

## 1

# Enhancements in firmware 2.10

Firmware version 2.10 includes the following enhancements to the previous version:

- *WEBconfig*
- SYSLOG module
- Firewall filter
- HTTP module
- DHCP client
- HTTP status

## 1.1

## Configuration with *ELSA WEBconfig*

You can use any web browser, even text-based, for basic setup of the device. *ELSA WEBconfig* uses setup wizards similar to *LANconfig* and has all you need for easy configuration of the *LANCOM* under all possible operating systems.

To connect to the *LANCOM*, there must be a TCP/IP LAN connection. Access is usually through the device's IP address:

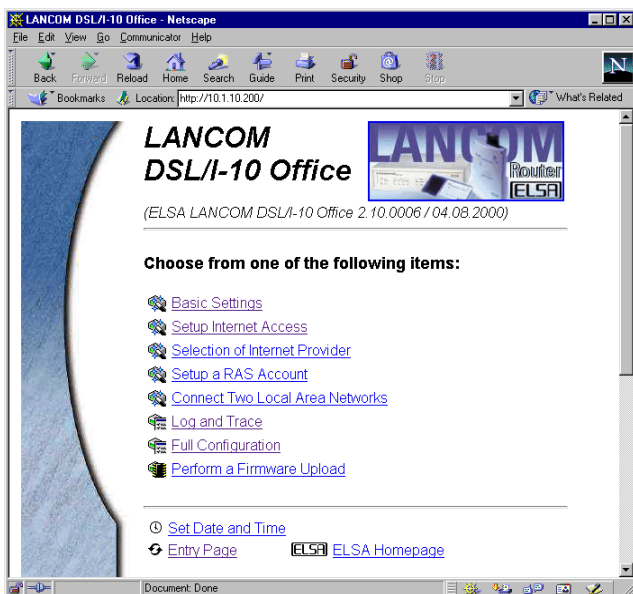
```
http://<LANCOM IP address>
```

An unconfigured or reset *LANCOM* actually responds to all IP addresses. The only requirement is that '254' must be at the end of the IP address (e.g. `http://10.0.0.254`, but also `http://192.168.0.254`).

*Once a DHCP server is enabled in the LAN, the exact IP address allocated to the LANCOM by the DHCP server must be addressed.*



Comprehensive, context-sensitive documentation on the individual *WEBconfig* pages and fields is accessible at all times in *WEBconfig* via the link 'Help (Reference Manual)'. More information on setting up the context-sensitive help system linked to *WEBconfig* can be found in the '1.4 HTTP module' section.



## 1.2 The SYSLOG module

The SYSLOG module gives the option of recording accesses to the *LANCOM*. 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 fulfils the function of a SYSLOG daemon.

## 1.2.1

### Setting up the SYSLOG module

There are several options for setting up the SYSLOG module:

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

## 1.2.2

### 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.

**SYSLOG clients - New Entry**

IP address: 10.1.0.160

Source:

☒ System      ☒ Login  
☒ System time      ☐ Console login  
☒ Connections      ☐ Accounting  
☐ Administration      ☐ Router

Priority:

☒ Alert      ☒ Error  
☒ Warning      ☒ Information  
☐ Debug

OK Cancel

SYSLOG comes from the UNIX world, in which specified sources are predefined. The *LANCOM* as supplied maps its own internal sources to the predefined sources. These are generally referred to as “facilities”.

The following table shows an overview of the switchable message sources and their significance. The last column also shows the alignment

between the internal sources of the *LANCOM* and the SYSLOG facilities as supplied.

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 eight priority stages defined in the SYSLOG are reduced to five stages in the *LANCOM*. 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
Debug	This is the lowest priority. Debug messages should never be sent.	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 *LANCOM* messages 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 *LANCOM* to the file '/var/log/lancom.log'.

## 1.3

### Firewall

The firewall filters of the *LANCOM* devices offer filter functions for individual computers and also for entire networks. 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.

The filters are set up with the aid of two tables. One is the object list, in which computers, networks, protocols etc. are defined as objects. The second is the rules list, in which source, target and action are described with the aid of the individual objects. The actual filter table is generated from these two tables.

This makes it unnecessary to create the filter list yourself, thereby eliminating the possibility of inconsistent entries appearing in the filter table.

#### Object list

The objects to be filtered can be defined in the object list. Objects can be:

- Protocols
- Single computers
- Whole networks
- Services

These elements can also be combined in any way. Objects can also be defined recursively. 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 everything enabled.

### The rules table

In the rules table the individual objects are combined into filter rules. The rules table contains the protocol to be filtered, the source objects, the target objects and the required filter action.

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 *LANCOM* can resolve the names in IP addresses. To do this the *LANCOM* 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).

### The 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.*

### 1.3.1

## Setting up the filter

There are several options for setting up the firewall filters:

- *WEBconfig*  
Full Configuration ► Setup ► IP router module ► Firewall
- *LANconfig*  
IP router ► Filter
- Telnet  
/Setup/IP-router-module/Firewall

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.

*Please note that during configuration with LANconfig, object tables that were set up by telnet or WEBconfig are only available in modified form after a rewrite.*



- 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 are specified here.
- Services  
The IP protocols, source and destination ports to which the filter rule should apply are specified here.

## 1.4

## HTTP module

You can specify the root document for the HTML help files with the HTTP module. In its default setting the Help link points to the ELSA web pages. If you wish to have the help files on a local drive, you can enter the directory for these files here.

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



## 1.5

### DHCP client

Firmware 2.10 allows the devices to take an IP address automatically from a DHCP server in the network. The menu item 'Setup/DHCP-module/Operating' has additional functions:

In 'Auto' status the device searches for other DHCP servers in the network. If one is found, its own DHCP server is not enabled and the device obtains an IP address from the one found. This only occurs if the device itself is still unconfigured, i.e. both Internet and Intranet address are still 0.0.0.0. Once configured, the automatically obtained address is no longer valid.

## 1.6

### HTTP status

Firmware 2.10 now provides a status 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.