



Dramatically simplifying voice and data networking



edgeboxx

USER MANUAL V4.6



Disclaimer

Precautions have been taken to assure accuracy of the information written in this user's manual. Typographic or pictorial errors that are brought to our attention will be corrected in subsequent issues.

Product specifications in this manual are nominal and are provided for the convenience of our customers. They are all correct at the date of publication. Critical Links reserves the right to make product changes from time to time, without prior notification, which may change certain specifications or characteristics shown. We therefore recommend you to check for changes or updates before using for customer projects or further product developments

No material will be accepted for return unless Critical Links grants permission in writing.

The handling, installation and usage of the edgeBOX are applicable to certain environments and may be required for code compliance. Features of the device will not provide protection against abuse, misuse, improper installation or maintenance. It is important that installation, operation and maintenance are performed in accordance with instructions supplied in the manual. Electricity and electrical devices must always be treated with caution and respect.

Product Support

The edgeBOX software is distributed according to the End User License Agreement EULA included at the end of this User Guide. By using the software you agree to be bound by this EULA. If you do not agree to the terms and limitations of the EULA you should not use the software.

End User License Agreement

For product technical support please visit the following web site <http://www.edgebox.com> or contact us at the following email address: support@critical-links.com.

Critical Links

695 Route 46 West
Fairfield, NJ 07004
USA

Phone: 973.276.9006
Support Hotline: +1 888 433 4326
Website: www.critical-links.com
Email: support@critical-links.com

Table of Contents

1. About edgeBOX	12
1.1. Introducing the award-winning edgeBOX	12
1.2. edgeBOX's main features	14
1.3. Unpack and install edgeBOX to the network	15
1.4. Connecting to edgeBOX's web interface	15
1.5. Connecting to edgeBOX's console	17
1.6. Working with edgeBOX LCD panel	18
2. Initial Configuration	19
2.1. Open edgeBOX web management	19
2.2. Connect edgeBOX to the internet	20
2.3. Define the internal network (LAN)	22
2.4. Indicate a hostname for the edgeBOX and a domain for the network	23
2.5. Check the date and time of the edgeBOX	24
2.6. Overview the firewall settings	24
2.7. Add users to the network	25
2.8. Change the password to access the edgeBOX web management	27
3. Router	28
3.1. Configure the internet connection (WAN interface)	28
3.2. Change the local network properties (LAN interface)	32
3.3. Change the DMZ settings	33
3.4. View and manage the VLANs	34
3.5. Change the hostname of the edgebox	35
3.6. Indicate a domain for the network	36
3.7. View the system routes	37
3.8. Manage static routes	39
3.9. Configure the DNS server	40
DNS General	41
Servers to forward to.....	42
DNS Domains	42
Hosts	43
New	45
Domain	46
ACL	48
SOA	50
Edit	50
Delete	51

Access Control	51
3.10. Use Dynamic DNS	53
3.11. Overview the settings of the DHCP service	54
3.12. Assign IP addresses using Ranges	55
3.13. Assign IP addresses using MAC-IP rules	56
3.14. Configure DHCP advanced settings	57
3.15. Enable NAT on the private networks	58
3.16. Use Port Forwarding	59
3.17. Specify websites not to cache and change the cache size	61
3.18. Update the ADSL modem firmware	63
4. Security	65
4.1. Firewall	65
General	66
DMZ	68
Black List	69
4.2. VPN	70
IPSec	70
Service State.....	71
Active Tunnels.....	71
VPN(s)	71
Add	72
General	72
Basic	72
Advanced.....	73
General	74
Proposals.....	76
Services Access.....	77
Host	78
Local Hosts Visible to External Hosts.....	79
Local Hosts Denied Access to Remote LAN.....	80
Edit	80
Status	80
General	81
Services Status.....	82
Logfile	83
Connection Status.....	84
Delete	84
PPTP	84
Service State.....	85
Authentication Type and Access Privileges.....	86
Remote Radius Configuration.....	87
IP ranges	87
Active Connections.....	88
VPN L2TP	88
4.3. Anti-Virus	89
Shares Scanner	89
Mail Scanner	90
General	91

Virus	91
Spam	92
More Options	93
Messages	93
Actions	94
Quarantine	95
Anti-Virus Engines	96
Sophos	96
Information	97
Upload and Install	98
Update	98
McAfee	98
Information	99
Upload and Install	99
Clamav	100
4.4. Content Filtering	100
Domains	101
Words in URL	103
5. Storage and Printers	105
5.1. Windows Domain	105
Service State	106
Global	106
WINS Options	107
5.2. File Sharing	107
Shares	108
Permissions	110
Homes	112
Public Safes	113
5.3. Printers	114
5.4. Quotas	115
Change Group of Quotas	116
5.5. Backup & Restore	117
Manual Backup	118
Automatic Backup	119
Restore	120
5.6. Maintenance	121
6. VoIP and IP-PBX	123
6.1. Phones	124
New Phone	125
VoIP	125
Advanced	126
Codecs	128
Analog	129
Advanced	130
ISDN	130
ISDN Info	131
Twinning	132
Edit Phone	133
Delete Phone	134

6.2. Inbound Calls	134
IVR Editor	134
Edit Context.....	135
Add Action.....	136
Goto Action.....	138
Remove Action.....	138
Internal	138
Add Action.....	139
Call Rules	139
Add Rule.....	140
DID Routes	141
New Route.....	142
DID Ranges	143
Sound Manager	144
6.3. Outbound Calls	146
LCR	146
New Route.....	147
Edit Route.....	149
Delete Route.....	149
Access Groups	149
Add Access Group.....	149
Edit Access Group.....	150
Delete Access Group.....	150
SIP Proxies	150
Basic	151
Authentication.....	152
Codecs	152
Remote Switch	153
Add	154
Edit	154
Delete	155
Virtual Routes	155
Enum Config	155
Authentication	156
Emergency	156
6.4. PBX Features	157
Queues	157
Add Queue.....	158
Agents	160
Conferences	161
Add Room.....	162
Prefixes	163
Hunt Group	165
Add HuntGroup.....	166
Voicemail	166
Fax Service	167
6.5. Hardware	171
ISDN BRI	172
Edit Port.....	172
ISDN PRI	174
Edit Span.....	175
Analogue FXO-FXS	177
Edit Port.....	177

Echo Cancellation	178
HPEC	179
6.6. Tools and Services	180
Manager	180
Billing Service	181
G.729 Licensing	182
Phone Auto Configuration	184
Configuration Assistant Call	187
Advanced NAT	188
7. QoS	191
7.1. Service State	192
7.2. Upload Information	192
Maximum Rate	193
Reserve	193
DSCP Marking	193
Allow other classes to borrow unused bandwidth	194
Pipes	194
7.3. Download Information	195
7.4. QoS Services	196
8. Wireless	199
8.1. Configure and turn on the wireless network	199
8.2. Indicate the type of authentication	201
8.3. Make the wireless network more secure	205
8.4. Make the wireless network public	206
9. Web Server and Email Server	208
9.1. Web Server	208
Service State	208
Max. Access	209
User Directories	209
Virtual Hosts	209
New	210
Edit	212
Delete	212
Change Webmaster password	212
9.2. Email Server	212
Basic	213
Advanced	214
Service State.....	214
Global	214
Email Domain(s).....	215
Webmail Domain.....	216
Storage	216
Max. Connections.....	216
Max. Message Size.....	216
Block Unresolvable Domains.....	216
POP before SMTP (Relay Support).....	216

SmartHost.....	217
Access Control.....	217
Alias	219
E-Mail Aliases.....	219
Email Queue	220

10. Users and Accesses 222

10.1. Add or remove users	222
10.2. Have a local administrator of edgebox	226
10.3. Configure access profiles	229
Internet	230
User Sessions	233
Services	235
VLAN	236
Other	238
10.4. Manage and authenticate users remotely	239
10.5. Use groups of users	242
10.6. Personalize the appearance of the login page	243

11. Reporting 247

11.1. System	247
CPU	247
Memory	248
Load	249
Disk Usage	250
Interfaces	251
11.2. Services	252
HTTP Access	252
Web Server	253
Firewall	254
Email	255
VoIP	256
VPN	257
11.3. Users	258
General	258
Accounting	259
HTTP Access	260
Email	260
VoIP	261
VPN	262

12. System 263

12.1. Date and Time	263
12.2. Administrator	266
12.3. Logging	267
Logs	267
Syslog	268
12.4. Software Updates	268

12.5. HotBackup	270
12.6. Accounting	273
12.7. Radius	273
12.8. SNMP	275
12.9. Items	276
12.10. Diagnostics	277
Interfaces	277
Ping	278
All Methods	278
ICMP	279
UDP	280
TCP	280
SYN	280
NSLookup	281
Host Names	281
Name Servers	282
Mail Servers	283
IP Addresses	284
Traceroute	284
DHCPLeases	286
12.11. Notifications	287
12.12. RAID	288
Disk Notifications	289
Replacing a faulty disk	290
12.13. Shutdown	292
13. Status	293
13.1. Summary	294
13.2. Users	294
13.3. Network	295
13.4. Services	296
13.5. Traffic Control	297
13.6. Hardware Monitor	299
13.7. Log Viewer	300
Blacklist Log	300
VoIP Log	301
13.8. About	302
14. Services	303
14.1. Main Menu	304
14.2. Public Safes	304
15. Applications	305
15.1. Web Mail	305
15.2. Flash Operator Panel (FOP)	306

FOP Login	308
Initiate a Call	309
External Calls	310
Transfer a call	311
Barging	311
Create an Agent	312
Queue Managment	312
Park-Unpark Calls	313
Conference Calls	313
Typical Caller Scenario	313
16. Appendix A: Authentication	314
16.1. Authentication architecture	314
16.2. Require users to login vs Group Policies	314
16.3. Putting all together	315
16.4. Remote configuration	316
17. Appendix B: Connecting to Wireless	318
17.1. 802.1x	319
17.2. WPA	321
18. Appendix C: Windows Integration	323
18.1. Configure edgebox to work as a PDC	323
19. Appendix D: VLAN based Infrastructure	325
19.1. Introduction	325
19.2. VLAN Scenario 1	326
19.3. VLAN Scenario 2	327
19.4. VLAN Scenario 3	328
19.5. VLAN Scenario 4	330
20. Appendix E: Others	332
20.1. Factory Reset	332
20.2. Virtual Hosts	332
20.3. View and understand the VoIP Log File	333
21. Public Safes	334
22. Acronyms	338

1 About edgeBOX



Critical Links' edgeBOX is a network appliance that consolidates the voice, data and IT functions at a Small and Medium Business (SMB). Specifically, it provides VOIP, Routing, Quality of Service, WiFi Access Point, Storage and Print server, Network Access Control (NAC), Security and Collaboration tools (email/web server etc) – which is currently delivered using up to 8 different, independent products/devices.



ROUTER



QUALITY OF SERVICE



WIFI



STORAGE & PRINT



VOIP



NETWORK ACCESS



SECURITY



COLLABORATION

- [Introducing the award-winning edgeBOX](#)
- [edgeBOX's main features](#)
- [Unpack and install edgeBOX to the network](#)
- [Connecting to edgeBOX's web interface](#)
- [Connecting to edgeBOX's console](#)
- [Working with edgeBOX LCD panel](#)

1.1 Introducing the award-winning edgeBOX

The edgeBOX appliance comes in 3 different form factors (with different redundancy & fault-tolerance options).



office

The edgeBOX Office Gateway caters for offices with up to 40 users



business

The edgeBOX Business Gateway is aimed at the medium sized business with up to 100 users



enterprise

The edgeBOX Enterprise model supports up to 300 users for the larger corporate environment

The edgeBOX comes with a wide range of interfaces to connect to the Internet and the PSTN (such as FXO/FXS, Ethernet, ISDN PRI/BRI, T-1/E-1 etc).

Every edgeBOX has an intuitive GUI that allows the user to access the box and configure the

various functions very easily. NOTE: The box already comes with a set of default configurations that will allow most customers to just literally power on the box and begin to use it; it also provides a customer the ability to customize the settings to support their environment.

The edgeBOX:

1. Dramatically simplifies the SMB voice and data infrastructure

- It replaces up to 8 independent products/devices with 1 device
- Reduces maintaining & managing several devices (and vendors)

2. Increases Productivity and Convenience at the SMB

- Provides the broadest range of voice, data and IT capability
- Managed through a simple, unified interface, even remotely

3. Reduces initial investment & recurring operational expenses over 60%

- Initial cost reduced to less than a third of a multi-device solution
- Recurring costs are nominal; remote, simplified management

4. Environmentally (and economically) friendly

- Much smaller carbon footprint lower power/space consumption
- Lower waste generated at end of life

The edgeBOX eliminates the traditionally painful trade-off between features, complexity and cost at a SMB. SMBs have had to incur a high degree of complexity (due to the many devices and vendors needed to be managed) and the attendant cost (due to expensive IT support) to get much needed voice and data features. Now with the edgeBOX a customer can get a broad range of voice, data and IT services for a fraction of existing costs. The edgeBOX is changing the rules of the game for the SMB. The SMBs can now focus on their core competence instead of worrying about the cost and complexity of managing their networking

The edgeBOX, by integrating the voice, data and IT features, in one appliance and managed by a simple GUI dramatically reduces the complexity and brings down the costs. The edgeBOX, based on open source standards, also ensures a best-of-breed solution that is competitively superior in terms of both feature richness and cost.

A remote based management system (iTEMS) ensures remote provisioning, monitoring and management of several edgeBOX appliances as well, further simplifying and cost reducing maintenance.

The edgeBOX incorporates a set of functional capabilities that are necessary when provisioning voice and data services at a SMB. If a VOIP service is to be provisioned, for example, in addition to configuring the IP-PBX, Quality of Service (QoS), Firewall, Router tables, email server, etc, have to also be usually configured. All this can be done right in the edgeBOX appliance from a GUI and without having to concern about the peculiarity of different devices, interoperability, and making all of them work together. This not only reduces the upfront cost but also speeds up service turn up.

The edgeBOX comes provisioned with a default configuration for the router/switch settings and also for commonly used SIP phones, further enhancing the user experience.

The number of features available on the edgeBOX is unmatched competitively and it provides more voice and data services than most SMBs would require currently. In addition, value-added application packages called edgePACKs, are also available for specific vertical segments; these further augment the networking services in the edgeBOX with application oriented capabilities. Current edgePACKs include the Learning Management System (for academia), Content Management System (for managing website content), and edgeExchange (for email, calendar and content sharing).

More information on the edgeBOX:

	695 Route 46 West Fairfield, NJ 07004 U.S.A +1.973.276.9006 www.critical-links.com 1-888-4-EDGEBOX
---	---

1.2 edgeBOX's main features

- **Internet connections** using **ADSL, Cable modems or other WAN Broadband devices**;
- Supports for **dynamic and static IP Address attribution**, also allowing the configuration of a **registered domain name**;
- **DHCP server** on the Intranet side with optional automatic name range generation;
- A **web server** on both the Internet and Intranet side, with optional **home pages** for every user of the network;
- **DNS Server** for both local private domain or as a **master name server** on the Internet;
- Internet **Mail Server** with **anti-spam control**.
- Support for **SMTP Relay** for Road Warriors;
- Full access control over the internal network services and the Internet access;
- **802.1x** Port based authentication with Single Sign On;
- **User based access control** to manage accesses to the network resources;
- **Group based access control** for third part applications integrated with edgeBOX;
- **VLAN** aware router. Supports **802.1Q** and **Inter-VLAN access policies**;
- See who is on your network and from what IP address;
- **User time and traffic based accounting**. Supports optional Radius session servers;
- Supports **Local User Authentication** or **Remote User Authentication** using a **Radius Server, LDAP Server** or using **Active Directory**;
- **Backup and Restore** of edgeBOX's configuration and of users's data.

- System updates from a remote server.
- **Dynamic DNS**. Supports the **DynDNS** or the **No-IP** services;
- Optional **Wireless Network** with edgeBOX's access point;
- **IMAP and POP3 Servers**. Integrated mail access using the internal web server;
- **VPN tunnels** based on the **IPSec** standard or the **PPTP** protocol;
- **Traffic control** in inbound and outbound traffic. Possibility of reserving bandwidth for important users in your company or for high priority traffic types, such as voice traffic;
- Support for a **dynamic Intranet** with **content management** capabilities;
- **VoIP** Features, including support for line fail over, Interactive Services, Call Rules, Sound Manager, Conference calls, Hunt Groups, Phone Auto Configuration, etc.
- Fax2Mail and Mail2Fax

1.3 Unpack and install edgeBOX to the network

To install the edgeBOX to your network please consult the **Quick Start Guide** flyer that was sent with your edgeBOX appliance.

The guide will quickly:

1. Introduce you to all the **edgeBOX components**,
2. Explain the **elements in the rear and front panels**,
3. Indicate how to **connect** edgeBOX to your **Internet Modem** and **Ethernet Switch**,
4. Show how to **power up the appliance**.




1.4 Connecting to edgeBOX's web interface

The edgeBOX appliance is **configured with a default factory configuration**. Typically, the first task after you connect the edgeBOX to the network is to change the default configuration, so that it meets your requirements.

You can **perform the initial configuration from a computer connected** either:

- directly to edgeBOX's LAN interface.
- or to a hub or a switch connected to edgeBOX's LAN interface.

 If you connect the computer directly to edgeBOX's LAN interface, you need to use a crossover network cable. If you connect a hub or a switch to edgeBOX's LAN interface, then you may use a standard network cable.

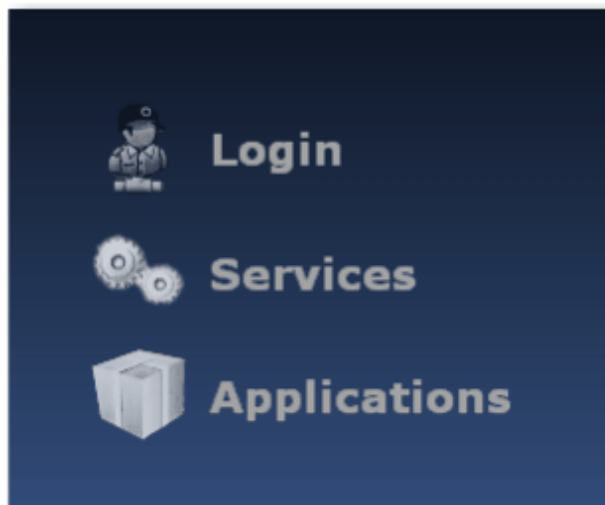
The LAN interface is initially configured with the IP address 192.168.100.254 and has the DHCP service active.

This way, **to connect the computer to the edgeBOX's network:**

- Configure it to obtain its local network IP Address from the edgeBOX using **DHCP**;
- Or configure it with a **static IP address**. The IP address used has to be within the range 192.168.100.0/24 (192.168.100.50 for example).

Then, from the computer:

1. With a browser, open the webpage <https://myedgebox.com> or <https://192.168.100.254:8011>.
2. After the page opens, click the **link Login**.



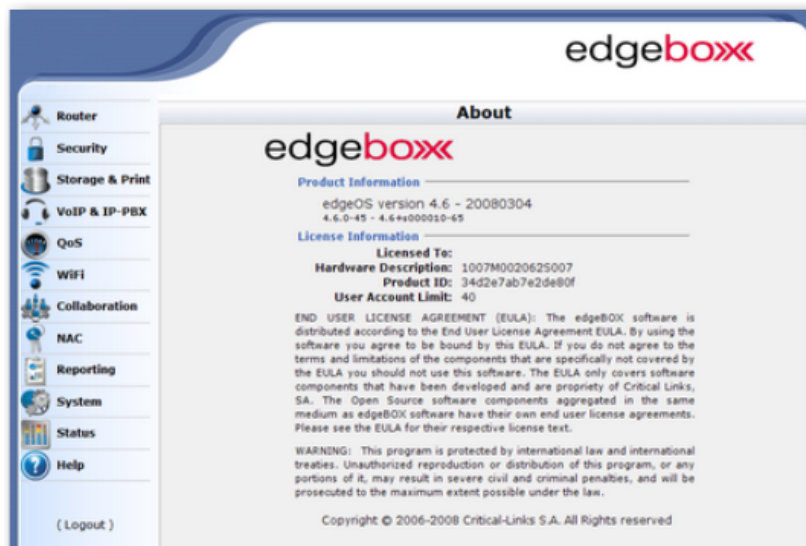
edgeBOX initial page

3. Use the username "admin" and the password "root" to login. This is the default password. For security reasons change it afterwards.
4. Click the **Login** button.


The edgeBOX web interface will then start load.

- It might take a few moments.
- You may have to accept one or more warning messages due to the Java Platform.

After the load is complete you will see the About page (it displays information about the edgeBOX version) and you can start configuring the edgeBOX.



edgeBOX web configuration - Homepage


 To use the edgeBOX web interface you need to have installed in the computer the Java Plug-in. Java Runtime Environment, version 1.4 or higher is needed.

1.5 Connecting to edgeBOX's console

It is also possible to connect directly to edgeBOX's console to manage the appliance using a command line interface (CLI), although you will have just a limited set of commands available.

To connect to edgeBOX's console:

1. Connect a keyboard to the PS2 port or any of the USB ports located on the rear panel;
2. Connect a monitor to the monitor port located in the rear panel;
3. The screen should display a prompt requesting a login/password to be entered.

 Use the command line only **if you are an advanced user**. Using it incorrectly may compromise edgeBOX's correct functioning or even stop it to work completely.

1.6 Working with edgeBOX LCD panel

The edgeBOX LCD panel is simple information panel which is available on **Business** and **Enterprise** type edgeBOXes.



edgeBOX's LCD panel

▼ View information about the network

To see information about the network on the LCD panel, press the Up or Down buttons near the LCD screen.

The information available is:

- **LAN IP** - The IP address of the Internal Network.
- **WAN IP** - The IP address of the Internet Connection.
- **DMZ IP** - DMZ IP address. The DMZ is often used as an internal Server network.
- **Gateway Address** - Default Gateway IP Address.
- **Firewall Status** - Firewall On, if the firewall is enabled or Firewall Off, if it is disabled.
- **User Authentication Status** - Enabled (LAN based users are required to authenticate) or disabled (LAN based user are not required to authenticate)

▼ Shutdown the edgeBOX

To shutdown the edgeBOX, press the Power button. edgeBOX will beep. Then,

- press the **Power** button again, and edgeBOX will beep twice and start the shutdown process,
- or press the LCD **Enter** button. edgeBOX will start the shutdown process and the message "Shutting down system. Wait..." will be displayed in the LCD.



You can also [shutdown the edgeBOX using the web interface](#)

2 Initial Configuration



If you turned on edgeBOX for the first time, you need to make an initial basic configuration so that edgeBOX can start work properly and be able to manage your network.

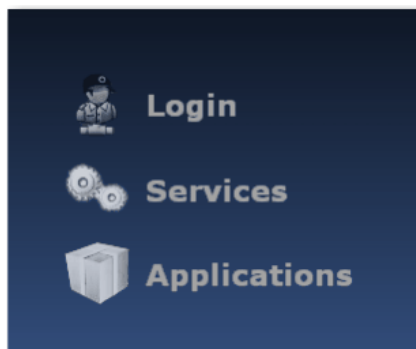
To quickly configure edgeBOX, do the next steps:

1. Open edgeBOX web management
2. Connect edgeBOX to the internet
3. Define the internal network (LAN)
4. Specify a hostname for the edgeBOX and a domain for the network
5. Check the date and time of the edgeBOX
6. Overview the default settings of the Firewall
7. Add users to the network
8. Change the password to access the edgeBOX web management

2.1 Open edgeBOX web management

To open the web interface of the edgeBOX:

1. Go to a computer **of the local network** (LAN).
2. With a browser, open the webpage <https://myedgebox.com>.
3. After the page opens, click the **link Login**.



edgeBOX initial page

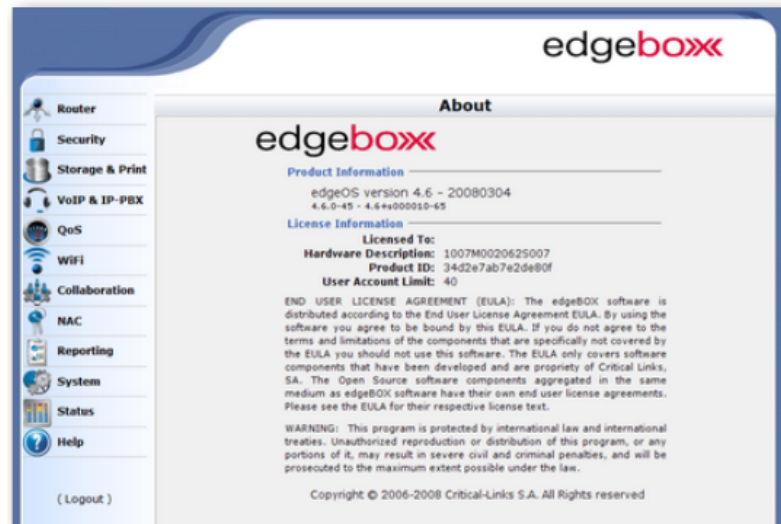
4. Use the username "admin" and the password "root" to login. This is the default password. For security reasons change it afterwards.

5. Click the **Login** button.


The edgeBOX web interface will then start load.

- It might take a few moments.
- You may have to accept one or more warning messages due to the Java Platform.

After the load is complete you will see the About page (it displays information about the edgeBOX version) and you can start configuring the edgeBOX.



edgeBOX web configuration - Homepage

 To use the edgeBOX web interface you need to have installed in the computer the Java Plug-in. Java Runtime Environment, version 1.4 or higher is needed.

Next Step: [Connect edgeBOX to the internet](#) >

Related Topics:

- [Add or remove users](#)

2.2 Connect edgeBOX to the internet

The **edgeBOX is the gateway** between your local network and the internet. The first step of the edgeBOX configuration is to connect it to the internet. To connect the edgeBOX to the internet **click the Router menu**. You should be on the Interfaces tab and Wan sub tab.

You can connect to the internet in 3 different ways or can just use the edgeBOX to manage your local network and not connect to the internet:

▼ **Use DHCP to get the needed information to connect to internet**

If you have a DHCP server that can give network information to the edgeBOX just **select the option DHCP** in the Connection Method. All the needed information will be **automatically obtained from the DHCP Server**.

▼ **Introduce the information manually using a Static connection**

You normally use a static connection if you have a **publicly registered domain**. In this case your IP address and gateway are always the same and you want to **configure the connection's properties yourself**.

Select Static in the Connection Method drop down list and then indicate:

1. The static IP address, and the netmask of your connection.
2. The IP address of your default gateway; the device that will receive and send the information to the Internet.
3. The IP address of your Name Server in the Primary DNS field.
4. Optionally, the IP address of your secondary Name Server, case you have one, in the Secondary DNS field.

▼ **Connect to the Internet using an ADSL connection**

You should choose the **PPPoE** option if your Internet connection is an **ADSL connection**. You have to indicate the following information then:

1. IP Address and Netmask (if you unselect the Obtain IP Automatically option).
2. Primary DNS Server IP Address and Secondary DNS Server IP Address (if you unselect the Obtain DNS Servers Automatically option)
3. Username and Password (your internet provider gives you this information)
4. VPI - a value from 0 to 255, VCI - a value from 32 to 2047 and Encapsulation Method (if you select the Internal Modem option)
 - Select the **Keep Alive** option if you want the edgeBOX to **keep trying to connect** to your internet provider **while the connection is not successfully established**. Otherwise, edgeBOX will try for only 30 seconds.
 - Select the option **Obtain IP Address Automatically** if you want the edgeBOX to **obtain the IP address** of the connection **dynamically during the setup**.
 - Select the option **Obtain Gateway Address Automatically** if you want the edgeBOX to **obtain the default gateway address** of the connection **dynamically during the setup**.
 - Select the Obtain DNS Servers Automatically option if you want the edgeBOX to obtain the IP addresses of the Primary and secondary DNS servers automatically, during the setup of the connection.

▼ **Use an ADSL connection with an internal modem**

The PPPoA method is used if you have an **ADSL connection** and an **internal modem**.

Select PPPoA connection method from the drop down list and select the **Internal Modem**

option. Then follow the steps like if you were connecting using an ADSL connection (like it is explained in the previous method).

▼ [Do not connect the edgeBOX to the Internet](#)

Select this option if you are just using the edgeBOX to manage your local network and **you do not want to connect to the Internet**. Select the option None in the Connection Method drop down list.

After you have chosen the method of connection, click the **Apply button** on the bottom right corner of the application **to save the change**.

Next Step: [Define the internal network \(LAN\)](#) >

2.3 Define the internal network (LAN)

You need to define the local network in the edgeBOX to make the edgeBOX work as the router of the network. **To define the local network:**

1. Click the Router menu.
2. Go to the Interfaces Tab and then to the LAN sub tab.

edgeBOX **has already a default local network** defined (192.168.100.254) so you don't have to configure it. However, you can change your LAN definitions if they do not fit the scenario of your network.

To change the local network:

1. Type the IP Address of the edgeBOX (IP Address of the edgeBOX's internal interface) in the IP Address field.
2. Type the network mask in the Subnet Mask field.
3. Click the Apply button on the bottom right corner of the tab to save the changes.



If you change the local network IP address, you will loose access to the edgeBOX web management.

- You need to indicate the new address of the edgeBOX in the browser to connect to the edgeBOX's web management. [View example.](#)

If you change the edgeBOX's IP Address to 10.1.1.254, type in your browser the address <https://10.1.1.254:8011>.

- You may also need to change the properties of the network connection of the computer you are using to manage the edgeBOX. [View example.](#)

If your computer receives the IP dynamically from the edgeBOX, you may need to ask the

operating system to repair the connection to gets a new IP address. Or if you have defined a static address in the connections of your computer, you need go change that address to a new IP address of the network.

Next Step: [Indicate a hostname for the edgeBOX and a domain for the network](#) >

2.4 Indicate a hostname for the edgeBOX and a domain for the network

Part of the edgeBOX initial configuration is to indicate the edgeBOX's network name and the domain of your network.

▼ What is the Hostname?

The Hostname is the **name by which the edgeBOX is known in the network** (the name that the computers of the network use to refer to the edgeBOX).

A hostname is a descriptive name. You can **choose any name you want**. If you have two offices and two edgeBOXes managing each one you can call one edgebox1 and the other edgebox2, for example.

▼ What is the Domain?


The Domain is **the name by which your network is known**.

If you do not have a registered domain, then you can give your network the domain you want. This domain will be private and **visible only within your network**. For example, if your company is called MegaSoft, then a possible domain could be megasoft.com.

If you have a registered domain, like critical-links.com, for example, then you can use that public domain. That domain is visible to everyone in the world throughout the Internet.

To change the hostname and the domain:

1. Click the **Router menu**.
2. Go to the Interfaces Tab and then to the Hostname and Domain sub tab.
3. Type the **hostname of the edgeBOX** in the Hostname field.
4. Type the **domain of the network** in the field Domain.
5. Click the Apply button on the bottom right corner of the tab to save the changes.

 If you change the domain or the hostname, you need to **reboot the edgeBOX so that the changes take effect**.

Next Step: [Check the date and time of the edgeBOX](#) >

2.5 Check the date and time of the edgeBOX

When you first install the edgeBOX, the date and time settings may be incorrect.

To verify the date and time **click the System menu**. The date and time properties are in the first tab. You can manage the date and time in one of two ways:

▼ [Use edgeBOX's date and time](#)

To correct the date and time:

1. Remove the selection from the option Use Network Time Protocol in case it is selected.
2. Type the actual day, month and year in the Date (D M Y) option.
3. Type the current hour, minutes and seconds in the Time (H M S) option.
4. Click the Apply button on the bottom right corner of the tab to save the changes.

▼ [Use a time server \(NTP Server\) on the internet to obtain the date and time](#)

An internet time server is a service that constantly gives your machine the accurate date and time. To use an internet time server:

1. Select the option **Use Network Time Protocol**.
2. Select a **time server** in the option Preferred NTP server from the list of time servers.
3. Click the **Apply button** on the bottom right corner of the tab **to save the changes**.

Next Step: [Overview the Firewall settings](#) >

2.6 Overview the firewall settings

When you configure the edgeBOX for the first time, **the firewall is by default already switched on and defined with a basic configuration**. To check the default configuration or change some settings:

1. Click the Security menu.
2. Go to the Firewall tab.

Options

☐ Require Users To Login ☒ Enable Firewall ☒ Enable WAN Ping Response

WebAdmin Access

☒ WAN ☒ DMZ

Services

Service	Internal	External	DMZ
flashoperator	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
dns	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
smtp	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ssh	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
imap	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ftp	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
http	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
pop3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
nagios	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
cti	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
monit	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ntp	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

☐ Select All

Firewall initial basic configuration

You can also select the **Require Users to Login** option. This will force the users of your network to login to have access to the Internet and will give you more control over who accesses the network services.

This is just a basic initial configuration. The firewall can have several configurations according to your needs. You can set those configurations now or come back to the Firewall settings area later on and improve the firewall's settings according to the services you'd like to provide in your network.

Next Step: [Add users to the network](#) >

Related Topics:

- [edgeBOX Firewall](#)

2.7 Add users to the network

You can allow everyone to use your network or just let specific users to use it. Allowing access only to specific users gives your network more security. To let only specific users access the network, you need to manage (create, edit and delete users) them and set how they authenticate (log in) in the network.

By default users are managed and authenticated locally on the edgeBOX.

▼ [Locally manage and authenticate users with the edgeBOX](#)

This is the default option so, in principle, you don't need to make any change. **To manage and authenticate users with the edgeBOX:**

1. Click the **NAC** menu.

2. Go to the **Authentication Type** tab.
3. Choose the **Local Server** option on the Authentication
4. Click the **Apply button** to save the change.

Then you need to create users, give them usernames and passwords and access privileges.
[How to create a new user?](#)

Several configurations are possible when creating users. For now, if it suites your intentions, just create users in a simple way (you can change the users privileges later), using this privilege settings:

- Assign users to the Generic Access Policy.
- Give users access to Regular Services - so users can use the internet, use email or transfer files, for example.
- Give users access to Windows Use - so users can access file and printer sharing, for example.

▼ [Remote manage and authenticate users with a remote server](#)

This means that you create, delete, etc. the users of the network **using a remote server** like Radius, AD or LDAP Server, **instead of the edgeBOX**. It also means that when the user logs in in his computer, **the authentication is made in that remote server** because it is there that his login and password are stored.

You can use **three types of Remote Servers**:

- [AD Server](#)
- [LDAP Server](#)
- [Radius Server](#)

[How to configure the remote authentication on the edgeBOX?](#)

▼ [Do not force users to authenticate](#)

You can allow users to **access the network without needing to log in**. If you choose this option you don't need to create or add users. However, you need to remove the selection from the options that forces users to login when accessing the network in the firewall section:

1. Go to the Security Section.
2. Go to the Firewall tab and General sub tab.
3. Unselect the Require User to Login option.
4. Click the Apply button on the bottom right corner of the tab to save the changes.



Not forcing users to log in is more insecure. It does not give you control over which services each user can or cannot access. It allows every person to use your network if they have access to a computer of your network.

By default, edgeBOX has already two users created. You can use them to view how they are configured and to do quick experiments, for example user authentication to access the network

services. Their usernames are "user" and "user2". The passwords of both of them is "password".

Next Step: [Change the password to access the edgeBOX web management](#) >

Related Topics:


- [Add or remove users](#)

2.8 Change the password to access the edgeBOX web management

When the edgeBOX is installed, the administrator's ("admin") **password is by default the word "root"**.

To change the password:

1. Click the **System menu**.
2. Go to the **Administrator tab**.
3. In the Password field type your **new password**.
4. Retype your new password in the Confirm Password field.
5. Click the **Apply button** in the bottom right corner of the application to **save the changes**.

 It is **very import** that you **change the** administrator's **password** to prevent unauthorized accesses.

3 Router



The Router section is where you can **overview and configure** most details and functionalities **of your network**.

- [set the internet connection](#) (WAN), [change the local network](#) (LAN) properties,
- [overview your virtual networks](#) (VLANs) and [specify a domain and a hostname](#).
- [observe the routes managed by the edgeBOX](#) (system routes) and create and [manage your own routes](#) (static routes).
- [configure edgeBOX's DNS server](#); add and remove domains, manage access controls (ACLs) or [use Dynamic DNS](#).
- [manage DHCP](#). edgeBOX has a DHCP server that allows you to automatically attribute IP addresses to the computers of your network based on ranges of IP address or based on specific IP Addresses.
- Allow computers of the network to connect to outer networks like the Internet - [NAT](#).
- Allow remote computers to connect to a specific computer within your private network so they can use services this computer shares, like a web service or an email service - [Port Forwarding](#).
- Indicate [web sites that you do not want the edgeBOX to cache](#).
- [Update the firmware of edgeBOX's optional SpeedTouch ADSL Modem](#).

3.1 Configure the internet connection (WAN interface)

This option allows you to change the configuration for the external Interface, i.e., **allows you to indicate how the edgeBOX connects to the Internet** or another external network.

To indicate the type of connection, select the desired protocol from the Connection Method drop down list. You can select one of the following methods:

▼ [Static - Set the properties of the Internet connection manually](#)

If you selected Static in the Connection Method drop down list, you need to indicate the:

- IP Address
- Netmask
- Default Gateway
- Primary DNS Server IP Address
- Secondary DNS Server IP Address (optional)

Afterwards, click the Apply button in the bottom right side of the tab to save the settings.

1. Select the Static option 2. Introduce the required information

The screenshot shows the 'WAN' tab in the Router configuration interface. The 'Connection Method' is set to 'Static'. The 'Connection Status' shows '[Mon 04 Feb 2008 12:35:38 GMT] DHCP up'. The IP Address, Netmask, Default Gateway, Primary DNS Address, and Secondary DNS Address fields are highlighted with a red box. The values entered are: IP Address: 192.168.90.8, Netmask: 255.255.255.0, Default Gateway: 192.168.90.254, Primary DNS Address: 127.0.0.1, and Secondary DNS Address: (empty).

 The primary and secondary DNS servers you add here will be added to the list of DNS Servers in the [list of servers to forward queries to](#).

▼ DHCP - Connect to the Internet through a DHCP server

If you chose the DHCP connection method, you don't need to enter any additional information. The edgeBOX will get all needed information from the DHCP server.

Just click the Apply button in the bottom right side of the tab and check the status returned.

Select the DHCP option The edgebox will get all the necessary information

The screenshot shows the 'WAN' tab in the Router configuration interface. The 'Connection Method' is set to 'DHCP'. The 'Connection Status' shows '[Mon 04 Feb 2008 12:35:38 GMT] DHCP up'. The IP Address, Netmask, Default Gateway, Primary DNS Address, and Secondary DNS Address fields are highlighted with a red box. The values entered are: IP Address: 192.168.90.199, Netmask: 255.255.255.0, Default Gateway: 192.168.90.254, Primary DNS Address: 192.168.90.254, and Secondary DNS Address: (empty).

▼ PPPoE - Configure an ADSL type Internet connection

You should choose the PPPoE option if your Internet connection is an ADSL connection. You will also have to indicate the following information:

- IP Address (if you remove the selection in the Obtain IP Automatically option)
- Primary DNS Server IP Address and Secondary DNS Server IP Address (if you remove the selection in the Obtain DNS Servers Automatically option)
- The IP Address of the default gateway (if you remove the selection in the Obtain Gateway Address Automatically option)
- Username and Password (your internet provider gives you this information)
- VPI - a value from 0 to 255, VCI - a value from 32 to 2047, and Encapsulation Method (if you select the Internal Modem option)

You can override the MTU. This may be required by your Internet service provider if it has a lower MTU to avoid packet segmentation for example. To override it, select the option **Override MTU** and change the value in the text field to the desired one.

Select the **Keep Alive** option if you want the edgeBOX to keep trying to connect to your internet provider while the connection is not successfully established. Otherwise, edgeBOX will try for only 30 seconds.

Select the option **Obtain IP Address Automatically** if you want the edgeBOX to obtain the IP address of the connection dynamically during the setup.

Select the **Obtain DNS Servers Automatically** option if you want the edgeBOX to obtain the IP addresses of the Primary and Secondary DNS servers automatically during the setup of the connection.

Select the option **PPPoE over VLAN** if you need your traffic to the Internet to go marked with the VLAN ID. Your Internet service provider may require you that. If you select this option, indicate the VLAN tag in the Tag field.

Connection Method: PPPoE

Connection Status: [Fri 10 Oct 2008 07:01:46 BST] DHCP up

IP Address:

Netmask:

Default Gateway:

Primary DNS Address:

Secondary DNS Address:

PPPoE over VLAN

Tag:

MTU

☐ Override MTU

MTU:

Connection Login

Username:

Password:

Connection Options

☐ Internal Modem ☒ Obtain IP Address Automatically ☒ Obtain DNS Servers Automatically

☒ Keep Alive ☒ Obtain Gateway Address Automatically ☒ PPPoE over VLAN

▼ **PPPoA - Set an ADSL type connection using an internal modem**

The PPPoA method is used if you have an ADSL connection and an internal modem.

Select the PPPoA connection method from the drop down list and select the Internal Modem option.

▼ **UMTS - Connect to the Internet using an UMTS or 3G network**

Choose this option if you want to connect to an UMTS or a 3G cellular network. This option is only available in the Connection Method drop down list if you have a cellular gateway card installed.

You have to indicate the following information:

- IP Address and Netmask
- Default Gateway
- Primary DNS Server IP Address and Secondary DNS Server IP Address
- Pin (identification number used to connect to the network)
- Protocol (only IP is currently supported)
- APN (name used to identify the network to connect. E.g.: internet.company.com)
- OPSYS (to select the mechanism to connect to the network):
 - a. Only connects to GSM Networks
 - b. Only connects to UMTS Networks
 - c. If you have a choice, connects to GPRS first
 - d. If you have a choice, connects to UMTS first

e. Automatically let V3G decide.

The Automatically Let V3G Decide option allows the network interface to determine which network to connect to.

An information area is also displayed showing details of the connection to the cellular network. Some of these details are the registration number, network provider, network type, signal strength and the connection status.

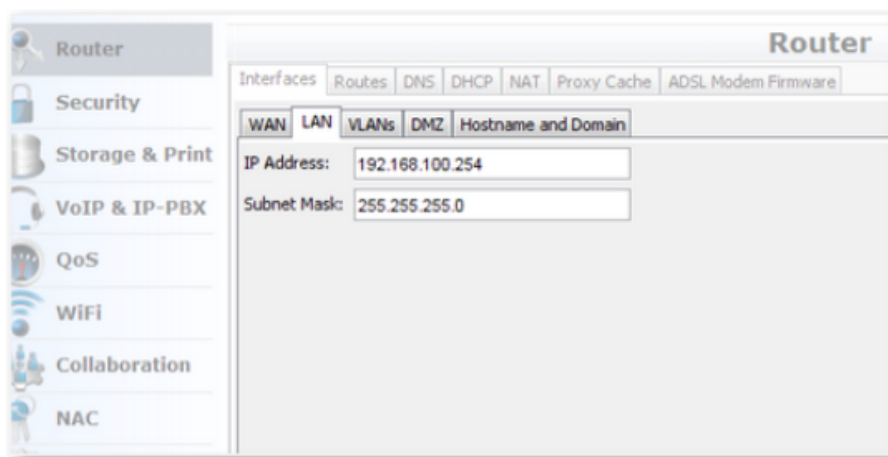


Contact your partner or supplier to obtain the list of currently supported UMTS hardware.

3.2 Change the local network properties (LAN interface)

To change the properties of your local (internal) network:

1. Type the desired **IP Address for the edgeBOX** (IP Address for the edgeBOX's internal interface) in the IP Address field.
2. Type the **network mask** in the field Subnet Mask.
3. Click the **Apply button** on the bottom right corner of the tab **to save the changes**.



LAN configuration panel



If you change the local network IP address, you will loose access to the edgeBOX web management.

- You need to indicate the new address of the edgeBOX in the browser to connect to the edgeBOX's web management. [View example.](#)

If you change the edgeBOX's IP Address to 10.1.1.254, type in your browser the address <https://10.1.1.254:8011>.

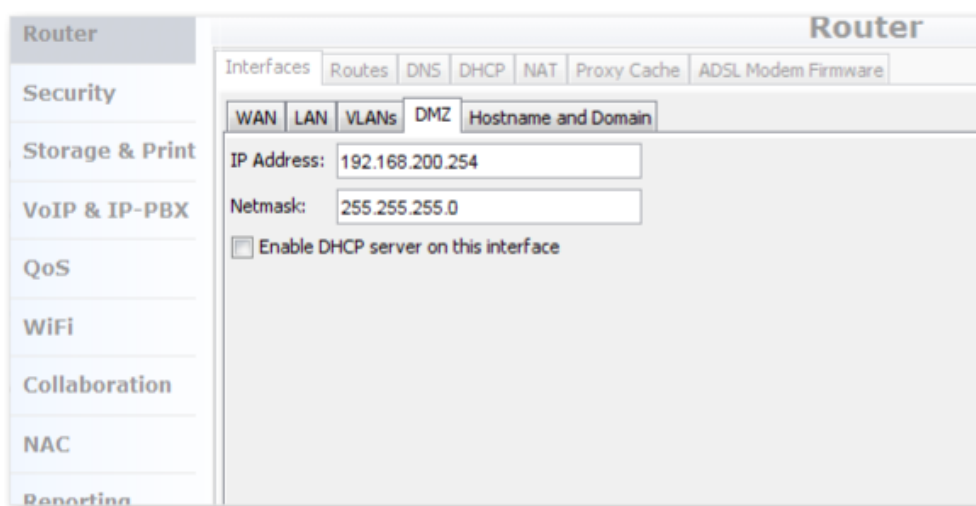
- You may also need to change the properties of the network connection of the computer you are using to manage the edgeBOX. [View example.](#)

If your computer receives the IP dynamically from the edgeBOX, you may need to ask the operating system to repair the connection to get a new IP address. Or if you have defined a static address in the connections of your computer, you need to change that address to a new IP address of the network.

3.3 Change the DMZ settings

To change the properties of your DMZ network:

1. Change the IP Address and the Netmask fields with the desired information.
2. Click the Apply button in the bottom right corner of the tab.
3. Select the Enable DHCP Server on this Interface if you wish to have DHCP also on the DMZ network.
4. Check the status returned to see if the operation was successful.



DMZ configuration panel



To have the Enable DHCP Server on this Interface option available, you need to have the firewall settings configured to allow DMZ.

▼ [Allow DMZ on the edgeBOX firewall](#)

1. Click the Security menu.
2. Select the Firewall tab and the DMZ subtab.
3. Select the option activate DMZ.
4. Click the Apply button on the bottom left corner of the tab.

3.4 View and manage the VLANs

edgeBOX allows you to have **up to five VLANs working on your network**. [Why to use VLANs?](#)

VLANs offer higher performance because they limit packet broadcasts in the network. They also provide additional security by separating groups of devices.

You can use VLANs, for instance, to:

- **Control bandwidth usage and make the network faster** - For example, you have more than 200 devices on your local network and your local network is getting slower because there is too many broadcast traffic (data that is sent from one computer to all computers in the network). VLANs will limit the broadcast only to the specified group of devices that are within a VLAN instead of broadcasting to all devices in the network.
- **Increase security** - If there are some groups of users that need more security due to the type of information they share between each other, a VLAN can isolate those users from the remaining network so that information will not be accessible for other groups.
- **Easily manage the network** - For example, separate users that have VoIP phones from users that do not have them.

Name	Tag	IP Address	Netmask	Enabled
Default VLAN (LAN)	1			yes
VLAN_A	4001	192.168.101.254	255.255.255.0	yes
VLAN_B	4002	192.168.102.254	255.255.255.0	yes
VLAN_C	4003	192.168.103.254	255.255.255.0	yes
VLAN_D	4004	192.168.104.254	255.255.255.0	yes
VLAN_E	4005	192.168.105.254	255.255.255.0	yes

Guest VLAN: VLAN_E

Edit Apply

VLANs configuration panel

On the VLAN panel you can:

- View the properties of the default VLAN. [What is the default VLAN?](#)

The default VLAN is your local network (LAN), i.e., if the packets of information that travel through your network don't specifically target a VLAN, they will be sent to the LAN.

- See and change properties of each VLAN in this panel.

▼ [Change the properties of a VLAN](#)

1. Select the desired **VLAN from the list** and click the **Edit button**.
2. Change the desired properties of the VLAN:
 - **Name** – A descriptive name to allow you to identify each VLAN.
 - **Tag** – The number that will be used on the network packets to allow the edgeBOX to send the packet to the correct VLAN. Each VLAN tag must be different.
 - **IP Address and Netmask** of the VLAN – Each computer on this VLAN will have an IP address from this range.
3. Click the **OK button**.
4. Click the **Apply** button to save changes.

▼ Disable or enable a VLAN

To disable a VLAN:

1. Select the desired enabled VLAN from the list and click the **Edit button**.
2. Unselect the Enabled option on the VLAN properties window.
3. Click the **OK button**. The Active property of the VLAN in the list should change to no.
4. Click the Apply button to save changes.

To enable the VLAN again, do the same process but select the Enabled option instead.

▼ Define the Guest VLAN

When you use 802.1x authentication on your switch, **the Guest VLAN is the VLAN the network users are temporarily assigned to** if they haven't authenticated yet or if they have introduced an incorrect username or password.

This VLAN usually has limited network privileges. It is commonly used to display information about how the users can authenticate properly into the network. After they authenticate, they are assigned to their respective VLANs. [View an example where VLAN 6 is used as the Guest VLAN...](#)

To configure the Guest VLAN:

1. Select the desired VLAN from the Guest VLAN drop down option list and click the Apply button.
2. Go to your switch then and configure it accordingly; indicate in the switch that the Guest VLAN is the VLAN you choose in edgeBOX.

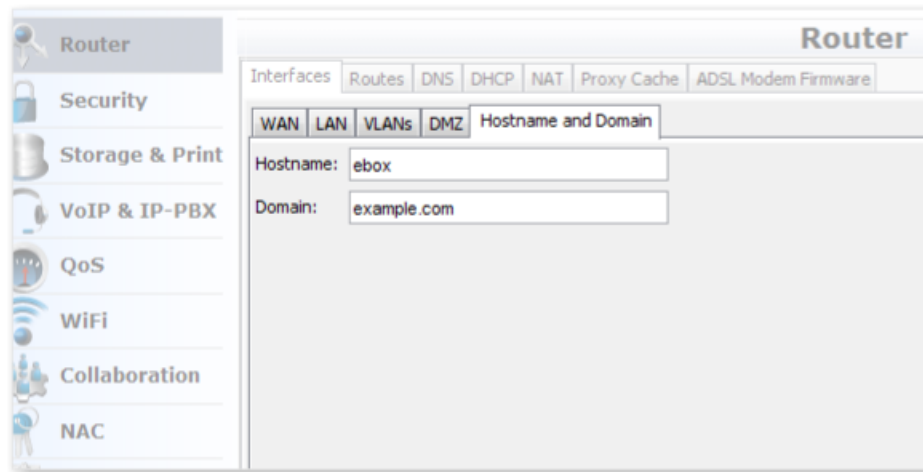
If you don't wish to have a Guest VLAN, select None in the Guest VLAN drop down list.

3.5 Change the hostname of the edgebox

You can find the Hostname of the edgeBOX in the Hostname and Domain sub tab of the Interfaces tab. [What is the Hostname?](#)

The Hostname **is the name by which the edgeBOX is known in the network** (the name that the computers of the network use to refer to the edgeBOX). A hostname is a descriptive

name. **You can choose any name you want.** If you have two offices and two edgeBOXes managing each one you can call one edgebox1 and the other edgebox2, for example.



Hostname and Domain configuration panel

To change the name of the edgeBOX (hostname):

1. Type the **new name** in the hostname text box (the hostname must have less than 16 characters).
2. Click the **Apply** button.
3. Click **Yes** in the confirmation message to reboot the edgeBOX
4. Check the status returned to see if the operation was successful.

i edgeBOX **does not update** the [reverse hosts files](#) of the [DNS Domains](#) when you **change the hostname** and you have networks defined on the edgeBOX (the local network or the VLANs) that do not belong to network classes A, B or C.

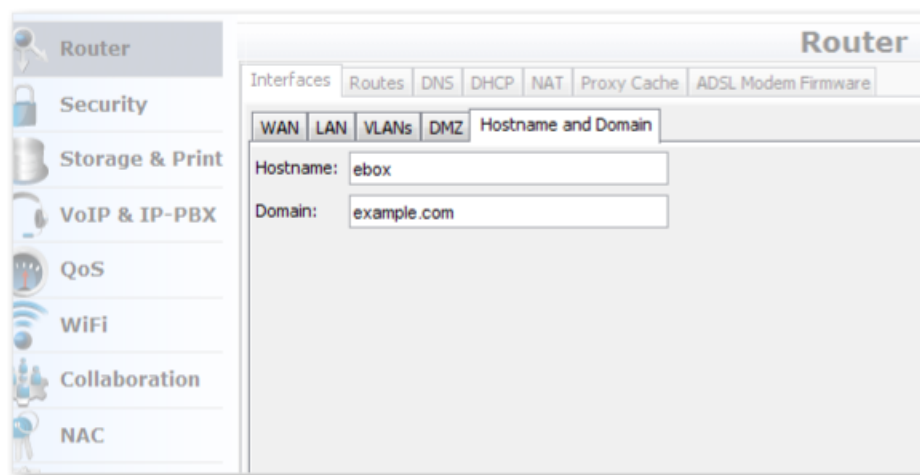
3.6 Indicate a domain for the network

You can find the Domain of the network in the Hostname and Domain sub tab of the Interfaces tab. [What is the Domain?](#)

The Domain is **the name by which your network is known**.

If you do not have a registered domain, then you can give your network the domain you want. This domain will be private and **only visible within your network**. For example, if your company is called MegaSoft then a possible domain could be megasoft.com.

If you have a registered domain, like critical-links.com, for example, then you can use that public domain. That domain is visible to everyone in the world throughout the internet.



Hostname and Domain configuration panel

To change the domain of the network:

1. Type the new domain in the domain textbox.
2. Click the **Apply** button.
3. Click **Yes** in the confirmation message to reboot the edgeBOX
4. Check the status returned to see if the operation was successful.

i If you change the domain you need to **reboot the edgeBOX so that the changes take effect.**

3.7 View the system routes

If the edgeBOX interfaces (WAN, LAN and VLAN properties) are configured correctly, **you should not need to make any changes to this tab** supposedly. The System Routes list should have several routes:

- **A route for your local network (LAN interface).**
If your local network is 192.168.100.0/24, for example, the list should have a route with the following information:
192.168.100.0 | 255.255.255.0 | 0.0.0.0 | LAN
- **A route for your DMZ network.**
If your local network is 192.168.100.200/24, for example, the list should have a route with the following information:
192.168.100.200 | 255.255.255.0 | 0.0.0.0 | DMZ
- **A route for every virtual local network (VLANs interfaces).**
If, for example, you have a VLAN named VLAN_B with the properties: 192.168.102.0/24 in the edgeBOX's vlan3 interface, the list should have a route with the following information:
192.168.102.0 | 255.255.255.0 | 0.0.0.0 | vlan3 (VLAN_B)

- **A route for the internet** (WAN interface).
If the network is 192.168.170.254/32, for example, the list should have a route with the following information:
192.168.170.254 | 255.255.255.255 | 0.0.0.0 | WAN
- **A route for the edgeBOX** (Loopback route).
A route that is used in case you do not have a connection to the exterior. The list should have a route with the information similar to:
127.0.0.0 | 255.0.0.0 | 0.0.0.0 | lo
- **A default route** (typically, the address of the WAN interface – the gateway address).
If your gateway has the IP address 192.168.170.254, for example, the list should have a route with the following information:
0.0.0.0 | 0.0.0.0 | 192.168.170.254 | WAN

The screenshot shows the 'Router' configuration window with the 'Routes' tab selected. It contains two tables: 'System Routes' and 'Static Routes'.

IP (destination)	Netmask	Gateway	Device
192.168.100.0	255.255.255.0	0.0.0.0	LAN
192.168.100.200	255.255.255.0	0.0.0.0	DMZ
192.168.101.0	255.255.255.0	0.0.0.0	vlan2 (VLAN_A)
192.168.102.0	255.255.255.0	0.0.0.0	vlan3 (VLAN_B)
192.168.170.254	255.255.255.0	0.0.0.0	WAN
127.0.0.0	0.0.0.0	0.0.0.0	lo
0.0.0.0	0.0.0.0	192.168.170.254	WAN

IP (destination)	Netmask	Gateway	Device
------------------	---------	---------	--------

At the bottom of the panel are three buttons: 'Add', 'Edit', and 'Delete'.

System and Static Routes configuration panel

In this panel you can also [manage Static Routes](#) - additional routes that you can create and modify.

3.8 Manage static routes

If the edgeBOX interfaces (WAN, LAN and VLAN properties) are configured correctly, all necessary routes should be created by the edgeBOX and you **should not need to create any routes manually** (any static routes).

If you need to manually configure routes on the edgeBOX, use the Static Routes list. You can:

▼ Create a new route

To create a new route, on the Routes panel:

1. Click the **Add button**. It will open a new dialog window.
2. Indicate the **IP address of the destination network or host**.
3. Indicate the **Netmask** of the IP address introduced before.
4. Indicate the **Gateway** (the machine to reach the destination network or host).
5. Click the **OK button to save the new route**.

The added route will appear in the Static Routes list.

▼ Edit a static route

To modify a created route, on the Routes panel:

1. Select the **route you want to modify** from the Static Routes list and click the **Edit button**. A window with the routes' properties will appear.
2. Change the desired properties of the route.
3. Click the **OK button** to save the changes and **check the returned status**.

▼ Delete a static route

To delete a created route, on the Routes panel:

1. Select the **route you want to delete** from the Static Routes list.
2. Press the **Delete button** below.
3. Check the **returned status** to see if the task was successfully.

The screenshot shows the 'Router' configuration window with the 'Routes' tab selected. It contains two tables: 'System Routes' and 'Static Routes'.

System Routes			
IP (destination)	Netmask	Gateway	Device
192.168.100.0	255.255.255.0	0.0.0.0	LAN
192.168.100.200	255.255.255.0	0.0.0.0	DMZ
192.168.101.0	255.255.255.0	0.0.0.0	vlan2 (VLAN_A)
192.168.102.0	255.255.255.0	0.0.0.0	vlan3 (VLAN_B)
192.168.170.254	255.255.255.0	0.0.0.0	WAN
127.0.0.0	0.0.0.0	0.0.0.0	lo
0.0.0.0	0.0.0.0	192.168.170.254	WAN

Static Routes			
IP (destination)	Netmask	Gateway	Device

At the bottom of the panel are three buttons: 'Add', 'Edit', and 'Delete'.

System and Static Routes configuration panel

In this panel you can also [overview the System Routes](#) - routes that are created and managed automatically by the edgeBOX based on the settings you have on for your LAN, WAN and VLANs.

3.9 Configure the DNS server

In the DNS tab you can view and change your the edgeBOX DNS Server configuration. DNS (Domain Name Server) is a service that can get information related to a domain, for example, what is the IP Address of a domain. [Learn about DNS](#) (wikipedia.org)

edgeBOX supports DNS through the well-known named server. It is possible to:

- configure **master, slave or forward** type name servers.
- grant **query access** from internal or external networks.

edgeBOX's DNS configurations are divided into the three first subtabs.

- [DNS General](#) – Shows the DNS status and the properties of the DNS server.
- [DNS Domains](#) – Where you can indicate all the domains that the DNS server will know.
- [Access Control](#) – Define access controls for the domains that the DNS server knows.

3.9.1 DNS General

On the bottom, you have two buttons, corresponding to two different actions:

- Stop/Start Service: The caption on this button will change depending on the service status; this button allows you to toggle its status.
- Apply: This button allows you to change the configuration.

DNS General | DNS Domains | Access Control | Dynamic DNS

Service State: **RUNNING**

Management of Reverse DNS: Auto

Global Options

Forward To

Server IP Address
192.168.90.254

Up

Down

New Delete

Lookup Mode: Local

Zone Transfer Format: Many

Zone Max. Transfer Time: 120 minutes

Stop Service Apply

- Service State: This item is read-only and provides information on the status of the service, i.e. if it is started or stopped.
- Management of Reverse DNS: Options are "Auto" (The reverse domain is automatically created) and "Manual" (the admin is responsible for creating the domain, if a reverse domain is required)
- Lookup Mode

If Forward is selected (this is an appropriate option, only if you have entered forwards), the edgeBOX will only forward queries.

If Local is chosen, requests are made to the forwarder and if not answered will attempt to find an answer locally.

- Zone Transfer Format: Options are "One at a time" and "Many".

Determines the format used by the server to transfer zones: many will pack as many records

as possible into a maximum sized message, whereas one will place a single record in each message.

- Zone Max.Transfer Time: Maximum time allowed for inbound zone transfers

3.9.1.1 Servers to forward to

This list contains the servers to where queries will be forwarded to if the domains queried are not in the list of domains. This will be the Name Server(s) used to resolve external domains. You will only be able to change this setting if you have a static configuration on the WAN side – otherwise this list is populated automatically from the information fetched from the DHCP or PPP server on connection setup. There are three actions possible:

New

A pop-window will appear. Just enter the IP address for the Name Server.

Delete

Select the Name Server IP and then select “Apply” for the changes to become effective.

Up/Down

To change the order in which the servers are queried.

3.9.2 DNS Domains

It is possible to configure master, slave and forward type name servers, as well as granting query access from internal or external networks.

In this table you have the list of domains configured, their type and access type. At least one entry should be shown here – the one corresponding to the local private domain. edgeBOX automatically creates the forward and reverse zones, and a set of hosts, depending on the configuration entered.

The available options are [Hosts](#), [New](#), [Edit](#) and [Delete](#).

The screenshot shows a web interface for configuring DNS domains. At the top, there are four tabs: "DNS General", "DNS Domains" (which is selected), "Access Control", and "Dynamic DNS". Below the tabs, the title "DNS Domains" is displayed. A table lists the configured domains. The table has five columns: "Domain Name", "Domain Type", "Resolve Settings", "Network", and "Access Type". One domain, "example.com", is listed with a "Master" type, "Direct" resolve settings, network "192.168.100", and "Internal" access type. Below the table, there are four buttons: "Hosts", "New" (highlighted with a blue dashed border), "Edit", and "Delete". An "Apply" button is located in the bottom right corner of the window.

Domain Name	Domain Type	Resolve Settings	Network	Access Type
example.com	Master	Direct	192.168.100	Internal

Hosts New Edit Delete

Apply

3.9.2.1 Hosts

This option allows management of the domain database. After highlighting a domain and pressing "Hosts", a new pop-up window will appear. In this window there is a table with all the entries for this domain database. Available actions are:

Name	Type	Value	TTL	Priority	PWP
ebox	A	192.168.90.254			
mail	A	192.168.90.254			
	MX	mail.example.com		10	
ns	A	192.168.90.254			
	NS	ns.example.com			

Add

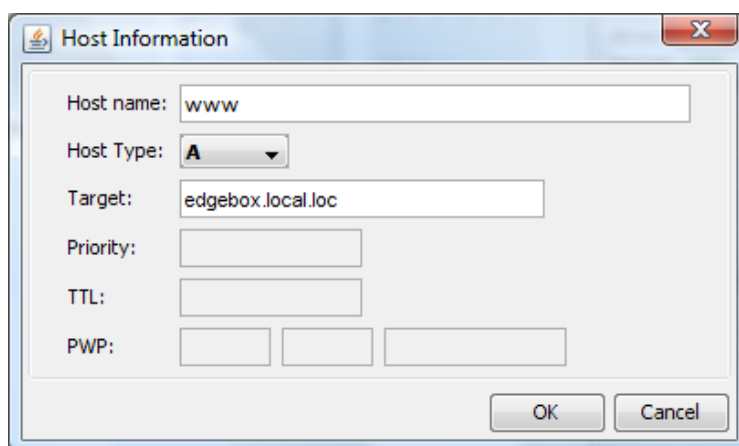
Allows you to add a new entry. A dialogue panel will be displayed requiring you to enter the following information:

- Host Name: the name of the host to be added;
- Host Type: Select from the list. Available choices are A, MX, NS, CNAME, SRV and TXT.
- Target: The IP or FQDN for this host
- Priority: Available if MX is selected. The lower this number, the higher the priority. This if one mail server is set as 5 and the other as 10, the mail server with a priority of 5 will be tried first.
- TTL: Allows you to specify how frequently domain data may change. It's common to set this value to several hours normally, but to push it down 5 minutes when changes to DNS are expected. The longer TTL means faster resolution times because of caching, but also means the data may be stale for longer.
- PWP (Priority, Weight, Port): Available if SRV Host Type is selected. Used when more servers are providing the same service

Priority: the priority of the target host, lower value means more preferred.

Weight: A relative weight for records with the same priority. Used in load balancing

Port: the TCP or UDP port on which the service is to be found.

A screenshot of a 'Host Information' dialog box. The dialog has a title bar with a small icon and a close button (X). Inside, there are several input fields: 'Host name' with the text 'www', 'Host Type' with a dropdown menu showing 'A', 'Target' with the text 'edgebox.local.loc', 'Priority' with an empty text box, 'TTL' with an empty text box, and 'PWP' with three empty text boxes. At the bottom right, there are 'OK' and 'Cancel' buttons.

Host Information

Host name:

Host Type:

Target:

Priority:

TTL:

PWP:

OK Cancel

Add Host Window

Edit

Allows you to change a record's information. The options available are the same as in "Add".

Delete

Deletes an entry from the database. Select the entry to delete and press "Delete".

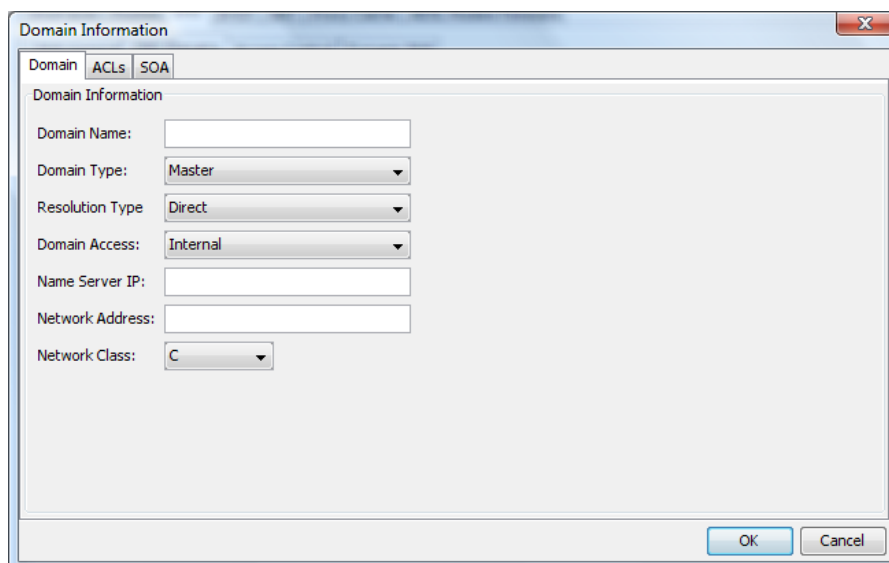
Remember that any of the changes made to the domain(s) database will only take effect after you select "Apply" in the main panel; if you don't select "Apply" then all changes will be lost.

3.9.2.2 New

This option allows configuration of a new domain. After you select this option a pop-up window will appear requiring you to enter the appropriate information:

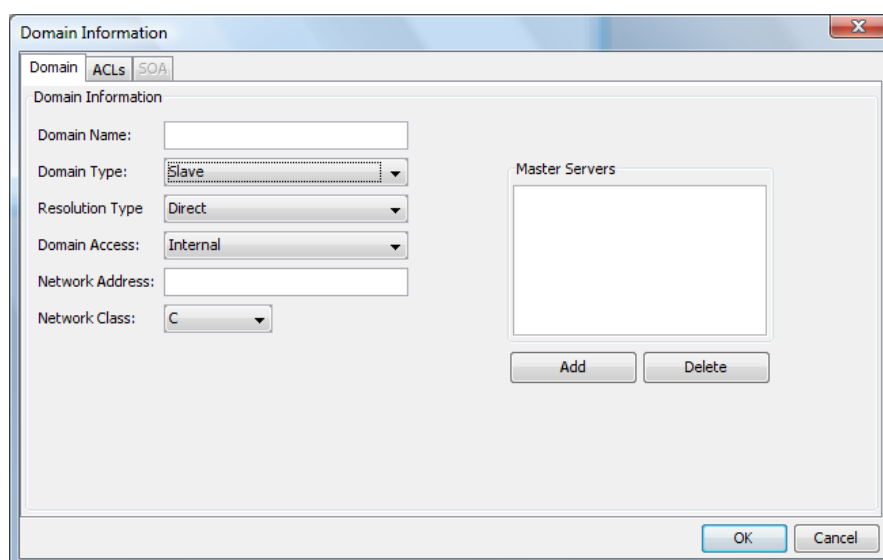
3.9.2.2.1 Domain

Three possible Domain Types are available, these are Master, Slave and Forwarder. Depending upon your choice, the available options vary as shown in the three images below:



The 'Domain Information' dialog box shows the 'Domain' tab selected. The 'Domain Type' is set to 'Master'. The 'Resolution Type' is 'Direct' and 'Domain Access' is 'Internal'. The 'Name Server IP' and 'Network Address' fields are empty. The 'Network Class' is set to 'C'. The 'OK' and 'Cancel' buttons are at the bottom right.

Field	Value
Domain Name	
Domain Type	Master
Resolution Type	Direct
Domain Access	Internal
Name Server IP	
Network Address	
Network Class	C

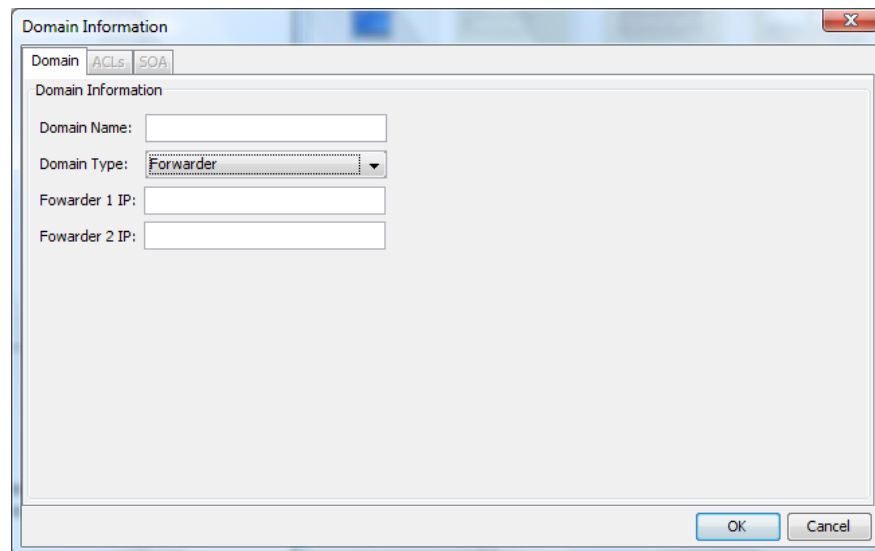


The 'Domain Information' dialog box shows the 'Domain' tab selected. The 'Domain Type' is set to 'Slave'. The 'Resolution Type' is 'Direct' and 'Domain Access' is 'Internal'. The 'Name Server IP' and 'Network Address' fields are empty. The 'Network Class' is set to 'C'. A 'Master Servers' section is visible on the right, containing an empty list box and 'Add' and 'Delete' buttons. The 'OK' and 'Cancel' buttons are at the bottom right.

Field	Value
Domain Name	
Domain Type	Slave
Resolution Type	Direct
Domain Access	Internal
Name Server IP	
Network Address	
Network Class	C

Master Servers

Buttons
Add, Delete



- Domain Name: the name of the new domain;
- Domain Type: Select a value from the list. The available selections are Master, Slave and Forwarder.

A master domain server is one which has the database for the domain stored locally (also called authoritative domain for that domain). It will answer the queries for that domain.

A Slave DNS gets its zone file information from a zone master and it will respond as authoritative for those zones for which it is defined to be a 'slave' (it is sometimes referred to as a secondary)

A forward domain server does not answer queries directly, but will forward them to another name server.

- Resolution Type: Direct and Reverse are the possible options. If Direct is chosen, when hosts are added, the forward entries are required (resolving names to IP's). If reverse is chosen, the host entries required map IP's to names
- Domain Access: Select a value from the list. The available selections are Internal and External. If you have a registered domain you will grant access to external networks to query this zone; otherwise for private domains you will most likely want to grant only to internal hosts for security reasons. This option is disabled for forward-type name servers.
- Name Server IP: The IP for this domain's name server. This option is disabled for forward-type name servers;
- Network Address: The network address for this network.
- Network Class: The network mask (A=255.0.0.0 or B=255.555.0.0 or C=255.255.255.0)
- Forwarder 1 IP/Forwarder 2 IP: If you've chosen type "Forward" this will be the IP addresses of the servers where queries for this domain will be forwarded.

3.9.2.2.2 ACL

Available for a Master or Slave domain (not forwarder) to control access to the domain.

The basic Internal domain allows access to query the domain from any LAN based IP

A basic External domain allows any IP to query the edgeBOX for this domain.

The panel below, shows that for this domain, only internal (any IP on the LAN, VLAN or DMZ) can make queries.

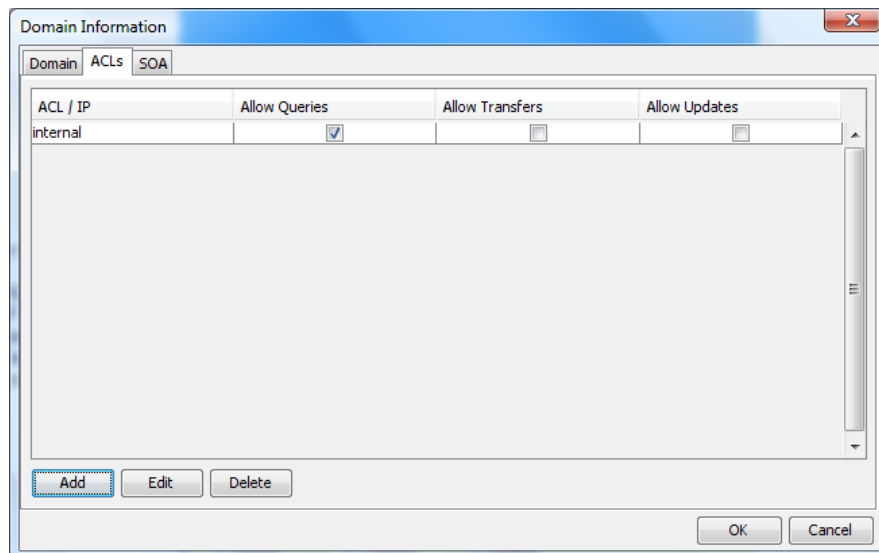
The panel shows:

ACL/IP: The named rule you are using for [access control](#)

Allow Queries: Indicates that queries are allowed for this (internal) domain

Allow Transfers: Indicates whether other servers are allowed to copy the zone information from the server

Allow Updates: Indicates whether other servers are allowed to submit dynamic updates to the edgeBOX for this domain

**Add**

This panel allows you to define the access for this domain. You can create access lists via the [Access Control](#) Panel

ACL Name: The name of the ACL you will add to this ACL list.

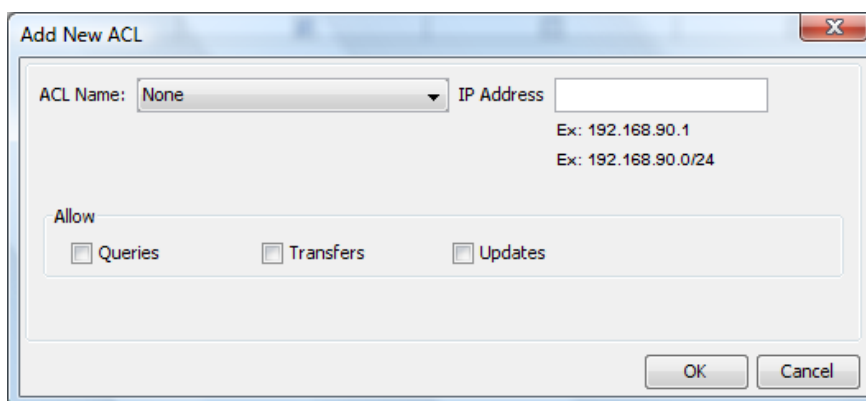
IP Address: You can add an IP or network, instead of selecting an ACL Name to add to the ACL Control List

Queries: If checked, queries are allowed for this ACL Name/IP Address

Transfers: If checked, servers in the ACL List are allowed to copy the zone information from the server

Updates: if checked, servers in the ACL List are allowed to submit dynamic updates to the

edgeBOX for this domain



The image shows a dialog box titled "Add New ACL". It has a close button (X) in the top right corner. Inside the dialog, there is a section for "ACL Name:" with a dropdown menu currently set to "None". To the right of this is an "IP Address" text input field. Below the IP address field, there are two example lines: "Ex: 192.168.90.1" and "Ex: 192.168.90.0/24". Below these fields is a section labeled "Allow" which contains three checkboxes: "Queries", "Transfers", and "Updates". At the bottom right of the dialog are "OK" and "Cancel" buttons.

Edit

Allows you to edit exiting ACL configuration for the domain

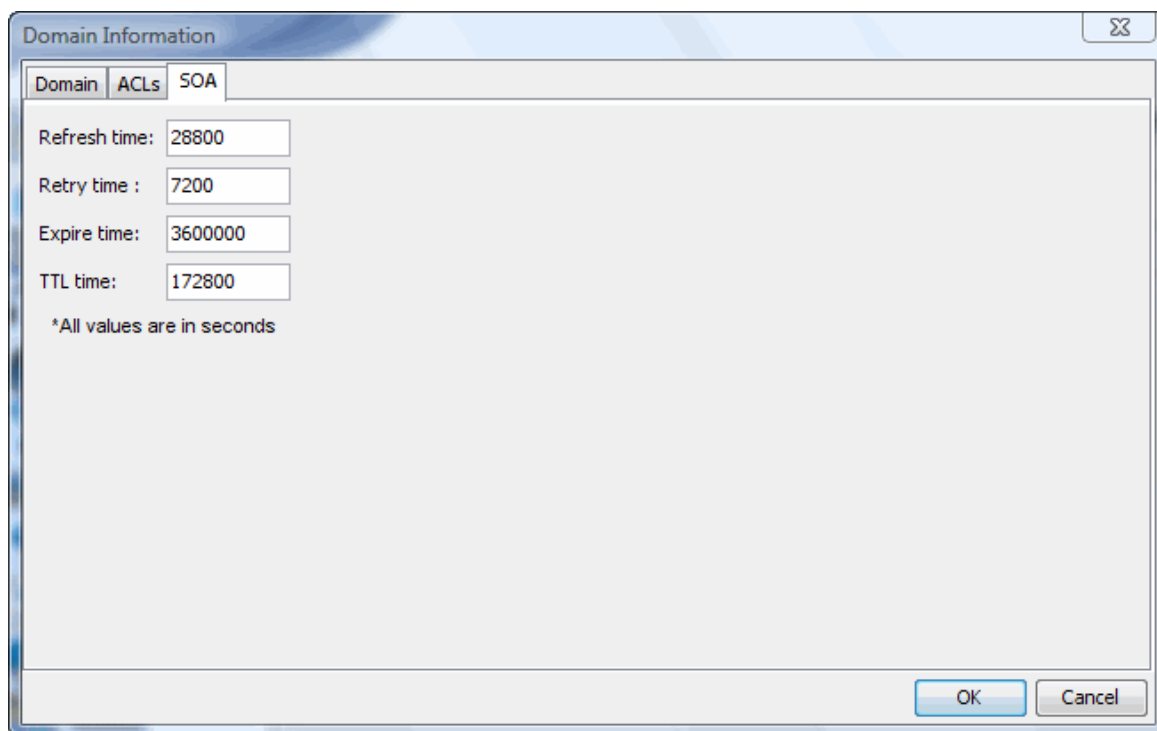
Select the ACL to edit and select "Edit". The options available are similar to the ones available when adding an ACL.

Delete

Deletes configuration information for a selected ACL. Select the ACL to delete and select "Delete".

3.9.2.2.3 SOA

This allows you to define a number of configuration parameters which will affect the selected domain.



The image shows a 'Domain Information' dialog box with three tabs: 'Domain', 'ACLs', and 'SOA'. The 'SOA' tab is selected. It contains four input fields for time values in seconds: 'Refresh time' (28800), 'Retry time' (7200), 'Expire time' (3600000), and 'TTL time' (172800). Below these fields is a note: '*All values are in seconds'. At the bottom right are 'OK' and 'Cancel' buttons.

Parameter	Value
Refresh time	28800
Retry time	7200
Expire time	3600000
TTL time	172800

*All values are in seconds

The available fields are:

- Refresh time: The number of seconds between the time that a secondary name server (slave) gets a copy of the zone (or sees that it hasn't changed), and the next time it checks to see if it needs a new copy.
- Retry time: The time which the edgeBOX will wait before querying a Master (if the master fails to respond to a request)
- Expire time: The number of seconds that lets the secondary name server(s) know how long they can hold the information before it is no longer considered authoritative.
- TTL time: Specifies the maximum amount of time other DNS servers and applications should cache the DNS record. You might wish to lower this if you are going to change your DNS entries and then increase it to a normal value after the changes have been made and tested

3.9.2.3 Edit

Allows you to change the configuration for an existing domain. Select the domain to edit and select "Edit". The options available are similar to the ones available when creating a [new domain](#).

3.9.2.4 Delete

Deletes configuration information for a selected domain. Select the domain to delete and select "Delete".

3.9.3 Access Control

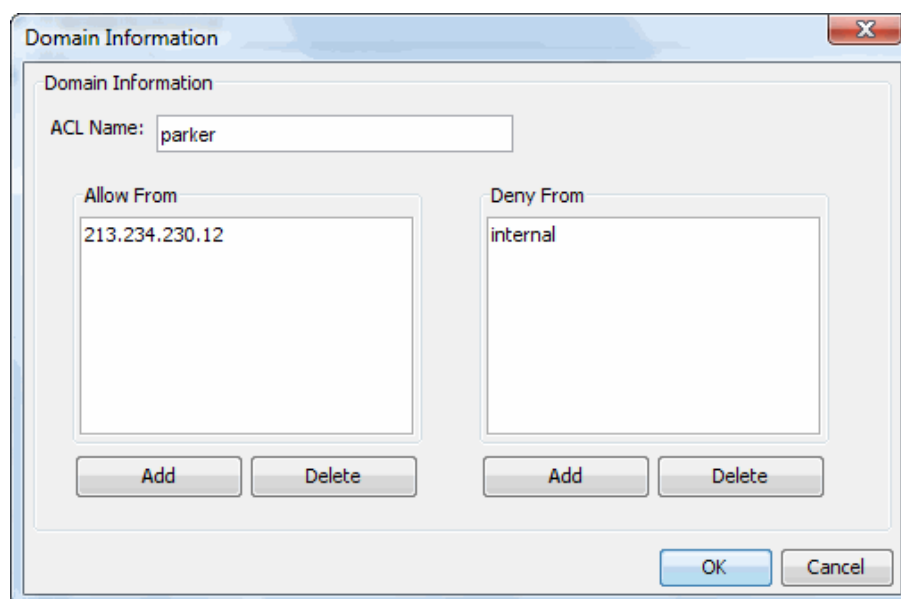
This panel allows you to deny/allow clients use of the edgeBOX to perform DNS lookups:

The screenshot shows the 'Access Control' tab in a router's configuration interface. At the top, there are four tabs: 'DNS General', 'DNS Domains', 'Access Control' (which is selected), and 'Dynamic DNS'. Below the tabs is the 'Access Control List' section, which contains a table with three columns: 'Name', 'Allow', and 'Deny'. The table has two rows: 'external' with 'any' in the 'Allow' column, and 'internal' with '127.0.0.1/8; 192.168.100.0/24; 192.168.104....' in the 'Allow' column. Below the table is a large empty text area. At the bottom left, there are three buttons: 'New', 'Edit', and 'Delete'. At the bottom right, there is an 'Apply' button.

Name	Allow	Deny
external	any	
internal	127.0.0.1/8; 192.168.100.0/24; 192.168.104....	

New Edit Delete Apply

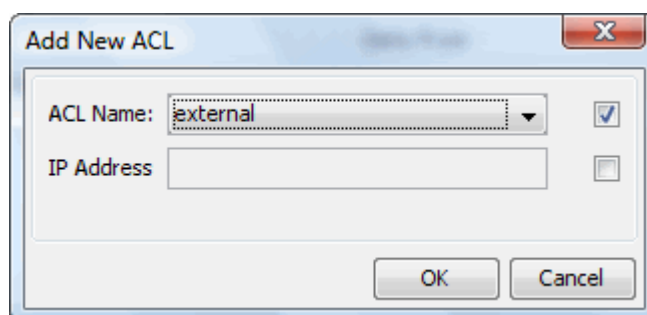
You may add individual IP's or a network of IP's (eg 192.168.100.0/24).



- **ACL Name** - The name of this ACL. Note that ACLs names must start with a letter and can consist of only letters and digits.
- **Allow from** - Access to this domain is available for IP's/Networks in this list.
- **Deny From** - Access to this domain is unavailable for IP's/Networks in this list.

Add

This allows you to add new entries to this ACL list. If ACL Name is checked, you can select an entry from the dropdown list, which include; external, internal, none, localhosts, localnets.



You can also check the IP address, to allow you to enter a specific IP (this deselects the ACL Name option and vice -versa). Entries which are created here are available for section (drop down menu) when setting the [ACL's](#) for a domain.

Note: Deny takes precedence over allow.

Delete

Highlight the entry in the "Allow From" or "Deny From" panel and pres the appropriate Delete button to remove an entry from the panel.

3.10 Use Dynamic DNS

Dynamic DNS is a service usually used when you **don't have a fixed IP Address** to connect to the Internet (static IP configuration on the WAN side) and you still **want to access your machines from external networks by a name of your choice**.

You can use one of the two supported dynamic DNS services:

- **DynDNS**
- **No-IP**

To see details on how to setup and manage an account on these services, consult www.dyndns.org or www.no-ip.org.

Enable Dynamic DNS

To enable dynamic DNS:

1. After you setup and manage an account on one these services, select that service in the Service Provider drop down option. A small form will appear below.
2. Indicate the **name you want to use** in the hostname field. This name is the **name that you created when you set up and managed the account** of the service. Type in the fully-qualified domain name (e.g.: `hostname.no-ip.org` or `hostname.dyndns.org`).
3. Indicate the **username and the password of the account** in the service account used for accessing the service chosen.
4. Click the **Apply** button to save the configuration.
5. If the operation was successful, click **Start Service**.

3.11 Overview the settings of the DHCP service

The DHCP Service assigns IP addresses to hosts (PCs, phones, etc.) on your internal network (both LAN and DMZ).

Router

Interfaces Routes DNS **DHCP** NAT Proxy Cache ADSL Modem Firmware

DHCP **Advanced**

Service State: **RUNNING**

Domain Name:

Max Lease Time: Default Lease Time:

Ranges

Start IP Address	End IP Address	Prefix
192.168.100.100	192.168.100.200	
192.168.101.100	192.168.101.200	
192.168.103.100	192.168.103.200	

MAC - IP

MAC Address	Fixed IP Address

System and Static Routes configuration panel

Information

- **Service State** – Indicates you the status of the service, i.e. running or stopped.
- **Domain name** – Shows you the current internal domain name of the edgeBOX.

▼ Start or Stop the DHCP Service

To start the service click the Start Service button and check the status returned to see if the task was successful. The Service State label should indicate running.

To Stop the service, do the same process.

Options

Lease Time - The Lease Time is the length of time for which the host can use the IP Address given him by the DHCP Service before he needs again to ask the DHCP Service for a new one.

- **Default Lease time** – default duration in seconds the host can use the given IP Address.
- **Max. Lease time** – hosts can just ask for an IP Address and receive it and use it for the default lease time, or they can ask for a specific lease time.
In those cases, the DHCP service will give the IP address for the requested duration if it is smaller than the max. lease time. Or it will give him the IP address with the max. lease time if the requested duration is higher.

▼ Change the Lease Time

To change the default lease time or the maximum lease time type the desired values (in seconds) in the Default Lease Time or the Max. Lease Time text fields. Then, click the Apply button to save the changes and check the status returned to see if the task was successful.

Related Topics:

- [Assign IP addresses using Ranges](#)
- [Assign IP addresses using MAC-IP rules](#)
- [Configure DHCP advanced settings](#)

3.12 Assign IP addresses using Ranges

Here you can **define ranges of IP Addresses** that will be assigned dynamically. When a computer in the network will request a IP Address, the DHCP will assign him an available IP address from one of the existing ranges.

- You can **create several IP address intervals** as long as they **don't overlap each other**.
- For each IP address interval you can **define a prefix** that will be added to the last portion of the IP assigned **to form the hostname sent**.

▼ Create a new range

To create a new range of IP Addresses:

1. Click the New button below the Ranges list in the DHCP tab.
2. On the dialog window indicate the lower IP address of the range in the Start IP textbox.
3. Indicate the higher IP address of the range in the End IP textbox.
4. Optionally, type the prefix – the name added to the end of the IP Address sent to form the computer's hostname. [View details about the prefix](#)
 - Example - If you enter mobile as the prefix and the domain if your network is local.loc, then a host that receives via DHCP the IP address 192.168.100.200 will have the hostname mobile-200.local.loc.
 - Email Server - If you have edgeBOX email server running and you want to have domains or hosts in the SMTP Relay list, in the email server's Access Control definitions, then you **must** indicate a prefix.
5. Click the OK button.
6. Click the Apply button in the DHCP tab to save the changes.

▼ Delete a range

To delete a range of IP Addresses:

1. Select the desired range from the Ranges list.
2. Click the Delete button below the list.
3. Click the Apply button to save the changes.

 If you delete a DHCP range, the computers that receive IP addresses from that range may not be able to connect to your network the next time they are switched on.

Related Topics:

- [Assign IP addresses using MAC-IP rules](#)
- [Overview the settings of the DHCP service](#)
- [Configure DHCP advanced settings](#)


3.13 Assign IP addresses using MAC-IP rules

The MAC-IP section allows you to **assign always a same**, specific **IP address to a computer**, each times it requests an IP address to connect to the network, by indicating the computer's MAC address.

▼ [Create a new MAC-IP Rule](#)

To assign a specific IP address to a specific device:

1. Click the **New button** below the MAC-IP list in the DHCP tab.
2. On the dialog window indicate the MAC address of the desired device in the MAC Address field.
3. Indicate the IP address you want the device to always receive in the IP Address field.
4. Click the **OK button** of the dialog window.
5. Click the **Apply button** of the DHCP tab **to save the changes**.

 To find the MAC address of a computer you can use the ipconfig /all command in the command line of Windows systems or ifconfig in the command line of Linux systems.

▼ [Delete a MAC-IP Rule](#)

To delete a MAC-IP DHCP rule:

- Select the desired rule from the MAC-IP list.
- Click the Delete button below the list.
- Click the Apply button to save the changes.

Related Topics:

- [Assign IP addresses using Ranges](#)
- [Overview the settings of the DHCP service](#)
- [Configure DHCP advanced settings](#)

3.14 Configure DHCP advanced settings

The Advanced options tab allows you to indicate a different device that will give the network Internet access. That is, the device that will work as a router. Use this option if you do not wish the edgeBOX to be your router (your gateway).

▼ [Use a different device as your gateway instead of the edgeBOX](#)

By default, the edgeBOX works as your gateway. To use a different device:

1. **Select the Use Custom Settings option.**
2. On the Gateway field indicate the **IP Address of the device that will be your gateway.**
3. Indicate the **external domain name** in the Domain Name field.
4. Add **one or more DNS Servers**. To add a DNS Server, click the New button of the Name Servers list and type the IP address of the desired DNS server in the pop up window.
5. **Click the Apply button to save the changes** and check the returned status to see if the task was successful.

▼ [Reset edgeBOX as gateway](#)

To reset the edgeBOX as your network gateway:

1. Remove the selection from the Use Custom Settings option.
2. Click the Apply button to save the changes and check the returned status to see if the task was successful.

Related Topics:

- [Assign IP addresses using Ranges](#)
- [Assign IP addresses using MAC-IP rules](#)
- [Overview the settings of the DHCP service](#)

3.15 Enable NAT on the private networks

In the NAT subtab you can view and change your NAT settings for your network. You can find this functionality in the NAT tab. [What is NAT?](#)

NAT (Network Address Translation) NAT translates the private IP addresses of computers in your local networks to a single public IP address, so that the computers can connect to outer networks like the Internet and have access to several services.

With NAT you are able to use private addresses in your internal network. All requests made from internal hosts are seen by the external networks as being made by edgeBOX which then translates the response packets' destination addresses to the originating internal host.

NAT is by default enabled on the edgeBOX. Also, by default it is already configured for the local network and for each of the VLANs. So you can connect to outer networks from the computers of your network immediately, without needed to configure anything.

▼ [Enable or disable NAT](#)

To enable NAT on the edgeBOX:

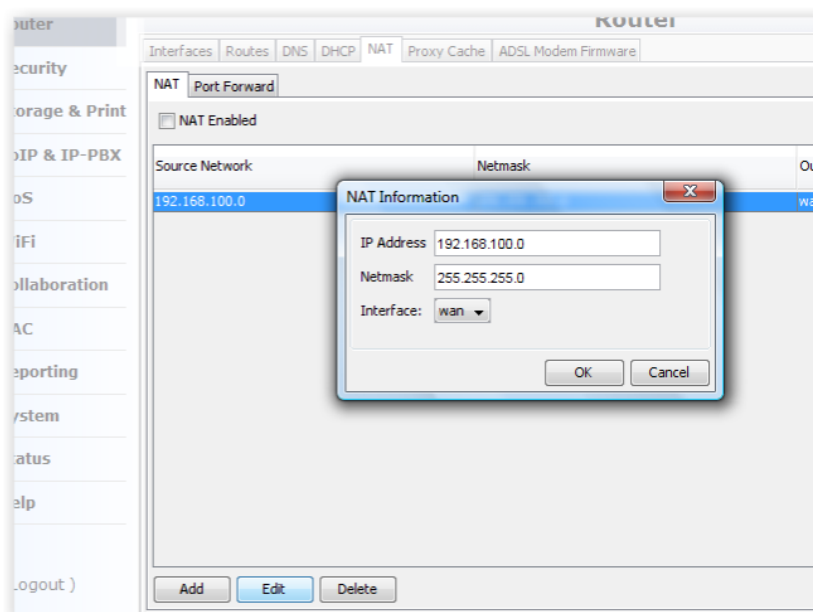
1. Select the option NAT Enabled on the NAT sub tab.
2. Click the Apply button on the bottom right corner of the tab.

To disable NAT remove the selection of the NAT Enabled option and click the Apply button.

▼ [Configure NAT on a network](#)

To configure NAT on an interior network:

1. Click the Add button below the list. A dialog window will appear.
2. Type the IP address and the netmask of the network you want to have NAT working (most likely it is your internal network, LAN).



3. Indicate the interface used to reach the network you just indicated in the Interface drop down list.
4. Click the OK button to close the window and save the information to the list.
5. Click the Apply button in the changes.

▼ Edit a NAT Configuration

To edit a NAT list entry:

1. Select the desired Nat configuration from the list and click the Edit button.
2. Modify the desired fields.
3. Click the OK button to close the window and update the information to the list.
4. Click the Apply button in the changes.

▼ Delete a NAT Configuration

To delete a NAT list entry:

1. Select the desired Nat configuration from the list and click the Delete button.
2. Click the Apply button in the changes.

3.16 Use Port Forwarding

You can find edgeBOX's Port Forwarding functionality in the subtab Port Forward, of the NAT tab. You can use port forwarding from your local network to the Internet and to your DMZ network (WAN and DMZ interfaces). [What is Port Forwarding?](#)

Port forwarding allows remote computers (e.g. public machines on the Internet) to connect to a specific computer within your private networks so they can use services that your computer shares, like a web service or an email service.

With port forwarding, you can make a service run on an internal host visible to the outside world, as if it was running on edgeBOX itself.

Port Forwarding Panel

▼ Add a port/service to Port Forward

To make one or more services available to exterior networks:

1. Define to each network you want to make it available (WAN or DMZ). Then **click the Add button** of the corresponding list (WAN or DMZ). A dialog window will appear.

2. **Indicate the external port** – the **port visible to exterior networks**. If you want to:
 - have just **one service visible**, select the External Port option and indicate the service's port in the textbox right after the label.

- have a **range of ports visible**, select the option From and indicate the the the begin value and the end value of the desired port range.
3. Indicate the **IP address of the computer** in your local network **that is running the service** you want to share in the Internal IP field.
 4. If you chose to:
 - make **just one service available, indicate the internal port** (the port where that service is running in the internal computer) in the Internal Port field.
 - make a **range of ports visible**, you can either **map all incoming requests** that arrive at those ports **to a single port** on the internal computer – select the Internal Port option and indicate the desired port, or you can **make a one-to-one mapping from the external port to the corresponding internal port** – select the Internal Range option.
 5. Click the **OK button** to close the window and save the information to the list.
 6. Click the **Apply button** to effectively save the changes.

▼ Edit a Port Forward configuration

To edit the properties of a service you have available (is in one of port forwarding lists):

1. **Select the corresponding list entry** of the desired list from the corresponding list and **click the Edit button** below the list.
2. In the properties window that will popup, change the desired properties.
3. **Click the OK button** to close the window and save the information to the list.
4. **Click the Apply button** to **effectively** save the changes.

▼ Delete a Port Forward configuration

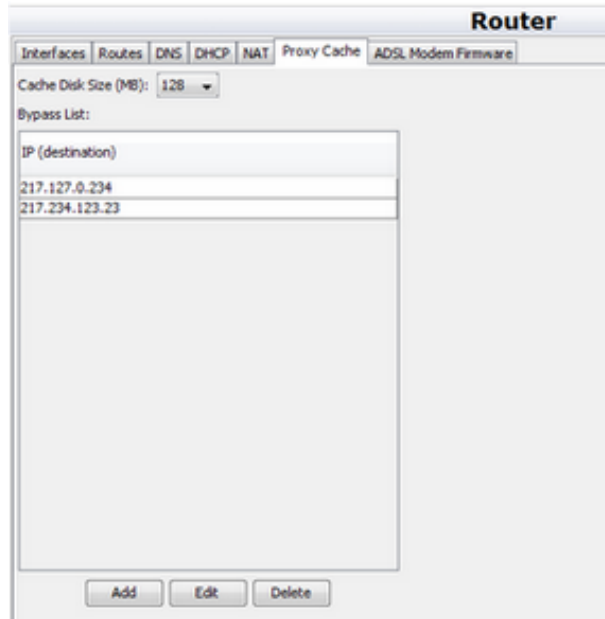
To delete a port forwarding configuration – to stop a service from being available to external networks:

1. Select the list entry you want to delete and **click the Delete button** below the list.
2. **Click the Apply button** to effectively delete the configuration.

3.17 Specify websites not to cache and change the cache size

You can indicate websites which you don't want the edgeBOX to make cache; cache exceptions. [About edgeBOX's cache.](#)

edgeBOX has a Proxy Server. It makes the webpages your network users consult more frequently to be loaded quicker. This is made by saving parts of the webpages in the edgeBOX.



Proxy Cache configuration panel

▼ Indicate cache exceptions

By default, edgeBOX caches all websites. You can indicate websites that you **don't** want the edgeBOX to cache. It may be useful for some specific websites, like websites that are very dynamic and their content changes constantly.

To indicate to the edgeBOX **not to** cache a website:

1. Click the **Add button** below the Bypass list.
2. Indicate the **IP address of the website** that the edgeBOX must not cache in the window that will pop up.
3. Click **OK** to add the IP address to the list.
4. Click **Apply to save** the IP Address that you added

▼ Edit a Cache Exception

To change the IP address of a website that you are currently not making cache:

1. Select the actual IP address of the website from the Bypass list and click the Edit button.
2. Indicate the **new IP address of the website** .
3. Click **OK** to update the IP address to the list.
4. Click **Apply to save** the IP Address that you changed.

▼ Delete a Cache Exception

Delete a cache exception if you want the edgeBOX to start caching a website it was not caching.

1. Select the IP address of the desired website from the Bypass list and click the **Delete**

button.

2. Click **Apply to save** the change.


▼ **Change the size of the Proxy Cache**


1. Select a value between 128MB and 8.192MB in the Cache Disc Size drop down list.
2. Click the Apply button in to save the change.

▼ **Do not cache websites (Stop the Service)**

By default edgeBOX caches the websites your network workers visit. This is, the Proxy Cache service is by default running. You can stop the service if you don't want edgeBOX to cache any websites.

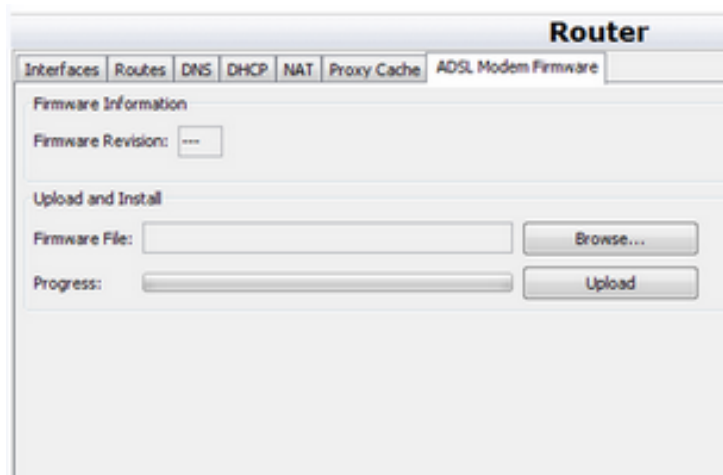
To stop edgeBOX's proxy cache click the **Stop Service** button in the bottom right side of the panel. To start caching websites again, click the Start Service button.

 **If you stop caching websites, edgeBOX will not be able to block access to websites** you may have blocked or block access to websites containing words and expressions you may have blocked in the [Content Filtering](#) options.

 If you have Premium traffic defined in the QoS section, this traffic is not cached by the edgeBOX.

3.18 Update the ADSL modem firmware

In the ADSL Modem Firmware tab you can upload and install the firmware for the SpeedTouch 330 USB ADSL modem, if you have one attached to the edgeBOX. You need to upload the correct firmware the first time you plug the modem into the edgeBOX.



The screenshot shows the 'Router' configuration interface with the 'ADSL Modem Firmware' tab selected. The interface includes a 'Firmware Information' section with a 'Firmware Revision' field. Below this is the 'Upload and Install' section, which contains a 'Firmware File' input field with a 'Browse...' button, a 'Progress' bar, and an 'Upload' button.

Firmware update panel for the ADSL modem

You can see the current version of the modem's firmware in the Firmware Revision display.

To upload and install the modem's firmware:

1. Get the firmware file from the modem's supplier and download it into your computer. You can obtain the firmware file at www.speedtouchdsl.com.
2. Extract the file from the downloaded ZIP file.
3. Click Browse and select the file from your computer.
4. Click Upload to upload the file to the edgeBOX and to install it (it may take a few minutes).

 Make sure you have the service FTP allowed on the [firewall](#) because the upload of the firmware file to the edgeBOX is made via FTP.

4 Security



This menu option allows you to review and change security settings such as:

- [Firewall](#) (services access, authorisation, black lists and DMZ configuration);
- [VPN IPsec](#) (Configure an encrypted IPsec tunnel(s)) and [VPN PPTP](#) (Configure an encrypted PPTP tunnel(s))
- [VPN L2TP](#) (Allows edgeBOX to act as a L2TP client)
- [Anti-Virus](#) (Scan File Shares and emails)
- [Content Filtering](#) of URL's

4.1 Firewall

This panel allows you to review and configure your Firewall configuration. By default, after installation, the firewall is on and external services are unchecked. However, https management (Webadmin Access) is allowed.

To become active, all actions performed in this page have to be committed by pressing the Apply button on the bottom-right panel. Three panels are available: [General](#), [DMZ](#) (if 3 NIC's are installed) and [Black List](#). To access each of these panels, select the appropriate tab.

Firewall Configuration Page

Firewall Configuration Page

4.1.1 General

Require users to login

If you check "require users to login", users will have to authenticate (providing username/password) in order to be able to access services and resources. Granting or revoking access to services and resources is done at the profile level. To know more about profiles see [Access Policies](#).

Enable Firewall

If this checkbox is turned off, edgeBOX will be working in pure router mode – all services will be available. If you turn this setting on, you will be able to control access to services and filter some type of attacks. If "require users to login" is enabled then you will not be able to change this

setting (it will be turned on by default).

Enable Wan Ping Response

If checked, allows machines to ping the WAN interface (useful for network fault debugging).

Normally, this would be unchecked.

WebAdmin Access

Wan

This checkbox controls whether the web administration interface can or cannot be accessed from the external network. Remember that if you are accessing the web interface from the external network and you deny access to it, you will not be able to reconnect again.

DMZ

This checkbox controls whether the web administration interface can or cannot be accessed from the DMZ network. Remember that if you are accessing the web interface from the DMZ network and you deny access to it, you will not be able to reconnect again.

Services

This panel allows you to grant or revoke access to the services running **on the edgeBOX** for hosts in the internal, external and DMZ networks. To grant access to a service (on the edgeBOX) in a network, just check the cell corresponding to the intersection of the service line with the network column. When you disable the firewall, all services are enabled by default.

Note: Enabling or disabling a service, allows or blocks access to that service on the edgeBOX. Blocking, for example, ftp, still allows users to ftp through the firewall to the outside.

Service	Internal	External	DMZ
flashoperator	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
dns	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
smtp	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ssh	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
imap	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ftp	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
http	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
pop3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
nagios	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
cti	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
monit	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
tftp	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
radius	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ldap	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
munin	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
voip	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
snmp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
samba	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
billing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
items	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

☐ Select All

4.1.2 DMZ

A DMZ is a small subnetwork that sits between a trusted internal network (for example, a Corporate internal network) and an untrusted external network (such as the Internet). This kind of network is used as a buffer between the two networks: hosts placed in this network are accessible either from trusted and untrusted networks, but cannot access the trusted network. Usually, these kinds of networks are used to house Internet servers (web servers, DNS servers, mail servers).

This interface is configured with an IP address range accessible from the external network (in case the external network is the Internet, this range will be a public range, and so your ISP must provide routing to it). Although this address space is accessible from the external network, you will have to explicitly grant access to hosts residing in it, via appropriate rules. Next, we will show the option available for configuring a DMZ.

GeneralDMZBlack List

☒ Enable DMZ

IP Address	Netmask	Port	Protocol
------------	---------	------	----------

Add

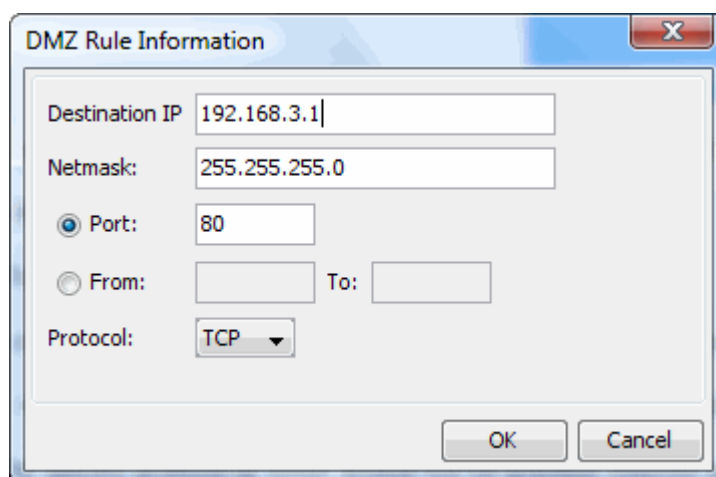
Edit

Delete

Apply

Enable DMZ

Checking this option will enable DMZ support. Make sure you configure an appropriate address range for the DMZ interface, and that traffic with this subnetwork as its destination, is being appropriately routed to edgeBOX. After checking this option you will need to create rules to grant access to hosts residing in this subnetwork. The rules are shown in a table which can be modified with the following options: New, Edit and Delete.



The image shows a 'DMZ Rule Information' dialog box with the following fields and options:

- Destination IP:** 192.168.3.1
- Netmask:** 255.255.255.0
- Port:** 80 (selected with a radio button)
- From:** (empty field) **To:** (empty field)
- Protocol:** TCP (selected in a dropdown menu)
- Buttons:** OK and Cancel

New

Allows you to enter a new rule. A pop-up window will display, requiring you to enter the following information:

- **Destination IP:** The host/range to which access will be granted;
- **Netmask:** The netmask to be used;
- **Port:** If you select this option, you will need to specify the single port to which access will be granted.
- **From... To:** if you select this option, you may specify a port range to which access will be granted
- **Protocol:** The specific protocol to which access will be granted. Choices available are TCP, UDP, ICMP and ALL.

Edit

Allows you to modify an existing rule. The options available are the same as in 'New'.

Delete

Selecting this option will eliminate the rule, revoking access to the host.

4.1.3 Black List

Deny all access to edgeBOX to specific external hosts (hosts on the Internet or WAN).

Add - Adds a Selecting this option will make a pop-up window appear. Just enter the IP address for the host you want to blacklist and then press OK.

Edit

Allows you to modify an entry in the black list table. A pop-up window will appear, filled with the entry selected. Press OK to change this entry in the table.

Delete

After selecting the host you want to eliminate from the list of blacklisted hosts, select "Delete". The line will be deleted from the list. You need to select "Apply" from the changes to become effective.

4.2 VPN

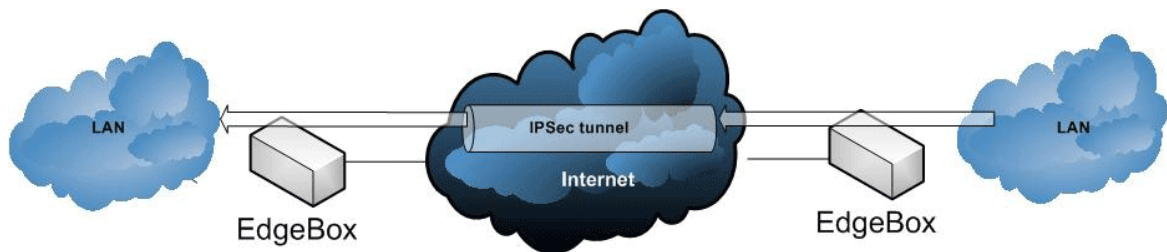
A Virtual Private Network (VPN) is a private network that uses a public network (usually the Internet) to connect remote sites or users together.

edgeBOX currently support three methods three methods of creating a VPN:

- [IPSec](#)
- [PPTP](#)
- [L2TP](#) (client)

4.2.1 IPSec

In this page you can review and change your IPSec VPN configuration. These kinds of VPNs are especially suited for establishing tunnels between two private networks over the Internet, connecting them securely.



IPSec VPN connecting two private networks

Globally you can perform two actions corresponding to the buttons present in the lower panel: toggle the service status (Start/Stop) and commit your changes (Apply). The elements present in this page are described below.

4.2.1.1 Service State

This element is read-only and gives the service status information (running or stopped).

4.2.1.2 Active Tunnels

This table shows you the active tunnels list. For each tunnel the following information will be displayed: local subnet, connection status, remote gateway and remote subnet.

4.2.1.3 VPN(s)

This table gives a list of the tunnels currently configured. Possible Operations are "Add", "Edit", "Status" and "Delete". You can also highlight an individual tunnel and start ("Start Tunnel" button) or stop ("Stop" button) the tunnel.

The screenshot shows a window with tabs for Firewall, VPN, Anti-Virus, and Content Filtering. The VPN tab is active, showing sub-tabs for IPsec, PPTP, and L2TP. The IPsec sub-tab is selected, displaying 'Service State: RUNNING' in green. Below this is a table for 'VPN(s):' with columns: Tunnel Name, Status, Local Network, Remote Gateway, and Remote Network. One tunnel named 'Tun' is listed with status 'Enabled', local network 'null/0', remote gateway '192.168.90.116', and remote network '192.168.91.0/24'. Below the table are buttons for 'Add', 'Edit', 'Status', 'Delete', 'Start Tunnel', and 'Stop'. At the bottom, there is a section for 'Active Tunnels' with columns: Local Subnet, Connection Status, Remote Gateway, and Remote Subnet. A 'Stop Service' button is located at the bottom right.

The "Start Service" button, allows you to start the IPsec service (this button then changes to a "Stop Service" button, to allow you to stop the service).

Note: If you stop the IPsec service, all tunnels will "fail"

Note: Each tunnel will be presented as a single entry (previous to V4.6, tunnels were represented but up to 3 entries)



Sometimes, when a tunnel is active for a long time or has no traffic passing through it, it stops working, even though the status displayed is Enabled. In this cases, if you received any complains that the tunnel is not working, Stop the tunnel and then Start it again to make the it work again.

4.2.1.3.1 Add

Adds a new tunnel configuration. After selecting this option a popup window will appear with a single (General) panel.

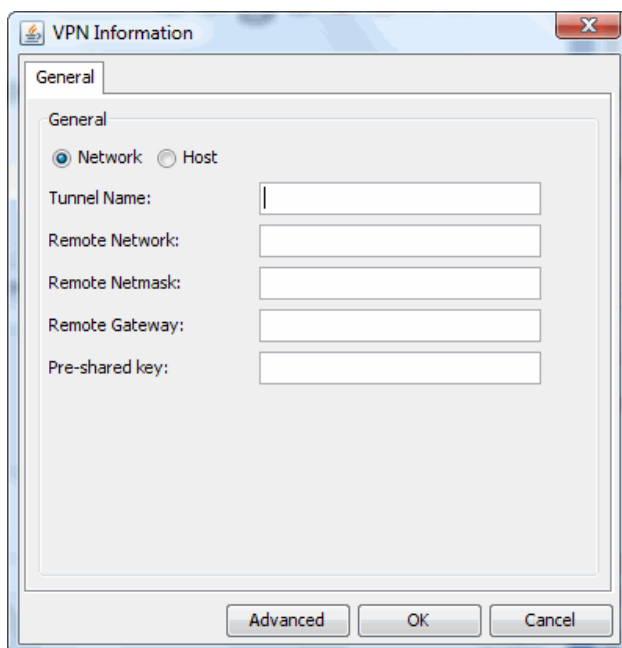
4.2.1.3.1.1 General

This panel allows you to configure general VPN settings.

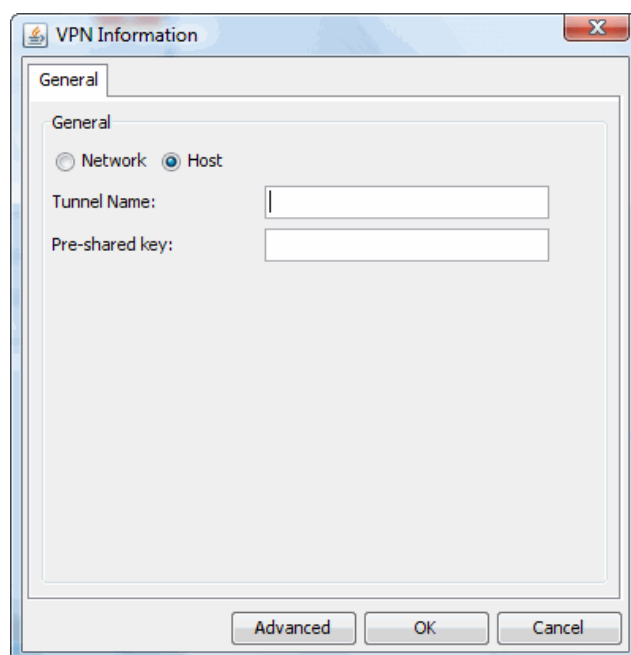
Choose between establishing a tunnel between the internal network and another network (Network), or between the internal network and a host (Host). The available fields will vary according to this choice.

The simplest method is to create a tunnel using the [Basic](#) (this is the default) panel. However, if you require more control over the configuration, you can select the [Advanced](#) button.

This panel allows you to configure a VPN tunnel with a minimum of information. That is, a number of parameters are automatically set for the user (you can view those parameters by selecting the [Advanced](#) button near the bottom of the Basic Panel).

Tunnel to a remote network**Tunnel to a remote computer**

The screenshot shows a window titled "VPN Information" with a close button (X) in the top right corner. Inside the window, there is a tab labeled "General". Below the tab, the text "General" is displayed. There are two radio buttons: "Network" (which is selected) and "Host". Below these are five text input fields with labels: "Tunnel Name:", "Remote Network:", "Remote Netmask:", "Remote Gateway:", and "Pre-shared key:". At the bottom of the dialog box, there are three buttons: "Advanced", "OK", and "Cancel".



Tunnel Name: A label chosen to identify this tunnel.

Remote Network: The IP address of the network we want to establish a tunnel with (eg 192.168.200.0)

Remote Netmask: Netmask to apply to the remote network IP address (eg 255.255.255.0).

Remote Gateway: The IP address for the gateway connecting to the remote network. This will be a public address.

Pre-shared Secret: Both local and remote ends of the tunnel must have the same key to initiate encryption. This key is the pre-shared secret (PSK).

The PSK should be generated from purely random characters.

Tunnel Name: A label chosen to identify this tunnel.

Pre-shared Secret: Both local and remote ends of the tunnel must have the same key to initiate encryption. This key is the pre-shared secret (PSK).

The PSK should be generated from purely random characters.

This panel allows you to view the default settings if you are creating an IPSec tunnel via the "Basic" method (note the button at the bottom of the panel, is now "Basic" to allow you to go toggle between the Basic and Advanced panel.

This panel has four tabbed entry panels for configuration.

The panels below show the options available for the "Advanced" selection (you can toggle between Basic and Advanced by selecting the Advanced and basic button)
Again, you can choose between establishing a tunnel between the internal network and another network (Network), or between the internal network and a host (Host).

The available fields will vary according to this choice.

Tunnel to a remote network

Tunnel to a remote computer

Aggressive Mode: Enables faster tunnel creation/operation as fewer messages are exchanged between peers, but exposes identities of the peers to potential eavesdropping, making it less secure.

Generally best to avoid aggressive mode if possible

Tunnel Name: A label chosen to identify this tunnel.

Tunnel Name: A label chosen to identify this tunnel.

Pre-shared key: Both local and remote ends of the tunnel must have the same key to initiate encryption. This key is the pre-shared secret (PSK).

The PSK should be generated from purely random characters.

Remote Network: The IP address of the network we want to establish a tunnel with (eg 192.168.200.0)

Remote Netmask: Netmask to apply to the remote network IP address (eg 255.255.255.0).

Remote Gateway: The IP address for the gateway connecting to the remote network. This will be a public address.

Pre-shared key: Both local and remote ends of the tunnel must have the same key to initiate encryption. This key is the pre-shared secret (PSK).

The PSK should be generated from purely random characters.

Local Network: This is the Local Network Address (eg 192.168.100.0)

Note that this must not be the same as the remote network.

Local Netmask: This is the Local Netmask for the network (eg 255.255.255.0)

Static IP: If checked, the Hostname/IP textfield is presented

Hostname/IP: Hostname or IP address of the remote PC

Local Network: This is the Local Network Address (eg 192.168.100.0)

Note that this must not be the same as the remote network.

Local Netmask: This is the Local Netmask for the network (eg 255.255.255.0)

Local ID Type: Options are: FQDN

IP Address

Email Address

Local ID: The Remote ID is used to explicitly set the ID of the local host.

Remote ID of the IPSec Client must match the Local ID of the IPSec Server

The entry is typically an IP address or a FQDN,

If the FQDN is preceded by an @ (eg [@critical.com](mailto:critical.com)), the system will not try to resolve the domain, but take it as a literal string (ie critical.com and not the FQDN critical.com)

This field is often left blank.

Remote ID: The Remote ID is used to explicitly set the ID of the remote host.

Remote ID of the IPSec Client must match the Local ID of the IPSec Server

The entry is typically an IP address or a FQDN,

If the FQDN is preceded by an @ (eg [@critical.com](mailto:critical.com)), the system will not try to resolve the domain, but take it as a literal string (ie critical.com and not the FQDN critical.com)

This field is often left blank.

Local ID Type: Options are: FQDN

IP Address

Email Address

Remote ID Type: Options are: FQDN

IP Address

Email Address

Local ID: The Remote ID is used to explicitly set the ID of the local host.

Remote ID of the IPSec Client must match the Local ID of the IPSec Server

The entry is typically an IP address or a FQDN,

If the FQDN is preceded by an @ (eg [@critical.com](#)), the system will not try to resolve the domain, but take it as a literal string (ie critical.com and not the FQDN critical.com)

This field is often left blank.

Remote ID:The Remote ID is used to explicitly set the ID of the remote host.

Remote ID of the IPSec Client must match the Local ID of the IPSec Server

The entry is typically an IP address or a FQDN,

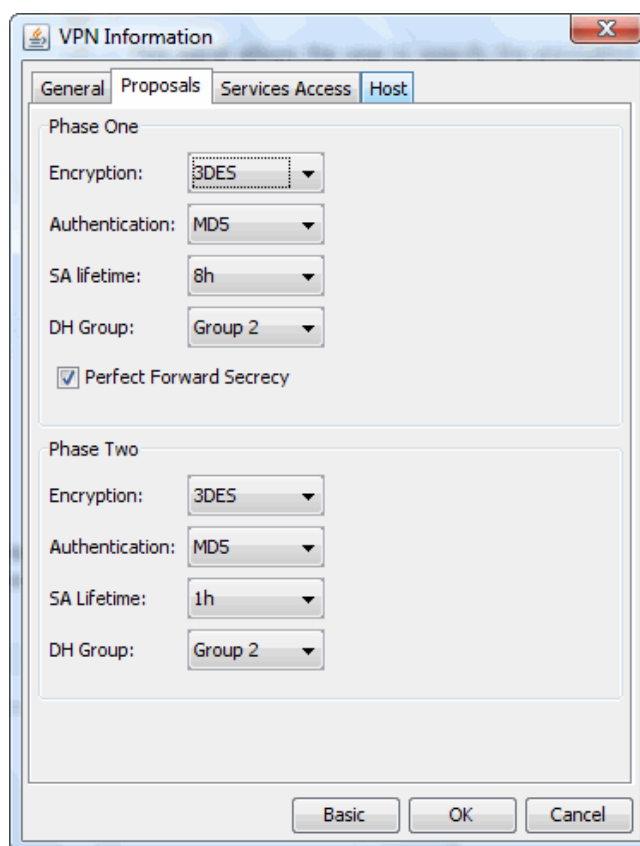
If the FQDN is preceded by an @ (eg [@critical.com](#)), the system will not try to resolve the domain, but take it as a literal string (ie @critical.com and not the FQDN critical.com)

This field is often left blank.

This panel allows the user to specify the encryption information for establishing the tunnel.

Option for Phase One are:

- Encryption: Options are 3DES or AES (128 bit encryption)
- Authentication: MD5 or SHA1
- SA Lifetime: 8 hours to 24 hours
- DH Group: Options are Group2 (1024bit) or Group5 (1536bit)
- Perfect Forward Secrecy: Usually set to on.



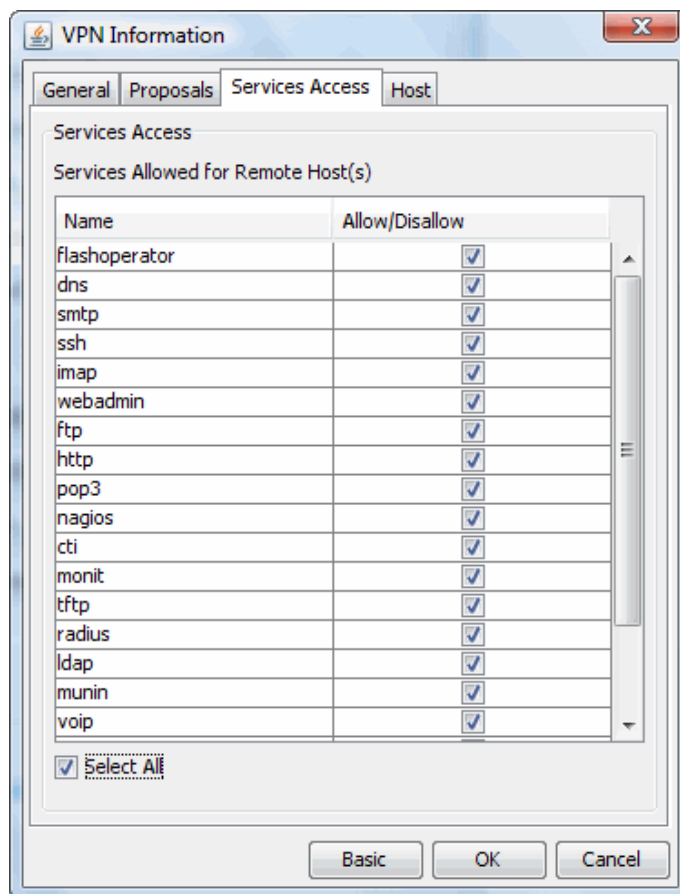
Option for Phase Two are:

- Encryption: Options are 3DES or AES (128 bit encryption)
- Authentication: MD5 or SHA1
- SA Lifetime: 1 hour to 8 hours
- DH Group: Options are Group2 (1024bit) or Group5 (1536bit)

Services Allowed for Remote Host(s)

In this table you can grant or revoke access to services running **on the edgeBOX** for hosts in the remote network. Check the cell corresponding to service desired to grant access, uncheck it to revoke access.

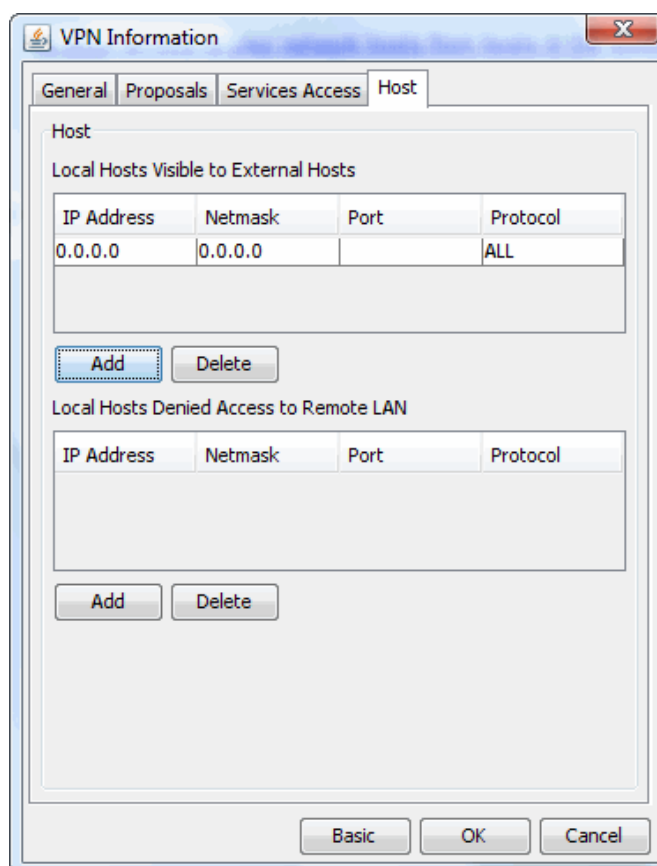
By default (Basic mode), all services are checked.



This panel allows you to configure access lists, specifically:

- [To allow access to your network hosts from hosts in the remote network](#)
- [To deny some of your local hosts access to the remote network.](#)

By default (Basic mode), all local LAN clients are accessible to the remote LAN



This panel allows you to configure local hosts' visibility from the external network. Available actions are "Add" and "Delete".

Add

After selecting "Add", a popup window will appear, requesting the following information:

- Origin: The IP address for the host in the network to which we want to grant access;
- Netmask: The netmask to apply;
- Port: The port which we want to grant access. This option may be disabled or ignored, depending on your choice of protocol. A range of ports may be specified by checking the Range box. The ports listed in the From and To fields will be granted access.
- Protocol: Select from the list. Available choices are: TCP, UDP, ICMP and ALL. If ALL or ICMP are selected then "Port" will be ignored.

Delete

Deletes an entry from this table. After selecting the entry, press "Delete". Removing an entry from this table is the same as denying access to the host/service from hosts in the external network.

By default all hosts in the network will be able to use the tunnel. This option allows you to configure local hosts' access to the tunnel. Available actions are "Add" and "Delete".

Add

After selecting "Add", a popup window will appear requesting the following information:

- Origin: The IP address for the host in the network to which we want to deny access to the tunnel;
- Netmask: The netmask to apply;
- Port: The port which we want to deny access to. This option may be disabled or ignored, depending on your choice of protocol. A range of ports may be specified by checking the Range box. The ports listed in the From and To fields will be denied access.
- Protocol: Select from the list. Available choices are: TCP, UDP, ICMP and ALL. If ALL or ICMP are selected then "Port" will be ignored.

Delete

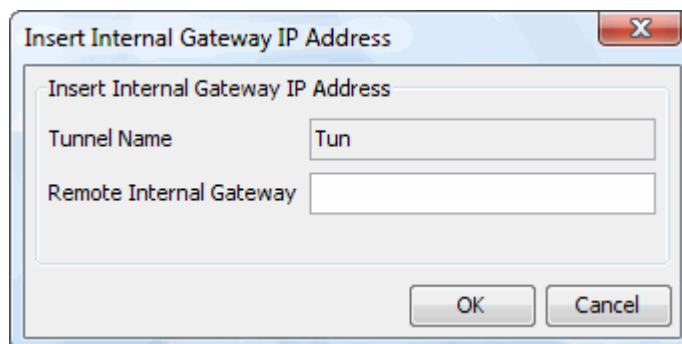
Deletes an entry from this table. After selecting the entry, press "Delete". Eliminating an entry from this table is the same as granting access to the tunnel for a host in the network.

4.2.1.3.2 Edit

This option allows you to change an IPSec tunnel configuration. Select a tunnel from the list and a popup window similar to the one in "Add" will appear. You can change the same options.

4.2.1.3.3 Status

Highlighting an active tunnel and pressing status results in the following pop up panel:



Tunnel Name

A read only field, showing the tunnel you selected for status information

Remote Internal Gateway

Enter the LAN IP address of the remote edgeBOX (eg 192.168.100.254)

After pressing the OK button, a form with 4 tabs will be presented, indicating information about the IPSec tunnel. The tabs are:

[General](#)

[Services Status](#)

[Logfile](#)

[Connection Status](#)

4.2.1.3.3.1 General

This is a read only panel showing the remote network information and the tunnel Negotiation summary.

The screenshot shows a window titled "Tun Status" with four tabs: "General", "Services Status", "Logfile", and "Connection Status". The "General" tab is selected and displays the following information:

Tunnel Information	
Tunnel Name	Tun
Remote Network	192.168.91.0/24
Remote Gateway:	192.168.90.116
Remote Internal Gateway	

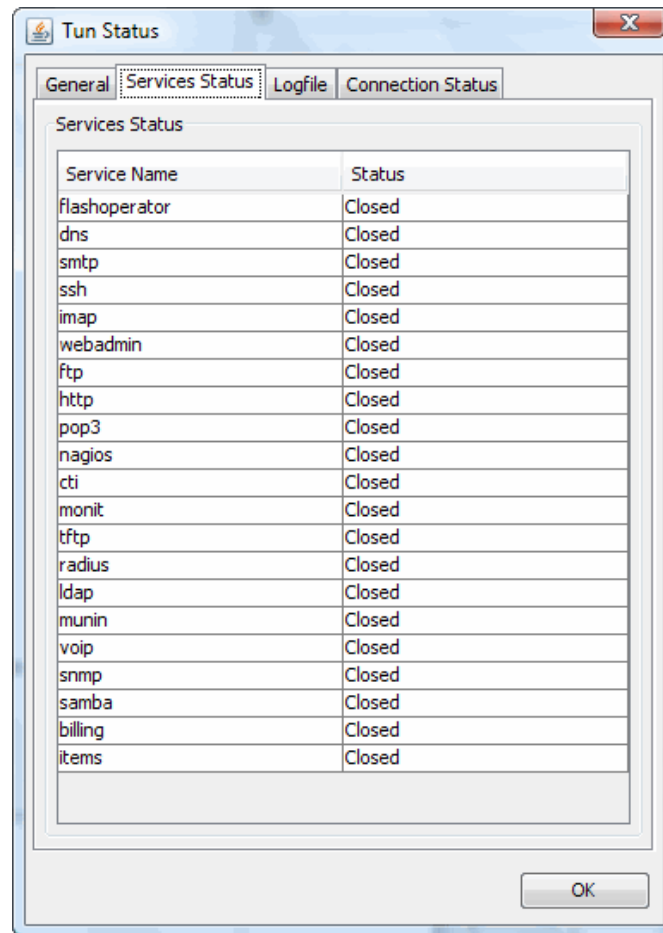
Negociation	
Phase one	Insucess
Phase Two	Insucess
key	Insucess

Possible Problem: No Tunnel to 192.168.90.116

OK

4.2.1.3.3.2 Services Status

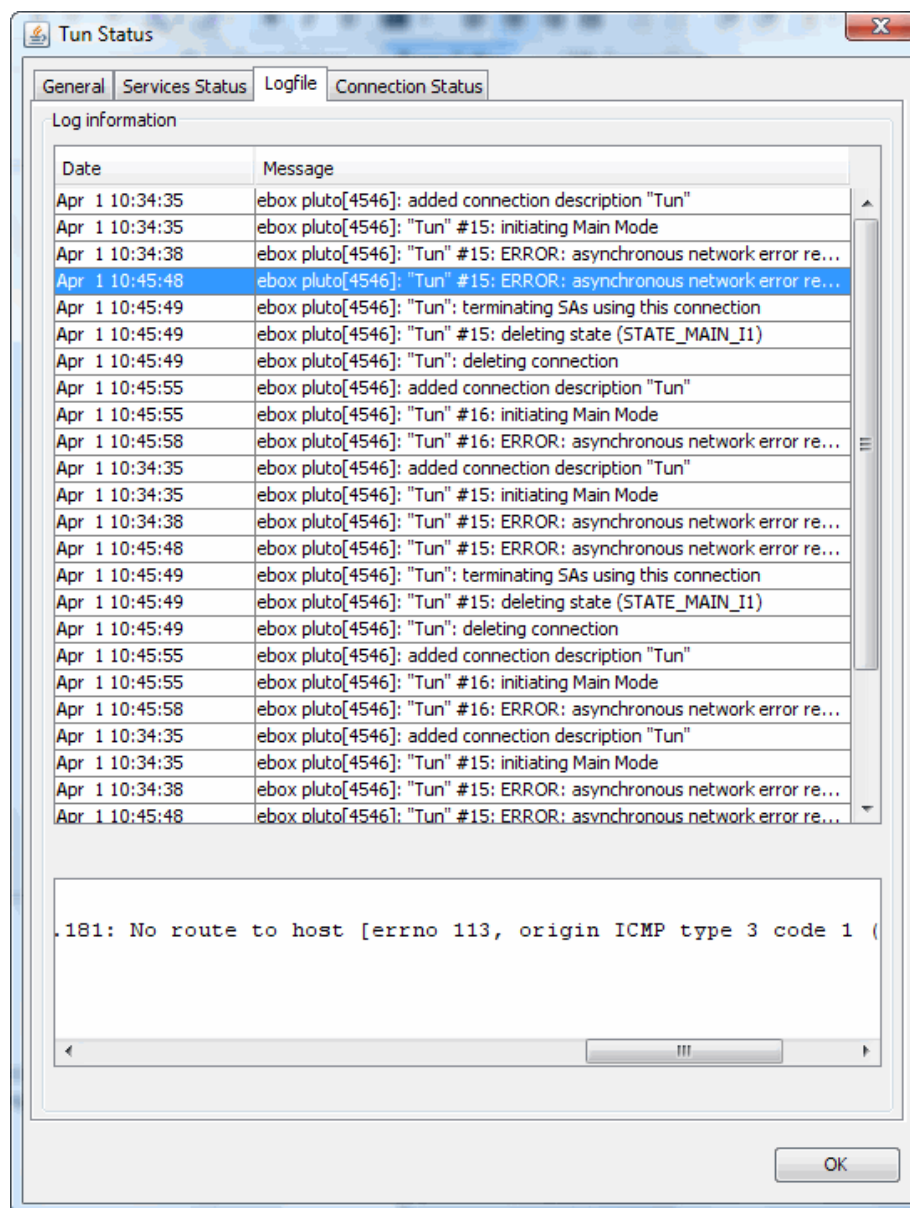
This panel displays information about the services available to local clients on the remote edgeBOX. For example, users on the local LAN will be able to access ftp on the Remote edgeBOX, as this service is "Opened", however they will not be able to access the http service as this is "Closed".



i The Radius status will always appear as Closed. edgeBOX cannot know the status remotely unless edgeBOX is included as Radius client on the remote server.

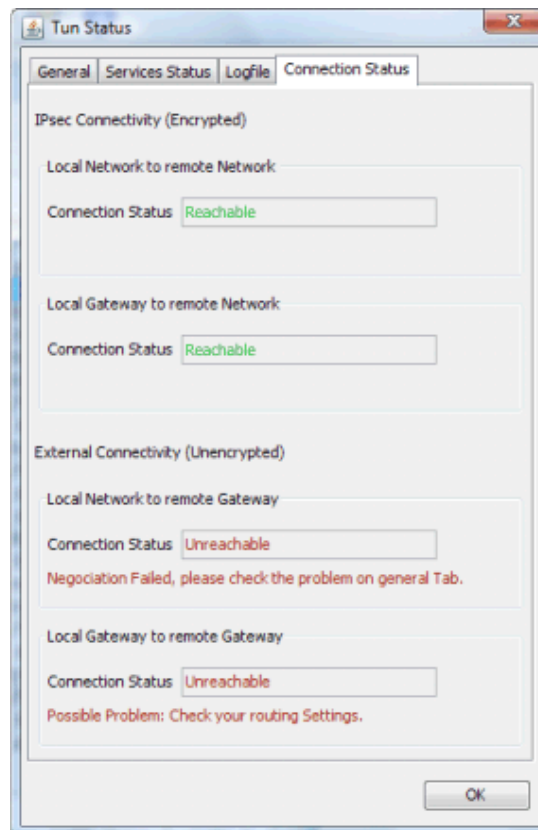
4.2.1.3.3.3 Logfile

This panel shows the logfile (at the time the request to view the status was made - ie it does not update) for the tunnel selected. Highlighting a row will present the message in the lower panel.



4.2.1.3.3.4 Connection Status

A read only panel summarising the the connection status.



4.2.1.3.4 Delete

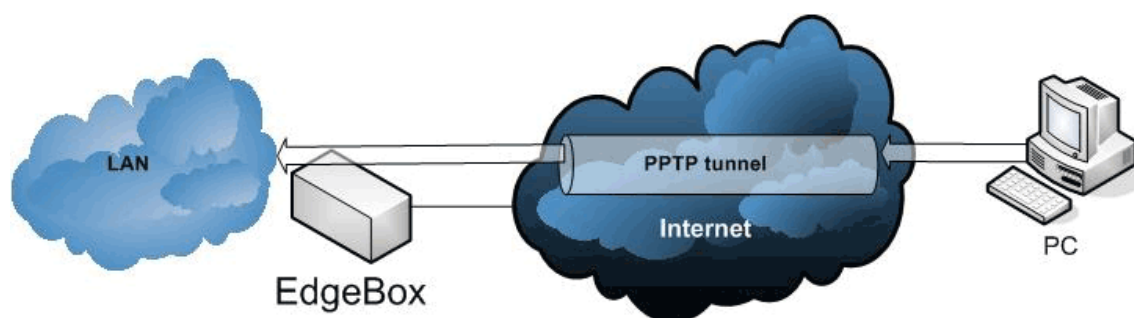
Removes a tunnel configuration. Select the IPsec tunnel you want to delete and then select the "Delete" button.

Note: The tunnel must be stopped before it can be deleted.

4.2.2 PPTP

In this page, you can review and change your PPTP VPN configuration. PPTP is used to establish VPN tunnels across the Internet. This allows remote users to access the internal network from anywhere on the Internet.

Note: To use PPTP you must have the [firewall](#) enabled.



PPTP tunnel connecting a host to a private network

Note: When using PPTP with the (local PC) default remote gateway option checked, you will not be able to access the Internet via the PPTP connection. This is because it makes more sense to access the internet via your local network, which reduces edgeBOX traffic and encryption overheads.

The available elements in this page are described next.


The screenshot shows the PPTP configuration window. At the top, there are tabs for IPsec, PPTP, and L2TP. The PPTP tab is selected. The Service State is displayed as **STOPPED**. Below this, the Authentication Type is set to **Local Authentication** (selected with a radio button). The Remote Radius Configuration section has fields for Server IP, Password, and Server Port (set to 1812). The IP Address Ranges section shows the Local range as 192.168.100.254, and the Remote range from 192.168.100.240 to 192.168.100.250. The Active Connections section is a table with columns for User, IP Address, and Time, currently empty. At the bottom right, there are buttons for Start Service and Apply.

4.2.2.1 Service State

This information is read-only and gives you the current status of the service. Possible values are running and stopped.

4.2.2.2 Authentication Type and Access Privileges

Selecting "Local Authentication" means that the authentication will be performed by edgeBOX's Radius server. No additional configuration is needed, such as Radius user creation. Authorization for PPTP VPN use is configured in the User Management panel.



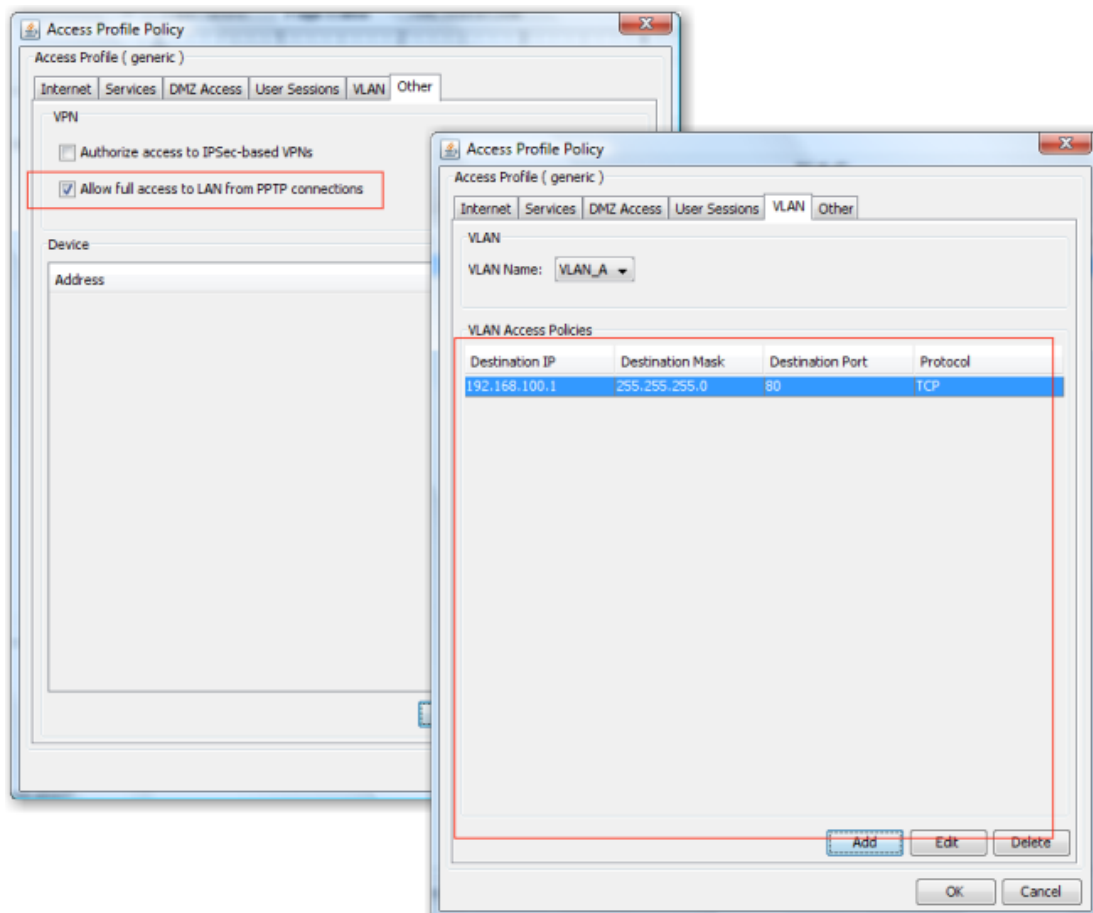
Authentication Type

☒ Local Authentication ☐ Remote Authentication

Access Privileges using Local Authentication

When a user accesses the network using a PPTP connection, the **privileges** the user has are related to the **access profile the user belongs to**. edgeBOX verifies the access rules defined on the profile of the user to determine access to the LAN and VLANs.

If the profile of the user has the **Allow full access to LAN from PPTP connections** option switched on then the user will have access to the LAN as if he was a regular LAN user, with access to the network services based on the profile policies he belongs to. Else, the user will have no access privileges at all besides the specific access rules defined in the **Access Profile's Destination Access Policies** list.



Access Profile properties

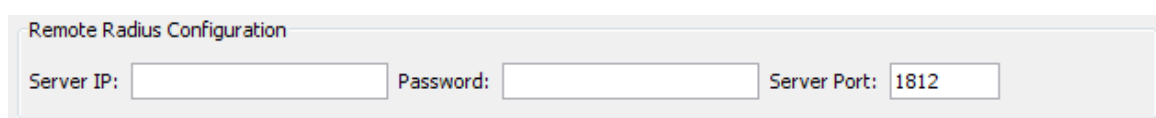
Access Privileges using Remote Radius Authentication

If you want **PPTP users** to authenticate in a **remote Radius server instead of the edgeBOX**, then all the process is made in the Remote Server, so **you don't need to create the users** in the edgeBOX.

PPTP users that authenticate in a remote Radius server **will always belong to the 'Default' access profile** as it is impossible for the edgeBOX to know who they are.

4.2.2.3 Remote Radius Configuration

Displays the remote Radius server used to authenticate users.



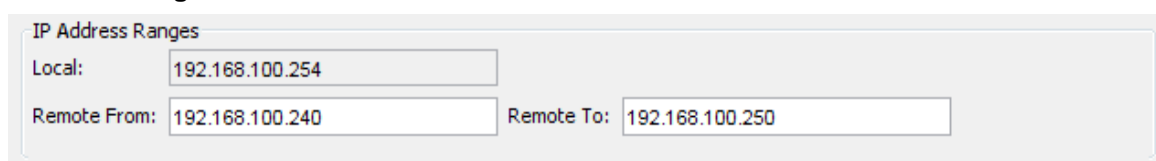
Remote Radius Configuration

Server IP: Password: Server Port:

- Server IP: IP address for the Radius server;
- Server Port: The port where the radius daemon is running;
- Password: shared secret between edgeBOX and the radius server;
- Time: amount of time after which the connection will timeout (in seconds) - Read Only

You have to select "Apply" in the main panel to make changes effective.

4.2.2.4 IP ranges



IP Address Ranges

Local:

Remote From: Remote To:

This element has the following information:

Local

This is edgeBOX's LAN interface IP address. The remote client PC will use this address as the gateway for the private network. This information is read-only.

Remote From and Remote to

These two fields allow you to set the IP address range which will be assigned to clients connecting through PPTP.

The address range should not overlap the DHCP range, nor should any static IP addresses in this range be defined.

4.2.2.5 Active Connections

A table where each connected user is listed as well as the IP address of the client machine from where the connection was established, and the time at which the connection was established.

4.2.3 VPN L2TP

Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by Internet service providers to enable the operation of a virtual private network (VPN) over the Internet.

This panel allows edgeBOX to be configured to act as a L2TP client.

- Server IP: IP address of server
- Username: Username on the server used for authentication
- Password: Password on the server used for authentication, which is the password for the above username
- PSK: Pre-Shared secret key (must match the one on the server)
- Keep Connection Alive: Polls the server to maintain the connection

Note: l2tp not encrypted, but simply allows the tunnel connectivity.

The screenshot shows the L2TP configuration interface. At the top, there are three tabs: 'IPsec', 'PPTP', and 'L2TP', with 'L2TP' being the active tab. Below the tabs, the 'Service State' is displayed as 'STOPPED' in red text. The 'Server Configuration' section contains the following fields: 'Server IP' with the value '222.222.222.222', 'Username' with the value 'test', 'Password' and 'PSK' both masked with dots. A checkbox labeled 'Keep connection alive' is checked. Below this, the 'Tunnel State' section shows 'Tunnel State: Inactive' in red text, with a 'Refresh' button. At the bottom right, there are two buttons: 'Start Service' and 'Apply'.

4.3 Anti-Virus

In this page you can review and change edgeBOX's Mail Scanner options.

Currently, support is available for three antivirus engines, Sophos, McAfee and ClamAV. edgeBOX is not shipped with the Sophos or the McAfee antivirus engines installed, so you will have to buy the appropriate number of licenses to use and upload them to edgeBOX.

The following panels are available for configuration, each accessible through a named tab:

- [Shares Scanner](#)
- [Mail Scanner](#)
- [Anti-Virus Engines](#).

We will describe each of these panels in the following sections.

4.3.1 Shares Scanner

This panel allows you to configure edgeBOX's shares scanner.

The screenshot shows the edgeBOX configuration web interface. At the top, there are four tabs: 'Firewall', 'VPN', 'Anti-Virus', and 'Content Filtering'. The 'Anti-Virus' tab is selected. Inside the 'Anti-Virus' section, there are three sub-tabs: 'Shares Scanner', 'MailScanner', and 'Anti-Virus Engines'. The 'Shares Scanner' sub-tab is active. The configuration area is divided into two main sections: 'Virus' and 'Options'. In the 'Virus' section, there is a checkbox for 'Virus Scanning' which is checked, and a 'Select Engine:' dropdown menu currently set to 'Clamav'. In the 'Options' section, there is a checkbox for 'Remove Infected Files' which is unchecked, and a checkbox for 'Automatic scanning' which is checked. Below these, there is a 'Scheduled Scanning' section with a 'Time to Perform Scans:' field set to '15' hours and '3' minutes. There is also a checkbox for 'Send Summary by Email' which is checked, and an 'Email:' text field containing 'admin@localhost'. An 'Apply' button is located at the bottom right of the configuration area.

Virus Scanner

The Virus Scanning package to use. Possible choices are Sophos, McAfee or ClamAV. (Sophos and McAfee engines are not shipped with edgeBOX, so these choices are not available from the dropdown, unless they are installed)

Virus Scanning

Check this option if you want to enable virus scanning.

Remove Infected Files

If you check this option, then files found to be infected will be deleted.

Automatic scanning

Automatic scanning is an option only available for the Clamav Antivirus. If you check this option, Clamav Antivirus will scan all files that are uploaded to the Shares immediately when they are uploaded.

Note: Automatic scanning is only possible for files with sizes up to **5MB** and that are placed in the shares normally, for example using the Windows Explorer. This is, if the network users upload the files using FTP for example, edgeBOX **will not be able to scan the files** at the moment of the upload.

Time to Perform Scans

Use this option to configure the time of the day when a scan of the file shares will be performed. This option will always be performed. If you have the Automatic Scanning option selected the files will be scanned when they are uploaded but the Share will still be scanned every day.

Send summary by e-Mail

Check this option if you want a shares' scan report to be sent by email.

Notification E-mail

The email address where the shares' scan report will be sent.

4.3.2 Mail Scanner

Allows you to configure the Mailscanner settings. The following panels are available for configuration, accessible through the named tabs located on the right:

- [General](#)
- [Messages](#)
- [Actions](#)
- [Quarantine](#)

4.3.2.1 General

Allows you to configure general MailScanner configurations. Available options are:

- [Antivirus engine selection](#)
- [Spam options](#)
- [Notification options](#)

The screenshot shows the MailScanner configuration window with the 'General' tab selected. The window has three tabs: 'Shares Scanner', 'MailScanner', and 'Anti-Virus Engines'. The 'General' tab is active, showing a sidebar with 'General', 'Messages', and 'Actions'. The main area is divided into sections: 'Virus' with a checked 'Virus Scanning' box and a 'Select Engine' dropdown set to 'Clamav'; 'Spam' with a checked 'Spam Checks' box, an unchecked 'Log Spam' box, and a 'Spam Actions' dropdown set to 'Deliver'; 'RBL Servers' with a list of servers (list.dsbl.org, bl.spamcop.net, dul.dnsbl.sorbs.net, dnsbl.njabl.org, cbl.abuseat.org) and 'Add'/'Delete' buttons; and 'More options' with checked boxes for 'Notify Senders' and 'Send Notices To Email' (set to 'sopa@hotmail.com'). An 'Apply' button is at the bottom right.

4.3.2.1.1 Virus

Virus Scanning

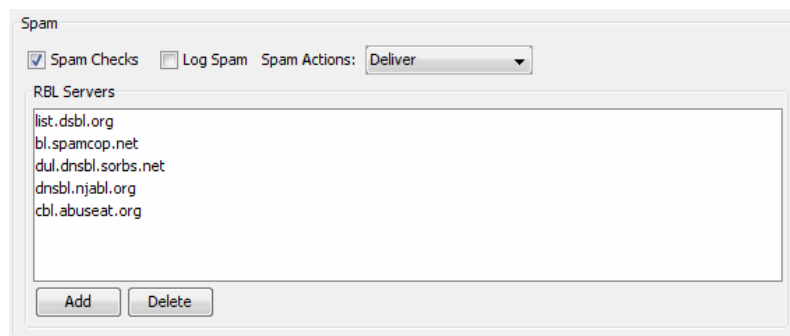
Check this option if you want to enable virus scanning.

Select Engine

The Virus Scanning package to use. Possible choices are Sophos (when installed), McAfee (when installed) and ClamAV.

This is a close-up of the 'Virus' section of the configuration window. It shows a checked checkbox for 'Virus Scanning' and a 'Select Engine' dropdown menu currently set to 'Clamav'.

4.3.2.1.2 Spam

**Spam Checks**

Check this option if you want the MailScanner to check if incoming messages are spam.

Log Spam

Check this option if you want the MailScanner to log spam messages to syslog.

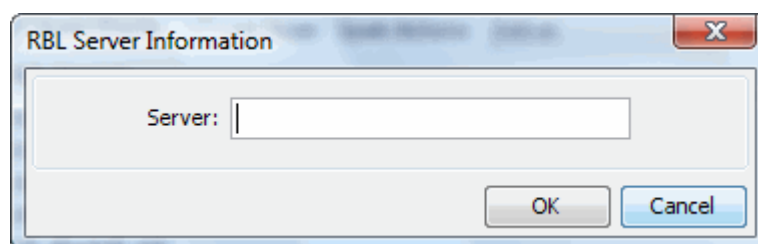
Spam Actions

The action to be applied to spam messages. Choose from the list of allowed values, which may be:

- Deliver: The message is delivered to the recipient as normal;
- Delete: The message is silently discarded;
- Attachment: The original message is converted to the attachment of the message.

RBL Servers

This feature allows you to have a anti-spam protection based on existing spammers' databases (The Realtime Blackhole List). After checking this option you will have to provide hosts serving these lists. To manage the list you have two options: "Add" and "Delete".

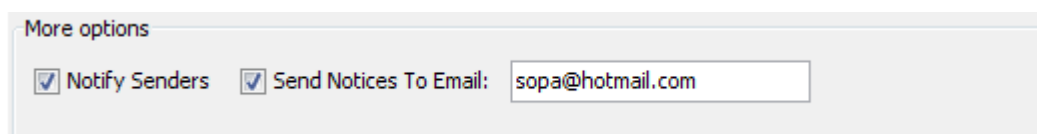
**Add**

Inserts a new host in the list of hosts that will be queried to check if the incoming mail domain was blacklisted. After selecting 'Add', a popup window will appear. Insert the hostname and select "OK". You then have to select "Apply" for changes to become effective. You can have as many hosts as you like. At the time of this publication examples of hosts providing such lists are: list.dsbl.org and bl.spamcop.net.

Delete

Deletes an entry for a host from the list. You have to select "Apply" to make this change effective.

4.3.2.1.3 More Options



More options

☒ Notify Senders ☒ Send Notices To Email:

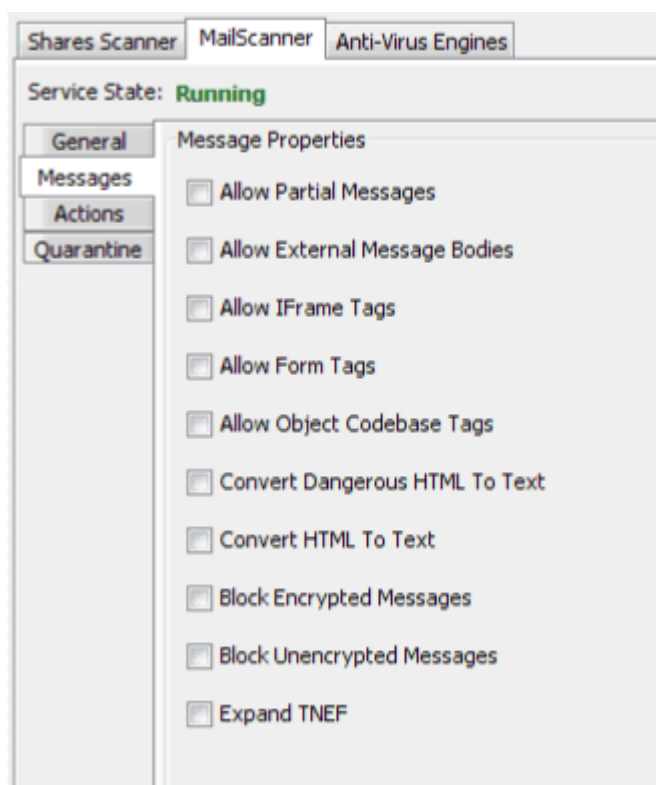
Notify Sender

If you check this option, notifications will be sent to infected messages' senders.

Send Notices To Email

If you check this option, then every time a spam message is received a specific user will be notified.

4.3.2.2 Messages



Shares Scanner MailScanner Anti-Virus Engines

Service State: **Running**

General
Messages
Actions
Quarantine


Message Properties

- ☐ Allow Partial Messages
- ☐ Allow External Message Bodies
- ☐ Allow IFrame Tags
- ☐ Allow Form Tags
- ☐ Allow Object Codebase Tags
- ☐ Convert Dangerous HTML To Text
- ☐ Convert HTML To Text
- ☐ Block Encrypted Messages
- ☐ Block Unencrypted Messages
- ☐ Expand TNEF

- **Allow partial messages** - allow messages that contain only a fraction of the attachments. As the scan is not performed on the whole message but on its fragments, it will not be done properly.

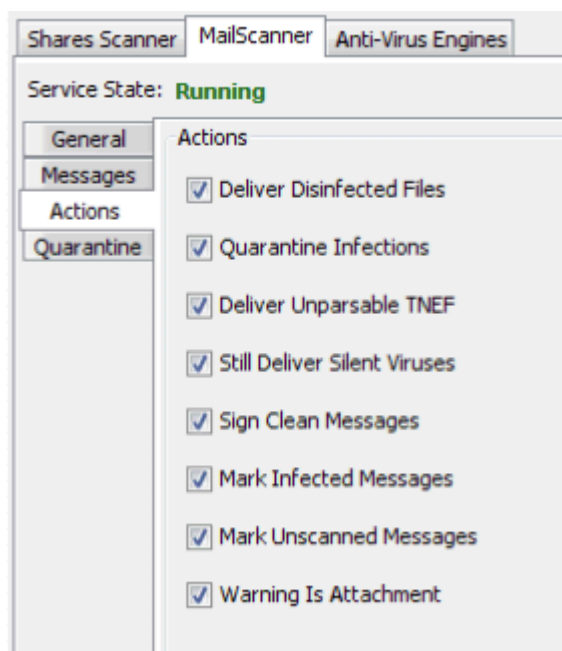
 Setting this option is very dangerous as viruses may go undetected.

- **Allow external message bodies** - allow messages where the body is stored in a remote server and not in the actual message. It will be up to the email client to fetch the message body later.

 Setting this option is particularly dangerous. MailScanner never scans the message body so it may allow viruses into your network.

- **Allow iframe tags** - allow messages to carry Iframe tags.
- **Allow form tags** - allow messages to carry Form tags.
- **Allow object codebase tags** - allow messages to carry Object codebase tags.
- **Convert dangerous HTML to text** - enable the conversion of Iframe and Object codebase tags into plain text. This is a good alternative to disallowing or leaving them untouched.
- **Convert HTML to text** - enable the conversion of all HTML tags into plain text.
- **Block encrypted messages** - enable blocking of encrypted messages.
- **Block unencrypted messages** - enable blocking of unencrypted messages.
- **Expand TNEF** - enable expanding of TNEF attachments that are joined in one WINMAIL.DAT file. If you don't check this option then the filenames within the TNEF attachments will not be checked.

4.3.2.3 Actions

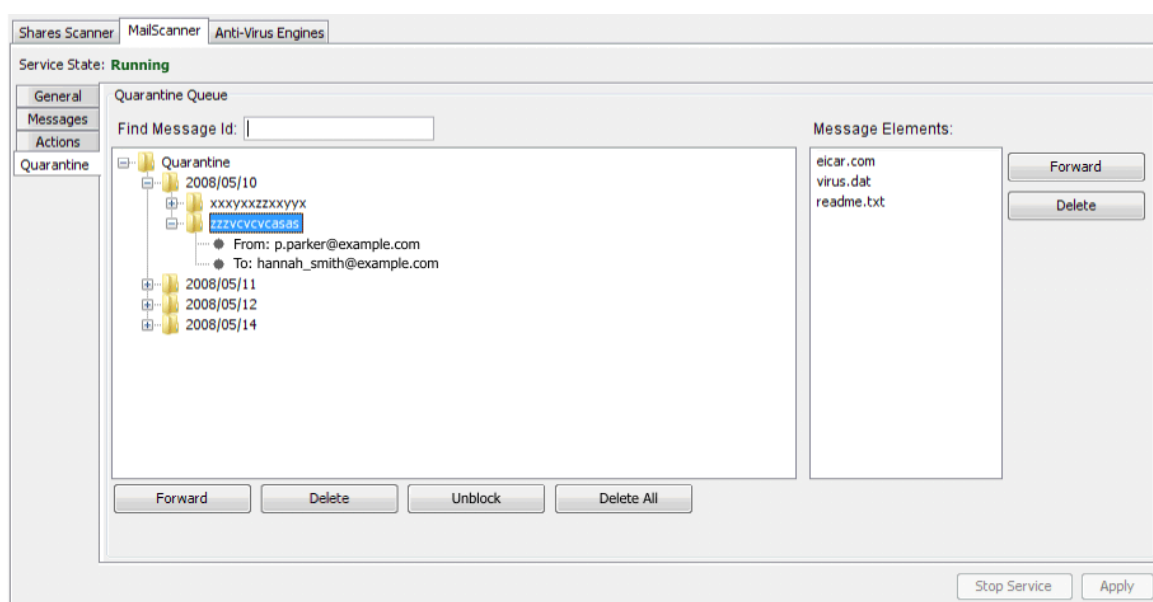


- **Deliver disinfected messages** - infected attached documents are automatically disinfected and sent to the original recipients.
- **Quarantine infections** - infected or dangerous attachments are stored in directories created under the quarantine directory.

- **Deliver unparseable TNEF** - allow the delivery of Rich Text Format attachments produced by some versions of Microsoft Outlook that cannot be completely decoded at present.
- **Still deliver silent viruses** - messages that originally contained a silent virus are still delivered, even if the addresses were chosen at random by the infected PC and did not correspond to anything a user intended to send.
- **Sign clean messages** - make MailScanner sign every clean message processed.
- **Mark infected messages** - If you check this option MailScanner will mark every infected message and every message that, for some reason had its attachments removed.
- **Mark unscanned messages** - mark every message that is not scanned by MailScanner.
- **Warning is attachment** - include warnings for dangerous or infected attachments will as an attachment. If this option is not selected then the warnings will simply be included as inline text.

4.3.2.4 Quarantine

View the incoming or outgoing emails that are put under quarantine (blocked) by edgeBOX because they may contain files with virus.




The emails are grouped by date inside folders in the list on the left. You can expand and browse through the folders to find the emails. If you expand an email you will be able to see the sender and the receiver of the mail. If you select an email, its attachments appear on the list on the right.

▼ Unblock a quarantined email

To remove a blocked email from quarantine and deliver it to its intended receiver:

1. Select the email to unblock from the emails list.
2. Click the Unblock and then the Apply button. The email will be sent to its original receiver.

 Make sure you remove all infected files of an email before you unblock it. Delete all attachments with viruses.

▼ **Delete an email**

1. Select the email to delete from the emails list.
2. Click the Delete and then the Apply button.

▼ **Forward an email to another person**

If you want to send a blocked email to a different person than its original receiver:

1. Select the email from the emails list.
2. Click Forward. A dialog window will appear.
3. Type in the email address of the person you want to forward the email to.
4. Click OK and then Apply to forward the email.

You can also make operations to the attachments of the emails. This is particularly useful to remove virus from the emails without deleting the email. This way you can remove the files that are infected and then still deliver the email to the receiver.

4.3.3 Anti-Virus Engines

This panel allows you to perform the installation of anti-viruses' engines (where applicable), and update their IDE files. Select the desired antivirus engine using the named tab on the right. Currently the supported anti-viruses engines are:

- [Sophos](#)
- [McAfee](#)
- [Clamav](#)

4.3.3.1 Sophos

This panel allows you to upload the Sophos antivirus engine required to perform antivirus scans. Remember that you will have to buy an appropriate number of licenses in order to use this engine. You may also check the virus definitions database version and update it.

Sophos Options

4.3.3.1.1 Information

This panel contains the elements described next.

Version

The antivirus engine version installed. This element is read-only.

Date of most recent IDE files

The date of the last virus definitions file installed.

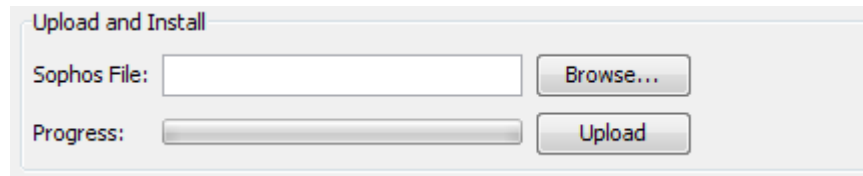
Update IDE Files

Selecting this button will download the latest virus definition files. You must have a current license for Sophos in order to do this. The edgeBOX also performs this update automatically on a daily basis.

4.3.3.1.2 Upload and Install

This panel allows you to install a Sophos antivirus engine:

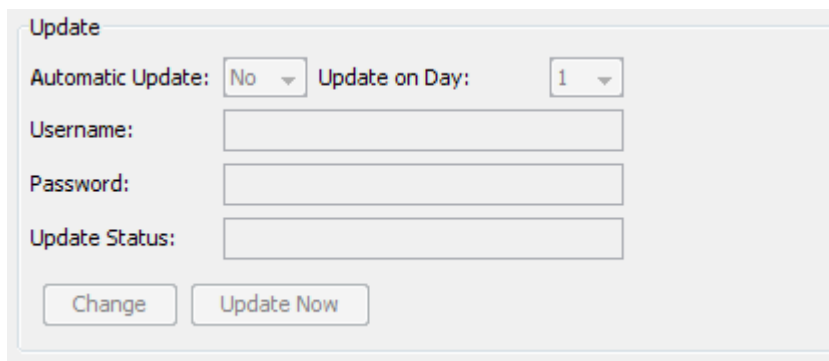
- Download the antivirus engine from the Sophos website. Bear in mind that you need to buy the appropriate number of licenses to use this software;
- Hit the "Browse" button and navigate to the location where you saved the antivirus engine file. Select it.
- Hit the "Upload" button and wait until the progress bar reaches 100%. Check the status returned to confirm the command was successful. This transfer is done via FTP so make sure that FTP traffic is allowed on the LAN side on your firewall configuration.



The screenshot shows a web-based interface titled "Upload and Install". It contains a text input field labeled "Sophos File:" followed by a "Browse..." button. Below this is a progress bar labeled "Progress:" and an "Upload" button.

4.3.3.1.3 Update

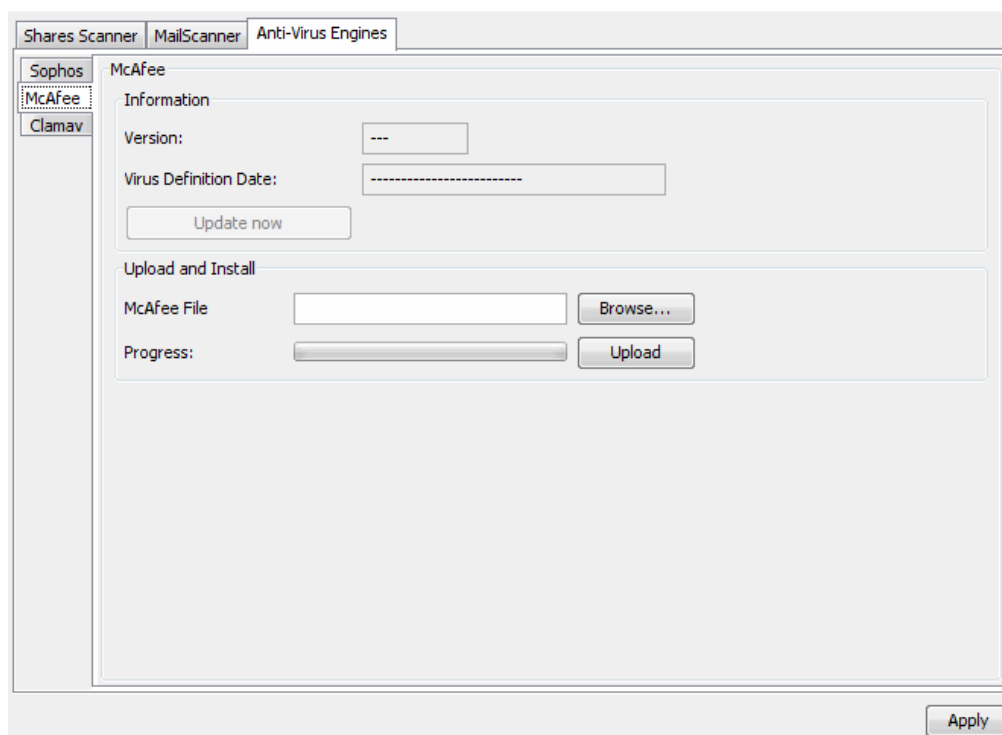
This panel allows the edgeBOX to keep the Sophos antivirus engine automatically updated on a monthly basis. Please enter the username and password you received with your Sophos License registration and select the day of the month for this update to be executed.



The screenshot shows a web-based interface titled "Update". It features a dropdown menu for "Automatic Update:" set to "No", and another dropdown for "Update on Day:" set to "1". Below these are text input fields for "Username:", "Password:", and "Update Status:". At the bottom, there are two buttons: "Change" and "Update Now".

4.3.3.2 McAfee

This panel allows you to upload the McAfee antivirus engine required to perform antivirus scans. Remember that you will have to buy an appropriate number of licenses in order to use this engine. You may also check the virus definitions database version and update it.



4.3.3.2.1 Information

This panel contains the following elements:

Version

The antivirus engine version installed. This element is read-only.

Date of most recent IDE files

The date the last virus definitions file was installed.

Update IDE Files

Selecting this button will download the latest virus definition files. You must have a current McAfee license in order to do this. The edgeBOX also performs this update automatically on a daily basis.

4.3.3.2.2 Upload and Install

This panel allows you to install a McAfee antivirus engine:

- Download the antivirus engine from the McAfee website. Bear in mind that you need to buy the appropriate number of licenses to use this software.
- Hit the "Browse" button and navigate to the location where you saved the antivirus engine file. Select it.
- Hit the "Upload" button and wait until the progress bar reaches 100%. Check the status returned to confirm the command was successful. The transfer is done via FTP so make

sure that FTP traffic is allowed on the LAN side on your firewall configuration.

4.3.3.3 Clamav

This panel allows you to check and update Clamav's IDE files. Clamav is a free antivirus engine and is shipped with edgeBOX.

Version

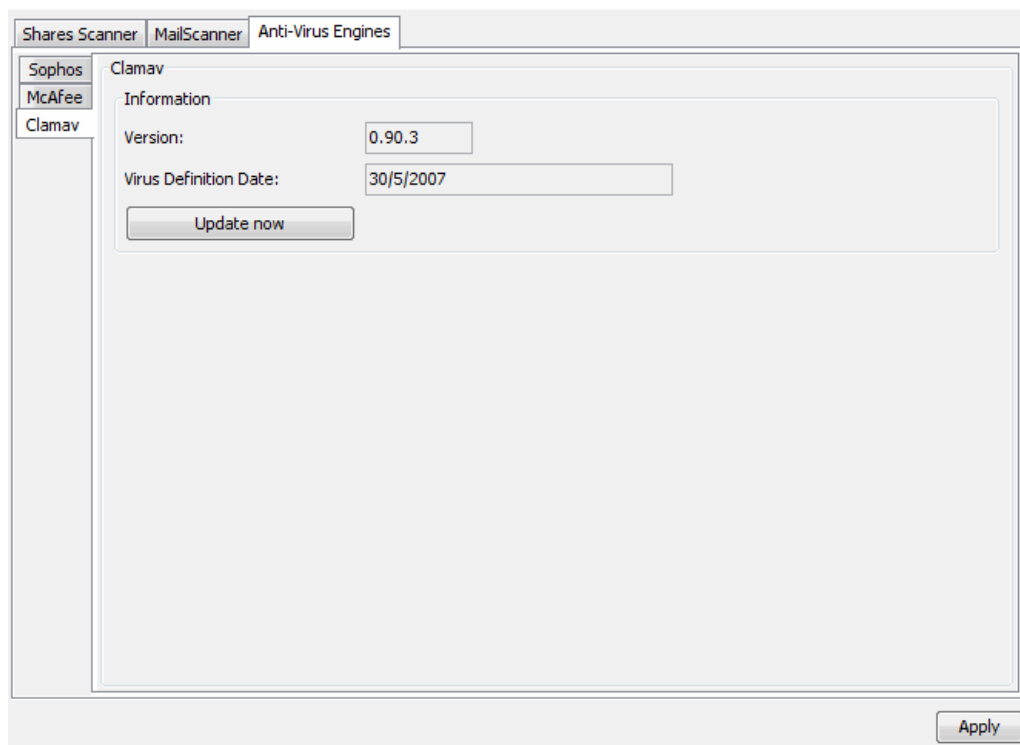
The antivirus engine version installed. This element is read-only.

Date of most recent IDE files

The date of the last virus definitions file installed.

Update IDE Files

Selecting this button will download the latest virus definition files. **edgeBOX also performs this update automatically on a daily basis.**



4.4 Content Filtering

The edgeBOX provides a web page filtering service that can be used to block access to web sites. Filtering can be performed on either domain names or by checking URLs for certain keywords.

The web filtering service only blocks words in URL and domains in HTTP (port 80) traffic; traffic

from HTTPS websites or FTP to a web filtered website can not be check by the Content Filtering.

Note: HTTP traffic that is configured to use Premium bandwidth cannot be blocked by Content Filtering. This is because Premium bandwidth HTTP traffic bypasses edgeBOX's Proxy Squid. Also, HTTP traffic that has QoS rules defined in the [QoS Services panel](#) cannot be blocked either.

4.4.1 Domains

Displays a list of the files that contain domains that are to be blocked.

Block http requests based on domain names access lists

Check this box to enable web filtering based on the uploaded file(s).

Enabled

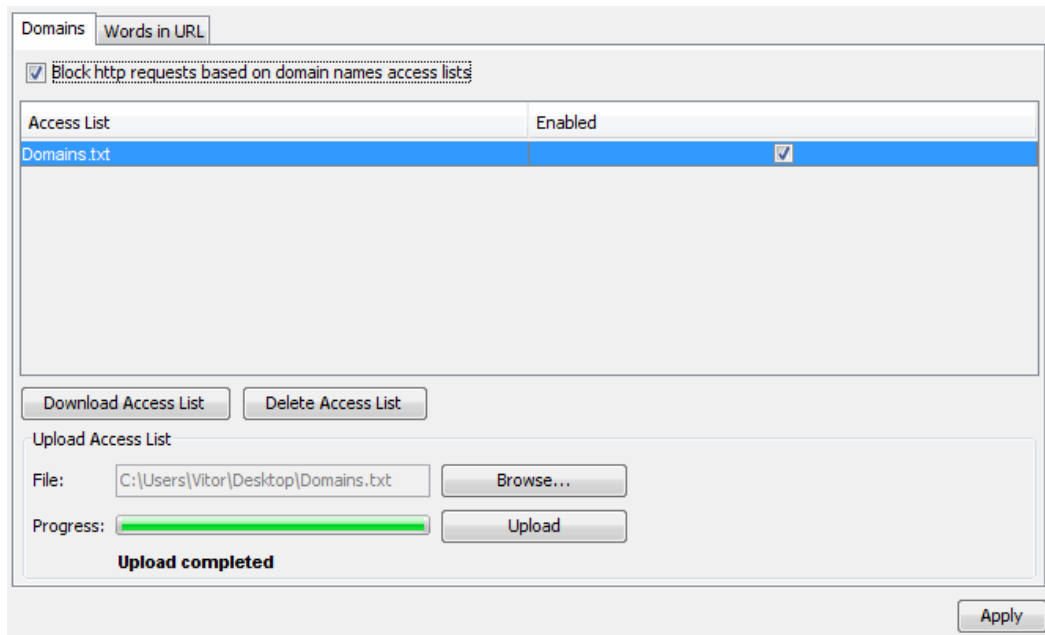
When checked, the contents of the file(s) is used to block URL's.

Delete Access List

Deletes the file from the edgeBOX and thus the domains in that file are no longer blocked.

Download Access List

This allows you to highlight a file in the Enabled Panel and download the file to your PC



Browse

Allows you to select a file to upload to the edgeBOX.

Upload

Once a file has been selected (via the Browse button), you can copy it to the edgeBOX via this button. Once uploaded, the new file will appear in the main Panel.

Make sure you have the service FTP allowed on the [firewall](#) because the upload of the file to the edgeBOX is made via FTP.

File Format

The format of the uploaded file is one entry per line.

Each line in the file may be a domain to deny, or can contain regex expressions

To find out more information about Regex expressions, visit: <http://www.regular-expressions.info>

Some one-line examples for the domain file are:

```
.net           Block anything.net (eg www.school.net or https://www.mylocal.net)
[-./]dog[-./] Blocks domains containing the word dog (eg www.ttdoggy.com)
[-./](dog|cat)[-./] Blocks domains containing the word dog or cat (eg www.catty.pt)
]             Note: There is no space before or after the | character
*\. (exe|bat) Blocks, for example, www.bad.pt/download/file.exe or
              www.verbad.com/getit.bat
```

When adding a domain to the file, the following rules apply:

A single domain will match all urls under that domain and is case-insensitive

As an example, if you specify test.com', it will match 'test.com' and 'test.com/help'.

A domain preceded by a dot will match that domain and all subdomains.

For example '.example.com' will match 'example.com' as well as 'new.example.com' or 'old.example.com'.

4.4.2 Words in URL

Displays a list of the files that contain words that are used to block website access.

Block http requests based on word access lists

Check this box to enable web filtering based on the uploaded file(s).

Enabled

When checked, the contents of the file(s) is used to block URL's.

Delete File

Deletes the file from the edgeBOX and thus the words in that file are no longer used to block website access.

Download

This allows you to highlight a file in the Panel and download the file to your PC

Access List	Enabled
Words.txt	<input type="checkbox"/>

Download Access List Delete Access List

Upload Access List

File: C:\Users\Vitor\Desktop\Words.txt Browse...

Progress: Upload

Upload completed

Apply

Browse

Allows you to select a file to upload to the edgeBOX.

Upload

Once a file has been selected (via the Browse button), you can copy it to the edgeBOX via this

button. Once uploaded, the new file will appear in the main Panel.

File Format

The format of the uploaded file is one entry per line.

When adding a word to the file, the following rules apply:

A single word will match all urls which contain that word, either completely or as a substring.

As an example, if you specify 'goo', it will match 'google.com and www.myinfo.pt/ToGoOver/help, as both URL's contain the word goo.

It matches the second URL as it contains ToGoOver, which contains the word GoO (recall that the word lists are not case sensitive).

5 Storage and Printers



This section details the menu's which allow Windows users access to edgeBOX attached Printers and Filesystems.

File system access is allowed via three methods:

- [Shares](#)
- [Homes](#)
- [Public Safes](#)

[Quotas](#) allows administrators to limit user file system resources

[Backup](#) and [Restore](#) allows administrators a simple GUI to protect the system configuration from accidental damage.

When the edgeBOX is acting as a PDC (Primary Domain Controller) and if the user's computer is on the same domain as the edgeBOX:

- The user will automatically be authenticated on edgeBOX
- The user will have a roaming profile (if this option is enabled)
- The user will receive a home directory share (Z: drive) from edgeBOX

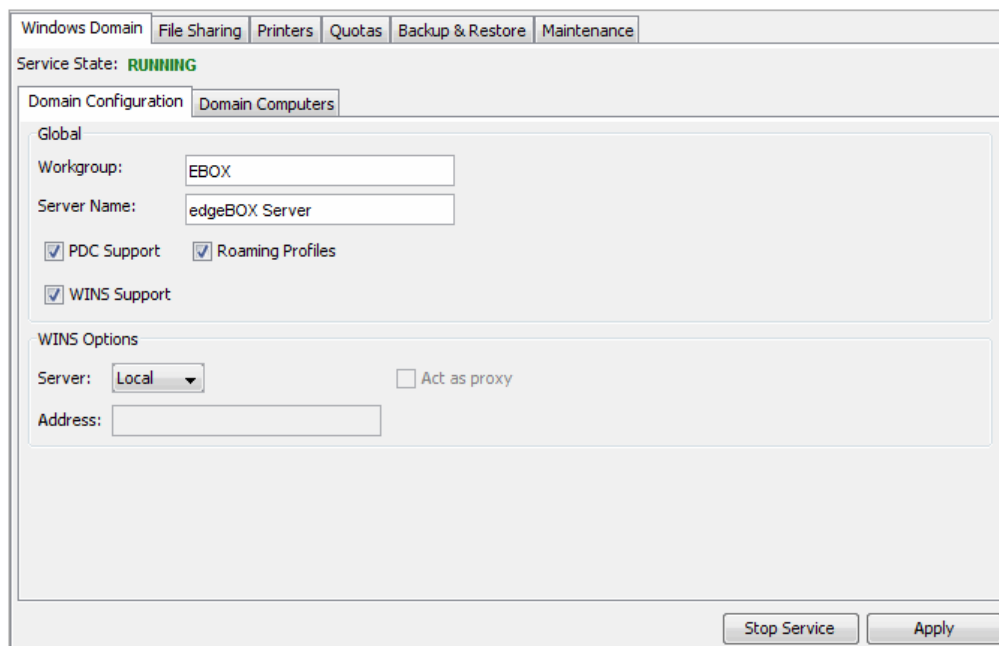
5.1 Windows Domain

This service allows edgeBOX to interact with other hosts as if it was a Windows server. Besides the usual file and printer sharing services, edgeBOX's may also act as a PDC and WINS server.

WINS performs name registration and resolution. Windows clients can query a WINS server directly, instead of using the usual broadcast method, thus resulting in an improvement in performance (the hosts don't need to process broadcast packets).

When edgeBOX acts as a PDC, users' desktop preferences are stored in edgeBOX (roaming profiles), and their home directory is mounted locally as Z: drive.

The service is provided to all authorised users listed on the Users panel.



The details of attaching a PC to the edgeBOX domain are given in [Appendix C](#)

5.1.1 Service State

Reports the current state of the Samba service: Stopped or Running. If the service is Stopped it can be started by clicking on the "Start Service" button at the bottom right hand corner of the panel. Similarly if the service is Running it can be stopped by clicking on the "Stop Service" button.

5.1.2 Global

This section is used to make the Samba service accessible to Windows clients.

Workgroup

The name of the Windows workgroup that Windows clients must belong to access the services provided.

Server Name

A brief description of the edgeBOX server to make it easier to identify when browsing the network.

Wins Support

If you check this option, edgeBOX will act as a WINS server, providing WINS name service registration and resolution. An [additional options](#) panel will allow you to configure its role.

PDC Support

If you check this option, edgeBOX will act as a Windows Primary Domain Controller. After applying, the SID for this domain will be visible next to the Workgroup.

Roaming Profiles

If you check this option, edgeBOX allow the client to write a roaming profile, which is stored on the edgeBOX and downloaded each time the user logs onto the domain. By default is option is unchecked.

WINS Support

If you check this option, edgeBOX will act as a WINS server, providing WINS name service registration and resolution. An [additional options](#) panel will allow you to configure its role.

5.1.3 WINS Options

Server

Available options are Local or Remote. If set to Local, edgeBOX will act as a WINS server.

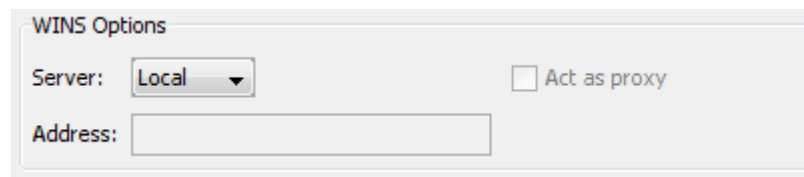
If set to Remote, edgeBOX will use a remote WINS server. In the later case, the following options will also be enabled:

Act as Proxy

If you check this option, edgeBOX will act as a WINS proxy, relaying registration and resolution requests from itself to another WINS server. edgeBOX will send the response back to the original client.

Address

Allows you to specify the IP address for the remote WINS server to be used.



The image shows a window titled "WINS Options". Inside, there is a "Server:" label followed by a dropdown menu currently showing "Local". To the right of this is an unchecked checkbox labeled "Act as proxy". Below the "Server:" label is an "Address:" label followed by an empty text input field.

5.2 File Sharing

The File Sharing allows to:

- Create and manage Shared Folders.
- Activate Home Directories for the users of the network.
- Define the properties of the temporary shared folders (Public Saves) that users can create.

5.2.1 Shares


Displays a list of the shared folders that are currently active. edgeBOX comes with an already created share named "Public" from factory. This share is accessible for all users to view and change files and folders inside it.

Shares	
Homes Public Safes	
Name	Description
Public	Public Share

You can create new shares, change access permissions of the shares or delete existing ones.

▼ Create a new shared folder

1. Click the New button below the list. A properties window will appear.
2. Type a suggestive name for the shared folder in the name field and a small description (less than 50 characters) of the purpose of the share in the description field.
3. Select from the Share Owner drop down list the user of the network that will be the owner of the share. This user must have Windows Use permissions.
4. Indicate the usernames of the users (separated by semi-colons) that are allowed to administer the shared folder in the Admins field. You don't need to include the username of the user that is the share owner; this user is automatically an administrator of the share.
5. Select the general permissions you want the share to have in the Options group:
 - **Public** - allows the share to be accessed and modified by all existent profiles and the guest user (the guest user requires no password). If using remote LDAP, the guest account will need to be created. If it is created with a password, then the guest account will also use this password.
 - **Readable** - allows the shared folder can be browsed and read by all existing profiles.
 - **Writeable** - allows the shared folder to be written by all users. If you do not select this option only the share owner and the administrators will be able to write to the share.
 - **Inherit Owner** - makes the user that is the share owner to be also the owner of all files created in the share and share sub folders.

 If you **do not select** this option when you create a new share or, if you **remove the selection** from this option when you edit a share, then **Windows users** of the network **will not be able to view the permissions selected by default** when they open the properties window of the share and go to the **Security tab**.

- **Inherit Permissions** - makes any files created in the share to have the same permissions as the share as.
 - **Hide Unreadable Files** - makes files inside the share that have no readable permissions invisible to the users.
6. If you want to [add specific permissions to given users or access profiles](#), go to the Permissions tab and indicate those permissions.
 7. Click OK to save the new shared folder.

▼ [Edit the properties of a shared folder](#)

1. Select the share you want to change the permissions.
2. Click the Edit button to open the properties window of the share.
3. Modify the desired [permissions](#) and settings of the share and click the OK button to save the changes.



Note that, when you are editing a share:

- If the **Public option** is not selected and **is changed to selected**, all existent profiles and the Guest user will be able to access and modify the share.
- If the **Writeable option** is not selected and **is changed to selected**, the permissions **will not change** - this only changes the writeable option in edgeBOX's smb.conf file.
- The Readable option is disabled.

▼ [Delete a shared folder](#)

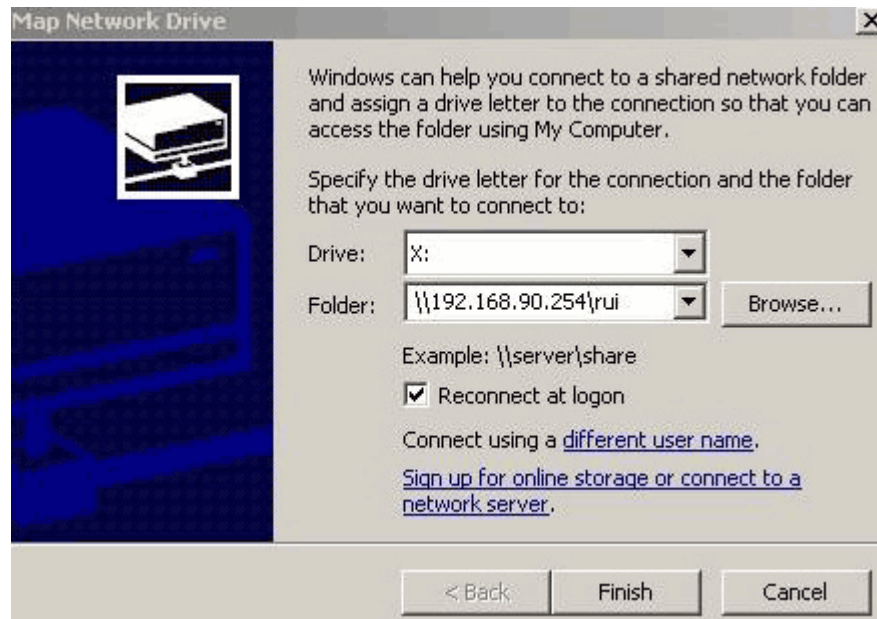
1. Select the share you want to delete from the list.
2. Click the Delete button.




Be careful when deleting shared folders; after clicking the Delete button the share is immediately deleted. No conformation is asked you, and you cannot undo the action.


▼ [Mount a shared folder on a computer of the local network](#)

1. Go to My Computer.
2. Select the Tools menu and the Map Network Drive option.
3. Select the character you to use for the drive.
4. Type the IP address of edgeBOX, followed by the name of the shared folder. For example:
\\192.168.90.254\rui.



 Windows does not allow you to mount shares with different username/passwords. It's possible to disconnect from a share using the command "net use * /delete". This will release all connections to shares.

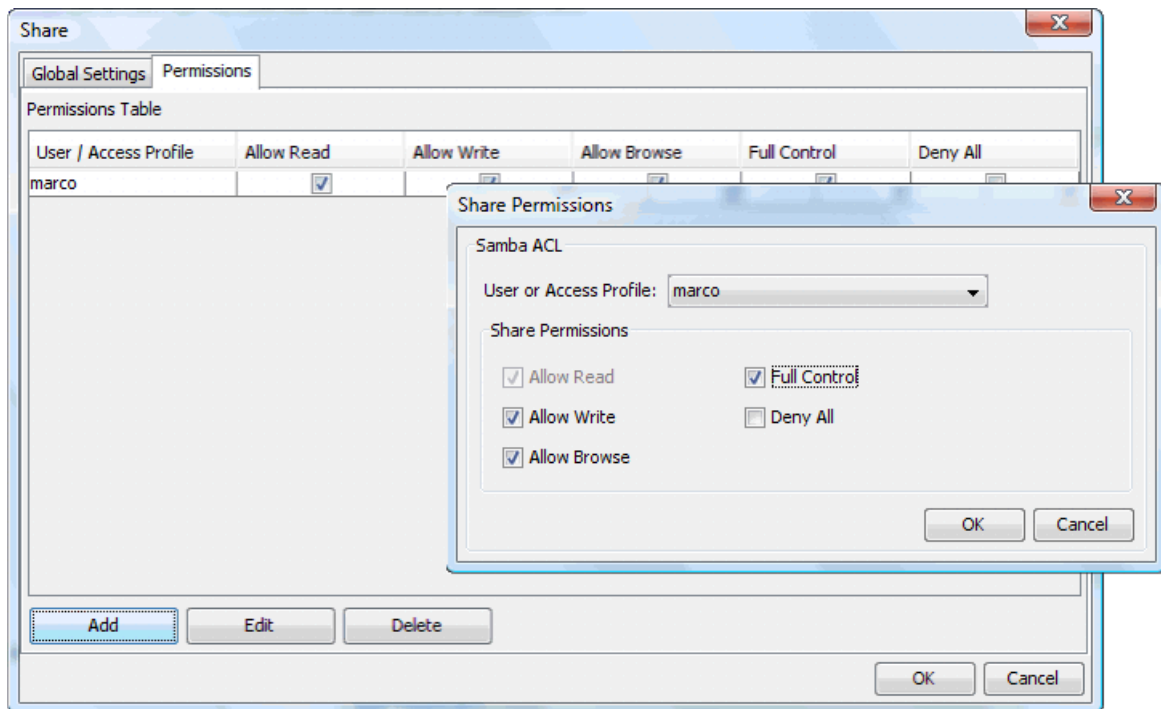
It's "net use" which will display which are the active shares and then "net use <share> /delete", which will disconnect that particular share.possible to specify which share to release, via the command

 If you **change the properties of a shared folder using Windows XP or Windows Vista**, in the Security tab of the shares properties window, **leave always selected at least one** deny or allow option when editing the permissions of a user or an access profile. Otherwise Windows will remove the user or access profile from edgeBOX share permissions' list.

5.2.1.1 Permissions

The Permissions tab allows you to **configure particular access permissions related to specific users or to Access Profiles**.


Note that these particular permissions do not override the general permissions of the Share, defined in the [Global Settings](#) tab. This is, if the share is only Readable and you give a specific user Full Control permissions, the user will still jus be able to read the share.



▼ Add permissions for a user or an access profile

To add a set of permissions to a specific user or access profile:

1. Click the Add button below the Permissions list. A dialog window will appear.
2. Select the user or the access profile you are settings specific permissions for, from the the drop down option.

 Access profiles are represented with an @ before the name, for example, the generic access profile is represented @generic.

3. Indicate the permissions you want to give to the user or profile:

- **Allow Read** - Allow the user/profile group to have read privileges for this share.
- **Allow Write** - Allow the user/profile group to have write privileges for this share.
- **Allow Browse** - Allow the user/profile group to have be able to browse the share.
- **Full Control** - Allow the user/profile group to have Full Control for this share.
- **Deny All** - Disallow the user/profile group access to this share.

4. Click the OK button to save the information into the Permissions list.

▼ Change the permissions set for a user or an access profile

To add a set of permissions to a specific user or access profile:

1. Click the Add button below the Permissions list. A dialog window will appear.
2. Select the user or the access profile you are settings specific permissions for, from

the the drop down option.



Access profiles are represented with an @ before the name, for example, the generic access profile is represented @generic.

3. Indicate the permissions you want to give to the user or profile:

- **Allow Read** - Allow the user/profile group to have read privileges for this share.
- **Allow Write** - Allow the user/profile group to have write privileges for this share.
- **Allow Browse** - Allow the user/profile group to have be able to browse the share.
- **Full Control** - Allow the user/profile group to have Full Control for this share.
- **Deny All** - Disallow the user/profile group access to this share.

4. Click the OK button to save the information into the Permissions list.

▼ Remove the permissions set to a user or a profile

If you do not want to have specific permissions for a given user or access profile anymore:

1. Select the line of the user or profile from the Permissions list and click the Delete button.
2. To make this change effective you have also to click the OK button of the Share properties window.

If you remove a profile from the list, no user that belongs to that profile will be able to access the Share unless the user has a specific entry in the list.

If you remove a user from the list, the user will still have access to the Share. His permissions will be defined by his access profile permissions.



If you add a new Access Profile in the NAC section of edgeBOX, a new line on Permissions table of all shares will be automatically created:

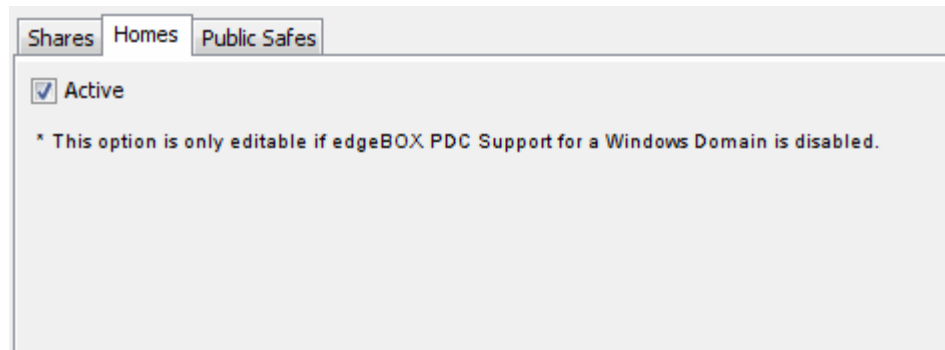
- This Access Profile will have read, write and execute permissions case the share is Public.
- This Access Profile will have read and execute permissions case the share is Writeable or Readable.
- This Access Profile will have no permissions case the share is Non Readable.

5.2.2 Homes

Authorised users can have a home directory on the edgeBOX. The home directory works as a network folder only accessible to the user.

Active

Activates the home directories for authorised edgeBOX users. The amount of space available to each user may be controlled by setting disk space quotas.



5.2.3 Public Safes

Public Safes are a great way to allow users to exchange files using a temporary folder. Safes can be request via the edgeBOX Services web page.

Active

Activates the Public Safes service.

Size Limit

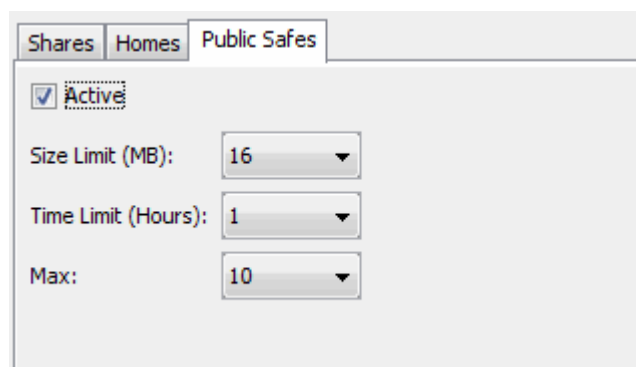
The amount of disk space assigned to a new safe. Safes can range in size from 4 to 1024 Mbytes.

Time Limit

The period a temporary safe is available. Periods range from 30 minutes up to 12 hours.

Max

The maximum number of Safes that can be active at a given time. Up to 20 Safes may be active at one time.



5.3 Printers

The printer must be connected to the edgeBOX via the edgeBOX USB port.

Note: In order to be able to share a printer the Samba service must be running. edgeBOX supports any printer that is supported by CUPS.

Connected

Displays a list of the printers currently plugged into the edgeBOX. Before a printer can be shared it must be configured. Select a printer and click on the Configure button to add it to the list of configured printers.

Configured

Displays a list of the printers currently shared over the network. To remove a printer from the network, select it from the list and click the Remove button.

The screenshot shows a web-based interface for managing printers. At the top, there is a navigation bar with tabs: "Windows Domain", "File Sharing", "Printers" (which is selected), "Quotas", "Backup & Restore", and "Maintenance". Below the navigation bar, the interface is divided into two main sections. The first section, titled "Connected", contains a table with three columns: "ID", "Name", and "URI". The table is currently empty. Below the table is a "Configure" button. The second section, titled "Configured", contains a table with three columns: "Name", "Description", and "URI". This table is also empty. Below this table is a "Remove" button.

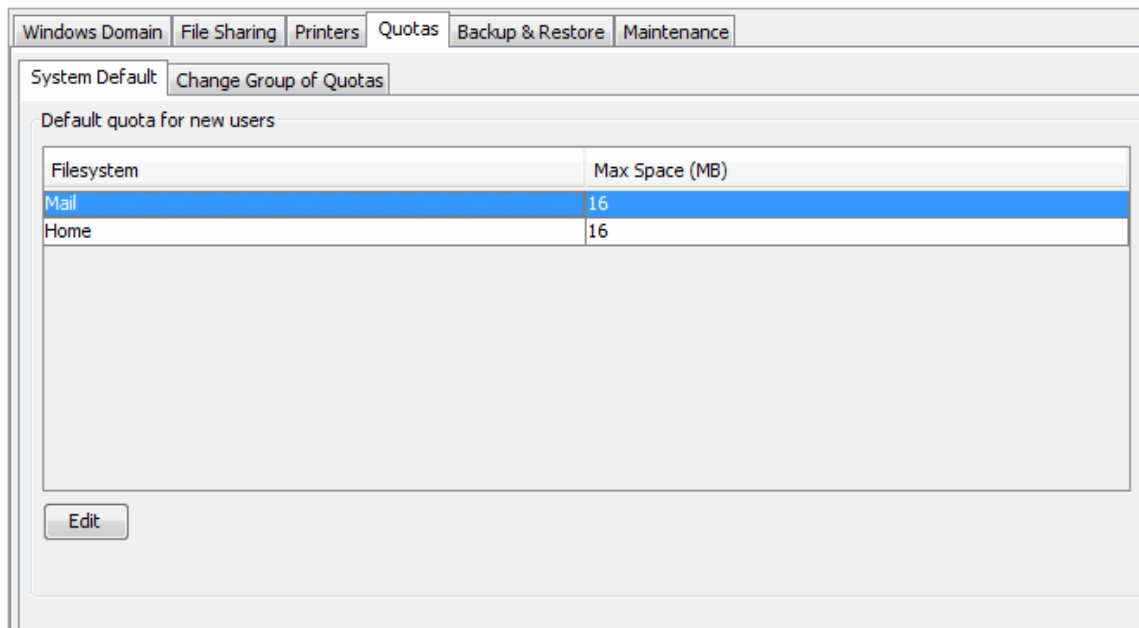
ID	Name	URI
----	------	-----

Configure

Name	Description	URI
------	-------------	-----

Remove

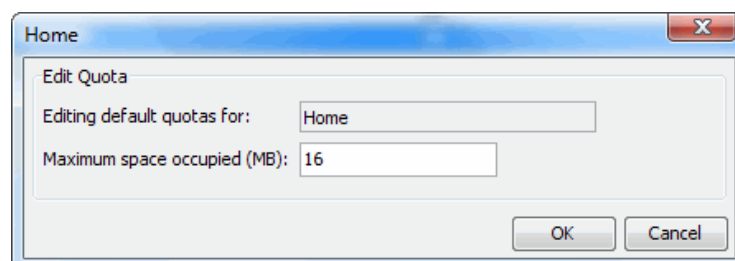
5.4 Quotas



Quota Configuration Page

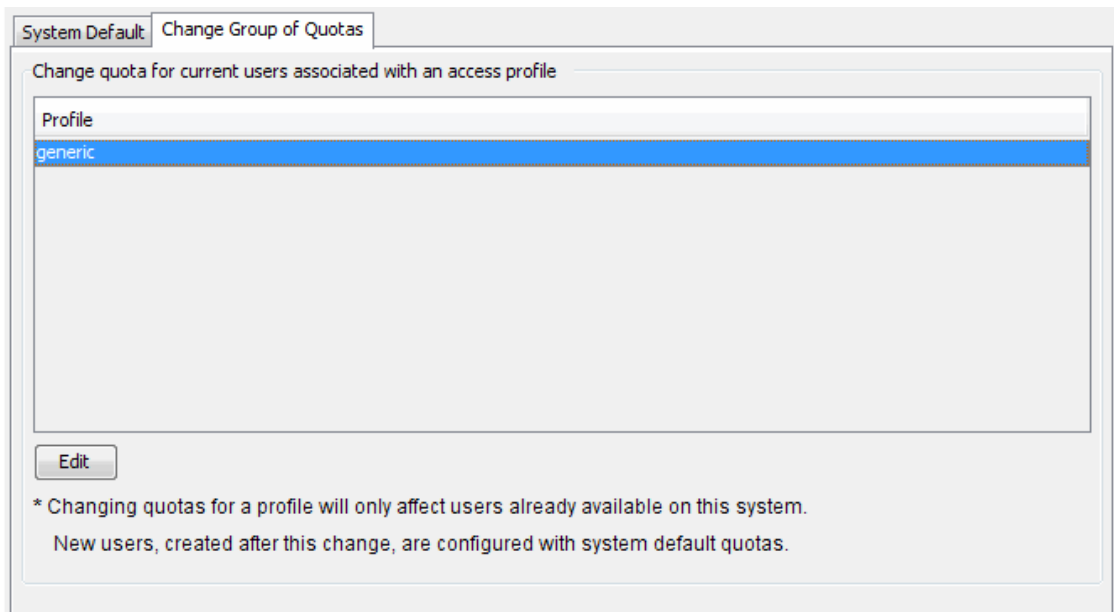
This menu option allows you to configure disk quotas. By setting disk quotas you are limiting the amount of disk space a user may consume. This feature is useful to keep disk usage at appropriate levels (and ultimately to prevent edgeBOX from running out of disk space). You have two file systems available for which you can set quotas, corresponding to the user's home directory and to the user's mail. To set users' quotas for one of these file systems:

- Select the file system for which you want to set quotas.
- Select "Edit". A popup window will appear.
- Change the desired value(s): Maximum number of Megabytes.
- Select "OK" to confirm or "Cancel" to abort changes.
- Check the status returned for errors.
- **Note** that the new Quotas are applied to new users only and not to existing users.

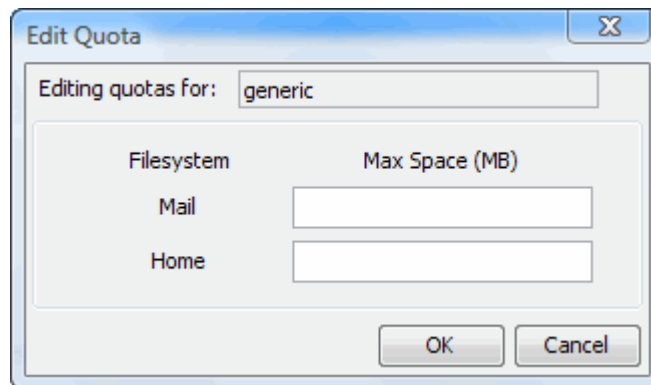


5.4.1 Change Group of Quotas

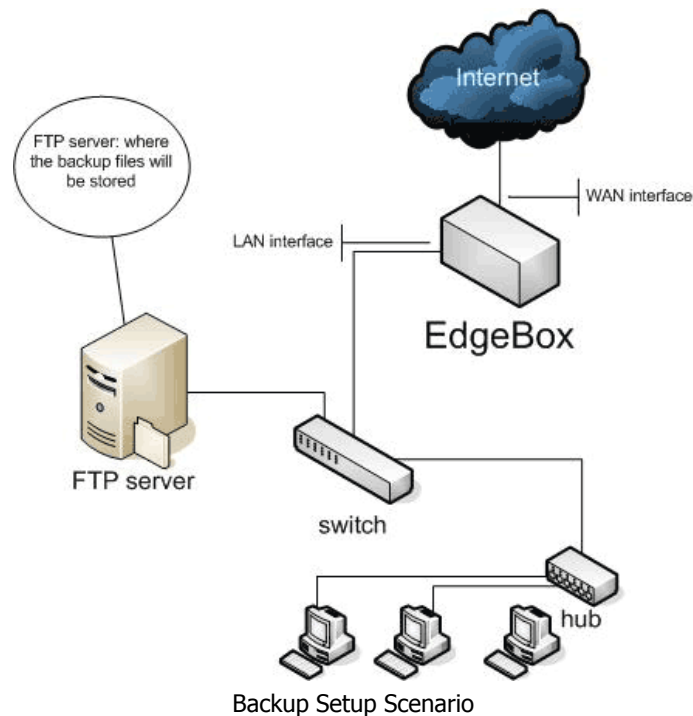
This panel allows to to set the quotas for users who are members of a [Profile group](#)



When editing the Group Quota, you can set limits for Mail and the home directories. Note that is new members are added to the profile group, they will inherit the system quota values and not the values previously entered for their Profile.



5.5 Backup & Restore



edgeBOX can schedule backups to occur periodically at a predefined time, day and date. These backups can be stored either on a remote FTP server, a Windows File Share, or on a locally connected USB disk (connected to the edgeBOX). Storage the backup on locally on the edgeBOX is not possible.

We advise you to define a backup policy from the start, to prevent the loss or corruption of data.

Recovery of a backup is only supported from the same version of edgeBOX that the backup was applied to (ie version X to the same version) and to the same architecture.

Also note, that during a backup and recovery, services are stopped and restarted.

Next, we will describe how to configure backups and how to perform a restore from a backup.

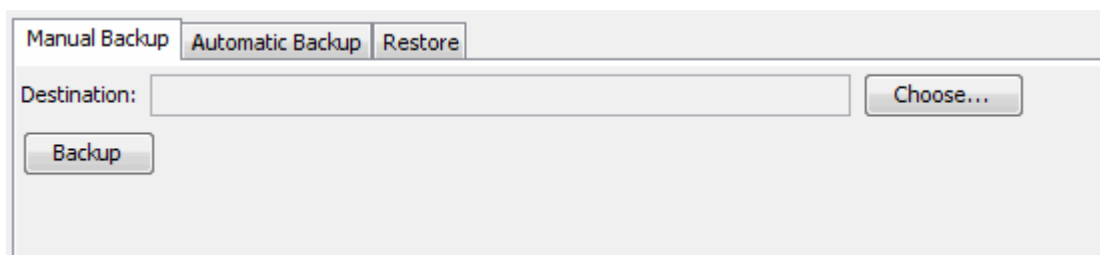
BACKUPS

- Backups may only be created/restored to/from a local USB disk, a remote FTP server, or a Windows File Share
- Backups and Recovery cause edgeBOX to stop many system and application processes (eg VoIP and authentication)
- Local USB disks **cannot** be formatted as NTFS
- Recovery is supported from the same version of the Operating system to the same version (eg v4.6 to v4.6).

- Recovery is supported from the same architecture to the same architecture
- Multiple edgeBOXes can use the same directory, as the backup files have a unique prefix associated with an edgeBOX
- Incremental backups are supported

5.5.1 Manual Backup

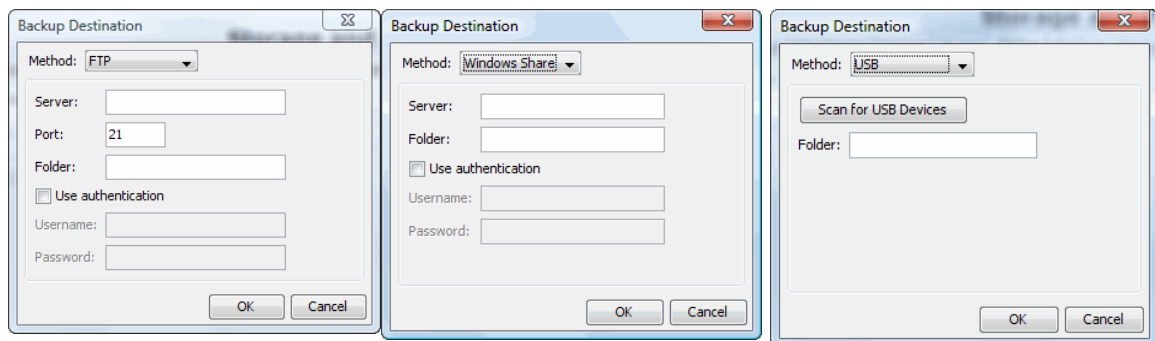
Manual backup allows you to undertake a backup immediately.



Selecting the choose button, presents you with three alternative backup option, which are "FTP", "Windows Share" and "USB". Save the backup on locally, on the edgeBOX it self is not possible.

Once all the relevant fields have been entered, press OK to save the configuration and then Backup to start the backup.

The options are:



Method: FTP allows you to select an FTP server which will store the backup files

Server: IP address of the FTP server

Method: Windows Share allows you to select a share from a windows server, which will store the backup files

Server: IP address of the Windows Server

Method: USB allows you to select a local USB disk (Not NTFS formatted) which will store the backup files

Scan for USB Devices: Will scan the local USB devices and present you with a drop down list to

enable you to select the device which will store the backup files

Port: FTP Port (usually 21)

Device: The chosen device (You may have more than 1 USB disk connected) on which the backups will be stored

Folder: Which folder on the FTP server where the backups will be stored

Folder: Which folder on the Windows Share will receive the backup files

Partition: If the device has more than 1 partition, you can select which one you will use to store the backup files.

Use Authentication: If checked the username and password fields will be active

Use Authentication: If checked the username and password fields will be active

Folder: Which folder on the USB device, where the backups will be stored

Username: The username of the account you are going to use on the FTP server

Username: The username of the account you are going to use on the Windows File server

Password: The password of the account which you are going to use on the FTP server

Password: The password of the account which you are going to use on the Windows File server

5.5.2 Automatic Backup

This panel allows you to specify a scheduled backup regime. for full and incremental backups.

Full Backup

You may create (or disable) a schedule for full backups.

The "Scheduling" dropdown has some specific entries which may be appropriate. If they are not appropriate, select "Other" to specify the time and frequency of the backup.

Note: If you select a date such as the 31st and the month has less than 31 days, the backup will not take place.

Note: If the folder of the FTP server or disk that is specified to store the backup, does not exist, the backup will fail (it will not automatically create the folder).

Incremental Backup

The same options are available for Incremental as for Full Backups, however, Incremental backups backup the files which have been modified since the last Full or Incremental Backup.

If you select a date such as the 31st and the month has less than 31 days, the backup will not take place.

Note: The full and Incremental backups should not be scheduled to occur at the same day and time. Typically, you would schedule a full backup during, say, Sunday 04:00 and incremental backups at 04:00 Mon-Sat.

5.5.3 Restore

This panel allows you to manually restore files from either a windows share, an FTP server or a local USB disk.

Press the "Choose" button to select the device where the files are stored and enter the appropriate details (directory, username etc, as required). Then press the "Get" button, which should show all (Incremental and Full) backups.

To restore, simply press the "Restore" button.

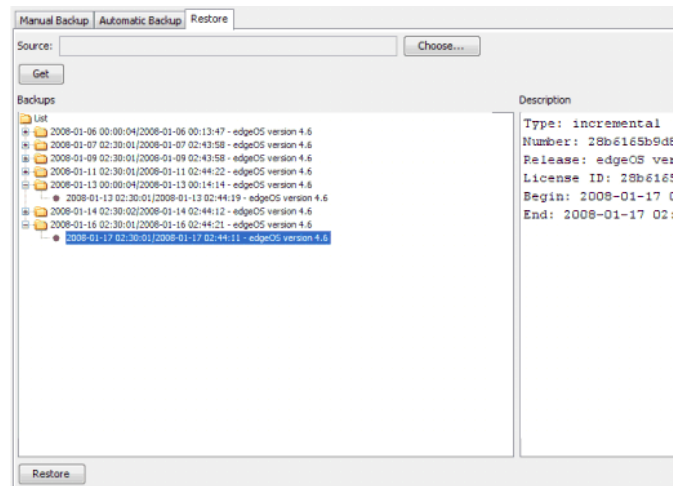
If you select an incremental backup, the system will restore this backup all all appropriate incremental backups and the full backup.

For example, If you have the following backup scheme:

Sun=Full

Mon-Sat=Incremental

and you restore the Wednesday Incremental, it will also restore the Tues and Mon Incremental and the Sun Full backup.



Note: During the restore process, edgeBOX will shut down services (ie calls will not be able to be made) and will reboot at the end of the restore process.

Note: A Restore is only supported when applied to the same version of edgeBOX that was backed up. That is:

Backup edgeBOX V4.6, restore to V4.6 - Supported

Backup edgeBOX V4.5, restore to V4.6 - Not Supported

Note: A restore only supports restoring to the same architecture (ie backup dell server, restore to IBM is not supported)

5.6 Maintenance

In the Maintenance module it is possible to schedule system database optimization in order to improve performance of VoIP service and the Reporting engine. The main reason to do this is to increase user responsiveness and overall usability. The performance can be significantly increased by simply enabling this feature, sometimes in order of magnitude of 4000%.

The Database Optimization can be done in several recurrence patterns, to know:

- **Disabled:** Disables optimization scheduling.

- **Every Week:** Performs Database Optimization on a weekly basis.
- **Every two weeks:** Performs Database Optimization on a biweekly basis.
- **Every four weeks:** Performs Database Optimization on a monthly basis.

For each previous recurrence pattern you can set a given time period during the day for running database optimization, by specifying the hour and minutes. Also, you can configure the day of the week when to run the maintenance tasks.

Note: Database Optimization consumes long periods of time to be completed, varying from a few minutes to some hours. This depends on the factors as the load of the edgeBOX and the amount of data being processed.

Please schedule your data optimization for a period of day where there is no (or low) load on your box, or when no services are being used to minimize the impact on services.

Example: A very simple example, is to set the edgeBOX database optimization tasks, weekly, every Saturday at 4:00am. This always depends on your service usage. Adapt the best solution for each case.

6 VoIP and IP-PBX



edgeBOX integrates the Asterisk IP PBX to deliver a comprehensive Internet telephony solution. The PBX allows for the integration of ordinary VoIP extensions with analogue or digital (ISDN) phone lines.

The VoIP configuration options are divided into six main categories which are not completely independent:

- [Phones](#)
- [Inbound Calls](#)
- [Outbound Calls](#)
- [PBX Features](#)
- [Hardware](#)
- [Options](#)

In addition, a Flash Operator Panel ([FOP](#)) is available (requires the [Web Server](#) to be running). This application allows the Operator to view the current status of the PBX and can use drop and drag functionality to make, for example, calls add move calls to queues.

The VoIP log files may be downloaded via FTP. This is achieved via the [logmaster](#) ftp account. The format of the log files are detailed in [Appendix G](#)

The initial edgeBOX configuration uses a set of pre-defined numbers. These are:

Voicemail	9999
Parking	700-715
Conf Call	9000+ (as you will increment this as you add Conferences)
National Prefix	0
International Prefix	00
Emergency Number	112 for EU countries

6.1 Phones

In this panel, the list of phones and extensions known to the system is displayed in a table.

Service State: **RUNNING**

Phones	Inbound Calls	Outbound Calls	PBX Features	Hardware	Tools and Services
Extension Number	Extension Name	Protocol	Voicemail	Published	Extension Status
2002	marco	SIP	Yes	No	Offline
2001	sales	SIP	No	Yes	Offline

New Phone Edit Phone Delete Phone

You can see the status of each phone in last column of the list. When a phone is Online you can see the IP address of the phone if you place the mouse over the Online text.

You can **add new phones**, **edit** the properties of existing phones or **delete** them.

After phones have been added to the system and associated with an extension, all VoIP clients need to register with edgeBOX to use the services it provides. This is usually achieved by configuring a web interface on the phone and entering details such as the IP of the edgeBOX, username and password to match that created on the phone on the edgeBOX.

edgeBOX comes with 3 already configured example phones. The phone "user" is associated with one of the example users that also exist by default. The other two phones, phone "desk" and phone "room", are not associated with any user.

- Phone "user" - Extension Number: "1000"; Extension Password: "1000"; Extension PIN: "1000".
- Phone "room" - Extension Number: "1010"; Extension Password: "1010"; Extension PIN: "1010".
- Phone "desk" - Extension Number: "1020"; Extension Password: "1020"; Extension PIN: "1020".

6.1.1 New Phone

Add a phone to the system and associate it with an extension. There are three types of phones you can specify:

- [VoIP](#)
- [Analog](#)
- [ISDN](#)

If the phone is created with the same Extension Name as the Username of an existing user, that user will be able to use Self-Service (available when a user logs in with their own credentials) to edit some of the phone properties.

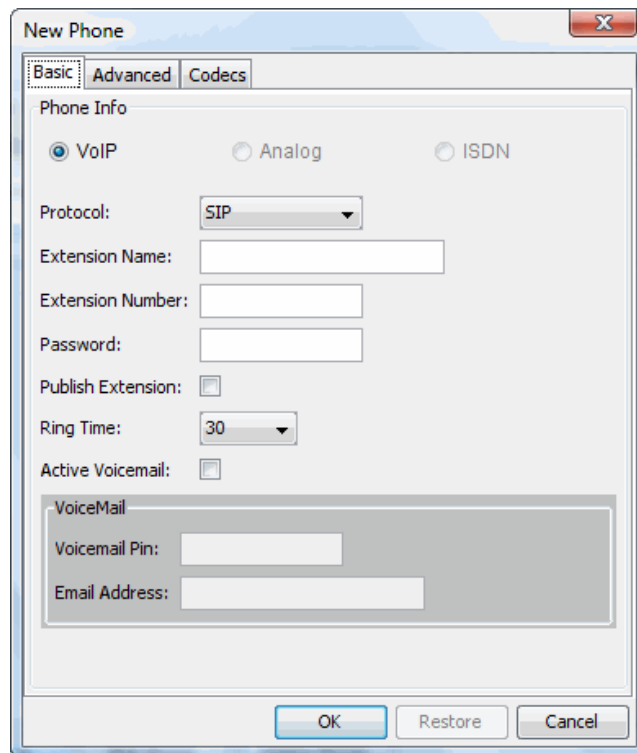
All phones must be associated with Phone [Groups](#). If a phone is not associated with a group, it will be entered into the default phone group (not the same as a group or profile for NAC). Outbound routes require specification of a phone group for access. Phones can be members of multiple phone groups.

Names and passwords must not be more than 40 characters in length and cannot contain special characters. The only exception is the + symbol, which is allowed in VoIP (for obvious reasons). In general it may be prudent to use names which are shorter than 17 characters.

6.1.1.1 VoIP

A VoIP phone has the following properties:

- Type of Phone: Choices are VoIP, Analog and ISDN
- Protocol: The protocol to be used by the phone. Possible choices are SIP or IAX2.
- Extension Name: This will be the name used by the client when registering the phone with edgeBOX.
- Extension Number: The number to be assigned to the new extension.
- Password: Password to be used when registering this phone with edgeBOX.
- Publish Extension: If checked, allows you to dial this phone directly with a public SIP URI.
- Ring Time: The phone timeout, which will go to voicemail, if voicemail is active
- Active Voicemail: If you check "Active Voicemail", you will need to enter:
 - A pin which the user will have to supply to access this mailbox.
 - An email address where the new voice mail notifications will be sent.



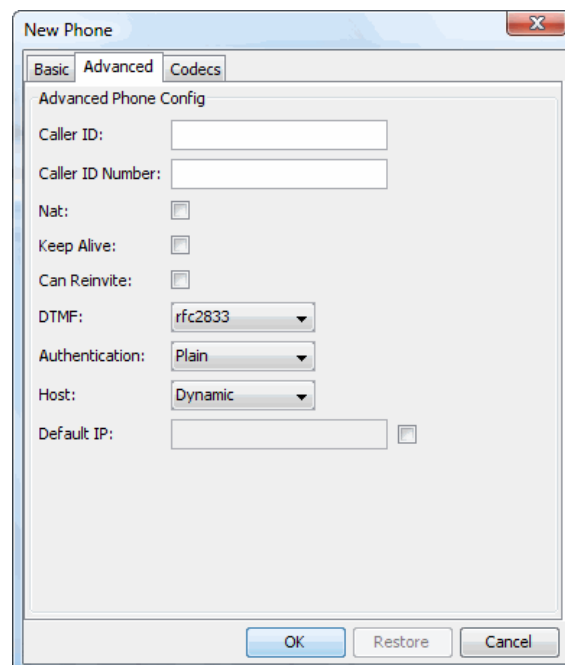
The 'New Phone' dialog box is shown with the 'Basic' tab selected. It contains the following fields and options:

- Phone Info:**
 - ☒ VoIP, ☐ Analog, ☐ ISDN
 - Protocol: SIP (dropdown)
 - Extension Name: (text field)
 - Extension Number: (text field)
 - Password: (text field)
 - Publish Extension: ☐
 - Ring Time: 30 (dropdown)
 - Active Voicemail: ☐
- VoiceMail:**
 - VoiceMail Pin: (text field)
 - Email Address: (text field)

Buttons at the bottom: OK, Restore, Cancel.

6.1.1.1.1 Advanced

This panel allows you to configure protocol-specific settings. Available options are:



The 'New Phone' dialog box is shown with the 'Advanced' tab selected. It contains the following fields and options:

- Advanced Phone Config:**
 - Caller ID: (text field)
 - Caller ID Number: (text field)
 - Nat: ☐
 - Keep Alive: ☐
 - Can Reinvite: ☐
 - DTMF: rfc2833 (dropdown)
 - Authentication: Plain (dropdown)
 - Host: Dynamic (dropdown)
 - Default IP: (text field) ☐

Buttons at the bottom: OK, Restore, Cancel.

- **CallerID:** The name by which calls will be identified to the called party. Usually identifies the person using the extension. If left blank, a default CallerID will be generated using the data introduced previously in the basic configuration panel.
- **Caller ID Number:** This is the number you wish to display to the person receiving the call.
- **NAT:** It is necessary when the phone is behind devices as a router or a firewall. NAT is enabled by default. Remove the selection from this option if you do not want to use it.
- **Keep Alive:** Sends a keep alive every 2 seconds.
- **Can Reinvite (SIP Only):** Asterisk sometimes needs to be able to re-insert itself into the media path in the middle of a call between the phones to provide services such as music on hold, transfer, parking etc (when they are requested). The SIP mechanism for this is the Reinvite.

Two phones which are connected can have the media stream changed mid-call using this mechanism, so Asterisk can “unstitch” the direct link and re-connect the Peers to itself. However, not all phones support this mechanism.

If you set Reinvite=no on a SIP channel, it indicates that the phone doesn't support the Reinvite mechanism for reconnecting the audio mid-call. In this case, Asterisk inserts itself into the media stream for the whole duration of the call, so that it is already there, if one of the parties requests one of these in-call features.

- **DTMF Mode:** The way the client deals with DTMF signaling. This parameter should be consistent with the client configuration. Available options are:
 - **Inband:** DTMF signaling within the call. Note that this type of signaling is not supported by the GSM codec.
 - **rfc2833**
 - **Info**
- **Authentication:** Plain or MD5 (SIP only): If MD5 is selected the password (used when registering the client) is encrypted by an MD5 hash.

Note: Before selecting the option MD5 in the Authentication dropdown box, to create an MD5 password you need first to create the MD5 hash based on the password you want to use. To do so:

1. Go to a Linux command line and type in the command `echo -n "<user>:<realm>:<secret>" | md5sum`. The user is the name of the phone. The realm is asterisk. The secret is the password that you will use on the phone. Case you are using a Microsoft Windows operating system you need to download a third-party program that can make MD5 hashes.
2. Copy the result of the command and paste it in the Password field of the first tab of the phone properties window.
3. Then select the MD5 option in Authentication drop down option.

- Host: available values are:
 - Static: If selected, you will need to specify the IP address for the client registering with the credentials entered, using the Hostname text box.
 - Dynamic (default): The client will provide its IP address when registering with edgeBOX.
- Default IP: This option will be available if you've selected "Dynamic" in the previous option. The default value is unchecked.

If you check this option you will need to supply an IP address which will be used by edgeBOX to try to communicate with the client, if it hasn't registered yet.

6.1.1.1.2 Codecs

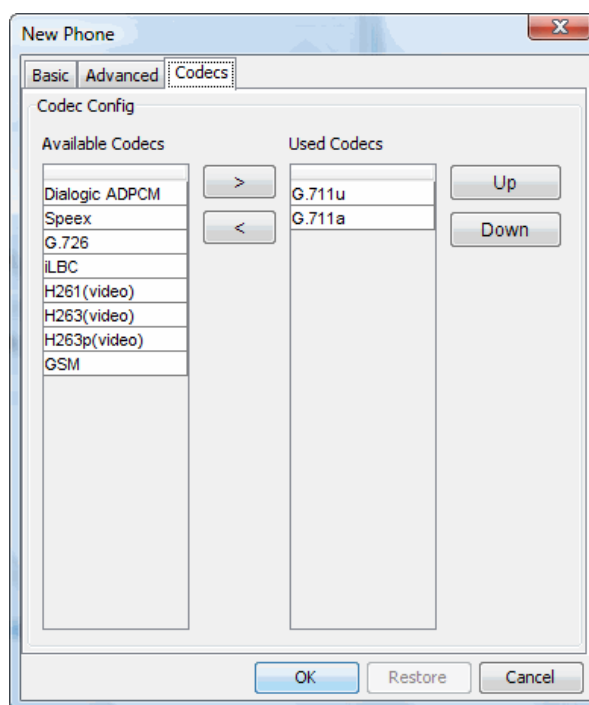
Codecs are used when converting an analogue voice signal to a digital one. edgeBOX supports several types of codecs allowing a flexible client configuration. The choice of the codec to be used usually results from a compromise between sound quality and bandwidth used. Available codecs are:

- ULAW (G.711u): Known as the native codec in modern communication lines. Provides good quality sound, at the expense of bandwidth. It is the most commonly used codec for VoIP calls because, besides being supported by most VoIP providers, it has the lowest latency as no type of compression is used. It is the codec used in PSTN and ISDN lines.
- ALAW (G.711a): Basically, a G.711 version used in E1 European lines.
- Dialogic ADPCcodec, suitable for robust voice communication over IP.
- GSM: Usually used on European mobile networks, this codec uses a small amount of bandwidth providing an acceptable quality of sound.

Select the codecs you wish to allow by highlighted them and using the > button. You can also select the order by highlighting the codec and selecting the Up or Down button. For example, if you purchase the G729 Codec, you would highlight it and press the > button. Then you may wish to move this codec to the top of the "Used Codecs" list so that it will be used first.

M: This is a legacy codec, kept for compatibility with version 3 of edgeBOX.

- Speex: Audio codec designed specifically for speech, and as such, well suited for VoIP.
- G.729: Offers good sound quality with conservative use of bandwidth. However, to be able to use it a [license](#) must be acquired.
- G.726 ADPCM can be interchanged between packet voice, PSTN, and PBX networks if the PBX networks are configured to support ADPCM.
- iLBC: Low bit rate



If there isn't a specific system requirement, the choice should be ULAW, because it is compatible with most phones and softphones available on the market.

- H26*: These codecs are used for video calls.

6.1.1.2 Analog

An analog phone has the following properties:

- **Type of Phone:** Choices are VoIP, Analog and ISDN
- **Line (FXS):** The [port](#) which the phone is connected to
- **Extension Name:** This will be the name used by the client when registering the phone with edgeBOX.
- **Extension Number:** The number to be assigned to the new extension.
- **Publish Extension:** If checked, allows you to dial this phone directly.
- **Ring Time:** The phone timeout, which will go to voicemail, if voicemail is active
- **Active Voicemail:** If you check "Active Voicemail", you will need to enter:
 - A **PIN** which the user will have to supply to access this mailbox.
 - An **email address** where the new voice mail notifications will be sent.
 - **Voicemail** timeout from the list

The screenshot shows the 'Edit Phone' dialog box with the 'Basic' tab selected. The 'Phone Info' section has three radio buttons: 'VoIP', 'Analog' (selected), and 'ISDN'. Below these are text fields for 'Extension Name' (containing 'analog'), 'Extension Number' (containing '505'), and 'Password'. There is a checkbox for 'Publish Extension' which is unchecked. Below that is a 'Ring Time' dropdown menu set to '30' and a 'Line (FXS)' dropdown menu set to 'Zaptel/1*'. The 'VoiceMail' section has an 'Active Voicemail' checkbox which is unchecked, and text fields for 'Voicemail Pin' and 'Email Address'. At the bottom are 'OK', 'Restore', and 'Cancel' buttons.

6.1.1.2.1 Advanced

In the advanced tab you can configure the following properties:

- **Caller ID** - Enter the caller ID for the line
- **Caller ID Number** - This is the number you wish to display to the person receiving the call.
- **Echo Cancel** - Software to cancel echo in the communications. It is active by default. If you don't want to use it on the phone, remove the selection for this option.
- **Fax Support** - If checked, will improve tone detection for the Fax machine by turning off echo cancellation whilst the fax is in operation.
- **Gain** - Varies the volume between an 8db gain or loss. This value should be adjusted depending on the network.

6.1.1.3 ISDN

An ISDN (Redis) phone has the following properties:

- Type of Phone: Choices are VoIP, Analog and ISDN
- Line (BRI): The line to which the phone is connected. The Second field is the MSN number

for the line

- Extension Name: This will be the name used by the client when registering the phone with edgeBOX.
- Extension Number: The number to be assigned to the new extension.
- Password: Password to be used when registering this phone with edgeBOX.
- Publish Extension: If checked, allows you to dial this phone directly (via enum) if the line is set to untrusted. If the line is [trusted](#), all phones can be contacted directly via enum, whether this option is checked or not.
- Ring Time: The phone timeout, which will go to voicemail, if voicemail is active
- Active Voicemail: If you check "Active Voicemail", you will need to enter:
 - A pin which the user will have to supply to access this mailbox.
 - An email address where the new voice mail notifications will be sent.
 - Voicemail timeout from the list

The screenshot shows a 'New Phone' configuration window with two tabs: 'Basic' and 'ISDN Info'. The 'ISDN Info' tab is active. Under 'Phone Info', the 'ISDN' radio button is selected. The 'Line (BRI)' field has a dropdown menu showing 'mISDN/2' and a text box with '123'. The 'Extension Name' field contains 'isdn'. The 'Extension Number' field contains '1001'. The 'Password' field is empty. The 'Publish Extension' checkbox is unchecked. The 'Ring Time' dropdown menu shows '30'. The 'Active Voicemail' checkbox is unchecked. Below these fields is a 'Voicemail' section with a 'Voicemail Pin' text box and an 'Email Address' text box. At the bottom of the window are 'OK', 'Restore', and 'Cancel' buttons.

6.1.1.3.1 ISDN Info

Go to [Hardware](#) Config to change Advanced Options (as the panel states).

6.1.1.4 Twinning

Twining enables you to almost **duplicate the behaviour of an extension** of the network on **another external phone**, as a cell phone for example. [Learn More](#).

If you activate and configure twinning with, for example, a cell phone:

- When a call arrives at the network phone (for example, extension 2001) then both the network phone and the cell phone will ring. The phone that will pick up the call is the one that will be first answered. This is useful, for example, when a user goes to lunch. He is able to pick up calls that come to his extension on his cell phone while lunching.



However, **when the user answers a call on his cell phone that was sent by edgeBOX through an analog line**, the user needs to **press the # (cardinal) key after answering**. This will inform edgeBOX that the call was picked up and edgeBOX will stop ringing the extension of the user. Otherwise the extension will keep on ringing despite the call having already been answered by the user.

- The user can make calls with his cell phone as if he was on his extension at work, even if he is at home. The user just needs to dial the number of the company. The answer will be answered by edgeBOX and the user will hear the dial tone again. The user can then make internal calls just by dialing the extension he wants to call or make outgoing calls that will appear to the recipient as being made by user's regular work phone.

▼ [Allow twinning on a phone](#)

The twinning feature is defined by each specific phone. By default phones are not allowed to twin with other phones like cell phones.

To allow a phone to twin with another one:

1. Select the desired network phone from the phone list and click the Edit Phone button.
2. Go to twinning tab and select the option Enable Twinning on This Phone.
3. You can also immediately enable turn the twinning on and indicate the phone you want this phone to twin with, or you can leave it up for the user of the phone to configure it himself.
4. Click the OK button to save the changes into the phone's list and then the Apply button to save.

▼ [Turn on twinning with another phone](#)

1. Select the desired network phone from the phone list and click the Edit Phone button.
2. Go to twinning tab.
3. Press Turn On. If twinning was never set on this phone than you have to specify the number of the you want to twin with. If twinning has been already configured before that the last phone number this phone has twinned with will appear. You can change it if you would like to twin with a different phone.
4. Click the OK button to save the changes into the phone's list and then the Apply button to save.

▼ [Change the number of the phone the network phone is twinning with](#)

1. Select the desired network phone from the phone list and click the Edit Phone button.
2. Go to twinning tab. There you can see the number of the phone this phone is currently twinning with.
3. To change the number press the Change Number button. A dialog window will appear. Type the new phone number in the field and press OK.
4. Click the OK button of the phone properties window to save the information to the list and then click Apply to effectively save the change.

▼ Turn off twinning

This is particularly useful when the user is close to both phones at the same time, the network phone and his personal cell phone, for example. In this cases, having both phones ringing at the same time is not really useful, so you can switch off twinning so just the company phone rings when a call is received, for example.

To turn twinning off of a phone:

1. Select the desired network phone from the phone list and click the Edit Phone button.
2. Go to twinning tab and press the Turn Off button. You will see that the status will change to OFF.
3. Click OK **to save** the change and then Apply in the bottom of the phones list.

Note that the feature is still allowed at the phone, it is just not enabled at the moment, this is, this phone is not twinning with another phone. But you, through edgeBOX's interface, or the phone's user, through the phone, can enable it again at any time.

▼ Enable and disabled twinning directly through the phone

You or the user of the phone with twinning can also enable, disable and change the number of the phone your extension is twinning with, directly on the phone itself instead of the edgeBOX. But to do so, twinning must be allowed on that phone.

- **Enable twinning** - on your phone, dial *90. Twining will be now enabled.
- **Disable twinning** - on your phone, dial *91. Twinning will be disabled.
- **Change the phone your phone is twinning with** - on your phone, dial *92* plus the phone number of the phone you want to twin. For example, if your cell phone is 912154014 you can dial *92*912154014.
- **Transfer an ongoing call from the cell phone to the network phone** - on your phone, dial *93* and the call you are answering in the cell phone will continue in the network phone.

6.1.2 Edit Phone

Allows you to modify details for existing phones. All fields may be changed, except the extension name.

6.1.3 Delete Phone

Allows you to delete a phone. There will be instances when you will not be able to perform this action. Specifically when:

- This extension is used in a context (for example in a Dial action. For more information, check [IVR Editor](#));
- This extension is used in an incoming rule (for more information, check [Call Rules](#));
- This extension's voicemail is used in an action.

6.2 Inbound Calls

This panel allows you to configure incoming call functionality, for example for calls originating from the PSTN network or internal calls between phones registered with edgeBOX. Several options are available for configuration, namely:

- [IVR Editor](#)
- [Internal](#)
- [Call Rules](#)
- [DID Routes](#)
- [DID Ranges](#)
- [Sound Manager](#).

You access each of this panels selecting the appropriate tab on the right.

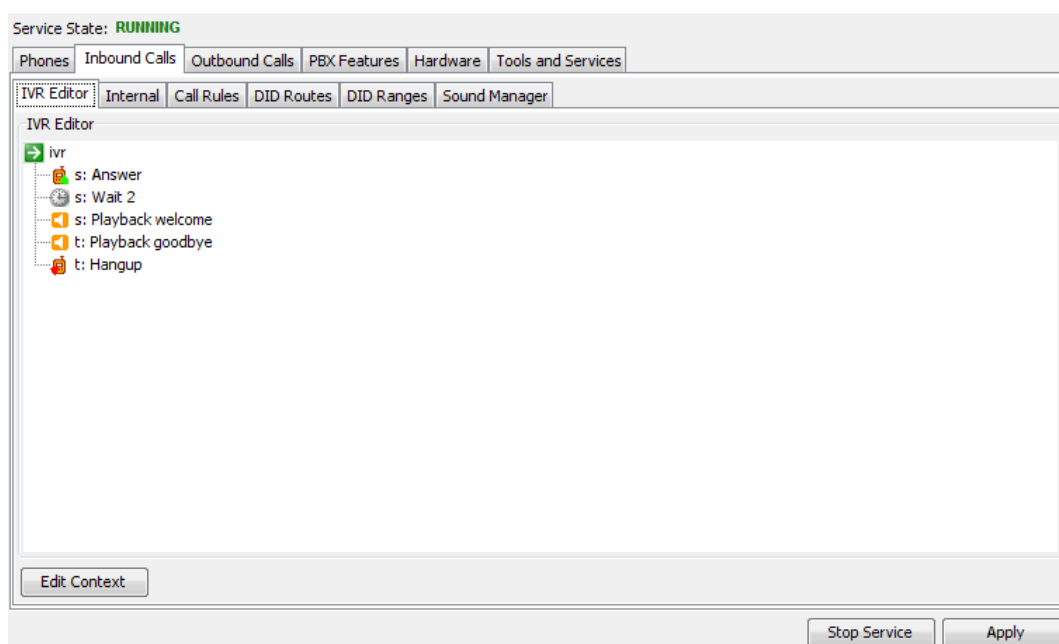
6.2.1 IVR Editor

edgeBOX provides a flexible IVR system, fully integrating all of edgeBOX's VoIP PBX functionalities, allowing the administrator to create response menus for a large range of applications. Callers using a touch tone phone will be able to navigate these menus by pressing the appropriate numbers.

An IVR system is made of contexts. Each context can have several actions, which in turn may trigger events, such as creating conferences, queues or connecting to another context, thus resulting in a navigation flow between different contexts.

The IVR system was implemented as a tree structure (see screen shot bellow), making it easy to understand the concept of navigating through the contexts. Each child node is either an action or a new context which may be expanded or minimised.

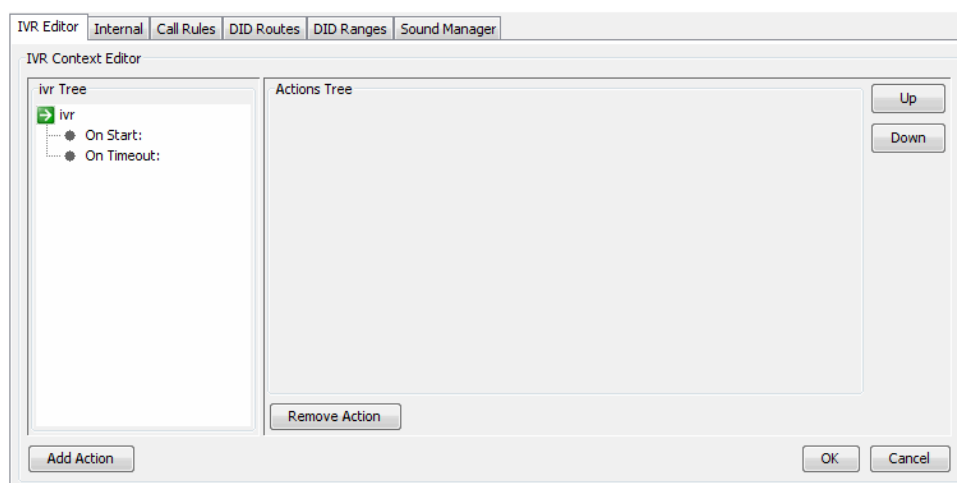
To add new actions to a context, select its icon and press "Edit Context" or, alternatively, double-click its icon.



6.2.1.1 Edit Context

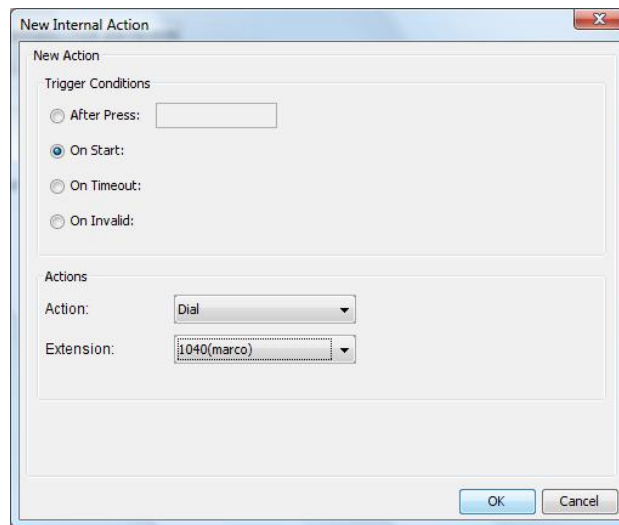
This panel allows you to modify a particular context. After selecting the desired trigger on the left panel, its list of actions will be visible on the panel on the right. Specifically, you will be able to:

- [Add new actions](#) by pressing the button "Add Action". A popup window will appear, requiring you to enter the action's details.
- [Remove actions](#) by pressing the button "Remove Action", after selecting the desired action and
- Modify an action's priority, selecting the desired action and using the up/down buttons on the right.



6.2.1.1.1 Add Action

This window allows you to add a new action to a context.



First, you will need to define which event will trigger this action:

- **After Press** - a sequence entered by the caller.
- **On Start** - this action will be automatically triggered when a context is called.
- **On Timeout** - this action will be triggered if there was no input from the caller 30 seconds after this context was called.
- **On Invalid** - this action is fired if the caller inputs a sequence with no action assigned to it in the context.

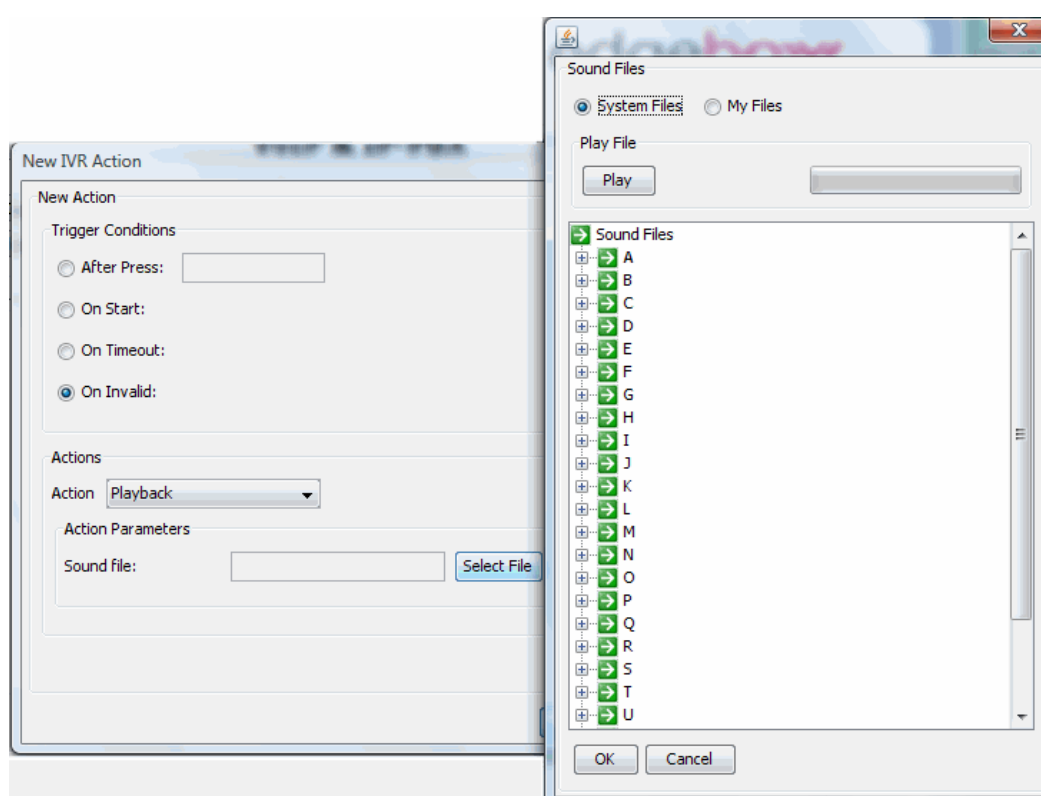
Then, you will need to define the action that will be done:

- **Dial** - a call will be placed for the chosen extension. You may choose any extension previously configured using the phones' panel, as well as any FXS mode analogue ports or any NT mode digital ports, available in BRI cards.
- **DialOut** - Allows you to specify a particular route for a specific tel number (eg to dial through a legacy PBX)
- **DISA** - Allows the user to authenticate and make calls as if he was on a phone of the edgeBOX. If you do not select the option of the DISA PIN, when the action DISA is executed, the user gets authenticated automatically. If you select that option and indicate a PIN, when the DISA action is executed edgeBOX will first ask the user the that PIN before it authenticates him.
- **Goto** - The call will be routed to another context. For more details, check [Goto Action](#).
- **Hangup** - this action will terminate the call.
- **Voicemail** - the call will be forwarded to the chosen extension's voicemail. You may choose any extension with an active voicemail.
- **Queue** - the call will be forwarded to a queue. You may choose any queue previously configured in the system.

- **MeetMe** - this call will join a conference. You may choose any static conference previously configured in the system.
- **HuntGroup** - all phones associated with the selected huntgroup will ring. The call will be forwarded to the first one to answer. You may choose any huntgroup previously configured in the system.
- **Answer** - Call will be answered
- **Background** - the selected sound file will be played but this time all numbers entered by the caller will be processed whilst the message is being played and resulting actions will be performed.
- **PlayBack** - the selected sound file will be played and all numbers entered by the caller will be ignored until the message has completed
- **Wait** - a pause is introduced in the call. You will need to specify the number of seconds this pause will last.

To select a sound file press the "Select Sound File" button. A new popup window will display, allowing you to choose the sound file either from "System Files", or from "My Sound Files" (files uploaded by the administrator).

You may listen to the files, using the "Play" button. This way, you may choose the sound file most appropriate for the situation.



6.2.1.1.1.1 Goto Action

One of the most important IVR actions, is the Goto action, which allows navigation between the available contexts.

After selecting this action, you need to supply the target context. This may be a previously created context or a new context.

You can go to an exiting context, which will appear in the "Select Context" drop down menu

If you want to create a new context, select the "New Context" option, and insert the new context name.

The edit context panel is divided in two main sections. On the left side it is possible to select the event that will trigger its actions. After selecting an event, its actions will be visible in the right panel. The actions are ordered by priority - with the top most being the ones executed first. The "Up" and "Down" buttons allow you to change the actions' execution order.

Note that you will need to press the "OK" button to confirm your changes then apply to activate them.

The IVR edition panel will then be visible again, where you can check all changes made to the context.

If you've created a goto action to a new context, it is possible to select this context to edit its actions.

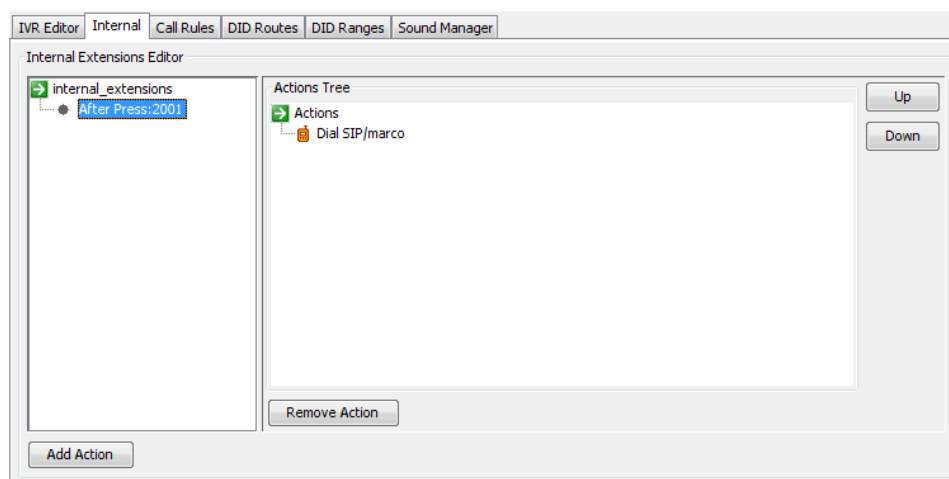
6.2.1.1.2 Remove Action

Allows you to remove an action from a context.

6.2.2 Internal

This panel allows you to configure internal extension routes. By default, a route is created at phone creation time when you supply an extension number. These routes may be completely changed, though.

The extensions are shown on the left panel and the actions are shown on the right side.



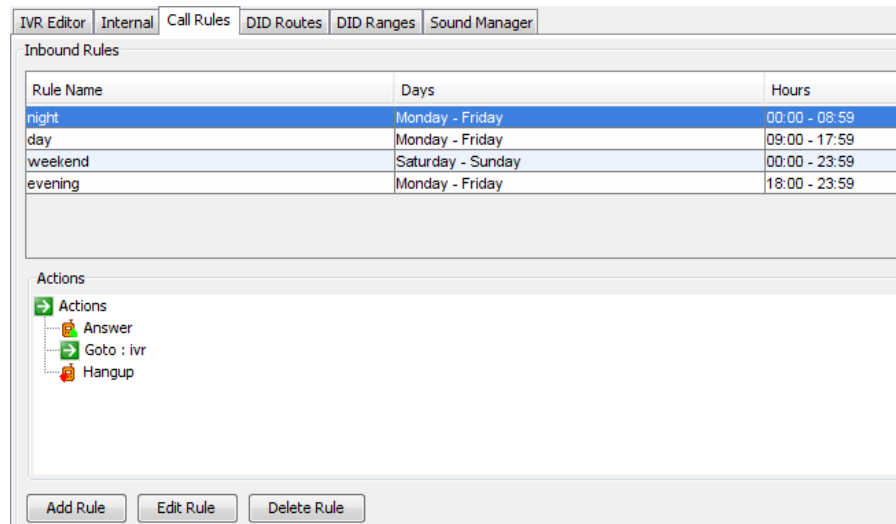
6.2.2.1 Add Action

The trigger conditions allow you to perform an action on timeout, or if a number is dialled. The options presented in this panel are the same as the ones in the IVR editor's [Add Action](#). You must also add an action here, to send calls to voicemail.

6.2.3 Call Rules

edgeBOX allows you to define rules to deal with incoming calls according to the hour/day in which they arrive. This way the administrator may define different actions depending on the hour of the day. For example, it is possible to play a message, warning that the company is closed during evening hours. It is also possible to define special rules for weekends and holidays.

edegBOX comes already with four pre-configured typical call rules and the usual voice prompts. You can change them to better fit your needs or just delete them if they do not apply to your scenario.



Call Rules panel with the pre-configured rules

Note: At least one rule needs to be defined for incoming calls.

Note: DID Routes (Next Section) take precedence over Call Rules. That is, if you define a DID route, the call rule will not be acted upon.

6.2.3.1 Add Rule

This panel allows you to create a call rule. For each rule definition, the time frame to which it applies and the actions to be executed have to be defined.

Time frame:

- **Weekdays:** If you select this option, you will need to select the weekdays between which this rule will be applied. For example, if we want to define a rule to be applied during the weekend, the limits should be defined as Saturday and Sunday.
- **Month Days:** If you select this option, you will need to select the month days between which this rule will be applied. Use this option when you want to define a rule to be applied to an holiday.
- **Hours:** Regardless of the option selected for days (Weekdays or Month Days), you will also need to select the hours interval to which this rule will be applied. If you want the rule to be valid for a whole day, this interval should be defined from 00:00 to 23:59.

Actions:

At least one action should be defined for each rule. The actions available here are exactly the same as when modifying a context in the [IVR panel](#). In the same way, the actions have an execution order, which may be changed using the "Up" and "Down" buttons.

Using the Goto action, the call may be forwarded to any context defined in the IVR. Bear in mind that for a call to enter the IVR flow, there should be an explicit rule here directing it to the IVR

(using a Goto action to the IVR context).

6.2.4 DID Routes

Using DID routes, it is possible to define rules for specific incoming call numbers. This functionality may be used when you wish to have a set of actions assigned to a specific number, for example to allow an internal extension to be accessed from outside directly.

You may [add a new DID route](#), selecting the "Add Route" button, modify a DID route, using the "Edit Route" button or remove a route, selecting the "Delete Route" button.

Please note that for DID routes to work, we assume that there is hardware capable of performing incoming number recognition installed in edgeBOX. For that to happen, a BRI or PRI card must be connected to a digital line. Or edgeBOX must have a FXO port, with an associated DID number.

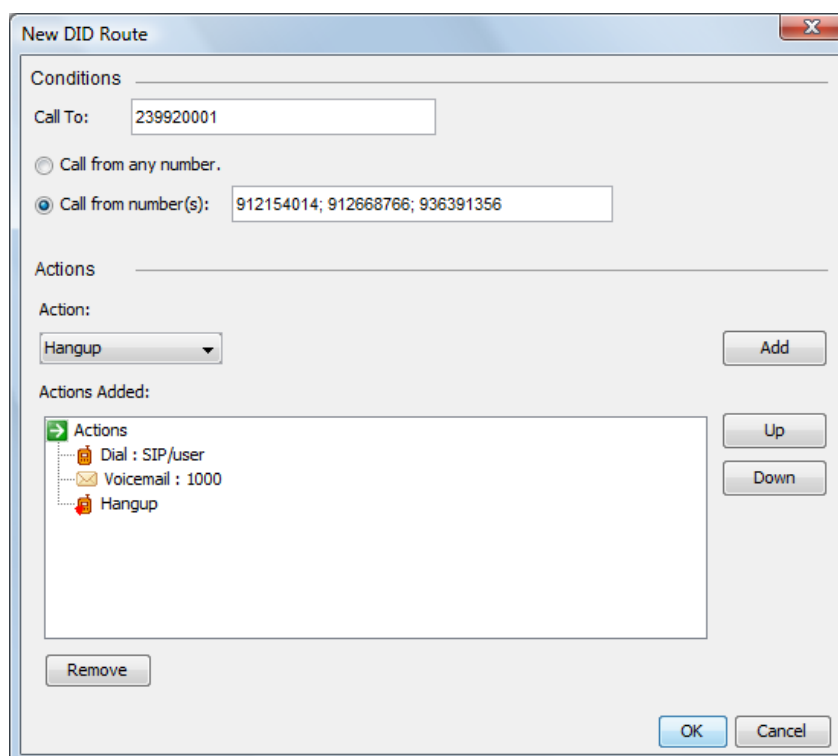
The screenshot shows the 'DID Routes' configuration window. At the top, there is a tabbed interface with the following tabs: 'IVR Editor', 'Internal', 'Call Rules', 'DID Routes' (which is the active tab), 'DID Ranges', and 'Sound Manager'. Below the tabs, the window is titled 'DID Routes'. It contains a large text input field labeled 'DID Route Number'. Below this field is an 'Actions' section, which includes a small gear icon and a button labeled 'Actions'. At the bottom of the window, there are three buttons: 'New Route', 'Edit Route', and 'Delete Route'.

6.2.4.1 New Route

To define a DID route:

1. Enter the phone number the caller dialed (the phone number the call is to) in the Call To field.
2. If you want you can restrict the numbers the call can come from (phone numbers of the callers) by selecting the option Call From Numbers and adding one ore more numbers in the text field after. If you do this, calls made from a number that is not in this list will not fall under this rule.
3. Add one or more actions when this condition is applied. To add an action, select the desired one from the Action drop down option, specify the additional parameters of the action case they exist, and click the Add button. The action will be added to the list.

The set of actions available are the same ones available in the [Add Action](#) popup windows in the [IVR context editor](#).



When this rule is applied to an incoming call, the actions of the rule will be executed in the order they are in the list.

6.2.5 DID Ranges

Use DID Ranges to configure multiple incoming lines sent to multiple extensions. It is most useful when you have sequential public numbers and you want that, each time a call arrives for one of these numbers, forward it to a different internal extension, in a set of sequential extensions. [View an Example.](#)

You have 20 public phone numbers: from 239 200 200 to 239 200 219 and you have 20 internal extensions: from extension 2000 to extension 2019 and you want to:

- Deliver calls to the number 239 200 200 in the extension 2000.
- Deliver calls to the number 239 200 201 in the extension 2001.
- Deliver calls to the number 239 200 202 in the extension 2002.
- ...
- Deliver calls to the number 239 200 219 in the extension 2019.

▼ Create a new DID Range

1. Go to the DID Range sub tab of the Incoming Calls tab.
2. Click the Add button below the list of DID Ranges.
3. Indicate the first number of the range of public phone numbers you want to use to make a DID Range in the field Initial Value. For example 239 200 200. If your range

of public phone numbers goes from 239 200 200 to 239 200 219.

4. Indicate the initial numbers of the extensions you want to forward the calls to in the Prefix field. This initial numbers are the numbers of the extensions that do not change. For example, if you want to use in the DID Range rule the extensions 2000 to 2019 then the first 2 number won't change. So you can type in 20 in the Prefix field.
5. In the Number of Digits to Match field type the number of digits that will be used in the rule. For example, if you want to forward calls that arrive at the numbers 239 200 200 to 239 200 219 to the extensions 2000 to 2019, in a sequential way then, type in 2 in this field. This means that edgeBOX will pick up the last two numbers of the public phone number a call is to, and add it to the number you have in the prefix to create the extension number where the call will be delivered.
6. Click the OK button to save the changes into the list and then the Apply button to permanently save.

Example: a call arrives to the number 239 200 213. edgeBOX picks up the last two digits (13) and adds them to the prefix (20) which results in the extension 2013. So it will deliver the call to the extension 2013.

▼ Delete a DID Range

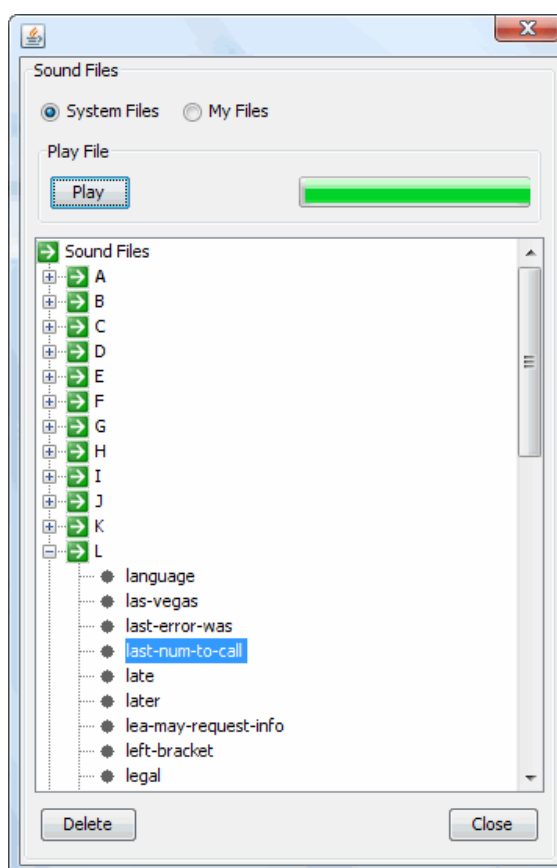
1. Go to the DID Range sub tab of the Incoming Calls tab.
2. Select the desired DID range.
3. Click the Delete button to remove the rule from the list.
4. Click Apply to effectively delete the rule.

6.2.6 Sound Manager

Sound Files Information

Shows how many system and additional sound files are available

You can delete and play the sound files by pressing the "Manage Files" button.




Upload Sound File

In order to use the "Playback" and "Background" actions, you need to select the sound file to use. This file may be a system file or a user file. This panel allows you to upload ".gsm" sound files. Select the desired file using the "Browser" button, and then select the "Upload" button.

If this operation is successful, the uploaded file should be available in the sound files management panel, where files may be played or deleted.

Sound Bank

You may use this panel to upload new system files (for example voicemail prompts).

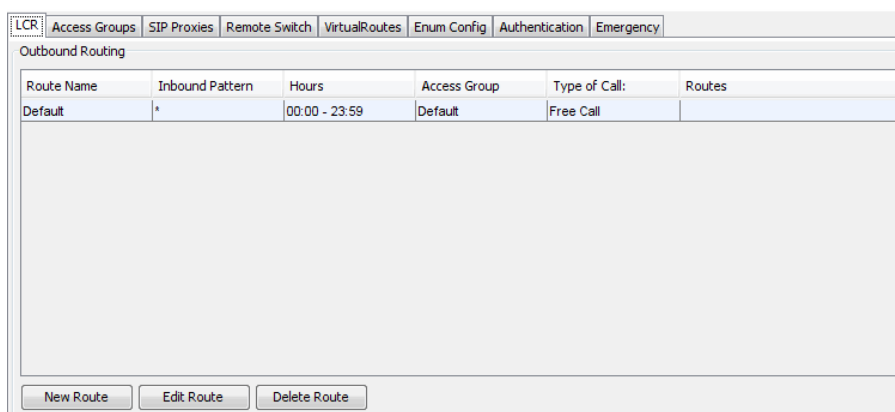
 Make sure you have the service FTP allowed on the [firewall](#) when uploading sound files or sound banks because the upload of the files to the edgeBOX is made via FTP.

6.3 Outbound Calls

This panel allows you to configure several aspects related with outgoing calls.

An outgoing call needs a route to be configured. There are two different kinds of outgoing routes:

- Direct connection to the PSTN network, using [hardware](#) installed on edgeBOX.
- Internet connection using a [SIP Proxy](#) or a [Remote Switch](#), or using the ENUM servers.



Route Name	Inbound Pattern	Hours	Access Group	Type of Call:	Routes
Default	*	00:00 - 23:59	Default	Free Call	

New Route Edit Route Delete Route

6.3.1 LCR

Outbound calls, identified by the appropriate InBound pattern (essentially an input pattern, such as 0044*), can be sent to a specified route (eg a mobile call may be sent to a low cost mobile provider, whilst calls to the USA, may be sent to a different provider)

For each of these types of calls, you will have to configure at least a route, a phone group to use this route and the patterns that will identify the group to which the call belongs. For instance, an international call will always be preceded by the "00" prefix (InBound) pattern.

Route Name	Inbound Pattern	Hours	Access Group	Type of Call:	Routes
Default	*	00:00 - 23:59	Default	Free Call	

New Route Edit Route Delete Route

6.3.1.1 New Route

- Inbound Pattern: Enter a Prefix number you wish to associate with, for example, a mobile number call (in this example, 9*).
- Name: Enter some descriptive text in the Name field
- Access Group: Select the Group (from the dropdown list)
- Type of Call: Select the type of call the members of this group may make
- Enter times for the From and To fields, which are the times this route is available (eg mobile calls allowed only after 18:00)
- Select a route (line) to use for this type of call. ZAP/1(in this example) is the port where the analogue line is attached.
- Enter the "Outbound Pattern" (usually the same as the "Inbound Pattern").
- Enter a Timeout in seconds. This is the timeout value edgeBOX uses before it will try the next route (if there is more than one route) to make the call.
- Enter (if Caller-ID is checked), your telephone line number. This can be useful if your line has more than one number associated with it. The Caller ID you set will be the 'apparent' number you have called from.

Note1: The 9* indicates a digit 9 followed by any other numbers. If you entered 9XXX, this would indicate a 9 followed by exactly 3 other digits (which may or may not include the digit 9)

The 'X's must be uppercase

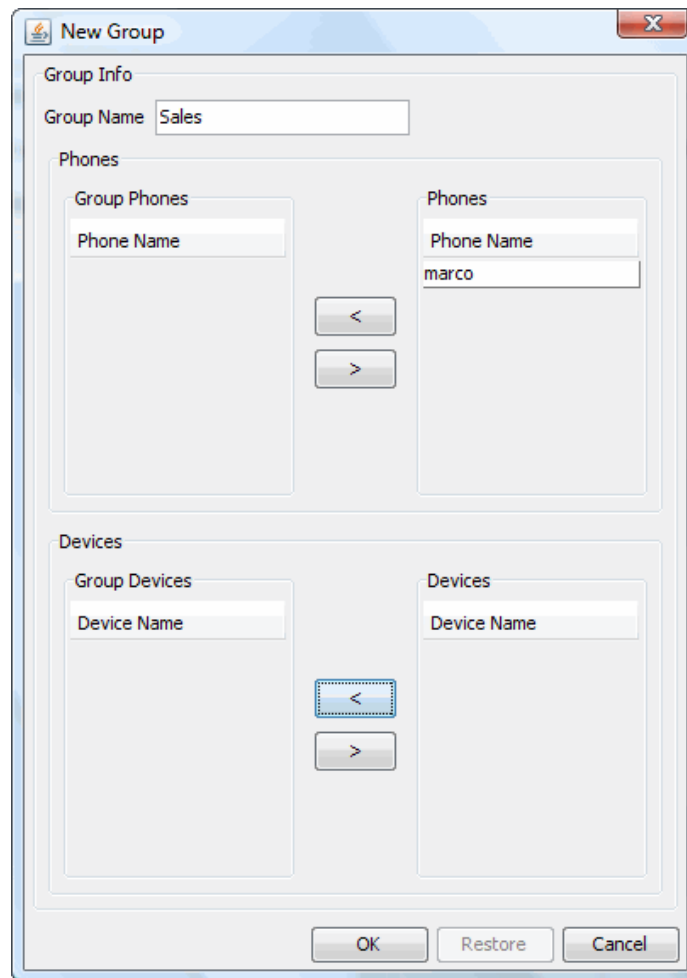
Note2: The outbound pattern may differ from the inbound, if you wish to automatically add prefixes. For example, when you dial a mobile number, you may wish to use a particular provider for the calls. To use this provider a prefix of 1010 needs to be added, thus your inbound pattern would be 9*, whilst your outbound pattern would be 10109*

Note3: If you have internal extensions which start with a 9 and you wish to ring a mobile number, which also starts with a 9, how does the edgeBOX know where to send the call, without the functionality of an external call prefix (as existed previously)?

edgeBOX uses the most specific to least specific method to make the call, with internal extensions considered to be the most specific. In this simple example:

Internal extension (eg 9771)	Checks this possibility first
Mobile call (eg 9*)	This has next highest priority to check
Other call (eg 65544881)	Falls to the default call path (*)

Holding down the Cntl key and selecting entries allows you to select several entries.



6.3.2.2 Edit Access Group

Allows you to add or remove items from the Group. Cntl and select allows you to select several entries.

6.3.2.3 Delete Access Group

Allows you to delete a group. The phones/devices are not deleted.

6.3.3 SIP Proxies

SIP Proxies allow the edgeBOX to connect to a SIP Proxy or to another edgeBOX PBX. Allowing public extensions to be dialed as if they were on the edgeBOX itself.

SIP Proxies can be configured via:

- Add Proxy
- Edit Proxy
- Delete Proxy

Selecting Add provides the following options: [Basic](#), [Authentication](#), and [Codecs](#)

Proxy Name	Host	Trusted Proxy	Authentication	Nat	State

6.3.3.1 Basic

- Proxy Name: Text to identify Proxy
- Host: IP address or hostname of Proxy
- Max Calls: Maximum number of simultaneous calls allowed
- CallerID: Telephone number which is sent to the receiver (useful if you have more than one number for a line)
- DTMF Mode: Options are: inband, info and rfc2833
- Trusted Proxy: If checked, the incoming call is considered as an internal call.
If unchecked, the call executes the ivr (as it is considered as an external call)
- Keep Alive: Attempts to keep the connection active

New Proxy

Basic | Authentication | NAT | Codecs

Proxy Configuration

Proxy Name:

Host:

Max Calls:

CallerID: ☐

DTMF:

☐ Trusted Proxy

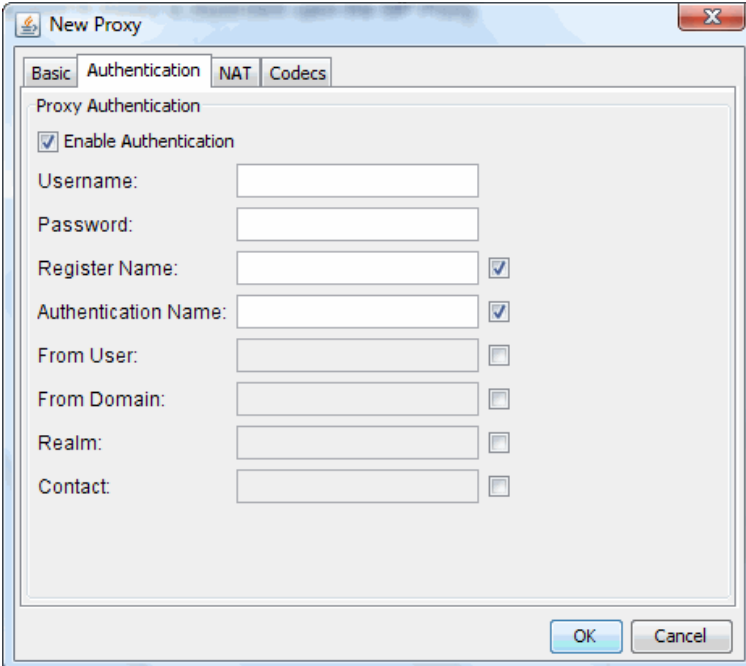
☐ Keep Alive

OK Cancel

6.3.3.2 Authentication

Authenticates against the provider's server address.

The information you need to supply is dependant upon the SIP Proxy.



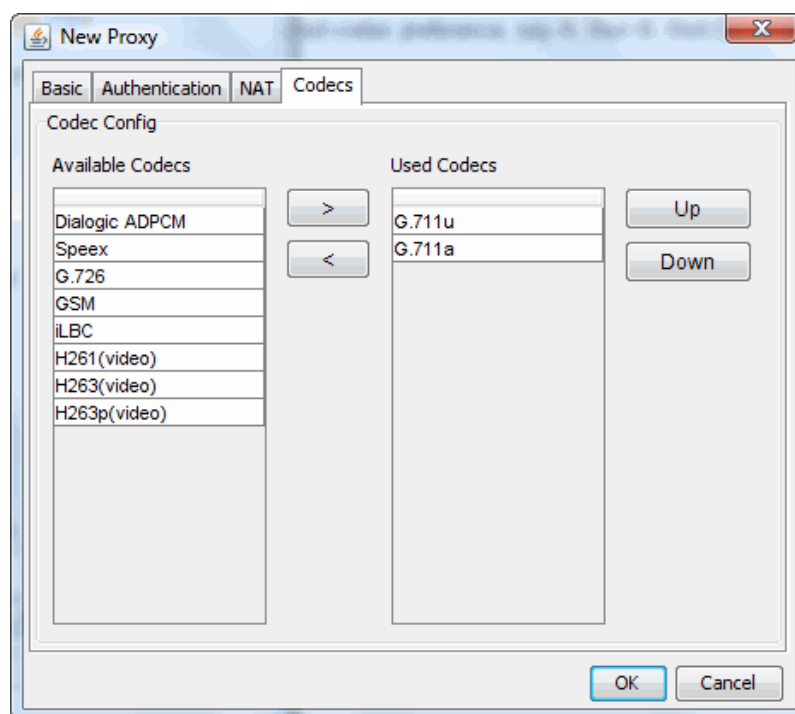
The screenshot shows a 'New Proxy' dialog box with four tabs: 'Basic', 'Authentication', 'NAT', and 'Codecs'. The 'Authentication' tab is selected. It contains a 'Proxy Authentication' section with the following fields and checkboxes:

- ☒ Enable Authentication
- Username:
- Password:
- Register Name: ☒
- Authentication Name: ☒
- From User: ☐
- From Domain: ☐
- Realm: ☐
- Contact: ☐

At the bottom right are 'OK' and 'Cancel' buttons.

6.3.3.3 Codecs

Select the codecs to be used (these codecs have to be supported by the provider). You can also select the preferred order of the Codecs. Thus if you have a preferred codec preference, say A, then B, then C and the other side has B, then A, A will be tried first, but as there is no match, B will be tried, there is a match, so this is chosen.

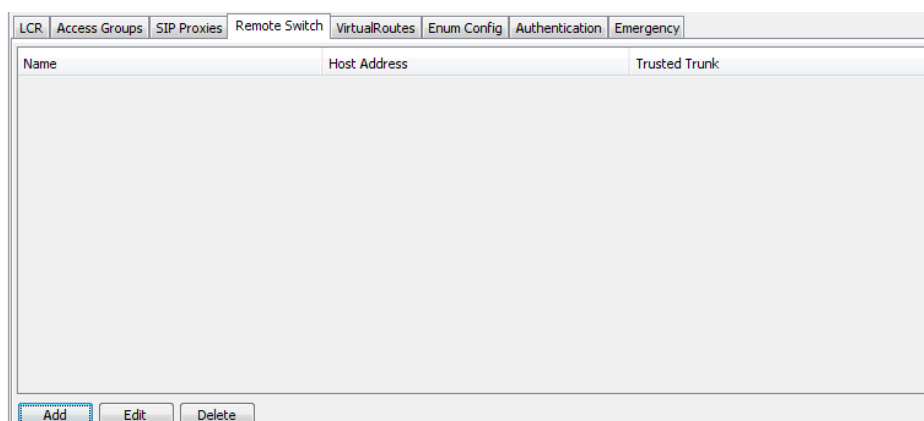


6.3.4 Remote Switch

The Remote Switching functionality allows the creation of an IAX trunk between two edgeBOXs. Calls between these devices benefit from an optimised connection, resulting in a better use in bandwidth.

You can check the remote switches configured in the system which are displayed in tabular form. Options available are:

- [Add](#): Add a remote switch configuration,
- Edit: Modify an existing remote switch configuration and
- Delete: Remove a remote switch configuration.



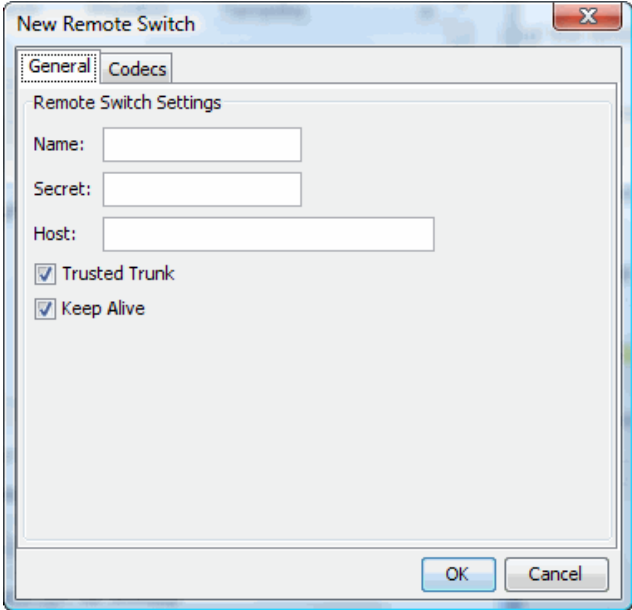
A benefit of this configuration is that an extension from edgeBOX A is able to call an extension registered in edgeBOX B, as if the phone was registered on edgeBOX A.

Note that besides calling internal extensions, all VoIP functionalities will be available for the remote edgeBOX users (making local calls, making call conferences, etc.), allowing you to make a conference call between two remote offices with no costs.

6.3.4.1 Add

Allows you to add a new remote switch configuration. You must supply the following data:

- **Name:** connection name. This name must be the same on both edgeBOX's which 'make up' the remote switch.
- **Secret:** password used to register with the remote edgeBOX. This secret must be the same on both edgeBOX's which 'make up' the remote switch
- **Host:** remote edgeBOX address;
- **Trusted Trunk:** Allows the PBX to receive incoming calls from the Remote PBX
- **Keep Alive:** Sends a keep alive to the remote PBX
- **Codecs:** Codecs to be used during calls between the two edgeBOXs (local and remote) and the preferred order of the Codecs



6.3.4.2 Edit

Highlighting the Remote Switch entry and pressing Edit allows the reconfiguration of an existing entry.

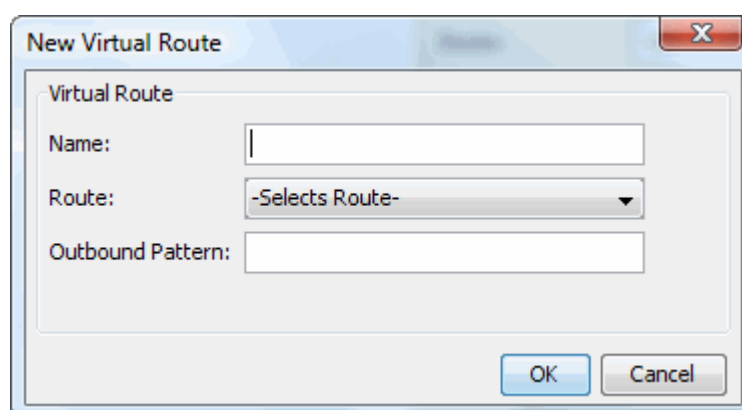
6.3.4.3 Delete

Highlighting the Remote Switch entry and pressing Delete allows the deletion of an existing entry.

6.3.5 Virtual Routes

Allow the creation, deletion and editing of a virtual route.

- Name: Any text you wish to enter
- Route: The route through which you will make the call.
- Outbound Pattern: The 'prefix' which will use this route



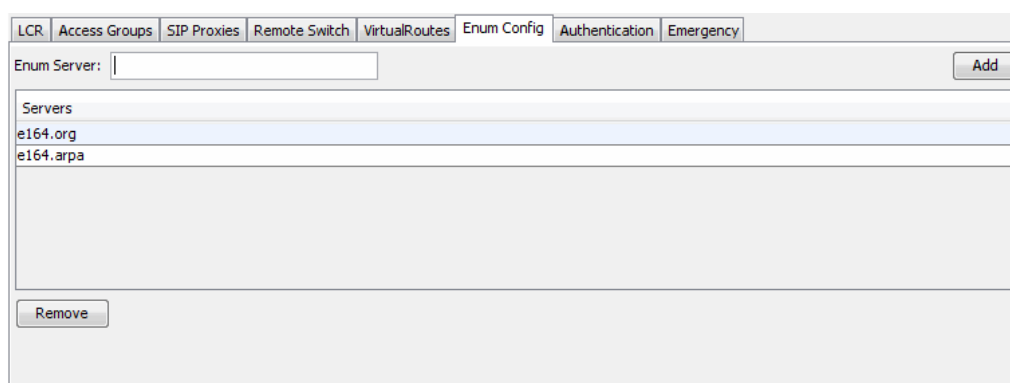
The image shows a 'New Virtual Route' dialog box. It has a title bar with a close button (X). Inside, there's a section titled 'Virtual Route' containing three fields: 'Name' (a text input field), 'Route' (a dropdown menu currently showing '-Selects Route-'), and 'Outbound Pattern' (a text input field). At the bottom right, there are 'OK' and 'Cancel' buttons.

6.3.6 Enum Config

edgeBOX supports Enum, which is a service mapping PSTN telephone numbers into VoIP URLs.

If you activate Enum, edgeBOX will send a query to each active server to try to lookup the called PSTN number.

If a matching answer is received the call will use the VoIP URL returned and so transparently divert to the Internet, having no cost. Otherwise, the call will follow the route configured in the [LCR](#).



The image shows the 'Enum Config' window within a software interface. It has a tabbed header with 'LCR', 'Access Groups', 'SIP Proxies', 'Remote Switch', 'VirtualRoutes', 'Enum Config' (selected), 'Authentication', and 'Emergency'. Below the header, there's an 'Enum Server:' label followed by a text input field and an 'Add' button. A list box titled 'Servers' contains two entries: 'e164.org' and 'e164.arpa'. At the bottom left, there is a 'Remove' button.

6.3.7 Authentication

edgeBOX supports authentication for outbound calls. Options are Off or On.

Authentication is based on a PIN number, which is assigned on user creation (see [Access Profiles](#)).

Outbound call permissions, i.e. the type of outbound calls a user is allowed to make, are also set on user creation.

This panel allows you to activate VoIP authentication. The system will block outbound calls if the user supplied invalid credentials or if the user doesn't have the necessary permissions to make the call.

If authentication is not active, the system will still check the type of each call, but just to find the best [LCR](#) to use. In this mode of operation users are not required to supply a PIN when making calls.

6.3.8 Emergency

Allows you to define the emergency services telephone number and the route to use for this number. This allows any phone (as long as there is an appropriate route) to dial this number, without a PIN.

Phones Inbound Calls Outbound Calls PBX Features Hardware Tools and Services

LCR Access Groups SIP Proxies Remote Switch VirtualRoutes Enum Config Authentication Emergency

Emergency Number

Number: 112

Route: -Selects Route-

- Selects Route-
- remote
- ANALOG-Zaptel/56
- ANALOG-Zaptel/57
- ANALOG-Zaptel/58
- ANALOG-Zaptel/59
- BRI-mISDN/1
- BRI-mISDN/2

6.4 PBX Features

This section describes edgeBOX's IP PBX advanced features. All these features can be used in the [IVR editor](#), making them available to calls coming from the external network. The following features will be described:

- [Queues](#)
- [Agents](#)
- [Conferences](#)
- [Parking](#)
- [HuntGroup](#)
- [Voicemail](#)
- [Fax Service](#)

A summary of the default edgeBOX PBX features is presented in the following table:

Action	Dial
Prefix to Hangup	*0
Prefix for Blind Transfer	#1 + Extension Number
Prefix for Supervised Transfer	*2 + Extension Number
Call Parking	#1 + 700

6.4.1 Queues

This panel allows you to manage edgeBOX's queuing system. These services are widely used, especially in Call Centers, where callers are usually placed in a queue before an operator answers the call.

Configured queues are shown in a tabular manner. You can [create new queues](#) using the Add Queue button, modify the details of existing queues (Edit Queue button) or remove a queue by selecting the queue and clicking Delete Queue.

Queue Name	Extension Nr	Queue Priority	Max Callers
------------	--------------	----------------	-------------

[Add Queue](#) [Edit Queue](#) [Delete Queue](#)

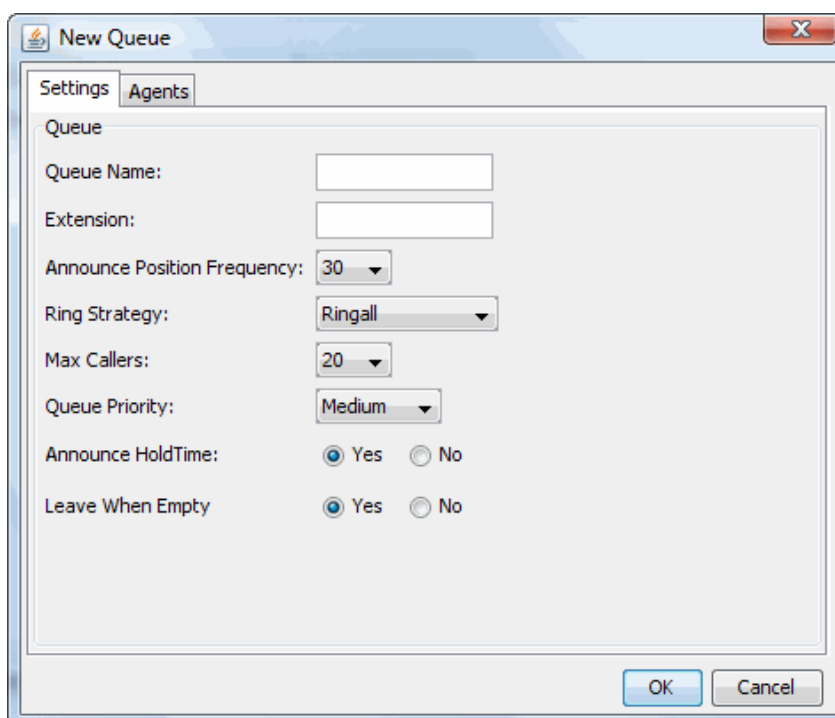
6.4.1.1 Add Queue

Allows you to create a new queue.

Settings

General queue settings are configured selecting the "settings" tab page. Available options are:

- Queue Name: name assigned to this queue;
- Extension: internal extension associated with this queue;
- Announce Position Frequency: time interval (in seconds) between queue position announcements;
- Ring Strategy: algorithm used to assign calls to agents:
 - RingAll: all agent phones will ring, and the call will be assigned to the one that answers first;
 - RoundRobin: selects each agent in turn;
 - LeastRecent: selects the agent which was least recently selected;
 - FewestCalls: selects the agent with least calls answered;
 - Random: selects an agent randomly;
 - RR with Memory: RoundRobin with memory, remembers which agent answered last and selects the next one.
- Max Callers: maximum number of calls that can be placed on this queue;
- Queue Priority: queue's relative priority to other queues configured;
- Announce Hold Time: set to Yes if you want queue position to be announced, set to No otherwise;
- Leave When Empty: set to Yes if you want calls queued to be terminated if there are no agents assigned to the queue.



The 'New Queue' dialog box is shown with the 'Settings' tab selected. It contains the following fields and options:

- Queue Name: [Text input field]
- Extension: [Text input field]
- Announce Position Frequency: 30 [Dropdown menu]
- Ring Strategy: Ringall [Dropdown menu]
- Max Callers: 20 [Dropdown menu]
- Queue Priority: Medium [Dropdown menu]
- Announce HoldTime: ☒ Yes ☐ No
- Leave When Empty: ☒ Yes ☐ No

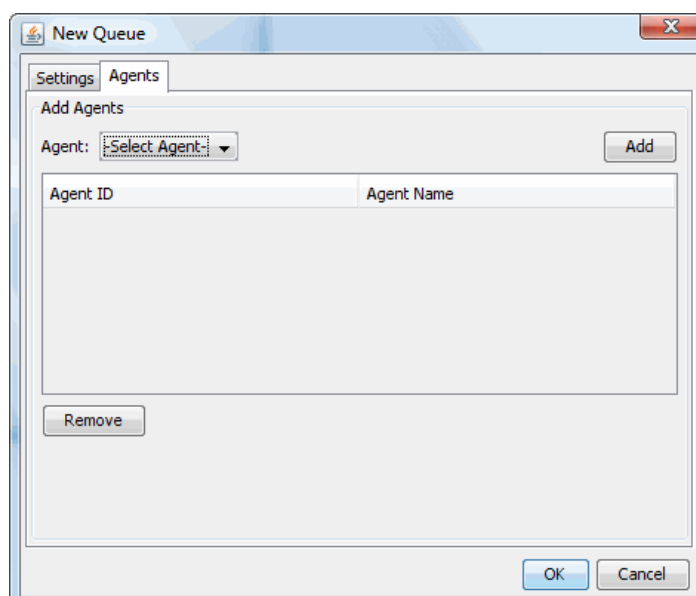
At the bottom right are 'OK' and 'Cancel' buttons.

Agents

For a queue to work correctly agents must be assigned to it, since queued calls are answered by agents.

To associate an agent with a queue select the "Agents" tab page. The agents assigned to this queue are displayed in a tabular manner.

To associate an agent with a queue select the desired agent in the agents' list, and then press the "Add" button. To remove an existing association, select it on the table and press "Remove". Note that to have an agent available on the agents' list it must have been previously created using the [Agents panel](#).



The 'New Queue' dialog box is shown with the 'Agents' tab selected. It contains the following elements:

- Add Agents section with an 'Agent: Select Agent-' dropdown menu and an 'Add' button.
- A table with two columns: 'Agent ID' and 'Agent Name'.
- A 'Remove' button below the table.

At the bottom right are 'OK' and 'Cancel' buttons.

6.4.2 Agents

This panel allows you to manage agents. Agents are persons that answer the calls send to Queues. [How do agents login and answer calls?](#)

Agents login and logout to indicate when they are ready to receive calls from queues, so that they don't receive calls at all times.

Depending on how you have the Callback Login settings configured, **agents can login and answer calls in two ways:**

- If **Callback Login is enabled**, an agent to login has to dial the Callback Login Extension. Then he can place his phone on hook and wait for calls. When a call from a queue is assigned to him, edgeBOX calls him back. To logout, the agent has to make call to the Callback Login Extension again.
- If **Callback Login is disabled**, an agent to login has to dial his Agent Login Extension. Then he must always have his phone off hook to wait for and receive calls that are assigned to him. To logout the agent has just to place the phone on hook. He will be logged out automatically.

▼ Create an agent

To create a new agent:

1. Click **Add Agent** bellow the Agents list. A dialog window will appear.
2. Indicate the number that identifies this agent in the Agent ID field.
3. In the Agent Name type a suggestive name for the agent.
4. Create a login for the agent by indicating a PIN number and an extension number (the extension must be unique, it cannot be in use by a phone or a conference, for example). The agent will use this login (Extension + PIN) to authenticate when he wants to receive calls from the queues.
5. Click the OK button to save the information into the list of agents and then the Apply button to save the new agent.

▼ **Edit the properties of an agent**

1. Select the desired agent from the Agents list and click the Edit Agent button.
2. In the agent properties window make the desired changes.
3. Click the OK button to save the information into the list of agents and then the Apply button to save the modifications made.

▼ **Delete an agent**

1. Select the agent you want to delete from the Agents list and click the Delete Agent button to delete the agent from the list.
2. Click the Apply to effectively delete the agent from edgeBOX.


Options

Configure general properties of the agents and the way they login and answer calls from queues.

▼ **Allow agents to put the phone on hook after logging in (Callback mode)**

To allow agents to put their phones on hook after they logged as agents, you have to select the option Enable of the Callback Login group. This way when a call from a queue is assigned to an agent, edgeBOX will callback the agent to transfer him the call.

When you enable this option you have to indicate an unique extension in the Callback Login Extension field. This extension will be the common extension that all agents will dial when they want to login and receive calls and when them want to logout.

 If you don't have this option enabled, agents must always keep their phones off hook to receive calls from queues. If they place the phone on hook they will not receive calls even tough they logged in.

▼ **Force agents to press # to answer incoming calls**

You can force the agents to press # to answer incoming calls from the queues by selecting Yes in the Require ACK option.

If you select No then when a call is assigned to an agent, the agent doesn't need to do anything, the call is answered automatically.

▼ **Change the time agents have to answer the calls that are assigned to them**

To change this time select the desired value (in seconds) from the Auto Logoff Time drop down option.

If this time is reached edgeBOX will send the call to the next agent, according to the attribution algorithm used in the queue.

6.4.3 Conferences

edgeBOX supports two types of conferences:

- Dynamic conferences (created by the users)
- Static conferences (created by the edgeBOX administrator).

Dynamic Conferences

Any registered user may dial the pre-defined extension and create a conference by pressing a number.

- To activate dynamic conferences, check Users can Create Conferences and supply an extension for this purpose (by default, it is 9000).
- To join this conference, users just have to dial the pre-defined dynamic conferences' extension (9000 in the example) and enter the conference number.

Static Conferences

Static conferences have to be created beforehand by the administrator. The list of static conferences configured is displayed in the panel below.

You may [create a new static conference](#), modify a static conference's details or remove the static conferences.

edgeBOX comes with an example static conference configured that you can use. The conference Number is 9010, the Moderator Pin is 9911 and the Participant Pin is 9910.

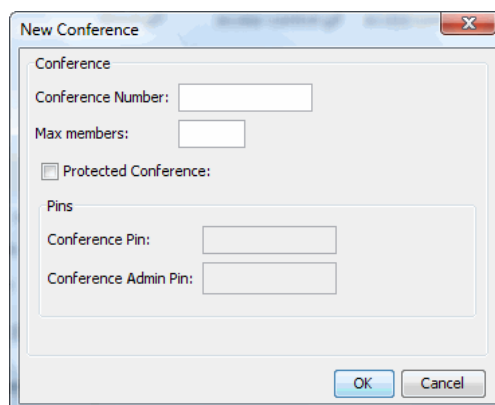
Conference Number	Public Conference
9010	No

6.4.3.1 Add Room

Allows you to create a new static conference. The following elements must be supplied:

- Conference Number: internal extension assigned to this conference;
- Max Members: Max number of members in the conference
- Protected Conference: If you enable this option, you will need to supply a conference PIN and an administrator PIN. Users will then have to enter the correct PIN to join this conference.

All configured static conferences can be used when you use the [IVR editor](#) to add a [MeetMe action](#).




6.4.4 Prefixes

Prefix to Hangup - Terminate the call.


Prefix for Blind Transfer - Transfer a call to another phone. [How to do it?](#)

1. When you are answering a call, inform the caller that you are going to transfer the call.
2. Dial the prefix for a blind transfer and the telephone number you wish to transfer the incoming call to. Example: #12001 to forward the call to extension 2001.
3. The caller is immediately connected to the number you transferred the call to.
4. You will hear the busy line tone, which means the transfer is complete and you can hang up.

 If you make a mistake when dialling the number you're transferring the caller to, you and the caller will be disconnected from the original call. Also, you cannot check to see if the number you are transferring the call is busy or offline, for example, before making the transfer. To do that use a Supervised Transfer instead.

Prefix for Supervised Transfer - Transfer a call to another phone by putting the call on hold and allowing you to call the phone your are transmitting the call to see if it allows the transfer. It is also know as "Attended Call Transfer". [How to do it?](#)

1. When you are answering a call, inform the caller that you are going to transfer the call.
2. Dial the prefix for a supervised transfer. The caller will no longer be able to hear you.
3. Dial the number of the phone number you wish to transfer the incoming call to. After the person answers, ask if you can transfer the call.
4. If the person says yes, hang up your phone and the call that is on hold will be transferred to the recipient. If the person says no wait until he/her hangs up. The call on hold will be transferred back to you and you can inform the person holding that it is not possible to transfer the call.

 If the person, to whom you are transferring the call to, doesn't answer the call in about

15 seconds, the call is transferred back to you. This also happens if that person answers the call but hangs up the phone before you (the supervisor) do.

Prefix for Pickup calls - Pick up a call from another phone that is ringing to your phone. [How to do it?](#)

To pick a call dial the Pick Up prefix plus the extension of the phone that is ringing. For example: *82001 if phone 2001 is ringing.

Number to Dial for Parking - Number to dial to place a call you are answering on hold. The caller will stop hearing you while the call is on hold. [How to do it?](#)

1. When you are answering a call, inform the caller that you are going to put him on hold.
2. Dial #1 plus the prefix configured for parking (number in the Number to Dial field). A sound message will inform you of the extension the call was parked into. For example 701.
3. The call is placed on parking. You can put down your phone and pick up the call from another internal phone later on by dialing 701 on the desired phone.

Parking Available Lines - Number of extensions available to assign for parked calls.

Parking Max Time - Maximum amount of time a call can remain on hold in parking. After that time the call will be shut down.



To park or transfer calls, the internal extension's [Can Reinvite](#) property must be switched off.

Other Prefixes

Follow Me - Allows you to forward calls that arrive at your internal extension to another extension or phone where you are at the moment. You can't do this operation in edgeBOX's interface, only in the network phones. [How to do it?](#)

To enable Follow Me:

- If you are close to your extension - Dial *14* plus the phone number or the extension number you want your calls to be forward to. For example, if you have a meeting on a meeting room, and there is a phone there (extension 4002), that you can pick up your extension and dial *14*4002, and all calls that arrive at your extension will be forward to the meeting room phone. Or you can indicate your personal cell phone number instead (*14*912154103), for example, this way all calls that arrive at your extension will be forward to your cell phone.
- If you are close to the extension you want to forward calls to - Dial *12* plus your extension number. For example, if you are on a meeting room and you want to forward calls that arrive at your extension (ext: 2013) to the phone that is on the meeting room, pick up the meeting room phone and dial *12*2013. All calls that arrive at your extension will be forward to the meeting room phone.

6.4.5.1 Add HuntGroup

This option allows you to create a new huntgroup. You will need to supply the following information:

- Name: the name for this huntgroup and
- Phones: the phones associated with the huntgroup. After selecting the desired extension press the "Add" button to add the phone to the huntgroup.

When configuring the [IVR](#) system, remember that all huntgroups configured may be used in the action "HuntGroup".

Phone Name	Phone Extension
marco	2001

6.4.6 Voicemail

In the voicemail configuration panel you can define some of its functional parameters. In general settings you can define:

- Voicemail Extension: Extension number where you can access the voicemail system and hear your messages.
- Max Messages: Maximum number of messages that a user can have in his/her mailbox.
- Max Length: Max length of message
- Min Length: Min length of message

You can also define parameters to the notification messages, ie messages edgeBOX sends when a user receives a new voicemail message:

- From Email: Origin e-mail address of notification messages.

- From String: Name of the entity originating notification messages.
- Attach: When active, the voicemail message is attached to the notification message in audio format.
- Message Language: Language used in notification messages. There are two available options: English and Portuguese.
- Signature: signature of the notification messages.

The screenshot shows a web-based configuration interface with a tabbed menu at the top. The tabs are: Queues, Agents, Conferences, Prefixes, HuntGroup, Voicemail (selected), and Fax Service. The main content area is divided into two sections: 'Voicemail Settings' and 'Notification Settings'. In the 'Voicemail Settings' section, there are four fields: 'Voicemail Extension' with the value '9999', 'Max Messages' with a dropdown set to '100', 'Max Length' with a dropdown set to '3' and the unit 'mins', and 'Min Length' with a dropdown set to '3' and the unit 'secs'. The 'Notification Settings' section contains five fields: 'From Email' with the value 'edgeBOX@enterprise.com', 'From String' with the value 'edgeBOX', 'Attach' with a dropdown set to 'Yes', 'Message Language' with a dropdown set to 'English', and 'Signature' with the value 'edgeBOX'.

Queues	Agents	Conferences	Prefixes	HuntGroup	Voicemail	Fax Service
Voicemail Settings						
Voicemail Extension: 9999						
Max Messages: 100						
Max Length: 3 mins						
Min Length: 3 secs						
Notification Settings						
From Email: edgeBOX@enterprise.com						
From String: edgeBOX						
Attach: Yes						
Message Language: English						
Signature: edgeBOX						

6.4.7 Fax Service

Send faxes (via a software modem) from a fax machine to edgeBOX's fax gateway. This fax is then converted to an email and sent to the fax mail account.

You may also send a fax via email. The email will be converted to fax format and sent to the remote fax machine.

Queues	Agents	Conferences	Prefixes	HuntGroup	Voicemail	Fax Service
--------	--------	-------------	----------	-----------	-----------	-------------

Notification Settings
Email Language: English
File Type: .pdf (PDF)

Account Name	DDI	Authentication Type	Email
fax_account	239920001	Local + Password	j.parker@gmail.com

New Edit Remove

▼ Create a new fax account

1. Go to the **Fax Service** sub tab of the **PBX Features** tab in the VoIP section.
2. Click the New button below the Fax Accounts list. A dialog window will appear.
3. Type the name of the email address that will be used by the network users to send emails that will be converted to faxes in the **Fax Server Account** field. For example, if you type fax_account and the domain on edgeBOX is example.com, then the fax server account will be fax_account@example.com.
4. In the **Receive Email** field indicate the email account of the person of your company that will receive all incoming faxes. Incoming faxes are converted by edgeBOX to emails and then delivered at this email address. You can, for example, fill this field with the email account of your company's receptionist.
5. In the **DDI** type your fax number. This is, the number people use when they sent faxes to your company.
6. Indicate the information you want to display in the top of the faxes edgeBOX sends: Type your company or organization name in the Company Name field and your fax number in the fax number field. Generally this fax number is the same number you typed in the DDI field.

New Fax Service

New Account

FAX Server Account:

Receive Email:

DDI:

Fax Number:

Company Name:

Number Retries:

Authorization

Type:

Password:

OK Cancel

7. Change the number of times edgeBOX tries to send a fax when the number it is trying to fax is busy in the **Number Retries** drop down option. By default edgeBOX retries to send a fax three times.
8. In the **Authorization Type**, indicate from which email accounts users can send the emails and if they are required to indicate a password.
 - Local means the network users can only send emails from the [Webmail](#) or from the edgeBOX local SMTP server. For instance, if they have their edgeBOX email account configured on Outlook and they send a fax through it, the fax will be accepted, but if they send the fax through a Gmail or Hotmail account or through an email account of another edgeBOX, for example, the fax will not be accepted.
 - Password means the users can send emails from any email account, however they have to specify a password on the body of the email to authenticate.
 - Local + Password means that the users have to use the Webmail or the SMTP server of edgeBOX to send the emails and they also have to specify a password in the body of the email to authenticate.
9. Click OK to save the new fax account to the list. Then click the Apply button in the bottom right side of the application to save permanently the new account.

▼ Change the properties of a fax account

To change one or more properties of a fax account, as the email where converted faxes are received:

1. Go to the **Fax Service** sub tab of the **PBX Features** tab in the VoIP section.
2. Select the desired fax account from the list and click the Edit button below the list.
3. Change the the desired properties and click OK to save the changes to the list. Then click Apply to permanently save the changed you made.

4. Click OK to save the the changes you made.

▼ [Delete a fax account](#)

1. Go to the **Fax Service** sub tab of the **PBX Features** tab in the VoIP section.
2. Select the fax account you want to delete in the list.
3. Click the Delete button below the list to delete the account from the list and then click the Apply button in the bottom of the panel to confirm the deletion.

▼ [Change the type of the attachments or the language of the emails](#)

By default, edgeBOX converts the received faxes to pdf files and sends them as email attachments to the fax reception email account you specified. Also, by default, edgeBOX sends all the faxes it receives as emails to the email account you specified in English language.

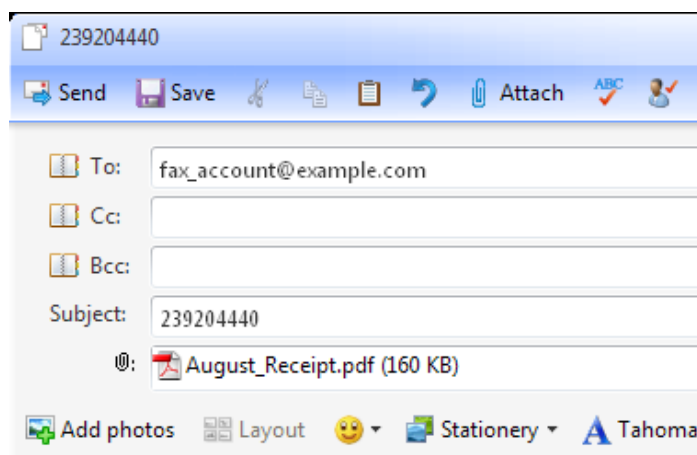
You can change the format the attachments and the language of the emails sent by edgeBOX. To change any of these settings:

1. Go to the **Fax Service** sub tab of the **PBX Features** tab in the VoIP section.
2. In the top left side of the panel change the language of the attachments' format to your desired settings.
3. Click the Apply button to save the changes.

▼ [How to send the faxes using emails?](#)

Imagine you wanted to send a receipt you just made to a client of yours:

1. Open an email client as Thunderbird or Outlook or edgeBOX's Webmail and create a new email.
2. Enter the email address of your edgeBOX fax account in the **To** field.
3. In the **Subject** type the fax number of your client.



PASSWORD: passwOrdforf@x|

4. **Convert** the document you want to send **to PDF or TIFF format** and **add it** to the email as an **attachment**. Note that the document cannot have more than 25 pages.
5. If authentication is required, type PASSWORD: plus the fax account password in the first line of the body of the message.
6. Send the email.

After edgeBOX receives this email in the fax email account, it will convert the file in attach into a fax and try to send it to the phone number you indicated in the Subject of the email.

A little while after, **you will receive an email** from edgeBOX **indicating if edgeBOX was able to deliver the fax** to the recipient **or if it couldn't deliver it** because of some error or because of the receiver fax being busy.

6.5 Hardware

edgeBOX supports automatic hardware detection. All **supported** (see hardware certified list on the Partner Site) VoIP cards are detected and the system is automatically configured so these cards can be used by the IP PBX.

Only information related to the card currently installed in the system will be displayed in this panel. The supported VoIP cards are:

- [ISDN BRI](#)
- [ISDN PRI](#)
- [Analog](#).

6.5.1 ISDN BRI

edgeBOX supports BRI VoIP cards.

It is possible to configure global settings such as the country national prefix as well as the prefix used to make international calls. Another option available for configuration is the call volume which may vary between an 8db gain or loss. This value should be adjusted depending on the network.

All ports detected will be displayed on the table where its operation mode can be checked. Ports are initialised in TE operation mode by default.

There are two port operation modes possible:

- TE mode: ports should be connected to ISDN lines.
- NT mode: ports should be connected to ISDN phones.

You may [change](#) the port working mode. To do so, select the desired port and press the "Edit Port" button. You may also double click the desired port.

The screenshot shows the EdgeBOX configuration interface. At the top, there are tabs: Phones, Inbound Calls, Outbound Calls, PBX Features, Hardware, and Tools and Services. The 'Hardware' tab is selected, and within it, the 'ISDN BRI' sub-tab is active. Below the sub-tabs, there are fields for 'ISDN Settings': 'National Prefix' (0), 'International Prefix' (00351), and 'Volume' (a dropdown menu). Below these fields is a table titled 'ISDN Ports' with the following data:

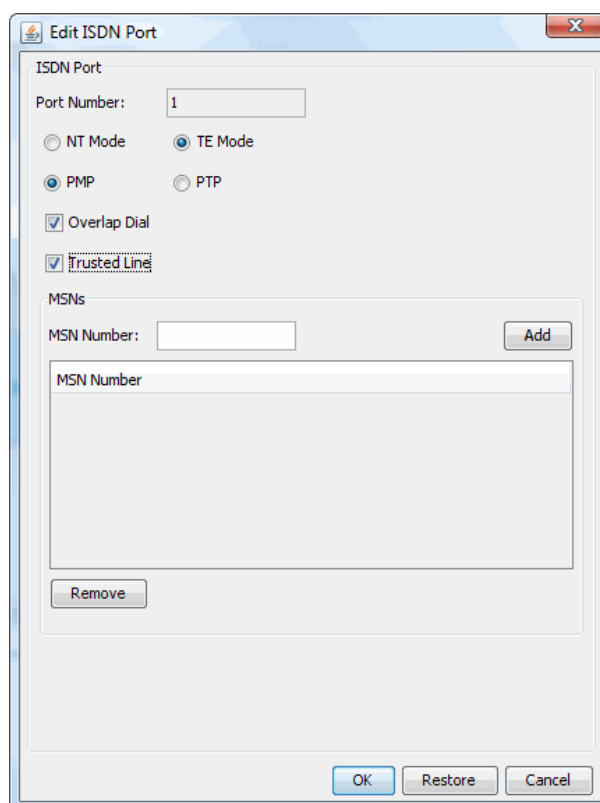
Port Number	Module	Port Mode	Port Type	Link
4	miSDN	nt	pmp	Down
3	miSDN	nt	pmp	Down
2	miSDN	te	pmp	Down
1	miSDN	te	pmp	Down

At the bottom left of the interface, there is an 'Edit Port' button.

6.5.1.1 Edit Port

When editing a BRI port, you can configure the port operation mode:

- Select **NT** if you want to connect an **ISDN phone** to the port.
- Select **TE** if you want to connect an **ISDN line** to the port.




If you select the TE mode (line) you also need to indicate:

- **Connection Type** - Point to Multi-Point (PMP) or Point to Point (PTP). PTP links allow only one TE to be connected. PMP links allow to connect up to 8 terminals in parallel along the bus.
- **Overlap Dial** - Select the option if you want to wait for all incoming digits before fallback to dial plan. It allows edgeBOX to integrate with PBX's which work with overlap digits.
- **Trusted Line** - Select the option if you want inbound and outbound calls through this line to be considered as internal calls by edgeBOX. This means that the inbound call rules and outbound call rules will not be applied to these calls.
- **MSN Numbers** - The MSN numbers are your public phone numbers. You can use the MSN numbers to restrict the inbound calls you accept on this ISDN line.
 - If you don't insert any MSN number, all calls that come in through this line are accepted and go to the inbound call rules.
 - If you insert one or more of your public numbers, then only the calls that arrive through this line to those specific numbers are accepted, any other calls are rejected by edgeBOX.

Ports in NT mode are available as phones when you edit the [IVR](#) and also in the [internal extensions](#) management.

Ports in TE are available as outbound routes when you edit the [LCR](#).

 When you change the port operation mode, edgeBOX's PBX will be reinitialized and all ongoing calls will be hung up.

6.5.2 ISDN PRI

One of the types of VoIP cards supported by edgeBOX is PRI Digium cards. These cards may have one, two or four spans. All spans detected will be displayed in a tabular manner, where you can also check some other span settings:

- Span Number: port number;
- Module: The Module which has been loaded for the card.
- Span Mode: port working mode (Available values are T1 or E1. This mode can be configured using a card jumper);
- Span Ports: number of ports associated with the span. (31 ports in E1 mode, 22 ports in T1 mode);
- Link: Indicates if the device driver considers the hardware to be available.
- Trusted Span: Show the trusted status of the span

Some of the span properties can be [changed](#). To do so, select the desired span and press the "Edit Span" button. You may also double click the desired span.

ISDN BRI
ISDN PRI
Analog
Echo Cancellation

PRI Spans Configuration

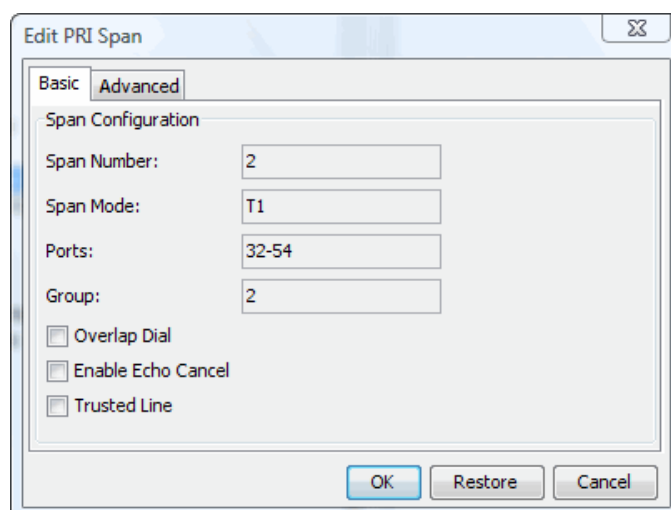
Span Number	Vendor	Model	Module	Span Mode	Span Ports	Link	Trusted Span
4	Sangoma	A101	Zaptel	E1	80-94,96-110	Down	No
2	Digium	TE205	Zaptel	T1	32-54	Down	No
1	Digium	TE205	Zaptel	E1	1-15,17-31	Down	No

Edit Span

6.5.2.1 Edit Span

The following settings may be changed:

- **SwitchType:** switching used by the line. Available options are:
 - EuroISDN, used in Europe;
 - National used in the USA.
 - qsig
 - dms100
 - 4ess
 - 5ess
- **Signalling:** signalling used by this span. Available options are:
 - PRI_CPE used on the client side;
 - PRI_NET used on the network side.
 - E&M
- **Timing, Framing and Coding:** Allows the admin to enter appropriate information supplied by their Telco or PBX supplier
- **Group:** group to which this span is associated to.
- **Overlap Dial:** On each PRI span it's now possible to enable/disable overlap dial. This option forces edgeBOX to wait for all incoming digits before fallback to dialplan.
- **Trusted Span:** Sets the span to be trusted, thus calls on this span are considered as internal calls



Edit PRI Span

Basic Advanced

Advanced Configuration

SwitchType: National

Signalling: CPE

Timing Clock Source: Slave

Framing: ESF

Coding: B8ZS

OK Restore Cancel

Edit PRI Span

Basic Advanced

Span Configuration

Span Number: 1

Span Mode: E1

Ports: 1-15,17-31

Group: 1

☐ Overlap Dial

☐ Enable Echo Cancel

☐ Trusted Line

OK Restore Cancel

Edit PRI Span

Basic Advanced

Advanced Configuration

SwitchType: EuroISDN

Signalling: CPE

Timing Clock Source: Slave

Framing: CCS

Coding: HDB3

☒ Enable CRC4

OK Restore Cancel

6.5.3 Analogue FXO-FXS

To allow connection to analogue lines, edgeBOX supports TDM Digium cards. FXO and FXS modules may be installed in this card:

- FXO Module: should be connected to an analogue line, allowing you to receive or make calls using the PSTN network;
- FXS Module: should be connected to an analogue phone.

⚠ Be careful not to connect phones lines (PSTN lines) in the FXS port. If you do so, the port will stop working.

Even if you unplug the phone line cable and connect an analog phone into the port, the port will still not work; you will have to reboot edgeBOX.

In these type of cards the only global configurable parameter is the Load Zone, where the country initials may be selected, so the dialtone used will be appropriate.

All ports detected as FXS will be available when [editing the IVR](#) and in the [internal extensions](#) management system. All ports detected as FXO will be available as outbound routes in the [LCR](#) management system.

The screenshot shows the 'Analogue' configuration tab in the edgeBOX interface. Under the 'Zone' dropdown, 'pt' is selected. Below, the 'Analogue Ports' section contains a table with the following data:

Port Number	Vendor	Model	Module	Port Type
59	Sangoma	A200	Zaptel	PSTN (FXO)
58	Sangoma	A200	Zaptel	PSTN (FXO)
57	Sangoma	A200	Zaptel	PSTN (FXO)
56	Sangoma	A200	Zaptel	PSTN (FXO)

An 'Edit Port' button is located at the bottom left of the configuration area.

6.5.3.1 Edit Port

Here you can configure several FXO or FXS port options. The FXS options are the same available when you configure an Analog phone.

Port Number - The number of the port in the TDM card.

Port type - FXS or FXO.

DID - A phone number for this line. Allows for DID routing for Analog lines.

Wait for Dial Tone - Configure the time to wait for a dial tone on the phone line (FXO port type).

For some phone lines, the system may need to wait a few seconds before dialing out. This will give the dial tone time to normalize.

Symptoms of these timing problems are associated with erratic dialing as the phone system will miss the first few dialed numbers.

The default is disabled. You can configure 1,2,3,5 and 10 seconds.

Trusted Line - This option is useful for scenarios with legacy PBXs.

Caller ID Number - A number to identify this outbound line.

Echo Cancel - Enable echo cancellation on this port.

Request Confirmation for Twinned Calls - You need to select this option if you have [Twinning](#) enabled on your analog phone and you are not in the USA.

When an analog phone is in Twinning, if the call is answered on the twin phone, edgeBOX is not able to know if the call was answered or not because of the analog line. So it is necessary to the user to press the # (cardinal) key after answering. This will inform edgeBOX that the call was picked up and edgeBOX will stop ringing the extension of the user. Otherwise the extension will keep on ringing despite the call having already been answered by the user.

To send this signal to edgeBOX, the Request Confirmation for Twinned Calls option must be selected.

Transmit / Receive Gain - This value should be adjusted depending on the network.

6.5.4 Echo Cancellation

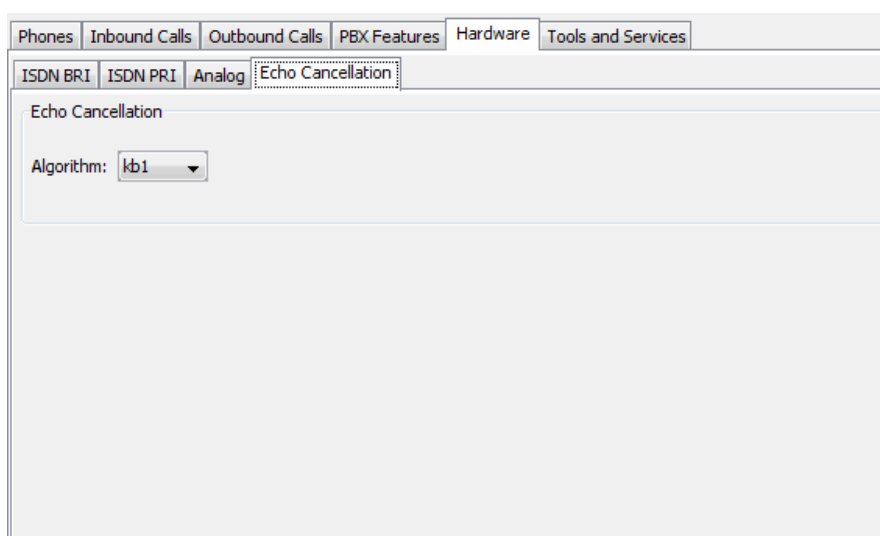
This panel offers a range of choices to allow for software echo cancellation.

The software determines the best configuration from the initial line characteristics and preserves the settings for the period of the call. The echo cancellation will only be applied to **analogue** phones, which have [echo cancellation checked](#). The two most useful ones are:

- High Performance Echo Cancellation (HPEC). Digium has introduced DSP-based echo cancellation modules for their multi-port T1/E1/J1 cards and 24-port analog card. This license needs to be purchased from Digium (although it is offered free with some products)
- Oslec, which is a free (as are all the others, except, hpec) echo cancellation "application"

You need to press apply if you change the echo cancellation type.

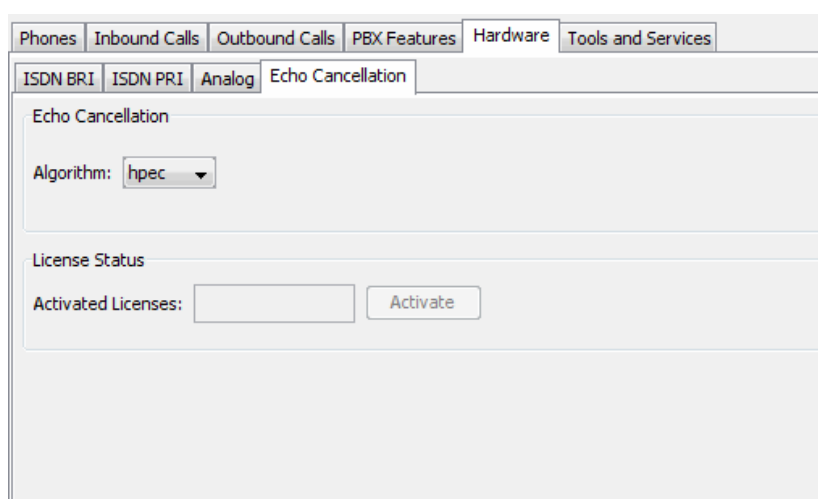
Note: This will restart asterisk and thus all current calls will be terminated!



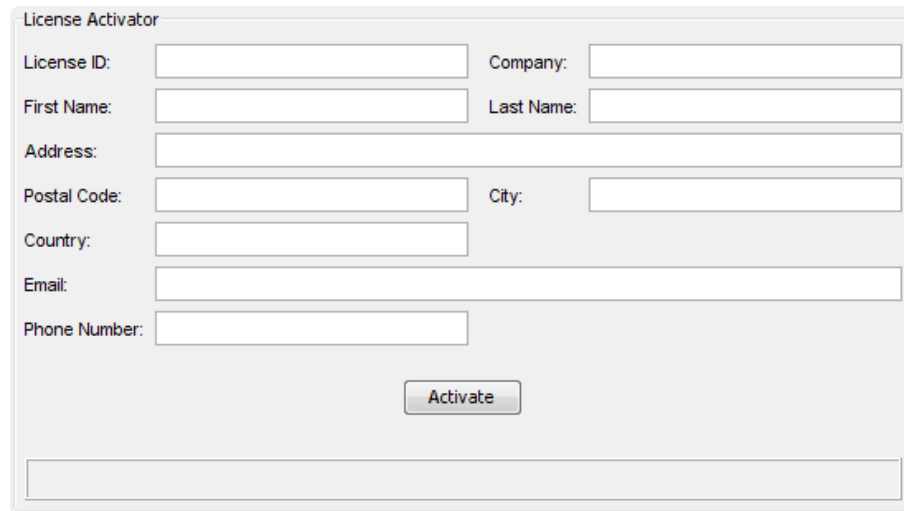
6.5.4.1 HPEC

This panel allows the administrator to enter the pertinent details to download and activate the license.

When hpec is selected and the "Apply" button pressed, the following panel will be presented:



To add a new license, press the "activate" button to be presented with the following panel:

A screenshot of a web form titled "License Activator". The form contains several input fields: "License ID:" and "Company:" on the first row; "First Name:" and "Last Name:" on the second row; "Address:" on the third row; "Postal Code:" and "City:" on the fourth row; "Country:" on the fifth row; "Email:" on the sixth row; and "Phone Number:" on the seventh row. Below these fields is a single "Activate" button. At the very bottom of the form is a long, empty rectangular box.

The License ID and Email fields need to be correct, the other fields are for information applied to the license.

6.6 Tools and Services

This panel allows you to configure edgeBOX PBX's general options.

6.6.1 Manager

Manager

If you enable the manager interface you will be able to establish a telnet connection to edgeBOX's IP PBX, allowing you such diverse administration options as placing calls remotely or receiving events related to the state of calls and extensions.

This interface may be useful if you own some kind of monitoring software which you want to integrate with edgeBOX.

You will need to supply the additional information:

- Username: username used for telnet authentication;
- Password: password to be used for telnet authentication;
- IP: IP address to be used by the remote host machine
- Netmask: Netmask to be used by the remote host machine.

Manager Service | G.729 Licensing | Phone Auto Configuration

☒ Enable

Username:

Password:

IP Address:

Netmask:

6.6.2 Billing Service

Allow billing software as Easylink, for example, to connect to edgeBOX's database. [What is billing software?](#)

Billing software is an application used to calculate call costs. EdgeBOX saves all important information about calls, as the time of the day a call was made, the line used, the duration of the call or the user that made the call. Billing software can connect to edgeBOX's calls database, retrieve that information and calculate all the cost for a billing service.

To allow billing software to connect to edgeBOX:

1. Click the VoIP menu and go to the Tools and Services tab and then the Billing Service sub tab.
2. Select the option Enable.
3. Indicate a username and a password. This is the username and password you will have to indicate in the billing software to connect to the edgeBOX.
4. Indicate from where the billing software can access edgeBOX by typing the IP address and netmask of the network where the computer with the billing software is. [View Examples.](#)

If the billing software can **only** be used **from computers on the local network**, for example, then you have to indicate the IP address of your local network, 192.168.90.0, for example, and then the netmask of your network; 255.255.255.0.

If it can **only** be used from **a specific computer of the local network** then need to type the fixed IP address of that computer; 192.168.90.128, for example, and then indicate that the IP address is only for one computer, using the netmask 255.255.255.254.

If it can **only** be used from **a specific computer outside the local network** then need to type the public IP address of that computer, 212.128.90.45, for example, and then indicate that the IP address is only for one computer, using the netmask 255.255.255.254.

5. Click Apply on the bottom right corner of the page to save the settings.

6. Go to edgeBOX's firewall (Security menu) and allow the billing service on the network that you indicated in step 4.

To connect the billing software on a computer to the edgeBOX, depending on the billing software you will use, you need to indicate:

- The username and password you specified on edgeBOX when you activated the billing service.
- The port used for the billing service: TCP port 5432.
- The database structure:
 - Database Model: Asterisc
 - Database Name: edgereporting
 - Table: cdr
 - Fields: all fields of the cdr table

If you **don't want to allow billing software** to connect to edgeBOX **no more**, remove the selection from the Enable option on the top of the tab and then click on the Apply button to save.

6.6.3 G.729 Licensing

G.729 Licensing

This panel allows you to add support for the G.729 codec. You need to download the codec from the Digium web site www.digium.com. Each license you purchase allows a single simultaneous use of the codec. Thus, if you purchase 3 licenses, 3 users can simultaneous use the codec, the fourth person will not be able to use this codec, unless one of the current users has completed their call.

The codec to purchase is: **codec_g729a_v32_i386** in the asterisk-1.2, x86-32 directory on the Digium site. After downloading to your PC, select the browse button and choose the codec file and then the upload button, which will then upload the file to the edgeBOX.

Make sure you have the service FTP allowed on the [firewall](#) because the upload of the codec file to the edgeBOX is made via FTP.

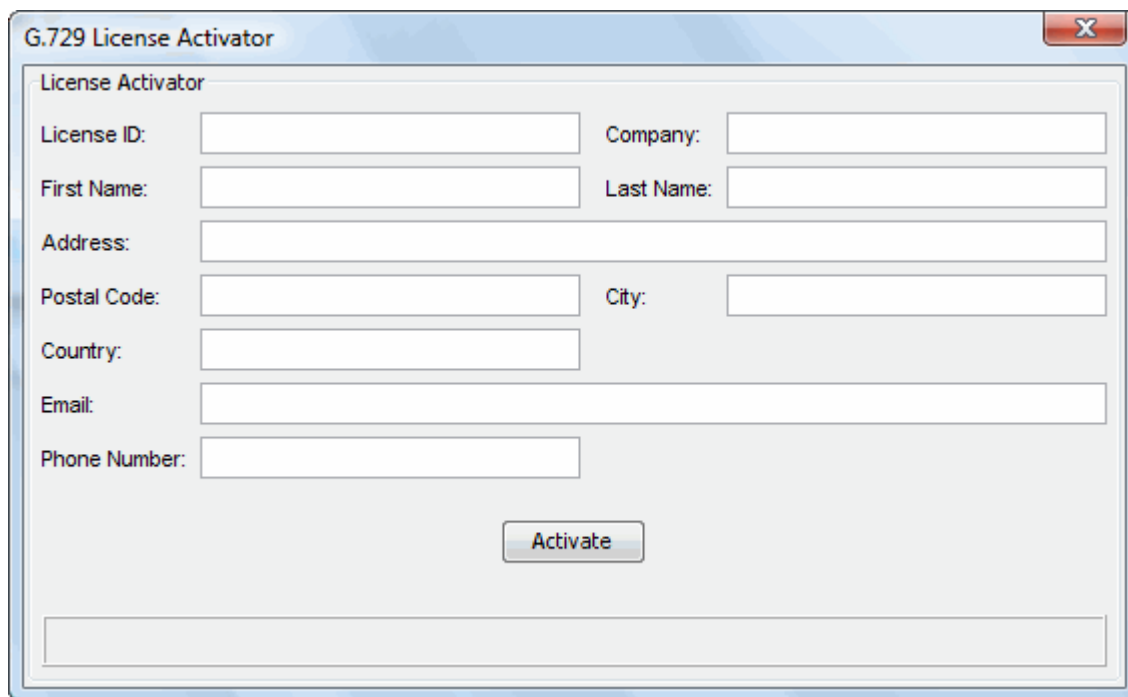
The screenshot shows a web interface with three tabs: 'Manager Service', 'G.729 Licensing', and 'Phone Auto Configuration'. The 'G.729 Licensing' tab is active. It contains a section titled 'Upload G729 codec file' with a 'Codec File:' label, a text input field, a 'Browse' button, and a 'Progress:' label with a progress bar. An 'Upload' button is located in the bottom right corner of this section. Below this section is a large, empty rectangular area.

After uploading the file, you will need to activate the license(s) (which will be locked to your edgeBOX hardware), by pressing the activate button.

The screenshot shows the same web interface as the previous one, but now with a 'License Status' section below the upload area. This section contains two rows: 'Activated Licenses:' with a text input field containing a hyphen and an 'Activate' button; and 'Licenses currently in use:' with a text input field containing a hyphen and a 'Refresh' button. Below this section is a large, empty rectangular area.

After pressing the Activate button, you will need to enter the License ID and other details which you entered when you purchased the License (as shown below).

Press Activate to complete the process.



The image shows a Windows-style dialog box titled "G.729 License Activator". It contains several input fields for user information: License ID, Company, First Name, Last Name, Address, Postal Code, City, Country, Email, and Phone Number. There is an "Activate" button at the bottom center. The dialog has a standard Windows title bar with a close button (X) in the top right corner.

6.6.4 Phone Auto Configuration

The Auto Phone Configuration allows you to **configure VoIP phones of your network directly on the edgeBOX**, avoiding this way, the configuration of each phone locally on the phone itself, or, avoiding the users to have to configure the phones themselves. [View more details about the phones configuration.](#)

When you connect a phone to the network for the first time it needs to be configured so it can make calls. This configuration is basically the attribution of an existing phone extension to the phone.

Analog Phones and Softphones need to be configured directly on the phone. But **VoIP phones can be configured either on the phone or directly on the edgeBOX** - Auto Phone Configuration. This way you can configure phones remotely, just using the edgeBOX's web interface.

▼ [Configure a detected phone](#)

To configure a phone that was connected to the network:

1. Go to the **Tools and Services** tab and the **Phone Auto Configuration** sub tab.
2. Click the **Available Phones** tab. Inside there's a list of the phones that are connected to the network.
3. You can click the Refresh button if the phone you want to configure is not listed; phones that have been connected just seconds before may not be listed yet.
4. Check the column **Configuration Status** of the phone you want to configure. It indicates if the phone is already configured or not. If the phone is not yet configured, **select the phone from the list** and click the **Configure** button.
5. In the dialog window that appears you can see the properties of the connected

phone. Click the **Select Ext.** button to assign an extension from the list of existing extensions of the edgeBOX. A window with all the extensions listed will appear.

6. Select the desired extension and click the **OK** button to assign the extension to the phone.
7. Click the **OK** button to save the changes to the list.
8. Click the Apply button to save the configuration.

▼ Change the configuration of a phone

If you want to change the Extension of a phone that is already configured:

1. Go to the **Tools and Services** tab and the **Phone Auto Configuration** sub tab.
2. Click the **Available Phones** tab. Inside there is a list of the phones that are connected to the network.
3. Select the phone you want to change the configuration from the list and click the **Configure** button.
4. In the dialog window that appears you can see the properties of the connected phone. Click the **Select Ext.** button to assign a different extension to the phone. A window with all the extensions listed will appear.
5. Select the desired extension and click the **OK** button to assign the extension to the phone.
6. Click the **OK** button to save the change into the list.
7. Click the Apply button to effectively save the configuration.

▼ Synchronize a phone's configuration with edgeBOX

If, for example, a user changes incorrectly the configuration of a phone, the phone may stop working properly. In these cases you can resend the correct configuration to the phone, so it can work properly again.

To synchronize the phones configuration with edgeBOX's saved configuration:

1. Go to the **Tools and Services** tab and the **Phone Auto Configuration** sub tab.
2. Click the **Available Phones** tab. Inside there list is a list of the phones that are connected to the network.
3. Select the phone you want to synchronize from the list and click the **Synchronize** button. edgeBOX will send the information to the phone and the phone will replace his existing configuration by the sent configuration.

▼ Ignore a phone

You can ignore a phone so that edgeBOX doesn't try to send it configurations nor try to call it to start the Configuration Assistant. [Why should I ignore phones?](#)

Ignoring phones can be usefully if you have some or even all phones or your network being managed by another device than the edgeBOX. In these situations you don't want edgeBOX to be trying to send configuration information to those phones from time to time.

To ignore a phone:

1. Go to the **Tools and Services** tab and the **Phone Auto Configuration** sub tab.
2. Click the **Available Phones** tab. Inside there list is a list of the phones that are connected to the network.
3. Select the phone you want to ignore the configuration from the list and click the **Ignore** button.
4. Click the Apply button to save the change.

▼ Stop ignoring a phone

If you want edgeBOX to **stop ignoring a phone** and send it configuration information again:

1. Select the phone from the list and click the Configure button.
2. In the properties window of the phone that will appear click the Don't Ignore button.
3. Click the Select Ext. button to assign an extension to the phone.
4. Click the OK button to save the information to the list.
5. Click the Apply button to save the change permanently.

▼ Remove the configuration of a phone

To remove the configuration of a phone:

1. Go to the **Tools and Services** tab and the **Phone Auto Configuration** sub tab.
2. Click the **Available Phones** tab. Inside there list is a list of the phones that are connected to the network.
3. Select the phone you want to remove the configuration from the list and click the **Release** button. edgeBOX will remove the extension that was assigned to the phone.
4. Click the Apply button to save the change.



If you release a phone, users will not be able to use that phone until you configure it again, by assigning it an extension.

You can also **configure phones that haven't yet been connected to the network but will be connected in the near future**. When those phones will be plugged in in the network for the first time, they will immediately receive the configuration you have defined and become configured and ready to use right away.


▼ Create and configure a new phone

1. Go to the **Tools and Services** tab and the **Phone Auto Configuration** sub tab.
2. Click the **Available Phones** tab.
3. Click the **New** button below the list of available phones. A properties window will appear.
4. Indicate the brand of the phone in the Model drop down list.
5. Type the MAC Address of the phone in the MAC Address field. The first half of the MAC address will be already filled because it represents the brand of the phone that you selected in the previous step.

6. Click the **Select Ext.** button to assign an extension from the list of existing extensions of the edgeBOX. A window with all the extensions listed will appear.
7. Select the desired extension and click the **OK** button to assign the extension to the phone.
8. Click the **OK** button to save the phone to the list.
9. Click the Apply button to save the new phone.

▼ Delete a created phone

1. Go to the **Tools and Services** tab and the **Phone Auto Configuration** sub tab.
2. Click the **Available Phones** tab.
3. Click the Apply button to effectively delete the phone.

 You can only delete phones that you have created and that have not been connected to the network. You can not delete connected phones because they really exist and are plug in in the network.

Related Topics:

- [Configuration Assistant Call](#)

6.6.5 Configuration Assistant Call

The Configuration Assistant is an automatic call that is made to a phone when it is first plugged in to the network. It guides the user through the configuration process of the phone. [Learn more.](#)

When you connect a phone to the network for the first time it needs to be configured so it can make calls. This configuration is basically the attribution of an existing phone extension to the phone.

Analog Phones and Softphones need to be configured directly on the phone. But **VoIP phones can be configured either on the phone or directly on the edgeBOX**- Auto Phone Configuration. This way you can configure phones remotely, just using the edgeBOX's web interface.

▼ Call phones when they are first connected and start the Configuration Assistant

To send a phone call starting the Configuration Assistant each time a user plugs in a new phone in the network (Callback Mode):

1. Go to the **Tools and Services** tab and the **Phone Auto Configuration** sub tab.
2. Click the **Configuration Assistant** tab inside the Phone Auto Configuration panel.
3. Select the option **Automatically call the phone and start the Configuration Assistant.**
4. Click the **Apply** button to save.

▼ Do not call phones when they are first connected to start the Configuration Assistant

If you don't want the user to receive the Configuration Assistant call when he connects a phone for the first time (Silent Mode):

1. Go to the **Tools and Services** tab and the **Phone Auto Configuration** sub tab.
2. Click the **Configuration Assistant** tab inside the Phone Auto Configuration panel.
3. Select the option **Do not make the Auto Configuration Assistant call**.
4. Click the **Apply** button to save.

You or the network users can also call the Configuration Assistant at any time (for instance, if they do not answer the Configuration assistant call) from a given phone to start the phone configuration process.

▼ [How to call the Configuration Assistant?](#)

To call the Configuration Assistant from a phone of the network, you or the user need to dial the number of the configuration assistant; number 1234.

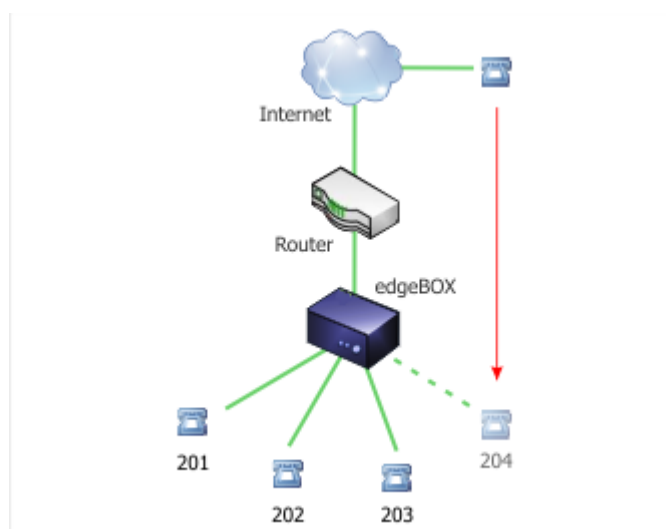
Note: It is only possible to dial the Configuration Assistant if the configuration was interrupted previously due to some problem and needs to be finished to configure the phone.

Related Topics:

- [Phone Auto Configuration](#)

6.6.6 Advanced NAT

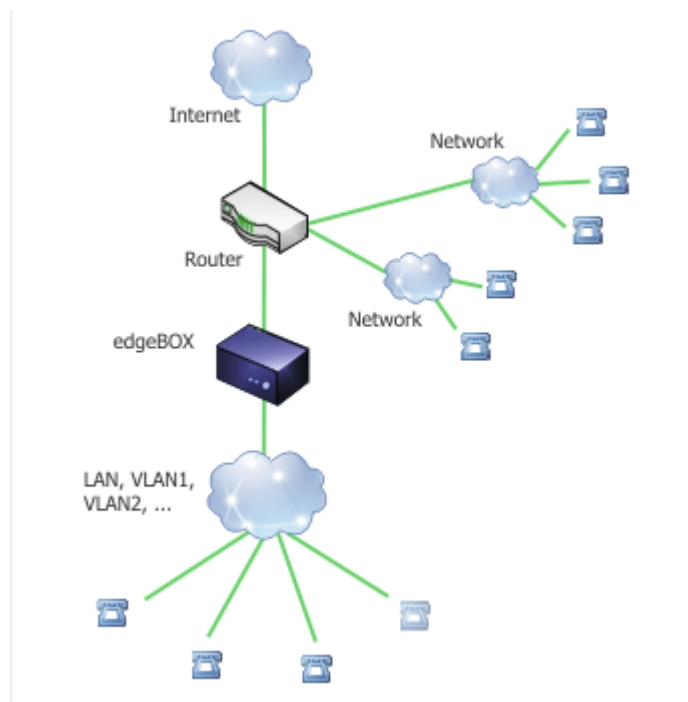
You need to configure Advanced NAT if you have a scenario where edgeBOX does not connect directly to the Internet but is behind a Router with NAT and Port Forward, and you want to allow remote phones (a phone you have at home, for example) to register in edgeBOX and behave as internal extensions.



To indicate that edgeBOX is behind a router:

1. Go to the the Advanced NAT tab and select the option My box is behind a router with NAT.
2. Indicate in the field below the router WAN IP address or its hostmane.
3. If you have local networks that are managed by the router and you have phones on those networks, select the option I have additional networks with phones to be served, and then, in the table below add an entry for each of those networks. [Learn More...](#)

edgeBOX can detect phones that are on its local networks (LAN, DMZ and the VLANs). However, as you have a router in front of edgeBOX you may also have local network managed by the router. And you may also have phones on those networks. edgeBOX cannot recognize these phones automatically because it is not managing these networks. So you need to indicate to edgeBOX the networks so it can recognize the phones and allow them to register.



4. Click the Apply button to save the settings.
5. To finish, you need then to configure on the router port forward from port 5060 of the router to port 5060 of edgeBOX.

7 QoS



One of the elements you can configure in a policy is the traffic control class. With this setting, you may assign a special priority to the traffic coming from or going to a given group of users, resulting in a better service for the group. Before this setting becomes effective you have to configure and start the traffic control service. To access the configuration page, select the QoS menu option and then the Traffic Control submenu option.

A page like the one shown below will be displayed. Possible actions are: Start/Stop Service, depending on whether the service is stopped or running and Apply, which will be used when you want to change an existing configuration. The available options are similar for each interface, so we will just cover the WAN interface (the DMZ tab will only appear if you have a DMZ interface - ie 3 NIC's). The available options are:

- [Upload Information](#)
- [Download Information.](#)

Traffic Control QoS Services

Service State: **Stopped**

WAN DMZ

Upload

Maximum Rate: 0 Kbps Reserve: 0 % 0 (KBits/s) ☐ DSCP Marking

☐ Allow other classes to borrow unused Premium bandwidth

Pipes

Total Allocated: 0%

Name	Bandwidth Allocated %	Rate (kbps)

The amount of reserved bandwidth above will be used to allocate EF based traffic Pipes

Add Edit Delete

Download

Maximum Rate: 0 Kbps Reserve: 0 % 0 (KBits/s) Amount of bandwidth reserved for Down Premium traffic Class

Start Service Apply

Note: To Give precedence to VoIP traffic, you should simply enter the Maximum Uprate and Downrate values and start QoS. All VoIP traffic would thus be marked as Gold, with all other traffic marked as BE (Best Effort)

The typical bandwidth weighting of BE, Bronze, Silver and Gold is as follows:

QoS Type	Weighting
Best Effort (BE)	10%

Bronze	20%
Silver	30%
Gold	40%

Traffic Congestion

When the network is contentious, BE packets are dropped first, then Bronze, then Silver (but still have minimums)

Pipes

Traffic allocated to a pipe cannot share bandwidth with any other pipe or with traffic not allocated to a pipe.

Thus if a pipe has been allocated 25% of the total bandwidth, it cannot use non allocated bandwidth, even though the pipe is full and there is spare bandwidth outside the pipe.

The reverse is also true.

Note: Traffic which uses Premium Bandwidth, cannot be blocked via [Content Filtering](#) and bypasses the Proxy.

7.1 Service State

This information is read-only and provides the current status of the service. Possible values are running and stopped. This is a global setting and applies to all interfaces.

7.2 Upload Information

In this section, you can configure the QoS settings for outgoing traffic. There are four pre-defined QoS classes, each corresponding to different levels of QoS priority: upGold, upSilver, upBronze and upBE. The latter is the default QoS class, with the lowest priority.

You may also reserve a percentage of bandwidth for custom classes (pipes). In the event of congestion, this percentage of bandwidth is always guaranteed for these pipes. The elements available are:

- [Maximum Rate](#)
- [Reserve](#)
- [DSCP Marking](#)
- [Pipes](#)

Upload

Maximum Rate: Kbps Reserve: % (KBits/s) ☐ DSCP Marking

☐ Allow other classes to borrow unused Premium bandwidth

Pipes

Total Allocated:

Name	Bandwidth Allocated %	Rate (kbps)

The amount of reserved bandwidth above will be used to allocate EF based traffic Pipes

7.2.1 Maximum Rate

Maximum available bandwidth for the outbound connection.

7.2.2 Reserve

This is the amount of the upload (outbound) bandwidth that is to be set as Premium bandwidth.

You can specify either the percentage or value in KBits/s.

Note: When pipes are created, you specify a percentage of this Premium Bandwidth, thus if Premium Bandwidth is 10% of 256KBit/s and you set a reserve of 50%, this reserve will be 50% of 10% of 256, which is approx 13KBits/s.

7.2.3 DSCP Marking

Check this box if you want packets classified and marked in accordance with the diffserv architecture. Enable this feature only if you have a QoS diffserv agreement with your ISP.

7.2.4 Allow other classes to borrow unused bandwidth

If you select this option you allow the reserved Premium bandwidth to be shared with the other QoS classes when it is not being used by the Premium class.

If you do not select this option, the bandwidth will always stay reserved for the Premium class even when it will not be used by it.

7.2.5 Pipes

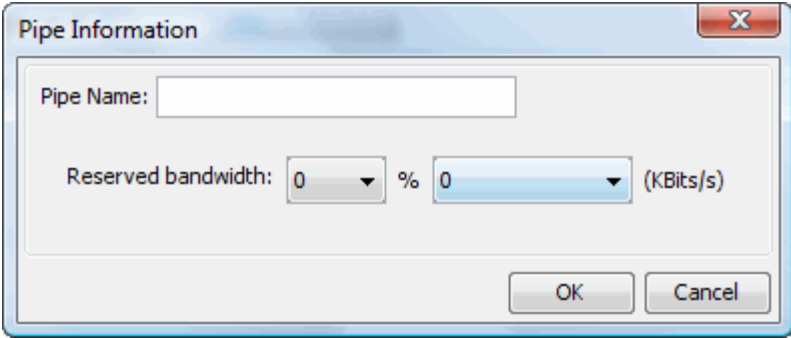
The bandwidth percentage reserved to upload priority traffic. You can then further subdivide this bandwidth, assigning a percentage of this bandwidth by creating pipes. In case of congestion, the bandwidth is guaranteed for each of these pipes.

Add

After selecting "Add", a popup window will display. The following information will be required:

- Pipe Name: The identification for this pipe;
- Reserved Bandwidth: The percentage or total of the **Premium bandwidth** reserved for this pipe.

After selecting "OK", the "Total Bandwidth" indicator will be updated, reflecting the amount of premium bandwidth already used by existing pipes. You will not be able to create more pipes after this bandwidth reaches 100%. Remember to select "Apply" in the main panel for changes to become effective.

A screenshot of a "Pipe Information" dialog box. It has a title bar with a close button (X). Inside, there is a text input field for "Pipe Name:". Below it, there is a "Reserved bandwidth:" label followed by two dropdown menus. The first dropdown shows "0" and the second shows "% 0". To the right of the second dropdown is the text "(KBits/s)". At the bottom right, there are "OK" and "Cancel" buttons.

Edit

Select the pipe you want to change and then select "Edit". A popup window similar to the one in "Add" will appear, allowing you to change all the information entered. After selecting "OK", the table will be updated, as well as the bandwidth indicator. You will not be able to make changes if the total pipes' bandwidth exceeds 100%. Remember to select "Apply" in the main panel for changes to become effective.

Delete

Select the pipe you want to delete and press "Delete". The pipe will be removed from the list and the bandwidth indicator will be updated. Remember to select "Apply" in the main panel, for changes to become effective.

7.3 Download Information

In this section you can configure the QoS settings for incoming traffic. The elements available are described next.

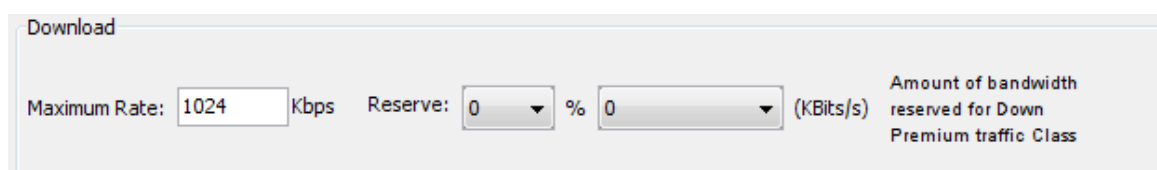
Maximum (down) Rate

Maximum available bandwidth for the download connection.

You can specify either the percentage or value in KBits/s.

Reserve

Available bandwidth percentage that will be assigned to priority download traffic. In the download connection there are just two QoS classes: downBE and downPremium. Traffic belonging to the QoS class downPremium will have an amount of bandwidth reserved, whereas for downBE (best-effort, the default), no guarantee will be given.



The screenshot shows a configuration window titled "Download". It contains two main settings: "Maximum Rate" and "Reserve". The "Maximum Rate" is set to "1024" Kbps. The "Reserve" is set to "0" % and "0" (KBits/s). A note on the right states: "Amount of bandwidth reserved for Down Premium traffic Class".

Setting	Value	Unit
Maximum Rate	1024	Kbps
Reserve	0	%
Reserve	0	(KBits/s)

7.4 QoS Services

Set quality of service classes to services, overriding quality of service settings for group traffic.

Direction	Class	Protocol	Source Addr...	Destination ...	Source Ports	Destination ...
LAN->WAN	upSilver	tcp	any	any	any	80
LAN->WAN	Test	tcp	any	any	any	1-1000

You can configure QoS classes by interface, protocol and port. For example, you can assign a special upload class for the Internet email service, and another for your DMZ email.

▼ Create a new QoS rule

1. Click the Add button. A properties window will be displayed.

2. Indicate the following properties:
 - **Source** - source interface. Options are WAN, LAN, LOCAL and DMZ (if available).
 - **Destination** - destination interface. Options are WAN, LAN, LOCAL and DMZ (if available). The options available change depending upon the Source chosen.
 - **Source IP Address** - where the traffic originates. You can specify an IP address, a range of addresses or indicate that it will apply to any IP address.
 - **Destination IP Address** - where the traffic goes to. You can specify an IP address, a range of addresses or indicate that it will apply to any IP address.
 - **Source Ports** - you can add single ports or a ranges of ports were the traffic originates.
 - **Destination Ports** - you can add single ports or a ranges of ports were the traffic goes to.
 - **Protocol** - protocol of the traffic: TCP, UDP, GRE or ESP.
 - **Class of Service** - Quality of service class to assign to the traffic for this service. For outbound traffic (for example, from the LAN to the WAN), choose from upBE, upBronze, upSilver, upGold, or choose a pipe if you have pipes created. For inbound traffic (for example, from the LAN to the WAN), choose from downBE and downPremium.
 3. Click OK for the entry to appear in the table.
 4. It to become effective you click the Apply button in the main panel.
- ▼ [Change the settings of an existing rule](#)
1. Select the rule you want to edit from the list.
 2. Click the Edit button. The properties window of the rule will pop up.
 3. Change the desired properties of the rule.
 4. Click the OK button to save the changes into the list.

5. Click Apply to save the rule.

▼ [Delete a QoS rule](#)

1. Select the rule you want to delete from the list.
2. Click Delete.
3. Click the Apply button to save.

▼ [Change the order edgeBOX uses the QoS rules](#)

If a service or a port is used in more than one rule, EdgeBOX uses the first rule of the list that has the service.

You can change the order the rules are checked by edgeBOX:

1. Select the rules (one at a time) in the list.
2. Use the UP and Down buttons to move the rule up or down on the list.
3. When you have the order defined click Apply to save the new order the rules are used.

The upstream packet classification (TC) is performed by filters by the following order:

- 1st - QoS service
- 2nd - Access profile
- 3rd - DSCP to configured QoS classes

If user authentication is active, the DSCP based classification will never be reached because access profile rules will always match because each profile is mapped into a configured QoS class.

As there is no transparent proxy support on the kernel packets going to port 80, they cannot be classified. To resolve this issue, upstream flows destined to port 80, bypass Squid whenever matched by a QoS service rules.

8 Wireless



In the WiFi menu you can configure and change the properties of the wireless network.

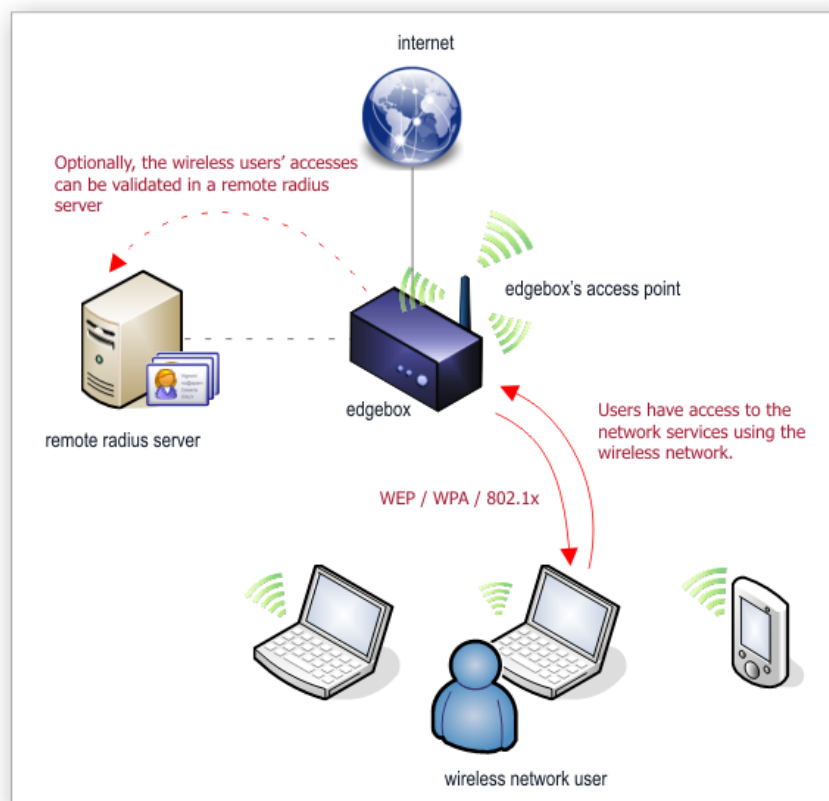
- [Configure and turn on the wireless](#)
- [Indicate the type of wireless authentication](#)
- [Make the wireless network more secureweb interface](#)
- [Make the wireless network public](#)

8.1 Configure and turn on the wireless network

edgeBOX allows you to have a wireless network and define several configurations to make more secure. [How does the wireless network works on the edgeBOX?](#)

edgeBOX provides a wireless LAN access to your office. It can operate with an embedded Access Point or as an 802.1x Access Point controller if you use several external Access Points spread through the network.

 **edgeBOX cannot manage external access points.** To manage these access points you need to use the specific access point's management interface.



As you can see in the image above, you can set several scenarios, as integrated authentication using edgeBOX users' accounts or external authentication using a remote Radius server. edgeBOX supports for WPA, WEP or 802.1x authentication.

As edgeBOX also provides IP-PBX features, you can combine them with the wireless features to create wireless VoIP phone access.

By default, edgeBOX's wireless network is already running with a factory configuration defined: the network name is mybusiness and the WPA password is mydemokey. This way, you can immediately start providing wireless access on your office, without having to configure anything on the edgeBOX.

▼ Change the configuration of the wireless network

1. Go to the Basic tab of the WiFi section.
2. Indicate a name for the wireless network in the Network Name field. The name of the wireless network is a name of your choice that will work as the public identifier of the network so users can connect to the network.
3. Go to the Advanced tab to select and configure the type of security protocol you want to use. You can use:
 - [static WEP keys authentication](#);
 - [WPA security](#);
 - [802.1x authentication](#);
 - or you use no security method if you want to have [public network](#) available for

everybody (network without authentication).

4. After selecting the type of security, click the Apply button to save.



Change the Channel of the wireless network

You will probably need to change the Channel of the wireless network if you have other devices than this edgeBOX providing wireless networks nearby; other Access Point devices or other edgeBOXes, per example, to avoid conflicts with the other devices. This is because each of the overlapping Access Points must have a different channel.

To change the the Channel of the edgeBOX's Access Point, select a channel that is not used in the overlapping networks in the Channel Selection drop down list in the Basic tab when you are creating the wireless network.

▼ Turn off the wireless network

If you wish to temporarily turn of the wireless network for any reason, or if you don't want to have a wireless network anymore, click the Stop Service button on the bottom right side of the WiFi section.

The wireless service will be stop, but the information about the wireless properties will not be deleted, so if you later on wish to make the wireless network available again. you just need to click the Start Service button.



If you **add a wireless card** to the edgeBOX, you need to **reboot edgeBOX** after you added the card.

Related Topics:

- [Indicate the type of authentication for the network](#)
- [Make the wireless network public](#)

8.2 Indicate the type of authentication

When you create your wireless network you choose protect it so that only the persons you choose may use it. To secure edgeBOX wireless network you can use one of the following authentication methods (protocols): [Which type of authentication should I use?](#)

The type of authentication you use depends on the devices that are going to access the wireless network. Per example, some smartphones or older network devices do not support WPA security yet, so you need to use WEP authentication to ensure compatibility with all devices.

If you don't need to grant compatibility to older devices, avoid using WEP authentication. WEP is relative relatively easy to break by hackers. use WPA with a strong password instead

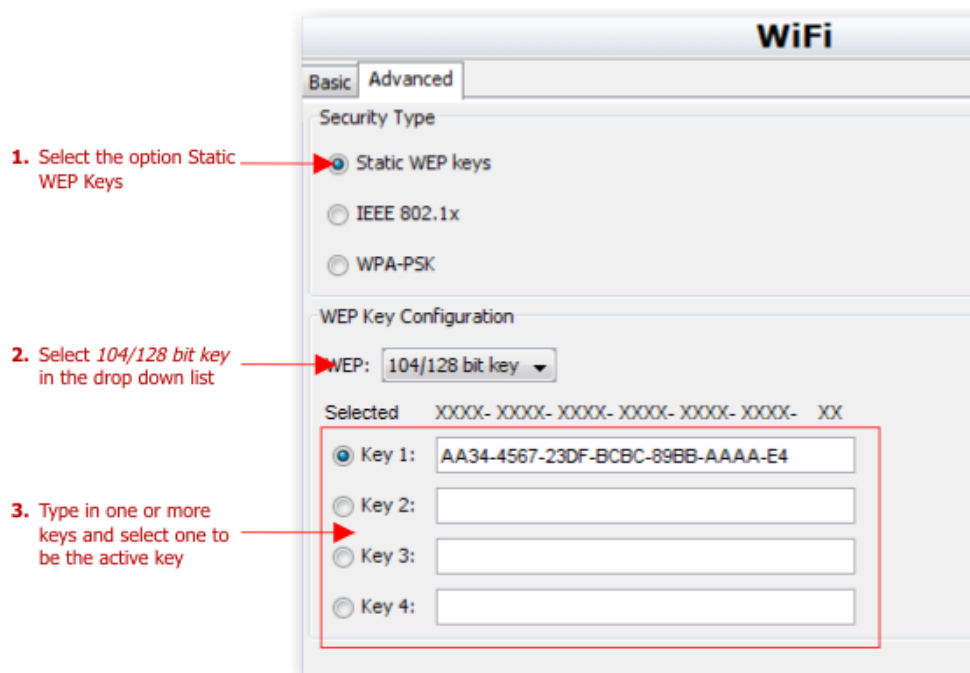
because it is more secure.

802.1x authentication is even more secure than WPA authentication. It is normally used to secure wireless networks on workplaces.

▼ Use static WEP keys authentication

To use WEP authentication on the wireless network:


1. Go to the Advanced tab and choose the Static WEP keys option.
2. To indicate the number of bits the keys should have keys you want to use, select the 104/128-bit key option from the WEP drop down list because it is more secure. Select only the None, 40/64-bit key option if you need to ensure compatibility if you will have devices accessing the network that do not support 104/128 bit keys.



3. Enter one or more keys in the text fields below. [How must the key be?](#)

The key must be formed using groups of hexadecimal characters (A to F and 0 to 9) separated by a '-'. Example of a 104/128 bit key:
ACBB-8EF2-3410-23AA-F8F0-EEEE-A2.

4. Select one of the keys you be the active key. One one key can be used at a time. To increase security, change the active key from time to time.
5. Click the Apply button to save.
6. Indicate the active key to the users of your network you want to be able to access the wireless network.

 If all your devices support WPA authentication, then use this type of authentication instead of the WEP keys. WEP is relative relatively easy to break.

If you need to use WEP then change regularly the WEP keys, to grant a certain level of security. This is not easy to accomplish if you have many users of the wireless network because you need to inform them all about the new active key each time you change it.

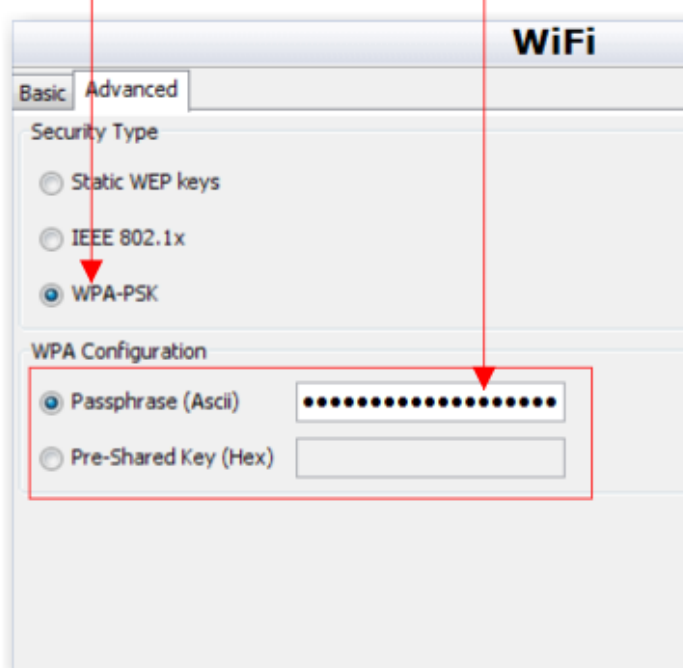
▼ Use WPA security

To use WPA authentication on the wireless network:

1. Go to the Advanced tab and choose the WPA-PSK option.

1. Select the option WPA-PSK

2. Choose if you want to use a text phrase or an hexadecimal key to be the network access key and type it in



2. Indicate a passphrase or a pre-shared key that will be used to authenticate to the network. [How must the passphrase or the pre-shared key be?](#)

- Pre-shared Key - must be composed only of exactly 64 hexadecimal characters (A to F and 0 to 9) and cannot have spaces.
- Passphrase - must be between 8 and 63 characters long and cannot contain spaces, nor special characters like | \ / : * ? ! < > ".

3. Click the Apply button to save.

4. Indicate the passphrase or the pre-shared key to the users of your network you want to be able to access the wireless network.

 Try always to have secure passphrases and pre-shared keys to increase the networks security. [Obtain random generated secure keys at the GRC website.](#)

▼ Activate 802.1x authentication

802.1x authentication means that each users who wants to enter the wireless network has to login using its own username and password, instead of using a network key that is shared by everyone.

To use 802.1x authentication on the wireless network:

1. Go to the Go to the Advanced tab and choose the 802.1x option.
2. Select WPA in the Encryption Type group. This is normally called WPA-Enterprise. If you have devices that do not support WPA accessing the wireless network, choose Dynamic WEP instead.
3. Define the place where users' username and password are validated when they try to login to access the wireless network. You can validate these credentials:

- [Locally on the edgeBOX](#)

It means that, edgeBOX will see if the username and password of the user exist in the edgeBOX's list of users and if they match. This is the default option and just have to verify if the Enable Remote Radius Server option is not checked. If it is checked, uncheck it.



For a user to be able to login, using the 802.1x method, the user needs to have 802.1x Access permissions. you can verify these settings in the properties of a user by [editing the user](#).

- [On a remote Radius server](#)

It means that, a remote Radius server will validate the users' credentials instead of the edgeBOX.

1. Check the option Enable Remote Radius Server. Below the option, fields to indicate how the edgeBOX can connect to the remote server will appear.
2. Type in the IP Address of the remote server in the IP Address field.
3. Indicate the password of the remote server in the Password field.
4. Change the value of the remote server's if you don't want to use the default port.



If you want to use the same remote radius server as the one you are using for the authentication the users in the local network (NAC menu), than leave the fields above empty. edgeBOX will then know that you want to use the same remote server.

5. If you also wish to save information like the time the users were connected or what did they do, you can save that information on a remote remote radius server. Check the option Enable Radius Accounting and indicate how edgeBOX can connect to the remote server.

4. Click Apply to save.

Related Topics:

- [Make the wireless network more secure](#)
- [Make the wireless network public](#) (with no authentication required)

8.3 Make the wireless network more secure


You can configure two settings on the edgeBOX to make your wireless network more secure, even if you are already using a secure type of authentication:

▼ [Allow only specific devices use the wireless network](#)

If you want just a list of specific computers and other network devices to be able to use the wireless network, that is, to be able to connect to edgeBOX's access point:

1. On the Basic tab, uncheck the option Allow all Clients. An empty list will appear below.
2. Fill the list with the MAC Addresses of each computer or device you want to be able to use the network. To add a MAC Address to the list, click the add button below the list, type the MAC Address on the dialog window that pops up and click OK.
3. After you add all the desired devices, click the Apply button in the bottom right side of the panel.

If you don't want a computer to belong to the list anymore, select the MAC Address of the computer from the list and click Delete. Then click the Apply button.

 If you don't have this option selected you still have control over who accesses your wireless network because users still need to authenticate using a wep key, or using 802.1x. This option is just to restrict even more the access to the network to specific devices.


▼ [Hide the network](#)

You can hide edgeBOX's wireless network from appearing in the list of available networks people see when they scan for available wireless networks they can connect to in they computers. [Why should I hide the wireless network?](#)

Hiding a wireless network is a way of improving the network's security. It makes difficult unauthorized access attempts; people won't try to enter a network if they do not know it exists in the first place.

To **hide the network**:

1. On the Basic tab, check the option **Hide SSID**.
2. Click the Apply button in the bottom right side of the panel.

 For your network users to use the hidden wireless network, they need will need to connect to the network manually. This process differs according to the Operating System your users are using.

Related Topics:

- [Indicate the type of authentication for the network](#)

8.4 Make the wireless network public

A public wireless network is a network with no authentication method. It means that everyone who receives the signal of the network will be able to enter it and use it.

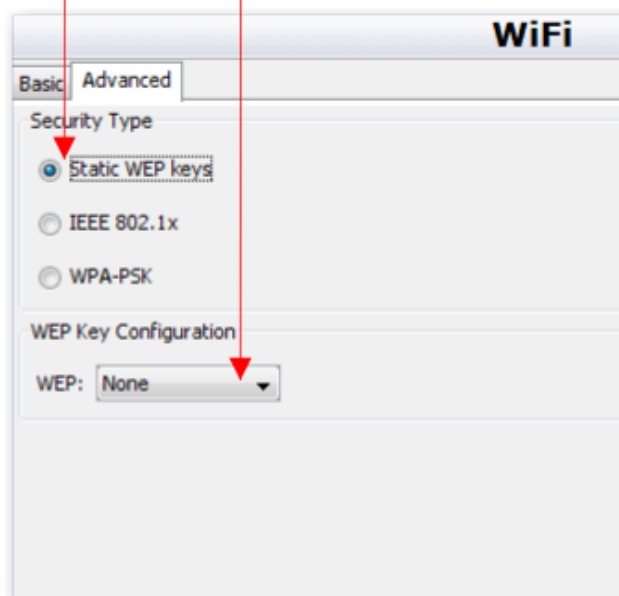
 **Avoid creating public wireless networks** if you **don't really want to make it available for everyone** for a given reason.

Wireless networks are more vulnerable to hackers and malicious software because the signal is available for everybody nearby edgeBOX's access point. If you don't protect the network, unauthorized people can get access to the information on the computers on the network and use the connection to access the Internet. Always [secure the wireless network](#) if you don't want everybody to access it.

If you want to **make your wireless network public**:

1. Go to the Advanced tab and choose the Static WEP keys option.

1. Select the option Static WEP Keys
2. Select *none* in the drop down list



2. Select none from the WEP drop down list.
3. Click the Apply button to save.

Related Topics:

- [Configure the wireless network](#)
- [Indicate the type of authentication for the network](#)

9 Web Server and Email Server



In the Collaboration menu you can:

- [Configure the Web Server](#)
- [Configure the Email Server](#)

9.1 Web Server

View and change the configuration **for the HTTP service** (Apache Web Server) **running on edgeBOX**. Two actions are possible, performed with the two buttons on the bottom-most panel: toggle service status (Start/Stop) and apply changes made to the configuration ("Apply" button). The available configuration options are described next.

Web Server **Email Server**

Service State: **RUNNING**

Max. Access:

User Directories:

Virtual Hosts

Virtual Host	Server Name	Document Root	Email	Proxies
--------------	-------------	---------------	-------	---------

Change webmaster password:

New Password:

Confirm Password:

9.1.1 Service State

This element is read-only and has the current status for the http server: Running or Stopped.

9.1.2 Max. Access

Here we set the maximum number of simultaneous access connections to the web server.

9.1.3 User Directories

Select from the list. Possible values: Yes/No.

If set to "Yes" users will be able to have personal web pages. Their homepage will be located in the user's home directory, under the public_html directory. The user will be able to manage their personal webpage through FTP – after logging on, they will automatically be placed in their directory.

The URL to access a user's personal webpage will be formed from the concatenation of the main URL with "~username".

For example, if the main URL is <http://edgeBOX.domain>, then noname's webpage will be located on <http://edgebox.domain/~noname> or <http://edgebox.domain/users/noname>.

9.1.4 Virtual Hosts

This panel allows you to configure virtual hosts. With virtual hosts, you are able to have the same web server running multiple websites. Possible actions are [New](#), [Edit](#) and [Delete](#).

9.1.4.1 New

After selecting the "New" button, a popup window will appear, requesting that you enter the following information:

- Virtual Host. Select from the list of values. Possible values are: LAN and LAN + WAN. Defines the scope of access to this virtual host.
- Server Name: The name of this virtual host. Remember that an A or CNAME record has to be added to the DNS for this setup to be complete. For example, if your domain is local.loc, and you add a virtual host for "docs.local.loc", then you will have to add an entry for host "docs" pointing to edgeBOX's IP address.
- Document Root: the location of the files in the file system.

All "User" websites will be located in the public_html folder, in the user's home directory. This directory is created when the user is created.

If "Path" is chosen, the directory (document root) is created automatically in the /home/wwwhost directory and is owned by webmaster

All "Path" websites will be located under /home/wwwhost, which is the filesystem directory where the webmaster user will be placed after logging on through FTP.

If "Path" or "No Document Root" is chosen, edgeBOX will either create an appropriate DNS host entry for the domain, or remind you that you will need to create one manually.

? If the domain for the new web server entry does not exist:

? and the edgeBOX is not the master domain, the administrator will be

informed that the DNS entry needs to be added manually on the system which is hosting the domain.

- ? and the edgeBOX is the master domain, then the new host for that domain will be added to the DNS domain and the administrator will be informed via a popup.

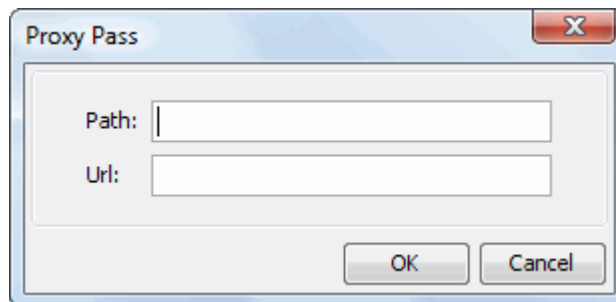
The DNS entry will only be created if the above condition exists and if the condition shown in the following table is true

(eg VHOST is allowed for Both Internal and External and the Domain is set to External Access)

Virtual Host Setting	DNS Domain Access = Internal	DNS Domain Access = External
LAN	Yes (LAN IP)	No
WAN and LAN	Yes	Yes (WAN IP)

If "No Document Root" is chosen, then no directory will be created for this website

If "New" is selected, the following panel allows the administrator to redirect requests to a proxy.



The image shows a Windows-style dialog box titled "Proxy Pass". It has a standard title bar with a close button (X). Inside the dialog, there are two text input fields: "Path:" and "Url:". Below these fields are two buttons: "OK" and "Cancel".

Thus, if the edgeBOX receives a request for the proxy domain, it will send the request to the proxy (as nominated in the URL field) and add the path (if there is one) to the request. For example, if Path=/support/4.6/ and url=http://192.168.100.150, a request to the edgeBOX for www.clk.com/support will be redirected from the virtual host to the proxy at http://192.168.100.150/support/4.6/

Note: Virtual hosts usually require a FQDN, rather than the IP used in this example.

Note: A typical value for path would simply be / (ie direct all requests to the root directory of the proxy)

- **Server Signature:** If checked, the email for the responsible person for this domain should be entered and will be shown when a user tries to access a page not available on the server.

9.1.4.2 Edit

This option allows you to change a Virtual host configuration. The fields available are the same as for the [new](#) virtual host window.

9.1.4.3 Delete

An entry has to be selected. To make this change effective, select "Apply".

Note that the DNS host information will not automatically be deleted when the web server host is deleted.

9.1.5 Change Webmaster password

This option allows you to change the password for user 'webmaster'. The user 'webmaster' has FTP access and owns the directory tree for the intranet and Internet websites. The FTP root directory will initially contain two directories ("intra" and "inter"), corresponding to these websites, but more may be created, for example for virtual hosts' websites.

To change the password, type the password in the "New Password" and "Confirm Password" fields, and select the "Change" button. Remember that this account is initially disabled so you will have to set a password in order to use it.

9.2 Email Server

edgeBOX implements the email service using Sendmail.

The two panels (Basic and Advanced) allow you to configure the mail server. Also, the two panels are linked so that changes in one panel will update appropriate settings in the other panel.

9.2.1 Basic

The basic panel allows you to set up the mail server with minimal effort. The panel options are:

Service Status:

Read Only Status summary. Status is Running or Stopped

Webmail Domain:

Allows you to choose the domain which you want to set as your webmail domain.

You can add and delete mail domains via the "Add" button

Only one domain may be a web mail domain.

For details on using and accessing the web mail functionality, check [Web Mail](#).

If you do not choose a domain, the WebMail Icon will not appear on the main applications panel.

Also note, that the [Web Server](#) must be running to access Web Mail

The screenshot shows the 'Email Server' configuration window with the 'Basic' tab selected. At the top, the 'Service State' is 'RUNNING'. Below this, there are two tabs: 'Basic' and 'Advanced'. Under the 'Basic' tab, there is a section for 'Webmail Options' which includes a checkbox for 'Enable Webmail' (checked) and a dropdown menu for 'Webmail Domain' set to 'example.com'. Below the dropdown are 'Add' and 'Delete' buttons. Another section, 'Allow Sending Mail From', contains two checkboxes: 'Internal LAN' and 'Internet', both of which are checked. At the bottom right of the panel are 'Stop Service' and 'Apply' buttons.

Internal LAN:

If checked, clients on the LAN or any VLAN (not the DMZ) are allowed to send mail

Internet:

If checked, users on the internet, can connect via pop3 and send mail from the edgeBOX.

This is the same setting as POP before SMTP in the advanced panel.

9.2.2 Advanced

The advanced panel allows access to more configuration options than the Basic panel.

Note that changes in this panel, will update appropriate panel entries in the Basic panel.

The screenshot shows the 'Advanced' configuration panel for EdgeBOX 4.6. At the top, there are tabs for 'Basic' and 'Advanced', with 'Advanced' being the active tab. Below these are sub-tabs for 'Global', 'Access Control', and 'Alias', with 'Global' being selected. The main configuration area is titled 'Email Domain or Hostname' and contains a large text input field with 'example.com' entered. Below this field are three buttons: 'Add', 'Edit', and 'Delete'. Further down, there is a checkbox labeled 'Enable Webmail on domain:' which is checked, followed by a dropdown menu showing 'example.com'. Below this, there is a 'Storage:' section with two radio buttons: 'Local' (selected) and 'Remote' (unselected), followed by an empty text input field. Below the storage section, there are two input fields: 'Max. Connections:' with a value of '0' and 'Max. Message Size:' with a value of '0', both followed by '(KBytes)'. Below these fields, there are two small text labels: '*0 means Unlimited'. Below the message size field, there are three checkboxes: 'Block Unresolvable Domains' (checked), 'POP Before SMTP (Relay Support)' (checked), and 'SmartHost' (unchecked). Below the 'SmartHost' checkbox is an empty text input field. At the bottom right of the panel, there are two buttons: 'Stop Service' and 'Apply'.

9.2.2.1 Service State

This element is read-only and shows the current service status (running or stopped).

9.2.2.2 Global

In this panel, you can configure general email options, such as:

- [Email domain\(s\) for which you will be receiving email](#)
- [Webmail Domain](#)
- [Type of storage used](#)
- [Max. simultaneous connections](#)
- [Max. message size](#)
- [Blocking of unresolvable domains](#)

- [POP Before SMTP \(for relay\)](#)
- [Smarthost](#)

Global Access Control Alias

Email Domain or Hostname

example.com

Add Edit Delete

☒ Enable Webmail on domain: example.com

Storage: ☒ Local ☐ Remote

Max. Connections: 0 Max. Message Size: 0 (KBytes)

*0 means Unlimited *0 means Unlimited

☒ Block Unresolvable Domains

☒ POP Before SMTP (Relay Support)

☐ SmartHost

9.2.2.2.1 Email Domain(s)

A list with the alternate hostnames for this host and domains for which it will accept mail. Each entry has to be a full-qualified domain name. Available actions are "Add", "Edit" and "Delete".

Add

After selecting this option, enter the Domain name select OK then click on the Apply button to make this change effective.

Edit

Allows you to modify the selected entry. To make this change effective, don't forget to select the "Apply" button.

Delete

Select the entry you want to delete and then click on "Delete". Don't forget to click "Apply" to make this change effective.

9.2.2.2.2 Webmail Domain

Allows you to choose the domain which you want to set as your webmail domain. Only one domain may be a web mail domain. For details on using and accessing the web mail functionality, check [Web Mail](#).

If you do not choose a domain, the WebMail Icon will not appear on the main applications panel.

Also note, that the [Web Server](#) must be running to access Web Mail

9.2.2.2.3 Storage

If you choose 'local', then all mail will be stored on edgeBOX; if you choose 'remote', you will have to provide a hostname or IP to which all mail will be sent.

9.2.2.2.4 Max. Connections

The maximum number of simultaneous connections. After this number, connections will be rejected. If set to 0, then there will be no limit.

9.2.2.2.5 Max. Message Size

The maximum size of messages that will be accepted. Setting it to 0, will accept messages of any size.

9.2.2.2.6 Block Unresolvable Domains

Checking this option will cause all mail that arrives from un-resolvable domains to be refused. This is the default behavior for security reasons (as using dynamic IP's is a very common technique used by spammers).

9.2.2.2.7 POP before SMTP (Relay Support)

Checking this option means that you are allowing relay from users authenticated through POP3.

This will be a limited authorisation, as it will expire some time later.

This setting is particularly useful for users who are connecting from external networks (while, traveling for example, the so called "Road Warriors") and for which we want to allow relaying.

Normally you only permit mails to be relayed (sent) from within your own network. But some users travel and connect from other places and you want to let those users send (relay) mail through your server.

Whenever someone logs in via POP3 mail, the server notes the IP address from which the connection was made, and permits relay from the IP for a limited time.

Note that you will have to grant access to the POP3 service from outside networks in the firewall configuration.

9.2.2.2.8 SmartHost

This allows you to send outgoing mail to another mailserver (which is called a "smarthost"). The smarthost will deliver your mail to the other mailservers on your behalf.

9.2.2.3 Access Control

In this panel, you will be able to configure access control options. The main panel shows the current ACL list.

You can view the list either "Based on Connection" or "By Source/Destination" by selecting the appropriate tab on the right hand side.

Connection Entity	Allow Relay	Allow Mail	Reject
192.168.100	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
192.168.101	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
192.168.102	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
192.168.103	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
192.168.104	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
192.168.105	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

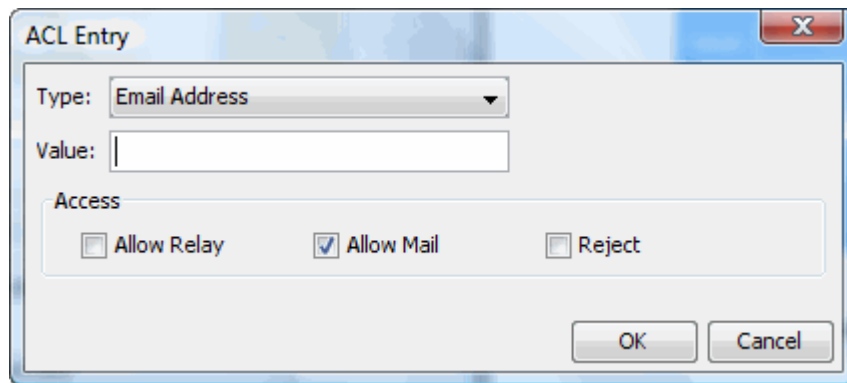
Based on Connection
By Source/Destination

Add Delete

Based on Connection

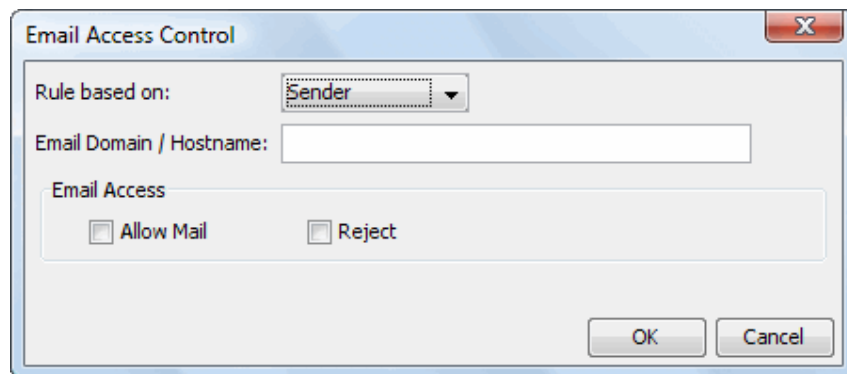
It is possible to add and remove mail relay and connection rules both for email addresses (as mail origin), host, network (eg 192.168.90, for a 'C' network) addresses and hostname/ domains.

You can also add entries for "Accept Mail", which will allow for "Unresolvable" domains to send mail to local domain clients.

The "ACL Entry" dialog box has a title bar with a close button (X). It contains a "Type:" dropdown menu set to "Email Address". Below it is a "Value:" text input field. Under the "Access" section, there are three checkboxes: "Allow Relay" (unchecked), "Allow Mail" (checked), and "Reject" (unchecked). At the bottom right are "OK" and "Cancel" buttons.

By Source / Destination

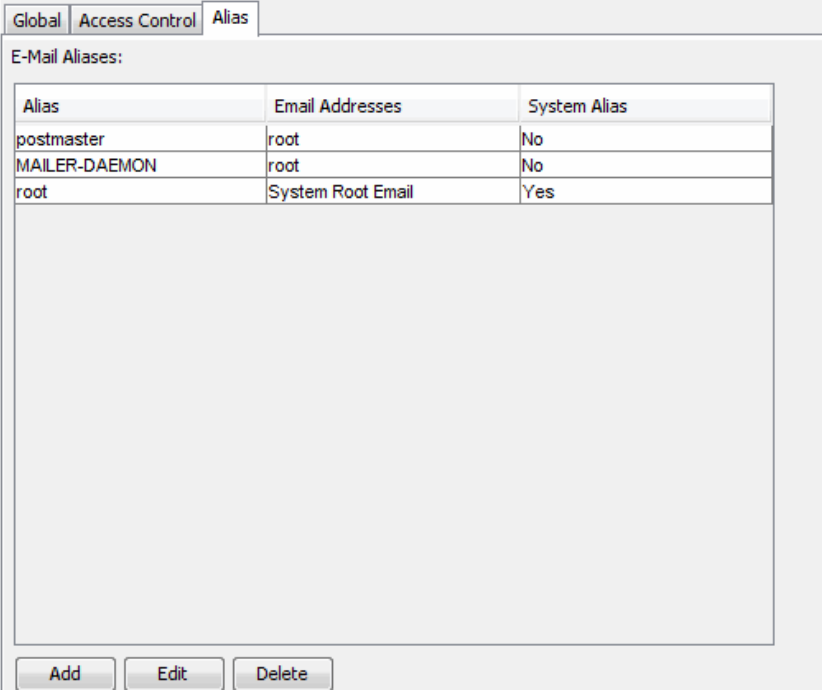
It is possible to add and remove rules based on the source or destination of the email address or domain.

The "Email Access Control" dialog box has a title bar with a close button (X). It contains a "Rule based on:" dropdown menu set to "Sender". Below it is an "Email Domain / Hostname:" text input field. Under the "Email Access" section, there are two checkboxes: "Allow Mail" (unchecked) and "Reject" (unchecked). At the bottom right are "OK" and "Cancel" buttons.

Note: When entering a value (eg the address or IP), you may use wildcards ("*"). If a given domain is listed, all sub domains will be banned. After selecting "OK" you have to select "Apply" in the main panel to make the changes effective.

9.2.2.4 Alias

In this panel, you may edit the aliases' list.



The screenshot shows a web interface with three tabs: 'Global', 'Access Control', and 'Alias'. The 'Alias' tab is selected. Below the tabs is a section titled 'E-Mail Aliases:' containing a table with three columns: 'Alias', 'Email Addresses', and 'System Alias'. The table contains three rows: 'postmaster' pointing to 'root' (System Alias: No), 'MAILER-DAEMON' pointing to 'root' (System Alias: No), and 'root' pointing to 'System Root Email' (System Alias: Yes). Below the table are three buttons: 'Add', 'Edit', and 'Delete'.

Alias	Email Addresses	System Alias
postmaster	root	No
MAILER-DAEMON	root	No
root	System Root Email	Yes

9.2.2.4.1 E-Mail Aliases

With this element you can provide alternate names for individual users, forward mail to another host or create mailing lists. This table has some predefined aliases related with management. You can choose to redirect mail for these aliases to another user, so that they receive the notifications. You may also define more descriptive names for your users instead of your 8-letter login names. Each entry has on the first column the alias name, and on the second column the email address to which it will expand. There are two operations available: "Add" and "Delete".

Note: the root alias will not appear on this list as it is configured elsewhere (System menu, Config submenu).

Add

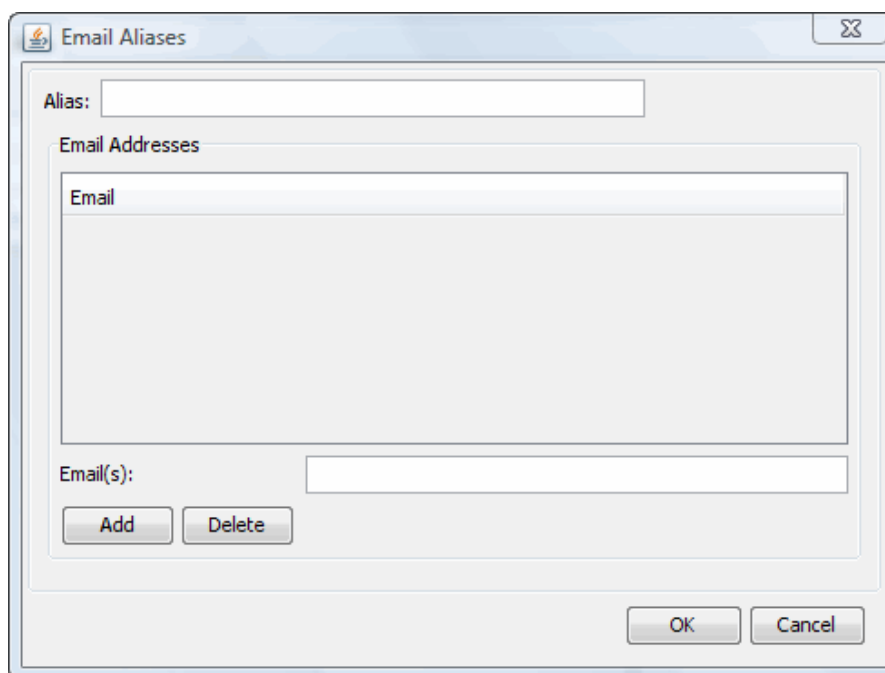
If you select this operation, a popup window will appear requesting the following information:

- Alias: the name of the alias you want to create;
- Email(s): the email or list of emails to which this alias will expand.
- After selecting Add and OK, don't forget to select "Apply" so the changes become effective.

Delete

To delete an alias, select it from the list and press "Delete". Don't forget to select "Apply" to make

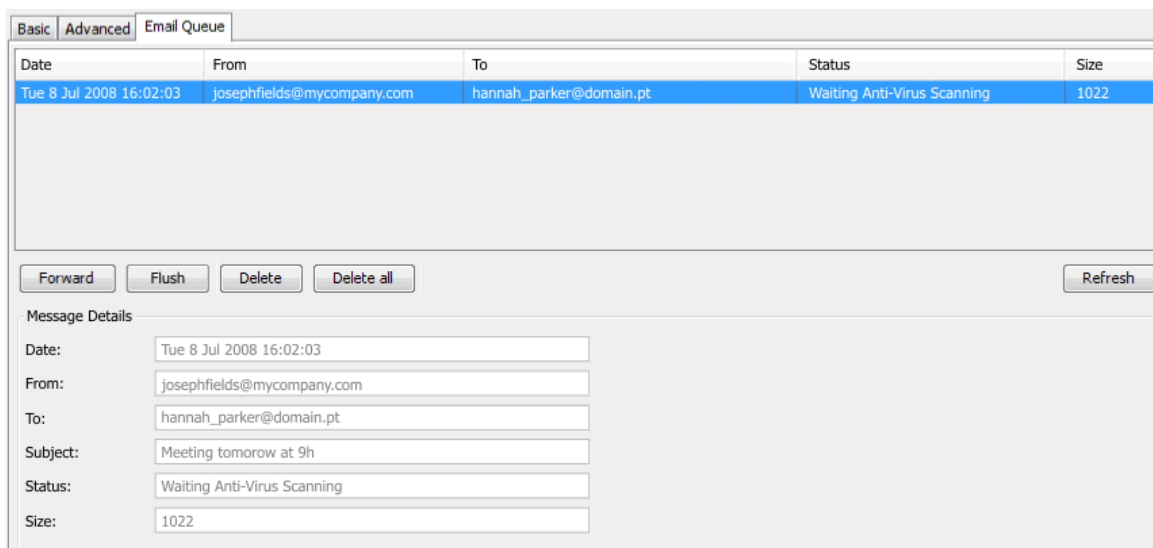
this change effective.



The 'Email Aliases' dialog box features a title bar with a close button. It contains an 'Alias:' text input field. Below it is a section titled 'Email Addresses' which includes a large, empty list box with the header 'Email'. At the bottom of this section is an 'Email(s):' text input field. Below the input fields are two buttons: 'Add' and 'Delete'. At the very bottom of the dialog are 'OK' and 'Cancel' buttons.

9.2.3 Email Queue

View **incoming and outgoing emails** that edgeBOX mail server is processing **at the present moment**, and also **emails** that for any reason (having a destination email address invalid, for example) are **blocked in edgeBOX email server**.



The 'Email Queue' interface has three tabs: 'Basic', 'Advanced', and 'Email Queue'. The 'Email Queue' tab is active, displaying a table with the following data:

Date	From	To	Status	Size
Tue 8 Jul 2008 16:02:03	josephfields@mycompany.com	hannah_parker@domain.pt	Waiting Anti-Virus Scanning	1022

Below the table are buttons for 'Forward', 'Flush', 'Delete', 'Delete all', and 'Refresh'. A 'Message Details' section is located at the bottom, showing the following information:

Date: Tue 8 Jul 2008 16:02:03
From: josephfields@mycompany.com
To: hannah_parker@domain.pt
Subject: Meeting tomorrow at 9h
Status: Waiting Anti-Virus Scanning
Size: 1022

▼ **Forward an email**

You can forward emails that are on the queue to another receiver. This can be very useful when, for example, an email is blocked on the queue because its destination email is invalid.

To forward an email to another receiver:

1. Select the desired email from the emails list and click Forward.
2. In the dialog windows that pops up indicate the email address of the new receiver.
3. Click OK.

▼ **Delete an email**

1. Select the desired email from the emails.
2. Click Delete.

▼ **Flush the list of emails**

Every 10 minutes edgeBOX tries to deliver all incoming and outgoing emails that are on the Email Queue. You can force edgeBOX to try to deliver them right away by clicking on the Flush button.

10 Users and Accesses



In the Network Access Control (NAC) menu you can manage users and restrict access to the network.

- [Add or remove users](#)
- [Have a local administrator of edgeBOX](#)
- [Configure access profiles](#)
- [Manage and authenticate users remotely](#)
- [Use groups of users](#)
- [Personalize the appearance of the login page](#)

10.1 Add or remove users

Here is where you can manage the users of your network and control access to the services your network offers (the services that are running on the edgeBOX).

You can allow everyone to use your network and the network services, or just let specific users use it. [Why just let specific users use it?](#)

It gives your network more security - If you have user authentication turned on, access to the network and the services will be granted only if the user makes a successful login into the edgeBOX.

It allows you to have additional services - Services that you can't have if you don't have users because these services need user accounts to work. Examples: home directories, mail boxes, etc.

To let only specific users access the network, you need to manage (create, edit and delete users) them and configure the way they should authenticate (log in) in the network.

By default, edgeBOX has already two users created. You can use them to view how they are configured and to do quick experiments, for example user authentication to access the network services. Their usernames are "user" and "user2". The passwords of both of them is "password".

▼ [Create a new user of the network](#)

To create a new network user in the edgeBOX:

1. Click **New** bellow list of existing users of the List sub tab of the Users tab.
2. In the New User window indicate a **username** for the user in the Username field. The username will be used by the user to login to the network. [How must the username be?](#)

The username must be between 3 and 20 characters long, has to start with a non-numeric character and cannot contain spaces, nor special characters like | \ / : * ? ! < > \".

3. Type the **first and the last names** of the user in the First Name and Last Name fields.
4. Select the **access profile** this user will belong to from the Access Profile drop down list. The access profile indicates the network privileges for a group of users, like the services they can use or the type of internet access they have. [What if the Access Profile drop down list is empty?](#)
 If the drop down list is empty, it means you have not created any Access Profiles. Leave this option as it is and continue to the next below. When you will click the OK button and save this user, edgeBOX will create a profile named generic and will give this user that profile.
5. Type a desired **password** for the user in the Password field. As the username, the password will be used by the user to login to the network if the authentication will be mandatory.
6. Check **one or more** services that the user **will be able to use**:
 - **Regular Services** - gives access to regular network services. Allows the user to **use the common services** that are **running on edgeBOX** like internet, email (POP3 and SMTP) or file transfer (FTP).
 - **PPTP/VPN** - allows to **connect to the local network when outside the office**. Connect to the network, using a secure tunnel (VPN), and use the network services (e.g. see emails or access documents on the home directory or on shared folders) from a remote place, as if being on the office.
 - **802.1x** - access to port based authentication devices. This includes access through a wireless access point or compatible switches. If you are using a secure authentication (802.1x) on your wireless and/or network you can allow the user to access the network.
 - **Windows Use** - allows the user to access **file and printers sharing**, or to use edgeBOX's PDC and WINS Server functionalities.
7. If you wish this user will be able to make calls (VoIP) and have his VoIP phone, check the option VoIP (note that doing this creates a phone extension, as if you were creating it in the phone extensions list of the [VoIP and IP-PBX](#) section). Indicate the following information:
 - **Extension Number** - the extension of the phone.
 - **Extension Password** - the password used to register.
 - **Authentication Pin** - the pin to be entered if the IP-PBX authentication is turned on, to check which type of calls the user has permission to make.
 - **Permissions** - the type of calls the user is allowed to make. Each of these types include its predecessors, so Long distance calls include Local calls, Mobile calls include both Long distance calls and Local calls, and so on.
8. Click the OK button to save the new user to the list.

▼ [Import users from a CSV file](#)

You can add a large number of network users to the edgeBOX by importing them from a CSV file in your computer.

1. Go to the Import sub tab of the Users tab in the NAC section.
2. Click the Browse button to open a select file dialog box.
3. Select the CSV file from your computer. [How must the information be arranged in the CSV file?](#)
 - The information in the file must be in the format: user;password;realname. Realname means "firstname lastname". One user per line.
 - If a user has no password, a random password will be generated. It can be changed later on.
4. Select the access profile you wish to give to all the imported users in the Destination Access Profile drop down list.
5. If you wish to delete **all the current network users** in the edgeBOX before importing the users of the file, **check** the option Purge Existing Users.
6. If a user of the file you are importing already exists in the list of the network users, check the option Replace Passwords On Existing Users if you wish that the password from the file, replaces the existing password.
7. Click the Upload button to upload the CSV file to the edgeBOX and import the users to the list of network users (importing the users may take a few minutes, please wait).

**About importing users:**

- You can only import users **if you are managing the network users on the edgeBOX**, that is, if you are not using Remote Authentication, as a LDAP server, for instance.
- If you try to **import more users than** the users you can have in the edgeBOX, according to **your license**, only the first users will be imported. When the license user limit is reached, the remaining users in the file are not imported.
- Make sure you have the service FTP allowed on the [firewall](#) when importing the users because the upload of the CSV file is made via FTP.

▼ [Edit the information of a user](#)

If you wish to edit some information of a user:

1. Go to the List sub tab of the Users tab in the NAC section.
2. Select the user from in the list of users and click the Edit button below the list.
3. In the user properties window that pops up, edit the desired information. If you do not want to change the password of the user, leave the password fields blank as they are.
4. Click OK to save the changes you made.

▼ [Delete a user](#)

To delete a network user from the edgeBOX:

1. Go to the List sub tab of the Users tab in the NAC section.

2. Select the user from in the list of users and click the Delete button below the list.
3. A confirmation message will appear. Click Yes if you really want to delete the selected user.

▼ Change the access profile of a user

The access profile of a user defines the services on the network he can access, like Internet, email, or VPNs. [About Access Profiles...](#)

To change the access profile of a user:

1. Go to the List sub tab of the Users tab in the NAC section.
2. Select the user from in the list of users and click the Edit button below the list.
3. In the user properties window that pops up, select the new access profile from the access profiles available in Access Profile drop down list.
4. Click OK to save the changes you made.

▼ Create an (VoIP) Phone Extension for a user

If you want to create an extension for a user, so the user can make (VoIP) phone calls:


1. Go to the List sub tab of the Users tab in the NAC section.
2. Select the user from in the list of users and click the Edit button below the list.
3. In the user properties window that pops up, check the option VoIP and indicate the following information:
 - Extension Number - the extension of the phone.
 - Extension Password - the password used to register.
 - Authentication Pin - the pin to be entered if the IP-PBX authentication is turned on, to check which type of calls the user has permission to make.
 - Permissions - the type of calls the user is allowed to make. Each of these types include its predecessors, so Long distance calls include Local calls, Mobile calls include both Long distance calls and Local calls, and so on.
4. Click the OK button to save the information entered and create the new extension.

▼ Add or remove a user from one or more groups

Groups are applications integrated with the edgeBOX like Moodle or OpenCMS. A user can belong to one or more Groups. [Working with Groups...](#)

To manage the groups a user belongs to:

1. Go to the Groups tab of the NAC menu.
2. Select the user you want to manage from the Users list (the bottom list) and click the Edit button below the list. A dialog window will appear with all the existing groups and indication of which groups the user belongs to.
3. Check the new groups you want the user to belong to and uncheck the groups you don't want the user to belong to anymore.
4. Click the OK button to save.

 **If you reach the maximum number of users your licence offers, you won't be able to add or import any more users.**

To create or import new users on the edgeBOX you need to delete existing users first or upgrade your edgeBOX solution. [See details about the different edgeBOX solutions in edgeBOX's website.](#)

Related Topics:

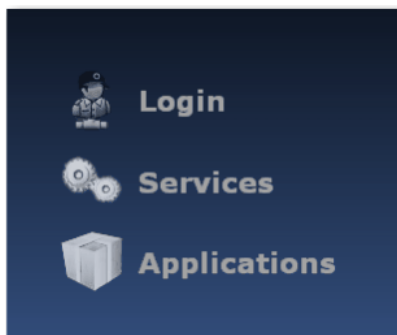
- [Manage and authenticate users on a remote server](#)
- [Configure access profiles for the users](#)
- [Add users to groups for edgeBOX's integrated applications](#)

10.2 Have a local administrator of edgebox

The local administrator is one of the users of your local network that you give the permission to manage parts of your network and configure some of your services; that is, that can access some sections of the edgeBOX web interface. [How can local admin user access the edgeBOX web interface?](#)

To have access to the edgeBOX, the local administrator has to:

1. Go to a **computer of the local network** (LAN).
2. With a browser, open the webpage <https://myedgeBOX.com>.
3. After the page opens, click the **link Login**.



edgeBOX initial page

4. Type the username and password he uses to authenticate to the network.
5. Click the **Login** button.

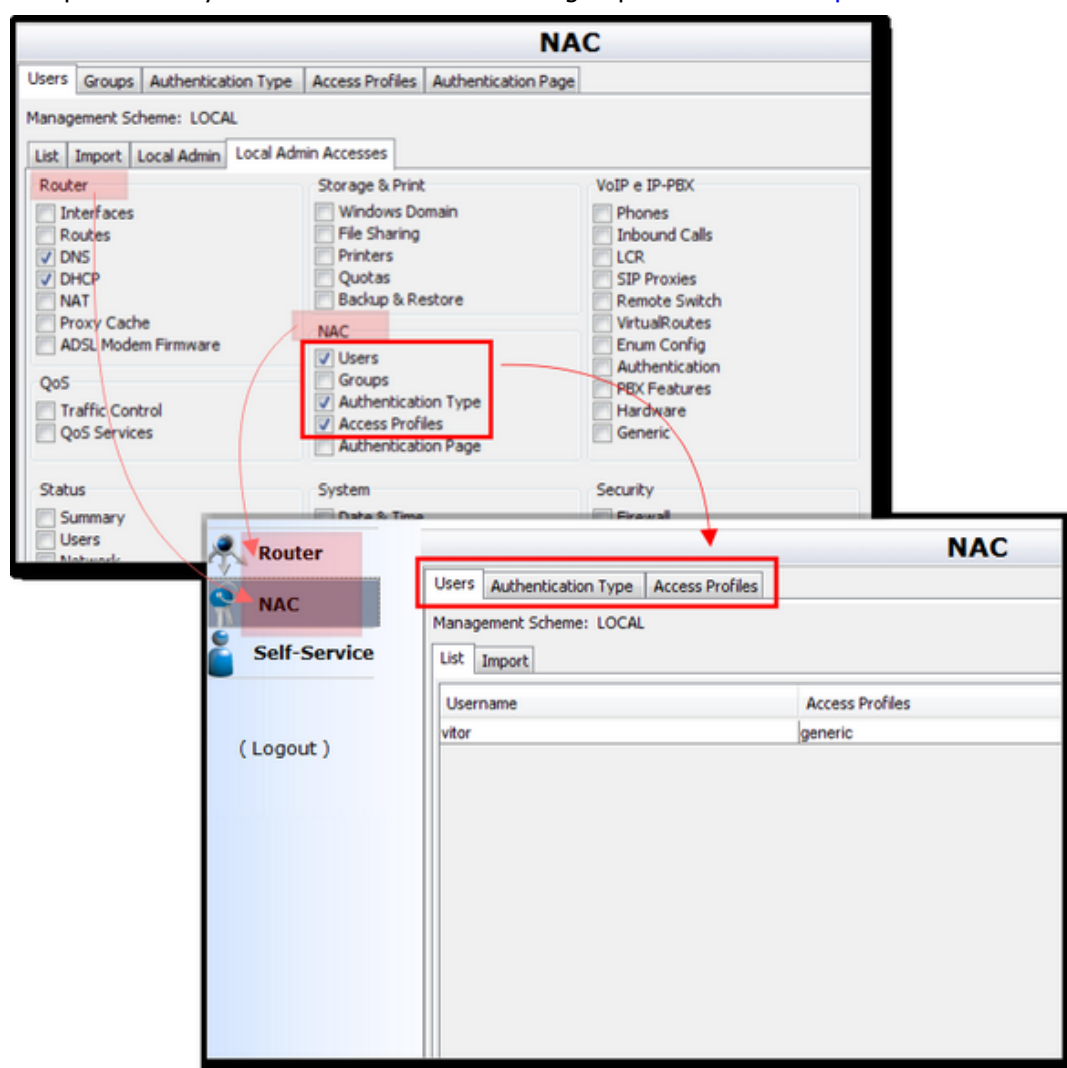
▼ [Create a local administrator of the edgeBOX](#)

To make a user of your network local administrator:

1. Go to the Local Admin sub tab of the Users tab in the NAC section.
2. Type the username of the user of your network you want to be the local administrator in the New Local Admin field. If you do not remember the username of the user you can see it in the list of users that is in the previous sub tab (List sub tab).
3. Click the Change button. If the username exists, the operation will be successful and the username will appear in the Local Admin field.

Now you need to indicate the areas and functionalities of the edgeBOX the local administrator will have access:

1. Go to the next sub tab (the Local Admin Accesses sub tab).
2. Check the areas you want the local administrator to have access. Each section (main menu option) of the edgeBOX is represented by a group and each tab of each section is represented by the check buttons inside the groups. [View an example](#)



As shown in the images above, when the local administrator will access the web management interface of the edgeBOX, he will only have available the menu items where there are functionalities he is allowed to administrate. In the example, the

Router and NAC sections because the administrator gave him permission to administrate functionalities that are inside those sections.

And when the local administrator enters one of the section he will only see the tabs (areas) he has permissions to administrate. The other tabs of the section will not be visible to him.

3. Click the Apply button in the bottom right side of the sub tab to save the changes.

▼ Change the local administrator

To change the user that is the network local administrator:

1. Go to the Local Admin sub tab of the Users tab in the NAC section. You can see the username of the current local administrator in the Local Admin label.
2. Type the username of the user of your network you want to be the new local administrator in the New Local Admin field. If you do not remember the username of the user you can see it in the list of users that is in the previous sub tab (List sub tab).
3. Click the Change button. If the username exists, the operation will be successful and the username will appear in the Local Admin field.

▼ Change the areas the local administrator can manage

To change the areas and functionalities of the edgeBOX the local administrator has access:

1. Go to the Local Admin Accesses sub tab of the Users tab in the NAC section. The options that are checked are the areas the local administrator has access currently.
2. Check the new areas you want the local administrator to have access.
3. Click the Apply button in the bottom right side of the sub tab to save the changes.

▼ Remove the local administrator

If you don't want to have a local administrator of the network:

1. Go to the Local Admin sub tab of the Users tab in the NAC section. You can see the username of the current local administrator in the Local Admin label.
2. With the New Local Admin text field empty, click the Change button. The username of the local administrator will disappear from the Local Admin label, which means that the operation was successful.



If you restore an old backup, the local administrator will not change.

edgeBOX has a backup and restore option that allows you to make backups of all the configurations and data. However, for security reasons **local administrator settings are not saved in edgeBOX backups**. [View example](#)

For example, if your local administrator was 'john_simmons' and you made a backup of the edgeBOX at that time, and a some time later you changed the local administrator to 'david_parker', and now you restore that old backup you made, **your local administrator will still be 'david_parker'**.

10.3 Configure access profiles

Profile configuration will be covered in this section. We will see the items available for configuration that will form a policy to apply to members of the profile.

Name	Internet Access	Service Access	DMZ Access
generic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

New Edit Delete

On this page is a list of profiles and their access to the services running on the box, to the Internet and to the DMZ network. If the cell is unchecked then the members of the profile have no access to this resource; if the cell is checked then the profile members have some level of access to this resource.

▼ Create a new access profile

To create a new access profile:

1. Go to the Access Profiles tab of the NAC section.
2. Click New below the list. A dialog window will appear.
3. Type the name you want to give the new access profile in the Access Profile field and click OK to save the new profile to the list. [How must the name be?](#)

The name must have between 2 and 8 characters, has to start with a non-numeric character and cannot contain spaces, nor special characters like | \ / : * ? ! < > `.
4. Select the created access profile in the list and click the Edit button below the list. A window that will allow you to configure all of the properties of the access profile will appear. You can configure properties for:

- [Internet Access](#)
- [Network Services Access](#)
- [User Sessions](#)
- [VLANs](#)
- [Other](#)

5. Click OK to save all the properties entered.

▼ [Add users to an access profile](#)

1. Go to the List sub tab of the Users tab in the NAC section.
2. Select the user from the list of users and click the Edit button below the list.
3. In the user properties window that pops up, select the new access profile from the access profiles available in Access Profile drop down list.
4. Click OK to save the changes you made.

▼ [Edit an access profile](#)

If you wish to edit the properties of an access profile:

1. Go to the Access Profiles tab in the NAC section,
2. Select the access profile you want to modify and click the Edit button below. A properties window of the selected access profile will appear.
3. After you change the desired properties, click OK to save the changes you made.

▼ [Delete an access profile](#)

To delete an access profile go to the Access Profiles tab in the NAC section, select the access profile you want to delete from the list and click the Delete button below.



You can only delete an access profile if there are no users with that profile. If one or more users have the access profile you want to delete, you need to first delete those users or change their access profile to another access profile, and just then, delete the access profile.

10.3.1 Internet

This panel allows configuration of the Internet access options.

You can set both an upload class and a download class (for more details on quality of service, check [Traffic Control](#)). The default values are upBE and downBE, meaning all traffic will have the same priority. You can, however, choose from the lists to give the Internet traffic to and/or from this group a specified priority by selecting another value.

Access Profile Policy

Access Profile (generic)

Internet Services DMZ Access User Sessions VLAN Other

Quality of Service

Upload Class: upBE Download Class: downBE

☒ Allow Internet Access

Time Period

Start: Hours: 0 Minutes: 0

Stop: Hours: 23 Minutes: 59

Incoming

IP	Netmask	Port	Protocol

Add Delete

Outgoing

IP	Netmask	Port	Protocol

Add Delete

OK Cancel

Allow Internet Access

If this option is unchecked, members with this profile will not have access to the Internet, so the next panel will be disabled. If you check this option you may then fine-tune Internet access using the options available in the next panel. [View an example](#)

Time Period

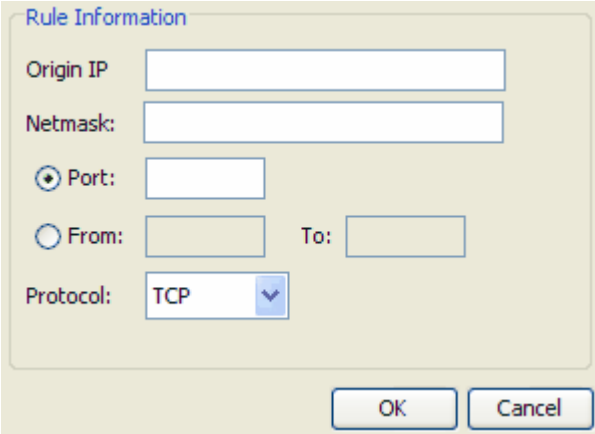
You can grant access for the whole day (the default) or just to a time interval. Insert the limits for this interval directly in the fields or using the up-down controls. It is not possible to allow access for a time period which spans midnight, as a user can only belong to one profile and the profile cannot be set to "overlap" midnight.

Incoming

By default all incoming traffic from the Internet is denied access to the internal network. With this option you can allow incoming traffic based on its origin, port and/or protocol. This table displays the list of allowed connections. The options available are "Add" and "Delete".

- ▼ [Create a new entry in the table](#)

After selecting "Add", a popup window similar to the one shown will appear requiring you to enter the following information:

A dialog box titled "Rule Information" with a light beige background. It contains several input fields: "Origin IP" (a text box), "Netmask:" (a text box), "Port:" (a radio button selected, followed by a text box), "From:" (a radio button unselected, followed by a text box), "To:" (a text box), and "Protocol:" (a dropdown menu showing "TCP"). At the bottom right are "OK" and "Cancel" buttons.

Rule Information

Origin IP:

Netmask:

☒ Port:

☐ From: To:

Protocol:

OK Cancel

- Origin IP: The IP address for the host/network which is starting the connection we want to allow;
- Netmask: The netmask to apply;
- Port: The service port we want to allow access to; this option will be disabled if the protocol chosen is either "ICMP" or "ALL";
- The Range check box allows a range of ports (using the From and To fields) to be specified for the incoming traffic.
- Protocol: Select from the list. Possible values are: TCP, UDP, ICMP and ALL.

After selecting "OK" you will also have to select "OK" in the main panel for changes to become effective.

▼ Delete an entry of the table

Deletes an entry from the table, denying traffic for this connection. After selecting the entry from the table, selecting "Delete" will remove it. You have to select "OK" in the main panel for changes to become effective.

Allowing incoming connections will only apply if NAT is not active for the external interface, i.e. the edgeBOX is working in pure router mode for this interface. If this is not the case, the internal network will not be visible from the outside and connections will always have to originate from the inside.

Outgoing

By default, all outgoing traffic is allowed, i.e. traffic originating from the internal network to the Internet is granted access. With this option we can deny outgoing traffic based on its destination, port and/or protocol. This table displays the list of connections denied. The options available are "Add" and "Delete".

▼ Create a new entry in the table

After selecting "Add" a popup window will appear requiring you to enter the following information:

- Destination IP: Host or network address which we want to deny connections to;
- Netmask: The netmask to apply;
- Destination Port: The service port we want to deny access to. This option will be disabled if the protocol chosen is either "ICMP" or "ALL".
The Range check box allows a range of ports (using the From and To fields) to be specified for the outgoing traffic.
- Protocol: Select from the list. Possible values are: TCP, UDP, ICMP and ALL.

After selecting "OK" you will also have to select "OK" in the main panel for changes to become effective.

▼ [Delete an entry of the table](#)

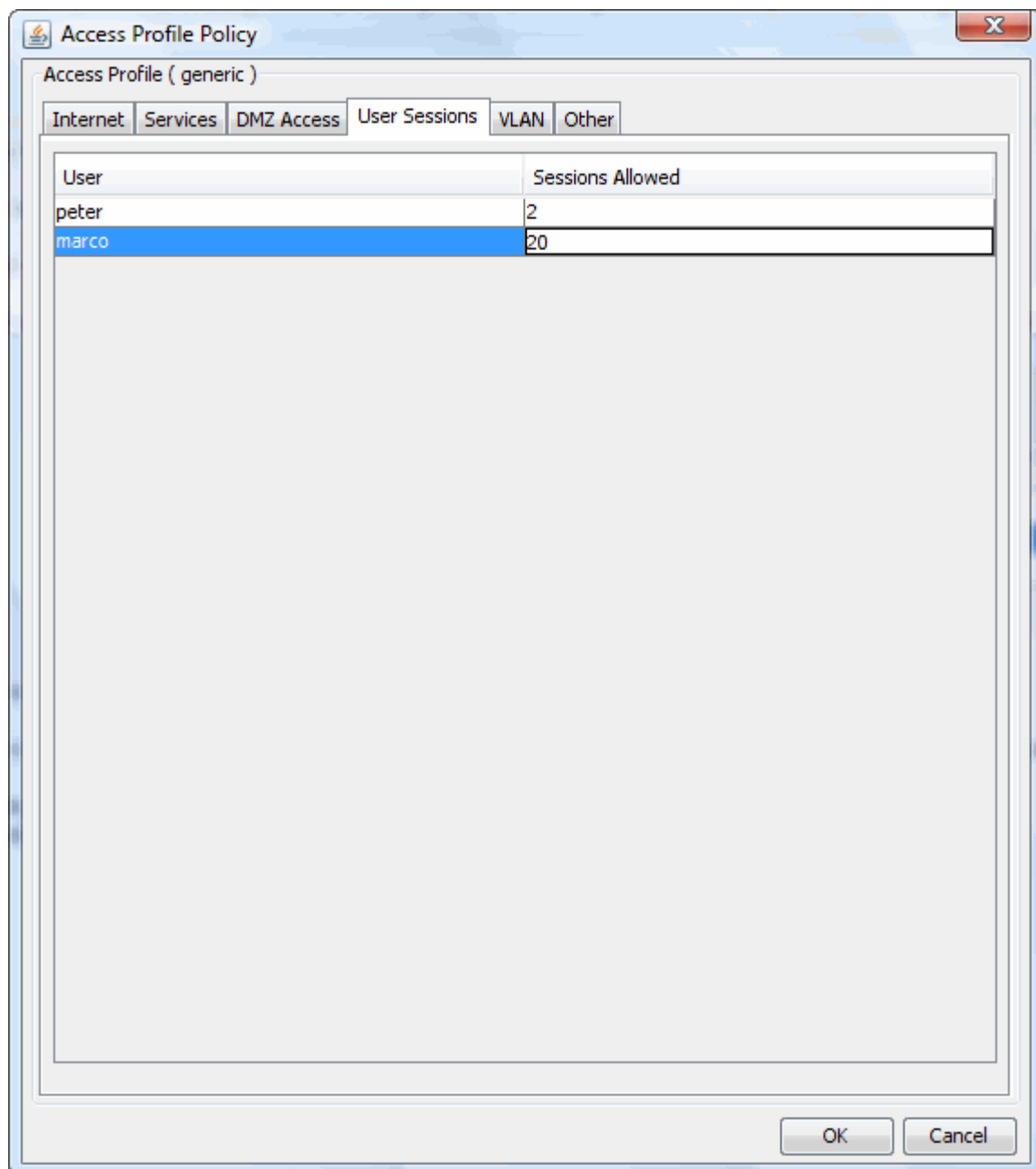
Deletes an entry from the table, allowing traffic for this connection. After selecting the entry from the table, selecting "Delete" will remove it. You have to select "OK" in the main panel for changes to become effective.

10.3.2 User Sessions

Allows you to Create, Edit or Delete a Profile.

If a Profile is deleted which is currently in use, the users of that profile are assigned to the profile generic. You cannot delete the generic profile. If you try to do so and refresh the panel, the generic profile remains

Note that the generic profile is created automatically when the first user is created, who does not have a profile specified.



If you edit a profile, a window similar to the one above is presented.

By double-clicking on the sessions (currently set at 2 for this user), you may alter the number of simultaneous sessions this user is allowed.

Note: Change the number of sessions and then **click to another cell**, before you press apply. yes it is online.

10.3.3 Services

In this panel we can configure the access options for the services. The items available for this option are:

Allow Service Access

If this option is unchecked members with this profile will not have access to the services running on the box and the next panel will be disabled. If you check this option you may then fine-tune service access using the options available in the next panel, which are described below.

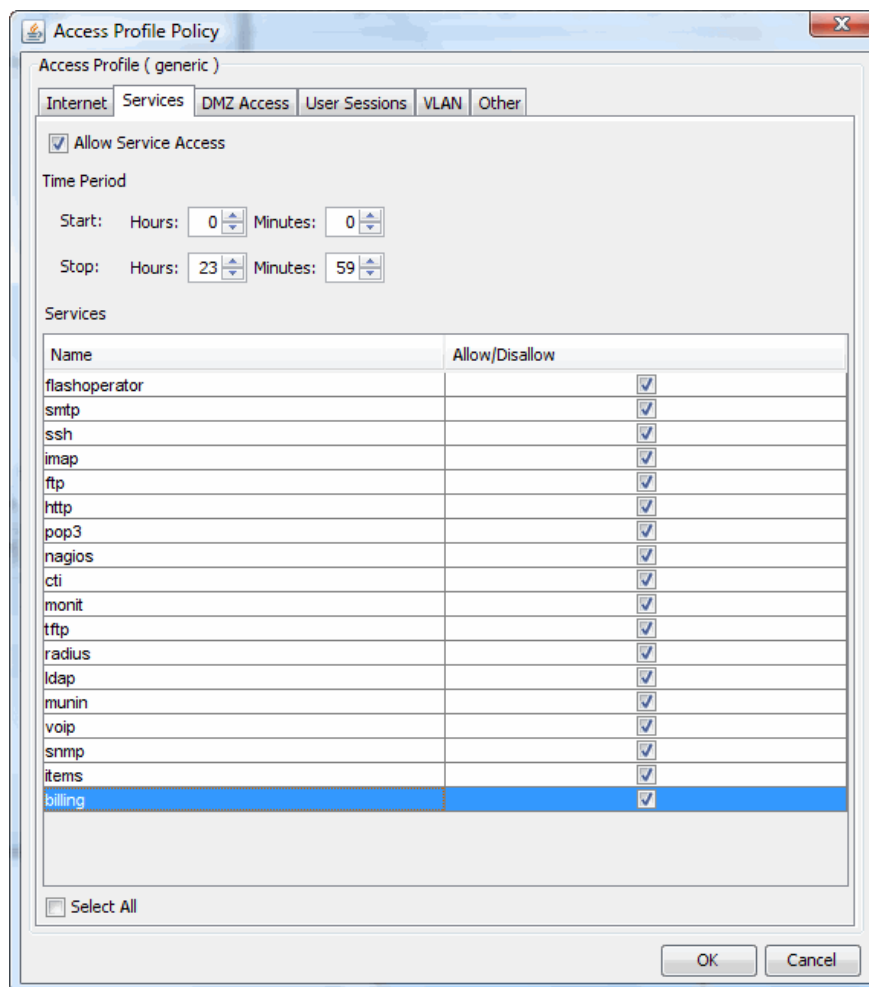
Time Period

You can grant access for the whole day (the default) or just to a time interval. Insert the limits for this interval directly in the fields or using the up-down controls.

Services

In this table you can choose exactly what services the profile members will be able to access. A check in the cell's service will grant access; not checking it will revoke access to it.

Note: These are services running on the edgeBOX. That is if you disallow ftp, the users in this profile group will not be able to access the edgeBOX ftp server, they will be able to access other ftp servers (as port 21 through the edgeBOX will NOT be blocked)



10.3.4 VLAN

This panel allows you to:

- Indicate that the users of this profile will belong to one of the available VLANs.
- Specify locations and ports/services the users will be able to access that by default they cannot access.

Indicate the VLAN the access profiles belong to

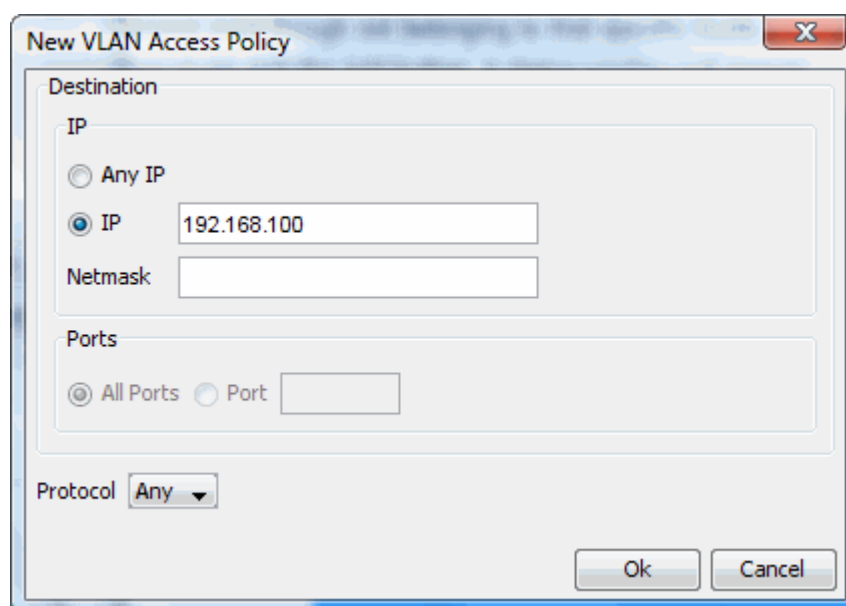
To indicate the VLAN the users of this Access profile belong to, select the desired VLAN from the VLAN Name drop down option. If you wish that the users of this access profile belong to the LAN network instead, select the option None from the drop down list. This option is relevant only when you have a switch or switches in your network infrastructure that support dynamic VLAN assignment. One of the supported L2 switches with this feature is the Procurve 2650. With this feature the switch will automatically move the switch port, where the user is connected and after

a successful 802.1x authentication, to this VLAN.

Add locations the users of the access profiles will access

By default, users in a given VLAN cannot communicate with users of other VLANs. This also includes destinations in the LAN. The LAN is also known as default VLAN. You can bound this VLAN characteristic by indicating exceptions, locations (services/ports) on other VLANs the users will be able to access even though not belonging to that specific VLAN.

To add an access permission to another VLAN click the Add button. A dialog window will appear.



The image shows a dialog box titled "New VLAN Access Policy". It has a close button (X) in the top right corner. The dialog is divided into several sections:

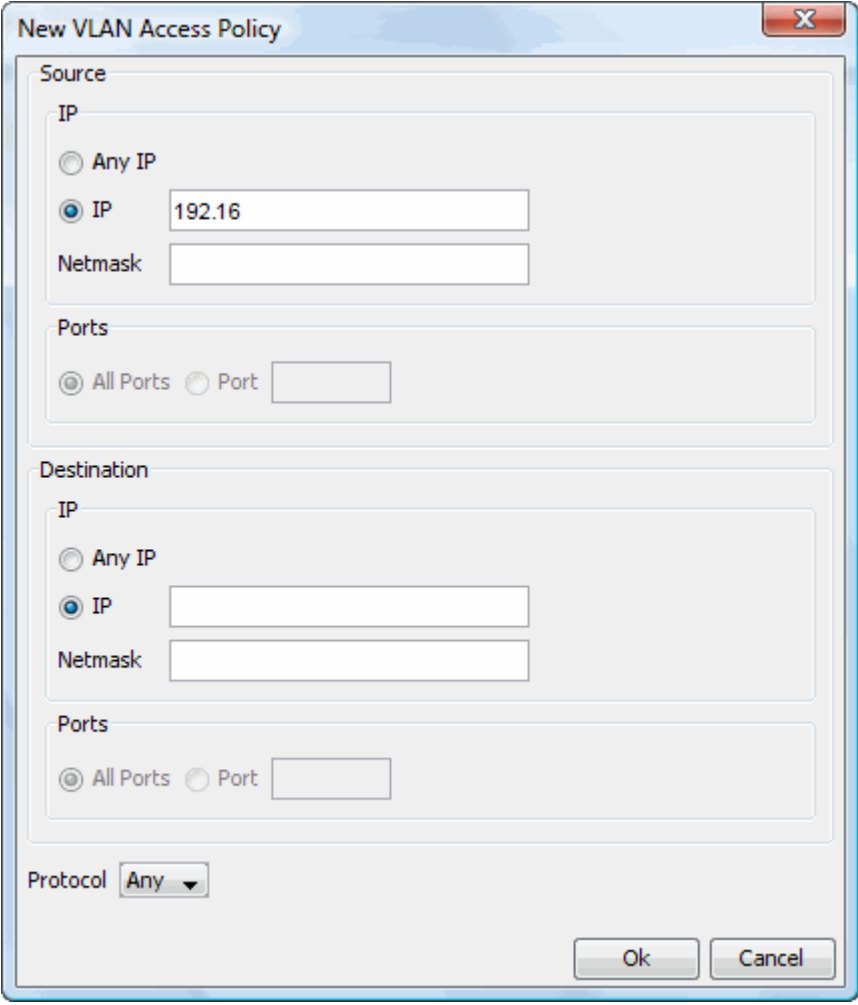
- Destination**: This section contains a group box labeled "IP". Inside, there are two radio buttons: "Any IP" and "IP". The "IP" radio button is selected. Next to it is a text field containing "192.168.100". Below this is a text field labeled "Netmask".
- Ports**: This section contains two radio buttons: "All Ports" (which is selected) and "Port". Next to the "Port" radio button is a text field.
- Protocol**: This section contains a dropdown menu currently set to "Any".

At the bottom right of the dialog are "Ok" and "Cancel" buttons.

The options available are:

- **Any IP** - Allow users to access all other VLANs.
- **IP** - Allow users to access a specific machine on another VLAN or even all computers of another VLAN. Type the IP address of the machine or of the VLAN.
- **Netmask** - Netmask of the machine or the VLAN typed in the IP field.
- **All Ports** - Allow users to access all services/port on the destination VLAN or machine.
- **Port** - Type just a specific port (service) that users will be able to access in the destination VLAN or destination machine
- **Protocol** - The type of communications the users are allowed to have with the destination machine or VLAN.

If the default profile is chosen, an extended panel is presented, which includes a Source panel:



The image shows a 'New VLAN Access Policy' dialog box. It is divided into two main sections: 'Source' and 'Destination'. Each section has an 'IP' subsection with radio buttons for 'Any IP' and 'IP'. The 'IP' option is selected in both, with text input fields for the IP address and a 'Netmask' field. Below the IP subsection is a 'Ports' subsection with radio buttons for 'All Ports' and 'Port', followed by a text input field. At the bottom of the dialog is a 'Protocol' dropdown menu set to 'Any'. 'Ok' and 'Cancel' buttons are at the bottom right.

Source

IP

☐ Any IP

☒ IP 192.16

Netmask

Ports

☒ All Ports ☐ Port

Destination

IP

☐ Any IP

☒ IP

Netmask

Ports

☒ All Ports ☐ Port

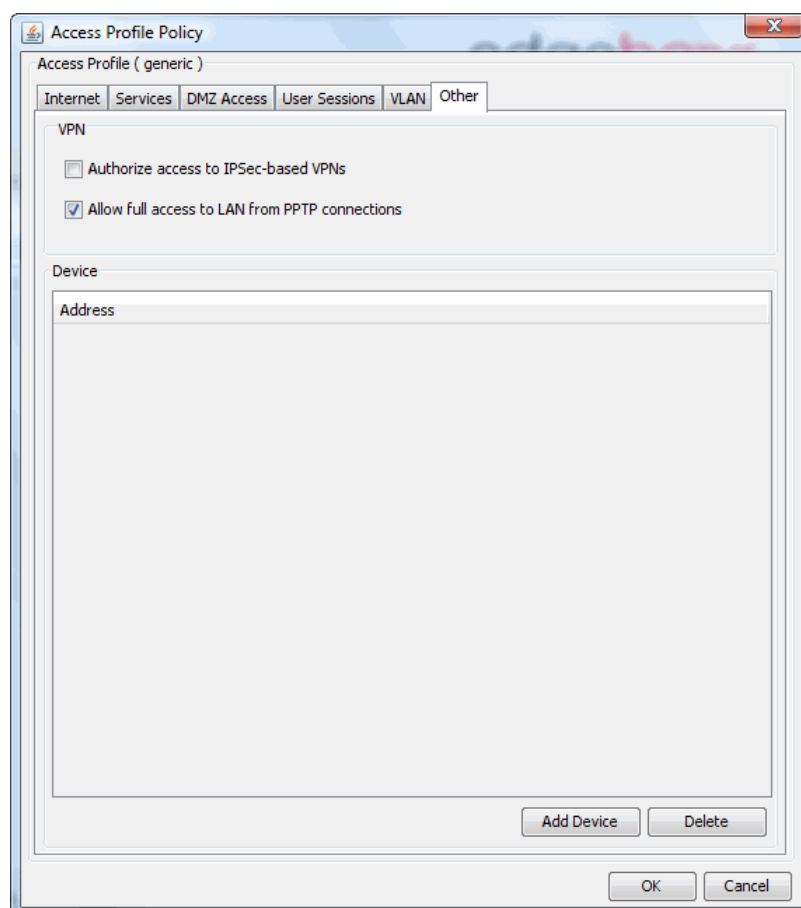
Protocol Any

Ok Cancel

10.3.5 Other

This Panel allows you to enter IP addresses, which will then be pre-authenticated, even though authentication is on. This is particularly useful for a server on the LAN or one of the VLANs.

Note: Devices on the DMZ, do not require authentication.



Allow full access to LAN from PPTP connections

If this option is enabled, the users in this profile when connecting through a PPTP VPN will have full access to the LAN.

Add a device or a range of devices

Besides containing users, a profile may also contain IP addresses. If an IP is added, that machine is allowed the access rights of the profile. This allows the machine to automatically authenticate with the edgeBOX, without the usual login screen. You can indicate a specific IP address of a machine or you can indicate a range of IP addresses. Indicating a range is most useful when you, for example, want all devices of a VLAN to be automatically authenticated.

10.4 Manage and authenticate users remotely

edgeBOX allows you to use remote user authentication. With remote authentication, users authenticate in a remote server instead of the edgeBOX when they try to login to the network.

You can authenticate users remotely using one of following types of servers:

- ▼ [Use a LDAP Server to authenticate the network users](#)

To authenticate users on a remote LDAP server:

1. Go to the Authentication Type tab on the NAC menu.
2. Choose Remote LDAP Server in the Authentication drop down option. A form to fill in the needed information to contact the remote server will appear below the drop down list.
3. Type in the required information so the edgeBOX can contact the server:
 - Type the IP address of the remote server in the Server IP field.
 - Indicate the LDAP domain configured in the Base Name field.
 - Type the edgeBOX LDAP client username and password that allows him to consult the LDAP Server in the LDAP Username and LDAP Password fields.
4. Check the Use for Authorization option if you wish to that the access privileges to the network services (Email, Internet, Secure connections, etc.) are always verified in the remote LDAP server and not locally in the edgeBOX.
5. Click the **Apply button** to save. Note that all existing users in the edgeBOX users' list will be deleted.




As users login for the first time, and their authentication is verified in the LDAP Server, their information is saved in the edgeBOX users list. Still, each time the users tries to login, the authentication will be done in the remote server.

▼ [Use a Radius Server to authenticate the network users](#)

To authenticate users on a remote Radius server:

1. Go to the Authentication Type tab on the NAC menu.
2. Choose Remote Radius Server in the Authentication drop down option. A form to fill in the needed information to contact the remote server will appear below the drop down list.
3. Type in the required information so the edgeBOX can contact the server:
 - Type the IP address of the remote server in the Server IP field.
 - Change the port used for authorization in the Server Port field if you don't want to use the default port, port 1812.
 - Type the edgeBOX radius client password that allows him to consult the Radius Server in the Password field. This Password is defined in the Remote Radius Server id the edgeBOX is in the list of clients of the server.
 - Change the default maximum amount of time that the edgeBOX waits for an answer of the Radius Server the value in the Timeout field if you don't want to use the default time period.
4. Check the Use for Authorization option if you wish to that the access privileges to the network services are always verified in the remote Radius server and not locally in the edgeBOX. [How to configure a Radius Server to perform users authentication and authorization?](#)
5. Click the **Apply button** to save. Note that all existing users in the edgeBOX users' list


will be deleted.


 As users login for the first time, and their authentication is verified in the Remote Radius Server, their information is saved in the edgeBOX users list. Still, each time the users tries to login, the authentication will be done in the remote server.

▼ Use an AD Server to authenticate the network users

To authenticate users using a remote Active Directory server:

1. Go to the Authentication Type tab on the NAC menu.
2. Choose Remote AD Server in the Authentication drop down option. A form to fill in the needed information to contact the remote server will appear below the drop down list.
3. Type in the required information so the edgeBOX can contact the server:
 - Type the IP address of the remote server in the Server IP field.
 - Indicate the active directory domain configured in the Base Name field.
Use the syntax cn=Group,dc=domain,dc=domain. For example, if the group is Support and the domain is critical-links.com, then type in cn=Support,dc=critical-links,dc=com.
 - Type the edgeBOX AD client username and password that allows edgeBOX to consult the AD Server in the AD Username and AD Password fields.
Use the syntax cn=username for the username. For example, if the username is joseph, type in cn=joseph.
4. Check the Import Users option if you wish to copy the information of the users that is in AD Server the to the edgeBOX's list of users.
5. Click the Apply button to save. Note that all existing users in the edgeBOX users' list will be deleted.

 As users login for the first time, and their authentication is verified in the Remote AD Server, their information is saved in the edgeBOX users list. Still, each time the users tries to login, the authentication will be done in the remote server.

 When you are using **remote LDAP or remote AD authentication**, the network users have first to login one time using the LAN user authentication before they can **login in the domain for the first time**.

Reset edgeBOX to local user authentication

Local authentication means that you manage the users of your network on the edgeBOX. It means that you create users giving them usernames and passwords and setting what services each can access in the edgeBOX. It also means that, when they are forced to login, when they try to access the services of your network, the login is verified in the edgeBOX.

Local user authentication is the default authentication scheme of the edgeBOX so if you didn't make any changes, it is the method you are using. If you changed to remote authentication and

you want to reset to local authentication:

1. Click the **NAC** menu.
2. Go to the **Authentication Type** tab.
3. Choose the **Local Server** option on the Authentication
4. Click the **Apply button** to save the change.

Related Topics:

- [Details about edgeBOX's authentication architecture](#)

10.5 Use groups of users

You can use groups if you have edgeBOX third-party applications; edgepacks. [What are edgepacks?](#)

EdgePACKs are optional modules for edgeBOX that add functionalities for particular markets or add a new set of features. Some examples are: eGroupWare, Moodle or Open CMS, among others. [Learn more details about edgepacks at edgeBOX's website.](#)

Groups have no direct use in the edgeBOX or the network. If you want to create groups of users that have different privileges and types of accesses in your network, you need to use [Access Profiles](#) instead.

▼ [Create a new group of users](#)

To create a new group of users:

1. Go to the Groups tab in the NAC section.
2. Click the New button below the Groups list. A dialog window will appear.
3. Type the name you want to give the group of users you are creating in the Group field and click OK to save the group to the list. [How must the name be?](#)
The name has to start with a non-numeric character and cannot contain spaces, nor special characters like | \ / : * ? ! < > `.
4. Select the created group in the top list and click the Edit button below the list. A window that will allow you to add users to the group will appear. The window displays all the users of your network.
5. Check the users you want to belong to the group from the list of network users. Check the Select All option if you wish to add all network users to the group.
6. Click OK to save the checked users to the group.




You can add a user **to more than one group** or not having him in any group at all.

▼ [Add or remove users from a group](#)

To add or remove users from a group:


1. Go to the Groups tab in the NAC section.
2. Select the desired group in the top list and click the Edit button below the list. A window that will allow you to add and remove users from the group will appear. The window displays all the users of your network. Checked users are the users that belong to the group.
3. Check the users you want to add to the group from the list of network users and uncheck the users you do not want to belong to the group anymore.
4. Click OK to save the changes you made.

 You can add a user to a group even if he already belongs to another group because users can belong to more than one group.

▼ Delete a group

To delete a group:

1. Go to the Groups tab in the NAC section.
2. Select the group to delete in the top list.
3. Click the Delete button below the list.

 When you delete a group you **do not delete** the users that belong to it. You only delete the group.

Notice also that, if a user only belongs to one group and you delete that group, the user may not be able to use some edgeBOX's third-party applications if a group is required because he will not belong to any group.

Related Topics:

- [Add or remove users](#)

10.6 Personalize the appearance of the login page

Personalize several aspects of the appearance of the login page the local users of the network will use to authenticate.

- Personalize **just some properties of the default page**, like the logo or the disclaimer message;
- Or **completely modify the look & feel of the page** by uploading your own HTML, CSS and image files.

Customize the default login page

Change the logo, the disclaimer message or the notice text of the default login page.

▼ [Insert or change your company logotype](#)

To display your company logo in the login page:

1. Select the Default option from the drop down list on the top of the tab.
2. Click the Browse button. It will open dialog window to select the logo from your computer.
3. Select the image with the logo from your computer. All most common image formats are supported.
4. Click the Upload button save the image to the edgeBOX.

To change the logo, do the same process. The image will be replaced by the new uploaded image.



You need to **check the properties of the edgeBOX firewall** before uploading the image because **the firewall may be blocking file transfers**. To allow file transfers allow the service FTP on the firewall.

▼ [Remove your company logo and restore the original logo](#)

If you wish to to remove your logo from the login page, **select the Default option** from the drop down list on the top of the tab and **click the Restore Default Logo button**. It removes your logo and restores the edgeBOX logo in the login page.

▼ [Show a message below the login form \(Notice\)](#)

To show a message bellow the login form (a Notice) of the login page:

1. Select the Default option from the drop down list on the top of the tab.
2. Type the desired text in the Notice text area.
3. Click the Upload button bellow the Disclaimer text area to save.

You you wish to remove the notice, clear all the text in the Notice text area and click the Upload button bellow the Disclaimer text area to save.

▼ [Change the disclaimer message on the bottom of the page](#)

The disclaimer message is the text that appears on the bottom of the login page. To change the text:

1. Select the Default option from the drop down list on the top of the tab.
2. Replace the existing text in the Disclaimer text area by your desired text.
3. Click the Upload button bellow to save.

If you do not wish to have any disclaimer, clear all the text in the Disclaimer text area and click the Upload button bellow to save.

View the changes

To view the changes and the appearance of the login page, go to a computer of the local network,

open a web browser, and type and try to open a random website. The new login page with the changes you made will appear.


Use a custom login page

Completely modify the look & feel of the login page by uploading your own HTML, CSS and image files.

▼ Upload the files for a custom login page

You can upload the files for your custom login page to edgeBOX to have a login page with a completely different appearance. To do so:


1. After creating your HTML file, your CSS file(s) and your images, **create a Zip file (.zip)** with all these files. [Show the requirements of the files.](#)
 - The zip file can contain image files, one or more CSS files and **one html file only**.
 - The zip file can not contain any folders or sub folders. All files must be all at the same level, that is, directly inside the zip file.
 - You must include the code `<!--AUTHENTICATION--!>` in the place where you want the login form to be placed in the HTML file. This code will then be replaced by the necessary code for the login form.
2. Select the Custom option from the drop down list on the top of the tab.
3. Click the Browse button and select the Zip file from your computer in the dialog window.
4. Click the Upload button to upload the zip file to the edgeBOX
5. When the upload process is finished, click **Preview to see how the page will look like**.
6. If the page is OK to you, click the Apply button to save the change and make this custom page the new login page.

 You need to **check the properties of the edgeBOX firewall** before uploading the Zip file or before previewing the page, because **the firewall may be blocking file transfers**. To allow file transfers allow the service FTP on the firewall.

▼ Download the files of the current custom login page

You you have a custom login page you can download the files of the page that are on the edgeBOX, so you can make changes and then upload them again to the edgeBOX. To do so:

1. Select the Custom option from the drop down list on the top of the tab.
2. Click the Download button, and save the zip file to your computer.

 You need to **check the properties of the edgeBOX firewall** before downloading the Zip file because **the firewall may be blocking file transfers**. To allow file transfers allow the service FTP on the firewall.



The users of the network only need to login in this page if you have the option Require

Users to Login activated in the firewall properties of the edgeBOX.

Related Topics:

- [Manage the firewall properties](#)

11 Reporting



View and export reports about edgeBOX's [System](#), [Services](#) and [Users](#).

For each report you can specify a Time Interval. It can be a begin/end day, a single day or hour, depending on the report you are seeing.

Time Interval

Begin Date: 2008-01-01

End Date: 2008-01-28

Apply

You can export the reports into a printable HTML page that you can print via a browser, or into a CSV file, for automated processing.

11.1 System

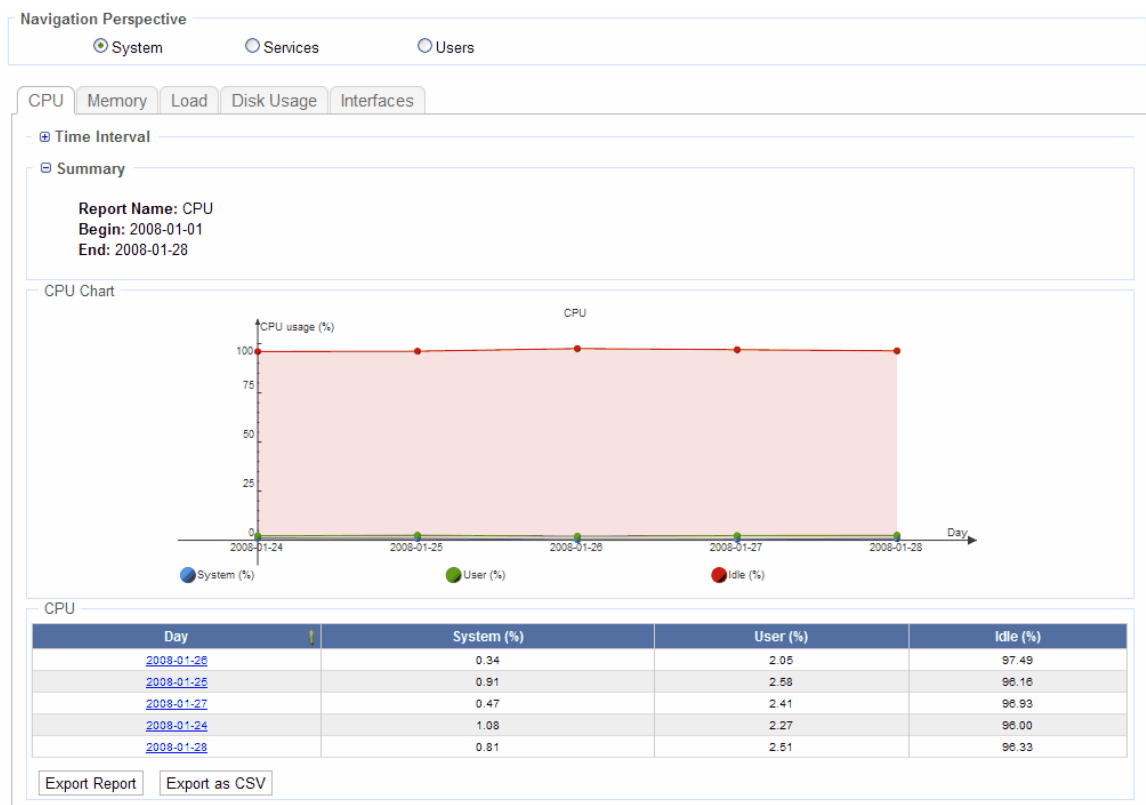
Displays information regarding edgeBOX's system usage:

- [CPU](#)
- [Memory](#)
- [Load](#)
- [Disk Usage](#)
- [Interfaces](#)

11.1.1 CPU

The CPU report shows **edgeBOX's processor usage, in percentage, per type of process: user's processes, system processes and idles.**

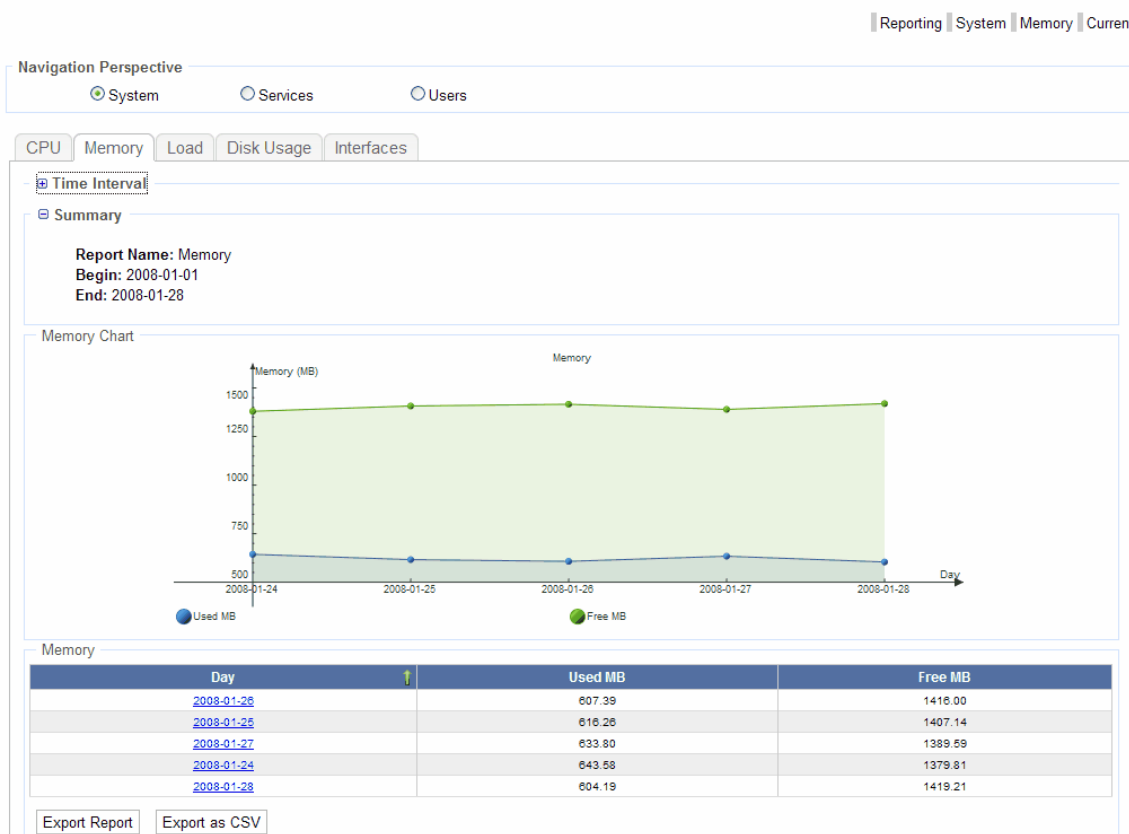
You can drill down each line into each day to view the CPU usage just for the selected day.



11.1.2 Memory

This report shows **used and free memory, in percentage**.

Drill down in each day to view the memory usage for that day only.

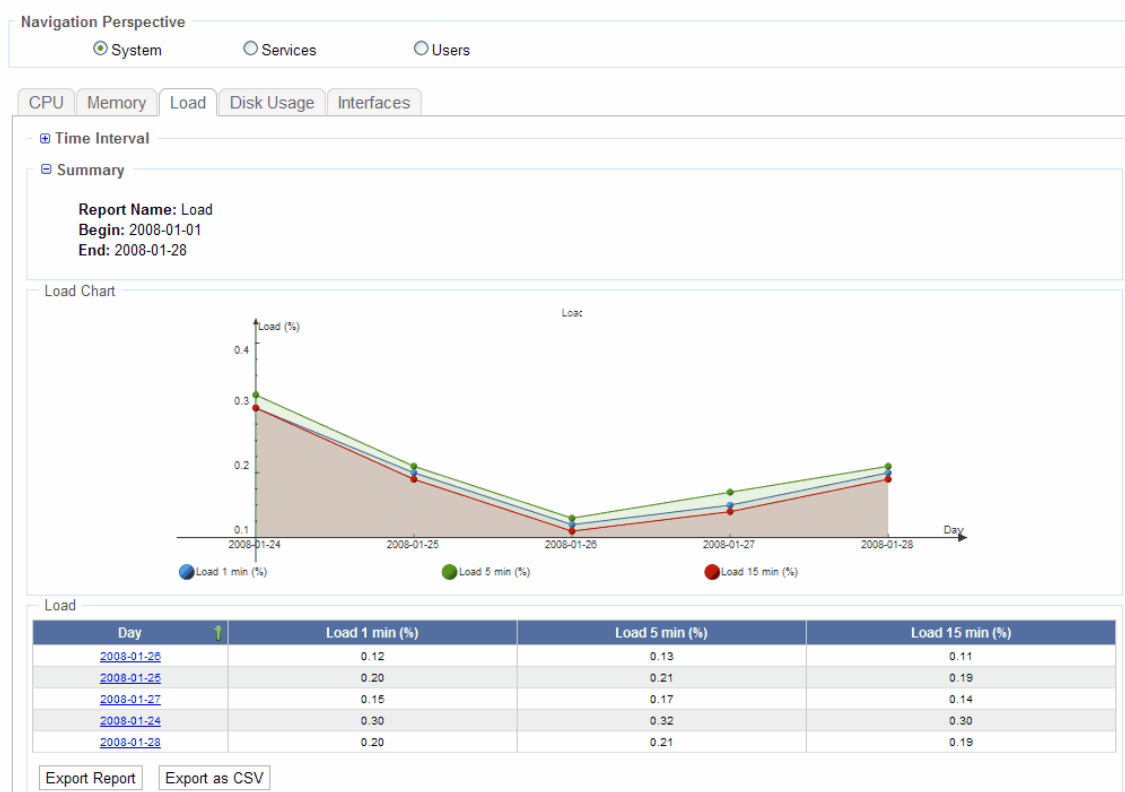


11.1.3 Load

The Load report displays **the load of the system through the number of active processes.**

Load 1 min (%) values indicate the active processes in one minute. Load 5 min (%) values indicate the active processes in 5 minutes. Load 15 min (%) values indicate the active processes 15 minutes.

Drill down into each day to view the load of the CPU for each day.

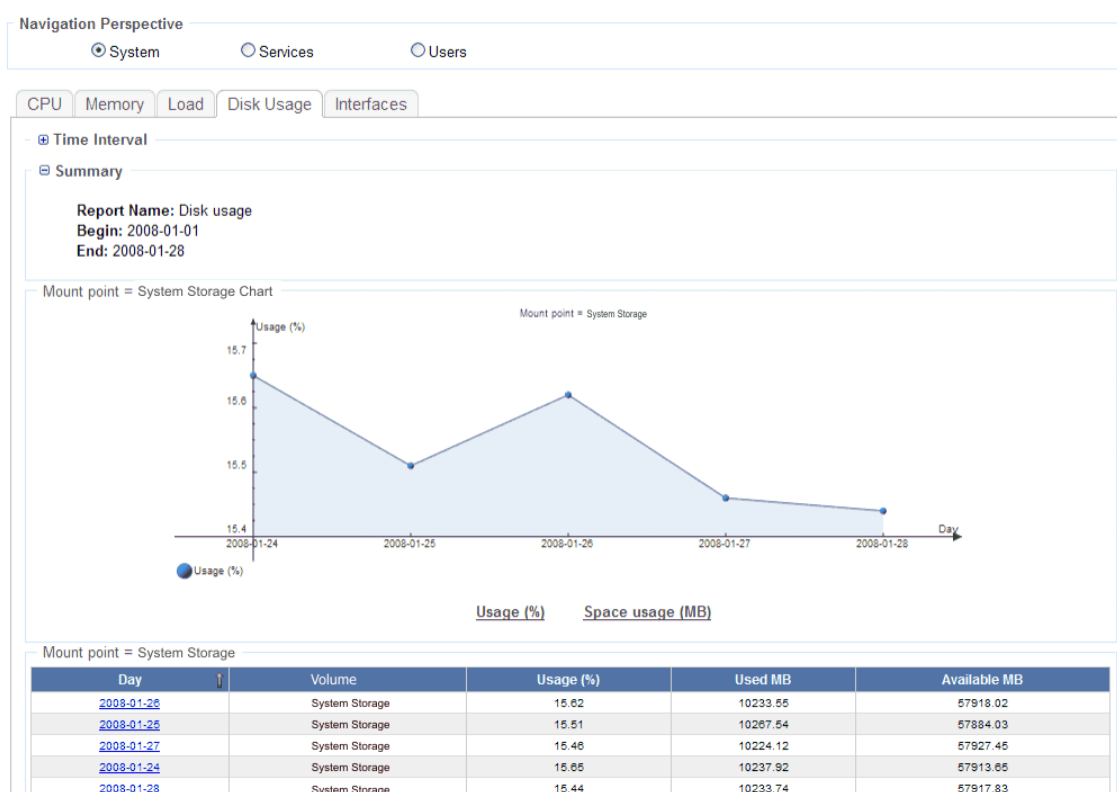


Values below 1 represent good CPU load, between 3 and 4 require you to monitor closely, and values over 5 require you to take action because the CPU is overloaded.

11.1.4 Disk Usage

This report displays the **hard disc usage, in percentage and in Mega Bytes**.

Scroll down to view disk usage for the other partitions. Drill down into each day to view the hard disc usage for that day only.

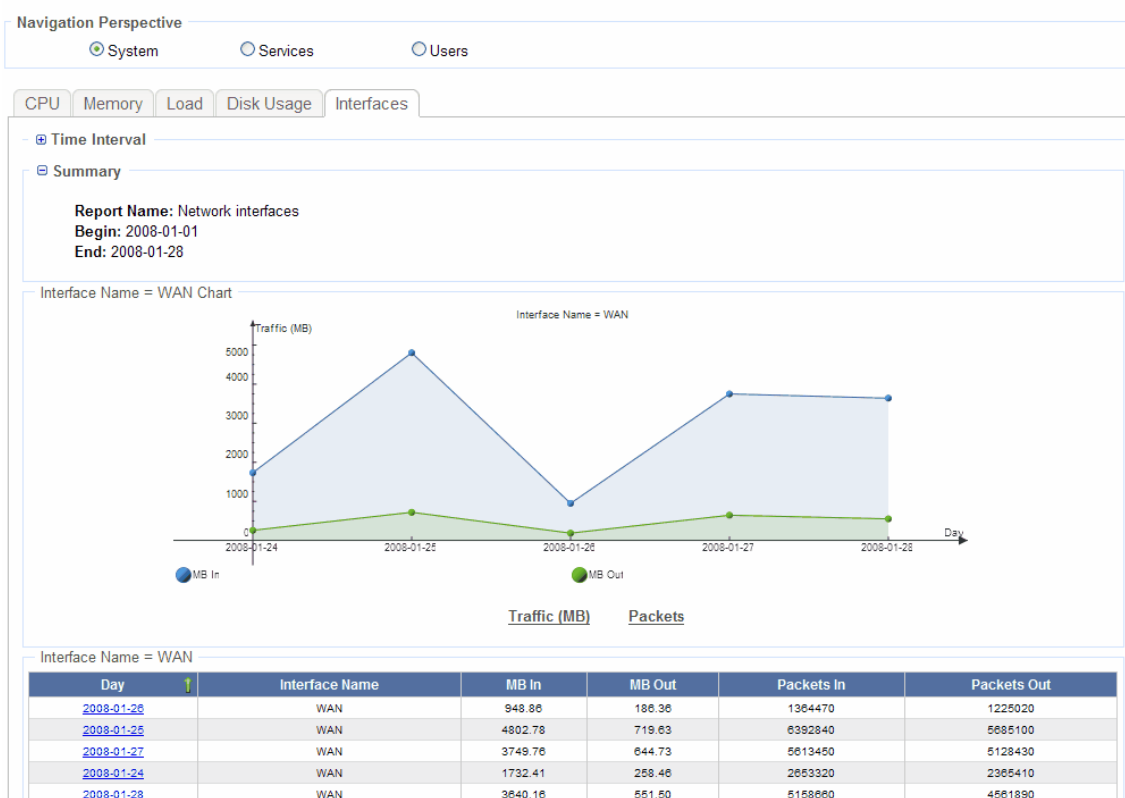


- The **System Storage** partition saves the **runtime system data information** (database, mail and log information).
- The **Home Storage** partition is used to save the **user account folders** and the **network shared folders** (Shares).

11.1.5 Interfaces

Shows the **traffic received and sent by edgeBOX in the WAN, LAN and DMZ interfaces**.

Drill down into each day to check the usage of the interface for that specific day. Scroll down to view information for the LAN and, if you have one, DMZ interfaces.



11.2 Services

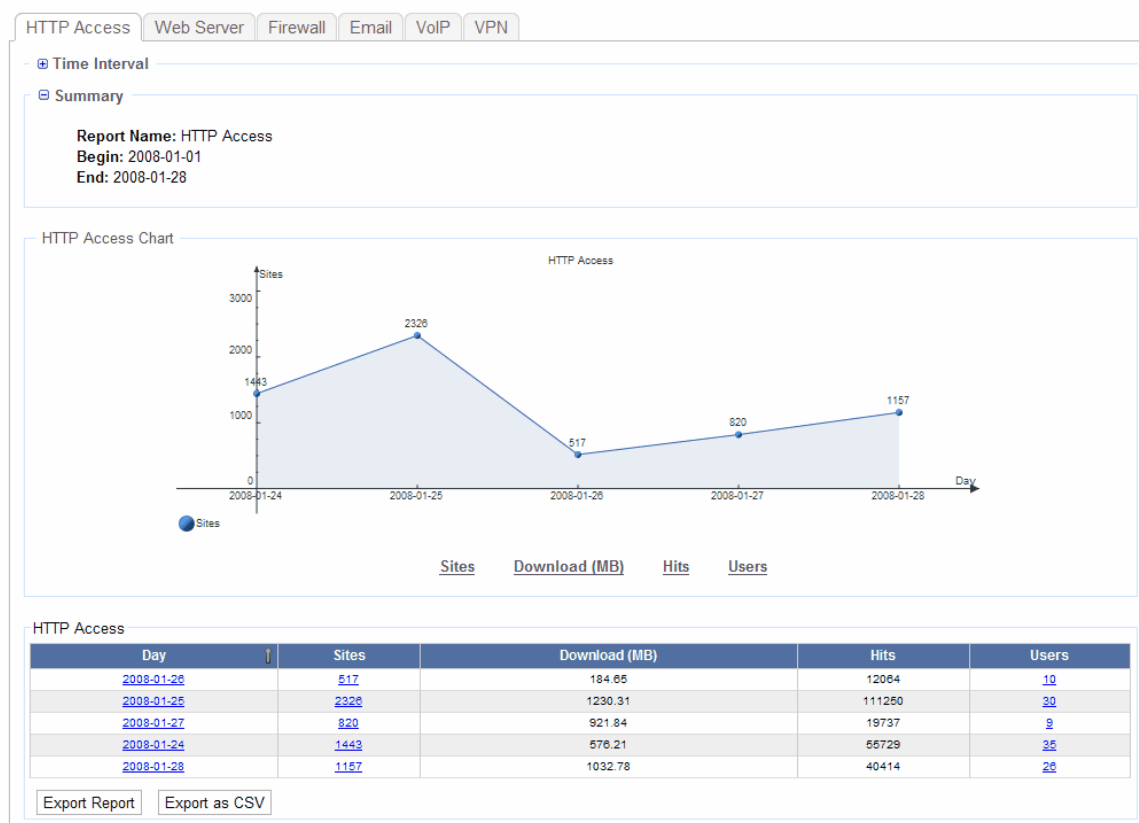
Displays reports showing information about the service usage.

- [HTTP Access](#)
- [Web Server](#)
- [Firewall](#)
- [Email](#)
- [VoIP](#)
- [VPN](#)

11.2.1 HTTP Access

The HTTP Accesses report displays information about **HTTP accesses through edgeBOX**. This means, the total number of sites, accumulated traffic in Mega Bytes, page hits and users yielding these accesses.

You can drill down into each line to see daily HTTP accesses and sites visited.

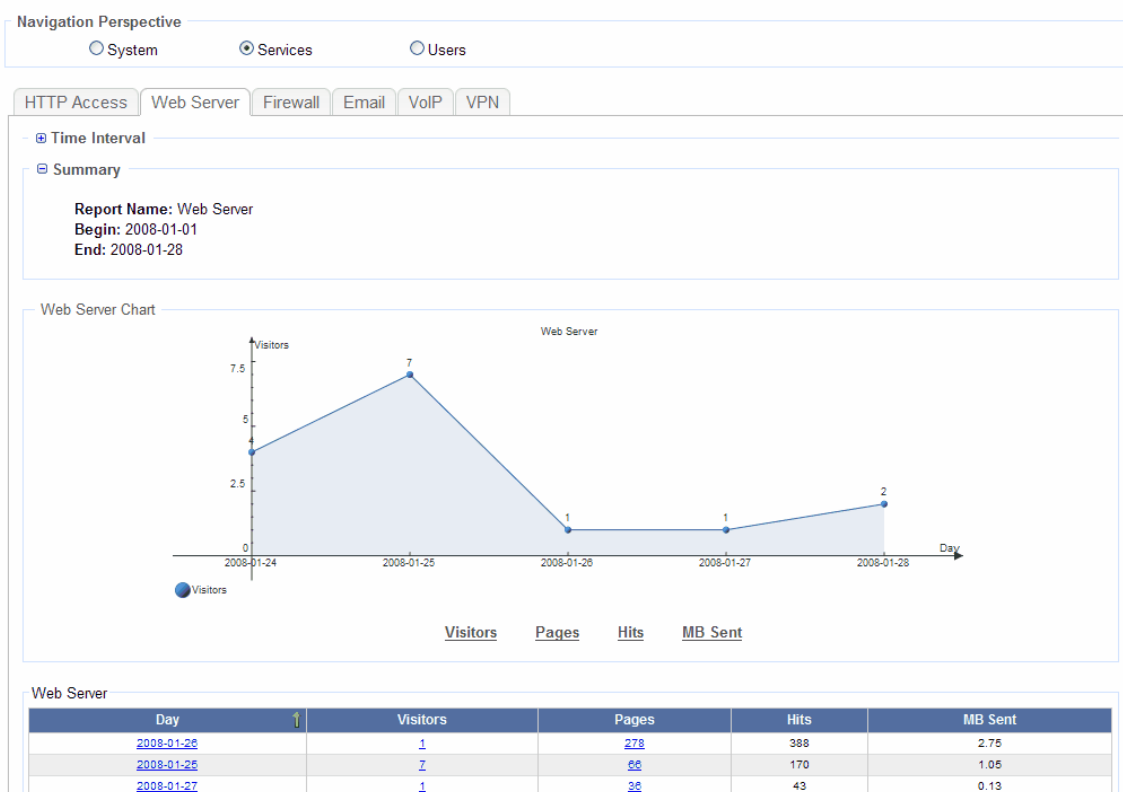


11.2.2 Web Server

The Web Server report shows **accesses to edgeBOX's web server**. It is where the Intranet and Extranet websites and the users' personal webpages are stored.

You can view the total number of visits to every page and the generated traffic, in Mega Bytes to edgeBOX's web server.

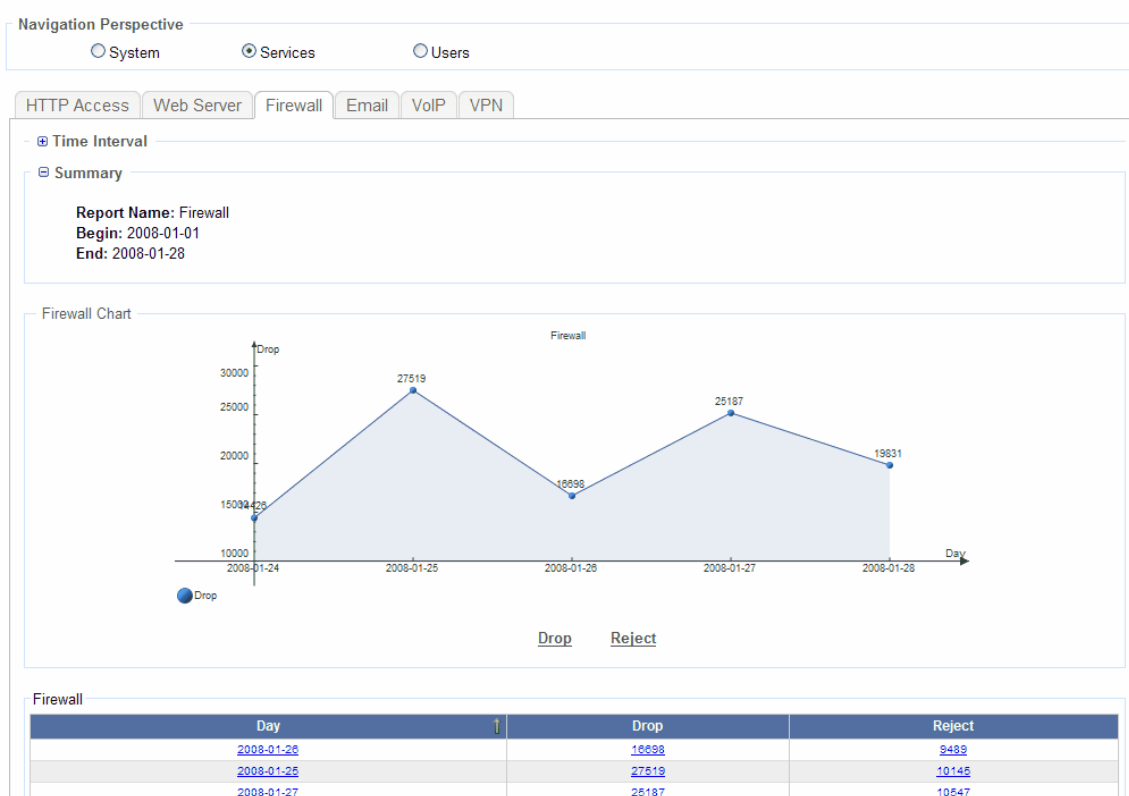
It is possible to drill down into each day to check the accesses on that specific day.



11.2.3 Firewall

This report shows Firewall related information as **dropped and rejected (sent back) network packets** grouped by day.

You can drill down each line to a specific time frame in order to identify actions applied to unauthorized network traffic.



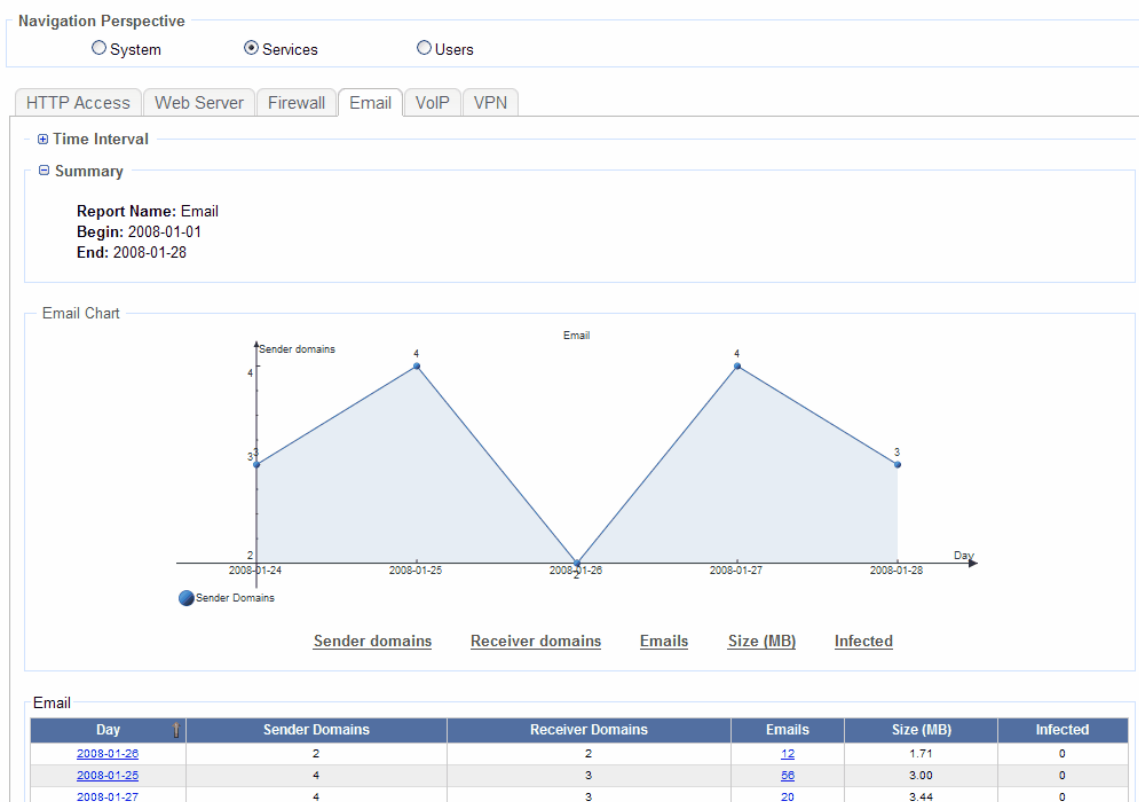
Generating this report may take some seconds because of the amount of packets that are constantly dropped or rejected by the firewall.

11.2.4 Email

The Email report shows **email service related information in the Services perspective**. This is, you can only see how many sender and receiver email domains (the @mail.com part of the email address) are processed for the sent and received email.

You can also view the amount of emails processed and, how many of those were detected as being infected with viruses by the Mail Scanner.

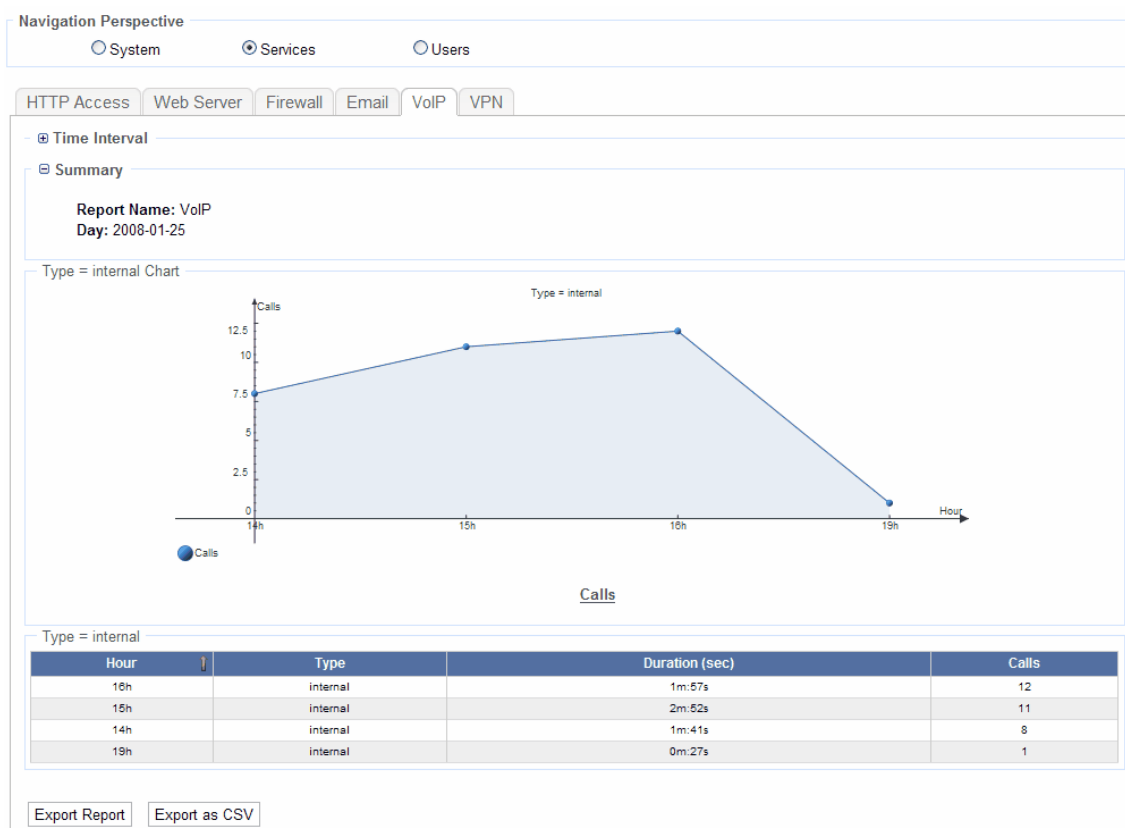
If you drill down in each line, you can identify singular email exchange info such as the sender or the receiver email, if it was locally delivered to edgeBOX, the size of the message and if it was infected with a virus.



11.2.5 VoIP

The VoIP report displays **VoIP service usage**. Calls are grouped into:

- Internal Calls - calls made between phones connected to edgeBOX.
- Outbound Calls - calls made to external phones.
- Inbound Calls - calls received from outside edgeBOX's network to internal phones connected to the edgeBOX.



The image above is a drilled-down detailed of the Internal Calls. The information available includes the duration of the calls and number of calls made.

11.2.6 VPN

The VPN report gives information about **the PPTP VPN tunnels in use in the edgeBOX**; number of users using the VPN service, the number of connections made, and accumulated duration of connections per day.



11.3 Users

Services data correlated with user information:

- [Accounting information](#)
- [HTTP Access](#)
- [Email](#)
- [VoIP](#)
- [VPN](#)

11.3.1 General

The General report summarizes the activity of users.

You can view the **inbound and outbound traffic** in Mega Bytes, **PPTP VPN tunnels** and the total duration of these tunnels, and **external calls made** and the duration of the calls.

The information is shown only in a tabular format; **it is not possible to drill down inside each line** as in other reports.

Reporting Users General Current

Navigation Perspective

System Services **Users**

General Accounting HTTP Access Email VoIP VPN

Time Interval

Summary

Report Name: General User Info
Begin: 2008-01-01
End: 2008-01-29

General User Info

Username	Traffic In (MB)	Traffic Out (MB)	VPN Tunnels	VPN Total Duration	External Calls	Call Duration
adiciobanu	0	0	2	56m:50s	0	0m:0s
Mhramos	0	0	0	0m:0s	0	0m:0s
alvaro	355	50	0	0m:0s	0	0m:0s
bd-vieira	332	71	0	0m:0s	0	0m:0s
braceta	288	79	0	0m:0s	0	0m:0s

11.3.2 Accounting

The Accounting report shows network traffic and sessions made by the network users.

You can check the **amount of downloads and uploads that are being processed for the users in each network interface** (WAN, LAN and DMZ).

You can drill down in each line of the table to view detailed information for each session of the users.

Navigation Perspective

System Services **Users**

General Accounting HTTP Access Email VoIP VPN


Time Interval

Summary

Report Name: Accounting
Begin: 2008-01-01
End: 2008-01-29

Accounting

User	Sessions	Duration (sec)	WAN In (MB)	WAN Out (MB)	LAN In (MB)	LAN Out (MB)	DMZ In (MB)	DMZ Out (MB)
192.168.90.92	0	0d:0h:0m:0s	0.48	0.00	0.02	0.00	0.00	0.00
192.168.90.46	0	0d:0h:0m:0s	57.26	0.00	0.32	0.00	0.00	0.00
alvaro	4	0d:8h:58m:52s	7.91	1.40	0.10	0.53	344.65	48.03
pegordo	2	0d:12h:48m:34s	1732.28	87.89	21.47	0.17	0.21	0.14
192.168.90.251	0	0d:0h:0m:0s	0.00	0.00	0.00	0.00	0.00	0.00
192.168.90.36	0	0d:0h:0m:0s	1.69	0.00	0.52	0.00	0.00	0.00
192.168.90.89	0	0d:0h:0m:0s	0.01	0.00	0.00	0.00	0.00	0.00

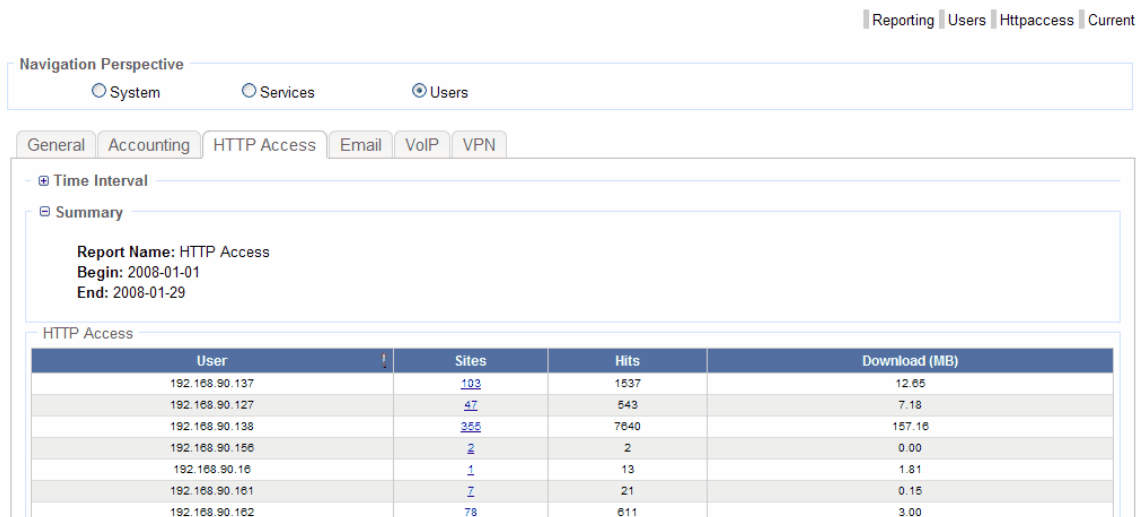
 If the option [Require Users to Login](#) is disabled, the user's IP Address is showed, instead of the user's username.

11.3.3 HTTP Access

The HTTP Accesses report displays information about **HTTP website accesses** made by the network users. **HTTPS website accesses are not showed.**

The report details the total number of sites, accumulated download traffic in Mega Bytes and number of page hits.

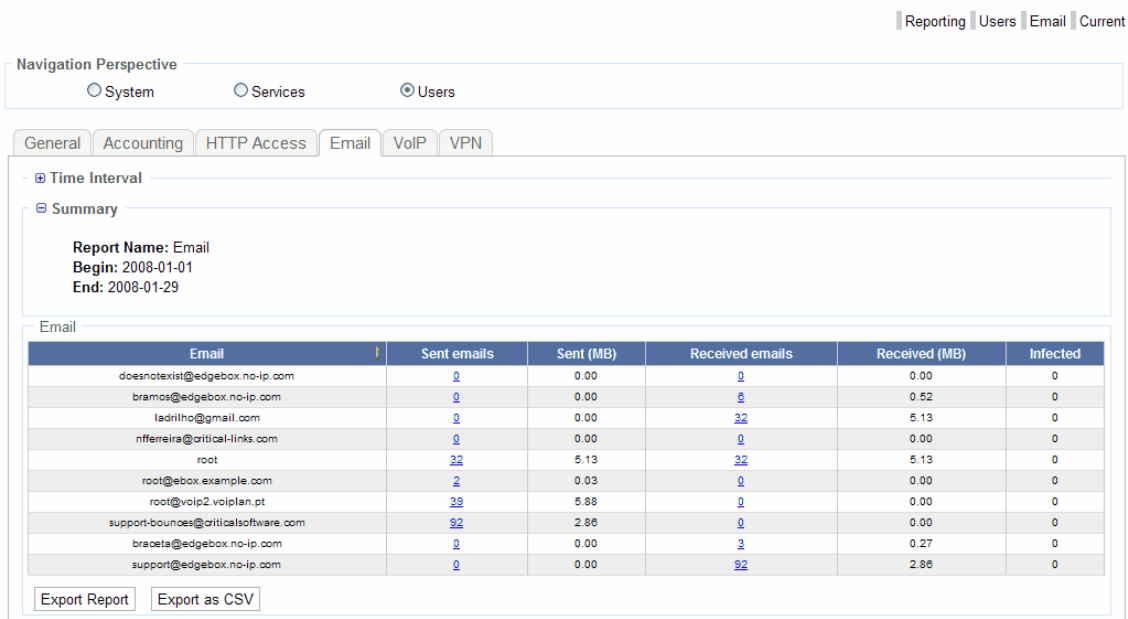
You can also drill down in each line of the table to see the sites visited for each user.



11.3.4 Email

The Email report shows **email service related information for each email address.**

You can drill down in each line to view email messages details for a particular email account.



11.3.5 VoIP

The VoIP report displays **VoIP calls for each phone or user**.

For all registered phones the Inbound, Outbound and Internal calls with their associated call duration is displayed.

Drill down into each type of calls to view the calls made for that type.

Reporting Users Voip Current

Navigation Perspective

System Services **Users**

General Accounting HTTP Access Email **VoIP** VPN

Time Interval

Summary

Report Name: VOIP
Begin: 2008-01-01
End: 2008-01-29

VOIP

Phone	Duration (sec)	Calls	Inbound (m:s)	Inbound Calls	Internal (m:s)	Internal Calls	Outbound (m:s)	Outbound Calls
SIP/bramos	416	31	0m:0s	0	0m:56s	31	0m:0s	0
SIP/braceta	191	16	0m:0s	0	3m:11s	16	0m:0s	0
SIP/abarbosa	1	2	0m:0s	0	0m:1s	2	0m:0s	0

Export Report Export as CSV

If you select a user's calls you can view calls to and from that user for the specified time period:

Reporting Users Voip By Phone All Calls

Navigation Perspective

System Services **Users**

General Accounting HTTP Access Email **VoIP** VPN

Time Interval

Summary

Report Name: VOIP
Begin: 2008-01-01
End: 2008-01-29

VOIP

Phone	Destination	Duration (sec)	Start	End	Type	Status
SIP/bramos	Hangup	0m:40s	2008/01/25 - 14:58:15	2008/01/25 - 14:58:55	internal	ANSWERED
SIP/bramos	VoiceMailMain	0m:12s	2008/01/25 - 14:59:03	2008/01/25 - 14:59:15	internal	ANSWERED
SIP/bramos	Hangup	0m:40s	2008/01/25 - 14:57:30	2008/01/25 - 14:58:10	internal	ANSWERED
SIP/bramos	Hangup	0m:0s	2008/01/25 - 14:57:26	2008/01/25 - 14:57:27	internal	NOANSWER
SIP/bramos	SIP/bramos	0m:1s	2008/01/25 - 14:56:41	2008/01/25 - 14:57:12	internal	ANSWERED
SIP/bramos	Hangup	0m:0s	2008/01/25 - 14:56:26	2008/01/25 - 14:56:26	internal	FAILED
SIP/bramos	Hangup	0m:0s	2008/01/25 - 14:56:18	2008/01/25 - 14:56:18	internal	FAILED
SIP/bramos	VoiceMailMain	0m:8s	2008/01/25 - 14:59:49	2008/01/25 - 14:59:57	internal	ANSWERED
SIP/bramos	VoiceMail	0m:23s	2008/01/25 - 15:03:26	2008/01/25 - 15:03:49	internal	ANSWERED
SIP/bramos	Hangup	0m:15s	2008/01/25 - 15:02:55	2008/01/25 - 15:03:10	internal	ANSWERED
SIP/bramos	Hangup	0m:40s	2008/01/25 - 15:01:55	2008/01/25 - 15:02:35	internal	ANSWERED
SIP/bramos	Hangup	0m:15s	2008/01/25 - 15:01:07	2008/01/25 - 15:01:22	internal	ANSWERED
SIP/braceta	SIP/bramos	0m:22s	2008/01/25 - 15:09:46	2008/01/25 - 15:10:12	internal	ANSWERED
SIP/bramos	SIP/braceta	0m:52s	2008/01/25 - 15:13:23	2008/01/25 - 15:14:17	internal	ANSWERED
SIP/bramos	VoiceMail	0m:4s	2008/01/25 - 15:13:17	2008/01/25 - 15:13:21	internal	ANSWERED

11.3.6 VPN

The VPN report gives a **summary of the PPTP VPNs on edgeBOX**. It shows the number of connections and the total duration of the connections.

Reporting Users Vpn Current

Navigation Perspective

System Services Users

General Accounting HTTP Access Email VoIP VPN

Time Interval

Summary

Report Name: VPN
Begin: 2008-01-01
End: 2008-01-29

VPN

User	Connections	Duration (sec)
adidobanu	2	2d:2h:56m:50s

Export Report Export as CSV

12 System



The System menu allows you to configure a variety of aspects of the edgeBOX, such as passwords and time.

12.1 Date and Time

View and adjust edgeBOX's date and time and synchronize with a preferred time server to keep the date and time always accurate.

The screenshot shows the 'Date & Time' configuration panel. At the top, there are tabs: 'Date & Time', 'Administrator', 'Logging', 'Software Updates', 'Hotbackup', and 'Ac'. The 'Date & Time' tab is selected. Below the tabs, the panel is divided into three sections: 'Date and Time Settings', 'Network Time Protocol', and 'TimeZone'. In the 'Date and Time Settings' section, there are spinners for 'Date (D M Y)' (1, 4, 2008) and 'Time (H M S)' (16, 15, 44). In the 'Network Time Protocol' section, there is a checked checkbox 'Use NTP to synchronize the system clock', a dropdown menu for 'Preferred NTP Server' (pool.ntp.org), and a 'Status: Disabled' label. In the 'TimeZone' section, there is a dropdown menu for 'Select:' (Europe/Lisbon).

▼ Adjust the date and time manually

1. Go to the Date and Time tab of the System menu.
2. Change the values of the date or the time in the Date and Time fields to adjust the them.
3. Click Apply in the bottom right side of the panel to save the changes.

▼ Synchronize the date and time with a Time Server on the Internet

You can use a time server on the Internet to keep date and time always accurate.

1. Go to the Date and Time tab of the System menu.
2. Select the option Use NTP to synchronize the system clock.
3. Select the NTP server you want to synchronize with from the drop down option.
4. Click Apply in the bottom right side of the panel to save the changes.

edgeBOX will try to synchronize with the selected server every day. You can see the status of the synchronization below the Time Server drop down option.



If edgeBOX's date and time is delayed more than 1000 seconds (17 minutes) edgeBOX will not synchronize and create an entry in the Log Viewer and send a notification by email.

▼ **Change the time zone**

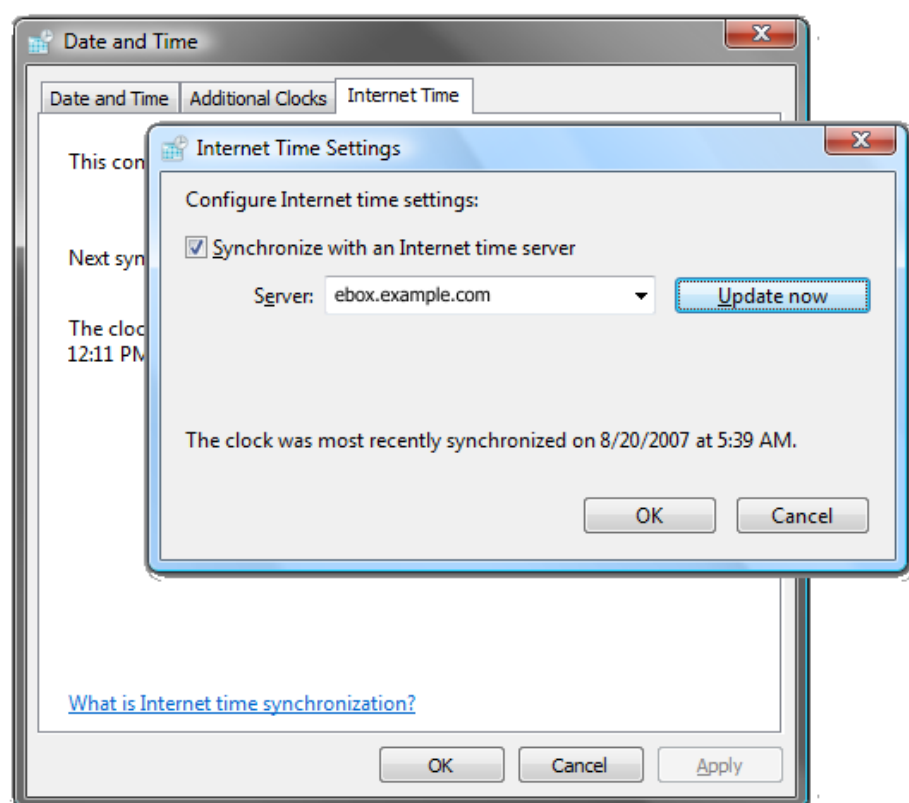
1. Go to the Configuration sub tab of the Software Updates tab.
2. Select the City or Zone closest to edgeBOX in the drop down option of the Time Zone group.
3. Click the Change button to save the changes.

▼ **Synchronize all devices on your network with edgeBOX's date and time**

Besides synchronizing its date and time with an Internet Time Server, edgeBOX can also work as a Time Server so you can synchronize all your network devices as phones, computers and servers with edgeBOX. This way you can keep an the same, accurate, time on every device of your network.

To synchronize a device with edgeBOX's date and time:

1. Go to the device's date and time settings.
2. Go to the part where you can synchronize with an Internet Time Server.
3. Indicate that the the time server you want to synchronize with is edgeBOX. To do that you can type in edgeBOX's IP address or edgeBOX's hostmane. For example, if edgeBOX's hostname is ebox and the network domain is example.com and edgeBOX's IP address is 192.168.100.254, than you can type ebox.example.com or 192.168.100.254.



12.2 Administrator

Change edgeBOX administrations settings:

▼ Change the admin password

When the edgeBOX is installed, the admin **password is by default the word root.**

To change the password:

1. In the Password field type the **new password**.
2. Retype your new password in the Confirm Password field.
3. Click the **Apply button** in the bottom right corner of the application to **save the changes**.

▼ Change the language of the web interface

EdgeBOX's web management interface supports English, Portuguese, German and Chinese language. To change the language:

1. Select the desired language in the drop down list of the Language group. If you select Chinese, you need to [install the East India Language files](#) to be able to see Chinese fonts.
2. Click the Apply button to save and the language will be changed.



You also change the language of the Self Service area of the users when you change edgeBOX's language.

▼ Indicate or change the email to receive system messages

EdgeBOX sends several types of system messages and notifications as emails as system warning or problems or available updates, for example.

To set the email were you want to receive these messages or to change it:


1. Type the desired email in the first email address field of the system messages group.
2. Click the Apply button to save.

▼ [Change the email of the sender field of system messages](#)

EdgeBOX sends several types of system messages as emails as system warning or problems or available updates, for example. By default system messages have on the sender field an email address like edgebox@example.com.

To change it:

1. Type the desired email in the second email address field of the system messages group.
2. Click the Apply button to save.

 The default sender email address edgebox@example.com is an invalid email. It is made of the word edgebox and edgeBOX's default internal domain: example.com.

You can change it to a valid email one so people can reply to those messages. Also, you can change it to a valid email to avoid problems with Email Servers because Email Servers generally validate domains when they deliver emails and example.com is not a valid public domain.

12.3 Logging

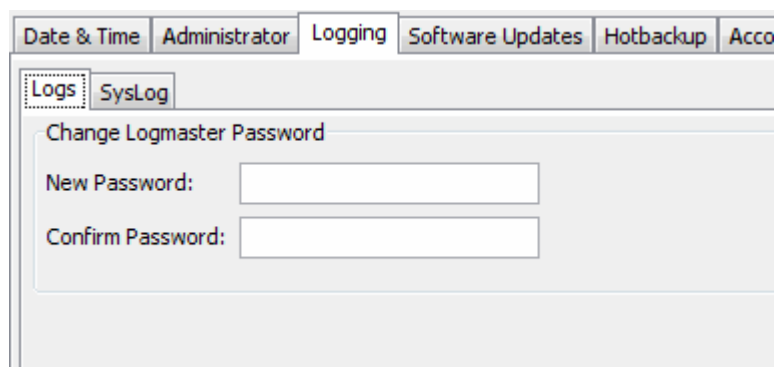
This menu allows you to configure elements of the logging system.

12.3.1 Logs

Change logmaster password: The logmaster account, allows you to ftp to the edgeBOX to extract:

- System Log Files (sys.log)
- Apache (HTTPS) Access Logs (access_log)
- VoIP [CDR's](#) (Master.csv files)

You set the logmaster password from this panel. Press Apply to update to the new password.



12.3.2 Syslog

This menu option allows you to configure remote logging. You need to configure a syslog server to accept connections from the edgeBOX. The available options on this page are now described.

Remote Logging

Checking this option will activate this feature.

Remote Location

The IP address for the remote syslog server to which edgeBOX will send syslog information. You can optionally include the port number. If the remote syslog server is running in a different port than the standard port 514.

12.4 Software Updates

View and install available updates for edgeBOX and edgeBOX's third part applications; the edgePaks.

The updates available are new functionalities, security updates or performance enhancements for the network services.

Available Updates

Name	Installed Version	Available Version
edgebox-activator	4.5.5-1	4.6-3
edgebox-peps	4.6-79	4.6+s000012-82
zaptel-bin	1.2.18-1	1.2.18-2
edgebox-factoryconf	4.6-4	4.6-7
edgebox-gui-java-modular	4.6.0-60	4.6.0-63
edgebox-voip	4.6-17	4.6-18
edgebox-dns	4.6-11	4.6-12
edgebox-manual	4.6-1	4.6-2

System Update Log

Name	Previous Version	New Version	Installation Date	Status
edgebox-groupware	noverion	4.6-2	Fri Mar 28 17:59:02 2008	installed
edgebox-gui-html	4.6-24	4.6-25	Fri Mar 28 20:01:04 2008	installed
edgebox-peps	4.6+s000012-80	4.6-79	Mon Mar 31 13:13:16 2008	installed

Clear Update Log

Update System Status: **Idle**

Check Install

- **Available Updates** - Displays a list of all of the updates that are currently available for edgeBOX and have not yet been installed.
- **System Update Log** - Reports all of the updates that have been applied to edgeBOX. The list can be cleared by clicking on the Clear Update Log button.
- **Clear Update Log** - Deletes the current update log
- **Check** - Clicking this button will immediately check for new updates, without installing them.
- **Install** - Installs all the Available Updates where the Install checkbox has been checked.

Update Mode Configuration

You can manually check for and install available updates, make edgeBOX check for updates and notify you of the updates so you can install them yourself, or ask edgeBOX to check for install updates automatically.

▼ Check for and install available updates manually

1. Go to the Configuration sub tab of the Software Updates tab.
2. Select Manual in the Update Mode drop down option.
3. Click the Change button to save the changes.

▼ Make edgeBOX check for and notify you of available updates

1. Go to the Configuration sub tab of the Software Updates tab.
2. Select Semi-Automatic in the Update Mode drop down option.
3. Indicate the frequency you want edgeBOX to check for updates in the Check for updates

every drop down option and the time of the day it should check for the updates in the Start Hour fields.

4. If you want to be notified of the new updates when you enter edgeBOX web interface, select the option **Notify me when updates are available**. If you want to be notified of the new updates by email, select the option **Notify by Email**.
5. Click the Change button to save the changes.

▼ [Make edgeBOX check for and install available updates automatically](#)

1. Go to the Configuration sub tab of the Software Updates tab.
2. Select Automatic in the Update Mode drop down option.
3. Indicate the frequency you want edgeBOX to check for updates in the Check for updates every drop down option and the time of the day it should check for the updates in the Start Hour fields.
4. Some updates require either a network service to be restarted or, for more important updates, edgeBOX must be rebooted. Depending on what you choose for this item, a window will pop-up after you log on to the web interface, warning you there are updates available that require action after being installed.
5. Select the option Notify by Email if you want also to receive email notifications regarding the need to reboot the system or restart services and to indicate that the updates where installed.
6. Click the Change button to save the changes.



If an error occurs while edgeBOX is trying to update, an notification will be displayed in the web interface indicating you the problem and asking you to try to install the update again.

12.5 HotBackup

If you have two edgeBOXes, Hotbackup allows you to configure one of them (the Master) to manage the network and daily replicate its configuration and storage data to the other edgeBOX (the Slave). The Slave edgeBOX works as a backup, ready to take over the master's place if a failure occurs.




The Slave and Master **must have identical operating system releases and revisions**. For example, if you update only the Master with a new revision of the edgeBOX's software, the Hotbackup process will not be possible. To grant this, You should **manage edgeboxes' updates manually** and not automatically. [Why?](#)

Also, the **base hardware on both edgeBOXes must be exactly the same** and the **extra function cards** installed on each must be identical and **plugged in in the same connectors**.

▼ [Set your edgeBOX as the Slave edgeBOX](#)

To set edgeBOX as a Slave edgeBOX (backup edgeBOX):

1. Select the option Slave in the Mode group.
2. Indicate below the network information the edgeBOX will have so that the Master edgeBOX can communicate with it during the Hotbackup process:
 - IP address
 - Netmask
 - Default Gateway
 - DNS server IP address
3. Click the **Apply button** to start the process. edgeBOX will reboot and run in Slave mode. In Slave Mode only the LAN interface is active. That's the interface to which you should connect your ethernet cable.


 When you set edgeBOX in Slave mode, you **lose access to the web interface** and you **can no longer use the edgeBOX for managing your network**. It will only work as a backup edgeBOX for the Master edgeBOX. Still, you will be able to access it using its command line interface, either locally using a keyboard/VGA or a serial console, or remotely via ssh. Although, you will be able to perform just a limited set of commands.

▼ Set your edgeBOX as the Master edgeBOX

You can only set your edgeBOX to run in master mode after you have an edgeBOX configured and working as a Slave edgeBOX. Also, the Slave must be accessible to the Master through the network.

To make your edgeBOX run in Master mode:

1. Select the option Master in the Mode group.
2. Indicate below the IP address of the Slave edgeBOX.
3. Set the time of the day you want to replicate the configuration and data of the master to the slave. The replication is made every day.
4. Click the apply button. edgeBOX will reboot and start work as a Master edgeBOX. If you have an edgeBOX with LCD display, you can view an "M" in the top right corner of the LCD, indicating that the edgeBOX is running as a Master edgeBOX.

 Choose a day time where your network has less activity, for example, during dawn, because in order **to make the replication**, the master **edgeBOX has to stop a considerable amount of network services** to grant that the configuration and information are correctly replicated.

▼ Check the status of the Slave edgeBOX

When you have an edgeBOX in Slave mode, you lose access to the web interface. Still you can check its status to view the connectivity and global consistency with the Master.

To check the Status of the Slave:

1. Go to the Hotbackup configuration panel of the Master edgeBOX.

2. Click the Check Status button.
3. Wait a few moments while the Master edgeBOX connects to the Slave edgeBOX and check its configuration in order to validate its operation as a Hotbackup Slave. If everything is alright, you will receive a message saying "Slave Status: Ok".

▼ Replicate edgeBOX's configuration to the Slave edgeBOX

In Hotbackup, the replication of the Master edgeBOX's configuration and data is made everyday at a given hour that you defined when you configured the Hotbackup process. Still you can ask the Master edgeBOX to replicate at any time:

1. Go to the Hotbackup configuration panel of the Master edgeBOX.
2. Click the Replicate Now button. The replication may take a few minutes.
3. Wait until you receive the message "Slave Status: Ok". It indicates the replication has finished.

 Make sure that your network has few activity when you ask edgeBOX to replicate. Note that, in order to replicate correctly, edgeBOX has to stop a considerable amount of network services.

▼ Stop edgeBOX from being in Master mode

If you have your edgeBOX running in Master Mode and you want to stop using HotBackup and make the edgeBOX run again in the default normal mode, then:


1. Select the option Disabled in the Mode group.
2. Click the Apply button.

edgeBOX will stop replicating his configuration to the slave edgeBOX and continue working normally.

▼ Make the Slave edgeBOX take-over if the Master edgeBOX fails

If your Master edgeBOX (the edgeBOX that is managing your network) is malfunctioning and you need the Slave edgeBOX (backup edgeBOX), to take it over:

1. Before initializing the process, check the status of the last replication in the Slave edgeBOX. Click the Check Slave button to do so.
2. If the Slave's last replication is OK, [shutdown the Master edgeBOX](#).
3. Connect all appropriate cables (eg ADSL, ISDN, Analogue etc) to the Slave edgeBOX.
4. Open the slave edgeBOX's Command Line Interface (CLI).
5. Type in the command `hotbackup returntonormalmode` or `hotbackup return to normal mode`. The Slave edgeBOX will take over all services previously provided and managed by the Master.

 When you stop the Slave edgeBOX to work as a slave and make it take over the master, you gain back access to edgeBOX's web interface. To login to the web interface, use the password that you used to login on the Master edgeBOX.

12.6 Accounting

This menu option allows you to review and configure the Radius servers used for accounting. Note that you can have authentication and accounting performed by the same server, or have different servers for each purpose. The table lists all the servers configured. The configured servers will be contacted in sequence, and the first one to answer will store the data. The accounting data applies only to the WAN interface. Available actions are "Add", "Edit" and "Delete".

Add

After selecting "Add" a popup will display, requesting you to enter the following information:

- Server IP: The IP address for the new server;
- Server Port: The port used. The default value is 1813, but another port may be used.
- Password: The password used by edgeBOX's radius client to access the server
- Confirm Password: Confirm the password you have entered
- Timeout: The maximum amount of time for connection setup with the RADIUS server. If this time is exceeded then the next server on the list (if any) will be contacted.

Edit

Change the settings for a listed server. After selecting the server configuration to edit, press "Edit". After changing the possible options and selecting "OK", you will have to select "Apply" in the main panel to make changes effective.

Delete

Deletes a server from the list after selecting it and pressing "Delete". You will have to select "Apply" in the main panel for changes to become effective.

Log Network Traffic

Select from the list, where possible values are "Off", "15 minutes", "30 minutes" and "60 minutes". This option allows you to control the period for which account information will be sent to the remote Radius accounting servers.

Note: Accounting is only available with authenticated sessions. This the (Security) Firewall, "[Require Users to Login](#)" should be checked and appropriate accounts set up.

12.7 Radius

This page allows you to view, delete and add remote Radius clients for user authentication. These are normally called NAS (Network Access server). The edgeBOX supports different types of 802.1x port based authenticators. Some of the devices supported include 802.1x switches with dynamic VLAN assignment like the Procurve 2650 or the Procurve 420 Access Point for Wireless communications with multiple SSID and dynamic VLAN assignment.

Supported EAP methods: PEAP-EAP-MSCHAPv2 and EAP-TTLS.

The screenshot shows the 'Authorized Clients' section of the EdgeBOX 4.6 web interface. At the top, there is a navigation bar with tabs: Date & Time, Administrator, Logging, Software Updates, Hotbackup, Accounting, Radius, SNMP, Items, Diagnostics, Notifications, RAID, and Shutdown. The 'Radius' tab is selected. Below the navigation bar, the 'Authorized Clients' section contains a table with the following data:

IP Address	Model	Name	VLAN
192.168.90.33	HP ProCurve 2650	test	<input checked="" type="checkbox"/>

Below the table, there are three buttons: 'Add', 'Edit', and 'Delete'. At the bottom right of the interface, there is an 'Apply' button.

If you select the Generic 802.1x Access Point or Generic 802.1x Switch from the drop down list, the IP address is the IP of the AP/Switch and the password the radius client password configured in the remote AP/Switch.

Name is any text you wish to enter to identify this unit.

If "Enable Dynamic VLAN assignment" is checked, the edgeBOX internal Radius server sends the correct VLAN id to the Switch or Access Point according to the User Access Profile. This feature allows the remote port based authentication device to put the user in the correct VLAN, independently of the port / SSID the user is currently connected. You must use a compatible port based authentication device.

The screenshot shows the 'Add Authorized Client' dialog box. It has a title bar with a close button (X). The dialog contains the following fields and controls:

- IP Address:
- Password:
- Name:
- Type:
- ☐ Enable Dynamic VLAN assignment

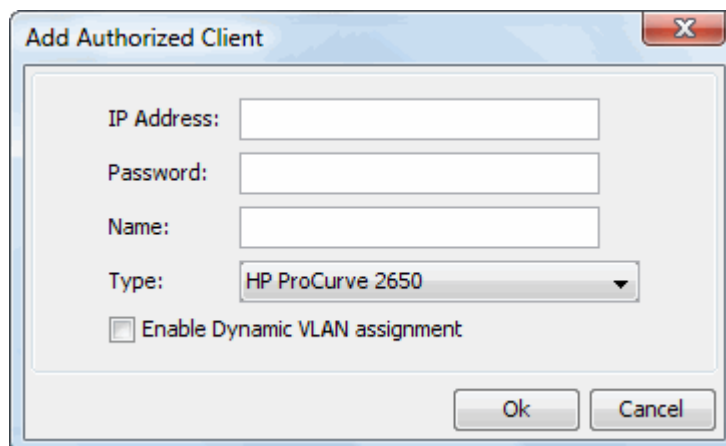
At the bottom right, there are 'Ok' and 'Cancel' buttons.

If you select the "HP ProCurve 2650" drop down, the IP address is the IP of the Switch and the password the login password of the switch.

Name is any text you wish to enter.

If "Enable Dynamic VLAN assignment" is checked, and after a successful 802.1x user authentication, the edgeBOX internal Radius server sends the correct VLAN id to this switch

according to the User Access Profile. This option allows the Procurve switch to put the user in the correct VLAN, independently of the port the user is currently connected.

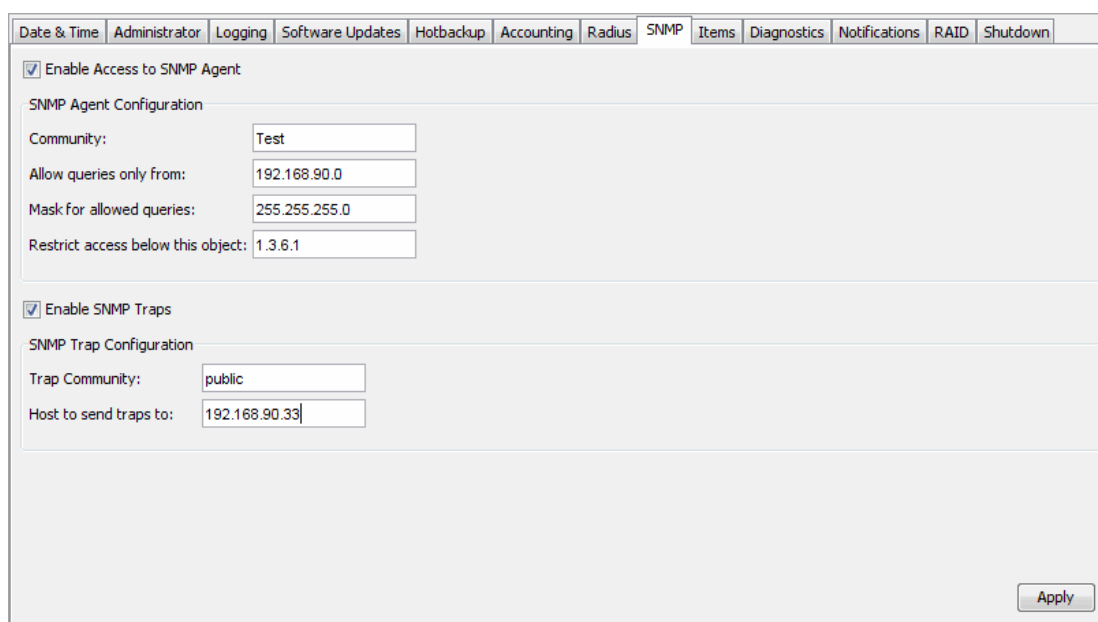


The 'Add Authorized Client' dialog box contains the following fields and options:

- IP Address:** Text input field.
- Password:** Text input field.
- Name:** Text input field.
- Type:** Dropdown menu with 'HP ProCurve 2650' selected.
- ☐ **Enable Dynamic VLAN assignment**
- Buttons:** 'Ok' and 'Cancel' at the bottom right.

12.8 SNMP

The status of the edgeBOX can be queried using the Simple Network Management Protocol. This panel controls the SNMP agent running on the edgeBOX.



The SNMP configuration panel includes the following sections and fields:

- Tabs:** Date & Time, Administrator, Logging, Software Updates, Hotbackup, Accounting, Radius, **SNMP**, Items, Diagnostics, Notifications, RAID, Shutdown.
- ☒ **Enable Access to SNMP Agent**
 - SNMP Agent Configuration**
 - Community:** Text input field with 'Test'.
 - Allow queries only from:** Text input field with '192.168.90.0'.
 - Mask for allowed queries:** Text input field with '255.255.255.0'.
 - Restrict access below this object:** Text input field with '1.3.6.1'.
- ☒ **Enable SNMP Traps**
 - SNMP Trap Configuration**
 - Trap Community:** Text input field with 'public'.
 - Host to send traps to:** Text input field with '192.168.90.33'.
- Buttons:** 'Apply' at the bottom right.

SNMP Agent Configuration

Configures read-only access to the edgeBOX.

- **Enable Access to SNMP Agent** - Enables the SNMP agent and allows read-only access to report the status of the edgeBOX.

- **Community** - The name of the community used when requesting access to the SNMP agent. Avoid well known strings such as "public", "private" or ones that are easy to guess, e.g. "edgeBOX". Specifically "public" is not allowed.
- **Allow queries only from** - The host name or IP address of a computer which will be granted sole access to the SNMP agent. Queries from any other address will be rejected.
- **Mask for allowed queries** - Allows the user to define a netmask to allow one to defines entire networks.
- **Restrict access below this object** - Enter an object identifier (OID). Access to objects below this level, by any SNMP client, are not allowed.

SNMP Trap Configuration

Allows notifications to be sent for requests to access objects by an SNMP client.

- **Enable SNMP Traps** - Enable notifications to be sent.
- **Trap Community** - The name of the community used when sending a notification.
- **Host to send traps to** - The host name or IP address of a computer where notifications will be sent.

12.9 Items

Allow communication between edgeBOX and an iTEMS server. An iTEMS server allows the management of several edgeBOXes at the same time.

- **Keep Alive** - time interval in minutes which the keep alive packet is sent to the iTEMS Server. The keep alive server will use this keep alive connection to warn iTEMS administrators of potential problems with the edgeBOX.
- **iTEMS Server** - the IP address of the iTEMS server.

The screenshot displays the 'Items' configuration tab within the System 277 web interface. At the top, a horizontal menu bar contains the following tabs: Date & Time, Administrator, Logging, Software Updates, Hotbackup, Accounting, Radius, SNMP, Items (which is currently selected), Diagnostics, Notifications, RAID, and Shutdown. Below the menu bar, the 'Keep Alive (min):' is set to 5, indicated by a dropdown arrow. The 'ITEMS Server:' field contains the IP address 192.168.60.34. The main area of the tab is a large, empty light gray rectangle. An 'Apply' button is located in the bottom right corner of the configuration area.

12.10 Diagnostics

The tabs in this panel allow you to use some basic diagnostic tools.

12.10.1 Interfaces

The following image shows the typical display for this panel, which shows the following information:

- **Interface:** The Interface name as would appear in an ifconfig (Unix) command
- **Type:** Interface type
- **Interface Desc:** Shows which Interface is associated with the LAN/WAN and DMZ
- **Mode:** Interface mode
- **Speed:** Speed in Mb/s
- **Has Link:** Shows which Interfaces are connected
- **Hardware Address:** MAC address
- **IP Address:** IP address
- **Netmask:** Netmask

Date & Time

Administrator

Logging

Software Updates

Hotbackup

Accounting

Radius

SNMP

Items

Diagnostics

Notifications

RAID

Shutdown

Interfaces

Ping

NSLookup

Traceroute

DHCP Leases

Interface List

Interfaces	Type	Interface Desc.	Mode	Speed	Has Link	MAC Address	IP Address	Netmask
vlan6	VLAN	VLAN_E					192.168.105.254	255.255.255.0
eth2	Ethernet	dmz			No	00:40:f4:8b:0f:07	192.168.200.254	255.255.255.0
eth3	Ethernet				No	00:40:f4:8b:0f:06		
vlan5	VLAN	VLAN_D					192.168.104.254	255.255.255.0
br0	Bridge (eth1,et...	lan					192.168.100.254	255.255.255.0
vlan4	VLAN	VLAN_C					192.168.103.254	255.255.255.0
eth0	Ethernet	wan	Full-duplex	100Mbps	Yes	00:40:f4:8b:0f:09	192.168.90.181	255.255.255.0
vlan3	VLAN	VLAN_B					192.168.102.254	255.255.255.0
vlan2	VLAN	VLAN_A					192.168.101.254	255.255.255.0
eth1	Ethernet				No	00:40:f4:8b:0f:08		

12.10.2 Ping

Utility to indicate network connectivity. It should be noted that not all devices will respond to a Ping.

12.10.2.1 All Methods

This produces a Ping which will try each method sequentially (ICMP, UDP, TCP then SYN)

If one of the methods receives a reply (eg ICMP), the other methods will not be attempted. If no reply is received after the Timeout (5 sec's in this example), the next method will be attempted until another 5 sec's has elapsed and so on until either a successful reply is received or all methods have timed out.

The screenshot shows a network utility window with tabs for Interfaces, Ping, NSLookup, Traceroute, and DHCP Leases. The 'Ping' tab is active. It contains three sections: Parameters, Optional Parameters, and Result. The Parameters section has a Host field with the value 192.168.90.254 and a Type dropdown menu set to ICMP. The Optional Parameters section has three spinners: Timeout set to 5, Packet Size set to 1,024, and Port set to 80. The Result section displays the outcome of the ping: Connectivity is Yes (in green), Round Trip Time is 3,495 ms, IP Address is 192.168.90.254, and Used Method is icmp.

Fields on the panel are:

- **Host:** Enter the IP address or FQDN (eg www.demon.net) that you wish to check for connectivity
- **Timeout:** Number of seconds before the method times out
- **Connectivity:** Read only field showing connectivity success (Yes) or failure (No)
- **Round Trip Time:** If a reply is received, the ping aborts and this field shows the total time to send and receive a reply
- **IP Address:** The IP address of the replying computer
- **Used Method:** The last method used in the Ping request

12.10.2.2 ICMP

Ping typically sends ICMP Echo Request messages (and receives Echo Response messages) to determine whether a host is reachable and how long packets take to get to and from that host.

Fields on the panel are:

- **Host:** Enter the IP address or FQDN (eg www.demon.net) that you wish to check for connectivity
- **Packet Size:** Size of packets sent in bytes
- **Timeout:** Number of seconds before the method times out
- **Connectivity:** Read only field showing connectivity success (Yes) or failure (No)
- **Round Trip Time:** If a reply is received, the ping aborts and this field shows the total time

to send and receive a reply

- **IP Address:** The IP address of the replying computer
- **Used Method:** The last method used in the Ping request

12.10.2.3 UDP

This is a stateless protocol which does not provide the reliability and ordering of TCP. That is, the sender does not know if any computer received the packet nor does the receiver know if all the packets have been received and if they are in the correct order.

Fields on the panel are:

- **Host:** Enter the IP address or FQDN (eg www.demon.net) that you wish to check for connectivity
- **Packet Size:** Size of packets sent in bytes
- **Timeout:** Number of seconds before the method times out
- **Connectivity:** Read only field showing connectivity success (Yes) or failure (No)
- **Round Trip Time:** If a reply is received, the ping aborts and this field shows the total time to send and receive a reply
- **IP Address:** The IP address of the replying computer
- **Used Method:** The last method used in the Ping request

12.10.2.4 TCP

Transmission Control Protocol (TCP) allows ping to send packets via a reliable and ordered protocol.

Fields on the panel are:

- **Host:** Enter the IP address or FQDN (eg www.demon.net) that you wish to check for connectivity
- **Packet Size:** Size of packets sent in bytes
- **Timeout:** Number of seconds before the method times out
- **Connectivity:** Read only field showing connectivity success (Yes) or failure (No)
- **Round Trip Time:** If a reply is received, the ping aborts and this field shows the total time to send and receive a reply
- **IP Address:** The IP address of the replying computer
- **Used Method:** The last method used in the Ping request

12.10.2.5 SYN

If the "SYN" protocol is specified, the ping method will only send a TCP SYN packet to the remote host then immediately return. If the syn packet was sent successfully, it will return a true value, otherwise it will return false.

Fields on the panel are:

- **Host:** Enter the IP address or FQDN (eg www.demon.net) that you wish to check for connectivity
- **Packet Size:** Size of packets sent in bytes
- **Timeout:** Number of seconds before the method times out
- **Connectivity:** Read only field showing connectivity success (Yes) or failure (No)
- **Round Trip Time:** If a reply is received, the ping aborts and this field shows the total time to send and receive a reply
- **IP Address:** The IP address of the replying computer
- **Used Method:** The last method used in the Ping request

12.10.3 NSLookup

Nslookup displays information that can be used to diagnose Domain Name System (DNS) problems.

12.10.3.1 Host Names

This page allows you to determine the Domain of a specified IP address

The screenshot shows a web interface with tabs for 'Interfaces', 'Ping', 'NSLookup', 'Traceroute', and 'DHCP Leases'. The 'NSLookup' tab is active. Under 'Parameters', 'Query for:' is set to 'Host Names' and 'IP Address:' is '194.159.246.194'. Under 'Optional Parameters', 'DNS Server:' is empty and 'Timeout' is '5'. The 'Result' section shows 'echannel.www.demon.net'.

The following parameters may be entered:

- **IP Address:** Enter the IP address of the machine of interest
- **DNS Server:** If set, allows you to specify a DNS Server (by IP or name) which will be used to resolve the IP address. If not set, the edgeBOX default name server is used for the lookup.

- **Timeout:** Number of seconds before the method times out

The Result panel shows the FQDN of the IP address that was entered.

12.10.3.2 Name Servers

This panel allows you to determine the nameservers for a specified domain

Parameters	
Query for:	Name Servers
Domain name:	daemon.net

Optional Parameters	
DNS Server:	
Timeout	5

Result	
Result	
	erebus.hades.net
	cerberus.hades.net
	tartarus.hades.net

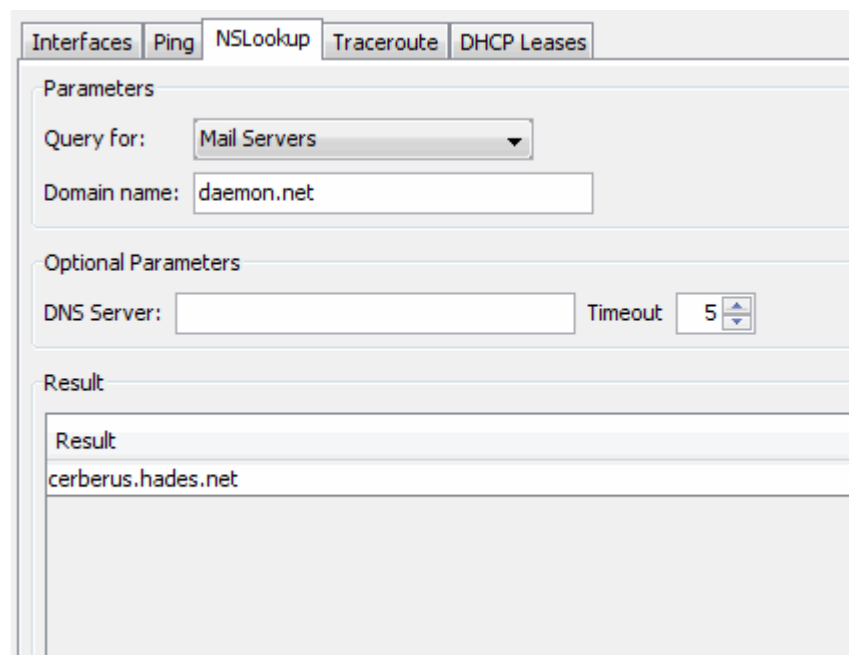
The following parameters may be entered:

- **Name Servers:** Enter the domain of interest
- **DNS Server:** If set, allows you to specify a specific DNS Server (by IP or name) which will be used to resolve the IP address. If not set, the default name server is used for the lookup.
- **Timeout:** Number of seconds before the method times out

The Result panel shows the DNS servers for the domain that was entered. (Typically this should result in 2 or 3 entries)

12.10.3.3 Mail Servers

This panel allows you to determine the mailservers for a specified domain



The screenshot shows a web-based interface with five tabs: 'Interfaces', 'Ping', 'NSLookup', 'Traceroute', and 'DHCP Leases'. The 'NSLookup' tab is selected. Below the tabs, there are three sections: 'Parameters', 'Optional Parameters', and 'Result'. In the 'Parameters' section, 'Query for:' is set to 'Mail Servers' and 'Domain name:' is 'daemon.net'. In the 'Optional Parameters' section, 'DNS Server:' is empty and 'Timeout' is set to 5. The 'Result' section shows a single entry: 'cerberus.hades.net'.

The following parameters may be entered:

- **Mail Servers:** Enter the domain of interest
- **DNS Server:** If set, allows you to specify a specific DNS Server (by IP or name) which will be used to resolve the IP address. If not set, the default name server is used for the lookup.
- **Timeout:** Number of seconds before the method times out

The Result panel shows the Mail Servers for the domain that was entered. (Typically this should result in 2 entries)

12.10.3.4 IP Addresses

This panel allows you to determine the IP address for a specified domain

Result
64.233.167.99
64.233.187.99
72.14.207.99

The following parameters may be entered:

- **Hostname:** Enter the domain/Host Name of interest
- **DNS Server:** If set, allows you to specify a specific DNS Server (by IP or name) which will be used to resolve the IP address. If not set, the default name server is used for the lookup.
- **Timeout:** Number of seconds before the method times out

The Result panel shows the IP address for the Host Name that was entered.

12.10.4 Traceroute

Traceroute allows you to view the network route that packets take to reach a specified host.

A reference for how traceroute (know as tracert on Windows) work can be found at: [Traceroute](#)

Note: It may take in excess of 10 seconds to complete the task.

The screenshot shows a network utility window with tabs for Interfaces, Ping, NSLookup, Traceroute, and DHCP Leases. The Traceroute tab is active. Under the 'Parameters' section, the 'Host' is set to 'google.com'. Under 'Optional Parameters', the 'Protocol' is set to 'ICMP' and 'Queries timeout' is set to '1'. The 'Result' section displays a table with the following data:

Hop	Host	RTT	Status
1	192.168.90.254	0.44ms	Reached the host.
1	192.168.90.254	0.54ms	Reached the host.
1	192.168.90.254	0.54ms	Reached the host.
2			This query timed out.
2			Unknown.
2			This query timed out.
3	62.48.140.126	33.07ms	Reached the host.
3	62.48.140.126	30.82ms	Reached the host.
3	62.48.140.126	30.82ms	Reached the host.
4	62.48.136.18	21.59ms	Reached the host.

The following parameters may be entered:

- **Host:** Enter the Domain/Host Name/IP Address of interest
- **Protocol:** ICMP or UDP
- **Queries Timeout:** Number of seconds before the method times out

The Result panel shows network path that the connection (packets) used to contact the Host. The Result panel shows:

- **Hop:** This is the number of times the connection moves from one network to another (crosses a router). The more hops, the longer the distance (in network terms)
- **Host:** The address of the host for the current Hop
- **RTT:** For each hop, traceroute then displays the Round Trip Time (RTT), or the time difference between when the probe was sent from and the time the response arrived for each packet.
- **Status:** Summary status

12.10.5 DHCPLeases

DHCP leases shows DHCP information for the edgeBOX clients.

IP Address	Status	Starts	Ends	MAC Address	Hostname
192.168.100.193	active	2008/04/01 15:31:27	2008/04/02 11:31:27	00:02:3f:63:9e:e0	"kitchen"

The DHCP Leases List shows:

- **IP Address:** The IP address offered to the client (eg 192.168.100.200)
- **Status:** Status of the lease (active or free)
- **Starts:** Start time for the lease (eg 2007/01/10 11:21:43)
- **Ends:** End time for the lease (eg 2007/01/11 11:21:43)
- **Hardware Address:** The Mac address of the client
- **Host Name:** Hostname of the client

You can **test the connectivity between edgeBOX and each client.**

To test it, select one client from the list and press the Ping button in the right bottom side of the panel. If there is connectivity, the client will be highlighted in green. If there is no connectivity, the row will be highlighted in red.

12.11 Notifications

Configure the system to send email notifications and SNMP traps.

The screenshot shows a web-based configuration interface for system notifications. At the top, there is a navigation bar with tabs: Date & Time, Administrator, Logging, Software Updates, Hotbackup, Accounting, Radius, SNMP, Items, Diagnostics, Notifications (selected), RAID, and Shutdown. Below the navigation bar, the 'Service State' is indicated as 'Running' in green. The main section is titled 'Email Notifications' and contains a table with the following data:

Notification Facilities	Email Address	Email Subject	Active
HARDWARE_MONITOR	p.parker@example.com	HardwareMonitor Notification	<input checked="" type="checkbox"/>
RAID	p.parker@example.com	Raid Notification	<input checked="" type="checkbox"/>

Below the table are buttons for 'Add', 'Edit', and 'Delete'. The next section is titled 'Traps Notifications' and contains a table with the following data:

Notification Facilities	Trap Type	Trap Manager	Trap Community	Trap OID	Snmp Version	Active
BACKUP	Enterprise	127.0.0.1	public	.1.3.6.1.2.1.88	2c	<input checked="" type="checkbox"/>

Below this table are also 'Add', 'Edit', and 'Delete' buttons. At the bottom right of the window are 'Stop Service' and 'Apply' buttons.

You may Add an email notification by selecting the Add button, below the Email notifications panel, as shown below:

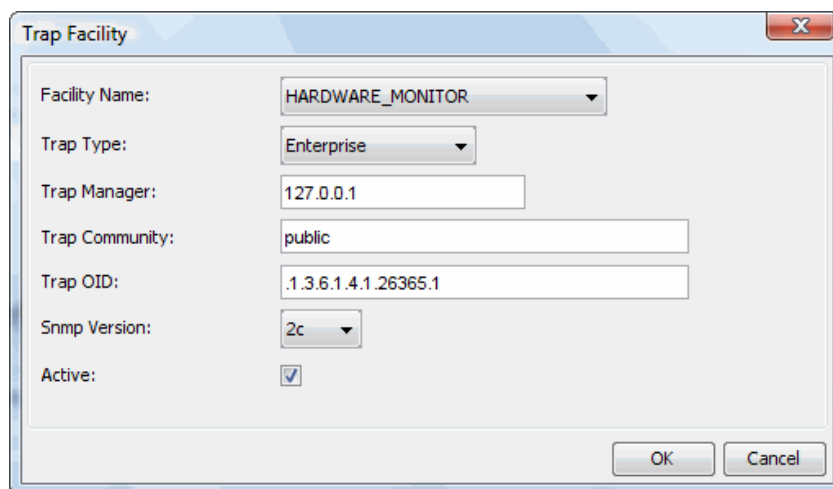
The 'Email Facility' dialog box is shown with the following fields and options:

- Facility Name:** A dropdown menu with 'HARDWARE_MONITOR' selected.
- Email Address:** A text input field containing 'root@localhost'.
- Email Subject:** A text input field containing 'HardwareMonitor Notification'.
- Active:** A checkbox that is checked.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

- **Facility Name** - Select HARDWARE_MONITOR if you want to receive emails for temperature changes and other hardware issues. Select RAID if you want to receive emails about hard disk status related to RAID.
- **Email Address** - The address to which the notifications will be sent.
- **Email Subject** - The subject of the email message.
- **Active** - If checked, the Notification is active, otherwise it is not.

You may Add SNMP trap notifications by selecting the Add button, below the Trap Notifications panel, as shown below:



- **Facility Name** - If HARDWARE_MONITOR is selected, SNMP traps will be sent, based on the [Hardware Monitor](#) panel for temperature and other hardware issues. If RAID is selected, Traps will be sent based on the Disk [Notifications](#) panel for disk based issues.
- **Trap Type** - Only Enterprise should be selected. Generic will be included for a future release.
- **Trap Manager** - IP address of the Server which will receive the traps.
- **Trap Community** - The community which has been configured on the server which will receive the traps.
- **Trap OID** - The Object Identifier configured on the server which will receive the traps.
- **SNMP Version** - SNMP versions 1 and 2c are available options .
- **Active** - If checked, the Trap Notification is active, otherwise it is not.

12.12 RAID

A RAID array distributes data across several physical disks which look to the operating system and the user like a single disk. Several different arrangements are possible. Currently, only RAID1 is supported and it is managed by the RAID panel.





RAID1 uses two (possibly more) disks which each store the same data, so that data is not lost so long as one disk survives. Total capacity of the array is just the capacity of a single disk. The failure of one drive, in the event of a hardware or software malfunction, does not increase the chance of a failure or decrease the reliability of the remaining drives (second, third, etc).

The panel has the following elements:

- At the top the array status is presented and it may have be one of the following:

- **Clean** - all disks in the array are active
- **Recovering** - the array is rebuilding, i.e, it is mirroring the disks
- **Degraded** - there is a faulty disk in the array
- A list, at the left side, with the array disks, and another list, at the right side, with the offline disks, i.e, the disks which are not included in the array
- A button to add a disk to the array and another button to remove a disk from the array. This actions will move the disk from one list to the other.

The disks status is illustrated by the following icons:

	Active or offline (if in the Right Hand Section)
	Invalid disk - the disk is invalid because it does not have the exactly the same size
	Rebuilding disk - the disk is rebuilding and synchronizing with the active disks
	Faulty disk - the disk is faulty possibly due to a hardware problem

12.12.1 Disk Notifications

If the status of the array changes, a notification action may be performed as defined on the [Notifications](#) panel. Notification actions will occurs under the following circumstances:

- **DeviceDisappeared** - A mirrored array which was previously configured, has lost a device and is no longer working as a RAID array
- **RebuildStarted** - The RAID array has started reconstruction (eg when a disk is replaced, the new disk has to be reconstructed from the good disk to form the array)
- **RebuildFinished** - The (new) disk has either completed construction (and is now part of the RAID1 array) or the construction was aborted.
- **Fail** - An active disk in the RAID mirror has been marked as faulty.
- **FailSpare** - A spare disk (i one is available), which was being rebuilt to replace a faulty device has failed.
- **DegradedArray**- The Array is degraded (eg disk failure)
- **SpareActive** - A spare disk (if one exists) which was being rebuilt to replace a faulty disk, has been successfully rebuilt and has been made active.

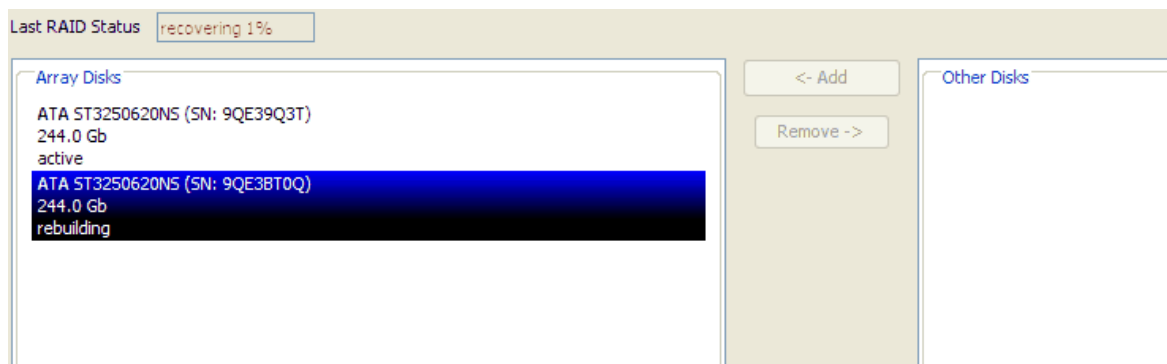
12.12.2 Replacing a faulty disk

If the array becomes degraded the faulty disk should be replaced. There are different ways to perform disk replacement:

No Hot Spare

To replace a faulty disk automatically, i.e, without the need of management intervention, just follow the steps:

1. Write down the serial number of the faulty disk
2. Shutdown the edgeBOX at the earliest opportunity
3. Replace the faulty disk (check the serial number) - the new disk must have the same capacity (in bytes) as the faulty disk.
4. Start the system



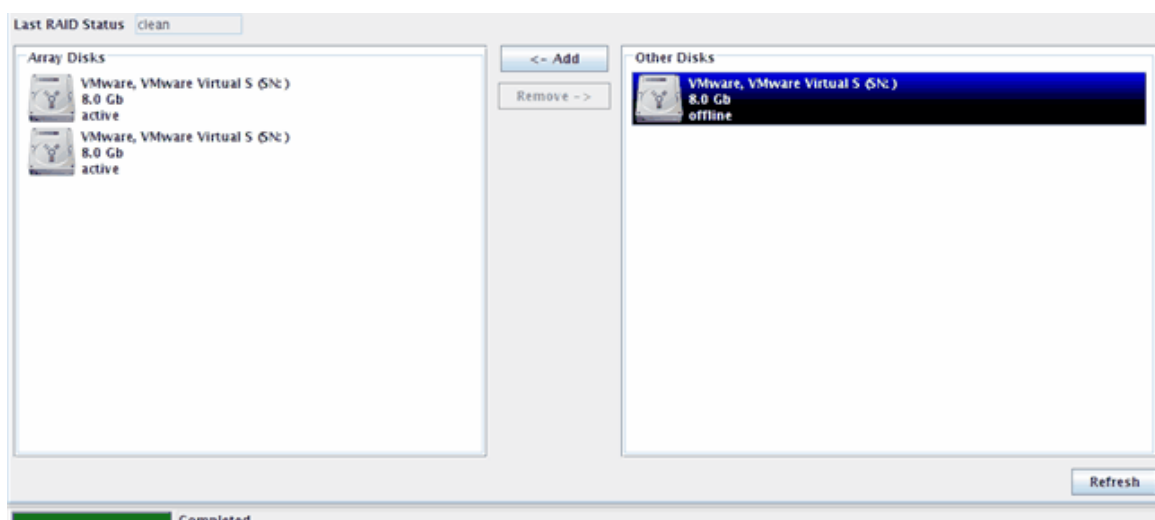
The new disk should synchronize with the active one. The array status may be checked on the RAID panel.

Note: The replacement disk must match the original disk, it cannot have a larger or smaller disk capacity (in Bytes)

Hot Spare

If the box has more than two disks, one may not have to shutdown the system immediately. A third disk (spare) may replace the faulty one. This action is accomplished by the following steps:

1. Highlight the faulty disk and press the "Remove" button
2. Highlight the Spare Disk and press the "Add" button, the new disk will be included on the RAID array and synchronization will begin.



If a spare disk is available in the "Array Disks" panel, it will be automatically used to rebuild the RAID array in the event of a disk failure with one of the current RAID disks.

To replace the faulty disk, highlight it and select the "Remove" button. Shut down the edgeBOX and remove and replace (if you wish) with a new disk which has the same Byte capacity as the faulty disk.



In this case, it would be prudent to add this replacement disk to the "Array Disk" panel for automatic replacement in the event of another disk failure.

Hotswap

Hotswap is also supported in the Enterprise Appliance, however the following precautions should be taken:

- Write down all disks serial numbers and respective slot to know which disk is the faulty one.

- The faulty disk may be replaced without shutting down the system. Synchronization process progress may be checked in the Raid panel.

12.13 Shutdown

This panel allows you to restart or shutdown edgeBOX. Restarting edgeBOX may take several minutes.

The screenshot shows the 'Shutdown' panel in the EdgeBOX interface. The panel has a tabbed header with the following tabs: Date & Time, Administrator, Logging, Software Updates, Hotbackup, Accounting, Radius, SNMP, Items, Diagnostics, Notifications, RAID, and Shutdown. The 'Shutdown' tab is currently selected. The main content area of the panel is titled 'Action to perform:' and contains two radio buttons: 'Restart' and 'Shutdown'. The 'Shutdown' radio button is selected. Below the radio buttons is a 'Confirm' button.

13 Status



Access edgeBOX status information and also some accounting reports, if you have selective authorization turned on.

- [Summary](#)
- [Users](#)
- [Network](#)
- [Services](#)
- [Traffic Control](#)
- [Hardware Monitor](#)
- [Log Viewer](#)
- [About](#)

13.1 Summary

Summary of the status of edgeBOX, namely, the Internet connection status, the usage of the CPU and memory, the available disc space, and firewall and services status.

The screenshot shows the 'Summary' tab of the edgeBOX interface. It is divided into two main sections: 'Network Information' and 'System Status'.

Network Information:

- Status: DHCP up
- Timestamp: Thu 15 May 2008 14:04:40 BST
- Type: dhcp
- IP Address: 192.168.90.135
- Netmask: 255.255.255.0
- Gateway: 192.168.90.254
- Primary DNS: 127.0.0.1
- Secondary DNS: (empty)


System Status:

- CPU Usage: 62% (blue bar)
- Memory in Use: 83% (blue bar)
- Swap in Use: 33% (blue bar)
- System Storage, Used: 1% (blue bar)
- Home Storage, Used: 0% (blue bar)
- UpTime: 0d 2h 30m

Firewall Information:

Authorization: off Firewall: on NAT: on

Service	Status	Start at Boot	Internal	External	DMZ
flashoperator	yes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
dns	yes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
smtp	yes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ssh	yes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
imap	yes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ftp	yes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
http	yes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
pop3	yes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

 High Memory in Use chart does not necessarily indicate low memory. edgeBOX leaves applications in memory and only release pages from memory as required.

13.2 Users

If the Require Users to Login option is enabled (on the firewall), this list will display the users currently authenticated. Also it displays the IP and MAC addresses and the access profile for each user.

Each entry contains the name of the interface, state (if it is up or down), bytes in and bytes out (for the sum of inbound and outbound bytes transferred via the interface). If the state is:

- **UP** - Either both WiFi and cabled connections are available, or, if you have only WiFi or cabled connections, this indicates that the connection is available.
- **UP (Wireless)** - The WiFi connection is available and a LAN port exists.
- **UP (Wired)** - The the wired connection is available and a WiFi connection exists.
- **Down - there is** no connectivity.

Connections

Each entry contains the source IP or user (the user will be displayed only if selective authorization is on), source port, destination IP and destination port.

13.4 Services

View the status of the edgeBOX services that can be started or stopped by you.

To change status of a service:

1. If you want to start a service, select the Start/Stop option of the desired service. If you want to stop a service, remove the selection from the Start/Stop option of the desired service.
2. Press the Apply button in the bottom right corner of the panel.

Summary	Users	Network	Services	Traffic Control	Hardware Monitor	Log Viewer	About
---------	-------	---------	----------	-----------------	------------------	------------	-------

Service State

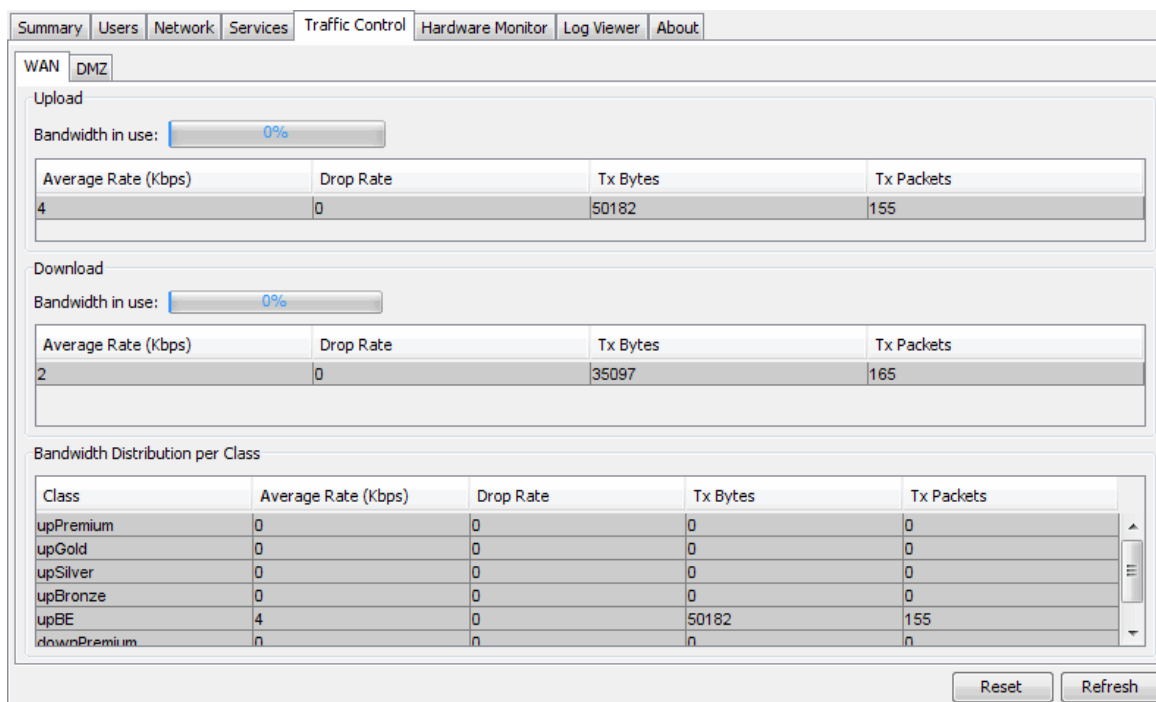
Name	Service Status	Start/Stop
ftp	RUNNING	<input checked="" type="checkbox"/>
dns	RUNNING	<input checked="" type="checkbox"/>
smtp	RUNNING	<input checked="" type="checkbox"/>
http	RUNNING	<input checked="" type="checkbox"/>
voip	RUNNING	<input checked="" type="checkbox"/>
samba	RUNNING	<input checked="" type="checkbox"/>
ssh	RUNNING	<input checked="" type="checkbox"/>
dhcp	RUNNING	<input checked="" type="checkbox"/>

Apply

13.5 Traffic Control

View traffic control statistics for the Internet connection (WAN) and for the DMZ network. They are **calculated for a period of 15 minutes** using **values** that are **collected every 2 minutes**.

- Click the **Refresh** button to calculate the statistics using **just values collected in the instant you click the button**. These values are just used to calculate these statistics; they **are not used** in the **calculations of the regular statistics** that are calculated for 15 minutes interval.
- Click the **Reset** button to reset the values of the Regular Statistics that are calculated for a 15 minutes interval.



Upload Group

Statistics about outbound traffic. The Bandwidth In Use indicates the percentage of bandwidth consumed. Below, the table indicates the average bandwidth used (Kbps), the dropped packets, transmitted bytes and transmitted packets.

Download Group

Download Group - Statistics about inbound traffic. The Bandwidth In Use indicates the percentage of bandwidth consumed. Below, the table indicates the average bandwidth used (Kbps), the dropped packets, transmitted bytes and transmitted packets.

Bandwidth Distribution per Class

Statistics by traffic control class. For each class, it is displayed the average bandwidth consumed (Kbps), dropped packets, transmitted bytes and transmitted packets.



Statistics for Bandwidth Distribution per Class only appear if you have the Traffic Control Service running and have Traffic Control Classes assigned to access profiles or to services. [Learn more...](#)

13.6 Hardware Monitor


Information of the velocity of edgeBOX's fans, the CPU speed and several status of the hard disk (s). It is updated every 15 seconds.

The screenshot shows a web-based interface with a tabbed menu at the top: Summary, Users, Network, Services, Traffic Control, Hardware Monitor (selected), Log Viewer, and About. Below the tabs, the 'S.M.A.R.T.' section is expanded, showing 'Hard Disk 1' with the following data:

Monitoring Enabled:	Yes
Overall Health:	Good
Temperature (°C):	+45
Bad Sectors Count:	0
Pending Sectors Count:	0
CRC Errors Count:	0
Total UpTime (Hours):	6515

Hard disks information:

- **Overall Health** - Yes or No. It is determined by the monitoring software of the disc, based on the values of the parameters that follow next.
- **Temperature.**
- **Bad Sectors Count** - Number of sectors which are unusable.
- **Pending Sectors Count** - Number of sectors waiting to be remapped to another part of the disk.
- **CRC Errors Count** - Number of errors when writing to the disk.
- **Total Up Time** - Number of hours since the disk has been switched on.

 You can receive email notifications about changes detected in the Hardware Monitor in the Notifications panel.

13.7 Log Viewer

View the logs for some of edgeBOX's services.

The screenshot shows the Log Viewer interface with the 'Log Viewer' tab selected. The 'Service' dropdown is set to 'BACKUP'. The 'Verbosity' is set to 'High'. The log table displays the following messages:

Date	Message
2008/04/01 12:22	backup[26283]: Backup: Can't locate Backup/Scheme/.pm in @INC (@INC contains: /eos/pep/common /eos/pep/ /usr/lib/perl/5.
2008/04/01 12:22	backup[26283]: Backup: line: 103
2008/04/01 12:22	backup[26283]: Backup: filename: /eos/pep/common/Backup.pm
2008/04/01 12:22	backup[26283]: Backup: package: Backup
2008/04/01 12:22	backup[26283]: Backup: Exception:
2008/04/01 12:22	backup[26283]: Backup: Scheme
2008/04/01 12:22	backup[26283]: Backup: START
2008/04/01 12:15	backup[25296]: Backup: Can't locate Backup/Scheme/.pm in @INC (@INC contains: /eos/pep/common /eos/pep/ /usr/lib/perl/5.
2008/04/01 12:15	backup[25296]: Backup: line: 103
2008/04/01 12:15	backup[25296]: Backup: filename: /eos/pep/common/Backup.pm
2008/04/01 12:15	backup[25296]: Backup: package: Backup
2008/04/01 12:15	backup[25296]: Backup: Exception:
2008/04/01 12:15	backup[25296]: Backup: Scheme
2008/04/01 12:15	backup[25296]: Backup: START

At the bottom, there are 'Previous Page', 'Next Page', and 'Refresh' buttons.

To view the log files select the desired log in the Service drop down list. You can view logs for the Antivirus, Authentication, Backup, [Blacklist](#), Content Filtering, Daemon, Hardware Monitor, Hotbackup, Kernel, Mail, RAID, [VoIP](#), WAN Interface.

Use the buttons Previous Page and Next Page to view all the content of the log files.

To view more or less details, switch the Verbosity between High or Low.



The verbosity is global to the Log Viewer and not specific to each log, so, in some of the logs, the information shown is always the same, regardless of the verbosity chosen.


13.7.1 Blacklist Log

The Blacklist log shows the **list of devices**, normally computers **that are temporarily forbidden to access the network services**, as the internet for example, **because they tried to access them repeatedly without authenticating in the edgeBOX first**. It can happen for several reasons, as trying to open a large number of web pages at the same time, for example, without having authenticated.

This log is most useful for troubleshooting; **when a computer of the network has problems to authenticate in the edgeBOX, it is most likely because it is temporarily in the blacklist.**

Date	Message
2008/04/29 17:41	webauth[16829]: BLACKLIST: 192.168.100.193 Windows-Update-Agent
2008/04/29 17:41	webauth[16830]: PREBLACKLIST: 192.168.100.193 Windows-Update-Agent
2008/04/29 17:07	webauth[13404]: PREBLACKLIST: 192.168.100.193 Mozilla/5.0 (Windows; U; Windows NT
2008/04/16 13:38	webauth[24742]: BLACKLIST: 192.168.100.188 Windows-Update-Agent
2008/04/16 13:38	webauth[24741]: PREBLACKLIST: 192.168.100.188 Windows-Update-Agent

- 1 - Date and time the computer was added to the blacklist.
- 2 - Code of the log file entry. webauth is the type of the code. It means Web Authentication.
- 3 - List the computer was added to:
 - If PREBLACKLIST then the computer has been added to a warning-type blacklist. It means that it is risking being added to the blacklist if it continues trying to access the network without authenticating.
 - If BLACKLIST then the computer has been added to the blacklist and is not allowed to authenticate or access the network services, as the internet for instance, for a while.
- 4 - IP address of the computer that is blacklisted.
- 5 - Application on the computer that tried to access the network without authenticating.

 **You cannot remove a computer from the blacklist yourself.** It is an automatic process. After a short period of time, edgeBOX will remove the computer from the list and it will be able to authenticate again.

13.7.2 VoIP Log

Information related to **phones' succeeded or failed attempts to register** in edgeBOX.

You can see:

- SIP succeeded registrations (shows the name of the extension and IP address received).
- SIP failed registrations (shows the reason: wrong password or non existing SIP account).
- IAX succeeded registrations.
- IAX failed registrations.
- Alarms clear on PRI channels.

13.8 About

Information about edgeBOX's software version, hardware settings and license definitions.

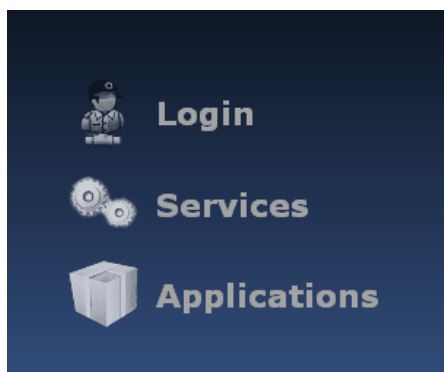
The screenshot shows the 'About' page of the edgeBOX web interface. The page has a navigation bar at the top with tabs: Summary, Users, Network, Services, Traffic Control, Hardware Monitor, Log Viewer, and About. The main content area displays the edgeBOX logo and two sections: 'Product Information' and 'License Information'. The 'Product Information' section shows 'edgeOS version 4.6.5' and 'Build 20081010-1'. The 'License Information' section shows 'Licensed To: testbed', 'Hardware Description: tw252-v2-9670 504000011', 'Product ID: 73e04455d732254a', and 'User Account Limit: 40'. Below these sections is the 'END USER LICENSE AGREEMENT (EULA)'. Red arrows point from text labels on the right to specific values in the screenshot: 'edgeBOX software version' points to '4.6.5', 'Version release date (ex: 26/08/2008)' points to '20081010-1', 'edgeBOX licence serial number' points to '73e04455d732254a', and 'Maximum numbers of users allowed by your license.' points to '40'.

Section	Field	Value	Description
Product Information	edgeOS version	4.6.5	edgeBOX software version
	Build	20081010-1	Version release date (ex: 26/08/2008)
License Information	Licensed To	testbed	
	Hardware Description	tw252-v2-9670 504000011	
	Product ID	73e04455d732254a	edgeBOX licence serial number
	User Account Limit	40	Maximum numbers of users allowed by your license.

END USER LICENSE AGREEMENT (EULA): The edgeBOX software is distributed according to the End User License Agreement EULA. By using the software you agree to be bound by this EULA. If you do not agree to the terms and limitations of the components that are specifically not covered by the EULA you should not use this software. The EULA only covers software components that have been developed and are propriety of Critical Links, Inc. The Open Source software components aggregated in the same

14 Services

On the initial page, besides 'Login' and 'Applications', you will find a third option: 'Services'.

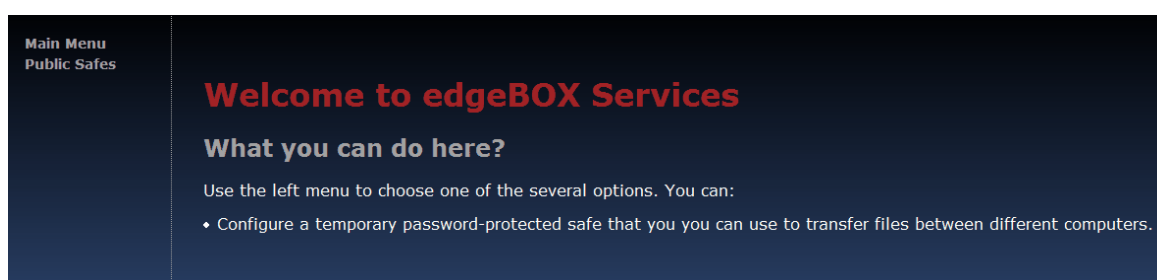


Please note this option will only be available for users connected through the LAN interface.

The following conditions must be met to use Public Safes:

- HTTP services must be running.
- Samba service must be running
- Public Safes must be allowed (Services on main top panel -> Samba -> Public Safes tab -> Check Active)

After following the 'Services' link on the initial page, you will enter the services page where the following options are available: Main menu and Public Safes



14.1 Main Menu

This option will take you back to the services initial page, where some information is displayed about the operations available.

14.2 Public Safes

Every user may configure a temporary storage space which will be available for a limited interval of time. The administrator initially configures the maximum space and time available using the Samba panel in the control centre, thus activating this feature. This page may then be used to create the safes.

After choosing this option, the list of existing safes will be displayed showing the remaining time active. The options available are create a new safe, remove a safe and go back.

Create a new safe

You will be asked to choose the size and the time the safe will be active. These values are limited by the values entered by the administrator. After confirming the values, the username and password for accessing the safe will be displayed on the screen. You will then be able to access the safe in the same way you access a share.

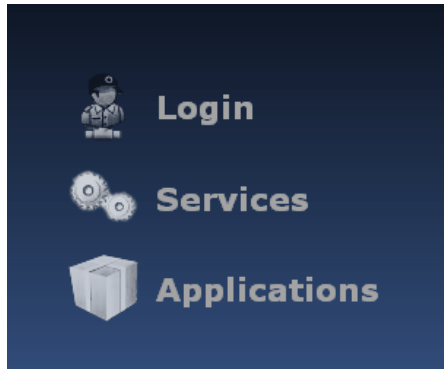
Remove safe

In the existing safes listing, there will be a link which will allow you to remove a safe before it is automatically deleted by the system. You will have to supply the username and passwords used to access the safe.

There is much more detail in The [Public Safes](#) section of Appendix C.

15 Applications

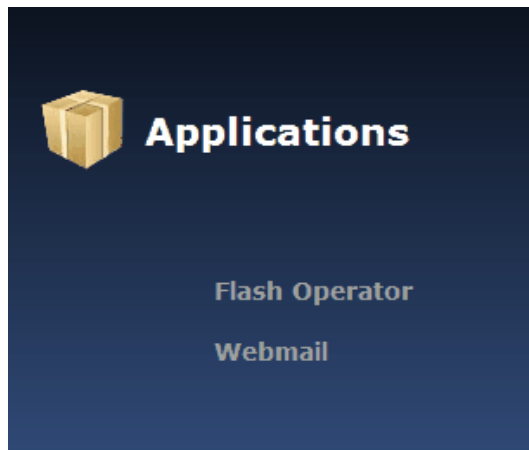
Additional applications are available from the Applications menu (eg Webmail, Flash Operator Panel, OpemCMS and Moodle).



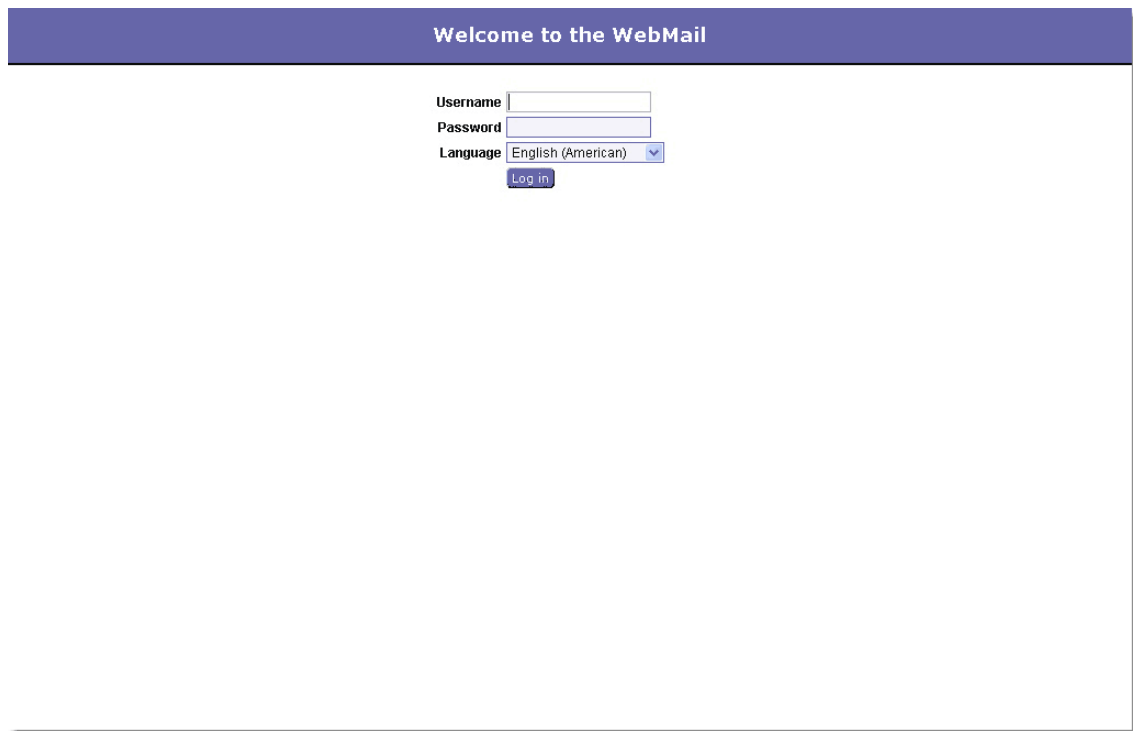
15.1 Web Mail

If you have the SMTP service running **with a web mail domain defined** (see [Email Domains](#)), the HTTP server [running](#) and you have allowed access to it, you may access the email service through a web browser.

Simply point your browser at the LAN IP of the edgeBOX (eg <https://myedgebox.com>) (or LAN IP).



Select Applications and then Webmail (If Webmail is not available, this is because it has not been configured, see [Email Domains](#) link above). You will be presented with the following screen:

The screenshot shows a web browser window with a purple header bar that reads "Welcome to the WebMail". Below the header, there is a login form. The form contains three labels: "Username", "Password", and "Language". Each label is followed by an input field. The "Language" field is a dropdown menu showing "English (American)". Below the input fields is a blue "Log in" button.

Welcome to the WebMail

Username

Password

Language

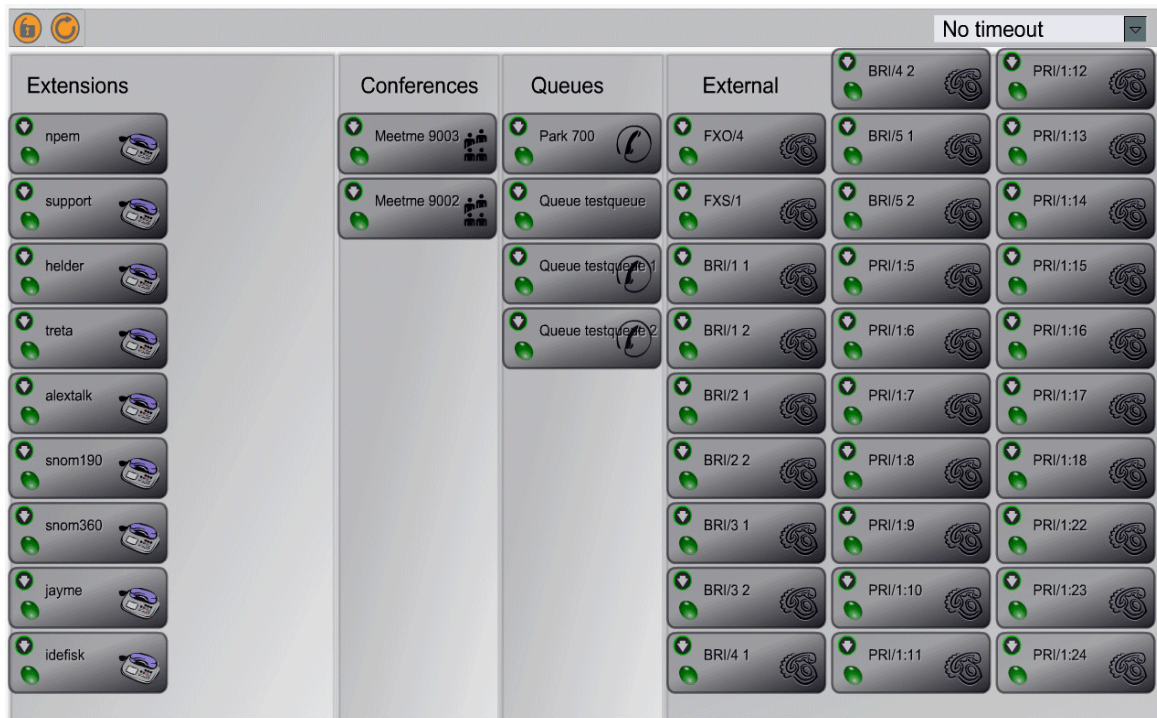
Simply select your preferred language and login with your edgeBOX username and password and use the intuitive interface to send and read emails stored on the edgeBOX.

15.2 Flash Operator Panel (FOP)

Flash Operator Panel (FOP) is a switchboard type application which is able to display information about the PBX activity in real time.

Note that if there are more entries than can be shown on the screen, the additional entries can be viewed by placing the mouse to the right of the screen, causing the screen to scroll to the right (and vice-versa)

You are reminded that you need to allow the FOP service on the [Firewall](#) Panel, for access and the [Web Server](#) must be running.



FOP allows you to view:

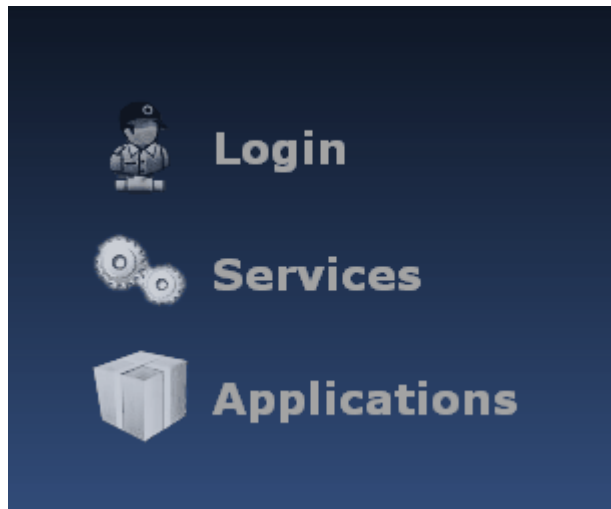
- Which extensions are busy, ringing or available
- Who is talking and to whom
- SIP and IAX registration status (Greys out if offline)
- MeetMe room status (number of participants)
- Queue status (number of users waiting)
- Parked channels
- Logged in Agents

FOP allows you to perform the following actions:

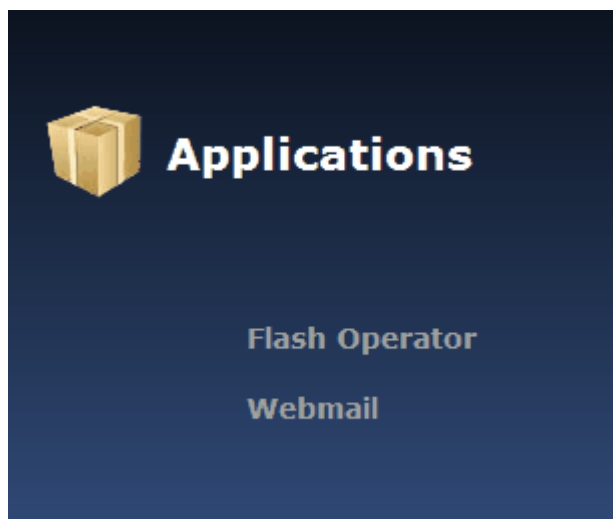
- [Hang-up](#) a channel
- [Transfer a call](#) leg via drag and drop
- [Initiate](#) calls via drag and drop
- [Barge](#) in on a call using drag and drop
- Drag and drop to [create an agent](#)
- [Manage queues](#)
- [Park/Unpark](#) calls

15.2.1 FOP Login

To Access the FOP Interface, enter the edgeBOX URL into your browser, which should present you with the following Menu.



Select the Applications menu and you should be presented with the following:



(If Webmail is not present on the Menu, this is because you have not selected a [Webmail domain](#))

When you select Flash operator, you will be presented with the following screen:

Flash Operator

Security Code:

Login

Operate

Username:

Password:

Login

The default Security Code login is: root

To alter this password, enter username and Password as admin and root (respectively) and set a new password.

15.2.2 Initiate a Call

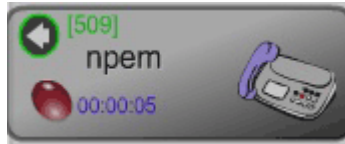


To create a call, simply drag the phone icon for the user of interest to the phone icon of the person you wish to call.



If, for example, you drag the npem phone icon to the jayme icon, npem's phone will ring.

If npem picks up the call, jayme's phone will ring and the call is established.



Once the call is established, both phones will change their green 'LED' to red and the extension number of the caller will be shown, as well as the duration of the call.

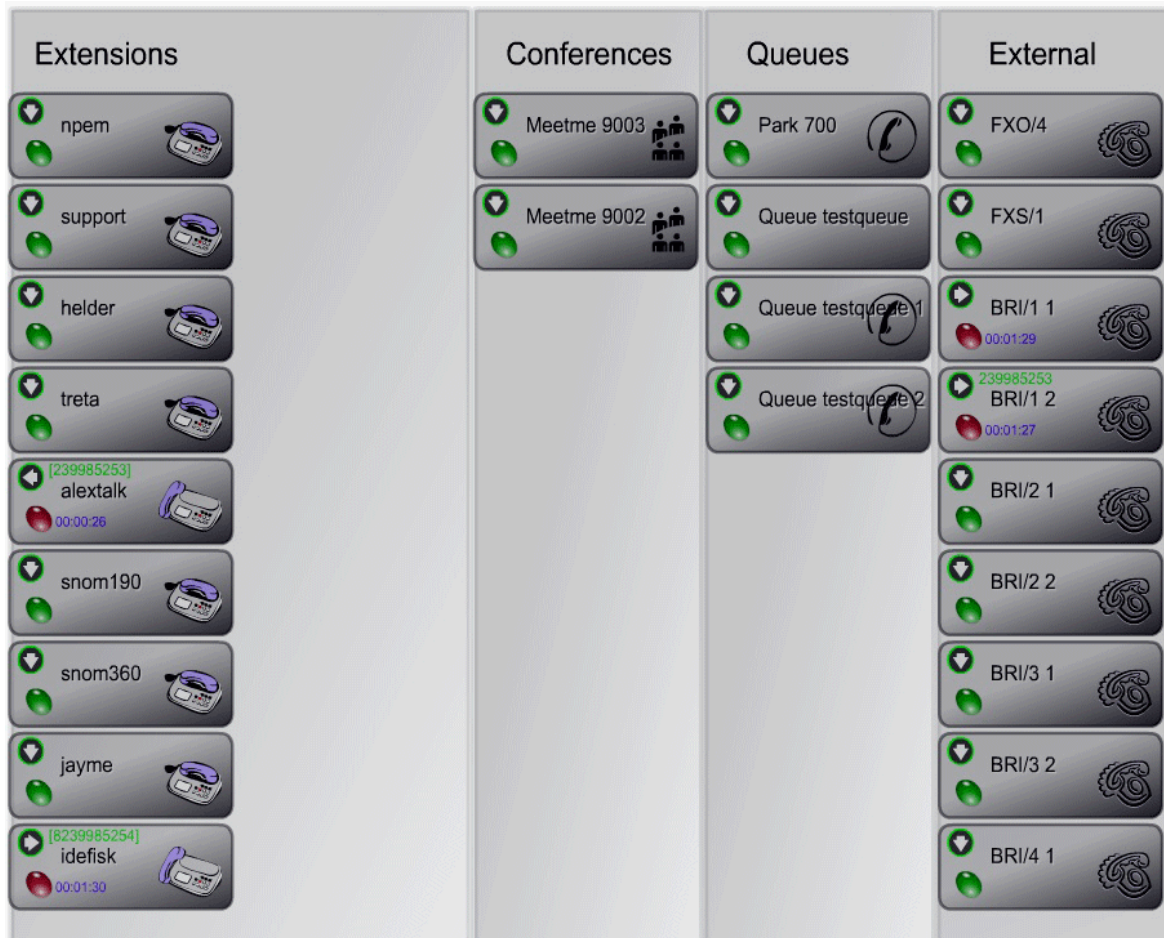
You may force the termination of a call, by double clicking on the red LED.

Note: If a phone is not currently registered with edgeBOX (as thus cannot be rung), the icon will be greyed out.

15.2.3 External Calls

A call which is from an outside line, tags the incoming route with the callers number and also tags the person they have called, with their telephone number.

In the large panel below, the caller has rung alextalk via the BRI/1 2 connection (as they both have the same tel number tag of the external caller).



Again, you may terminate a call by double clicking the red LED of the phone (or the line).

15.2.4 Transfer a call

To transfer a call, you simply drag the icon to the panel where you wish to place the call. Thus you could drag a callers icon to a phone, or to a Queue, or park the call (etc).

15.2.5 Barging

Barging allows the operator to interfere with an active call. Thus if 2 users have established a call, you could (although this is not generally recommended) drag a phone to one of the phones which is already connected, to establish a new call (leaving one of the users with a disconnected call!).

15.2.6 Create an Agent

Assuming that you have configured a [Queue](#), you can add phones to the Queue to act as Agents for the Queue.

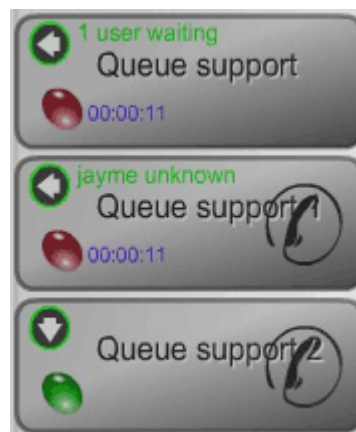
To add an Agent, simply drag the phone to the Queue (the phone LED will change from green to yellow).



To delete the Agent, drag the phone to the queue again (the LED will change from yellow to green).

15.2.7 Queue Managment

Each Queue, consists of three panels, as shown below.



The top panel (Queue Support) shows the status of the queue (1 caller waiting for an Agent) and the queue name (support)

The next two panels show the top two (longest in queue) clients in the queue.

To add a client to the queue, simply drag the ringing phone to the queue, or drag one of the phones which has established a phone connection.

Note: You can reset a queue by double clicking on Queue's (top panel of the three) LED. If you do this, all callers in the queue will be removed.

15.2.8 Park-Unpark Calls

To park a call, simply drag their phone, or their incoming line, to the Parked queue.



The phone/line will then show the their parked position.

You can then drag the parked phone icon to a phone (or elsewhere) to establish a call.

15.2.9 Conference Calls

To enter a conference, simply drag the phone icon (or line) to the conference icon, which will cause the phone to ring.



The Conference will show the number of users of the conference.

15.2.10 Typical Caller Scenario

A typical scenario is as follows:

- A caller (A) rings and is routed to the operator (B). They request C's extension.
- The operator can see that C is not on a call and can drag the line icon to C's phone, or
- The operator can put the caller on hold (by dragging the incoming line to the park icon) and drag the operator phone icon to C's icon to ring C and ask if they wish to take the call.
- The Operator can now either drag the icon from park to C's icon or drag the park icon to their phone icon and explain that C cannot take the call.

16 Appendix A: Authentication

edgeBOX runs several services under which you have to provide credentials. There are a several possible authentication scenarios and configurations.

In this appendix, edgeBOX's authentication architecture will be explained. It is important to understand these concepts, as they will be needed if you want to deploy a remote authentication scenario.

We will be shown what happens when the "Require users to login" option is enabled. The complete sequence of events will be reviewed and detailed. Finally, some remote configuration examples will be shown.

16.1 Authentication architecture

Authentication (proving who you are) and authorisation (what you can do) are handled in a mixed manner in edgeBOX. Considering first a local authentication scenario, upon user creation you need to provide a password and define which services a user will be authorised to use.

Services available in edgeBOX are:

- Regular services, such as POP3, IMAP, FTP and Internet access for LAN users;
- Windows use (Samba Print and Filesharing);
- Allow authentication from wireless and wired 802.1x port based authentication devices on the LAN;
- PPTP
- VoIP.

Internally, edgeBOX uses a Radius server, configured to use a LDAP backend.

16.2 Require users to login vs Group Policies

Connections originating from the LAN to the Internet, to the DMZ network and to services running on edgeBOX are granted by default. But you may choose to limit this access by enforcing an access policy. This is done by enabling "Require users to login" on the Firewall panel. The policies are enforced at the [firewall](#) level.

This is always the first level of access to be tested - if users are required to login (here 'users' refer to LAN users), any connections of the type mentioned above (the exceptions is to edgeBOX's authentication page and to edgeBOX's control centre) are denied - they are in fact discarded by the firewall.

If an user wants to access the Internet, the following steps must be taken:

- The user accesses edgeBOX's authentication page or some website running on port 80 (which causes a redirection to edgeBOX's authentication page);
- The user enters his credentials (username/password);
- If the credentials entered were valid, the user may or may not be granted access, depending on his policy profile.

From this moment on, and if this user's policy grants him access to the Internet, he will be able to access any remote service. Furthermore, a pop-up window will be displayed, allowing him to log out. This pop-up window must be kept open to keep the user authenticated. If this window is closed and no network traffic is detected originating from this user's machine, the authentication will time out and the user will have to re-authenticate in order to access the Internet. The timeout is set to five minutes.

Policies/profiles allow the following items to be configured:

- QoS classes assigned to WAN/DMZ connections;
- Access to the Internet: time interval and services;
- Access to edgeBOX's services: time interval and services;
- Access to the DMZ: time interval and services;
- Inter VLAN access.
- Access to IPsec VPNs.

As have been mentioned previously, the policies are handled at the firewall level. After an user authenticates, appropriate firewall rules are loaded in order to enforce his policy profile. A user authenticating from a PC in the LAN will in fact revert to an IP/MAC address pair, and each rule loaded will refer to this pair. If the profile to which the user belongs to was granted access to the Internet, a firewall rule will be loaded allowing all traffic originating from this host to the Internet.

If a profile contains an IP address and users are required to login is enabled, then firewall rules reflecting this policy profile featuring this IP will automatically be loaded, making it a static entry. That is, if a user uses a machine with an IP in a profile, they will be automatically authenticated by the edgeBOX and will have the profile's privileges (rather than the users profile privileges)

A typical use of this feature is to automatically allow servers to access the Internet. Suppose you have a Windows update server. By making its IP a member of a group with access to the Internet will automatically enable access to the Internet for this server.

16.3 Putting all together

Suppose a user inside a LAN tries to access the Internet or an edgeBOX service and "Require users to login" is enabled. The complete sequence of events is as follows:

- If the user tries to access edgeBOX's port 8010/8011, access is granted;
- Otherwise, if the user tries to access a website on port 80 or edgeBOX's authentication page, the authentication page is displayed;

- Otherwise (any other application), access is denied by the firewall.
- After entering his credentials, edgeBOX's Radius server is queried. If a reject argument is found, access is denied (authorization failed);
- Otherwise, LDAP is queried. if the password does not match, access is denied (authentication failed);
- Otherwise, access is granted (authorization AND authentication succeeded);
- At this point, rules reflecting this user's group policy are loaded into the firewall. The IP/MAC address pair in these rules are the user's PC IP/MAC address pair.
- If the user has requested a web page and his policy allows, his browser will be redirected to the web page requested and a small window will pop-up, containing a message indicating success and a logout button. Otherwise, access will be denied.
- If the user closes the pop-up window and no network traffic is generated for 6 minutes, the rules will be unloaded from the firewall and further connections denied. The user will have to reauthenticate.
- Otherwise, the user will be granted access according to his policy.

16.4 Remote configuration

So far we have assumed edgeBOX handles both authentication and authorization using its local radius and ldap servers. However, these two functions can be delegated on remote servers, allowing for a multitude of different configurations and scenarios.

Due to the concept of system-wide authentication, all services will be authenticated against the scheme chosen, be it local or remote. There are some services however, namely PPTP and Wireless that allow you to use another (Radius) server to perform authentication.

The following matrix displays the possible combinations for authentication/authorization schemes:

Authorisation	Authentication
Local Radius	Local LDAP
Local Radius	Remote LDAP
Local Radius	Remote AD
Local Radius	Remote Radius
Remote Radius	Remote Radius
Remote LDAP	Remote LDAP

The first line matches edgeBOX's local configuration (all local). You can have a remote configuration replicating this configuration, in which Radius performs authorisation, having a LDAP backend performing authentication/authorisation.

Special remarks have to be made when you delegate authorisation/authentication on a remote LDAP or Radius or Active Directory (without "import users" checked) server. As users are remote, they are not known to edgeBOX before they make their first successful login. Before this happens

no user account is created locally and the same applies for edgeBOX's local Radius and LDAP servers (edgeBOX always keeps a local copy).

When using Active Directory as a remote authentication scheme, you have the option to import the users. In such a configuration, local accounts and entries will be created locally.

If you are using local authorisation, you will still be able to edit user's permissions. In this scenario, after an user logs in for the first time, he will be granted permission to only access "regular services" and no others (eg wireless or windows use).

Bear in mind that although a remote scheme is used, you can still add local users before those users make their first login. This can be useful if you want to set their service permissions beforehand (when using local authorisation) or to set the group to which they will belong (by default they are assigned to the generic group).

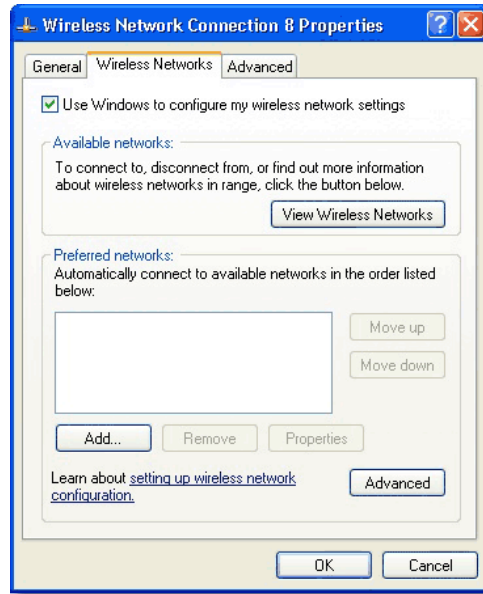
Depending on the scheme used, the way a user may perform his first login will vary. The next table displays this information:

Authentication Scheme Used	First Login
Local, AD (with user import) or Remote LDAP	using any service: FTP, POP3, PPTP, WiFi or LAN
Remote Radius or AD (without user import)	only using LAN authentication.

17 Appendix B: Connecting to Wireless

In this appendix, it will be shown how to configure a MS Windows client station to connect to edgeBOX's [wireless access point](#) using [802.1x](#) and [WPA](#).

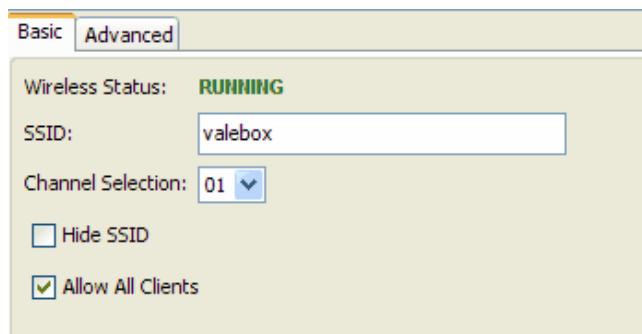
Not all wireless cards will support these security schemes - a firmware upgrade may be needed in some cases. Some cards have their own managing software. In the examples that follow, only the native MS Windows client was used. To be able to have MS Windows controlling your Wireless connection, you must start the "Wireless Zero Configuration" service.



Wireless configuration applet.

Notice that windows is being used to configure wireless

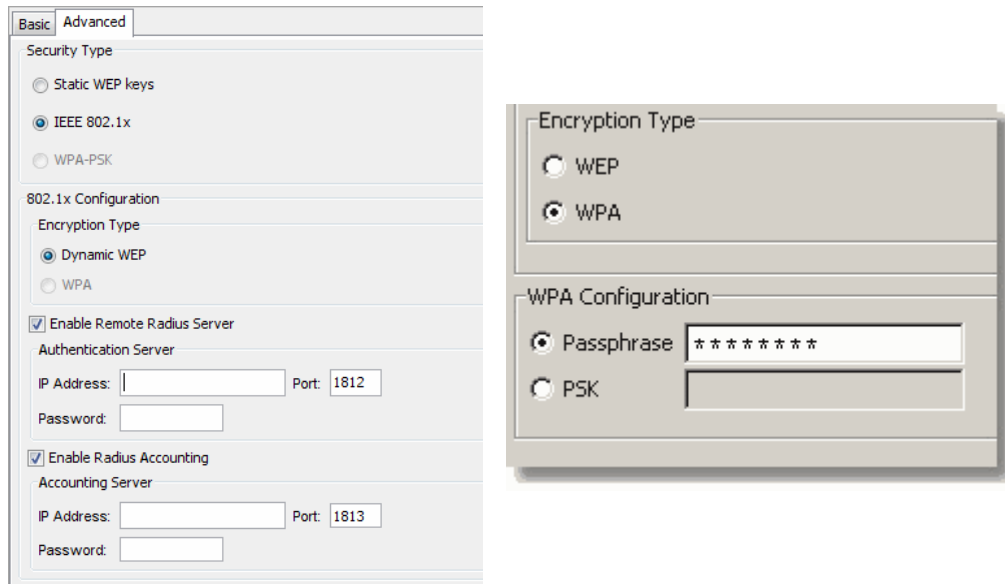
In the examples that follow, the following general configuration will be used:



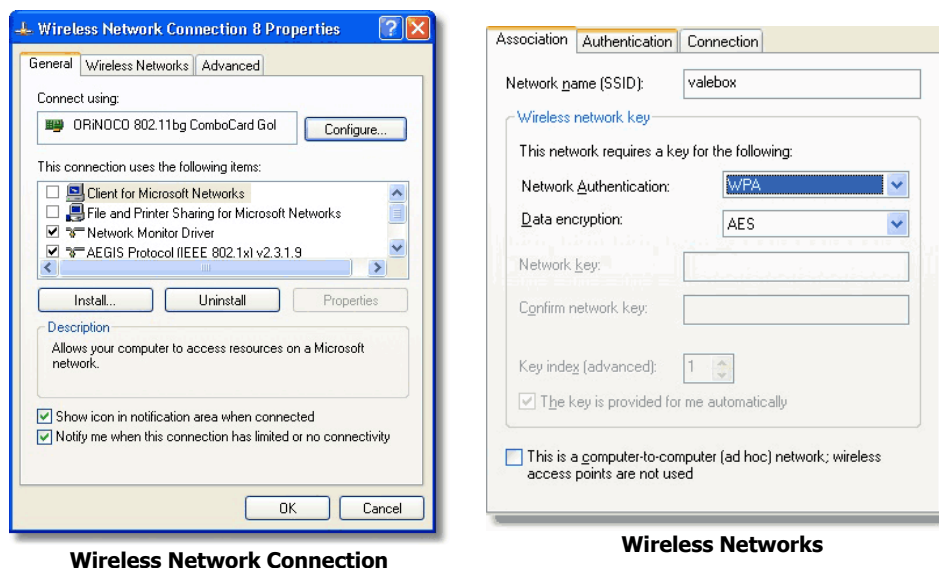
17.1 802.1x

Remember that in order to use 802.1x, you need to authorise "Wireless Security" on the user management.

The following pictures illustrate the configuration used on edgeBOX.



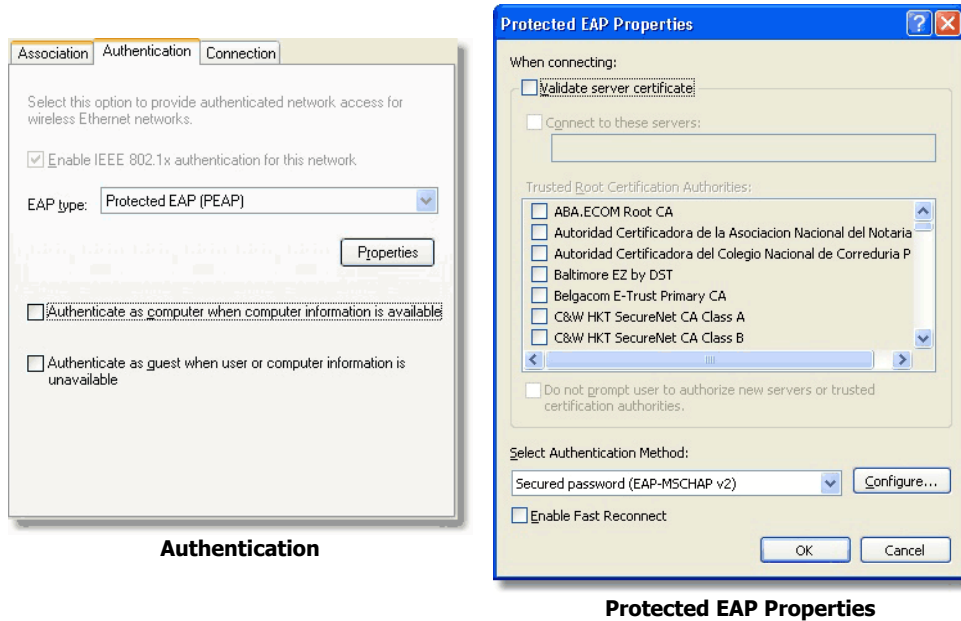
On MS Windows, double-click the "Wireless Network Connection" icon and select the "Wireless Networks" tab. Make sure the SSID entered is consistent with that defined on edgeBOX (valebox on our example). Choose "WPA" for "Network Authentication" and "AES" for "Data Encryption". Select then the "Authentication" tab.



Wireless Network Connection

Wireless Networks

On the Authentication tab, select "Protected EAP (PEAP)" as the "EAP type". Press the "Properties" button. On the dialog window that pops-up, uncheck the "Validate server certificate" checkbox, and select "Secure password" as the Authentication Method. Press the "Configure" button.



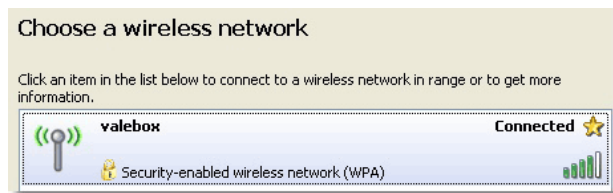
On the dialog window that pops-up, uncheck the "Automatically use my Windows..." checkbox. Press "OK" on all dialogs to confirm this configuration.



If the configuration succeeds, you should see a balloon warning you to enter credentials to connect to the wireless network. Clicking on the balloon will display a prompt requiring you to enter the username and password for a user authorised to connect to the Wireless network.



If the connection was successful, its status will appear as "Connected".



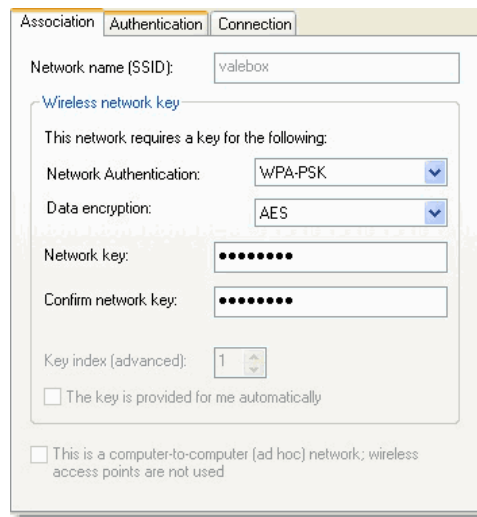
17.2 WPA

If edgeBOX was configured to use WPA as the security scheme, the following settings must be configured on the client:

- Network Authentication: WPA-PSK
- Data Encryption: AES.

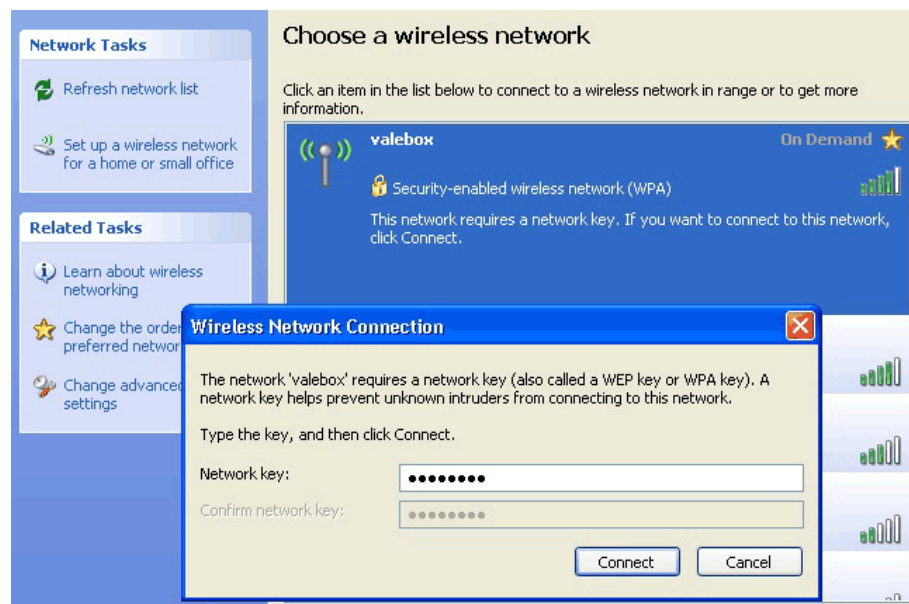
Additionally, the network key to be used must also be supplied. Remember that if you choose to use a preshared key, it must be 64 hexadecimal characters long, if less than 64 characters, it may be ascii or hex. If this connection is configured to be established manually, when you try to connect to it a dialog window will be shown, asking you to supply the network key.

You may obtain an automatically generate key from the website <https://www.grc.com/passwords.htm>.



The 'Wireless Configuration' dialog box has three tabs: 'Association', 'Authentication', and 'Connection'. The 'Authentication' tab is active. It contains the following fields and options:

- Network name (SSID): valebox
- Wireless network key section:
 - This network requires a key for the following:
 - Network Authentication: WPA-PSK (dropdown)
 - Data encryption: AES (dropdown)
 - Network key: [masked]
 - Confirm network key: [masked]
 - Key index (advanced): 1 (spinner)
 - ☐ The key is provided for me automatically
- ☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless Configuration

The 'Network key dialog' is shown over a 'Choose a wireless network' window. The background window lists the 'valebox' network as 'On Demand' and 'Security-enabled wireless network (WPA)'. The dialog box contains the following text and fields:

Wireless Network Connection

The network 'valebox' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key: [masked]

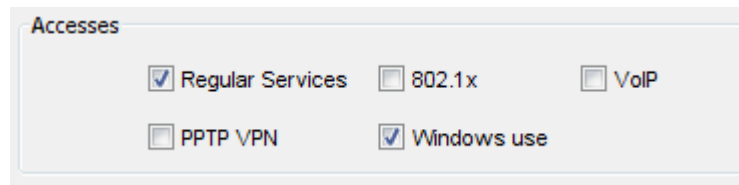
Confirm network key: [masked]

[Connect] [Cancel]

Network key dialog

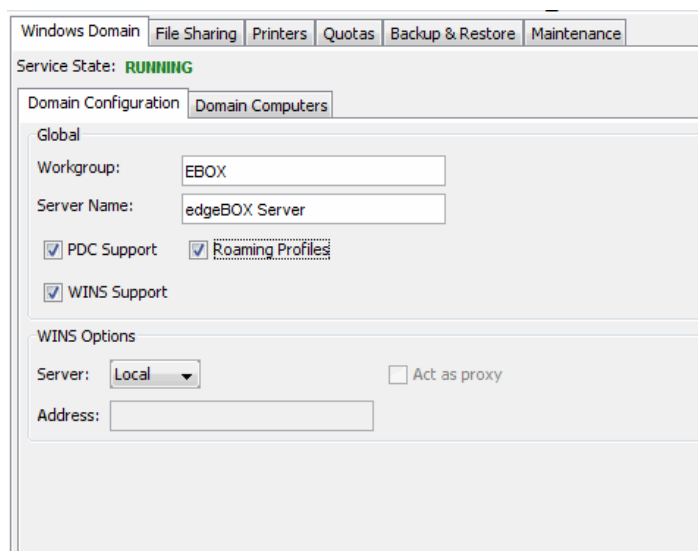
18 Appendix C: Windows Integration

In this appendix it will be shown how to use some of Samba's features, namely how to use [edgeBOX as a PDC](#) and how to use the [public safes](#) functionality. Remember that users must be authorized to use "Windows use" upon their creation in the system.



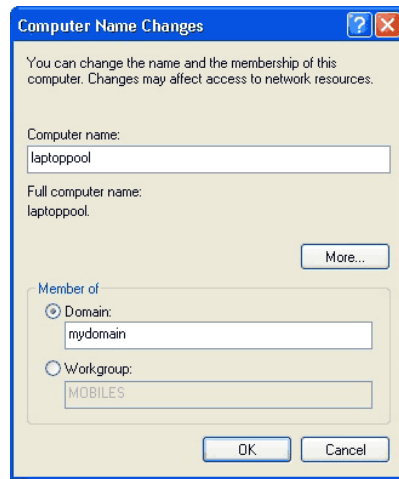
18.1 Configure edgebox to work as a PDC

To configure edgeBOX to work as a PDC all it has to be done is to check the "PDC Support" option on the "Storage and Print" -> "Windows Domain" panel.



To add a machine to edgeBOX's domain, select "System" under the Windows Control Panel, and then select the "Computer Name" tab. Select the "Change" button. In the dialog window that pops-up, select the "Domain" option and enter your domain name (in our example it was "mydomain").

After you select "OK" to confirm the domain change, you will be required to supply credentials of a user belonging to the domain administrator's group. In edgeBOX, you have to specifically supply the username "Administrator", which has the same password as the admin user (defaults to root).



change domain dialog

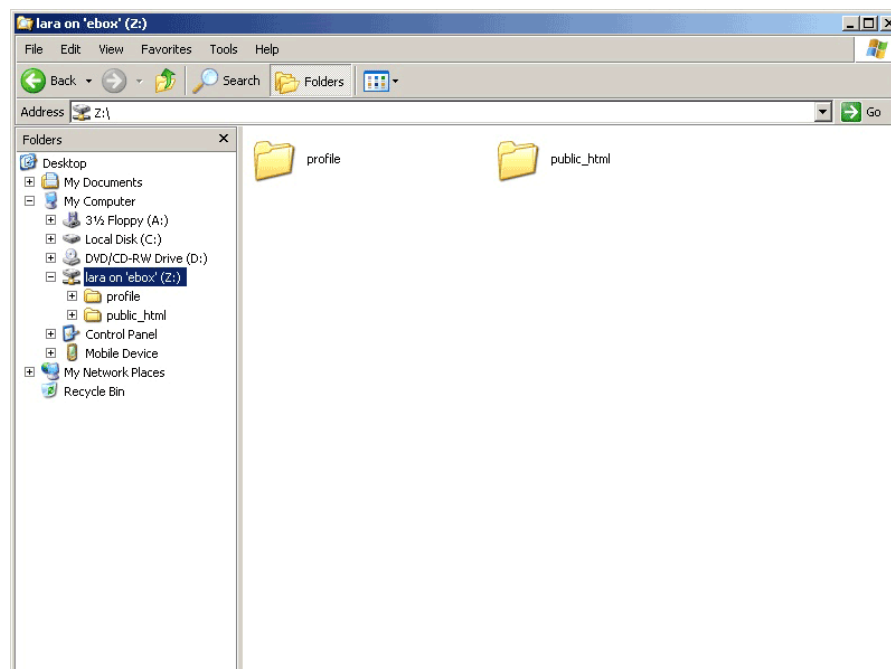


join domain dialog

If the operations was successful, the following dialog will be displayed.



After rebooting the machine, log on to edgeBOX's domain (it should be available on the domains' list). The user's home directory will be mounted as Z:. In the picture below the user's directory content is shown, where the public_html directory can be accessed. This is the directory where the user's personal web page will be located. The other directory shown (profile) is where the roaming profile data will be stored, so the user will retain her desktop definitions after logging off.



19 Appendix D: VLAN based Infrastructure

Introduction to VLANs in the context of the edgeBOX.

19.1 Introduction

With the introduction of VLANs in the edgeBOX architecture we have significantly increased the type of scenarios where an edgeBOX Business Gateway can be deployed. From a basic network infrastructure with generic 802.1Q Switches to full port based authentication devices with dynamic VLAN assignment, a broad range of scenarios are possible.

Some of the supported features depend on the type of Switch or Wireless AP used for deployment.

- For basic VLAN scenarios any 802.1Q switch will work. For advanced features like port based authentication, dynamic vlan assignment, 802.1x with single sign on or automatic guest VLAN more advanced switches will be needed.
- For switches with L3 features it is important to disable inter vlan routing on the switch. Inter vlan routing is done in the edgeBOX with access profile enforcement.

Type of Authenticators supported:

- **Procurve 2650 Series** - 802.1Q, 802.1x SSO and Dynamic VLAN assignment
- **Procurve 420 Wireless AP** (Firmware 2.2.2 or later) - Support for 802.1Q, 802.1X, Dynamic VLAN assignment
- **D-Link DES-1252** - 802.1Q, 802.1x SSO, manual session timeout configuration
- **D-Link DES-1228** - 802.1Q, 802.1x SSO, manual session timeout configuration
- **SMC Tigerswitch 6726 AL2** - 802.1Q
- **Generic L2 switch with 802.1Q VLAN** - 802.1Q VLAN only
- **Generic L2 switch with 802.1Q VLAN and 802.1x** - 802.1Q VLAN + 802.1x Port based authentication. No single sign on available.
- **Generic Wireless AP with 802.1x** - 802.1x Authentication only. No single sign on available.

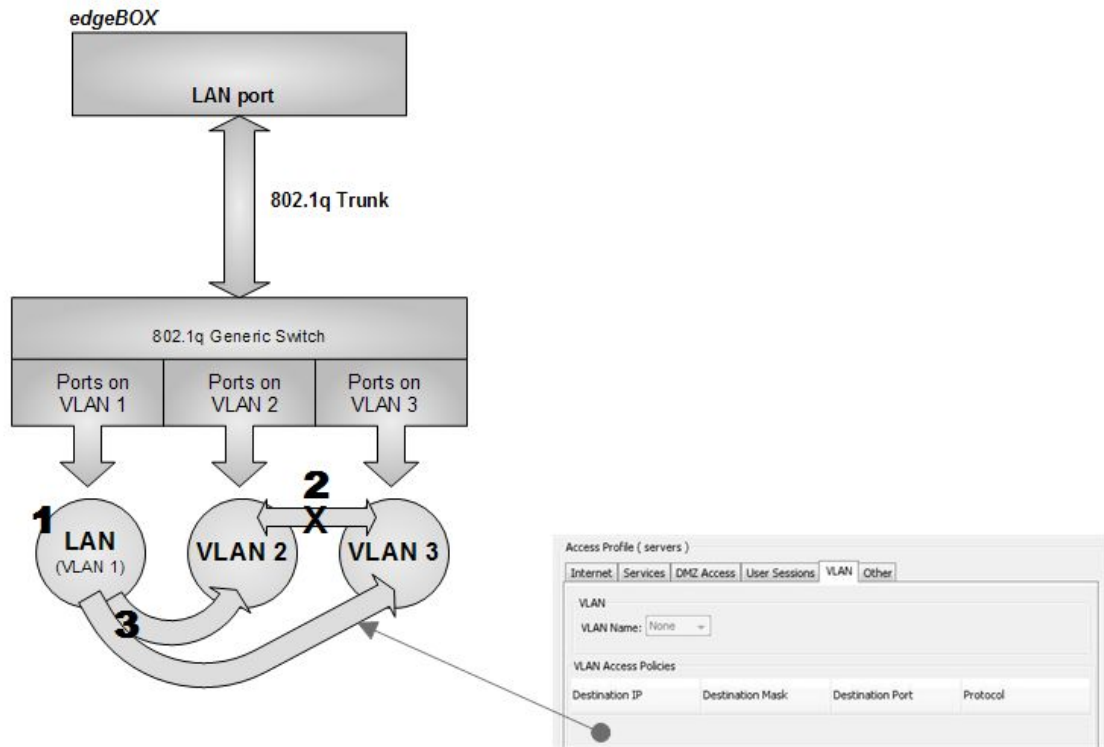
Type of 802.1x supplicants tested (PEAP-EAP-MSCHAPv2):

- Windows XP SP2
- MacOS X
- Windows Vista
- Windows Vista SP1

19.2 VLAN Scenario 1

Characteristics of this scenario:

- Standard 802.1q compatible switch
- No 802.1x port based authentication
- No Dynamic VLAN assignment
- No native Guest VLAN on switch



This is the most basic scenario when deploying VLANs with edgeBOX. In this case the LAN port of the edgeBOX is connected to a trunk port in the switch. The port on the switch must be configured as 802.1q trunk, allowing all configured VLANs to pass through the link.

1 - When using VLANs, the LAN zone is the same as VLAN 1 (id 1). In most cases the VLAN 1 is the default VLAN on a new installed switch, and this means all ports are by default configured as being part of that VLAN.

2 - By default, all traffic between VLAN zones is blocked. This means the edgeBOX firewall does not allow routing of traffic between VLANs unless the administrator configures it with different type of access rules.

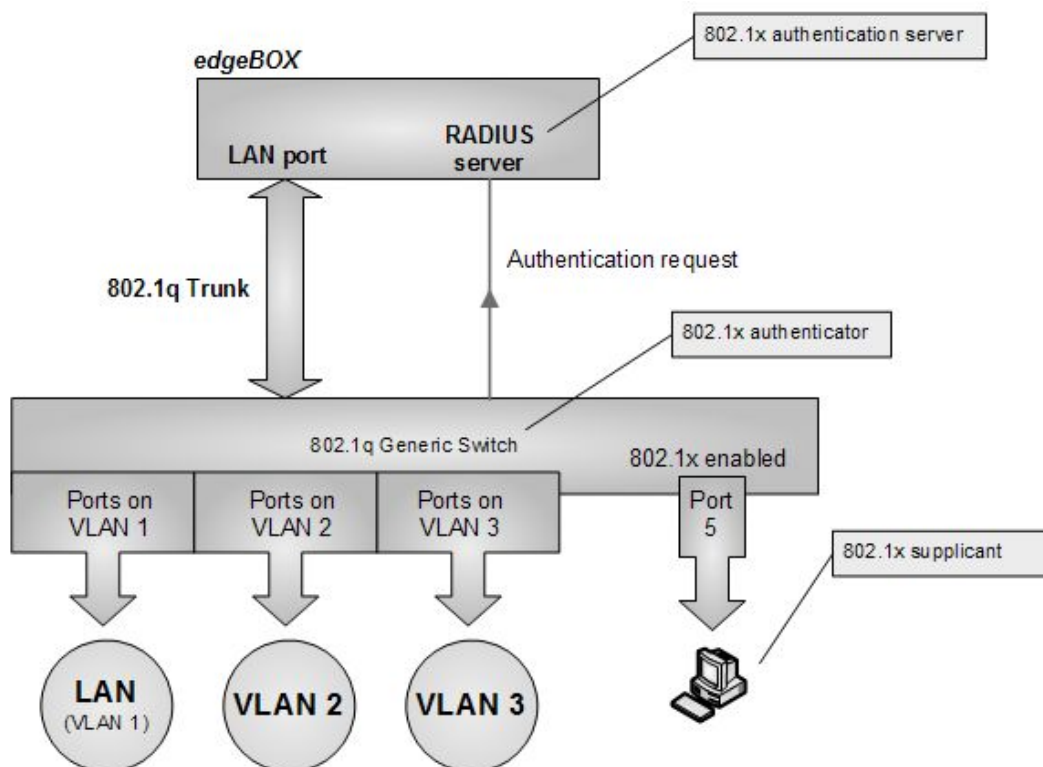
3 - Access Rules between VLAN segments can be configured per access profile in the VLAN tab.

4 - The only type of user authentication available is Web Login. When a user authenticates successfully, the firewall enforces the configured User Access Profile rules for WAN, DMZ and access to other VLAN segments. If the user is not able to authenticate with success, then all traffic to and from this user will be filtered with the default rules for non-authenticated users.

19.3 VLAN Scenario 2

Characteristics of this scenario:

- Standard 802.1q compatible switch with 802.1x
- Support for 802.1x port based authentication
- No Dynamic VLAN assignment
- No native Guest VLAN on switch



This is basically the same as Scenario 1. The only addition is that we have some or all ports on the switch configured for 802.1x port based authentication.

To enable support for 802.1x port based authentication we need to configure the switch to use the edgeBOX as the Radius server for authentication and enable the ports where we want this enforced. On the edgeBOX this 802.1x based switch, the radius client, needs to be authorized, and this is done in System->Radius->Add.

The edgeBOX supports protocol PEAP-EAP-MSCHAPv2. Both Windows XP and Vista include supplicants with native support for this authentication type.

In this scenario, for a client PC connected to one of the switch ports configured with 802.1x, the switch detects the presence of a client and initiates the 802.1x protocol. The authentication request, made by the Client PC supplicant, will be forwarded by the switch to the configured Radius server for authentication. If the authentication is successful the switch will open the respective port and the client will be part of the static VLAN configured on that Port. At this point the client will get an IP address if configured with dhcp and the edgeBOX DHCP server is enabled.

If the authentication is not successful then the port will be closed and the user will not get access to the network.

The main advantage of using 802.1x is that the user will not be able to access the network until he is able to get a successful authentication.

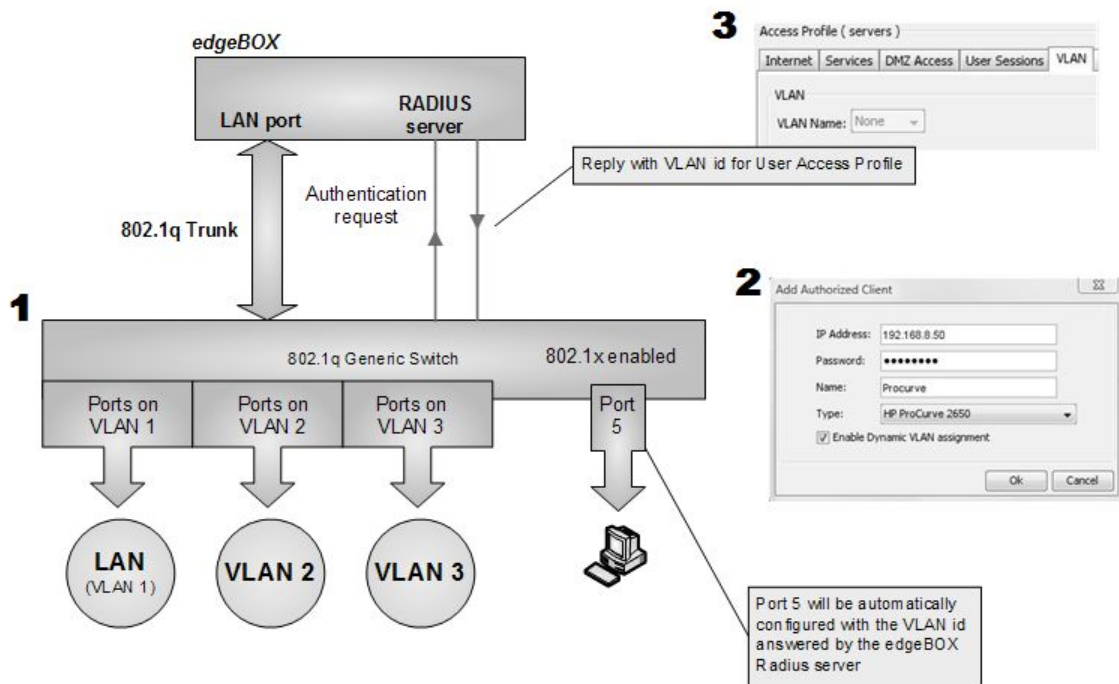
Support for Single Sign On (SSO)

Scenarios based on 802.1x include support for automatic user login. The only requirement is that a supported 802.1x switch is used to deploy those scenarios. A supported switch includes the calling station MAC address in the Radius Access Request packet and is able to process session timeout. In case the 802.1x switch does not support the calling station attribute, the port based authentication is still done but the user will need to do a normal weblogin when accessing the Internet or services running on the gateway.

19.4 VLAN Scenario 3

Characteristics of this scenario:

- 802.1q compatible switch with 802.1x and dynamic VLAN assignment
- Support for 802.1x port based authentication
- Support for Dynamic VLAN assignment – (HP Procurve switch)
- No native Guest VLAN on switch



This is scenario 3 with a switch that supports VLAN dynamic assignment. In this case, after a successful authentication, the switch moves the associated port to the VLAN configured for that user access profile. Without a successful authentication the port will be closed and the user won't be able to access the network.

During 802.1x authentication and on success, the Radius server sends additional attributes to the 802.1x authenticator in the switch with information regarding the VLAN id for that particular user. The edgeBOX supports assignment of a VLAN per access profile.

The following is needed to deploy this feature:

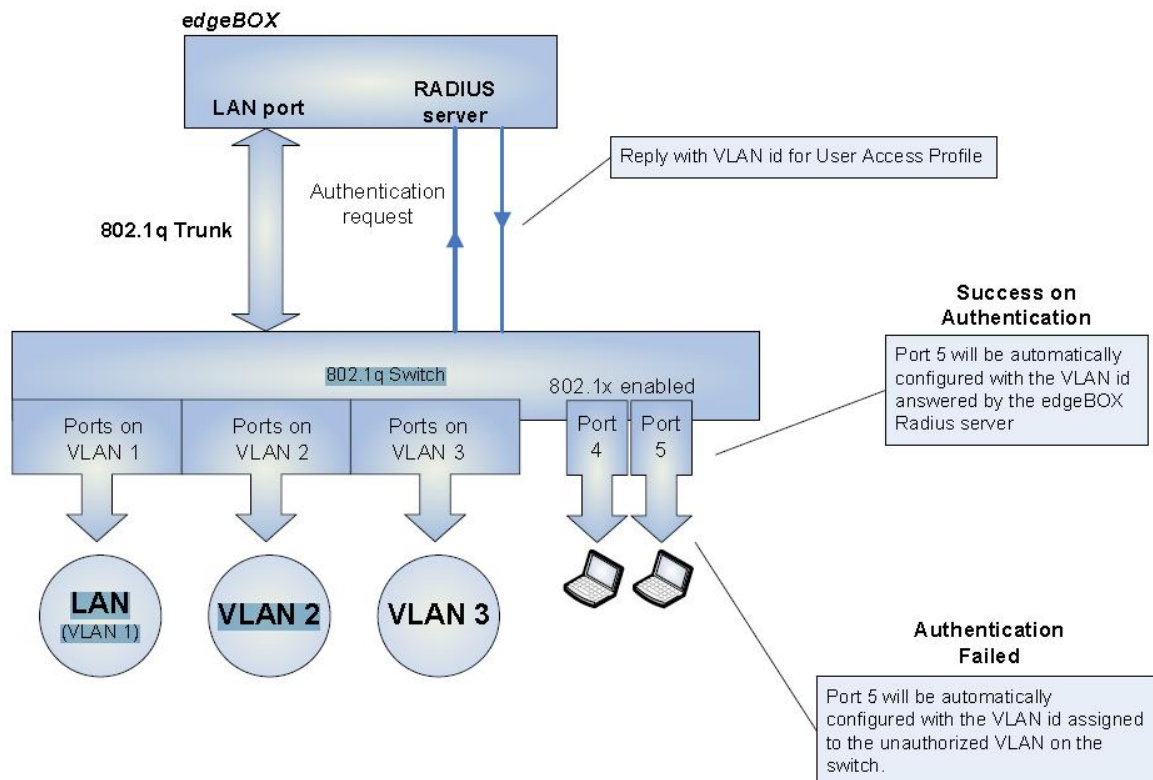
1. The network infrastructure must be setup with Procurve 2650 or compatible switches in terms of Radius dynamic Vlan assignment. The HP Procurve follows RFC2868 / 3580 with with Tunnel-Private-Group-ID of type string.
2. Configure the radius client as referred in Scenario 2, select the correct client type and enable Dynamic VLAN assignment.
3. Configure the User Access Profiles with the correct VLANs. See NAC->Access profiles->"Profile"->VLAN->VLAN Name.

The advantage of this scenario is the fact that we can effectively do network access control by port and at same time we are able to put the user in the correct VLAN even if he does a login outside of his main work space.

19.5 VLAN Scenario 4

Characteristics of this scenario:

- 802.1q compatible switch with 802.1x and dynamic VLAN assignment
- Support for 802.1x port based authentication
- Support for Dynamic VLAN assignment – (HP Procurve switch)
- Native Guest VLAN on switch – (HP Procurve switch)



This is scenario 4 with a switch that supports guest VLAN when operating with 802.1x and VLAN dynamic assignment. This is similar with scenario 3 and the only difference is when the 802.1x user is not able to authenticate. At this point the switch automatically configures the port to another VLAN – the Unauthorized-Client VLAN. The unauthorized-client VLAN can be configured using the 802.1x Open VLAN mode in the Procurve 2650.

As soon as the switch assigns the unauthorized-client VLAN to that port, the connected host is able to get an IP through DHCP. If the edgeBOX authentication is enabled, the user will be presented with the edgeBOX web login page when trying to access the Internet.

A practical example:

- Switch ports 4 and 5 are setup for 802.1x with Unauthorized-Client VLAN assigned to VLAN6. These ports are located in a meeting Room.

- User01 is a member of the engineering profile, configured for VLAN3 (see #3 in scenario 3).
- User01 has his laptop ethernet connection setup for 802.1x authentication.
- Engineering profile has access to Internet, LAN and a few servers located in VLAN2.
- Guest01 is a member of the guest profile.
- Guest01 is a guest user with just a regular dhcp configuration on his laptop.
- Guest profile is configured to have open access to the Internet only. Users in this profile are not able to access any of the other VLANs or LAN.
- When User01 connects to port 4, a successful 802.1x authentication takes place and the switch port is automatically configured for VLAN3. User01 is able to work on his own VLAN and access any other places allowed by his Engineering access profile.
- When Guest01 connects to port 5, the switch is not able to start a 802.1x authentication and automatically opens the port on VLAN6. At this point he is able to get an IP address through dhcp and when trying to access the Internet he will be presented with the authentication page. With a successful web login authentication, the edgeBOX enforces the guest profile for this user and he is able to access the Internet but nothing else.
- Any other user that tries to connect to one of these ports, without a successful authentication, will be isolated in VLAN6.

20 Appendix E: Others

Information about how to make a factory reset to edgeBOX, how to create virtual hosts and how to view and understand the VoIP Log file.

20.1 Factory Reset

The factory reset option is only available through the CLI. It is available through the VGA console, the serial port or using SSH to connect to one of the IP addresses of the edgeBOX.

Log in to the CLI with user "admin" and use the command "system factory" to initiate a factory reset. Please be aware that this option clears all configuration, user data and updates since the first time the edgeBOX was installed. As soon as this command is executed, the system will reboot and the hard disks will be re-imaged with the original first install contents.

20.2 Virtual Hosts

You can host several websites in edgeBOX and access them using different hostnames. The HTTP server will fetch the correct website requested. This is the web server's [virtual hosts](#) feature. Next is a description on how to create virtual hosts.

Suppose you want to have an internal domain local.loc, and want to have two websites: www.local.loc (the main website, for example a company's website) and a departmental website, for example marketing.local.loc. To have this configuration, you should perform the following steps:

1. Create DNS hosts for the websites you want to create. In this case, if the internal IP of edgeBOX is 192.168.100.254, you will have to create A records in DNS, pointing to this address for www and marketing. For information on creating records on DNS, check [Hosts](#).

Note: The edgeBOX will attempt to create the DNS entries for you.

2. Next, you will need to upload files to your websites. For clarity, you can create two separate directory trees for your websites. The steps to do this are:
 - In GUI under the HTTP panel [change/set the webmaster's password](#) (if you haven't done so yet);
 - Connect to edgeBOX's FTP server with the webmaster username and password.
 - Upload the files for your websites;
3. For the virtual hosts' configuration, under the HTTP panel select [New](#) in the virtual hosts section to create a new virtual host. In the window that pops-up, insert the following:
 - Virtual Host: LAN (in this case, we are configuring a LAN-only accessible virtual host);
 - Server Name: marketing;

- Document Root: change to "path" and insert "marketing" (the name of the directory created - this is a relative path to the web site's root);
 - Email: the email for the webmaster responsible for this website. It is not a mandatory field.
4. After applying this information, you will be able to access marketing.local.loc. However, the main website will probably not be available and so, you will need to create another virtual host, this time for your main web site. Select "New" again, to add a virtual host and enter the following data:
- Virtual Host: LAN;
 - Server Name: www;
 - Document Root: inter.
5. After applying this information, you should be able to access your main site using http://www.local.loc, and the marketing website using http://marketing.local.loc.

20.3 View and understand the VoIP Log File

You can obtain the VoIP log files via **FTP** with the **logmaster account**. They are stored with the filename **Master.csv** (the current log file). The log files are rotated daily (Master.csv.1-7) and **kept for seven days**, after which the oldest file is overwritten by the new log file.

The entries in the Log file have the following meaning:

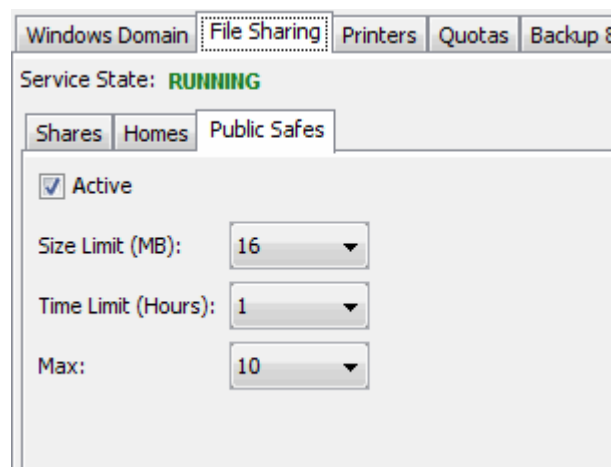
accountcode	What account number to use (Only used when Authentication is enable)
src	Caller*ID number
dst	Destination extension
xt	Destination context
clid	Caller*ID with text
channel	Channel used
dstchannel	Destination channel if appropriate
lastapp	Last application if appropriate
lastdata	Last application data (arguments)
start	Start of call (date/time)
answer	Anwer of call (date/time)
end	End of call (date/time)
duration	Total time in system, in seconds (integer)
billsec	Total time call is up, in seconds (integer)
disposition	What happened to the call: ANSWERED, NO ANSWER, BUSY
amaflags	What flags to use: see amaflags::DOCUMENTATION, BILL, IGNORE

21 Public Safes

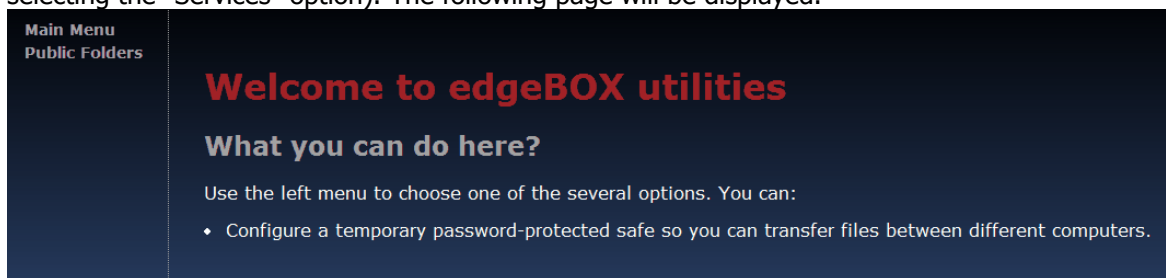
Safes are available only for LAN users and may be used when there's a need for a temporary space for storage. Any user on your network can ask for a box to store files and access it as a normal Windows share. To be able to use safes, the following conditions must be met:

- The Samba service must be started;
- Public Safes must be active;
- The user must be authorised to use Samba.

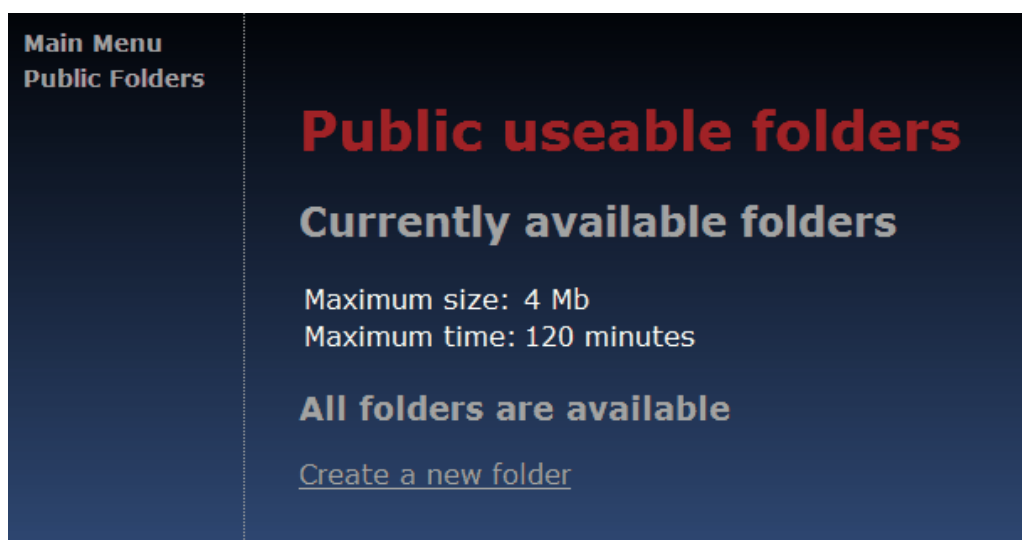
The options available for configuration are the maximum size of safes, their maximum availability and the maximum number of safes active at the same time.



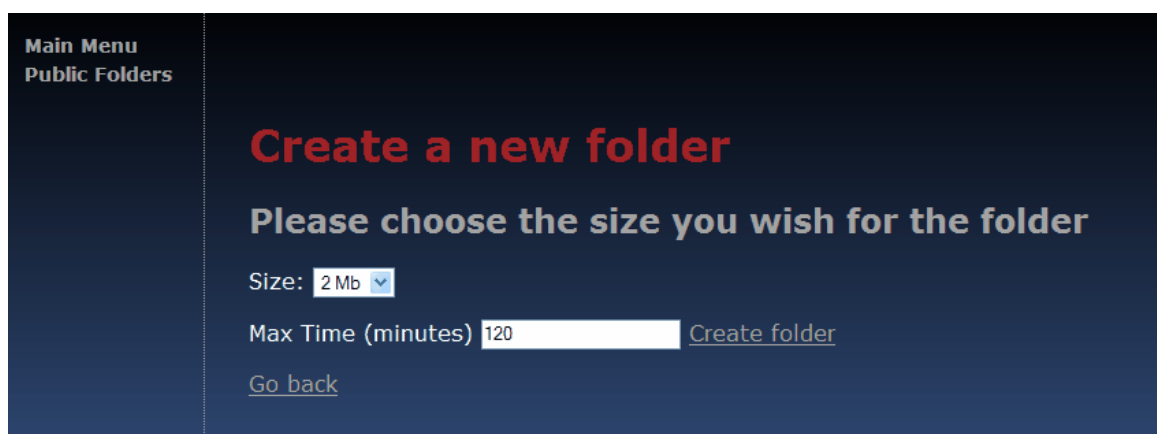
Any LAN user can request a safe accessing the utilities page (<http://<lan address>:8010> and selecting the "Services" option). The following page will be displayed.



Follow the link "Public Folders". Currently available safes will be displayed, as well as the current safes' configuration parameters. To create a new safe, select "Create a new safe".

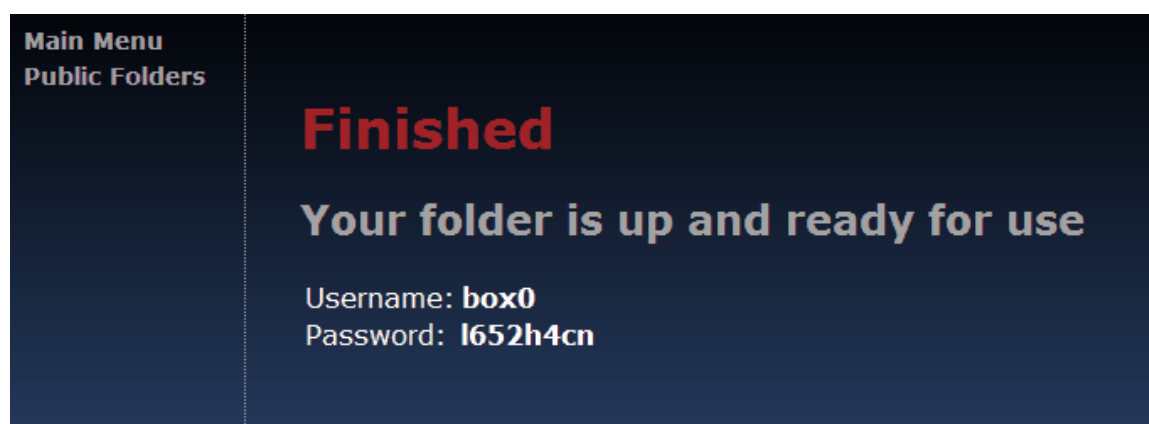


Select the desired settings for your safe. Sizes available will always be less than or equal to the maximum size configured, as well as the maximum time the safe will be available. To create the safe, select "Create safe".



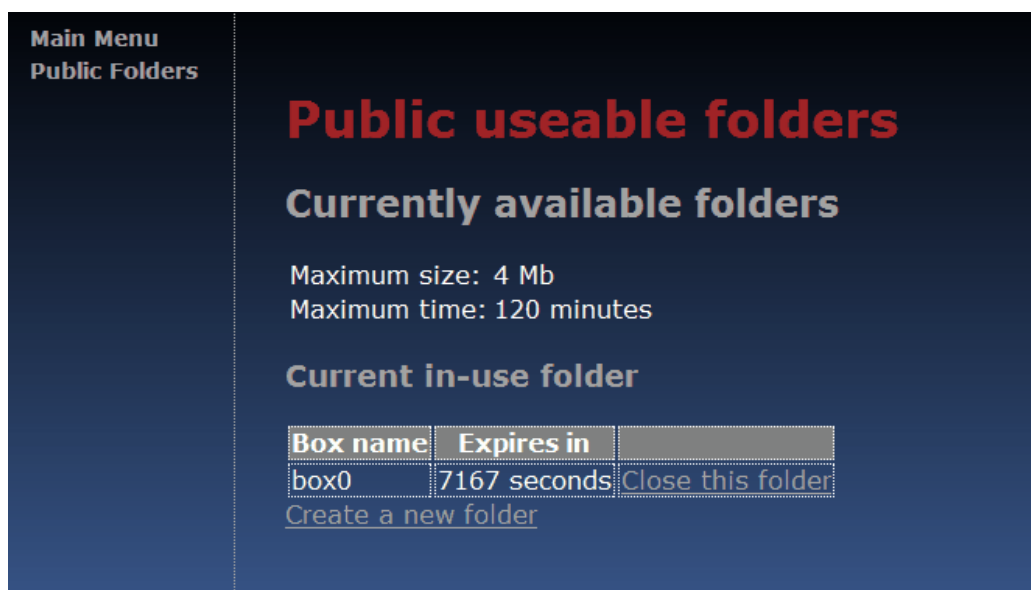
Safe creation window

If the safe was successfully created, credentials to access it will be displayed.



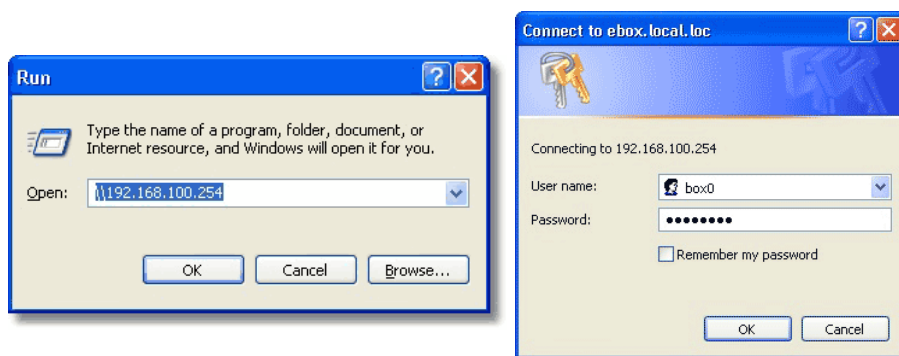
credentials to access the safe

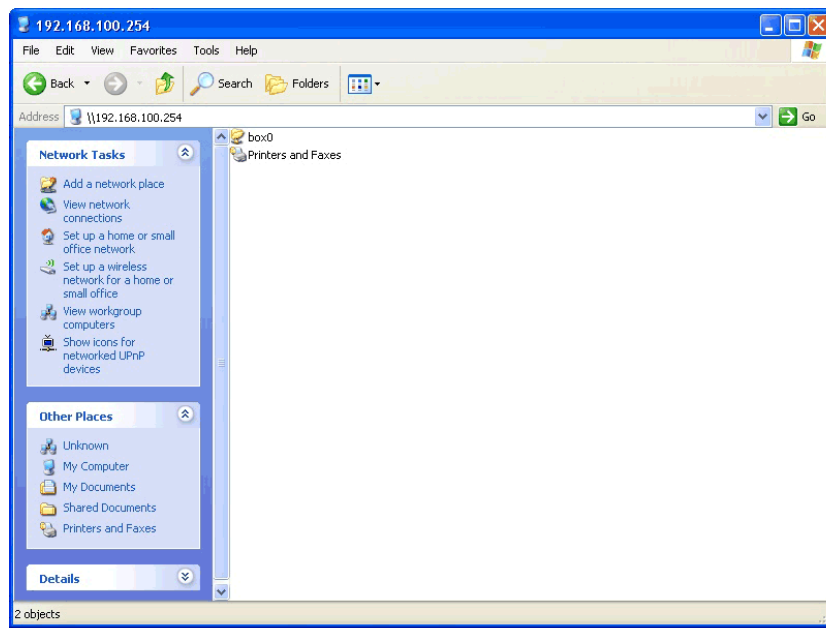
Selecting "Public Folders" again will now display the safe just created.



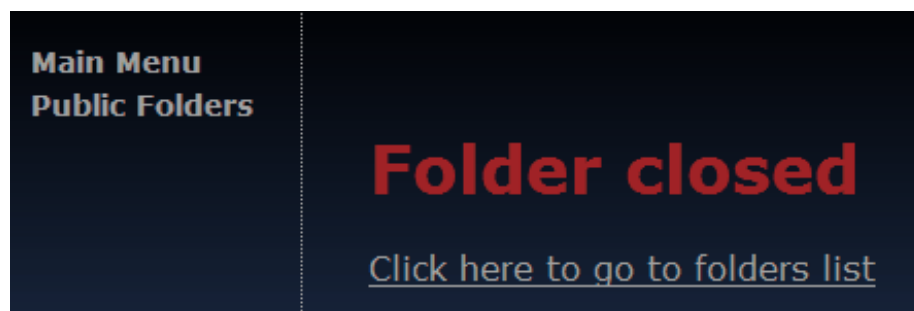
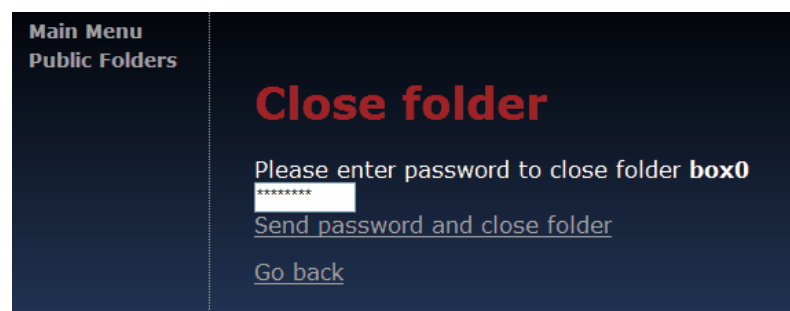
Public safes list

To use the safe, access it like a normal windows share, entering the credentials supplied to authenticate.





If you want to close the safe before its time expires, go to the Services > "Public Folders" menu and follow the "Close this Folder" link next to the safe you want to close. You will need to supply the password for the safe. If the operation completes successfully, the message "Folder closed" will be displayed.



Note: When a Folder is closed (manually or after the timeout), the folder and contents are deleted.

22 Acronyms

Throughout the edgeBOX interface the following acronyms are used:

AD	Active Directory
ADSL	Asymmetric Digital Subscriber Line
AP	Access Point
CDR	Call Detail Records
CLI	Command Line Interface
CN	Common Name
CNAME	Canonical Name
DB	Database
DC	Domain Component
DHCP	Dynamic Host Configuration Protocol
DID	Direct Inward Dialing
DNS	Domain Name Server
DSCP	Differentiated Services Code (Control) Point
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
FOP	Flash Operator Panel
FXO	Foreign eXchange Office
FXS	Foreign eXchange Subscriber
GRE	General Routing Encapsulation
HPEC	High Performance Echo Cancellation
HTTP	HyperText Transfer Protocol
IAX	Inter-Asterisk eXchange
ICMP	Internet Control Message Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPSEC	IP Security
ISP	Internet Service Provider
iTEMS	Desktop based application used to manage and monitor groups of edgeBOXes
ITSP	Internet Telephony Service Provider
IVR	Interactive Voice Response
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Interchange Format
LLC	Logical Link Control

MAC	Media Access Control
MX	Mail Exchange
NAC	Network Access Control
NAT	Network Address Translation
NS	Name Server
NTP	Network Time Protocol
OID	Object Identifier
PBX	Private Branch eXchange
PDC	Primary Domain Controller
PDF	Adobe Portable Document Format
POP	Post Office Protocol
POTS	Plain Old Telephone Service
PPPOA	Point-To-Point Over ATM
PPPOE	Point-To-Point Over Ethernet
PPTP	Point-To-Point Tunneling Protocol
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network
QOS	Quality Of Service
SIP	Session Initiation Protocol
SME	Small Medium Enterprise
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Service Set Identifier
TCP	Transport Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications Service
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
VC	Virtual Circuit
VCi	Virtual Channel Identifier
VOIP	Voice Over Internet Protocol
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WINS	Windows Internet Naming Service
WPA	Wi-fi Protected Access