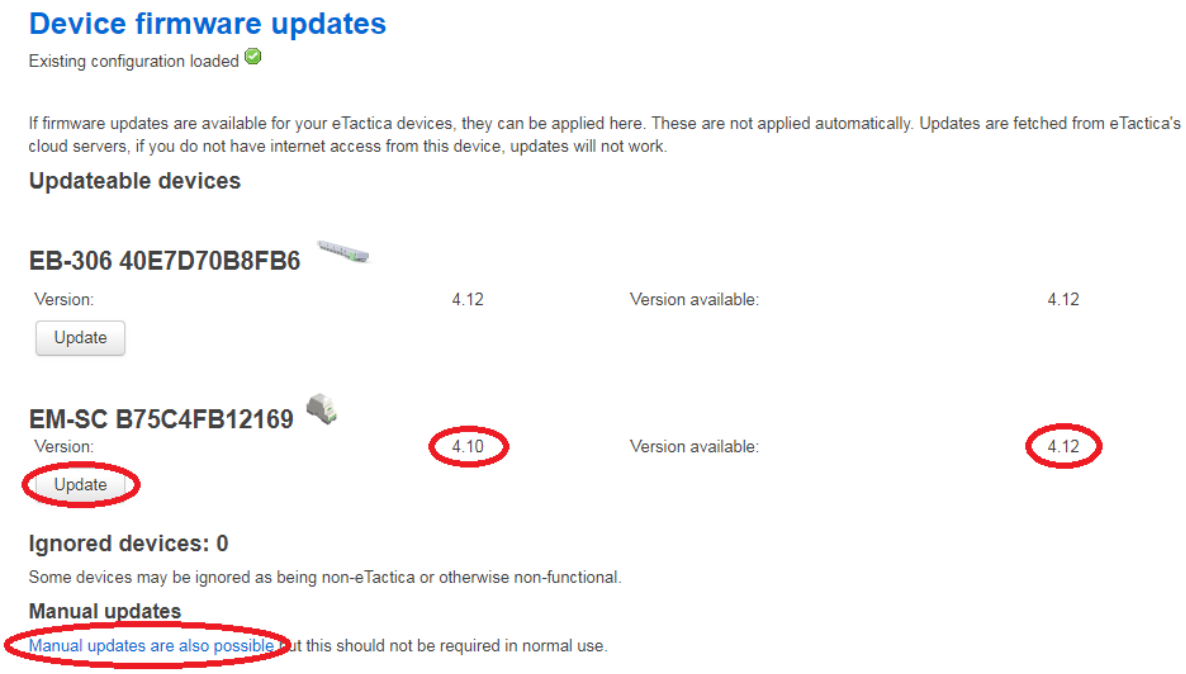
Step 1 - Go to Administration page

Click on the *[Administration]* link near the bottom of the page.

Step 2 - Choose "Devices Updates" page

From the top menu, choose *RME->Status and Health* and click on the *[Device Updates]* tab.

You will see a list of all the eTactica devices that are configured on your gateway, the version number of the current firmware and newest firmware version that is available. For each device there is a *[Upgrade]* button.



Click on the *[Upgrade]* button for the first device you want to update, a progress bar will appear, wait for the update to finish, then start the next update and so on until you are finished. Only one update can be running at a time, as they are all using the same communication channel.

Device firmware update, the manual way

Manual updates are also possible, but this should not be required in normal use.

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/releases/
2. Follow the link with the highest version number devices-vxx.yy:

- *"../releases/devices-v4.12/"*

3. Download the file for the device you are working with (EB-xxx or EM-SC/FC)

The update procedure.

Go to the “Device Updates” page, see previous chapter, near the bottom of the page is a link to the Manual Updates page Manual updates are also possible and click on that link. Use the default Modbus Host port: localhost:1502. Type in the Modbus Address of your device in either decimal or hex. Click *[Choose File]* and locate the firmware image file and open it. Restart your device by unplugging and plugging the Modbus cable. While the device led is blinking rapidly, just after bootup, click the *[Start]* button to flash the new firmware (you will only have a few seconds). A progress bar will appear, and in a few seconds, it should have finished.

13. 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

If both eTactica Connection and Time Synchronization fail, then you probably have no Internet connection.

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 and it will show the number of devices working, if you have more devices installed than are counted, go to *Setup->Config Devices* page to configure the missing devices.

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 the message says, "Modbus protocol", it means that a device that had been working, has stopped responding. If the message says, "unrecognized", it means that the device has never responded since the gateway last started, so there might be a wrong configuration somewhere. "No SPI" means that an EM power meter is responding, but has an internal communication error, usually because there is no voltage on the voltage inputs.

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
- One device faulty in a way that disrupts communication on the device bus, test by disconnecting one device at a time. You could start by disconnecting in the middle to see which half is working

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*.

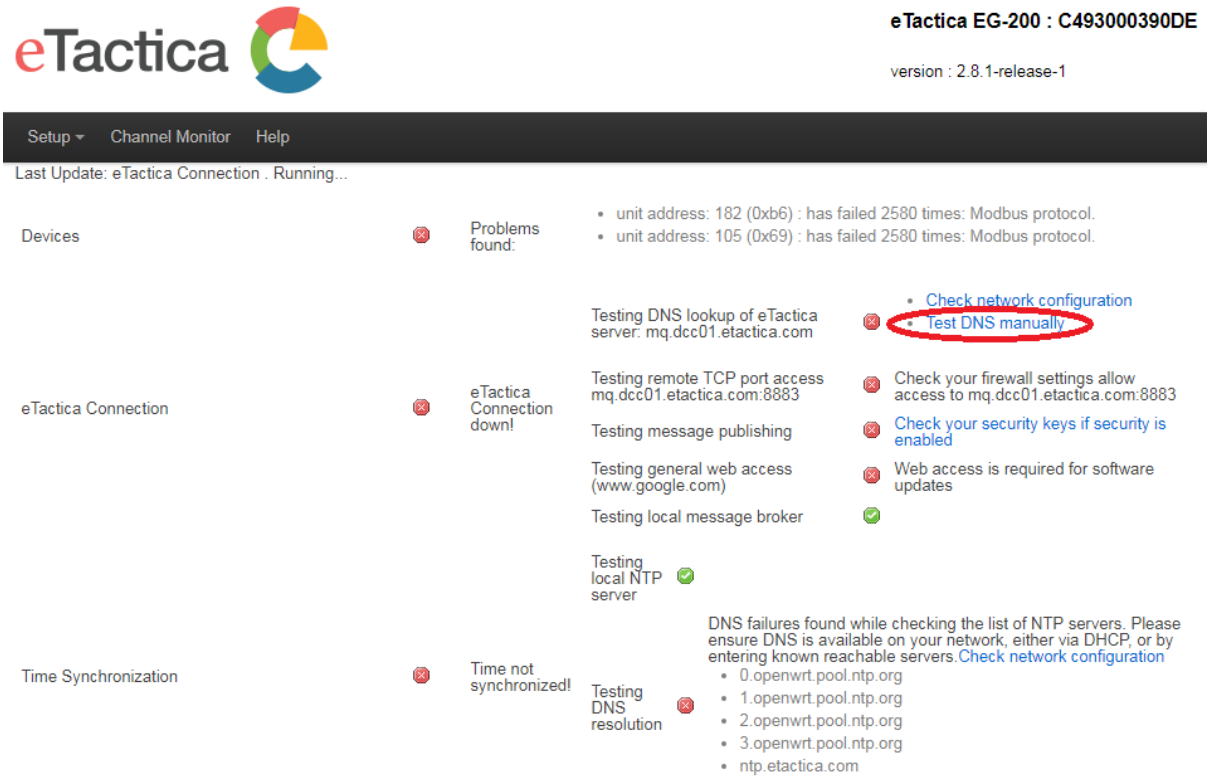
For Ethernet connection, first please check again that the network cable is plugged in at both ends (RJ45 LAN connector light should be on). For Wi-Fi connection, please make sure that you have configured the gateway for Wi-Fi properly. See chapter 8, *Network Settings*.

If you are using a 3G/4G modem for Internet connection, check that it is powered and working and that somebody has paid the bill for the SIM card.

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

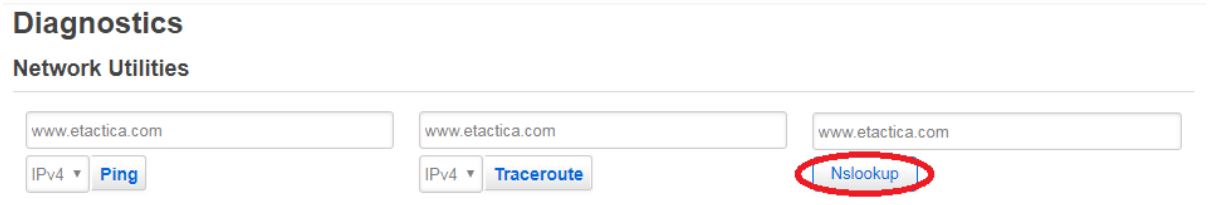
1) Testing DNS lookup of eTactica server

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 screen appears, offering three different network diagnostic tools.

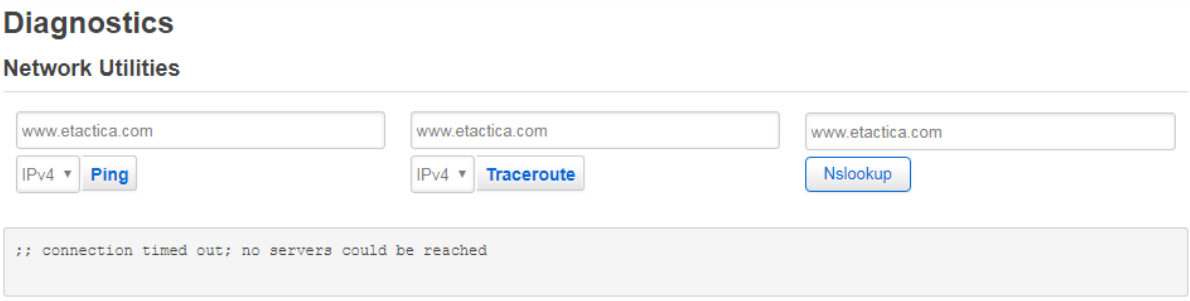


To test DNS resolution, either press the *[Nslookup]* button, using the default name or enter any name that should exist, such as www.google.com or www.ibm.com.

If everything is 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*. Please that not all webhosts allow ping.

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

If this fails, it's not necessarily a major problem for everyday operation. 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. **If the gateway hasn't gotten time synchronization it will not send messages.**

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.

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

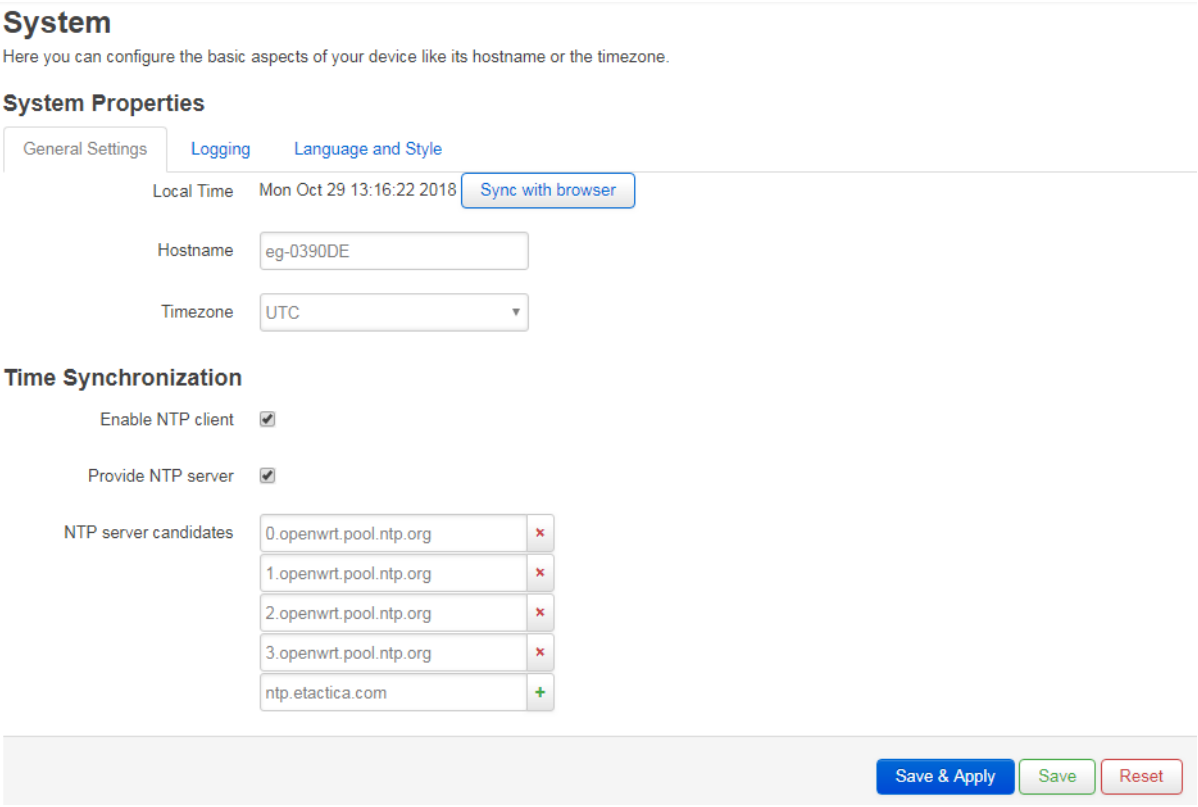
Click on the *[Administration]* link near the bottom of the page.

Step 2 - Go to System setup

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

Step 3 - 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

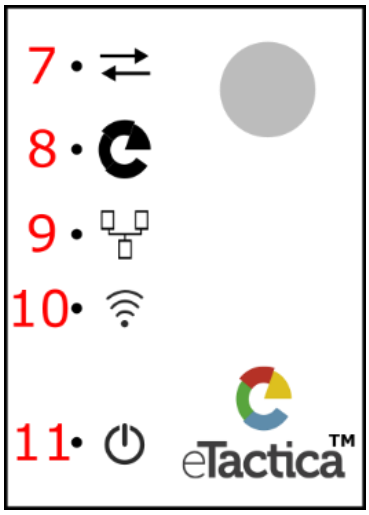
Soft reset

The reset button on the back of your gateway device, can be pressed once briefly, to simply reboot the gateway. The gateway can also be reset through the administration web console. Go to the Administration page, from the top menu choose System->Reboot and click on the *"Perform reboot"* button.

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.

Status lights



7. Modbus: Flashes when Modbus command are sent.
8. eTactica: On when the gateway has a connection to the eTactica web
9. Ethernet: On when the Ethernet cable is connected, flashes when there is traffic on the line.
10. Wi-Fi: Shows that Wi-Fi is on, flashes when there is some traffic
11. Power: On when the gateway is powered

Logs

There are two logs available, kernel log and system log. They can be useful when troubleshooting if you have some serious knowledge of the inner workings of the gateway, which is probably unlikely unless you are working at eTactica.

The kernel log comes from operating system and is kept from startup. It has usually some activity in the first minute or so, but hardly anything after that.

The system log is from everything else on the gateway and only goes back a short time. You may see that some processes are running or restarting but that is usually just because that feature is not being used.

The home page should be your first step in troubleshooting, but if it is not helpful, you can have look at the logs to see if there something of use there. If you're asking an eTactica technician for help, please send a screenshot of the main page and copy of the logs.

Accessing the logs

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

Click on the *[Administration]* link near the bottom of the page.

Step 2 - Go to the Kernel/System log pages

From the top menu, choose *Status->System Log* or *Status->Kernel Log*. Select all the text in the log (not just one page), copy it and save it as a .txt file or paste it directly in an e-mail message.

14. 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	13.03.2017	Various things updated, e.g. plugins Channel Monitor, Internet connection through Wi-Fi troubleshooting, EG-200 added.	Ragnar Einarsson
4.2	13.12.2018	Various things updated, e.g. regarding Powersync and other changes in firmware up to version 2.8.1, MQTT chapter added back in, EG-100 removed.	Ragnar Einarsson