

1 Enhancements in firmware 2.20

Firmware version 2.20 provides the following enhancements over the predecessor version:

- *WEBconfig* and HTTP module
- HTTP status
- Firewall filter
- Support for modem dial-up (up to V.90)
- SYSLOG module

1.1 Configuration with *ELSA WEBconfig*

The device can be configured using any web browser, including text-based browsers. The *ELSA WEBconfig* application is integrated in *ELSA LANCOM Business* devices. All you need is a web browser to access *ELSA WEBconfig*.

ELSA WEBconfig features setup wizards similar to those of *ELSA LANconfig* for the convenient configuration of *ELSA LANCOM Business* devices. Unlike *ELSA LANconfig*, *WEBconfig* works under any operating system that will support a web browser.

A LAN connection via TCP/IP (PPP for remote configuration) must be established to use *ELSA WEBconfig*. *ELSA WEBconfig* is accessed via the IP address of the *ELSA LANCOM Business* device. You must therefore know this address.

What is the IP address of the router?

An unconfigured *ELSA LANCOM Business* router will appear in your network under the IP address x.x.x.254. In the case of Class A networks with a subnet mask of 255.255.0.0 and network address of 10.1.x.x, the address will be 10.1.0.254. To determine the effective IP address of your router, you therefore need to know your network number and netmask.

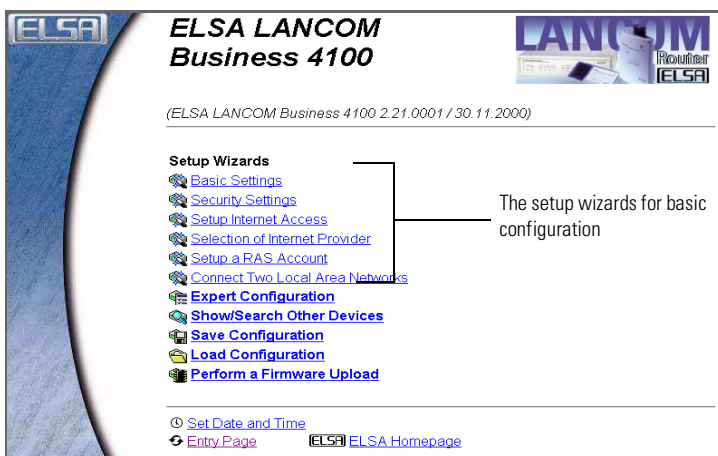
Communication with the device can then be realized within the network using a web browser and Telnet via this IP address.

Calling up *WEBconfig*

Start your web browser (Internet Explorer, Netscape Navigator) and enter the following Internet address:

```
http://<IP address of LANCOM>
```

The following main menu will be displayed:



Extensive, context-sensitive documentation for the individual expert configuration functions can be accessed at any time using the **Help (reference manual)** link.

The **ELSA WEBconfig** help files (HTTP module)

The **Help (reference manual)** link points to help files in HTML format. In its default setting, the Help link points to the ELSA web pages.

You may also download the help files from the ELSA web pages and save them at the location of your choice. We recommend storing the help files on your local computer, or on a server that you can access at any time. This can be either a file server or a web (HTTP) server.

Storing the files on a local machine has the advantage that the files are accessible in the event of a network malfunction. On the other hand, installing the files on a server will permit access to the help function from anywhere in the network without the need to install the help files on every computer. Access to the server via the network is a precondition for this, of course.

Once you have selected an option and stored the help file at the appropriate place, the path to the file must be entered in *ELSA WEBconfig*. In *ELSA WEBconfig*, please select **Expert Configuration ► Setup ► HTTP Module ► Document Root**.

Two important points should be noted with regard to the syntax:

- ① Specify the path only up to the directory containing the complete help file structure.

For example, if you have created the help file structure '400\1\4100\ in the local directory 'C:\ELSA\HTMLRef', then specify 'file://C:/ELSA/HTMLRef' as the document root.

- ② Minor differences will apply to the path depending on the type of installation (local, file server, HTTP server) and operating system. Examples are given in the table, with. The names and paths used can be selected freely.

Version	Operating systems	Example
Local	Windows	file://C:/ELSA/HTMLRef
	Linux	file://usr/lib/ELSA/HTMLRef
Fileserver	Windows NT, Windows 2000, Novell, UNIX	file://Server1/ELSA/HTMLRef
HTTP server	all	http://<IP-Adresse>/ELSA/HTMLRef

Replace the placeholder <IP-Adresse> with the valid IP address of the HTTP servers in 'x.x.x.x' format, for example '128.7.9.155'.

You can download the current version of the HTML Help from the ELSA web pages at any time.



1.2

HTTP status

Firmware 2.20 now provides a statistics menu for HTTP configuration. You will find the following information under /Status/TCP-IP statistics/HTTP statistics:

HTTP access	Total number of pages opened
HTTP not found errors	Number of accesses to pages not found in the device
HTTP authentication errors	Number of accesses rejected because of a missing or wrong password
HTTP protocol errors	Number of accesses that could not be answered by the device because an unknown HTTP query was sent or this form of query was not permitted (e.g. setting values over a read-only connection)

The command **Delete Values** resets all counters to zero. This also occurs implicitly with a **Delete Values** in the TCP/IP menu.

1.2.1

Data packet filtering—firewall

The firewall filters of the *ELSA LANCOM Business* devices feature filter functions for individual computers and also for entire networks. These filters effectively protect your network against intruders.

Setting up the filter

There are several options for setting up the firewall filters:

- **LANconfig**

IP router ► Filter

*The filter function can only be accessed in LANconfig if 'Complete View of Configuration' is selected under **View ► Options**.*

- **WEBconfig**

Expert Configuration ► Setup ► IP router module ► Firewall

- **Telnet**

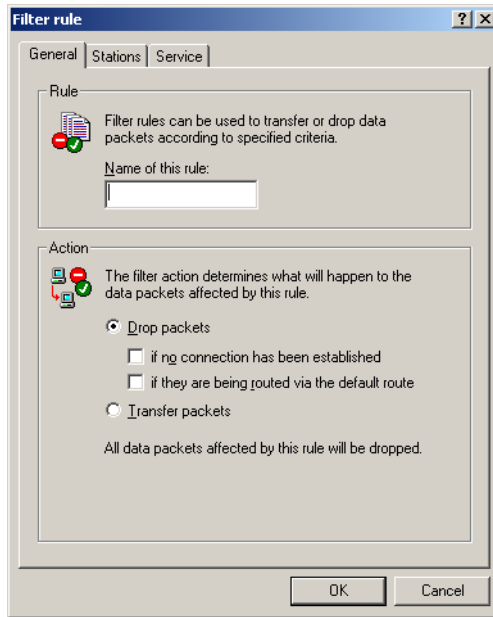
/Setup/IP router module/Firewall

Please note that all procedures access the same configuration data. For example, if you change the filter settings in LANconfig, this will also have a direct effect on the values under WEBconfig and Telnet.



Setting up filters under *ELSA LANconfig*

It is particularly easy to set up the filter with *ELSA LANconfig*. The following tabs under 'Filter' can assist you to define the filter rules.



- 'General'
The name of the filter service and what should happen with the data packets (action) are specified here.
- 'Stations'
The stations for which the filter rule should apply—as sender or receiver of the packages—are specified here.
- 'Services'
The IP protocols, source and destination ports to which the filter rule should apply are specified here.

Setting up filters under *ELSA WEBconfig* or Telnet

The configuration under *WEBconfig* or Telnet is somewhat more difficult than under *LANconfig*.

Here the filter functions are set in the filter list which is based on the entries of two other tables. The first is an object table in which the computer, networks, protocols, etc. are defined as objects. The second is a rules table in which source, target and action are described with the aid of the individual objects. The actual filter list is generated from these two tables.

The filter list can also be created directly, but this is not required. Making the required entries in the object and rules tables is sufficient for the filter list to be generated. This ensures that no inconsistent entries are made in the filter list.

What can be filtered? Source and target filters can be set for individual ports or for ranges of ports. In addition, individual protocols or any combinations of protocols (TCP/UDP/ICMP) can be filtered.

A definable action can be executed as soon as a filter condition occurs.

Object tables

The elements or objects to be used in the rules table are defined in the object table. Objects can be:

- Protocols
- Single computers
- Whole networks
- Services

These elements can also be combined in any way. Objects can also be defined hierarchically. Therefore, objects for the TCP and UDP protocols can be defined first. Then objects can be added later for items such as FTP (= TCP + Ports 20 and 21), HTTP (= TCP + Port 80) and DNS (= TCP, UDP + Port 53). They can then be combined to one object that contains all definitions of the individual objects.

The direct descriptions that you can include here will be covered in more detail in the following section on the “rules table”.

The rules table

The objects are associated with filter rules in the rules table. The rules table contains the protocol to be filtered (which you have defined in the object table), the source objects, the target objects and the filter action to be performed.

The protocol and the source or target objects can contain combined objects and also direct descriptions (e.g. %P6 for TCP), which are separated by '+' or spaces. A direct description is indicated by '%'. Possible descriptions are:

Description	Function
%A	IP address
%M	Netmask
%S	Service (port)
%L	Local network
%H	Host name
%P	Protocol (TCP/UDP/ICMP etc.)

Similar descriptions can generate lists separated by commas, such as host lists/address lists (%A10.0.0.1, 10.0.0.2) or ranges separated by hyphens, such as port lists (%S20-25). Insertion of a '0' or an empty string indicates the any object:

all computers: %A0.0.0.0

all services: %S0

all protocols: %P0

Host names can only be used if the *ELSA LANCOM Business* can resolve the names in IP addresses. To do this the *ELSA LANCOM Business* must have learnt the names via DHCP or NetBIOS, or the assignment must be entered statically in the DNS or IP routing table. An entry in the IP routing table can associate an entire network to a host name.

Filter list

The filter list is ultimately put together from the object table and the rule table. This forms the merge quantity of all filters defined by the rules and objects.

Please note that filters are not created in the event of an error in input nor are error messages output. If you configure the filters manually, you should always check that the desired filters have been created.



1.3 Support for modem dial-up

ELSA LANCOM Business routers support analog dial-up connections via their ISDN S₀ connections. Conventional modems can thus dial in directly. V.90, V.34 and V.32bis are the available modulation types.

Only one analog connection is currently supported at any given time. If a second modem attempts to connect it will receive a busy signal.

All ISDN channels are set up to accept both digital and analog calls by default. This setting can be restricted to either analog or digital. The menu for this setting can be found under:

- **LANconfig**

Communication ► Router interfaces

- **WEBconfig**

Expert configuration ► Setup ► WAN module ► Router interface list

- **Telnet**

Setup/WAN-module/Router-interface-list

1.4 The SYSLOG module

The SYSLOG module gives the option of recording accesses to the *ELSA LANCOM Business*. This function is of particular interest to system administrators, because it allows a full history of all activities to be kept.

To be able to receive the SYSLOG messages, you will need an appropriate daemon or client. In UNIX/Linux the SYSLOG daemon, which is installed by default, generally does the recording. It reports either directly through the console or writes the protocol to a SYSLOG file.

In Linux the file `/etc/syslog.conf` directs which facilities should be written to which log file. Check in the configuration of the daemon whether network connections are explicitly monitored.

Windows does not have any corresponding system functions. You will need special software that fulfills the function of a SYSLOG daemon.

1.4.1

Setting up the SYSLOG module

There are several options for setting up the SYSLOG module:

- **LANconfig**
Management ► Messages
- **WEBconfig**
Full configuration ► Setup ► SYSLOG module, or
Log and Trace ► Configure SYSLOG module
- **Telnet**
/Setup/SYSLOG module

1.4.2

Example configuration with *ELSA LANconfig*

Create SYSLOG client

- ① Start *ELSA LANconfig*. Under 'Management', choose the 'Messages' tab.
- ② Turn the module on and click **SYSLOG clients**.
- ③ In the next window click **Add...**
- ④ First enter the IP address of the SYSLOG client, and then set the sources and priorities.

The screenshot shows a dialog box titled "SYSLOG clients - New Entry". It contains the following fields and options:

- IP address:** A text box containing "10.0.1.160".
- Source:** A group of checkboxes:
 - ☒ System
 - ☒ System time
 - ☒ Connections
 - ☐ Administration
 - ☒ Login
 - ☐ Console login
 - ☐ Accounting
 - ☐ Router
- Priority:** A group of checkboxes:
 - ☒ Alert
 - ☒ Warning
 - ☐ Debug
 - ☒ Error
 - ☒ Information

Buttons for "OK" and "Cancel" are located at the top right.

SYSLOG comes from the UNIX world, in which specified sources are predefined. *ELSA LANCOM Business* associates its own internal sources with these predefined SYSLOG sources, the so-called "facilities".

The following table provides an overview of the significance of all message sources that can be set in the *ELSA LANCOM Business*. In addition, the last column of the table indicates the association of the

internal sources of the *ELSA LANCOM Business* and the SYSLOG facilities.

Source	Meaning	Facility
System	System messages (boot processes, timer system etc.)	KERNEL
Logins	Messages regarding login and logout of a user during the PPP negotiation and errors occurring during this process.	AUTH
System time	Messages regarding changes to the system time	CRON
Console logins	Messages regarding console logins (Telnet, outband, etc), logouts and errors occurring during this process.	AUTHPRIV
Connections	Messages regarding establishing and releasing connections and errors occurring during this process (display trace).	LOCAL0
Accounting	Accounting information after release of a connection (user, online time, transfer volume).	LOCAL1
Administration	Messages regarding configuration changes, remotely executed commands etc.	LOCAL2
Router	Regular statistics on the most frequently used services (sorted by port numbers) and messages regarding filtered packets, routing errors etc.	LOCAL3

The original eight priority stages defined in the SYSLOG are reduced to five stages in the *ELSA LANCOM Business*. The following table shows the relationship of alarm level, significance and SYSLOG priorities.

Priority	Meaning	SYSLOG priority
Alarm	All messages requiring the attention of the administrator are collected under this heading.	PANIC, ALERT, CRIT
Error	All error messages that can occur during normal operation without requiring administrative intervention are sent to this level (e.g. connection errors).	ERROR
Warning	Error messages that do not affect normal operation of the device are sent to this level.	WARNING
Information	All messages that are purely informative in character are sent to this level (e.g. accounting information).	NOTICE, INFORM

Priority	Meaning	SYSLOG priority
Debug	Transfer of all debug messages. Debug messages generate a high data volume and impair the correct operation of the unit. They should therefore be disabled in regular operation and should only be used for troubleshooting.	DEBUG

- ⑤ When you have defined all parameters, confirm your input with **OK**. The SYSLOG client will be written to the SYSLOG table.

Facilities

All messages from *ELSA LANCOM Business* can be assigned to a facility with the **Facility Assignment** button and then are written to a special log file by the SYSLOG daemon with no additional input.

Example

All facilities are set to 'local7'. Under Linux in the file '/etc/syslog.conf' the entry

```
local7.* /var/log/lancom.log
```

writes all outputs of the *ELSA LANCOM Business* to the file '/var/log/lancom.log'.

