

A Addendum to LCOS Version 8.0

A.1 Overview

- 'IPSec over HTTPS' →Page 1
- 'Basic HTTP file server for LCOS 8.0' →Page 3
- 'Automatic upload of firmware or configuration from external data media' →Page 4
- 'SSH client' →Page 6
- 'Alternative boot config' →Page 9
- 'Alternative DHCP server for forwarding' →Page 13
- 'Channel-load display in WLC mode' →Page 13
- 'Changes in LANconfig' →Page 14
- 'Activating 802.1x accounting for logical WLANs in WLAN controllers' →Page 15
- 'LANCOMContent Filter' →Page 16
- 'DFS3' →Page 33
- 'Alternative URLs for CRLs' →Page 34
- 'Broken link detection' →Page 34

A.2 IPSec over HTTPS

A.2.1 Introduction

In some environments it is impossible to establish a secured VPN connection over an existing Internet connection due to an interim firewall that blocks the ports used by IPsec. To be able to set up an IPsec-secured VPN connection in such a situation, LANCOM VPN routers support the technology known as IPSec over HTTPS.

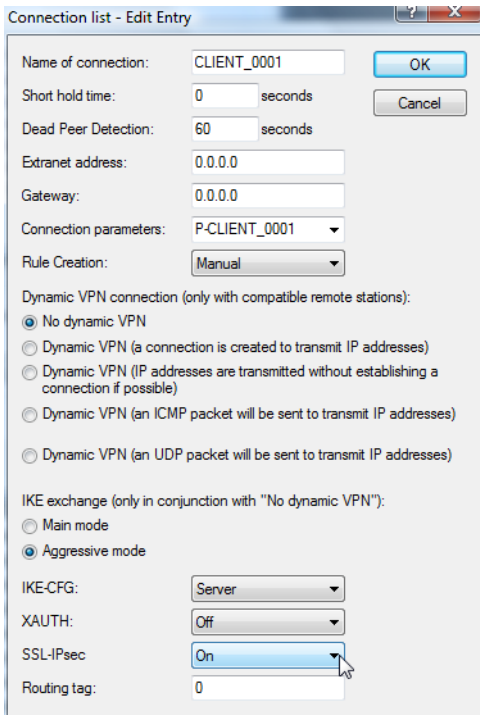
The first attempt always tries to establish data communications with standard IPsec. If the connection cannot be established (e.g. because IKE port 500 is blocked by a cellular network), then an attempt is then automatically made to establish a connection that encapsulates the IPsec VPN in an additional SSL header (port 443, like https).

Note that IPSec over HTTPS technology only works when both ends of the connection support this function and that the corresponding options have been activated. IPSec over HTTPS is available in LANCOM VPN routers with LCOS 8.0 or higher, and with the LANCOM Advanced VPN Client 2.22 or higher.

A.2.2 Configuring IPSec over HTTPS technology

For the active establishment of a connection from one LANCOM VPN device to another VPN remote by using IPSec over HTTPS technology, activate the option in the VPN name-list entry that corresponds to the remote site.

- LANconfig: VPN ► General ► Connection list
- WEBconfig: LCOS menu tree ► Setup ► VPN ► VPN remote sites



■ **SSL-IPsec**

With this option you activate IPsec over HTTPS technology when actively establishing a connection to this remote site.

Possible values:

- On, off

Default:

- Off

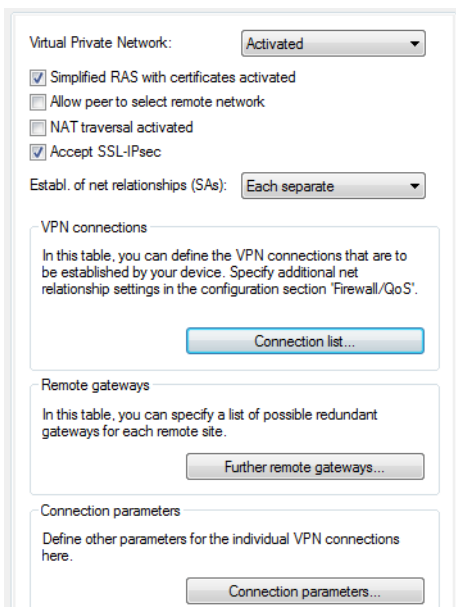


Note that when the IPsec over HTTPS option is activated, the VPN connection can only be established when the remote site also supports this technology, and when the remote site is set up to receive passive VPN connections that use IPsec over HTTPS.

Activate the option in the general VPN settings to enable passive connection establishment to a LANCOM VPN device from another VPN remote that works with IPsec over HTTPS technology (LANCOM VPN device or LANCOM Advanced VPN client).

■ LANconfig: VPN ► General

■ WEBconfig: LCOS menu tree ► Setup ► VPN



■ **Accept SSL-IPsec**

With this option your system accepts passive attempts to connect when the remote site supports IPsec over HTTPS technology.

Possible values:

- On, off

Default:

- Off



The LANCOM Advanced VPN Client supports automatic fallback to IPsec over HTTPS. With this setting, the VPN client initially attempts to establish a connection **without** using the additional SSL encapsulation. If the connection cannot be made, the device then tries to connect **with** the additional SSL encapsulation.

A.2.3 Status displays for IPsec over HTTPS technology

The status displays show whether IPsec over HTTPS technology is being used on each of the active VPN connections.

- WEBconfig: LCOS menu tree ▶ Setup ▶ VPN ▶ Connections

Connections																
Peer	State	Last-Error	Mode	SH-Time	phys.-Conn.	B1-DT	Remote-Gw	Nat-Detection	SSL-Encaps.	Crypt-Alg	Crypt-Length	Hash-Alg	Hash-Length	Hmac-Alg	Hmac-Length	Comp
CLIENT	Ready	(none)	Active 0		NETCOLOGN	9999	0.0.0.0	no-nat	No	(none)	0	(none)	0	(none)	0	(none)
LCS	Connection	(none)	Active 9999		NETCOLOGN	9999	213.217.69.77	no-nat	No	AES	128	HMAC_MD5	128	(none)	0	(none)

A.3 Basic HTTP file server for LCOS 8.0

A.3.1 Introduction

The HTTP server integrated into the LCOS uses the HTTP protocol to connect to an external storage medium, so providing a basic data server.

This function is supported by all LANCOM devices with a USB connector.

A.3.2 Preparing the USB storage medium

The following describes how to set up a USB medium for operating with a LANCOM device:

- File system: Format the USB medium with the FAT16 or FAT32 file system.
- Base directory: Create the directory `public_html` on the USB medium. The LCOS HTTP server only accesses the files and subdirectories in this directory. All other files on the USB medium are ignored.
- USB connection: Connect the mass storage device to the USB connector on the LANCOM.

A.3.3 Determine the mount point of the USB medium in the LCOS

When a USB medium is connected to a LANCOM device, a mount point is created automatically for the LCOS's internal management of the medium. This mount point always remains the same for a certain USB medium, even after rebooting or restarting. Different media are each allocated their own unique mount point.

The mount point must be known in order to access the files on the USB medium. The mount points for USB media are shown in the status table:

- WEBconfig: LCOS menu tree ▶ Setup ▶ File system ▶ Volumes

Volumes					
ID	Mountpoints	Filesystem	Unmountable?	Free	Size
BlkDev-1	/PKBACK#.001, /usb	FAT32	1	53382 KB	122 MB
MiniFs	/minifs	MiniFs	0	209 KB	256 KB

The status table displays all of the volumes discovered by the device.

- MiniFs is the flash file system integrated into most devices.
- BlkDev-n are descriptors for the known USB media. If there is just one USB mass storage device connected, it is named BlkDev-1 and is mounted under /usb.

A.3.4 Accessing the files on a USB medium

Use the following URL to access the files on the USB medium by using the HTTP server in the LCOS:

- `http://<IP address of device>/filesrv/<mount point>/<file name>`
 If, for example, the file is named `coupon.jpeg` and it is stored in the base directory `\public_html` of the only USB medium, then you can access it with the following link:
`http://<IP address of device>/filesrv/usb/coupon.jpeg`



Files can be accessed with HTTPS as well as HTTP.

A.3.5 Supported content type

The HTTP server in the LCOS uses the file extension to determine the MIME content type required to display the content correctly in a browser. The following extensions are currently recognized and will be translated into the correct MIME content type:

- `.htm` and `.html` for HTML files
- `.gif`, `.jpg`, `.jpeg`, `.png`, `.bmp`, `.pcx` for images in the corresponding format
- `.ico` for icon files
- `.pdf` for Adobe Acrobat PDF files
- `.css` for cascading style sheet files

A.3.6 Directory structure

The directory `public_html` can contain sub-directories. The LCOS HTTP server observes certain rules for accessing the directories:

- If a file named `'index.html'` exists in the sub-directory, then this is sent to the HTTP client, or else:
- If a file named `'index.htm'` exists in the sub-directory, then this is sent to the HTTP client, or else:
- The file server simply displays a list of the files and sub-directories in the main directory.

A.4 Automatic upload of firmware or configuration from external data media

A.4.1 Introduction

LANCOM devices with a USB connector can be commissioned very easily with the aid of an external data medium. Firmware files, loaders and even full configurations or scripts can be uploaded into the device from a USB medium.

A.4.2 Automatic upload of loader and/or firmware files

With this function activated and a USB medium mounted, the device searches for a loader and/or firmware files in the directory "Firmware". All files in the directory with the file extension `".upx"` will be considered for automatic loading if they are for the correct device type. This is done by reading the file headers and processing the files according to the following rules:

- If at least one `.upx` file with a loader is found, then the loader with the highest version number is loaded, unless the device already contains a loader with a higher version number.
- If at least one firmware file is found, then the firmware with the highest version number is loaded into the device, assuming that its version number is not equal to that of active or inactive firmware versions already in the device.

During the automatic load procedure, the device's power LED and online LED blink alternately. If a loader is uploaded first, the device will restart after this and it will commence a second automatic upload if new firmware is found. During this second load procedure, too, the device's power LED and online LED blink alternately.


The automatic uploading of loaders and/or firmware may, if applicable, be followed by further uploads of configuration files and/or script files.

Once the automatic upload procedure is complete, all LEDs on the device light up in green for 30 seconds. The USB medium can be removed.


A.4.3 Automatic upload of configuration and/or script files

With this function activated and a USB medium mounted, the device searches for a configuration and/or script files in the directory "Config". All files in the directory with the file extension `".lcs"` or `".lcf"` will be considered for automatic loading if they are for the correct device type. This is done by reading the file headers and processing the files according to the following rules:

- A full configuration ".lcf" is always loaded before a script ".lcs". Full configurations will only be loaded if the device type matches the device doing the loading, and if the firmware version entered into the header is the same as the active firmware in the device. If several suitable full configurations are found, then selection procedure follows these criteria:
 - The configuration header contains a device serial number that matches that of the device doing the upload.
 - The configuration header contains a MAC address that matches that of the device doing the upload.
 - If multiple configuration files are left over after applying these selection criteria, then the configuration with the most recent date is taken.

 When saving an off-line configuration, the header parameters for configuration files can be set manually in LANconfig's file dialog.

- If there is no full configuration available, then a script file (".lcs") is used instead, if available. If several suitable scripts are found, then selection procedure follows these criteria:
 - The script header contains a device serial number that matches that of the device doing the upload.
 - The script header contains a MAC address that matches that of the device doing the upload.
 - The script header contains a firmware version that matches that of the device doing the upload.
 - If multiple script files are left over after applying these selection criteria, then the script with the most recent version number or date is taken.

 The header parameters for scripts can be set manually by using a text editor. In the corresponding script file, enter "SERIAL:" and/or "MAC:" and, if applicable, a firmware version.

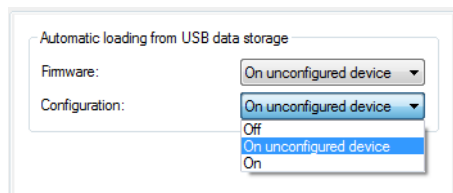
During the automatic load procedure, the device's power LED and online LED blink alternately.

Once the automatic upload procedure is complete, all LEDs on the device light up in green for 30 seconds. The USB medium can be removed.

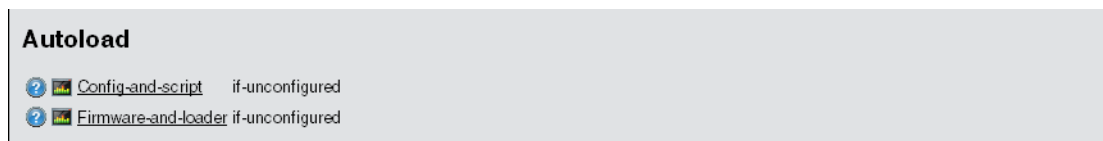
A.4.4 Configuration

The configuration for automatic loading is to be found under the following menu:

- LANconfig: Management ► USB data storage



- WEBconfig: LCOS menu tree ► Setup ► Autoload



■ Firmware

This option activates the automatic loading of loader and/or firmware files from a connected USB medium.

Possible values:

- Off
Automatic loading of loader and/or firmware files is deactivated.
- On
Automatic loading of loader and/or firmware files is activated.

When a USB medium is mounted, a suitable loader and/or firmware file is uploaded to the device. The USB medium is mounted when it is plugged into the USB connector on the device, or when it is restarted.

- On unconfigured device
Automatic loading of loader and/or firmware files is only activated when the device has its factory settings. A configuration reset can be used to return the device to its factory settings at any time.

Default:

- On unconfigured device



This option is set to "inactive" in the Security Settings Wizard or the Basic Settings Wizard.

Configuration

This option activates the automatic loading of configuration and/or script files from a connected USB medium.

Possible values:

- Off

Automatic loading of configuration and/or script files is deactivated.

- On

Automatic loading of configuration and/or script files is activated.

When a USB medium is mounted, a suitable configuration and/or script file is uploaded to the device. The USB medium is mounted when it is plugged into the USB connector on the device, or when it is restarted.

- On unconfigured device

Automatic loading of configuration and/or script files is only activated when the device has its factory settings. A configuration reset can be used to return the device to its factory settings at any time.

Default:

- On unconfigured device



This option is set to "inactive" in the Security Settings Wizard or the Basic Settings Wizard.

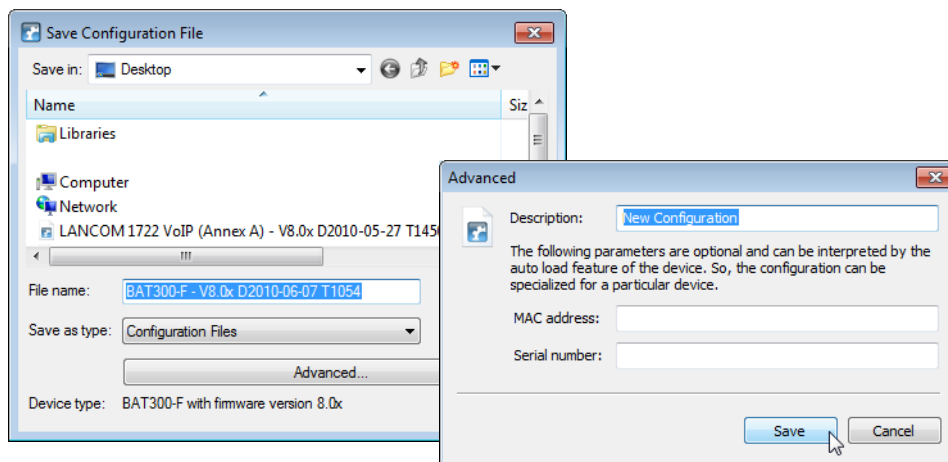


A device can be fed with an undesirable configuration by resetting it to its factory settings and inserting a prepared USB data media. To prevent this you have to deactivate the reset switch.

A.4.5 Meta data for configuration files

Configuration files can be marked with the serial number and/or MAC number of a device to facilitate the automatic loading from a USB data medium. The auto-load function in the devices then ensures that only the configuration or script with the matching serial number is uploaded to the device.

LANconfig provides the option of storing this information as meta parameters when a configuration is saved. When saving the configuration in LANconfig, click on the **Advanced** button:



A.5 SSH client

A.5.1 Introduction

In addition to an SSL server for the secure and authenticated dialing-in to LANCOM devices, LCOS also features an SSH client. This SSH client enables SSH connections to be established from a LANCOM device to a remote server, such as another LANCOM device or a Unix server. This function is highly useful if it is impossible to connect directly to a remote device, but if there is an indirect connection via the LANCOM device that can be accessed from both subnets instead.

The SSH client can be started with simple commands at the command line interface, similar to the OpenSSH client on a Linux or Unix system.

A.5.2 CLI arguments for the SSH client

The SSH connection to a remote system is initiated with the following command:

- `ssh [-?] [-h] [-b/-a loopback-address] [-p port] [-C] [-j interval] [user@]host [command]`
 - `-?`, `-h`: Display a brief help text about the available arguments
 - `-b`, `-a`: Enables the sender address (loopback address) to be specified. This option is especially important in connection with ARF.
 - `-p`: Specifies the port to be used. If the port is not specified here, the default is TCP port 22.
 - `command`: The SSH client either starts an interactive shell on the remote system or it can execute a single command. If no command is entered, the interactive shell starts.
 - `user`: User name for logging in to the remote system. If you do not explicitly enter a user name here, then the user name for your current local session is used for logging in at the LCOS CLI.
 - `-C`: If this option is specified, the SSH client uses the zlib algorithm to attempt to negotiate a method for data compression with the remote system. If the remote system does not support compression, then the data is transmitted uncompressed. The use of compression is generally worthwhile only for slow connections (e.g. ISDN). With fast connections, the performance loss from the additional overhead due to compression tends to be greater than the gain from reduced data amounts.
 - `-j interval`: If the connection to the remote system is routed via a NAT router or a firewall, it may be worthwhile to leave the connection running permanently. With an interactive SSH session, data is not transferred at all at certain phases, which can lead to disconnection because of timeouts. In such cases the SSH client can regularly transmit keep-alive packets. These are irrelevant to the remote station, but they inform the gateway that the connection is still being used. This argument specifies the interval in seconds for transmitting keep-alive packets. The keep-alive packets are only transmitted when the SSH client is not sending other data to the remote system.

A.5.3 CLI arguments for the Telnet client

Telnet can be used as an alternative to the SSH client to establish a connection to a remote station with the following command:

- `telnet [-?] [-h] [-b loopback-address] host [port]`
 - `-?`, `-h`: Display a brief help text about the available arguments
 - `-b`: Enables the sender address (loopback address) to be specified. This option is especially important in connection with ARF.
 - `port`: Specifies the port to be used. If the port is not specified here, the default is TCP port 23.

A.5.4 Public keys for authentication

Authentication with SSH works with public keys sent from the remote system. If an SSH client needs to connect to an SSH server, the server sends the public key to the client, which then looks for that key in its files. The following situations can occur here:

- The SSH client finds the key in its list of known server keys, and the key is allocated to the corresponding host name or IP address. The SSH connection can be established without further activity from the user.
- The SSH client does **not** find the key in its list of known server keys, and also no other key of the same type (RSA or DSS) for the corresponding host name or IP address. The SSH client assumes that this is the first connection to the server. It shows its public key and the associated fingerprint. The user can verify the key using a copy from another source, and can then decide whether the server should be stored in the list of known SSH servers. If the user declines this verification, the SSH connection is broken immediately.
- The SSH client finds a key for the corresponding host name or IP address, but this is different from the key currently in use. Both keys are displayed, but the SSH connection will be terminated because the SSH client suspects a man-in-the-middle attack. If the public key on the remote system was recently changed, then the administrator has to delete the outdated entry from the list of known servers.

After successfully verifying the server key, the administrator can enter the password for accessing the remote system. The password cannot be entered directly at the command line.

SSH connections are usually closed at the server, e.g. by entering "Exit" in the shell. Sometimes it may be necessary to close the SSH connection with the client, e.g. if the application on the server has problems. The SSH client in the LCOS uses the same character string as OpenSSH to close the connection, i.e. tilde - dot.



If the LCOS CLI session itself was opened with an OpenSSH client, you must use the string tilde – tilde – dot; otherwise the wrong connection will be closed.

A.5.5 Creating SSH keys

SSH authentication works with two different procedures:

- Interactive with password entry by keyboard
- By exchanging public keys

Keys have to be created for each individual as there are no predefined standard keys. For this reason, LANCOM devices with their factory settings only support authentication by password.

Keys are generated by entering the command `sshkeygen` at the command line on the device that the administrator want to run the SSH client on. The following syntax applies:

- `sshkeygen [-?] [-h] [-t dsa|rsa] [-b bits] [-f output-file]`
 - `-?`, `-h`: Display a brief help text about the available arguments
 - `-t`: This argument sets the key type.

SSH supports two types of key:

RSA keys are most widely used and have a length between 512 and 16384 bits. If possible you should work with keys of 1024 to 2048 bits in length.

DSS keys follow the standard set down by the National Institute of Standards and Technology (NIST) and are typically used in environments which are required to comply with the Federal Information Processing Standard (FIPS). DSS keys are always 1024 bits long, but they are slower to process than a corresponding RSA key.

An RSA type key will be generated if no key type is specified.

- `-b`: This argument sets the length of the RSA key in bits.
If no length is specified, the default value is 1024 bits.
- `-f`: Enables a file name for the key to be specified.

After generating the key, the public part must be transmitted to the remote system. The public part of the key can be displayed with the following command:

- `show ssh idkeys`

This command generates output similar to the following:

```
Configured Client-Side SSH Host Keys For User 'root':
ssh-rsa AAAAB3NzaC1yc2EAAAABEQAQAQEA2
8BtNFFInAi8I5B1a0wq5g2YfwIX20/vMX+9SLZ
AJVAhFnhdOG4wjTpLVuaQRNlITpBESPaWPLqoA
...
wd0T0nkuNQ== root@sshctest
```

Even though the output is divided into a number of lines, it is a single key consisting of three parts:

- The first part shows the key type (`ssh-rsa` or `ssh-dss`).
- The second part is the binary output of the key itself, coded as Base64.
- The third part contains the host name and is intended for entering comments.

This file can be edited with a convenient function in WEBconfig (WEBconfig ► Extras ► Edit list of allowed SSH public keys). Copy the first and second parts and replace the third part with a list of users to limit the use of this key to a selection of LCOS administrators.

A.5.6 Editing the files

During operations, the SSH client uses various files which may require manual editing.

The list of known SSH servers

The SSH client uses the list of known SSH servers to store the corresponding key. This file is changed each time a connection is established to an SSH server for the first time and the administrator accepts the key displayed for the remote system.

Each key is stored to a line in this file and contains three fields:

- The name or IP address of the remote system as entered into the SSH command when establishing the connection.
- The key type, i.e. `ssh-rsa` or `ssh-dss`.
- The binary output of the key itself, coded as Base64.



Once an administrator has accepted the public key of an SSH server, this key applies to all LCOS administrators; there is no differentiation at user level.

The files `ssh_id_rsa` and `ssh_id_dsa`

These files contain the keys generated with the `sshkeygen` command, i.e. the keys for authenticating the remote SSH server in PEM format. The keys for all LCOS administrators are stored in a central file which is accessible to root administrators only. It is not possible to upload or download this with WEBconfig.

The ID files have the following structure, which defines the use of a key for a certain LCOS administrator:

```
*** User xyz
Key
*** End
```

A.5.7 Priorities for SSH authentication

SSH authentication follows a strict order of priorities:

- The first method always attempts to authenticate by means of public key, unless the remote system does not support this method or the current LCOS administrator does not possess a public key.
- The second method is the interactive authentication by keyboard where public-key authentication is unavailable or when the remote system has rejected the public key of the current LCOS administrator. Depending on the application, interactive authentication may consist of exchanging a number of messages between the SSH client and SSH server. In the simplest case, the password just has to be entered one time.

A.5.8 Rights for operating the SSH client

Rights to work with the SSH client can be allocated on an individual basis to each administrator of LANCOM devices.

The rights for the administrators are to be found in the following menu:

- LANconfig: Management ► Admin ► Additional administrators
- WEBconfig: LCOS menu tree ► Setup ► Config ► Admins



A.6 Alternative boot config

A.6.1 Introduction

The way that a LANCOM device operates is determined by its configuration. The configuration is defined by the user and stored to a special portion of the flash memory that remains intact even when the device is restarted (configuration memory). When shipped, the configuration memory is empty because it does not yet have a user-defined configuration. Once in operation, the configuration memory can be deleted again by carrying out a configuration reset. If a device with an empty configuration memory is restarted or rebooted, the parameter values are taken from a boot configuration containing default values for the respective model.

A configuration is only written to the configuration memory if at least one parameter has been changed. The full configuration is written to the configuration memory. Even if only the device name is changed, current values for all of the parameters available to the device are stored to the user-defined configuration. Values for unchanged parameters are taken from a boot configuration.

LANCOM devices can make use of three different boot configurations:

□ Alternative boot config

- LANCOM factory settings: These are the default values for the model as shipped, i.e. the LANCOM standard. The standard boot configuration is contained in the device's firmware.
- Customer-specific standard settings: These are the customer's own standard settings for the model in question. These are used when the configuration memory is empty but the LANCOM default settings should not be used. This function provides LANCOM devices with persistent settings (i.e. remaining available however many times the device is rebooted or reset) that contain customer-specific standard settings for the boot procedure. Customer-specific standard settings are **not** deleted by a configuration reset. Customer-specific standard settings are stored to the first boot memory space.
- Rollout configuration: This configuration is useful for large-scale rollout scenarios where multiple devices need a boot configuration that differs from the LANCOM default configuration. The rollout configuration is activated by pressing the reset key for a particular length of time. The specialized rollout configuration is stored to the second boot memory space.

A.6.2 Using the boot configuration

When started normally, the LANCOM devices try to use the available configurations in a set order:


- User-defined configuration (in the configuration memory)
- Customer-specific standard settings (in the first boot memory space)
- LANCOM factory settings (in firmware)

The customer-specific standard settings are taken automatically and in preference to the LANCOM factory settings, assuming that the configuration memory is empty.

The rollout configuration is activated with the reset button. The reset button fulfills various functions depending upon how long the button is pressed:

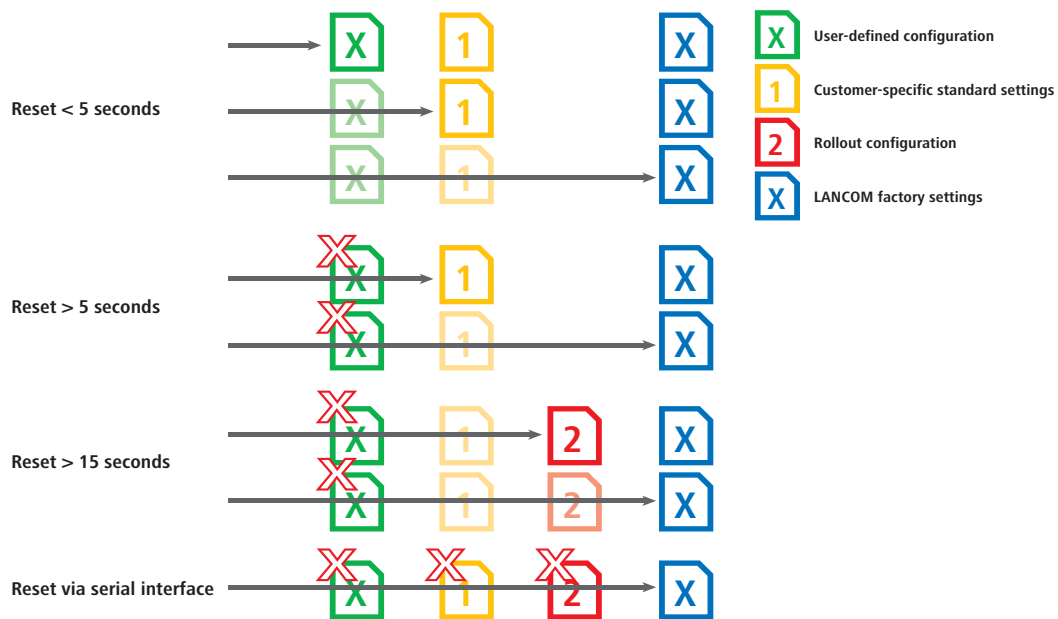
- Less than 5 seconds: Boot (restart), whereby the user-defined configuration is loaded from the configuration memory. If the user-defined configuration is empty, then the customer-specific standard settings (first memory space) are loaded instead. The loading of the customer-specific standard settings is visible when all LEDs on the device light up briefly in red. Similarly, the LANCOM factory settings are loaded if the first memory space is empty.
- Longer than 5 seconds until the **first** time that all device LEDs light up: Configuration reset (deletes the configuration memory) followed by a restart. In this case the customer-specific standard settings (first memory space) are loaded instead. The loading of the customer-specific standard settings is visible when all LEDs on the device light up briefly in red. The LANCOM factory settings are loaded if the first memory space is empty.
- Longer than 15 seconds until the **second** time that all device LEDs light up: Activating the rollout configuration and deleting the user-defined configuration. After restarting, the rollout configuration is started from the second memory space. The loading of the rollout configuration is visible when all LEDs on the device light up twice briefly in red. The LANCOM factory settings are loaded if the second memory space is empty.

The rollout configuration is activated directly after restarting if the reset button is pressed for more than 15 seconds. The next time the device is restarted, the normal boot sequence applies again automatically (user-defined configuration, customer-specific standard settings, LANCOM factory settings).

 If the reset button has been deactivated in the configuration (set to 'Ignore' or 'Boot only'), it is impossible to load the rollout configuration.

The following diagram illustrates which configuration is loaded by the different reset procedures, depending on the status of the device. Examples:

- If the button is pressed for less than 5 seconds, the user-defined configuration is loaded. If this is not available, then the customer-specific standard settings are loaded. If this is not available then the LANCOM factory settings are loaded.
- If the reset button is pressed for more than 15 seconds then the user-defined configuration is loaded. If this is not available then the rollout configuration is loaded. If this is not available then the LANCOM factory settings are loaded.



A.6.3 Restoring the LANCOM factory settings via the serial port

If both memory spaces are taken up with customer-specific standard settings **and** a rollout configuration, then the device cannot be reset to the LANCOM factory settings by using the reset button. If it becomes impossible to access the configuration (e.g. in case of a lost password), then the LANCOM factory settings can only be restored by means of the serial interface.


The serial interface can be used to load firmware into the device. Entering the serial number instead of the configuration password results in the device configuration being reset to its ex-factory settings. In this way you can regain access to the device if it becomes impossible to restore the LANCOM factory settings in any other way.

- ① Use the serial configuration cable to connect the device to a computer.
- ② On the computer, start a terminal program such as Hyperterminal.
- ③ Open a connection with the settings 115200bps, 8n1, hardware handshake (RTS/CTS).
- ④ In the terminal program's welcome screen, press the Return key until the request to enter the password appears.
- ⑤ Enter the serial number that is displayed under the firmware version and press Return again.

```

Outband-115200 Bit/s OK
#
| LANCOM L-54ag Wireless
| Ver. 7.26.0002 / 19.09.2007
| SN. 013020600159
| Copyright (c) LANCOM Systems
|
Connection No.: 001 (Outband-115200 Bps)
Password:
System is going down ...
@W@
| FLASHROM-Upload
| LANCOM L-54ag Wireless
| Copyright (C) LANCOM Systems
| Ver. 2.06.0001 / 22112006 / 16:30
Start Xmodem Upload
$ _
    
```

- ⑥ The device now expects a firmware upload. You initiate this in Hyperterminal by clicking on **Transfer ► Send file** and selecting X-Modem as the transfer protocol.

 Uploading the firmware in this way completely deletes the configuration, including the boot configuration, and returns the device to its ex-factory settings! This deletes all of the files stored on the device, including any rollout certificates. For this reason you should only use this option if you have no other way of accessing the device. The configuration and boot configuration are deleted even if the firmware upload is interrupted.

A.6.4 Storing and uploading the boot configurations

The customer-specific standard settings and the rollout configuration are saved in a compressed format. By means of the command line function, the current device configuration can be saved as customer-specific standard settings or as a rollout configuration. Use the following command for this:

■ `bootconfig -savecurrent [1,2, all]` or `bootconfig -s [1,2, all]`

Entering the appropriate number ensures that either the first boot memory space for the customer-specific standard settings is selected, or the second boot memory space for the rollout configuration. The parameter "all" writes the current configuration to both memory spaces at the same time.

WEBconfig can also be used to upload customer-specific settings or the rollout configuration into the device:

■ WEBconfig: LCOS menu tree ► File management ► Upload configuration

Upload Configuration


Enter the path and file name of the configuration file.

Save configuration as first alternative boot configuration

Save configuration as second alternative boot configuration

Filename:

Here you select the configuration file to be used and you activate the purpose as either customer-specific standard settings and/or rollout configuration.

 If both memory spaces are taken up with customer-specific standard settings **and** a rollout configuration, then the device cannot be reset to the LANCOM factory settings by using the reset button. In this case you should use the function 'Restoring the LANCOM factory settings via the serial port' →Page 11.

A.6.5 Deleting the boot configuration

The alternative and the special boot configurations cannot be deleted with the normal file functions. Use the following command for this:

■ `bootconfig - remove [1,2, all]` or `bootconfig -r [1,2, all]`

Selecting the appropriate number ensures that the corresponding boot memory space is selected. The parameter "all" causes both memory spaces to be deleted at once.

A.6.6 Working with certificates

In order for VPN and SSL/TLS to function after a configuration reset, a standard certificate can be stored to the device as a PKCS#12 container. This standard certificate is only used by the customer-specific standard settings and the rollout configuration.

- If the customer-specific standard settings are loaded, the standard certificate is copied to the normal certificate storage location for VPN and SSL/TLS. This ensures that it remains available even after rebooting.
- If the rollout configuration is loaded, the standard certificate for VPN is used, but it is not copied. This means that in case of a restart (even without a configuration reset) the device has no access to the certificate.

You can upload the standard certificate into the device with WEBconfig.

■ WEBconfig: LCOS menu tree ► File management ► Upload certificate or file

Upload Certificate or File

Select which file you want to upload, and its name/location, then click on 'Start Upload'.
In case of PKCS12 files, a passphrase may be necessary.

File Type:

File Name/Location:

Passphrase (if required):

Caution: Files are not being checked for correct contents or passphrase during upload. These checks are performed by the individual modules using these files. When uploading certificates, possible error messages can be seen in the VPN status trace immediately after download.

Select the certificate and commence the upload with **Start upload**.

A.7 Alternative DHCP server for forwarding

A.7.1 Introduction

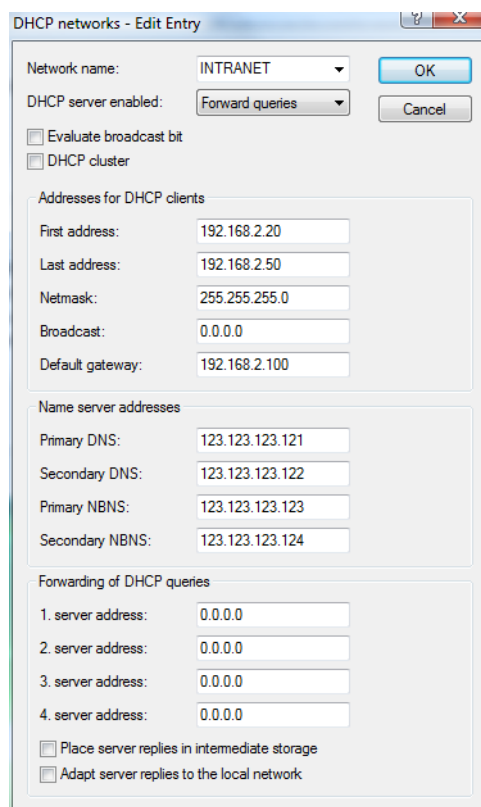
The DHCP server offers various operating modes. In the forwarding mode, the device acts in the local network like a DHCP relay and forwards requests to one of more pre-defined DHCP servers. This setting facilitates the operation of central DHCP servers in another network.

All DHCP messages sent by DHCP clients as a broadcast are forwarded to all predefined DHCP servers. The client selects the first server to answer and sends all subsequent messages as unicasts directly to that server. If the selected server becomes unavailable, the client once again transmits broadcast messages and selects another DHCP server.

A.7.2 Configuration

To configure the DHCP server for forwarding, refer to the following menus:

- LANconfig: TCP/IP ► DHCP ► DHCP networks
- WEBconfig: LCOS menu tree ► Setup ► DHCP ► Network list



■ 1st server address

This is where the IP address for the upstream DHCP server is entered when the mode 'Relay requests' is selected.

Possible values:

- IP address or the broadcast address of the network in which the server is located. The broadcast address is the highest address in an IP network. All packets sent to this address are received by all hosts.

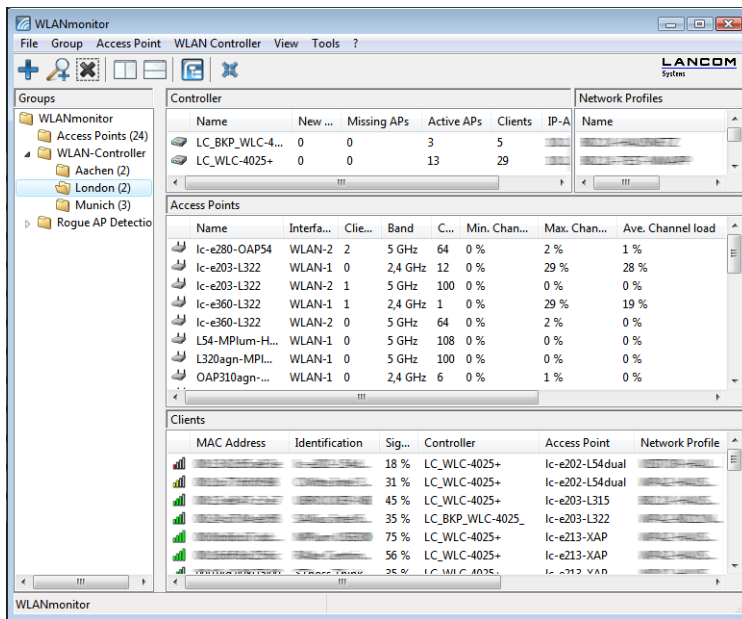
Default:

- 0.0.0.0

A.8 Channel-load display in WLC mode

The loads on the various channels used by each access point which is managed by a WLAN Controller are displayed as three values, the minimum, maximum and average channel load. The values displayed are measured every three minutes. Consequently, the first values are displayed after three minutes at the earliest.

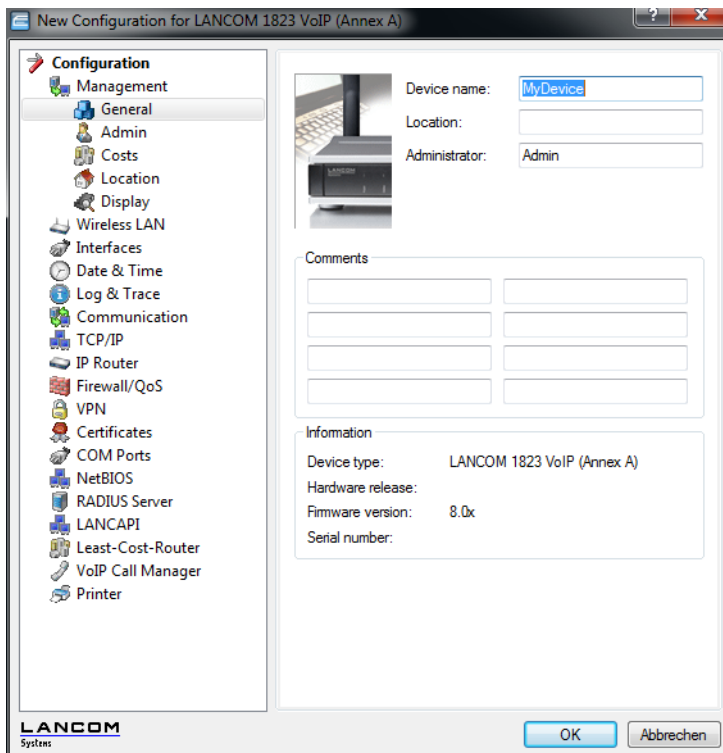
□ Changes in LANconfig



A.9 Changes in LANconfig

A.9.1 LANconfig configuration tree

As of version 8.00, the two top layers of the configuration menu in LANconfig are permanently visible in a dedicated area as a "configuration tree". This new structure makes it easier to navigate through the program for quick switching between the main configuration areas.

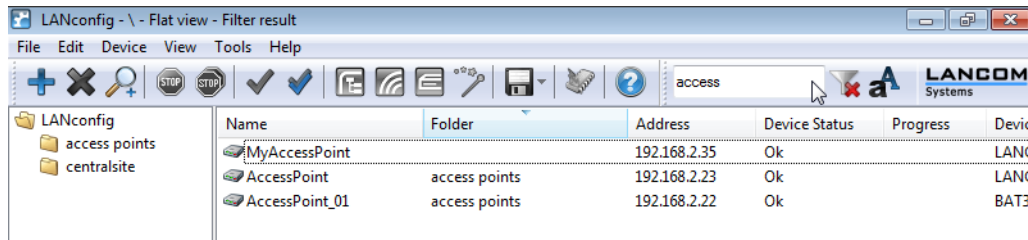


A.9.2 Dynamic filter

The dynamic filter in LANconfig provides an easy way of restricting the information displayed about the devices. Enter the desired filter criterion into the filter field. Filter criteria may be any of the displayed properties, such as: Device name, folder, IP address, device status, device type, serial number, etc.

LANconfig reduces the current folder view to the number of items where the filter criterion matches any of the properties (even within strings). You can reset the filter with the filter symbol next to the filter field. You can restrict the result to exactly matching expressions of the filter criterion with the symbol for capitalization (default: off). Otherwise

the search is not case-sensitive. The dynamic filter has direct impact on the folder view with each character you type. The filter results are always due to the selected folder. The dynamic filter can be used together with 'flat view mode'. Then all matches of the selected and all subsequent folders are shown at the same time.



A.9.3 Restricting access to web-server services

Access to a device with HTTP for the purposes of configuration can be enabled, disabled or restricted to read-only. Independent of this, access to web-server services can be controlled separately, for example to allow communication from CAPWAP with HTTP, even though HTTP access is otherwise disabled.

■ LANconfig: Management ► Admin ► Access to web-server services

■ HTTP port

For each method of access (i.e. LAN, WAN, WLAN, depending on the device) you can set the access rights for web-server services for the device's HTTP server port.

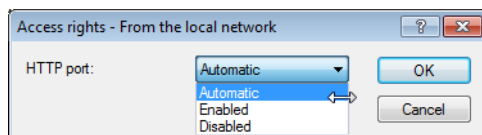
Possible values:

- Automatic: The HTTP server port is open as long as there is a service registered (e.g. CAPWAP). If no service is registered, the server port will be closed.
- Enabled: The HTTP port is always open, even if access to the configuration by HTTP is disabled. Direct access to the configuration can be prevented here, although the automatic configuration of APs by a wireless LAN controller remains possible.
- Disabled: The HTTP port is closed. No services can use the web server. If access to the configuration by HTTP is enabled, then a message is issued stating that the web server is unavailable.

□

Default:

- The default setting for all access methods is "Automatic".



A.10 Activating 802.1x accounting for logical WLANs in WLAN controllers

The configuration for logical WLAN networks is to be found in the following menu:

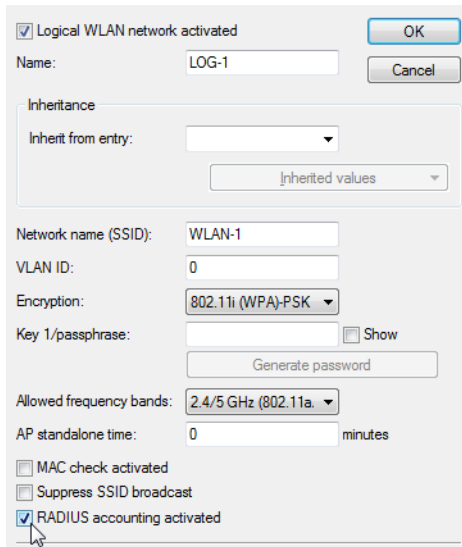
■ LANconfig: WLAN Controller ► Profiles ► Logical WLAN networks (SSIDs)

■ WEBconfig: LCOS menu tree ► Setup ► WLAN management ► AP configuration ► Network profiles



As of LCOS 8.0 it is possible to activate RADIUS accounting by 802.1x for each individual SSID. Former versions of the firmware provided RADIUS accounting by 802.1x globally for all of the SSIDs only.

□ LANCOMContent Filter



■ **RADIUS accounting activated**


This is where you can activate RADIUS accounting for this logical WLAN network.

Possible values:

- Yes, No

Default:

- No

 The access points supporting the logical WLAN network as configured by the WLAN controller must have an LCOS version 8.00 or higher.


A.11 LANCOMContent Filter

A.11.1 Introduction


The LANCOM Content Filter enables you to filter certain content from your network, so preventing access to Internet pages with content that is illegal or offensive. It also enables you to stop private surfing on specific sites during working hours. This not only increases staff productivity and network security but also ensures that the full bandwidth is available exclusively for your business activities.

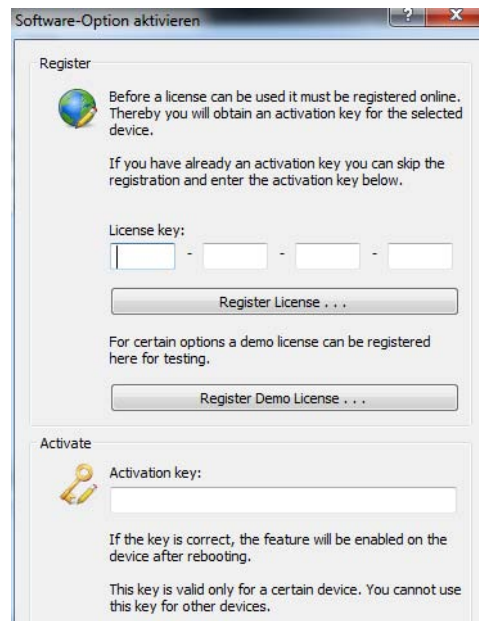
The LANCOM Content Filter is an intelligent content filter that works dynamically. It contacts a rating server that evaluates Internet sites reliably and accurately in accordance with the categories that you select.

The LANCOM Content Filter operates by checking the IP addresses behind the URLs that are entered. For any given domain it is possible to differentiate according to the path, meaning that specific areas of a URL may be rated differently.

 It is not possible for users to avoid the LANCOM Content Filter website rating simply by entering the website's IP address into their browsers.
The LANCOM Content Filter checks only unencrypted websites via HTTP.

The LANCOM Content Filter license you purchase is valid for a certain number of users and for a specific period (for one or three years). You will be informed of the expiry of your license in good time. The number of current users is monitored in the device, with the users being identified by their IP address. You can configure what should happen when the number of licensed users is exceeded: Access can either be denied or an unchecked connection can be made.

 You can test the LANCOM Content Filter on any router that supports this function. All you have to do is to activate a 30-day demo license for each device. Demo licenses are generated directly with LANconfig. Click on the device with the right-hand mouse key and select the context menu entry **Activate software option**. In the dialog that follows, click on the button **Register demo license**. You will automatically be connected to the website for the LANCOM registration server. Simply select the required demo license and you can register your device.



All settings relating to categories are stored in category profiles. You select from predefined main and sub-categories in the LANCOM Content Filter: 58 categories are divided into 14 subject groups such as "Pornography, Nudity", "Shopping" or "Illegal Activities". You can activate or deactivate each of the categories in these groups. Sub-categories for "Pornography/Nudity" are, for example, "Pornography/Erotic/Sex" and "Swimwear/Lingerie".

When configuring these categories, administrators have an additional option of activating an override. When the override option is active, users may still access the forbidden site for a particular period of time by clicking on a corresponding button, but the administrator will be notified of this by e-mail, syslog, or SNMP trap.

The category profile, whitelist and blacklist can be used to create a content filter profile that you can assign to particular users by means of the firewall. For example you can create a profile called "Employees_department_A" and assign this to all of the computers in that department.

When you install the LANCOM Content Filter, basic default settings are created automatically. These only need to be activated for the initial start. You can subsequently customize the behavior of the LANCOM Content Filter to match your own requirements.

A.11.2 Requirements for using the LANCOM Content Filter

The following requirements must be met before you can use the LANCOM Content Filter:

- 1 The LANCOM Content Filter option has been activated.
- 2 The firewall must be activated and an appropriate firewall rule must select the content filter profile.
- 3 The content filter profile must specify a category profile and if desired a whitelist and or blacklist for each part of the day. A content filter profile can consist of several different entries to provide different levels of protection during different parts of the day.

If a certain part of the day is not covered by an entry, access to websites will go unchecked for this period.



If the content filter profile is subsequently renamed, the firewall must also be modified.

A.11.3 Quick start

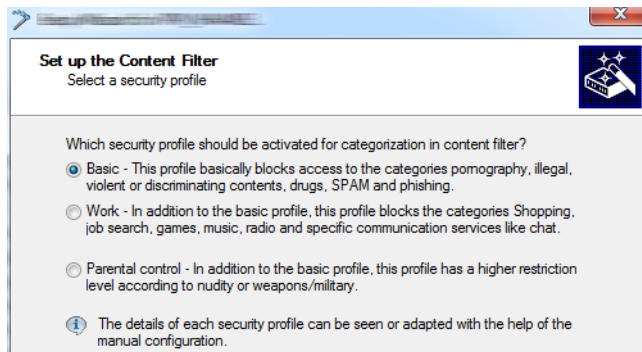
After installing the Content Filter, all the settings have been made to get it up and running quickly.



The operation of the Content Filter may be restricted by your country's data protection regulations or by company guidelines. Please check any regulations that may apply before putting the system into operation.

You activate the Content Filter by:


- 1 Start the Setup Wizard for the device.
- 2 Select the Setup Wizard for configuring the Content Filter.



3 Select one of the pre-defined security profiles (basic, work, parental control):

- Basic profile: This profile mainly blocks access to the categories pornography, illegal, violent or discriminatory content, drugs, SPAM and phishing
- Work profile: In addition to the settings for the basic profile, this profile also blocks the categories shopping, job search, gaming, music, radio and certain communications services such as chat.
- Parental-control profile: In addition to the settings for the basic profile, this profile also blocks nudity and weapons/military.

Should the firewall be deactivated, the Wizard will switch the firewall on. The Wizard then checks if the firewall rule is set correctly for the content filter and, if necessary, will take corrective measures. After activating the Content Filter with the steps outlined above, all stations in the network are being filtered according to the settings of the selected content-filter profile and the as-yet empty blacklist and whitelist. You can adapt these settings for your purposes, if necessary.

 Detailed information about manually configuring the content filter is available in the Content Filter manual available as a PDF download from www.lancom.eu.

A.11.4 Standard settings in the LANCOM Content Filter

The following elements have been created in the default configuration of the LANCOM Content Filter:

- A firewall rule
- Three firewall action objects
- Three content filter profiles
- Two timeframes
- A blacklist
- A whitelist
- Three category profiles

Firewall rule

The preset firewall rule is named CONTENT-FILTER and uses the action object CONTENT-FILTER-BASIC.

Firewall action objects

There are three firewall action objects: CONTENT-FILTER-BASIC, CONTENT-FILTER-WORK and CONTENT-FILTER-PARENTAL-CONTROL. These action objects work with the corresponding content-filter profiles.

Content filter profiles

There are three content filter profiles. All content-filter profiles use the timeframe ALWAYS, the blacklist MY-BLACKLIST and the whitelist MY-WHITELIST. Each content-filter profile uses one of the predefined category profiles:

- CF-BASIC-PROFILE: This content-filter profile features a low level of restrictions and works with the category profile BASIC-CATEGORIES.
- CF-PARENTAL-CONTROL-PROFILE: This content-filter profile protects minors (e.g. trainees) from unsuitable Internet content, and it works with the category profile PARENTAL-CONTROL.
- CF-WORK-PROFILE: This content-filter profile is intended for companies wishing to place restrictions on categories such as Job Search or Chat. It works with the category profile WORK-CATEGORIES.

Name	Time frame	Blacklisted	Whitelisted	Category profile
CF-BASIC-PROFILE	ALWAYS	MY-BLACKLIST	MY-WHITELIST	BASIC-CATEGORIES
CF-PARENTAL-CONTROL-PROFILE	ALWAYS	MY-BLACKLIST	MY-WHITELIST	PARENTAL-CONTROL
CF-WORK-PROFILE	ALWAYS	MY-BLACKLIST	MY-WHITELIST	WORK-CATEGORIES

Timeframe

There are two predefined timeframes:

- ALWAYS: 00.00-23.59 hrs
- NEVER: 00.00-0.00 hrs

Blacklist

The preset blacklist is named "MY-BLACKLIST" and it is empty. Here you can optionally enter URLs which are to be forbidden.

Whitelist

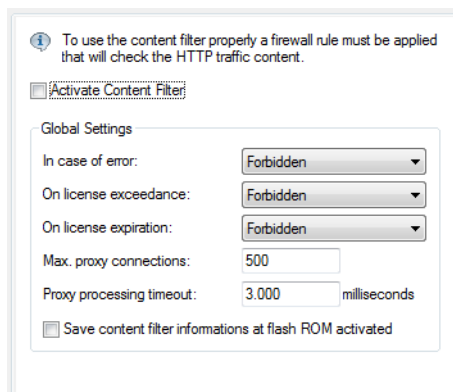
The preset whitelist is named "MY-WHITELIST" and it is empty. Here you can optionally enter URLs which are to be allowed.

Category profiles

There are three category profiles: BASIC-CATEGORIES, WORK-CATEGORIES and PARENTAL-CONTROL. The category profile specifies the categories which are to be allowed and forbidden, and for which one an override can be activated.

A.11.5 General settings

Global settings for the LANCOM Content Filter are made here:



LANconfig: Content-Filter ► General

WEBconfig: LCOS menu tree ► Setup ► UTM ► Content-Filter ► Global-Settings

■ **Operating**

This is where you can activate the LANCOM Content Filter.

■ **Action-on-Error:**

This is where you can determine what should happen when an error occurs. For example, if the rating server cannot be contacted, this settings either allows the user to surf without restrictions or access to the entire web is blocked.

Possible values:

- Block, Pass

Default:

- Block

■ **Action-on-License-Exceedance:**

This is where you can determine what should happen when the licensed number of users is exceeded. Users are identified by their IP address. The system keeps count of the IP addresses that connect via the LANCOM Content Filter. When the eleventh user establishes a connection with a 10-user license, no further checking is performed

by the LANCOM Content Filter. Depending on this setting, the unlicensed user can either surf the web without restrictions, or access to the entire web is blocked.

Possible values:

- Block, Pass

Default:

- Block



The users of the content filter are automatically removed from the user list when no connection has been made from the IP address concerned via the content filter for 24 hours.

■ **Action-on- License-Expiration:**

The license to use the LANCOM Content Filter is valid for a certain period. You will be reminded of the license expiry date 30 days, one week and one day before it actually expires (at the e-mail address configured in LANconfig: Log & Trace ► General).

This is where you can specify what should happen when the license expires (i.e. block everything or allow everything through). After the license used expires, this setting either allows the user to surf the web without restrictions, or access to the entire web is blocked.

Possible values:

- Block, Pass

Default:

- Block

■ **Max. proxy connections**

This setting is for the maximum allowable number of simultaneous proxy connections. This limits the load that can be placed on the system. A notification is sent if this number should be exceeded.

Possible values:

- 0 to 999999 connections

Default:

- Depends on device

■ **Proxy processing timeout**

Specifies the maximum time in milliseconds that the proxy can take for processing. A timeout error page is displayed if this time is exceeded.

Possible values:

- 0 to 999999 milliseconds

Default:

- 3000 milliseconds

Special values:

- The value 0 sets no time limit. Values less than 100 milliseconds make no sense.

A.11.6 Settings for blocking

You adjust the website-blocking settings here:

Alternative blocking URL:

A text to be shown at blocking can be defined here.

A text to be shown on error can be defined here.

The device determines the correct source address for the destination network automatically. If a certain source address should be used insert it here.

Alt. source IP for block URL:

LANconfig: Content-Filter ► Blocking

WEBconfig: LCOS menu tree ► Setup ► UTM ► Content-Filter ► Global-Settings

■ URL-To-Show-On-Blocking:

This is where you can enter the address of an alternative URL. If access is blocked, the URL entered here will be displayed instead of the requested website. You can use this external HTML page to display your company's corporate design, for example, or to perform functions such as JavaScript routines, etc. You can also use the same HTML tags here as in blocking text. If you do not make any entry here, the default page stored in the device will be displayed..

Possible values:

- Valid URL address

Default:

- Blank

■ Alt. source IP for block URL / Loopback to use on blocking:

This is where you can configure an optional sender address to be used instead of the one that would normally be automatically selected for this target address. If you have configured loopback addresses you can specify them here as sender address.

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ (caution: If there is an interface called "DMZ", its address will be taken in this case)
- LBO ... LBF for the 16 loopback addresses
- GUEST
- Any IP address in the form x.x.x.x

Default:

- Blank



The sender address specified here is used unmasked for every remote station.

Block-Text

This is where you can define text to be displayed when blocking occurs. Different blocking texts can be defined for different languages. The display of blocking text is controlled by the language setting transmitted by the browser (user agent).

Language	Text
default	The site <CF-URL/> is blocked because <CF-IF BL>it is blacklisted by the administr
de	Die Webseite <CF-URL/> wurde blockiert, da <CF-IF BL>sie vom Administrator ver
en	The site <CF-URL/> is blocked because <CF-IF BL>it is blacklisted by the administr

■ Language

Entering the appropriate country code here ensures that users receive all messages in their browser's preset language. If the country code set in the browser is found here, the matching text will be displayed.

You can add any other language.

Examples of the country code:

- de-DE: German-Germany
- de-CH: German-Switzerland
- de-AT: German-Austria
- en-GB: English-Great Britain
- en-US: English-USA



The country code must match the browser language setting exactly, e.g, "de-DE" must be entered for German ("de" on its own is not sufficient). If the country code set in the browser is not found in this table, or if the text stored under that country code is deleted, the predefined default text ("default") will be used. You can modify the default text.

Possible values:

- 10 alphanumerical characters

Default:

- Blank

■ **Text**

Enter the text that you wish to use as blocking text for this language.

Possible values:

- 254 alphanumerical characters

Default:

- Blank

Special values:

You can also use special tags for blocking text if you wish to display different pages depending on the reason why the website was blocked (e.g. forbidden category or entry in the blacklist).

The following tags can be used as tag values:

- <CF-URL/> for a forbidden URL
- <CF-CATEGORIES/> for the list of categories why the website was blocked
- <CF-PROFILE/> for the profile name
- <CF-OVERRIDEURL/> for the URL used to activate the URL (this can be integrated in a simple <a> tag or in a button)
- <CF-LINK/> adds a link for activating the override
- <CF-BUTTON/> for a button for activating the override

You can use a tag with attributes to display or hide parts of the HTML document: <CF-IF att1 att2> ... </CF-IF>.

Possible attributes are:

- BLACKLIST: If the site was blocked because it is in the profile blacklist
- CATEGORY: If the site was blocked due to one of its categories
- ERR: If an error has occurred.

Since there are separate text tables for the blocking page and the error page, this tag only makes sense if you have configured an alternative URL to show on blocking.

- OVERRIDEOK: If users have been allowed an override (in this case, the page should display an appropriate button)

If several attributes are defined in one tag, the section will be displayed if at least one of these conditions is met. All tags and attributes can be abbreviated to the first two letters (e.g. CF-CA or CF-IF BL). This is necessary as the blocking text may only contain a maximum of 254 characters.

- Example:

<CF-URL/> is blocked because it matches the categories <CF-CA/>.
Your content profile is <CF-PR/>.
<CF-IF OVERRIDEOK>
<CF-BU/></CF-IF>



The tags described here can also be used in external HTML pages (alternative URLs to show on blocking).

Error-Text

This is where you can define text to be displayed when an error occurs.

Language	Text
default	The site <CF-URL/> is blocked because <CF-IF BL>it is blacklisted by the administr
de	Die Webseite <CF-URL/> wurde blockiert, da <CF-IF BL>sie vom Administrator ver
en	The site <CF-URL/> is blocked because <CF-IF BL>it is blacklisted by the administr

■ **Language**

Entering the appropriate country code here ensures that users receive all messages in their browser's preset language. If the country code set in the browser is found here, the matching text will be displayed.

You can add any other language.

Examples of the country code:

- de-DE: German-Germany

- de-CH: German-Switzerland
- de-AT: German-Austria
- en-GB: English-Great Britain
- en-US: English-USA



The country code must match the browser language setting exactly, e.g, "de-DE" must be entered for German ("de" on its own is not sufficient). If the country code set in the browser is not found in this table, or if the text stored under that country code is deleted, the predefined default text ("default") will be used. You can modify the default text.

Possible values:

- 10 alphanumerical characters

Default:

- Blank

■ **Text**

Enter the text that you wish to use as error text for this language.

Possible values:

- 254 alphanumerical characters

Default:

- Blank

Special values:

You can also use HTML tags for the error text.

The following empty element tags can be used as tag values:

- <CF-URL/> for a forbidden URL
- <CF-PROFILE/> for the profile name
- <CF-ERROR/> for the error message
- Example:
<CF-URL/> is blocked because an error has occurred:
<CF-ERROR/>

A.11.7 Override settings

The override function allows a website to be accessed even though it is classified as forbidden. The user must click on the override button to confirm that the forbidden page should be opened. You can configure this feature so that the administrator is notified when the override button is clicked (LANconfig: Content-Filter ► Global-Settings).



If the override type "Category" has been activated, clicking on the override button makes **all** of the categories for that URL accessible to the user. The next blocking page to be displayed has just one category explaining why access to the URL was blocked. After clicking on the override button, all of the allowed categories are displayed. If the override type "Domain" has been activated, then the entire domain can be accessed.

The settings for the override function are to be found here:

The screenshot shows a configuration window for the override function. At the top, there is an information icon and a text box stating: "Override offers the opportunity to enter a blocked site anyway. The system can be configured in this respect to inform the administrator." Below this, there is a checked checkbox labeled "Override activated". Underneath, there are three fields: "Override duration:" with a value of "5" and "minutes" next to it; "Override type:" with a dropdown menu currently set to "Category & Domain"; and "Alternative override URL:" with an empty text input field. Below these fields, there is a text box that says "A text to be shown on override can be defined here." and a button labeled "Override text...". At the bottom of the window, there is another information icon and a text box: "The device determines the correct source address for the destination network automatically. If a certain source address should be used insert it here." Below this is a dropdown menu labeled "Alt. source IP for override URL:".

LANconfig: Content-Filter ► Override

WEBconfig: LCOS menu tree ► Setup ► UTM ► Content-Filter ► Global-Settings

■ **Override-Active**

This is where you can activate the override function and make further related settings.

■ **Override-Duration**

The override duration can be restricted here. When the period expires, any attempt to access the same domain and/or category will be blocked again. Clicking on the override button once more allows the website to be accessed again for the duration of the override and, depending on the settings, the administrator will be notified once more.

Possible values:

- 1-1440 (minutes)

Default:

- 5 (minutes)

■ **Override-Type:**

This is where you can set the type of override. It can be allowed for the domain, for the category of website to be blocked, or for both.

Possible values:

- Category: For the duration of the override, all URLs are allowed that fall under the affected categories (as well as those which would already have been allowed even without the override).
- Domain: For the duration of the override all URLs in this domain are allowed, irrespective of the categories they belong to.
- Category-and-Domain: For the duration of the override, all URLs are allowed that belong to this domain and also to the allowed categories. This is the highest restriction.

Default:

- Category-and-Domain

■ **URL-To-Show-On-Override:**

This is where you can enter the address of an alternative URL. In the event of an override, the URL entered here will be displayed instead of the usual website. You can use this external HTML page to display your company's corporate design, for example, or to perform functions such as JavaScript routines, etc. You can also use the same tags here as in the override text. If you do not make any entry here, the default page stored in the device will be displayed..

Possible values:

- Valid URL address

Default:

- Blank

■ **Override sender IP address:**


This is where you can configure an optional sender address to be used instead of the one that would normally be automatically selected for this target address. If you have configured loopback addresses you can specify them here as sender address.

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ (caution: If there is an interface called "DMZ", its address will be taken in this case)
- LBO ... LBF for the 16 loopback addresses
- GUEST
- Any IP address in the form x.x.x.x

Default:

- Blank

 The sender address specified here is used unmasked for every remote station.

Override text

This is where you can define text that is displayed to users confirming an override.

Language	Text
default	<CF-IF OK>Successfully overrode </CF-IF><CF-IF CA BO>the categories <CF-CAT/></CF-IF>
de	<CF-IF CA BO>Die Kategorien <CF-CAT/> sind</CF-IF><CF-IF BO> auf der Seite <CF-DO/></CF-IF>
en	<CF-IF OK>Successfully overrode </CF-IF><CF-IF CA BO>the categories <CF-CAT/></CF-IF>

■ Language

Entering the appropriate country code here ensures that users receive all messages in their browser's preset language. If the country code set in the browser is found here, the matching text will be displayed.

You can add any other language.

Examples of the country code:

- de-DE: German-Germany
- de-CH: German-Switzerland
- de-AT: German-Austria
- en-GB: English-Great Britain
- en-US: English-USA



The country code must match the browser language setting exactly, e.g. "de-DE" must be entered for German ("de" on its own is not sufficient). If the country code set in the browser is not found in this table, or if the text stored under that country code is deleted, the predefined default text ("default") will be used. You can modify the default text.

Possible values:

- 10 alphanumerical characters

Default:

- Blank

■ Text

Enter the text that you wish to use as override text for this language.

Possible values:

- 254 alphanumerical characters

Default:

- Blank

Special values:

You can also use HTML tags for blocking text if you wish to display different pages depending on the reason why the website was blocked (e.g. forbidden category or entry in the blacklist).

The following tags can be used as tag values:

- <CF-URL/> for the originally forbidden URL that is now allowed
- <CF-CATEGORIES/> for the list of categories that have now been allowed as a result of the override (except if domain override is specified).
- <CF-BUTTON/> displays an override button that forwards the browser to the original URL.
- <CF-BUTTON/> displays an override link that forwards the browser to the original URL.
- <CF-HOST/> or <CF-DOMAIN/> displays the host or the domain for the allowed URL. The tags are of equal value and their use is optional.
- <CF-ERROR/> generates an error message in the event that the override fails.
- <CF-DURATION/> displays the override duration in minutes.

You can use a tag with attributes to display or hide parts of the HTML document: <CF-IF att1 att2> ... </CF-IF>.

Attributes can be:

- CATEGORY when the override type is "Category" and the override was successful
- DOMAIN when the override type is "Domain" and the override was successful
- BOTH when the override type is "Category-and-Domain" and the override was successful

□ LANCOMContent Filter

- ERROR when the override fails
- OK if either CATEGORY or DOMAIN or BOTH are applicable

If several attributes are defined in one tag, the section should be displayed if at least one of these conditions is met. All tags and attributes can be abbreviated to the first two letters (e.g. CF-CA or CF-IF BL). This is necessary as the blocking text may only contain a maximum of 254 characters.

- Example:

```
<CF-IF CA BO>Categories <CF-CAT/> are </CF-IF><CF-IF BO> in domain <CF-DO/></CF-IF><CF-IF DO>.
Access to domain <CF-DO/> is allowed for </CF-IF><CF-IF OK> f&uuml;r <CF-DU/> minutes. <br><CF-LI/
></CF-IF><CF-IF ERR>Override error :<br><CF-ERR/></CF-IF>
```

A.11.8 Profiles in the LANCOM Content Filter

This is where you can create content filter profiles that are used to check websites for prohibited content. A content filter profile always has a name and, for various time periods, it activates the desired category profile and, optionally, a blacklist and a whitelist.

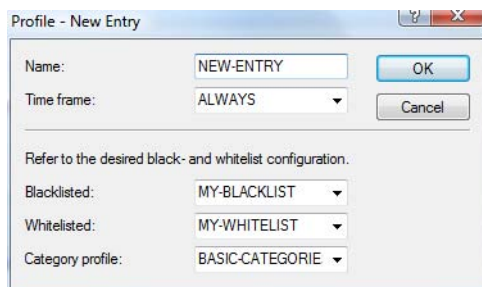
In order to provide different configurations for the various timeframes, several content-filter profile entries are created with the same name. The content filter profile is thus made up of the sum of all entries with the same name. The firewall refers to this content-filter profile.



Please note that you must make corresponding settings in the firewall in order to use the profiles in the LANCOM Content Filter.

Profiles

The settings for the profiles are to be found here:



LANconfig: Content-Filter ▶ Profiles ▶ Profiles

WEBconfig: LCOS menu tree ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profiles ▶ Profiles

■ **Name**

The profile name that the firewall references must be specified here.

Possible values:

- Name of a profile

Default:

- Blank

■ **Timeframe**

Select the timeframe for this category profile and, optionally, the blacklist and the whitelist. The timeframes "ALWAYS" and "NEVER" are predefined. You can configure other timeframes under:

LANconfig: Date/Time ▶ General ▶ Timeframe

WEBconfig: LCOS menu tree ▶ Setup ▶ Time ▶ Timeframe

One profile may have several lines with different timeframes.

Possible values:

- Always
- Never
- Name of a timeframe profile

Default:

- Blank



If timeframes overlap when multiple entries are used for a content filter profile, all pages contained in one of the active entries will be blocked for that period of time. If a period remains undefined when several entries are used for a content filter profile, access to all websites is unchecked for this period.

■ **Blacklist**

Name of the blacklist profile that is to apply for this content filter profile during the period in question. A new name can be entered, or an existing name can be selected from the blacklist table.

Possible values:

- Name of a blacklist profile
- New name

Default:

- Blank

■ **Whitelist**

Name of the whitelist profile that is to apply for this content filter profile during the period in question. A new name can be entered, or an existing name can be selected from the whitelist table.

Possible values:

- Name of a whitelist profile
- New name

Default:

- Blank

■ **Category-Profile**

Name of the category profile that is to apply for this content filter profile during the period in question. A new name can be entered, or an existing name can be selected from the category table.

Possible values:

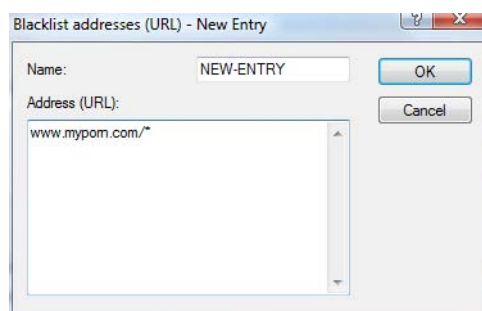
- Name of a category profile
- New name

Default:

- Blank

Blacklist addresses (URL)

This is where you can configure websites which are to be blocked.



LANconfig: Content-Filter ► Profiles ► Blacklist addresses (URL)

WEBconfig: LCOS menu tree ► Setup ► UTM ► Content-Filter ► Profiles ► Blacklists

■ **Name**

Enter the name of the blacklist for referencing from the content-filter profile.

Possible values:

- Blacklist name

Default:

- Blank

■ **Address (URL)**

Access to the URLs entered here will be forbidden by the blacklist.

Possible values:

- Valid URL address

□ LANCOMContent Filter

The following wildcard characters may be used:

- * for any combination of more than one character (e.g. www.lancom.* encompasses the websites www.lancom.de, www.lancom.eu, www.lancom.es, etc.)
- ? * for any one character (e.g. www.lancom.e* encompasses the websites www.lancom.eu, www.lancom.es)



Please enter the URL **without** the leading http://. Please note that in the case of many URLs a forward slash is automatically added as a suffix to the URL, e.g. www.mycompany.de/. For this reason it is advisable to enter the URL as: www.mycompany.de* .

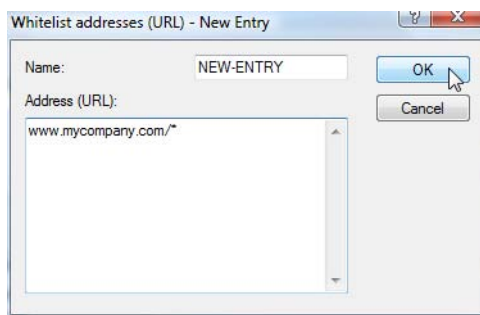
Individual URLs are separated by a blank.

Default:

- Blank

Whitelist addresses (URL)

This is where you can configure websites to which access is to be allowed.



LANconfig: Content-Filter ▶ Profiles ▶ Whitelist addresses (URL)

WEBconfig: LCOS menu tree ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profiles ▶ Whitelists

■ **Name**

Enter the name of the whitelist for referencing from the content-filter profile.

Possible values:

- Name of a whitelist

Default:

- Blank

■ **Addresses (URL)**

This is where you can configure websites which are to be checked locally and then accepted.

Possible values:

- Valid URL address

The following wildcard characters may be used:

- * for any combination of more than one character (e.g. www.lancom.* encompasses the websites www.lancom.de, www.lancom.eu, www.lancom.es, etc.)
- ? * for any one character (e.g. www.lancom.e* encompasses the websites www.lancom.eu, www.lancom.es)



Please enter the URL **without** the leading http://. Please note that in the case of many URLs a forward slash is automatically added as a suffix to the URL, e.g. www.mycompany.de/. For this reason it is advisable to enter the URL as: www.mycompany.de* .

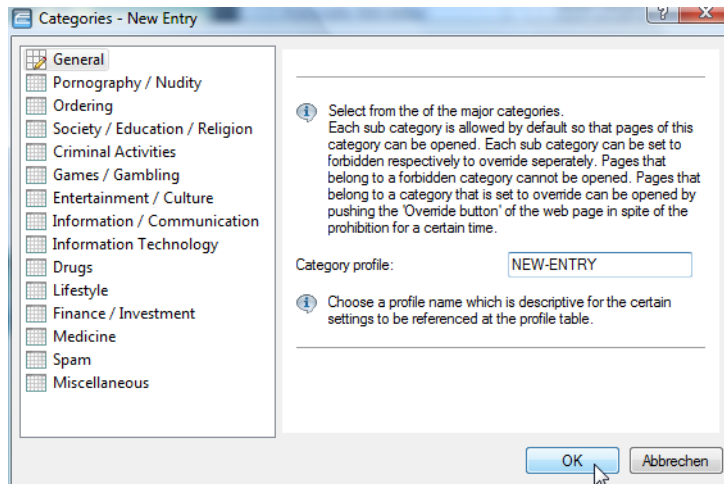
Individual URLs are separated by a blank.

Default:

- Blank

Category- Profiles

Here you create a category profile and determine which categories or groups should be used to rate websites for each category profile. You can allow or forbid the individual categories or activate the override function for each group.



LANconfig: Content-Filter ► Profiles ► Categories

WEBconfig: LCOS menu tree ► Setup ► UTM ► Content-Filter ► Profiles ► Category-Profiles

■ Category profile

The name of the category profile for referencing from the content-filter profile is entered here.

Possible values:

- Name of a category profile

Default:

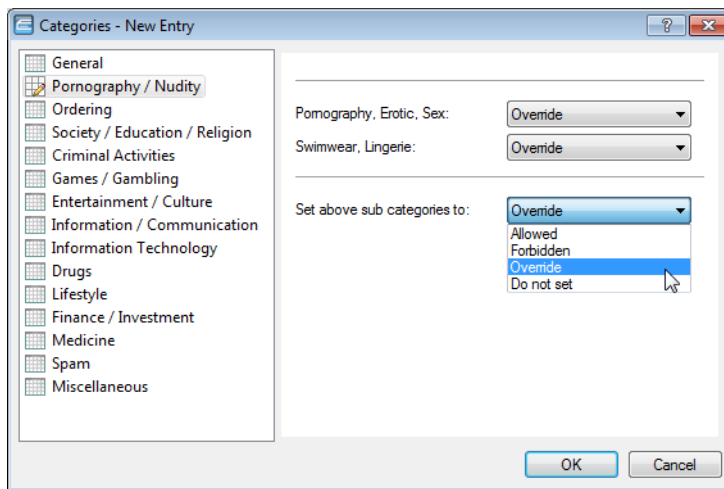
- Blank

■ Category settings

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

The following main categories can be configured:

- Pornography/Nudity
- Shopping
- Society/Education/Religion
- Illegal Activities
- Games/Gaming
- Entertainment/Culture
- Information/Communication
- Information Technology
- Drugs
- Lifestyle
- Finance/Investment
- Medicine
- Spam
- Miscellaneous



The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

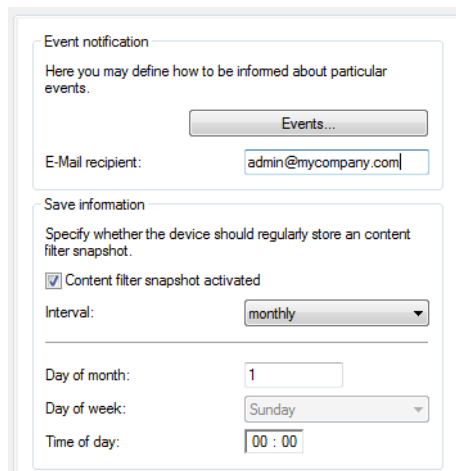
- Allowed, forbidden, override

Default:

- Override

A.11.9 Options with the LANCOM Content Filter

This is where you can determine whether you wish to be notified of events and where LANCOM Content Filter information is to be stored.



LANconfig: Content-Filter ► Options

WEBconfig: LCOS menu tree ► Setup ► UTM ► Content-Filter ► Global-Settings

■ Events:

This is where you define how you wish to receive notification of specific events. Notification can be made by e-mail, SNMP or SYSLOG. You can specify that messages for different events should be output in different ways.

Error:

- For SYSLOG: Source "System", priority "Alarm".
- Default: SNMP notification

License expiry:

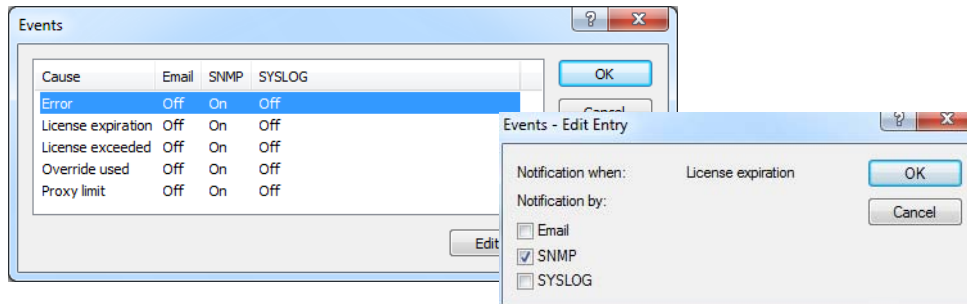
- For SYSLOG: Source "Admin", priority "Alarm".
- Default: SNMP notification

License exceeded:

- For SYSLOG: Source "Admin", priority "Alarm".
- Default: SNMP notification

Override applied:

- For SYSLOG: Source "Router", priority "Alarm".
 - Default: SNMP notification
- Proxy limit:
- For SYSLOG: Source "Router", priority "Info".
 - Default: SNMP notification



■ **E-mail recipient:**

An SMTP client must be defined if you wish to use the e-mail notification function. You can use the client in the device, or another client of your choice.



No e-mail will be sent if no e-mail recipient is defined.

WEBconfig: LCOS menu tree ► Setup ► UTM ► Content-Filter ► Global-Settings ► Snapshot

■ **Content-Filter-Snapshot**

This is where you can activate the content filter snapshot and determine when and how often it should be taken. The snapshot copies the category statistics table to the last snapshot table, overwriting the old contents of the snapshot table. The category statistics values are then reset to 0.

■ **Interval**

Here you decide whether the snapshot should be taken monthly, weekly or daily.

Possible values:

- Monthly
- Weekly
- Daily

Default:

- Monthly

■ **Day of month:**

For monthly snapshots, set the day of the month when the snapshot should be taken.

Possible values:

- Max. 2 characters

Default:

- 1



It is advisable to select a number between 1 and 28 in order to ensure that it occurs every month.

■ **Weekday:**

For weekly snapshots, set the day of the week when the snapshot should be taken.

Possible values:

- Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

Default:

- Monday

■ **Time:**

If you require a daily snapshot, then enter here the time of day for the snapshot in hours and minutes.

Possible values:

- Maximum 5 characters, format HH:MM

□ LANCOMContent Filter

Default:

- 00:00

A.11.10 Additional settings for the LANCOM Content Filter

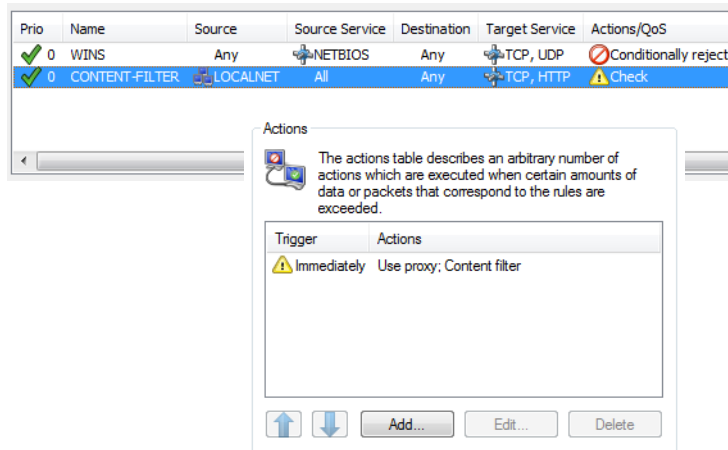
Firewall settings for the content filter

The firewall must be activated in order for the LANCOM Content Filter to function. You can activate the firewall under:

LANconfig: Firewall/QoS ► General

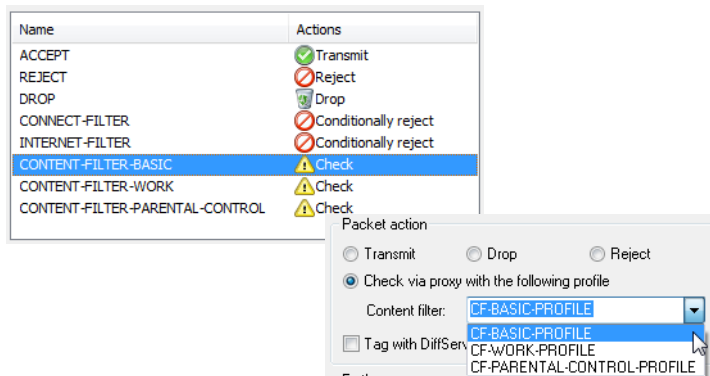
WEBconfig: LCOS menu tree ► Setup ► IP-Router ► Firewall

In the default configuration, you will find the firewall rule CONTENT-FILTER that refers to the action object CONTENT-FILTER-BASIC:



i The firewall rule should be limited to the target service “http” so that only outgoing HTTP connections are examined. Without this restriction all packets will be checked by the content filter, which could lead to a loss of system performance.

A content-filter related firewall rule must contain a special action object that uses packet actions to check the data according to a content-filter profile. In the default configuration you will find the action objects CONTENT-FILTER-BASIC, CONTENT-FILTER-WORK and CONTENT-FILTER-PARENTAL-CONTROL, each of which refer to their corresponding content-filter profile:

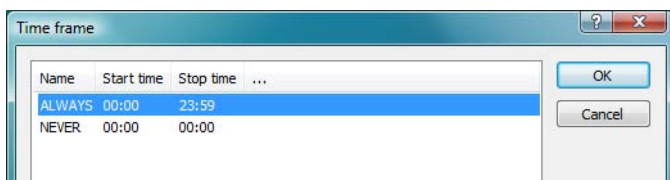


Example: When a web page is accessed, the data packets pass through the firewall and are processed by the rule CONTENT-FILTER. The action object CONTENT-FILTER-BASIC checks the data packets using the content-filter profile CONTENT-FILTER-BASIC.

Timeframe

Timeframes are used to define the periods when the content-filter profiles are valid. One profile may have several lines with different timeframes. Different lines in a timeframe should complement each other, i.e. if you specify WORKTIME you will probably wish to specify a timeframe called FREETIME to cover the time outside of working hours.

The timeframes “ALWAYS” and “NEVER” are predefined. You can configure other timeframes under:



LANconfig: Date/Time ► General ► Timeframe

WEBconfig: LCOS menu tree ► Setup ► Time ► Timeframe

■ **Name**

Enter the name of the timeframe for referencing from the content-filter profile.

Possible values:

- Name of a timeframe

Default:

- Blank

■ **Start**

Here you set the start time (time of day) when the selected profile becomes valid.

Possible values:

- Maximum 5 characters, format HH:MM

Default:

- 00:00

■ **Stop time**

Here you set the stop time (time of day) when the selected profile ceases to be valid.

Possible values:

- Maximum 5 characters, format HH:MM

Default:

- 23:59

■ **Weekdays**

Here you select the weekday on which the timeframe is to be valid.

Possible values:

- Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

Default:

- Activated for Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

You can form a time schedule with the same name but with different times extending over several lines:

Name	Start time	Stop time	...
ALWAYS	00:00	23:59	
LEISURE	00:00	07:00	
LEISURE	12:01	13:00	
LEISURE	17:01	23:59	
NEVER	00:00	00:00	

A.12 DFS3

A.12.1 Introduction

In mid 2010 a new version (1.5.1) of the standard EN 301 893 came into force, bringing with it a change in the usage of wireless LAN frequencies in the ranges 5.25 – 5.35 GHz and 5.47 – 5.725 GHz. The new EN 301 893-V1.5 regulates the DFS (Dynamic Frequency Selection) method for the protection of radar stations from WLAN systems working in this frequency range. By using DFS to detect active radar stations from radio-signal patterns, WLAN systems can automatically switch their operating channel. Unlike the EN 301 893-V1.3 (DFS2) regulation used to date, the new standard EN 301 893-V1.5 is referred to as "DFS3".

A radar pattern can be described in terms of its pulse rate, pulse width and the number of pulses. Former DFS technology was only able to detect fixed radar patterns as defined by the various combinations of pulse rate and pulse width which were stored in the WLAN device. According to DFS3 systems must now be able to recognize

changing pulse rates and pulse widths as radar patterns. Furthermore, two or three different pulse rates may be used within a radar signal.



Channels 120, 124 and 128 in the 5.6 – 5.65 MHz frequency range as used by weather radar are subject to special conditions of use. The DFS implementation in LCOS does not support these requirements, and so these three channels have been disabled in the newer versions.

A.12.2 Configuration

All WLAN systems put into operation after EN 301 893-V1.5 came into effect are required to use DFS3 in the 5 GHz band. To activate DFS3 in your WLAN device, select the following menu items:

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ Radio settings

■ Preferred DFS scheme

Here you can select between DFS2 (EN 301 893-V1.3) and DFS3 (EN 301 893-V1.5).

- Possible values:
 - EN 301 893-V1.5
 - EN 301 893-V1.3
- Default:
 - EN 301 893-V1.5

When upgrading from a firmware version older than LCOS version 8.00 to an LCOS version 8.00 or higher, the existing setting of DFS2 (EN 301 893-V1.3) remains in effect.



No selection can be made for devices permanently set to DFS3, for those with processors that do not support DFS3 or for those which transmit on the 2.4 GHz frequency only.

A.13 Alternative URLs for CRLs

A.13.1 Introduction

The address where a certificate revocation list (CRL) can be collected is normally defined in the certificate (as `crDistributionPoint`). LCOS has a table where alternative CRLs can be specified. After a system start the CRLs are automatically collected from these URLs. These are used in addition to the lists offered by the certificates.

A.13.2 Configuration

The table for the alternative CRL URLs can be found under the following paths:

LANconfig: Certificates ▶ CRL ▶ Alternative URLs

WEBconfig: LCOS menu tree ▶ Setup ▶ Certificates ▶ CRLs ▶ Alternative URL table

■ Alternative URL

Here you enter the URL where a CRL can be collected.

- Possible values:
 - Any valid URL with max. 251 characters.
- Default:
 - Blank

A.14 Broken link detection

When an access point is not connected to the cabled LAN, it is normally unable to fulfill its primary task, namely the authorization of WLAN clients for access to the LAN. The broken-link detection function allows a device's WLAN to be disabled if the connection to the LAN should fail. Clients associated with that access point are then able to login to a different one (even if it has a weaker signal).

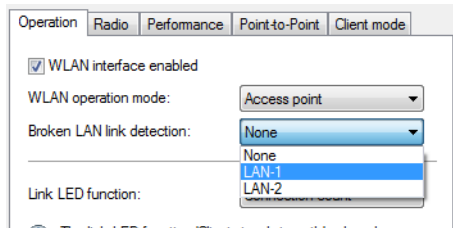
Until LCOS version 7.80, broken-link detection always applied to LAN-1, even if the device was equipped with multiple LAN interfaces. Furthermore, deactivation affected all of the WLAN modules in the device.

With LCOS version 8.00, broken-link detection could be bound to a specific LAN interface.

The settings for broken link detection are to be found under the following paths:

LANconfig: Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Operation

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ Operational



■ **Broken LAN link detection**

This function allows the WLAN modules in a device to be disabled if the allocated LAN interface has no connection to the LAN.

Possible values:

- No: Broken-link detection is disabled.
- LAN-1 to LAN-n (depending on the LAN interfaces available in the device). All of the WLAN modules in the device will be deactivated if the LAN interface set here should lose its connection to the cabled LAN.

Default:

- No

i The interface descriptors LAN-1 to LAN-n stand for the logical LAN interfaces. To make use of this function, the physical Ethernet ports on the device must be set with the corresponding values LAN-1 to LAN-n.

i Broken-link detection can also be used for WLAN devices operating in WLAN client mode. With broken-link detection activated, the WLAN modules of a WLAN client are only activated when a connection exists between the relevant LAN interfaces and the cabled LAN.