

■ connecting your business



Addendum

LCOS 9.10

Contents

1 Addendum to LCOS version 9.10.....	8
2 Overview of new features of the LCOS version 9.10.....	9
3 Smart certificates.....	12
3.1 Using smart certificates.....	12
3.1.1 Creating templates for certificate profiles.....	13
3.1.2 Creating a profile in LANconfig.....	14
3.1.3 Certificate creation with WEBconfig.....	17
3.1.4 Certificate management with WEBconfig.....	18
3.1.5 Managing certificates in LANmonitor.....	20
3.1.6 Creating certificates via URL-API.....	20
3.1.7 Tutorials.....	21
3.2 Additions to the Status menu.....	28
3.2.1 SCEP-CA.....	28
3.3 Additions to the Setup menu.....	38
3.3.1 Web interface.....	38
4 High availability clustering.....	57
4.1 Automatic configuration synchronization (Config Sync) with the LANCOM WLC High Availability Clustering XL option.....	57
4.2 Automatic configuration synchronization (Config Sync) with the LANCOM VPN High Availability Clustering XL option.....	58
4.3 Setting up configuration synchronization.....	59
4.4 1-Click WLC High Availability Clustering Wizard.....	64
4.5 Additions to the Status menu.....	67
4.5.1 Sync.....	67
4.6 Additions to the Setup menu.....	85
4.6.1 Config Sync.....	85
4.6.2 Sync.....	86
5 Configuration.....	96
5.1 TR-069 support.....	96
5.1.1 CPE WAN Management Protocol (CWMP).....	96
5.1.2 Additions to the Setup menu.....	101
5.1.3 Additions to the Status menu.....	109
5.2 Encrypted storage of configurations with LANconfig.....	112
5.2.1 Saving and loading device-configuration and script files.....	113
5.2.2 Additions to the Status menu.....	116
5.3 Each device has its own SSL key & changes to the default SSL settings.....	118
5.3.1 Automatic generation of device-specific SSH/SSL keys.....	118
5.3.2 Manually create custom SSH keys.....	118
5.3.3 Additions to the Setup menu.....	120

6	Diagnosis.....	121
6.1	Advanced config version information under Status.....	121
6.1.1	Additions to the Status menu.....	121
6.2	SSH identifier in the event log.....	122
6.2.1	Additions to the Status menu.....	122
7	LCMS.....	123
7.1	Proxy authentication via NTLM.....	123
7.1.1	Proxy.....	123
7.2	Special LANconfig icon for devices in a cluster or using Config Sync.....	124
7.3	Special LANmonitor icon for devices in a cluster or using Config Sync.....	125
7.4	LANCOM "Wireless Quality Indicators" (WQI).....	125
7.5	Extended number of characters for device names.....	126
7.6	Different notations for MAC addresses.....	126
7.6.1	Different notations for MAC addresses.....	127
7.7	LANconfig: Text corrections relating to access rights.....	127
8	IPv6.....	128
8.1	Prefix-exclude option for DHCPv6 prefix delegation.....	128
8.1.1	Prefix-exclude option for DHCPv6 prefix delegation.....	128
9	ISDN.....	129
9.1	Additions to the Status menu.....	129
9.1.1	PCM-SYNC-SOURCE.....	129
9.1.2	PCM-Switch.....	129
10	RADIUS.....	130
10.1	Comment field for RADIUS clients.....	130
10.1.1	Additions to the Setup menu.....	130
10.2	More attributes for RADIUS requests.....	132
10.3	Accounting status types "Accounting On" and "Accounting Off".....	133
10.3.1	Accounting status types "Accounting On" and "Accounting Off".....	134
10.4	Larger volume budgets in the RADIUS server and Public Spot.....	134
10.4.1	Additions to the Setup menu.....	135
10.5	RADIUS server: Realm discovery for computer authentication.....	136
10.5.1	Additions to the Setup menu.....	136
10.6	RADIUS client: Additional source ports for requests when necessary.....	137
10.6.1	Additional source ports for access requests.....	137
10.7	User-defined RADIUS attributes.....	137
10.7.1	RADIUS attributes configurable.....	137
10.7.2	Additions to the Setup menu.....	138
11	Public Spot.....	144
11.1	Restricting administrators to voucher output only.....	144
11.1.1	Wizard for creating and managing users.....	144
11.1.2	Setting up limited administrator rights for Public Spot managers.....	144
11.2	Specify volume budget on vouchers.....	145
11.3	XML interface: Enhanced VLAN handling.....	146

11.3.1 Additions to the Setup menu.....	147
11.3.2 Messages to and from the authentication server.....	148
11.4 "Small header image": Optimized display for 19" devices.....	150
11.5 New button "Manage user wizard".....	150
11.5.1 Additions to the Setup menu.....	151
11.6 Only show user accounts generated by the currently logged-on administrator.....	151
11.6.1 Additions to the Setup menu.....	151
11.7 Evaluation of DHCP option 82 in RADIUS and Public Spot.....	152
11.7.1 AP-specific login to a central Public Spot.....	152
11.7.2 Additions to the Setup menu.....	153
11.8 Additions to the Status menu.....	154
11.8.1 Max. no. users.....	154
11.8.2 PbSpot authenticated users.....	155
11.8.3 PMS authenticated users.....	155
11.8.4 Local configured users.....	155
11.9 Additions to the Setup menu.....	155
11.9.1 Password input set.....	155
11.9.2 Hide CSV export.....	156
12 WLAN.....	157
12.1 Upgrade to 16 SSIDs per WLAN module.....	157
12.2 WLAN disabled by default.....	157
12.3 Wildcards for MAC address and SSID filters.....	157
12.3.1 Access-control list.....	158
12.3.2 Additions to the Setup menu.....	159
12.4 Conformity with current ETSI radio standards in the 2.4GHz/5GHz bands.....	167
12.4.1 DFS configuration.....	167
12.4.2 Additions to the Setup menu.....	169
12.5 Time of the DFS rescan configurable via LANconfig.....	170
12.6 P2P support for 802.11ac.....	170
12.7 Client mode for 802.11ac.....	170
12.8 Bandwidth limit for each WLAN client per SSID.....	170
12.8.1 Additions to the Setup menu.....	170
12.9 Opportunistic key caching (OKC) adjustable on the client side.....	171
12.9.1 Additions to the Setup menu.....	171
12.10 Counter for WPA login attempts.....	172
12.10.1 Additions to the Status menu.....	172
12.11 Point-to-point links via 802.11ac.....	174
12.12 Additions to the Setup menu.....	174
12.12.1 Channel change delay.....	174
12.13 Additions to the Status menu.....	174
12.13.1 Delete values.....	174
13 WLAN management.....	175
13.1 AutoWDS operation.....	175
13.1.1 Additions to the Status menu.....	175

13.2 Disable responses to CAPWAP requests from a WAN connection.....	176
13.2.1 Protection against unauthorized CAPWAP access from the WAN.....	176
13.2.2 Additions to the Setup menu.....	177
13.3 Additional date information for central firmware management.....	178
13.3.1 Firmware management table.....	178
13.3.2 Additions to the Setup menu.....	178
13.4 Display of channel and frequency of clients logged on to the AP.....	179
13.4.1 Additions to the Status menu.....	179
13.5 Using LANconfig to backup certificates.....	180
13.5.1 Using LANconfig to backup and restore certificates.....	180
13.6 Displaying the certificate status of an AP.....	181
13.6.1 Additions to the Status menu.....	182
13.7 On/off switch for AP LEDs per WLC.....	182
13.7.1 Device LED profiles.....	183
13.7.2 Additions to the Setup menu.....	183
13.7.3 Additions to the Status menu.....	185
13.8 Managing Wireless-ePaper and iBeacon profiles with WLCs.....	188
13.8.1 ESL- and iBeacon profiles.....	189
13.8.2 Additions to the Setup menu.....	190
13.9 The modules iBeacon and Wireless ePaper have an additional "Managed" mode.....	194
13.9.1 Additions to the Setup menu.....	194
13.10 WLAN profiles divided into basic and advanced profiles.....	196
13.11 General LBS profile and device location profile.....	196
13.11.1 General LBS profile and device location profile.....	197
13.11.2 Additions to the Status menu.....	199
13.11.3 Additions to the Setup menu.....	199
13.12 Additions to the Status menu.....	200
13.12.1 Acquire statistical data.....	200
13.13 WLC Clustering Wizard.....	200
14 VPN.....	201
14.1 SCEP-CA function in VPN environments.....	201
14.2 SCEP algorithms updated.....	201
14.2.1 Configuring the CAs.....	201
14.2.2 Additions to the Setup menu.....	203
14.3 Loopback address for L2TP connections.....	208
14.3.1 Additions to the Setup menu.....	208
14.4 Download link for the public portion of the CA certificate.....	209
14.4.1 Download link for the public portion of the CA certificate.....	209
14.5 Configurable one-time password (OTP) for SCEP-CA.....	209
14.5.1 Configuring challenge passwords.....	210
14.5.2 Additions to the Setup menu.....	211
14.6 Deleting VPN error messages in the status table.....	212
14.6.1 Additions to the Setup menu.....	212
14.7 IPv4 addresses for VPN tunnels in the IP parameter list.....	213

14.7.1 Additions to the Setup menu.....	213
15 Routing and WAN connections.....	216
15.1 Client binding.....	216
15.1.1 Client binding.....	216
15.1.2 Load balancing with client binding.....	216
15.1.3 Enhancements in the menu system.....	218
15.2 Interface binding "Any" removed in IPv4.....	223
15.2.1 Defining networks and assigning interfaces.....	223
15.2.2 Additions to the Setup menu.....	223
15.3 Generic routing encapsulation (GRE).....	224
15.3.1 Understanding the generic routing encapsulation (GRE) protocol.....	224
15.3.2 Additions to the Setup menu.....	226
15.3.3 Additions to the Status menu.....	229
15.4 Ethernet-over-GRE tunnel (EoGRE).....	231
15.4.1 Ethernet-over-GRE (EoGRE).....	232
15.4.2 Additions to the Status menu.....	234
15.4.3 Additions to the Setup menu.....	234
15.5 Loopback addresses for RIP.....	238
15.5.1 Additions to the Setup menu.....	238
15.6 PPPoE snooping new.....	239
15.6.1 PPPoE snooping.....	239
15.6.2 Additions to the Setup menu.....	239
15.7 Default settings in the access table for WAN connections.....	242
15.7.1 Additions to the Setup menu.....	242
16 Backup solutions.....	249
16.1 Backup connections for dual-SIM devices.....	249
16.1.1 Configuration of the backup connection.....	249
16.1.2 Additions to the Setup menu.....	250
17 Other services.....	251
17.1 Prefer perfect forward secrecy (PFS) for connections.....	251
17.1.1 Additions to the Setup menu.....	251
17.2 E-mail notification from the Content Filter.....	253
17.2.1 Options for the LANCOM Content Filter.....	253
17.2.2 Additions to the Setup menu.....	255
17.3 TACACS+ extension for the passwd command.....	256
17.4 Input field for DHCP options extended to 251 characters.....	256
17.4.1 Additions to the Setup menu.....	256
18 Other parameters.....	258
18.1 Profile.....	258
18.2 Renegotiations.....	258
18.3 TLS connections.....	259
18.3.1 Port.....	259
18.4 Renegotiations.....	259

18.5 LBS-Tracking.....	260
18.6 LBS-Tracking-List.....	260
18.7 OKC.....	261
18.8 Network name.....	261
18.9 Manage user wizard.....	262
18.9.1 Show status information.....	262
18.10 Renegotiations.....	262
18.11 LBS-Tracking-List.....	263
18.12 Max. number of concurrent updates.....	263
18.13 CAPWAP-Port.....	264
18.14 RS count.....	264
18.15 RS count.....	265
18.16 Flash restore.....	265
18.17 Additions to the Status menu.....	265
18.17.1 DSLAM chipset manufacturer dump.....	265
18.17.2 DSLAM manufacturer dump.....	266
18.17.3 DSLAM chipset manufacturer dump.....	266
18.17.4 DSLAM manufacturer dump.....	266




1 Addendum to LCOS version 9.10

This document describes the changes and enhancements in LCOS version 9.10 since the previous version.

2 Overview of new features of the LCOS version 9.10

We have implemented a variety of new features in the LCOS version 9.10.

Table 1: New features of the LCOS version 9.10

 <p>SMART CERTIFICATE</p>	<p>Smart Certificate</p> <p>LANCOM sets a milestone in the area of security.</p> <p>Maximum security with VPN access: You will quickly benefit from the feature now integrated into LANCOM devices for the convenient creation of digital certificates—free of the need for an external certificate authority! Set up your VPN connections with self-created certificates for secure encryption. This maximum-security feature is included with all current LANCOM central-site VPN gateways, WLAN controllers, and with all current LANCOM routers upgraded with the LANCOM VPN 25 option.</p>
 <p>HIGH AVAILABILITY CLUSTERING</p>	<p>High availability clustering</p> <p>Grouping and centralized management of multiple WLAN controllers and central-site VPN gateways</p> <p>You can collect multiple WLAN controllers or central-site VPN gateways into a high-availability cluster. The LANCOM High Availability Clustering options combine multiple devices into a cluster. There are many benefits resulting from this, including the central management and the convenient configuration synchronization (Config Sync) of all devices in the cluster. You profit hugely when setting up intelligent backup scenarios, because only one WLAN controller or central-site VPN gateway in the cluster needs to be configured—a massive time-saving for the administrator. What's more, high-availability clustering enables automatic load balancing and the issue of cluster certificates.</p>
 <p>100+ FEATURES</p>	<p>More than 100 further features</p> <p>More security, more management, more virtualization.</p> <p>There are many new ways for you to benefit from further professionalizing your network management. As of LCOS 9.10, you can encrypt your configuration, flexibly interconnect remote networks via a GRE tunnel, also called the "virtual Ethernet cable", you can grant the WLAN users the same bandwidth on a per-SSID basis, and you can install high-performance point-to-point links via Gigabit Wireless with up to 1.3 Gbps.</p>

Further features

Client bandwidth management per SSID

More control over the amount of bandwidth used per WLAN client: The bandwidth limit can be configured for every client on each SSID (download and upload) .

GRE-Tunnel

Maximum flexibility of connectivity between remote networks: With generic routing encapsulation (GRE), packets are encapsulated and transported in a tunnel between the two endpoints.

Ethernet over GRE tunnel

The "virtual Ethernet cable" is ideal for connecting two networks through a layer-2 tunnel, for example via IPSec VPN.

16 SSIDs

Each WLAN radio module can now be configured to support 16 individual SSIDs. This allows twice as many WLAN services to be available in parallel—in the case of dual-radio access points with two WLAN radio modules, this can be up to 32!

Display active Public Spot licenses

LANmonitor displays the current and the maximum possible number of Public Spot users, and it sends a message when license usage reaches 90%.

Load balancer client binding

New applications in load-balancing scenarios – related sessions on a WAN line are recognized and kept open for demanding applications such as online banking.

TR-069 support

"Zero-touch management" – the TR-069 protocol allows the automatic provisioning and a secure, encrypted remote management of a router in provider environments.

Encrypted storage of configurations with LANconfig

Prevent unauthorized access to your configurations – in LANconfig, configuration files are encrypted and securely stored with password protection.

E-mail notification from the LANCOM Content Filter

Notifications by e-mail in case of content-filter events can be triggered immediately or daily, on request.

Greater number of characters

The number of characters available for assigning device names has been extended to 64.

Newer SCEP algorithms

More security with certificates: For encryption the SCEP algorithms AES192 and AES256 are supported, as are SHA256, SHA384, and SHA512 for signature verification.

New DynDNS providers in the Setup Wizard

The providers "Strato" and "feste-ip.net" have been added to the DynDNS Wizard.

Configuration assignment by WLC can be deactivated

Greater security against rogue APs: You can now configure whether a WLAN controller automatically assigns a configuration to a new access points over a WAN link.

LEDs can be switched off by WLCs

The LEDs of managed WLAN devices can switched off centrally from the WLAN controller.

Monitoring configuration changes

Easy validation of configuration changes by means of the displayed hash values, timestamps, and change counters.

Improved control over Public Spot volume budgets

Public Spot volume budgets can now be set to exceed a data volume of 4 GB, and the budget set for each user can also be printed on the voucher.

Direct entry into voucher creation for the Public Spot

Greatly simplified access to Public Spot voucher generation: Automatic forwarding to the appropriate page—ideal for untrained personnel!

3 Smart certificates



As of LCOS version 9.10 you have the option to use a LANCOM router to create and issue digital certificates.

Furthermore, LANmonitor as of LCOS version 9.10 displays an overview of active and revoked certificates.

Table 2: Overview of function rights

Description: [1]LANconfig, [2]Setup menu	Hex notation in the console	Rights description
1. CA-Web-Interface Wizard	0x1000000	Creates profiles for the CA web interface
2. CA-Web-Interface		

3.1 Using smart certificates

The configuration of the SCEP client for the generation and distribution of certificates can quickly become a complex and laborious task in extensive network infrastructures. This work required for this task can be reduced with the help of predefined, selectable profiles and access via a web interface.

A LANCOM router enables you to create and issue highly secure certificates. It is easy to manage the certificates via the WEBconfig interface of the corresponding device. An external CA is no longer required, which is particularly advantageous for small-scale infrastructures.

Using the Certificate Wizard from LANCOM, even users without certificate know-how can create certificates in just a few steps.

The devices administrator creates the profile as a collection of certificate properties. It contains the configuration of the certificate and also a unique certificate ID. From this point on, all you need to do to create and distribute a certificate is to select one of the profiles.

Profiles can also be managed in LANconfig under **Certificates > Certificate handling** in the section **CA web interface**.

CA web interface

Here you configure the web interface of the CA on your device.

3.1.1 Creating templates for certificate profiles

In LANconfig, profiles are created under **Certificates > Certificate handling > Templates**.

 A "DEFAULT" a template is already available.

The administrators specifies which of the profile properties are mandatory and which are to be edited by the user. The following options are available:

- No: The field is invisible, the value entered is considered to be a default value.
- Fixed: The field is visible, but cannot be changed by the user.
- Yes: The field is visible and can be changed by the user.
- Mandatory: The field is visible, the user must enter a value.

These permissions apply to the following profile and ID fields:

Profile fields


- Key usage
- Key usage (extended)
- RSA key length
- Validity period
- Create CA certificate
- Password

Identifier


- Country code (C)
- Locality name (L)
- Organization (O)
- Organization unit (OU)
- State or province (ST)
- E-mail (E)
- Surname (SN)

3 Smart certificates

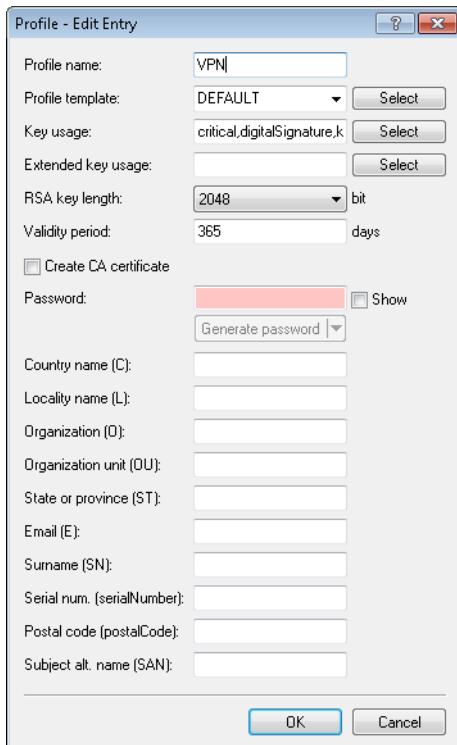
- Serial no. (serialNumber)
- Postal code (postalCode)
- Subject alt. name


 If the Templates table is empty, the user can only see the input fields for the profile name, the common name (CN), and the password. The other profile fields retain the default values as set by the device administrator.

3.1.2 Creating a profile in LANconfig

 The user needs the appropriate access rights to create, select, modify and assign profiles.

In LANconfig, profiles are created under **Certificates > Certificate handling > Profile**.



 By default three profiles are already available for common application scenarios.

Profile name

The unique name of the profile.

Profile template

Select a suitable profile template here, if applicable.

The profile template specifies which certificate information is mandatory and which can be changed. Templates are created under **Certificates > Certificate handling > Templates**.

Key usage

Specifies for which application the profile is to be used. The following usages are available using the **Select** button:

Table 3: The available key usages

Value	Meaning
critical	This restriction requires the extended key usage to be considered. If the extension is not supported, the certificate is rejected as invalid.
digitalSignature	If this option is used, the public key is used for digital signatures.
nonRepudiation	With this option set, the key is used for digital signatures of a non-repudiation service, i.e. one with a rather long-term character such as notary public service.
keyEncipherment	If this option is set, the key is used for encrypting other keys or security information. It is possible to restrict the use of encipher only and decipher only .
dataEncipherment	If this option is set, the key is used for encrypting user data (but not other keys).
keyAgreement	If this option is used, the "Diffie-Hellman" algorithm is used for key agreement.
keyCertSign	If this option is set, the key is applied to certificates for signature verification. This is useful for CA certificates, for example.
cRLSign	If this option is set, the key is applied to CRLs for signature verification. This is useful for CA certificates, for example.
encipherOnly	This is only useful with the Diffie-Hellman keyAgreement.
decipherOnly	This is only useful with the Diffie-Hellman keyAgreement.



Multiple comma-separated entries can be selected.

Ext. key usage

Specifies the extended application for which the profile is to be used. The following usages are available using the **Select** button:

Table 4: Extended usages

Value	Meaning
critical	
serverAuth	SSL/TLS Web server authentication
clientAuth	SSL/TLS Web client authentication
codeSigning	Signing of program code
emailProtection	E-mail protection (S/MIME)
timeStamping	Furnishing data with reliable time stamps
msCodeInd	Microsoft Individual Code Signing (authenticode)
msCodeCom	Microsoft Commercial Code Signing (authenticode)
msCTLSign	Microsoft Trust List Signing
msSGC	Microsoft Server Gated Crypto
msEFS	Microsoft Encrypted File System
nsSGC	Netscape Server Gated Crypto



Multiple comma-separated entries can be selected.

RSA key length

Sets the length of the key.

Validity period

Specifies the duration, in days, for which the key is valid. After this period, the key becomes invalid unless the user renews it.

Create CA certificate

Indicates whether this is a CA certificate.

Password

Password to protect the PKCS12 certificate file.

The following input creates a certificate ID. The following options are available:

Country code (C)

Enter the country identifier (e.g. "DE" for Germany).

This entry appears in the subject or issuer of the certificate under `C=` (**C**ountry).

Locality name (L)

Enter the name of the locality.

This entry appears in the subject or issuer of the certificate under `L=` (**L**ocality).

Organization (O)

Specify the organization that issues the certificate.

This entry appears in the subject or issuer of the certificate under `O=` (**O**rganization).

Organization unit (OU)

Specify the unit within the organization that issues the certificate.

This entry appears in the subject or issuer of the certificate under `OU=` (**O**rganization **U**nit).

State or province (ST)

Enter the State or province.

This entry appears in the subject or issuer of the certificate under `ST=` (**ST**ate).

E-mail (E)

Enter an e-mail address:

This entry appears in the subject or issuer of the certificate under `emailAddress=`.

Surname (SN)

Enter a surname.

This entry appears in the subject or issuer of the certificate under `SN=` (**Sur**Name).

Serial no. (serialNumber)

Enter a serial number.

This entry appears in the certificate under `serialNumber=`.

Postal code (postalCode)

Enter the location post code.


This entry appears in the subject or issuer of the certificate under `postalCode=`.

Subject alt. name (SAN)

The "Subject Alternative Name" (SAN) links additional data with this certificate. The following data are allowed:

- E-mail addresses
- IPv4 or IPv6 addresses
- URIs
- DNS names
- Directory names
- Any names

This entry appears in the subject or issuer of the certificate under `subjectAltName=` (e.g. `subjectAltName=IP:192.168.7.1`).

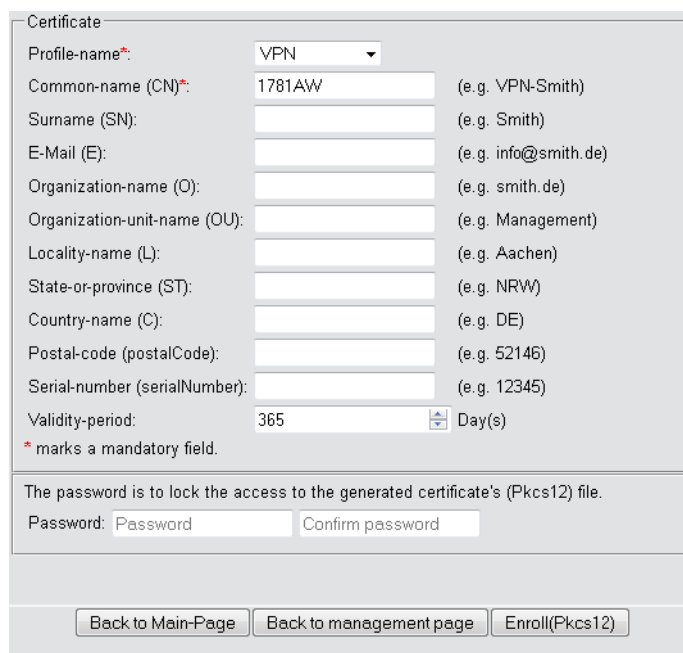
 The certificate issuer assigns the general name "CN". The "CN" is required as a minimum.

3.1.3 Certificate creation with WEBconfig


 You need the appropriate access rights to select, modify and assign profiles.

To create your certificates, navigate to the WEBconfig of the LANCOM device.


1. To create a certificate using the web interface, navigate to the view **Setup Wizards > Manage certificates** and select **Create new certificate**.



2. From the **Profile name** drop-down menu, select the profile to be used as the basis for the certificate.

 Empty templates only contain fields with the selection "No". If the user selects a profile based on an empty template, the input mask displays only the common name. The other profile fields retain the default values as set by the device administrator.

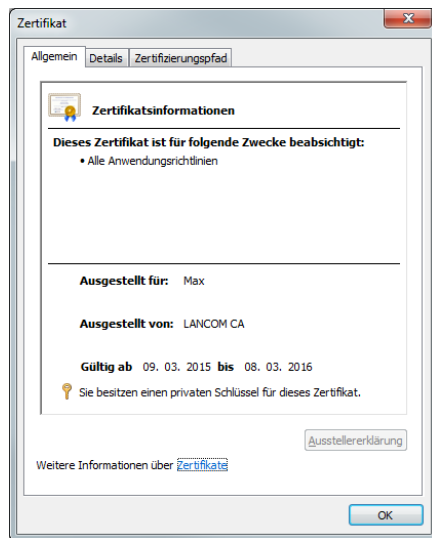
3. Fill out the **common name (CN)** field. Set a validity period for the certificate and give it a secure password (PIN). The other fields such as **Email** and **Organization name** are optional information. However, under certain circumstance this information can help to find the certificate recipient if there are problems with the certificate.

 The following characters are allowed in the password: [A-Z][a-z][0-9]#@{}~!\$%&'()*+,-./;<=>?[\]^_`.

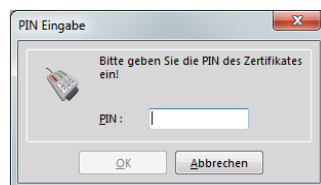
- To complete of the changes, click the **Enroll (PKCS12)** button. In the following dialog box, you can set the name and location of the file.

 The newly created certificates appear in the certificate status table under **Status > Certificates > SCEP-CA > Certificates**.

- Issue the newly enrolled certificate to the recipient together with the access password set in step 3.



- The recipient is now able to use a secure VPN dial-in. For the dial-in to succeed, the user must enter the password (PIN) set in step 3.



3.1.4 Certificate management with WEBconfig

 You need the appropriate permissions to be able to manage the certificates.

To manage a certificate via the web interface, navigate to the view **Setup Wizards > Manage certificates**. This gives you an overview of the enrolled certificates, which you can revoke if necessary.

Show 10	entries per page	Back to Main-Page	+ Create new certificate	🚫 Revoke	✅ Set as valid again	Search: <input type="text"/>			
<div><div>☐</div><div>Page</div></div>	Index	DN	SerialNumber	Status	Creation-Date	Ending-Time	Revocation-Time	Revoke-Reason	Profile-name
<div><div>☐</div></div>	1	CN=17B1AW	647B18	Valid	2015-03-27 12:28:46	2016-03-26 12:28:46		<div>▼</div>	VPN
<div><div>☐</div></div>	2	CN=17B1AW-4G	647B19	Valid	2015-03-27 12:29:19	2016-03-26 12:29:19		<div>▼</div>	VPN
	Index	DN	SerialNumber	Status	Creation-Date	Ending-Time	Revocation-Time	Revoke-Reason	Profile-name
Showing 11 to 12 of 12 entries									<div><div>First page</div><div>Previous page</div><div>1</div><div>2</div><div>Next page</div><div>Last page</div></div>

The column headers have the following meanings:

Page

This column is used to mark the entry.

Index

Displays the sequential index of the entry.

Name

Displays the name the certificate.

Serial number

Contains the serial number of the certificate.

Status

Displays the current status of the certificate. Possible values are:

- V: Valid
- R: Revoked
- P: Pending

Creation date

Displays the date of the certificate's creation (date, time).

Ending time

Indicates the date and time of (regular) certificate expiry.

Revocation time

Indicates the date and time of (premature) certificate revocation.

Revoke reason

Indicates the cause of the premature revocation. The selection is made via a drop-down selection list.

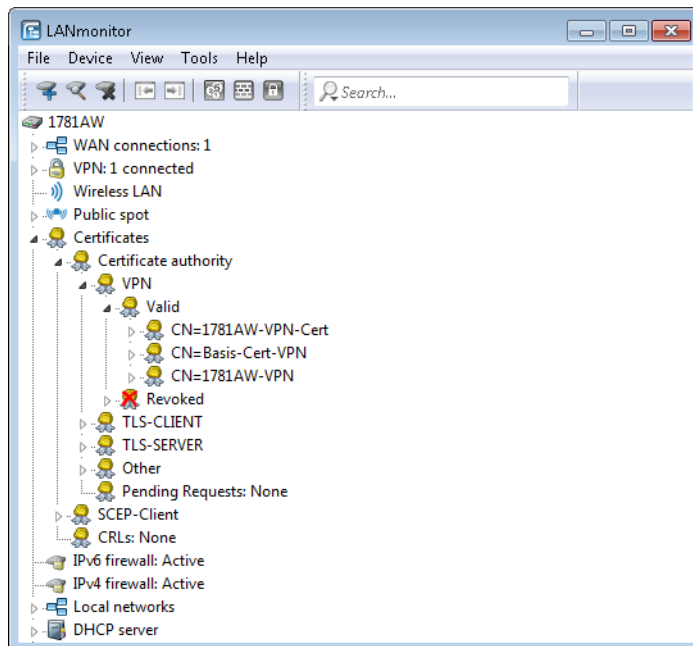
To revoke a certificate, select it in the **Page** column, in the **Revoke reason** column you select why you are revoking the certificate, and then click the **Revoke** button.

The column entries for **Status**, **Revocation time** and **Revoke reason** change accordingly.

To reverse a revocation, highlight the certificate again in the first column and click **Set as valid again**.

3.1.5 Managing certificates in LANmonitor

LANmonitor displays the active and revoked certificates, as well as the certificate requests from the SCEP clients.



To revoke a certificate, right-click on the corresponding certificate and select **Revoke certificate** from the context menu.

An overview of all revoked certificates is located in the **Revoked** section.

Certificate requests from SCEP clients can be seen in the **Pending requests** section. Right-click on the corresponding request and select either **Reject** or **Accept** in the context menu.

3.1.6 Creating certificates via URL-API

A special API can greatly simplify the creation of certificates for a complex and extensive network infrastructure.

For example, you can use a script to automate the process by sending a call to a URL with parameters attached. The following parameters are possible:

- a: Specifies the profile name.
- b: Specifies the common name.
- c: Specifies the surname.
- d: Specifies the email.
- e: Specifies the organization.
- f: Specifies the organization unit.
- g: Specifies the locality.
- h: Specifies the State or province.
- i: Specifies the country.
- j: Specifies the postal code.
- k: Specifies the serial number.
- l: Specifies the subject alternative name.
- m: Specifies the key usage.
- n: Specifies the extended key usage.
- o: Specifies the key length
- p: Specifies the validity period in days.
- q: Specifies the password for the PKCS12 file.

- \pm : Indicates whether this is a CA certificate.
 - 1: CA certificate
 - 0: No CA certificate

! The Wizard only processes the parameters set with the appropriate permissions in the presets table.

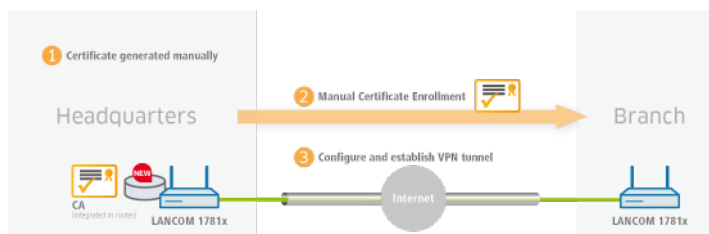
The call to the URL with the appropriate parameters looks like this:

192.168.10.74/scepwizard/a=VPN&b=iPhone&q=company

3.1.7 Tutorials

Setting up a CA and creating and using certificates for a VPN connection

This tutorial describes how you enable a CA (certificate authority) on a LANCOM router and how the CA helps you to create and use new certificates for a VPN connection between two LANCOM routers (manual certificate distribution).



! All devices need to be set with a valid date and time.

1. You enable the certificate authority in LANconfig and you set the device as the root CA. You will find these settings under **Certificates > Cert. authority (CA)**.

☒ Certificate authority (CA) active

CA hierarchy

☒ This device is the root certificate authority (Root CA).

☐ This device is a sub certificate authority (Sub CA).

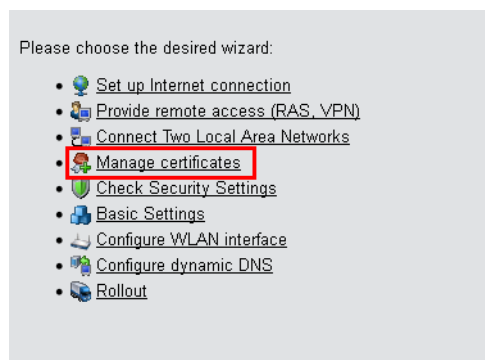
Path length:

☐ Automatically request a certificate for this sub-CA.

This menu contains all of the settings you need for retrieving a certificate for the sub-CA.

Automatic certificate request...

2. You are now able to create CA certificates for the VPN endpoints that will later provide the connection.
 - a) The Setup Wizard **Manage certificates** helps you to create certificates easily and conveniently.



- b) The first page of the Wizard is an overview of all certificates previously issued by the CA.



The certificate of the CA itself is not displayed here.

Show 10	entries per page	Back to Main-Page	+ Create new certificate	Revoke	Set as valid again		
<div><div></div><div>Page</div></div>	<div><div></div><div>Index</div></div>	<div><div></div><div>DN</div></div>	<div><div></div><div>SerialNumber</div></div>	<div><div></div><div>Status</div></div>	<div><div></div><div>Creation-Date</div></div>	<div><div></div><div>Ending-Time</div></div>	<div><div></div><div>Revocation-</div></div>
<div><div></div></div>	11	CN=1781AW	647B18	Valid	2015-03-27 12:28:46	2016-03-26 12:28:46	
<div><div></div></div>	12	CN=1781AW-4G	647B19	Valid	2015-03-27 12:29:19	2016-03-26 12:29:19	
	<div><div></div><div>Index</div></div>	<div><div></div><div>DN</div></div>	<div><div></div><div>SerialNumber</div></div>	<div><div></div><div>Status</div></div>	<div><div></div><div>Creation-Date</div></div>	<div><div></div><div>Ending-Time</div></div>	<div><div></div><div>Revocation-</div></div>

Showing 11 to 12 of 12 entries

With the **Create new certificate** button you start the process that generates a new certificate.

- c) Under the entry to **Enroll certificates**, you have the option to configure the profile, the official name of the certificate (common name or CN), and other information that is useful for identifying the certificate. Set the validity period of the certificate and the password for the Pkcs12 file that contains the new certificate, the corresponding private key, and the certificate of the CA.

Certificate

Profile-name*: VPN
Common-name (CN)*: 1781AW (e.g. VPN-Smith)
Surname (SN): (e.g. Smith)
E-Mail (E): (e.g. info@smith.de)
Organization-name (O): (e.g. smith.de)
Organization-unit-name (OU): (e.g. Management)
Locality-name (L): (e.g. Aachen)
State-or-province (ST): (e.g. NRW)
Country-name (C): (e.g. DE)
Postal-code (postalCode): (e.g. 52146)
Serial-number (serialNumber): (e.g. 12345)
Validity-period: 365 Day(s)
* marks a mandatory field.

The password is to lock the access to the generated certificate's (Pkcs12) file.
Password:

Back to Main-Page
Back to management page
Enroll(Pkcs12)

Once you have entered all the necessary information, you create the certificate by clicking the button **Enroll (Pkcs12)**. The dialog for saving the Pkcs12 file appears automatically once the certificate has been created on the device. This process can take several seconds.

- d) In the **Save the Pkcs12 file** window, choose the location and name of the Pkcs12 file. By default, the file is named according to the following format:

pkcs12<YYYY_MM_DD-hh_mm_ss>.p12

YYYY: Year

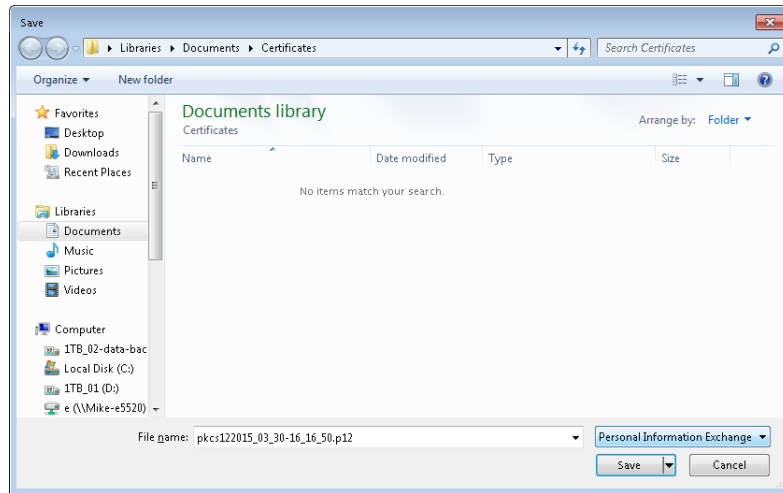
MM: Month

DD: Day

hh: Hour

mm: Minute

ss: Second



! As shown by the example, the file can have any name.

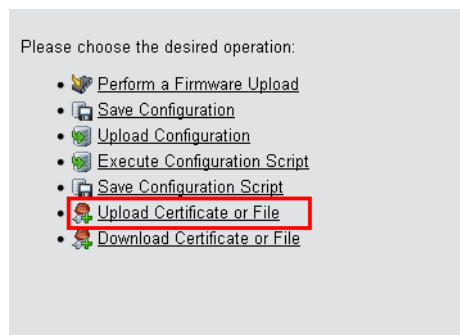
e) Use the same method to create further certificates.

Show: 10	entries per page	Back to Main-Page		+ Create new certificate	Revoke	Set as valid again	Search:		
Page	Index	DN	SerialNumber	Status	Creation Date	Ending Time	Revocation Time	Revoke Reason	Profile name
<input type="checkbox"/>	1	CN=1781AW	647B18	Valid	2015-03-27 12:28:46	2016-03-26 12:28:46			VPN
<input type="checkbox"/>	2	CN=1781AW-4G	647B19	Valid	2015-03-27 12:29:19	2016-03-26 12:29:19			VPN
Showing 11 to 12 of 12 entries									
									First page Previous page 1 2 Next page Last page

! Overview page with two created certificates.

3. In order to use the certificates for a VPN connection, you need to upload them to the devices.

a) Uploading to the corresponding VPN endpoints is easy to do with WEBconfig under **File management > Upload certificate or file**.



b) **Upload certificate or file**

First, select the file type and where to save it. For VPN connections, please choose an unused VPN container.

! As long as no certificates were set up for VPN, all of the VPN containers are unused.

In the next step you select the Pkcs12 file that contains the certificate that you want to use for this VPN endpoint. Enter the password that you have set for the file in step 2.c.

Finally, start the upload.

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: VPN - Container (VPN1) as PKCS#12-File (*.pfx, *.p12)

File Name/Location: Durchsuchen... pkcs122...1AW.p12

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.

☐ Replace existing CA certificates

Start Upload



This process is required for all VPN endpoints. Please bear in mind that each VPN endpoint needs a certificate of its own.

4. Establish a VPN connection between two VPN endpoints. This is carried out via the Setup Wizard **Connect two local area networks (VPN)**.
 - a) In the Setup Wizard, set the VPN connection authentication to **Certificates (RSA signature)**.

Setup-Assistent für 1781AW

Zwei lokale Netze verbinden (VPN)
VPN-Verbindungs-Authentifizierung auswählen

Es werden zwei Arten der VPN-Verbindungs-Authentifizierung unterstützt.
Wählen sie die Art der VPN-Verbindungs-Authentifizierung:

☐ Gemeinsames Passwort (Preshared Key)

☒ Zertifikate (RSA Signature)

Information

Bitte beachten Sie, dass bei RSA Signature digitale Zertifikate nach dem X.509-Standard sowohl für dieses Gerät als auch für den Client benötigt werden. Diese müssen per HTTP(S) ins Gerät geladen werden, damit die hier konfigurierte VPN-Verbindung zustande kommen kann.
Außerdem ist es bei der Verwendung von Zertifikaten erforderlich, dass das Gerät über eine gültige Systemzeit verfügt.

< Zurück Weiter > Abbrechen

- b) In the **Local and remote identity** window, specify the "ASN.1-Distinguished-Name". This is the official name of the certificate plus any additional information that you entered in step 2.c. You can see this additional information in the overview of certificates (step 2.e) in the "Name" column. For the **Local identity**, enter the information for the certificate on the local machine. The item **Remote identity** contains the certificate information of the other VPN endpoint.

Setup-Assistent für 1781AW

Zwei lokale Netze verbinden (VPN)
Welche "Identitäten" beschreiben die für diese VPN-Verbindung verwendeten Zertifikate?

Um die zu verwendenden Zertifikate auszuwählen, müssen deren Identitäten (Subjects) hier angegeben werden. Sie finden die Identitäten in den Zertifikaten selbst.

Lokaler und entfernter Identität-Typ sind sogenannte ASN.1-Distinguished-Names.

Lokale Identität: /CN=1781AW

Entfernte Identität: /CN=1781VA-4G

Die Identitäten sind Schrägstrich- oder Komma-separierte Aufzählungen von Typ-/Wert-Paaren (RDNs, siehe RFC 2253), zum Beispiel:
/CN=Max Mustermann/OU=Abteilung/O=Firma/C=DE oder
CN=Max Mustermann, OU=Abteilung, O=Firma, C=DE

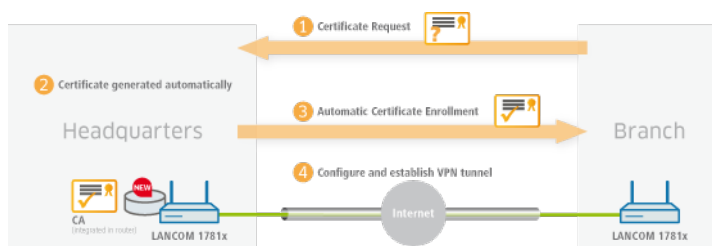
Dabei ist auf die Reihenfolge und auf die Groß-/Klein-Schreibung zu achten.

< Zurück Weiter > Abbrechen

- c) Continue to run the Wizard. You repeat this process for the other VPN endpoint of this VPN connection.

Setting up a CA and creating and using certificates for a VPN connection with certificate rollout via SCEP

This tutorial describes how you enable a CA (certificate authority) on a LANCOM router and how the CA helps you to create and use new certificates for a VPN connection between two LANCOM routers (certificate distribution via SCEP).



! We only explain the menu items that are important for the successful conclusion of the tutorial.

! All devices must be set with the correct date and time and the certificate authority must be accessible via "HTTPS".

1. You enable the certificate authority in WEBconfig or LANconfig and you set the device as the root CA. You will find these settings under **Certificates > Cert. authority (CA)**.

☒ Certificate authority (CA) active

CA hierarchy

☒ This device is the root certificate authority (Root CA).

☐ This device is a sub certificate authority (Sub CA).

Path length:

☐ Automatically request a certificate for this sub-CA.

This menu contains all of the settings you need for retrieving a certificate for the sub-CA.

Automatic certificate request...

2. SCEP clients can automatically obtain certificates by SCEP (simple certificate enrollment protocol). A necessary step for this is for you to set a general challenge password in the root CA. Set a password at **Certificates > Certificate handling**.

! If you write the configuration back to the device after enabling the CA, the CA automatically generates a general challenge password.

Certificate issuing

Set here the certificate parameters used for SCEP requests.

Validity period: days

General challenge password:

Here you can create individual challenge passwords.

Challenge table...

Set here the security features used by the CA.

CA encryption...

You are now able to create CA certificates for the VPN endpoints that will later provide the connection.

3 Smart certificates

3. In order for the VPN endpoints to obtain their certificates via SCEP, the SCEP client must be configured on each of them. This setting is located under **Certificates > SCEP client**.

SCEP client usage

☒ SCEP client usage activated

The parameters for using the SCEP (Simple Certificate Enrollment Protocol) can be selected here.

Retry after error: 30 seconds

Check pending requests: 120 seconds

Device cert. update before expiry: 2 days

CA cert. update before expiry: 3 days

Here you can define further parameters relating to the CA.

CA table...

Here you can define further parameters relating to the certificate.

Certificate table...

- a) Specify the further information about the certificate authority under **Certificates > SCEP client > CA table**. This table contains information about the CA from which a certificate is to be obtained.

CA table - New Entry

Name: CA-HEADOFFICE

URL: https://1.1.1.1/cgi-bin/p

Distinguished name: /CN=COMPANY CA/O=

Identifier:

Encryption algorithm: DES

Signature algorithm: MD5

Fingerprint algorithm: Off

Fingerprint:

☒ Registration-Authority: Enable automatic approval (RA Auto-approve)

Source address (opt.): INTRANET Select

OK Cancel

Name

The name can be freely selected and used to identify this device.

URL

The URL is always constructed in the same way: `https://<IP address>/cgi-bin/pkiclient.exe`. Replace `<IP address>` with the IPv4 address where the CA is accessible from the WAN.



If the VPN endpoint is also the CA, you need to enter the loopback address here.

Distinguished name

The distinguished name of the CA (see screenshot in step 1).

- b) The additional information about the certificate that the CA is to issue to this device is specified under **Certificates > SCEP client > Certificate table**.

Name

The name can be freely selected and used to identify this device.

CA Distinguished Name

The CA distinguished name (see screenshot in step 1).

Subject

The desired distinguished name of the certificate. In this example, only the common name is used.

Challenge password

The general challenge password set on the certificate authority (see step 2).

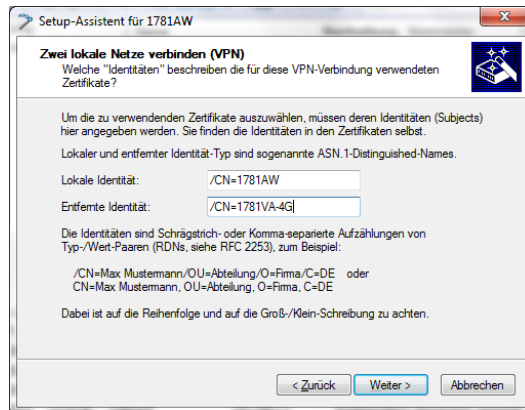
Usage type

The location where this certificate is to be stored. In this example "VPN 1".

4. Once you have set up a SCEP client on each of the VPN endpoints, you can establish a VPN connection between two VPN endpoints. This is carried out via the Setup Wizard **Connect two local area networks (VPN)**.
 - a) In the Setup Wizard, set the VPN connection authentication to **Certificates (RSA signature)**.

- b) In the **Local and remote identity** window, specify the "ASN.1-Distinguished-Name". This is the official name of the certificate plus any additional information that you entered under "Subject" in step 3.b. For the **Local**

identity, enter the information for the certificate on the local machine. The item **Remote identity** contains the certificate information of the other VPN endpoint.



- c) Continue to run the Wizard. You repeat this process for the other VPN endpoint of this VPN connection.

3.2 Additions to the Status menu

3.2.1 SCEP-CA

Displays an overview of SCEP CA certificates and requests and allows you to manage these certificates.

SNMP ID:

1.61.2

Telnet path:

Status > Certificates

Certificates

Displays current SCEP CA certificates and allows you to manage them.

SNMP ID:

1.61.2.1

Telnet path:

Status > Certificates > SCEP-CA

Certificate status table

This table displays the status of current SCEP CA certificates.

SNMP ID:

1.61.2.1.1

Telnet path:**Status > Certificates > SCEP-CA > Certificates****Index**

Displays the sequential index of the entry.

SNMP ID:

1.61.2.1.1.1

Telnet path:**Status > Certificates > SCEP-CA > Certificates > Certificate status table****Serial number**

Displays the serial number of the certificate.

This entry appears in the certificate under `serialNumber=`.

SNMP ID:

1.61.2.1.1.2

Telnet path:**Status > Certificates > SCEP-CA > Certificates > Certificate status table****Status**

Displays the status of the certificate. Possible values are:

- V: Valid
- R: Revoked
- P: Pending

SNMP ID:

1.61.2.1.1.3

Telnet path:**Status > Certificates > SCEP-CA > Certificates > Certificate status table****Creation date**

Displays the creation date of the certificate.

SNMP ID:

1.61.2.1.1.4

Telnet path:**Status > Certificates > SCEP-CA > Certificates > Certificate status table****Ending time**

Displays the expiry time of the certificate.

This entry appears in the certificate under `validity`.**SNMP ID:**

1.61.2.1.1.5

Telnet path:**Status > Certificates > SCEP-CA > Certificates > Certificate status table****Revocation time**

Displays the certificate revocation time if the certificate has been revoked.

SNMP ID:

1.61.2.1.1.6

Telnet path:**Status > Certificates > SCEP-CA > Certificates > Certificate status table****Revoke reason**

Displays the reason for certificate revocation if the certificate has been revoked.

SNMP ID:

1.61.2.1.1.7

Telnet path:**Status > Certificates > SCEP-CA > Certificates > Certificate status table****Possible values:****unspecified**

No reason given.

keyCompromise

The private key is compromised.

cACompromise

The private CA key is compromised.

affiliationChanged

Details of the holder or the issuer of the certificate have changed.

superseded

The certificate is outdated and has been replaced by a new certificate.

cessationOfOperation

The certificate is no longer required for the original purpose.

certificateHold

The certificate is on hold until it is finally revoked or released again.

privilegeWithdrawn

The certificate contains a right that is not longer valid.

aACompromise

The private AA key is compromised.

MAC address

Displays the MAC address of the device for which the certificate was issued.

SNMP ID:

1.61.2.1.1.8

Telnet path:

Status > Certificates > SCEP-CA > Certificates > Certificate status table

Name

Displays the CN of the certificate.

SNMP ID:

1.61.2.1.1.9

Telnet path:

Status > Certificates > SCEP-CA > Certificates > Certificate status table

Profile name

Displays the name of the profile that the certificate is based on.

SNMP ID:

1.61.2.1.1.10

Telnet path:

Status > Certificates > SCEP-CA > Certificates > Certificate status table

Revoke certificate

This action revokes a certificate. This is necessary if the certificate has been compromised or if there have been changes (rights, information about the issuer) to the certificate.

This action requires the specification of up to three parameters in the form `<Index> , <Reason> [, <Date>]`:

Index

The index of the corresponding certificate in the certificate table (required).

Reason

The reason of the revocation (required). The following values are possible:

- 0: Unspecified
- 1: Key compromise
- 2: CA compromise
- 3: Affiliation changed
- 4: Superseded
- 5: Cessation of operation
- 6: Certificate hold
- 8: Remove from CRL
- 9: Privilege withdrawn
- 10: Attribute authority compromise

Date

This specification describes the time in UTC format (YYMMDDHHSSZ) when the certificate is compromised (optional if you specify the reasons 1, 2 and 10).



Specify the parameters each separated by a comma and without spaces.



Entering ? generates a help text.

SNMP ID:

1.61.2.1.2

Telnet path:

Status > Certificates > SCEP-CA > Certificates

Set certificate on hold

This action sets a certificate on "Hold". This option is available if you want to clarify the status of the certificate before fully revoking it.

This action requires a parameter to be specified in the form `<Index>`:

Index

The index of the corresponding certificate in the certificate table (required).



Entering ? generates a help text.

SNMP ID:

1.61.2.1.3

Telnet path:**Status > Certificates > SCEP-CA > Certificates****Declare certificate as valid again**

With this action you declare a certificate that was previously on "Hold" to be valid again.

This action requires an index list to be specified in the form <Index1> , <Index2> , <Index3>:

Indexn

The indexes of the corresponding certificates in the certificate table (required).



Specify the indexes each separated by a comma and without spaces.



Entering ? generates a help text.

SNMP ID:

1.61.2.1.4

Telnet path:**Status > Certificates > SCEP-CA > Certificates****Requests**

Displays current requests for SCEP CA certificates and allows you to manage them.

SNMP ID:

1.61.2.2

Telnet path:**Status > Certificates > SCEP-CA****Pending-Requests**

This table displays the status of pending requests for SCEP CA certificates.

SNMP ID:

1.61.2.2.1

Telnet path:**Status > Certificates > SCEP-CA > Requests**

Index

Displays the sequential index of the entry.

SNMP ID:

1.61.2.2.1.1

Telnet path:

Status > Certificates > SCEP-CA > Requests > Pending-requests

Transaction ID

Displays the transaction ID of the entry.

SNMP ID:

1.61.2.2.1.2

Telnet path:

Status > Certificates > SCEP-CA > Requests > Pending-requests

MAC address

Displays the MAC address of the requesting device.

SNMP ID:

1.61.2.2.1.3

Telnet path:

Status > Certificates > SCEP-CA > Requests > Pending-requests

Name

Displays the name of the requesting device.

SNMP ID:

1.61.2.2.1.4

Telnet path:

Status > Certificates > SCEP-CA > Requests > Pending-requests

IP address

Displays the IP address of the requesting device.

SNMP ID:

1.61.2.2.1.5

Telnet path:**Status > Certificates > SCEP-CA > Requests > Pending-requests****PKI-Status**

Displays the status of the public-key infrastructure of the requesting device.

SNMP ID:

1.61.2.2.1.6

Telnet path:**Status > Certificates > SCEP-CA > Requests > Pending-requests****Reason**

Displays the reason for the request.

SNMP ID:

1.61.2.2.1.7

Telnet path:**Status > Certificates > SCEP-CA > Requests > Pending-requests****DN**

Displays the fingerprint for the request.

SNMP ID:

1.61.2.2.1.8

Telnet path:**Status > Certificates > SCEP-CA > Requests > Pending-requests****Receive date**

Displays the time of the request.

SNMP ID:

1.61.2.2.1.9

Telnet path:

Status > Certificates > SCEP-CA > Requests > Pending-requests

Issue certificate

With the syntax `do Issue-Certificate [index-list]` you issue a SCEP-CA certificate for a device. `[index-list]` is a comma-separated list of the indexes from the table "Pending requests". Each request index entered here receives a certificate.

SNMP ID:

1.61.2.2.2

Telnet path:

Status > Certificates > SCEP-CA > Requests

Grant all certificates

With the syntax `do Issue-Certificate` you issue a SCEP-CA certificate for all devices. You do not have to specify any additional parameters. All pending requests will receive a certificate.

SNMP ID:

1.61.2.2.3

Telnet path:

Status > Certificates > SCEP-CA > Requests

Decline request

With the syntax `do Decline-Request [index-list]`, you reject the request from a device. `[index-list]` is a comma-separated list of the indexes from the table "Pending requests". Any request with the index you specified will be declined. The requesting device does not receive a certificate.

SNMP ID:

1.61.2.2.4

Telnet path:

Status > Certificates > SCEP-CA > Requests

Deny all requests

With the syntax `do Deny-all-requests [index-list]`, you reject the requests from all devices. You do not have to specify any additional parameters. All pending requests will be rejected.

SNMP ID:

1.61.2.2.5

Telnet path:**Status > Certificates > SCEP-CA > Requests****Delete-pending-request**

You delete a pending request with the syntax `do Delete-Pending-Request [index-list]`.
[index-list] is a comma-separated list of the indexes from the table "Pending requests". Any request with the index you specified will be deleted.

SNMP ID:

1.61.2.2.6

Telnet path:**Status > Certificates > SCEP-CA > Requests****Delete-all-pending-requests**

With the syntax `do Delete-all-pending-requests` you delete all pending requests. You do not have to specify any additional parameters. All pending requests will be deleted.

SNMP ID:

1.61.2.2.7

Telnet path:**Status > Certificates > SCEP-CA > Requests****CA-Status**

Displays the current status of SCEP-CA certificates and allows you to manage them.

SNMP ID:

1.61.2.3

Telnet path:**Status > Certificates > SCEP-CA****Log table**

This table displays current events relating to the CA status.

SNMP ID:

1.61.2.3.7

Telnet path:**Status > Certificates > SCEP-CA > CA-Status****Web interface**

This directory gives you an overview of the settings for the SCEP-CA web interface.

SNMP ID:

1.61.2.4

Telnet path:**Status > Certificates > SCEP-CA****Profiles**

The configured profiles are shown in this table. To view the certificate properties, click on a profile name.

SNMP ID:

1.61.2.4.1

Telnet path:**Status > Certificates > SCEP-CA > Web-Interface****Template**

The templates for the certificate profiles are shown in this table. To view the custom settings, click the name of a template.

SNMP ID:

1.61.2.4.2

Telnet path:**Status > Certificates > SCEP-CA > Web-Interface**

3.3 Additions to the Setup menu

3.3.1 Web interface

In this directory, you configure the settings for the SCEP-CA web interface.

SNMP ID:

2.39.2.14

Telnet path:**Setup > Certificates > SCEP-CA****Profiles**

In this table you create profiles with collected certificate properties.



By default three profiles are already available for common application scenarios.

SNMP ID:

2.39.2.14.1

Telnet path:**Setup > Certificates > SCEP-CA > Web-Interface****Profile name**

Here you assign a unique name for the profile.

SNMP ID:

2.39.2.14.1.1

Telnet path:**Setup > Certificates > SCEP-CA > Web-Interface > Profiles****Possible values:**

Max. 32 characters from `[A-Z][0-9]@{ }~!$%&'()+-/, : ; < = > ? [\] ^ _ .`

Default:*empty***Key usage**

Specifies for which application the profile is to be used. The following usages are available:

- critical
- digitalSignature
- nonRepudiation
- keyEncipherment
- dataEncipherment
- keyAgreement
- keyCertSign
- cRLSign

- encipherOnly
- decipherOnly

Multiple comma-separated entries can be selected.

SNMP ID:

2.39.2.14.1.2

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Profiles

Possible values:

Max. 251 characters from [A-Z][a-z][0-9]#{|}~!"\$%&'()*+,-./:;<=>?[\]^_`~

Default:

critical,digitalSignature,keyEncipherment

Extended key usage

Specifies the extended application for which the profile is to be used. The following usages are available:

- critical
- serverAuth: SSL/TLS Web server authentication
- clientAuth: SSL/TLS Web client authentication
- codeSigning: Signing of program code
- emailProtection: E-mail protection (S/MIME)
- timeStamping: Furnishing data with reliable time stamps
- msCodeInd: Microsoft Individual Code Signing (authenticode)
- msCodeCom: Microsoft Commercial Code Signing (authenticode)
- msCTLSign: Microsoft Trust List Signing
- msSGC: Microsoft Server Gated Crypto
- msEFS: Microsoft Encrypted File System
- nsSGC: Netscape Server Gated Crypto

Multiple comma-separated entries can be selected.

SNMP ID:

2.39.2.14.1.3

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Profiles

Possible values:

Max. 251 characters from [A-Z][a-z][0-9]#{|}~!"\$%&'()*+,-./:;<=>?[\]^_`~

Default:

empty

RSA key length

Sets the length of the key.

SNMP ID:

2.39.2.14.1.4

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Profiles

Possible values:

1024

2048

3072

4096

8192

Default:

2048

Validity period

Specifies the duration, in days, for which the key is valid. After this period, the key becomes invalid unless the user renews it.

SNMP ID:

2.39.2.14.1.5

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Profiles

Possible values:

Max. 10 characters from 0123456789

Default:

365

CA

Indicates whether this is a CA certificate.

SNMP ID:

2.39.2.14.1.6

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Profiles

Possible values:

Yes
No

Default:

No

Password

Password to protect the PKCS12 certificate file.

SNMP ID:

2.39.2.14.1.7

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Profiles

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#{|}~!$%&'()*+,-./:;<=>?[\]^_`~`

Default:

empty

Country

Enter the country identifier (e.g. "DE" for Germany).

This entry appears in the subject or issuer of the certificate under C= (Country).

SNMP ID:

2.39.2.14.1.8

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Profiles

Possible values:

2 characters from `[A-Z][0-9]@{|}~!$%&'()*+,-./:;<=>?[\]^_`~`

Default:

empty

Locality name

Enter the name of the locality.

This entry appears in the subject or issuer of the certificate under L= (Locality).

SNMP ID:

2.39.2.14.1.9

Telnet path:**Setup > Certificates > SCEP-CA > Web-Interface > Profiles****Possible values:**Max. 32 characters from `[A-Z][0-9]@{ }~!$%&'()+-,:;=>?[\]^_.`**Default:***empty***Organization**

Enter the organization that issues the certificate.

This entry appears in the subject or issuer of the certificate under O= (Organization).

SNMP ID:

2.39.2.14.1.10

Telnet path:**Setup > Certificates > SCEP-CA > Web-Interface > Profiles****Possible values:**Max. 32 characters from `[A-Z][0-9]@{ }~!$%&'()+-,:;=>?[\]^_.`**Default:***empty***Organization unit name**

Enter the organization that issues the certificate.

This entry appears in the subject or issuer of the certificate under OU= (Organization Unit).

SNMP ID:

2.39.2.14.1.11

Telnet path:**Setup > Certificates > SCEP-CA > Web-Interface > Profiles****Possible values:**Max. 32 characters from `[A-Z][0-9]@{ }~!$%&'()+-,:;=>?[\]^_.`**Default:***empty*

State or province

Enter the State or province.

This entry appears in the subject or issuer of the certificate under `ST= (STate)`.

SNMP ID:

2.39.2.14.1.12

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Profiles

Possible values:

Max. 32 characters from `[A-Z][0-9]{ | }~!$%&'()+- , / : ; < = > ? [\] ^ _ .`

Default:

empty

E-mail

Enter an e-mail address:

This entry appears in the subject or issuer of the certificate under `emailAddress=`.

SNMP ID:

2.39.2.14.1.13

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Profiles

Possible values:

Max. 36 characters from `[A-Z][0-9]{ | }~!$%&'()+- , / : ; < = > ? [\] ^ _ .`

Default:

empty

Surname

Enter a surname.

This entry appears in the subject or issuer of the certificate under `SN= (SurName)`.

SNMP ID:

2.39.2.14.1.14

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Profiles

Possible values:

Max. 32 characters from `[A-Z][0-9]{ | }~!$%&'()+- , / : ; < = > ? [\] ^ _ .`

Default:*empty***Serial number**

Enter a serial number.

This entry appears in the certificate under `serialNumber=`.

SNMP ID:

2.39.2.14.1.15

Telnet path:**Setup > Certificates > SCEP-CA > Web-Interface > Profiles****Possible values:**

Max. 32 characters from `[A-Z][0-9]@{ | }~!$%&'()+- , / : ; < = > ? [\] ^ _ .`

Default:*empty***Postal code**

Enter the location post code.

This entry appears in the subject or issuer of the certificate under `postalCode=`.

SNMP ID:

2.39.2.14.1.16

Telnet path:**Setup > Certificates > SCEP-CA > Web-Interface > Profiles****Possible values:**

Max. 25 characters from `[A-Z][0-9]@{ | }~!$%&'()+- , / : ; < = > ? [\] ^ _ .`

Default:*empty***Template**

Select a suitable profile template here, if applicable.

The profile template specifies which certificate information is mandatory and which can be changed. Templates are created under **Setup > Certificates > SCEP-CA > Web-Interface > Template**.

SNMP ID:

2.39.2.14.1.17

Telnet path:**Setup > Certificates > SCEP-CA > Web-Interface > Profiles****Possible values:**Max. 31 characters from `[A-Z][0-9]@{ }~!$%&'()+-./:;<=>?[\]^_.`**Default:***empty***Subject-Alternative-Name**

Specify the subject alternative name (SAN) here. The SAN contains further information for use by applications.

SNMP ID:

2.39.2.14.1.18

Telnet path:**Setup > Certificates > SCEP-CA > Web-Interface > Profiles****Possible values:**Max. 254 characters from `[A-Z][0-9]@{ }~!$%&'()+-./:;<=>?[\]^_.`**Default:***empty***Template**

In this table, you define the templates for certificate profiles.

Here you specify which of the profile properties are mandatory and which are to be edited by the user. The following options are available:

- No: The field is invisible, the value entered is considered to be a default value.
- Fixed: The field is visible, but cannot be changed by the user.
- Yes: The field is visible and can be changed by the user.
- Mandatory: The field is visible, the user must enter a value.



A "Default" template is already available.

SNMP ID:

2.39.2.14.2

Telnet path:**Setup > Certificates > SCEP-CA > Web-Interface**

Name

Give the template a unique name here.

SNMP ID:

2.39.2.14.2.1

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Template

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{ }~!$%&'()*~:-<>?[\]_.`

Default:

empty

Key usage

Specifies for which application the profile is to be used.

SNMP ID:

2.39.2.14.2.2

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Template

Possible values:**Yes**

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Extended key usage

Specifies the extended application for which the profile is to be used.

SNMP ID:

2.39.2.14.2.3

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Template

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

RSA key length

Sets the length of the key.

SNMP ID:

2.39.2.14.2.4

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Template

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Validity period

Specifies the duration, in days, for which the key is valid. After this period, the key becomes invalid unless the user renews it.

SNMP ID:

2.39.2.14.2.5

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Template

Possible values:**Yes**

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

CA

Indicates whether this is a CA certificate.

SNMP ID:

2.39.2.14.2.6

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Template

Possible values:**Yes**

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Password

Password to protect the PKCS12 certificate file.

SNMP ID:

2.39.2.14.2.7

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Template

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Country

Specifies the country identifier (e.g. "DE" for Germany).

SNMP ID:

2.39.2.14.2.8

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Template

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Locality name

Specifies the locality.

SNMP ID:

2.39.2.14.2.9

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Template

Possible values:**Yes**

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Organization

Specifies the organization issuing the certificate.

SNMP ID:

2.39.2.14.2.10

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Template

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Organization unit name

Specifies the unit within the organization that issues the certificate.

SNMP ID:

2.39.2.14.2.11

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Template

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

State or province

Specifies the State or province.

SNMP ID:

2.39.2.14.2.12

Telnet path:**Setup > Certificates > SCEP-CA > Web-Interface > Template****Possible values:****Yes**

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

E-mail

Specifies the e-mail address.

SNMP ID:

2.39.2.14.2.13

Telnet path:**Setup > Certificates > SCEP-CA > Web-Interface > Template****Possible values:****Yes**

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Surname

Specifies the surname.

SNMP ID:

2.39.2.14.2.14

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Template

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Serial number

Specifies the serial number.

SNMP ID:

2.39.2.14.2.15

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Template

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Postal code

Specifies the postal code.

SNMP ID:

2.39.2.14.2.16

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Template

Possible values:**Yes**

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Subject-Alternative-Name

The "Subject Alternative Name" (SAN) links additional data with this certificate.

SNMP ID:

2.39.2.14.2.17

Telnet path:

Setup > Certificates > SCEP-CA > Web-Interface > Template

Possible values:**Yes**

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

3 Smart certificates

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

4 High availability clustering

As of LCOS version 9.10, all devices in a defined group take on any changes to the configuration of any device within this group.



As of LCOS version 9.10, the LANCOM WLC High Availability Clustering XL option and the LANCOM VPN High Availability Clustering XL option enable you to collect several devices to a cluster. This applies to the LANCOM WLAN controllers (LANCOM WLC-4025+ and LANCOM WLC-4100) and LANCOM central-site VPN gateways (LANCOM 7100+ VPN and LANCOM 9100+ VPN). This options provides highly convenient central management in combination with configuration synchronization (Config Sync) between all of the clustered devices. In WLAN controller-based installations you additionally benefit from automatic load balancing, intelligent high-availability scenarios, and the issuing of cluster certificates.

4.1 Automatic configuration synchronization (Config Sync) with the LANCOM WLC High Availability Clustering XL option

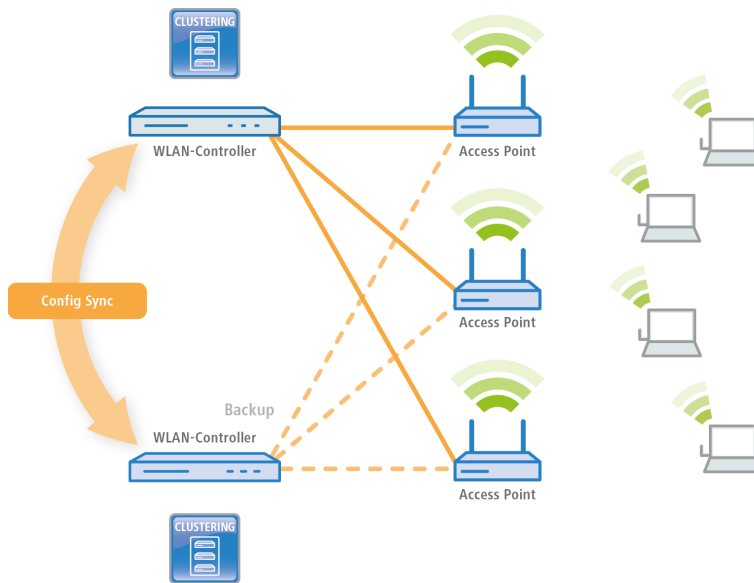
Example application, WLAN controllers:

WLAN infrastructures have become an integral part of modern corporate networks. In the age of the "all wireless office", the increasing demands on the availability of a WLAN solution make it essential to have a reliable backup and high-availability solution. In WLAN infrastructures with a single WLAN controller, any failures or maintenance downtimes (such as a firmware update) of the WLC until now caused the APs connected to it to switch to standalone operation. Consequently, the APs in standalone mode were no longer able to access the features that are provided centrally by the WLC such as a Public Spot, IEEE 802.1X authentication, or Layer-3 tunnels.

In order to avoid this and to maintain the full operation of all WLAN capabilities even if a WLC should be temporarily unavailable, one or more redundant or backup WLCs should be employed. In the backup event, the APs automatically switch from the temporarily unavailable WLC to a backup WLC. The backup WLC has the same configuration (e.g. AP table or WLAN profiles) as required by the primary WLC of the APs. The initial setup of the WLCs and any subsequent configuration changes must be carried out separately and identically on each device—an enormous effort for the administrator. Manual maintenance of the configurations between multiple identical devices could lead to outdated or non-synchronous configurations on the backup WLCs, which in the case of a backup event could lead to a critical state for the entire WLAN infrastructure. The resulting troubleshooting usually turns out to be a real challenge. The users of the WLAN clients experience a loss of productivity, which could have major consequences company-wide.

New with the LANCOM WLC High Availability Clustering XL option: This software option allows multiple WLCs to be grouped into a highly-available cluster. In this way, configuration changes, features and enhancements made on one WLC are automatically transferred between the other WLCs in the cluster, without having to make manual changes on

each individual device. Common parameters in a cluster (e.g. WLAN profiles, AP tables, or Public Spot settings) remain synchronized, individual parameters (such as the IP address of the WLC) are not exchanged.



The LANCOM WLC High Availability Clustering XL option offers greatly simplified administration and huge time savings because you only need to configure one WLC in the cluster. The WLC then transfers the changes to the other cluster devices automatically. In the case of maintenance downtime (e.g. for a firmware update) or even the failure of a WLC, the APs automatically connect to another WLC which, thanks to Config Sync, already has the identical configuration without any intervention by the administrator. The result is a convenient way to high availability.

The prerequisites for a device to be a valid member of a cluster are:

- The LANCOM WLC High Availability Clustering XL option (as of LCOS version 9.10) must be available.
- IP communications must be available to all other devices, e.g. via LAN, WAN, or VPN.
- It must be in the list of group members that is stored in each device.
- A valid certificate must be available
- It needs to authenticate itself by certificate as a member of the cluster.

4.2 Automatic configuration synchronization (Config Sync) with the LANCOM VPN High Availability Clustering XL option

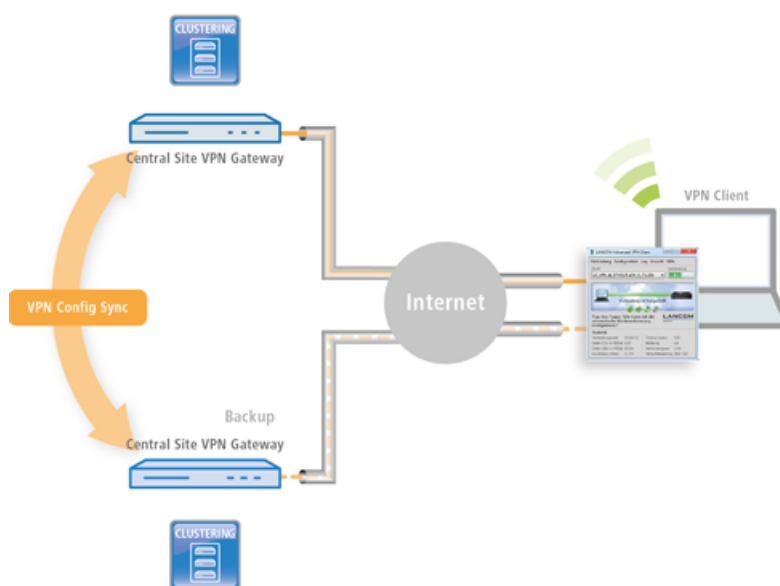
Example application, VPN:

VPN infrastructures have been a part of corporate networks for a long time now. The demands on the availability of VPN gateways have increased sharply in recent years. Whereas VPN solutions in professional scenarios were mainly temporary in the past, e.g. for sales representatives with VPN clients, these days home or branch offices are often permanently linked to the main office via a VPN tunnel. They support voice services (VoIP), database applications, or file services, for example. With increasing dependence on VoIP services or critical business applications, the need for reliable backup and high-availability of the VPN solution has increased.

In order for VPN services in larger-scale critical network infrastructures to remain highly available, it is advisable that you operate one or more backup VPN gateways in addition to the primary VPN gateway. In this case, the failure or downtime of a central-site VPN gateway causes another device to operate as a backup. The VPN connection is automatically established via the accessible backup central-site VPN gateway.

For this purpose the backup central-site VPN gateway needs to have the same configuration as the primary central-site VPN gateway. In particular VPN user data and the firewall configuration must be present on both devices in order for a user to be authenticated and the services to be provided correctly. This requires a manual setup of each individual device—in other words, a huge amount of work for the administrator.

New with the LANCOM VPN High Availability Clustering XL option: This option allows multiple central-site VPN gateways to be grouped into a cluster. In this way, configuration changes, features and enhancements made on one central-site VPN gateway are automatically transferred between the cluster devices, without having to make manual changes on each individual device. Common parameters in a cluster (e.g. VPN user database, firewall) remain synchronized, individual parameters (such as the IP address) are not exchanged.



The prerequisites for a device to be a valid member of a cluster are:

- The LANCOM VPN High Availability Clustering XL option (as of LCOS version 9.10) must be available.
- IP communications must be available to all other devices, e.g. via LAN, WAN, or VPN.
- It must be in the list of group members that is stored in each device.
- A valid certificate must be available
- It needs to authenticate itself by certificate as a member of the cluster.

4.3 Setting up configuration synchronization

In order for configuration synchronization to function, all of the devices to be configured need to have valid certificates. In the interests of easy certificate distribution, you first need to configure a SCEP-CA on one of the devices.

4 High availability clustering

1. To do this it is necessary to enable the SCEP server under **Certificates > SCEP CA**. If you set up the configuration synchronization on a WLC, it is most likely that the SCEP server is already active.

☒ Certificate authority (CA) active

CA hierarchy

☒ This device is the root certificate authority (Sub CA).
☐ This device is a sub certificate authority.

Path length:

☐ Automatically request a certificate for this sub-CA.

This menu contains all of the settings you need for retrieving a certificate for the sub-CA.

[Automatic certificate request...](#)

CA/RA certificates

Set here the certificate parameters as used by the CA or RA (Registration Authority).

CA Distinguished Name:

RA distinguished name:

[Advanced...](#)

Event notification

Here you may define the notification form which has to be used if the CA has an initialization error or can not respond a request.

☐ Activate event logging (SYSLOG)
☐ Activate E-Mail notification
☒ Send backup reminder email

E-Mail recipient:

2. Then you enable the SCEP client on any device that is to work with configuration synchronization (including the SCEP CA device) under **Certificates > SCEP client**. If you set up the configuration synchronization on a WLC, it is most likely that the SCEP client is already active.

SCEP client usage

☒ SCEP client usage activated

The parameters for using the SCEP (Simple Certificate Enrollment Protocol) can be selected here.

Retry after error: seconds

Check pending requests: seconds

Device cert. update before expiry: days

CA cert. update before expiry: days

Here you can define further parameters relating to the CA.

[CA table...](#)

Here you can define further parameters relating to the certificate.

[Certificate table...](#)

3. Add a new entry for the SCEP server to the **CA table**.

The values for the CA table match the settings of the SCEP server from step 1 and are thus the same for all stations. For the URL you enter `http://IPADR/cgi-bin/pkiclient.exe`, replacing IPADR with the IP address of the device configured as SCEP-CA.

If you set up the configuration synchronization on a WLC, a corresponding entry for the WLC operation will already be available. This entry can also be used to obtain a certificate for configuration synchronization, and in this case there is no need to make any changes to the CA table.

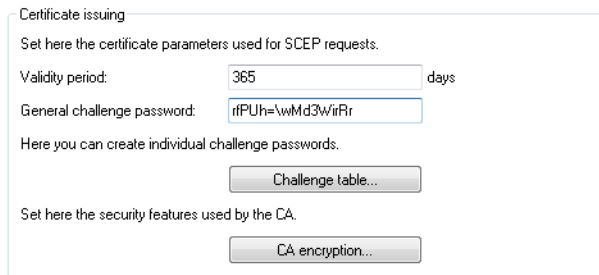
4. The **Certificate table** in the SCEP client needs a new entry for the retrieval of a configuration synchronization certificate. The **CA distinguished name** is the one you used when you created the CA table entry.

As the subject, enter each device's own IP address (e.g. /CN=IPADR /O=COMPANY/C=DE), replacing IPADR with the IP address of the device configured as SCEP-CA.

! In order for the configuration synchronization to function, it is absolutely necessary for the IP address of the device to be included in the certificate's subject.

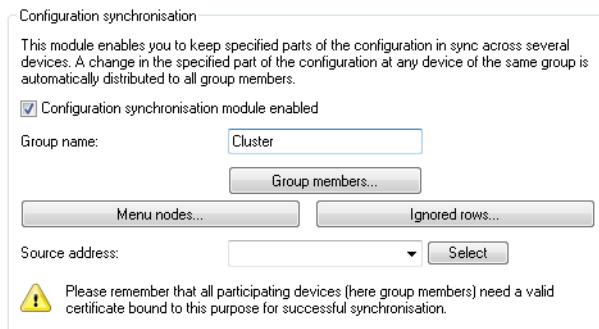
Set the **Usage type** to "Configuration synchronization". Also, adjust the **Key length** to "2048 bits". Set a **Name** of your choice for the table entry.

The challenge password of the device configured as SCEP CA is located in its configuration under **Certificates > Certificate handling > General challenge password**.



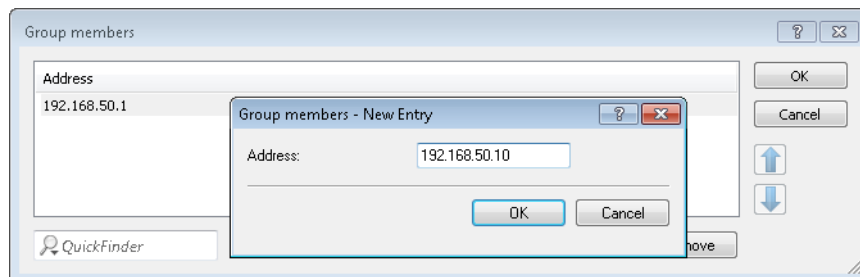
Certificate issuing
 Set here the certificate parameters used for SCEP requests.
 Validity period: 365 days
 General challenge password: rPUh=\wMd3w/rRr
 Here you can create individual challenge passwords.
 Challenge table...
 Set here the security features used by the CA.
 CA encryption...

5. This concludes the set up of the SCEP CA and the SCEP client for the retrieval of configuration synchronization certificates. At this time you can write the configuration back to the device in order to retrieve the certificates.
6. Now activate the configuration synchronization under **Management > Synchronization** with the option **Configuration synchronization module enabled**. Under **Cluster name** you can also set a name that appears in the LANconfig device list.



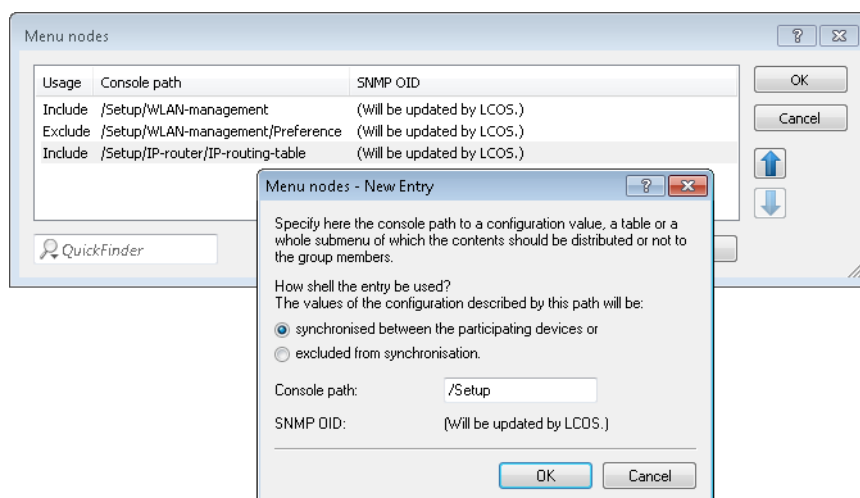
Configuration synchronisation
 This module enables you to keep specified parts of the configuration in sync across several devices. A change in the specified part of the configuration at any device of the same group is automatically distributed to all group members.
☒ Configuration synchronisation module enabled
 Group name: Cluster
 Group members...
 Menu nodes... Ignored rows...
 Source address:
 Select
 Please remember that all participating devices (here group members) need a valid certificate bound to this purpose for successful synchronisation.

7. Under **Cluster members**, enter the IP addresses of **all** of the devices that are to be members of the cluster.

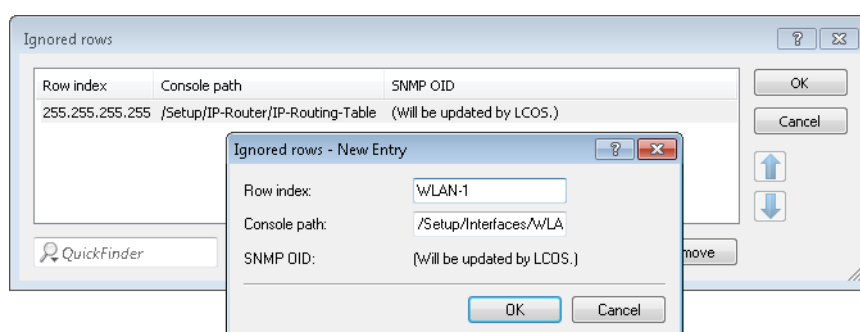


Group members
 Address
 192.168.50.1
 Group members - New Entry
 Address: 192.168.50.10
 OK Cancel
 QuickFinder

8. Under **Menu nodes** you specify the menus you want to synchronize. If you wish to explicitly exclude menu nodes from the synchronization, set the **Usage** to "excluded from synchronization".



Under "Ignored rows" you can optionally specify the rows of a table that should be excluded from synchronization. Example: The default route on VPN gateways, which should be different for each gateway. The rest of the routing table can be synchronized by making an entry in the **Menu nodes**.



9. The set up of configuration synchronization is now concluded for this device. You can write the configuration back to the device.
10. Perform steps 2 through 9 on the other devices that belong to the cluster. When configuring each SCEP client, point to the SCEP CA of the first device, as indicated above.
11. Now start the cluster on the device that should initially distribute its configuration to the other cluster members. To do this in LANconfig, select the appropriate entry from the device list and, in the context menu, click **[Start cluster...]**.
12. The cluster is now in operation. You can check the state of the cluster in WEBconfig under **Status > Config > Sync > Status**. Now, configuration changes made on any cluster member are synchronized to the other members.

Please note the following requirements:

- The correct time must be set on all of the involved devices (certificate checks).
- The IP address of each device must appear in the subject of its own certificate.
- To menu trees for synchronization must be the same on both devices (which is not always the case with different firmware versions or device options).
- If any changes are made to the configuration of the configuration synchronization (menu nodes, etc.) after the cluster was started already, then the cluster must be restarted.

4.4 1-Click WLC High Availability Clustering Wizard

With the 1-Click WLC High Availability Clustering Wizard, you can use LANconfig to simultaneously configure multiple WLCs under the following conditions:

- All of the WLCs have the WLC High Availability Clustering XL option enabled.
- At least one WLC is fully configured. This is the case if it is already managing APs.
- At least one WLC has a basic configuration (at least the name and IP address are set).

 In case of doubt, you should start the Basic Settings Wizard on the corresponding WLC.

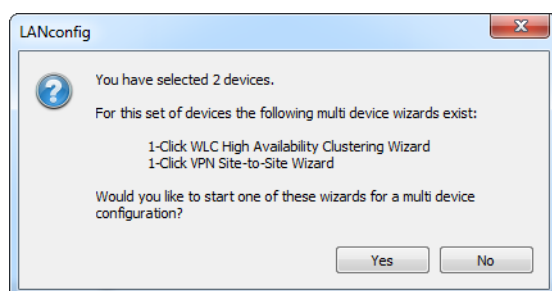
 All WLCs in the cluster have the same rights.

1. In the device list, select the two WLCs that you want to configure together.

There are two ways to start the WLC Clustering Wizard:

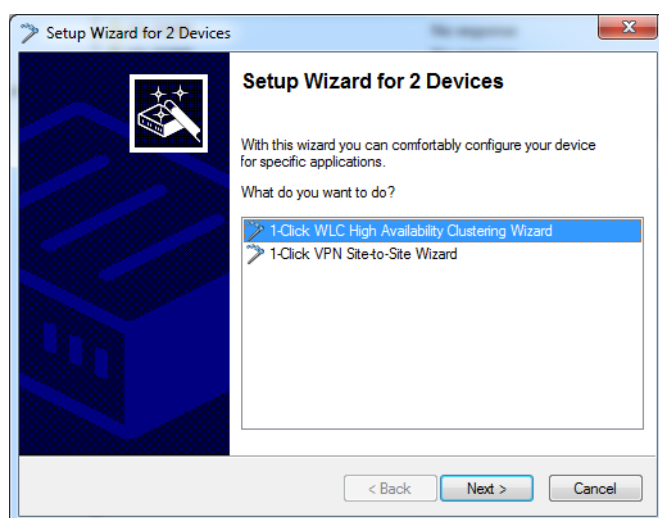
- In the device list, drag & drop the unconfigured WLC onto the configured WLC.
- Select the two WLCs in the device list and, after a right-click, select the item **Setup Wizard** from the context menu.

LANconfig then displays the following message:

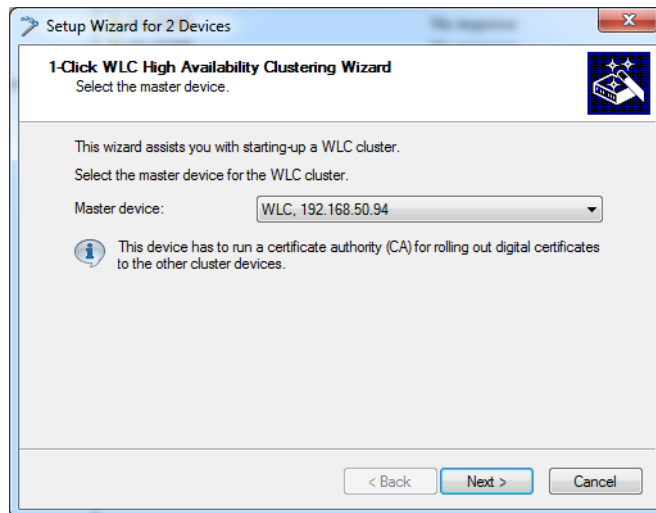


Start the Setup Wizard by clicking on **Yes**. The Setup Wizard starts with the selection dialog for the multiple-devices Wizard.


2. Select the "1-Click WLC High Availability Clustering Wizard" and then click **Next**.



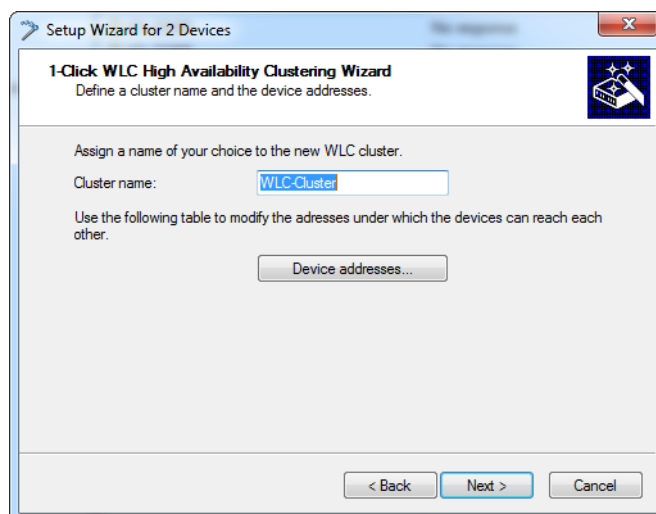
3. Select the master device, and then click **Next**



The master device is the preconfigured WLC. After you finish, the Setup Wizard transfers its configuration to all of the other selected WLCs.

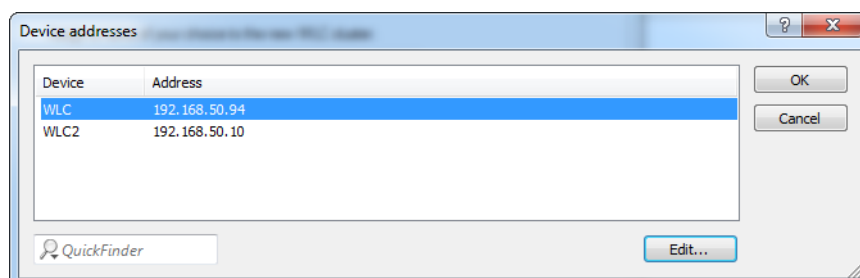
-  This query does not appear if you transfer the configuration to another WLC via drag & drop. In this case, the Setup Wizard automatically takes the "dragged" WLC to be the master device.

4. Assign a cluster name and click **Device addresses**.



The Setup Wizard suggests a cluster name, although you can change this if you so wish.

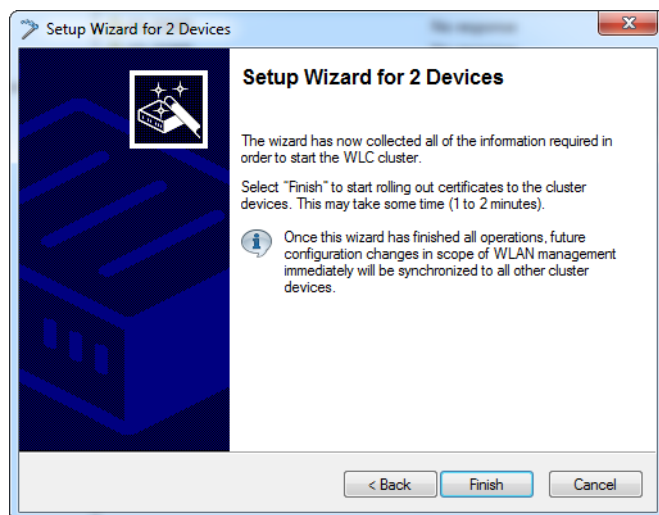
5. Enter the device addresses of all of the WLCs in the cluster.



By default, the Setup Wizard enters the devices that LANconfig is able to reach. Make any necessary changes, for example by entering devices that are accessible via VPN.

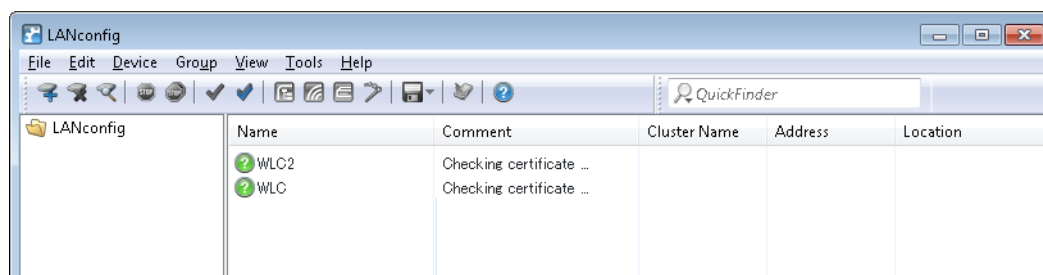
Click **OK**, and then click **Next**.

6. Click **Finish** to complete the Setup Wizard.



The Setup Wizard now loads the configuration of the master device to the selected WLCs.

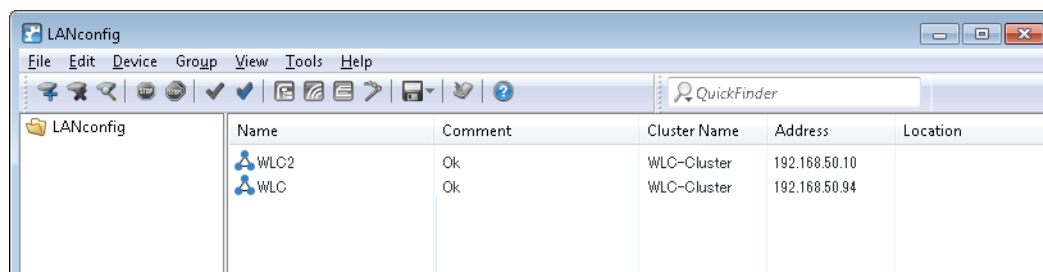
7. The device list displays the WLCs as follows:



The Setup Wizard has configured the SCEP client on all WLCs so that they can fetch a Config Sync. LANconfig now waits until the certificates are available for all of the WLCs.

 Creation of the certificates may take up to one minute.

8. Once the certificates are available for all of the WLCs, LANconfig displays the status "OK" for these WLCs along with the cluster icon and the configured name of the cluster.



From now on, Config Sync configures the complete path **Setup > WLAN management** between all of the participating cluster members. Config Sync immediately synchronizes any configuration changes on any of the WLCs to all of the other WLCs in the cluster.

The master unit operates a master-CA, while all of the other WLCs operate a sub-CA of this master-CA. APs which connect to a WLC other than the master WLC will receive a valid certificate from it, if required.

4.5 Additions to the Status menu

4.5.1 Sync

This menu displays the status values of the automatic configuration synchronization.

SNMP ID:

1.11.51

Telnet path:

Status > Config

State

This entry shows the state of the device during the automatic configuration synchronization.

SNMP ID:

1.11.51.1

Telnet path:

Status > Config > Sync

Possible values:

Off
PKCS#12 file corrupt
TCP list failed
Not started yet
Incompatible firmware
Incompatible menu node
Own address wrong
No snapshot
Time unknown
OK

New cluster

This table shows you the values of the current automatic configuration synchronization.

SNMP ID:

1.11.51.2

Telnet path:**Status > Config > Sync****Name**

This entry shows the name of the current configuration synchronization.

SNMP ID:

1.11.51.2.1

Telnet path:**Status > Config > Sync > New Cluster****Cluster members**

This entry shows information about the group members of the cluster.

SNMP ID:

1.11.51.2.2

Telnet path:**Status > Config > Sync > New Cluster****ID**

This entry shows the ID of the entry.

SNMP ID:

1.11.51.2.2.2

Telnet path:**Status > Config > Sync > New Cluster > Group Members****Address**

This entry shows the address of the group member.

SNMP ID:

1.11.51.2.2.3

Telnet path:**Status > Config > Sync > New Cluster > Group Members**

This device

This entry indicates whether this is the device in question.

SNMP ID:

1.11.51.2.2.4

Telnet path:

Status > Config > Sync > New Cluster > Group Members

Possible values:

Yes

No

Menu nodes

This entry indicates the menu nodes that are included in the automatic configuration synchronization.

SNMP ID:

1.11.51.2.3

Telnet path:

Status > Config > Sync > New Cluster

ID

This entry shows the ID of the entry.

SNMP ID:

1.11.51.2.3.2

Telnet path:

Status > Config > Sync > New Cluster > Menu Nodes

Path

This entry shows the path of the menu node.

SNMP ID:

1.11.51.2.3.3

Telnet path:

Status > Config > Sync > New Cluster > Menu Nodes

SNMP OID

This entry shows the SNMP-ID of the menu node.

SNMP ID:

1.11.51.2.3.4

Telnet path:

Status > Config > Sync > New Cluster > Menu Nodes

Index columns

This entry shows the index column of the menu node.

SNMP ID:

1.11.51.2.3.5

Telnet path:

Status > Config > Sync > New Cluster > Menu Nodes

Ignored rows

This entry shows information about table rows that are excluded by the automatic configuration synchronization.

SNMP ID:

1.11.51.2.4

Telnet path:

Status > Config > Sync > New Cluster

ID

This entry shows the ID of the entry.

SNMP ID:

1.11.51.2.4.2

Telnet path:

Status > Config > Sync > New Cluster > Ignored Rows

Path

This entry shows the path of the table node.

SNMP ID:

1.11.51.2.4.3

Telnet path:**Status > Config > Sync > New Cluster > Ignored Rows****SNMP OID**

This entry shows the SNMP-ID of the table node.

SNMP ID:

1.11.51.2.4.4

Telnet path:**Status > Config > Sync > New Cluster > Ignored Rows****Index columns**

This entry indicates the table row that is excluded from the automatic configuration synchronization.

SNMP ID:

1.11.51.2.4.5

Telnet path:**Status > Config > Sync > New Cluster > Ignored Rows****State**

This entry shows the status of the automatic configuration synchronization.

SNMP ID:

1.11.51.2.5

Telnet path:**Status > Config > Sync > New Cluster**

Possible values:

Off
Invalid
Not running
Running
Changed

Info

This entry shows general information about the automatic configuration synchronization.

SNMP ID:

1.11.51.2.6

Telnet path:

Status > Config > Sync > New Cluster

Home

With this action, you distribute the device configuration to all other members of the group. At the same time, this launching time is the reference point for the group. From this time on, the cluster is considered to be activated.

SNMP ID:

1.11.51.2.7

Telnet path:

Status > Config > Sync > New Cluster

Cluster time

This entry shows the cluster time.

SNMP ID:

1.11.51.3

Telnet path:

Status > Config > Sync

Local configuration

This menu provides information about the local device configuration.

SNMP ID:

1.11.51.4

Telnet path:**Status > Config > Sync****Detected modifications**

This entry shows the changes that were detected.

SNMP ID:

1.11.51.4.1

Telnet path:**Status > Config > Sync > Local-config****Detected at**

This entry indicates the point in time when a change was made by another device.

SNMP ID:

1.11.51.4.1.2

Telnet path:**Status > Config > Sync > Local-config > Detected modifications****Path**

This entry shows the changed path.

SNMP ID:

1.11.51.4.1.4

Telnet path:**Status > Config > Sync > Local-config > Detected modifications****Type**

This entry shows the type of change.

SNMP ID:

1.11.51.4.1.5

Telnet path:**Status > Config > Sync > Local-config > Detected modifications****Possible values:****Set scalar**

The modification affected a value.

Set row

The modification added a table row.

Delete row

The modification removed a table row.

Value

This entry shows the changed value.

SNMP ID:

1.11.51.4.1.6

Telnet path:**Status > Config > Sync > Local-config > Detected modifications****Applied modifications**

This entry shows which configuration changes this device initiated.

SNMP ID:

1.11.51.4.2

Telnet path:**Status > Config > Sync > Local-config****Applied at**

This entry indicates the point in time when a change was made by this device.

SNMP ID:

1.11.51.4.2.2

Telnet path:**Status > Config > Sync > Local-config > Applied modifications**

Path

This entry shows the changed path.

SNMP ID:

1.11.51.4.2.4

Telnet path:

Status > Config > Sync > Local-config > Applied modifications

Type

This entry shows the type of change.

SNMP ID:

1.11.51.4.2.5

Telnet path:

Status > Config > Sync > Local-config > Applied modifications

Possible values:**Set scalar**

The modification affected a value.

Set row

The modification added a table row.

Delete row

The modification removed a table row.

Value

This entry shows the changed value.

SNMP ID:

1.11.51.4.2.6

Telnet path:

Status > Config > Sync > Local-config > Applied modifications

Result

This entry shows the result of the change.

SNMP ID:

1.11.51.4.2.7

Telnet path:

Status > Config > Sync > Local-config > Applied modifications

Possible values:**OK**

Configuration synchronization was successful.

OK(Msg-sent)**OK(End-of-line)****OK(Close)****OK(Abort)****OK(More)****OK(Started)**

Configuration synchronization was started.

No login**Syntax error****No path**

No path specified for the configuration synchronization.

Path unresolvable

Wrong path specified for the configuration synchronization.

Part ambiguous

The path in the configuration synchronization is ambiguous.

No menu stack**Not settable**

The configuration synchronization tried to set or modify a value, where this is not possible.

Value invalid

The configuration synchronization tried to set a value outside the valid range.

Read-only conn.

The connection to a device has no write permissions.

Action failed

The connection to a device has no execute permissions.

Table is full

The configuration synchronization tried to write another line in a full table.

Was ignored**Wrong password**

The login attempt to another device failed due to a wrong password.

Path name empty

The path to a configuration synchronization is specified without the value to be modified.

End-of-line**Running cluster**

This menu provides information about an ongoing cluster configuration synchronization.

SNMP ID:

1.11.51.5

Telnet path:**Status > Config > Sync****ID**

This entry shows the ID of the ongoing configuration synchronization.

SNMP ID:

1.11.51.5.1

Telnet path:**Status > Config > Sync > Running-Cluster****Name**

This entry shows the name of the ongoing configuration synchronization.

SNMP ID:

1.11.51.5.2

Telnet path:**Status > Config > Sync > Running-Cluster****Cluster members**

This table contains the groups members of the ongoing configuration synchronization.

SNMP ID:

1.11.51.5.3

Telnet path:**Status > Config > Sync > Running-Cluster****ID**

This entry shows the ID of the entry.

SNMP ID:

1.11.51.5.3.2

Telnet path:**Status > Config > Sync > Running-Cluster > Group-Members**

Address

This entry shows the address of the device.

SNMP ID:

1.11.51.5.3.3

Telnet path:

Status > Config > Sync > Running-Cluster > Group-Members

This device

This entry indicates whether this entry relates to this device.

SNMP ID:

1.11.51.5.3.4

Telnet path:

Status > Config > Sync > Running-Cluster > Group-Members

Possible values:

Yes
No

Menu nodes

This table contains the menu nodes of the ongoing configuration synchronization.

SNMP ID:

1.11.51.5.4

Telnet path:

Status > Config > Sync > Running-Cluster

ID

This entry shows the ID of this entry.

SNMP ID:

1.11.51.5.4.2

Telnet path:

Status > Config > Sync > Running-Cluster > Menu-Nodes

Path

This entry shows the path of the menu node.

SNMP ID:

1.11.51.5.4.3

Telnet path:

Status > Config > Sync > Running-Cluster > Menu-Nodes

SNMP OID

This entry shows the SNMP-ID of the menu node.

SNMP ID:

1.11.51.5.4.4

Telnet path:

Status > Config > Sync > Running-Cluster > Menu-Nodes

Index columns

This entry shows the index column of the menu node.

SNMP ID:

1.11.51.5.4.5

Telnet path:

Status > Config > Sync > Running-Cluster > Menu-Nodes

Ignored rows

This table contains the table rows ignored by the ongoing configuration synchronization.

SNMP ID:

1.11.51.5.5

Telnet path:

Status > Config > Sync > Running-Cluster

ID

This entry shows the ID of this entry.

SNMP ID:

1.11.51.5.2

Telnet path:**Status > Config > Sync > Running-Cluster > Ignored-Rows****Path**

This entry shows the path of the table node.

SNMP ID:

1.11.51.5.3

Telnet path:**Status > Config > Sync > Running-Cluster > Ignored-Rows****SNMP OID**

This entry shows the SNMP-ID of the table node.

SNMP ID:

1.11.51.5.4

Telnet path:**Status > Config > Sync > Running-Cluster > Ignored-Rows****Row index**

This entry indicates the table row that is excluded from the automatic configuration synchronization.

SNMP ID:

1.11.51.5.5

Telnet path:**Status > Config > Sync > Running-Cluster > Ignored-Rows****Config history**

This menu provides information about the configuration history of the device.

SNMP ID:

1.11.51.6

Telnet path:**Status > Config > Sync****Snapshot received at**

This entry indicates when the device received a snapshot.

SNMP ID:

1.11.51.6.1

Telnet path:**Status > Config > Sync > Config-History****Snapshot timestamp**

This entry contains the timestamp of the received snapshot.

SNMP ID:

1.11.51.6.2

Telnet path:**Status > Config > Sync > Config-History****Snapshot**

This table displays information about the last snapshot.

SNMP ID:

1.11.51.6.3

Telnet path:**Status > Config > Sync > Config-History****Path**

This entry contains the path to a menu node.

SNMP ID:

1.11.51.6.3.2

Telnet path:**Status > Config > Sync > Config-History > Snapshot**

Value

This entry contains the value of the corresponding path.

SNMP ID:

1.11.51.6.3.3

Telnet path:

Status > Config > Sync > Config-History > Snapshot

Modifications

This table contains the modifications to the configuration since the last snapshot.

SNMP ID:

1.11.51.6.4

Telnet path:

Status > Config > Sync > Config-History

Renew snapshot

Click this item to create a new snapshot of the current device configuration.

SNMP ID:

1.11.51.6.5

Telnet path:

Status > Config > Sync > Config-History

Replicas

This table contains information about the devices participating in the automatic configuration synchronization.

SNMP ID:

1.11.51.7

Telnet path:

Status > Config > Sync

ID

This entry contains the ID of the entry.

SNMP ID:

1.11.51.7.2

Telnet path:**Status > Config > Sync > Replicas****Address**

This entry contains the address of the device.

SNMP ID:

1.11.51.7.3

Telnet path:**Status > Config > Sync > Replicas****Resolved address**

This entry contains the resolved IPv4 or IPv6 address of the device.

SNMP ID:

1.11.51.7.4

Telnet path:**Status > Config > Sync > Replicas****Connection state**

This entry contains the state of the connection to the remote device.

SNMP ID:

1.11.51.7.5

Telnet path:**Status > Config > Sync > Replicas**

Possible values:

Not connected
DNS lookup
Connecting
OK
DNS lookup failure
TCP connect failure
TLS connect failure
Closed by replica
Incompatible firmware
Transfer error

State

This entry contains the state of the remote device.

SNMP ID:

1.11.51.7.6

Telnet path:

Status > Config > Sync > Replicas

Possible values:

Unknown
Missing messages
Missing updates
Old cluster
New cluster
No snapshot
Time unknown
OK

Cluster time

This entry contains the time of the configuration synchronization.

SNMP ID:

1.11.51.7.7

Telnet path:

Status > Config > Sync > Replicas

Last message received at

This entry indicates when the remote device received its last message.

SNMP ID:

1.11.51.7.8

Telnet path:**Status > Config > Sync > Replicas****Last update received at**

This entry indicates when the remote device received its last configuration update.

SNMP ID:

1.11.51.7.10

Telnet path:**Status > Config > Sync > Replicas****Last message sent at**

This entry indicates when the remote device sent its last message.

SNMP ID:

1.11.51.7.12

Telnet path:**Status > Config > Sync > Replicas**

4.6 Additions to the Setup menu

4.6.1 Config Sync

Indicates whether a config sync is possible (restricted) via this interface.

SNMP ID:

2.11.15.10

Telnet path:**Setup > Config > Access-Table****Possible values:****VPN**

Access is only possible via VPN.



VPN-capable devices only.

Yes

Access is generally possible.



By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.



Default setting for the WAN interface.

Default:

Yes

No

4.6.2 Sync

In this directory, you configure the automatic configuration synchronization.

SNMP ID:

2.11.51

Telnet path:

Setup > Config

Operating

Activates or deactivates the automatic configuration synchronization.

SNMP ID:

2.11.51.1

Telnet path:

Setup > Config > Sync

Possible values:

No

Yes

Default:

No

New cluster

Here you can configure the scope of a configuration synchronization.

SNMP ID:

2.11.51.2

Telnet path:

Setup > Config > Sync

Name

Enter an identifier for this entry.

SNMP ID:

2.11.51.2.1

Telnet path:

Setup > Config > Sync > New Cluster

Possible values:

Max. 254 characters from [A-Z][0-9]@{ }~!\$%&'()+-./:; <=>? [\] ^ _ .

Default:

Default

Cluster members

This table lists devices that participate in the automatic configuration synchronization.

SNMP ID:

2.11.51.2.2

Telnet path:

Setup > Config > Sync > New Cluster

Idx.

Index for this entry in the list.

SNMP ID:

2.11.51.2.2.1

Telnet path:

Setup > Config > Sync > New Cluster > Group Members

Possible values:

Max. 5 characters from 0123456789

Default:

empty

Address

IP address of the corresponding device.

SNMP ID:

2.11.51.2.2.2

Telnet path:

Setup > Config > Sync > New Cluster > Group Members

Possible values:

Max. 63 characters from [A-Z][0-9]@{ | }~!\$%&'()+- , / : ; < = > ? [\] ^ _ .

Possible arguments:

IPv4 address

IPv6 address

Default:

empty

Menu nodes

Here you configure which configuration items are to be contained in the automatic configuration synchronization. This enables you to include or exclude values, tables, and entire menus.

SNMP ID:

2.11.51.2.3

Telnet path:

Setup > Config > Sync > New Cluster

Idx.

Index for this entry in the list.

SNMP ID:

2.11.51.2.3.1

Telnet path:

Setup > Config > Sync > New Cluster > Menu Nodes

Possible values:

Max. 5 characters from 0123456789

Default:

empty

Include

Specify here whether the specified menu node is included in or excluded from the automatic configuration synchronization.

SNMP ID:

2.11.51.2.3.2

Telnet path:

Setup > Config > Sync > New Cluster > Menu Nodes

Possible values:

Include
Exclude

Default:

Include

Path

Enter the path to the menu node. This can be a value, a table, or a complete menu.

SNMP ID:

2.11.51.2.3.3

Telnet path:

Setup > Config > Sync > New Cluster > Menu Nodes

Possible values:

Max. 127 characters from [A-Z][a-z][0-9]@{ }~!\$%&'()+-./:;<=>?[\]^_`

Default:

/Setup

SNMP OID

Show the SNMP-ID of the specified menu node.



The display is updated after you save the entry.

SNMP ID:

2.11.51.2.3.4

Telnet path:**Setup > Config > Sync > New Cluster > Menu Nodes****Possible values:**

2

Default:

2

Ignored rows

If you include a table into the automatic configuration synchronization, this item is used to determine which rows of this table are to be excluded from it.

SNMP ID:

2.11.51.2.4

Telnet path:**Setup > Config > Sync > New Cluster****Idx.**

Index for this entry in the list.

SNMP ID:

2.11.51.2.4.1

Telnet path:**Setup > Config > Sync > New Cluster > Ignored Rows****Possible values:**

Max. 5 characters from 0123456789

Default:*empty***Row index**

Here you specify the row number (index) to be excluded from the automatic configuration synchronization.

SNMP ID:

2.11.51.2.4.2

Telnet path:**Setup > Config > Sync > New Cluster > Ignored Rows****Possible values:**

Max. 127 characters from [A-Z][a-z][0-9]#{|}~!"\$%&'()*+,-./:;<=>?[\]^_`~

Default:*empty***Path**

Specify the path to the node of the table that is contained in the automatic configuration synchronization.

SNMP ID:

2.11.51.2.4.3

Telnet path:**Setup > Config > Sync > New Cluster > Ignored Rows****Possible values:**

Max. 127 characters from [A-Z][a-z][0-9]@{|}~!"\$%&'()*+,-./:;<=>?[\]^_`~

Default:*/Setup***SNMP OID**

Show the SNMP-ID of the specified table node.



The display is updated after you save the entry.

SNMP ID:

2.11.51.2.4.4

Telnet path:**Setup > Config > Sync > New Cluster > Ignored Rows****Possible values:**

2

Default:

2

Home

Starts the automatic configuration synchronization for this entry.

SNMP ID:

2.11.51.2.5

Telnet path:

Setup > Config > Sync > New Cluster

TLS connections

In this directory, you specify the address and port to be used by the device to accept incoming configuration changes.

SNMP ID:

2.11.51.3

Telnet path:

Setup > Config > Sync

Port

Specify the port to be used by the device to receive incoming configuration changes.

SNMP ID:

2.11.51.3.1

Telnet path:

Setup > Config > Sync > TLS-Connections

Possible values:

Max. 5 characters from [0–9]

0 ... 65535

Default:

1941

Loopback address

Specify the loopback address to be used by the device to receive incoming configuration changes.

SNMP ID:

2.11.51.3.2

Telnet path:

Setup > Config > Sync > TLS-Connections

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9].-: %`

Possible arguments:

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

LBO ... LBF for the 16 loopback addresses

Any valid IPv4 or IPv6 address

Default:

empty

Renew snapshot

In this directory you configure the snapshots.

SNMP ID:

2.11.51.4

Telnet path:

Setup > Config > Sync > Renew-Snapshot

Modification limit

Enter the modification limit here.

SNMP ID:

2.11.51.4.1

Telnet path:

Setup > Config > Sync > Renew-Snapshot

Possible values:

Max. 10 characters from `0123456789`

Special values:

0

This value disables the function.

Default:

2048

Kept modifications

This value specifies the number of kept modifications.

SNMP ID:

2.11.51.4.2

Telnet path:**Setup > Config > Sync > Renew-Snapshot****Possible values:**

Max. 10 characters from 0123456789

0 ... 4294967295 Powers of two

Special values:

0

This value disables the function.

Default:

256

Renew snapshot

This action renews the snapshot.

SNMP ID:

2.11.51.4.3

Telnet path:**Setup > Config > Sync > Renew-Snapshot****Local configuration**

In this directory you specify the number of applied and detected modifications.

SNMP ID:

2.11.51.5

Telnet path:**Setup > Config > Sync > Local Config****Detected modifications**

Specify the number of detected modifications.

SNMP ID:

2.11.51.5.1

Telnet path:**Setup > Config > Sync > Local Config**

Possible values:

Max. 10 characters from 0123456789

Applied modifications

Specify the number of applied modifications.

SNMP ID:

2.11.51.5.2

Telnet path:

Setup > Config > Sync > Local Config

Possible values:

Max. 10 characters from 0123456789

5 Configuration

5.1 TR-069 support

As of LCOS version 9.10, our routers support certain features of the TR-069 (CWMP) specification for automated provisioning and the securely encrypted remote management of routers, for example in provider environments.

5.1.1 CPE WAN Management Protocol (CWMP)

The CPE WAN Management Protocol (CWMP) enables devices to be remotely configured via a WAN link. Communication between the device (customer premises equipment, CPE) and the configuration server (auto configuration server, ACS) is conducted via SOAP/HTTP(S) in the form of remote procedure calls (RPC). A large number of RPCs are specified for the CWMP, the following of which are implemented in LCOS:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- GetParameterNames
- FactoryReset
- Reboot
- Download
 - Firmware-Update
 - Script download (*.lcs files)

LCOS additionally supports the manufacturer-specific RPC:

- X_LANCOM_DE_Command



To find more information about the parameters of the RPC, visit the [Broadband Forum](#).

The CPE supports the following types of authentication at an ACS:

- HTTP Basic
- HTTP Digest
- HTTPS by client certificate

Setting up CWMP with LANconfig

In LANconfig, the CPE WAN Management Protocol is configured under **Management > CWMP**.

CWMP activated

Enables or disables CWMP.

ACS URL

Here you enter the address of the ACS (auto configuration server) which the CPE (customer premises equipment) connects to. The address is entered in the IPv4, IPv6, or FQDN format.

HTTP and HTTPS are permitted, although the use of HTTPS is preferred. Otherwise the devices transmit device-specific parameters, such as passwords or access data, unencrypted. Before you can use HTTPS, the trusted root certificate for verifying the server identity needs to be uploaded to the device.

ACS username

Enter a user name for the device to use when connecting with the ACS (auto configuration server).

ACS password

Enter a password for the device to use when connecting with the ACS (auto configuration server).

Remote administrator

Select one of the configured device administrators to be used by the ACS (auto configuration server) when connecting to this device. The name you select must be an enabled device administrator with appropriate privileges, i.e. root access to change the firmware.

Source address

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address. If you have configured loopback addresses, you can specify them here as source address.



If the source address set here is a loopback address, then the device will use this unmasked even for remote stations that are masked.

The device accepts addresses in various input formats:

- Name of the IP network (ARF network), 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", then the device takes its address).
- LB0 ... LBF for one of the 16 loopback addresses or its name

- Any IP address in the form x.x.x.x.

Periodic inform activated

Enables or disables the sending of periodic inform messages from the device to the ACS (auto configuration server).

Periodic inform interval

This is the interval in seconds between two periodic inform messages sent by the device to the ACS (auto configuration server). The ACS then requests further information from the device.

The default value is 1200 seconds (20 minutes). Do not set a value that is too small, as inform messages increase network load. The interval does not commence before the device and server have exchanged all of the necessary information.

Allow file transmission

This switch allows you to transfer a firmware or a script file from the ACS (auto configuration server) to this device.

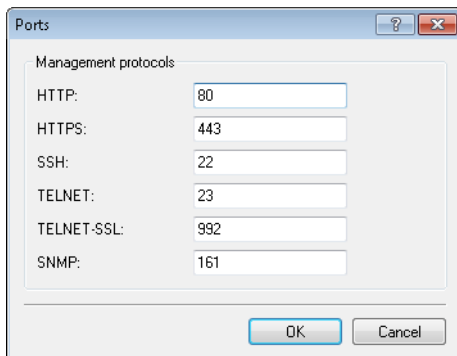
Manage firmware updates

This switch allows the ACS (auto configuration server) to make firmware modifications to the device.

Allow changing of the username

This switch allows the ACS (auto configuration server) to change the device administrator or to change the name and password of the device administrator used to connect to the device.

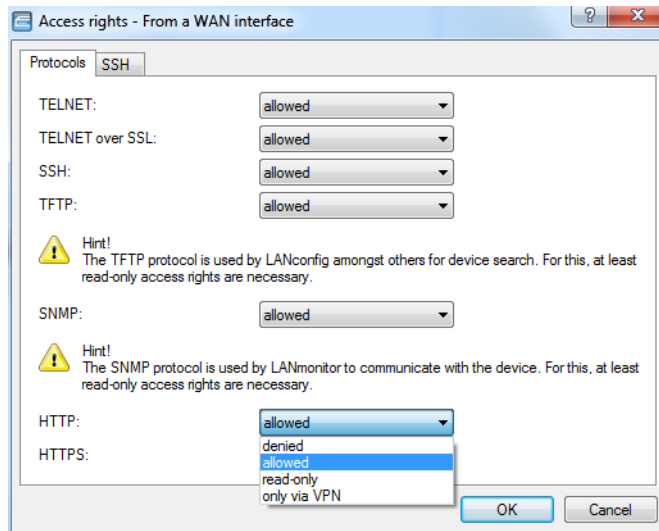
In the default setting, the connection request URL uses HTTP port 80. You configure this in LANconfig under **Management > Admin** in the section **Management protocols** under **Ports**.



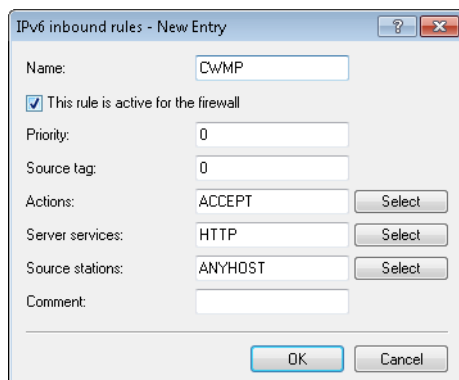
Management protocols	
HTTP:	80
HTTPS:	443
SSH:	22
TELNET:	23
TELNET-SSL:	992
SNMP:	161

OK Cancel

In order for an ACS to request the device to connect, it must be possible to access the corresponding HTTP port via the WAN or VPN. This requires that access either via WAN or VPN is allowed in LANconfig under **Management > Admin** in the section **Configuration access ways** under **Access rights > From a WAN interface**.



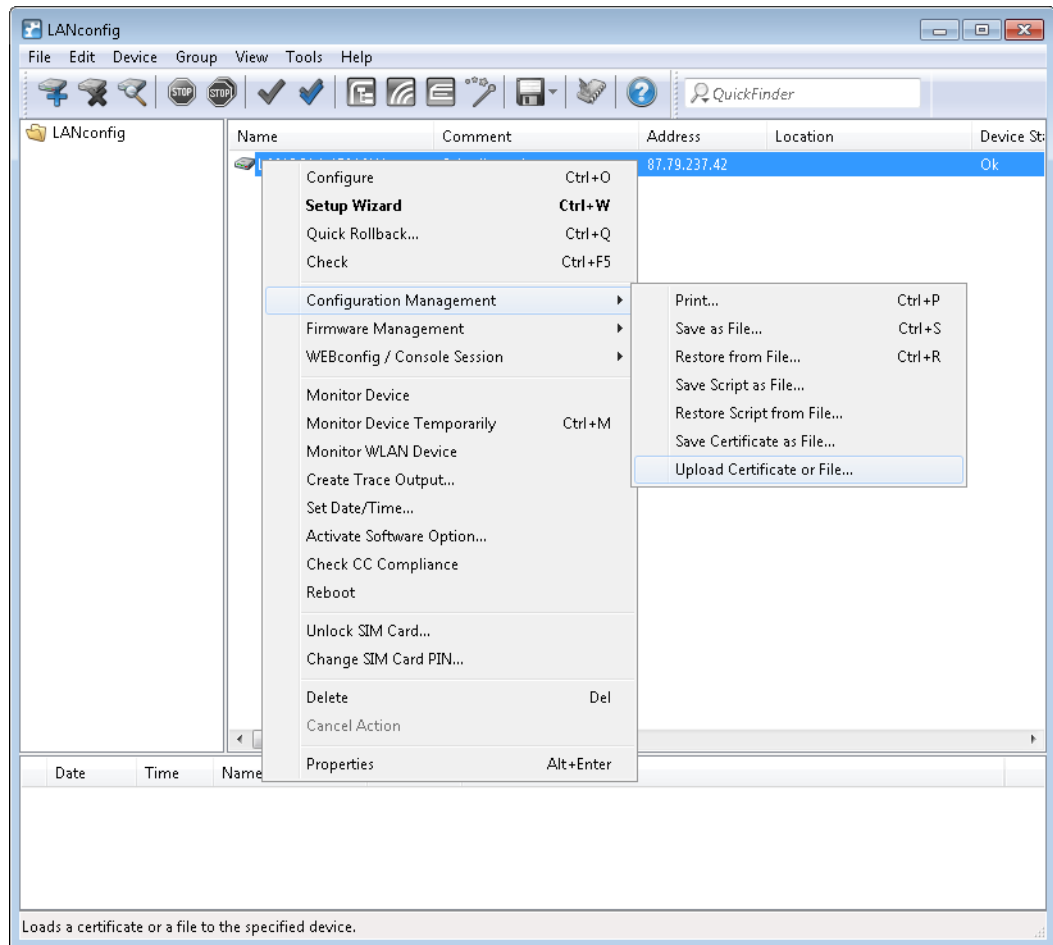
If you use IPv6, you additionally need to set the IPv6 firewall to allow access to the corresponding port under **Firewall/QoS > IPv6 rules > IPv6 inbound rules**.



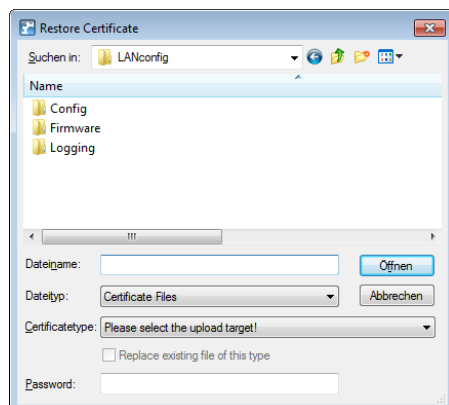
i The connection request is only possible with authentication by means of user name and password.

If HTTPS is used in the ACS URL, the CPE validates the ACS certificate. To this end, you first have to save the CWMP root CA certificate on the CPE. If the CPE is unable to validate the server certificate against the existing root CA certificate, it rejects the connection. The certificate is uploaded either by LANconfig or WEBconfig. In LANconfig you do this as follows:

1. In the device view section, right-click on the corresponding device and, under **Configuration management**, select the item **Upload certificate or file**.



2. In the dialog that follows, set the certificate type to "CWMP root CA certificate" and click **Open**.




When using SSL/TLS for authentication at the CPE, you upload the client certificate and the private key by means of PKCS#12 file (CWMP container as PKCS#12 file) onto the CPE.

Device configuration via CWMP

All CWMP parameters are configured on the command line either by a script file or by the manufacturer-specific RPC `X_LANCOM_DE_Command`.

Configuration via script

The CWMP download command `<cwmp:download>` is used to configure the device by means of a script file (*.lcs). The file type is 3 Vendor Configuration File. The URL is the address of the server where the configuration script is stored.

 LANconfig files of the *.lcf format are not supported.

Configuration by means of manufacturer-specific RPC `X_LANCOM_DE_Command`

The `X_LANCOM_DE_Command` function is defined as follows:

Request

```
<cwmp:X_LANCOM_DE_Command>
<Command> CLI-Kommando </Command>
</cwmp:X_LANCOM_DE_Command>
```

Response

```
<cwmp:X_LANCOM_DE_CommandResponse>
<Status>1</Status>
<Result>1</Result>
</cwmp:X_LANCOM_DE_CommandResponse>
```

The following example sets the IPv4 address of the device to the "INTRANET":

```
<cwmp:X_LANCOM_DE_Command>
<Command>set /Setup/TCP-IP/Network-list/INTRANET {IP-address} 192.168.80.1</Command>
</cwmp:X_LANCOM_DE_Command>
```

Due to the asynchronous execution of the console commands, the `X_LANCOM_DE_Command` always reports a successful execution of the command, regardless of whether the command was executed correctly or not. A successful execution requires the config status to be read out under **Status > Config**.

To check the configuration status, you can read out the following CWMP parameters before or after using the script or `X_LANCOM_DE_Command`:

- InternetGatewayDevice.DeviceInfo.X_LANCOM_DE_ConfigVersion
- InternetGatewayDevice.DeviceInfo.X_LANCOM_DE_LastScriptComment
- InternetGatewayDevice.DeviceInfo.X_LANCOM_DE_LastScriptErrorLine
- InternetGatewayDevice.DeviceInfo.X_LANCOM_DE_LastScriptSuccessful

 The values correspond to the status values under **Status > Config**.

5.1.2 Additions to the Setup menu

CWMP

The CPE WAN Management Protocol (CWMP) enables devices to be remotely configured via a WAN link. Communication between the device (customer premises equipment, CPE) and the configuration server (auto configuration server, ACS) is conducted via SOAP/HTTP(S) in the form of remote procedure calls (RPC).

SNMP ID:

2.44

Telnet path:

Setup

NTP server

This directory displays the NTP server for time synchronization as configured by the CWMP.

SNMP ID:

2.44.1

Telnet path:

Setup > CWMP

NTP-Server-1

Displays the first NTP server.

SNMP ID:

2.44.1.1

Telnet path:

Setup > CWMP > NTP-Server

NTP-Server-2

Displays the second NTP server.

SNMP ID:

2.44.1.2

Telnet path:

Setup > CWMP > NTP-Server

NTP-Server-3

Displays the third NTP server.

SNMP ID:

2.44.1.3

Telnet path:

Setup > CWMP > NTP-Server

NTP-Server-4

Displays the fourth NTP server.

SNMP ID:

2.44.1.4

Telnet path:**Setup > CWMP > NTP-Server****NTP-Server-5**

Displays the fifth NTP server.

SNMP ID:

2.44.1.5

Telnet path:**Setup > CWMP > NTP-Server****Operating**

Enables or disables CWMP.

SNMP ID:

2.44.2

Telnet path:**Setup > CWMP****Possible values:****No**
Yes**Default:**

No

Allow file download

This switch allows you to transfer a firmware or a script file from the ACS (auto configuration server) to this device.

SNMP ID:

2.44.3

Telnet path:**Setup > CWMP**

Possible values:

No
Yes

Default:

No

Inform retry limit

Here you specify how many times the CPE attempts to deliver an inform message to the ACS after a failure.

SNMP ID:

2.44.4

Telnet path:

Setup > CWMP

Possible values:

Max. 10 characters from 0123456789

Default:

10

Special values:

0
Retry disabled

Source address

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address. If you have configured loopback addresses, you can specify them here as source address.



If the source address set here is a loopback address, then the device will use this unmasked even for remote stations that are masked.

SNMP ID:

2.44.5

Telnet path:

Setup > CWMP

Possible values:

Max. 16 characters from [A-Z][a-z][0-9]@{ }~!\$%&'()+-,/:;=>?[\\]^_`~

Special values:

Name of the IP network (ARF network), 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", then the device takes its address).

LB0 ... LBF for one of the 16 loopback addresses or its name

Any IP address in the form x.x.x.x.

Default:

empty

ACS URL

Here you enter the address of the ACS (auto configuration server) which the device connects to. The address is entered in the IPv4, IPv6, or FQDN format.

SNMP ID:

2.44.6

Telnet path:

Setup > CWMP

Possible values:

Max. 255 characters from [A-Z][a-z][0-9]@{ }~!\$%&'()+-./:;<=>?[\]^_`~

Default:

empty

ACS username

Enter a user name for the device to use when connecting with the ACS (auto configuration server).

SNMP ID:

2.44.7

Telnet path:

Setup > CWMP

Possible values:

Max. 255 characters from [A-Z][a-z][0-9]@{ }~!\$%&'()+-./:;<=>?[\]^_`~

Default:

empty

ACS password

Enter a password for the device to use when connecting with the ACS (auto configuration server).

SNMP ID:

2.44.8

Telnet path:**Setup > CWMP****Possible values:**

Max. 255 characters from [A-Z][a-z][0-9]@{ }~!\$%&'()+-./:;<=>?[\]^_`

Default:*empty***Periodic inform activated**

Enables or disables the sending of periodic inform messages from the device to the ACS (auto configuration server).

SNMP ID:

2.44.9

Telnet path:**Setup > CWMP****Possible values:****No**
Yes**Default:**

No

Periodic inform interval

This is the interval in seconds between two periodic inform messages sent by the device to the ACS (auto configuration server). The ACS then requests further information from the device.

The default value is 1200 seconds (20 minutes). Do not set a value that is too small, as inform messages increase network load. The interval does not commence before the device and server have exchanged all of the necessary information.

SNMP ID:

2.44.10

Telnet path:**Setup > CWMP****Possible values:**

Max. 10 characters from 0123456789

Default:

1200

Special values:

0

Periodic-Inform disabled

Periodic inform time

Specify the periodic inform time. This entry in the "dateTime" format contains the time for the first inform message.

Example: 0001-02-03T03:04:05+06:00.

SNMP ID:

2.44.11

Telnet path:**Setup > CWMP****Possible values:**

Max. 63 characters from [A-Z][a-z][0-9]@{ | } ~ ! \$ % & ' () + - , / : ; < = > ? [\] ^ _ . `

Default:*empty***Connection request username**

Select one of the configured device administrators to be used by the ACS (auto configuration server) when connecting to this device. The name you select must be an enabled device administrator with appropriate privileges, i.e. root access to change the firmware.

SNMP ID:

2.44.12

Telnet path:**Setup > CWMP****Possible values:**

Max. 255 characters from [A-Z][a-z][0-9]@{ | } ~ ! \$ % & ' () + - , / : ; < = > ? [\] ^ _ . `

Default:*empty***Updates managed**

This switch allows the ACS (auto configuration server) to make firmware modifications to the device.

SNMP ID:

2.44.13

Telnet path:**Setup > CWMP****Possible values:****No****Yes****Default:**

No

Allow user change

This switch allows the ACS (auto configuration server) to change the device administrator or to change the name of the device administrator that it uses to connect to the device.

SNMP ID:

2.44.14

Telnet path:**Setup > CWMP****Possible values:****No****Yes****Default:**

No

Provisioning code

Displays the ACS provisioning code.

SNMP ID:

2.44.15

Telnet path:**Setup > CWMP**

Parameter key

Displays the parameter key.

The ACS uses the parameter key to maintain an overview of its changes.

SNMP ID:

2.44.16

Telnet path:

Setup > CWMP

Command-Key

Displays the command key of the ACS.

SNMP ID:

2.44.17

Telnet path:

Setup > CWMP

5.1.3 Additions to the Status menu

CWMP

This menu shows you certain features of the TR-069 (CWMP) specification.

SNMP ID:

1.85

Telnet path:

Status > CWMP

Operating

This menu shows you whether CWMP is activated.

SNMP ID:

1.85.1

Telnet path:

Status > CWMP

Possible values:

Yes
No

Allow file download

This menu shows you whether the device is allowed to download firmware or script files from an external server.

SNMP ID:

1.85.2

Telnet path:

Status > CWMP

Possible values:

Yes
No

Provisioning code

This entry shows the provisioning code as configured by the provider.

SNMP ID:

1.85.3

Telnet path:

Status > CWMP

Parameter key

Shows the CWMP parameter key.

SNMP ID:

1.85.4

Telnet path:

Status > CWMP

Command-Key

Shows the CWMP command key.

SNMP ID:

1.85.5

Telnet path:**Status > CWMP****NTP-Server-1**

This entry shows you the first NTP server for time synchronization.

SNMP ID:

1.85.6

Telnet path:**Status > CWMP****NTP-Server-2**

This entry shows you the second NTP server for time synchronization.

SNMP ID:

1.85.7

Telnet path:**Status > CWMP****NTP-Server-3**

This entry shows you the third NTP server for time synchronization.

SNMP ID:

1.85.8

Telnet path:**Status > CWMP****NTP-Server-4**

This entry shows you the fourth NTP server for time synchronization.

SNMP ID:

1.85.9

Telnet path:**Status > CWMP****NTP-Server-5**

This entry shows you the fifth NTP server for time synchronization.

SNMP ID:

1.85.10

Telnet path:**Status > CWMP****Allow user change**

This entry indicates whether the ACS is allowed to change the local administrator (applies for user name and password).

SNMP ID:

1.85.11

Telnet path:**Status > CWMP****Possible values:**

Yes

No

5.2 Encrypted storage of configurations with LANconfig

As of LCOS version 9.10, it is possible to encrypt configuration and script files and to give them a checksum. Configuration files can be given password protection for encryption and secure storage with LANconfig, so preventing any unauthorized access to configurations.

Table 5: Overview of all commands available at the command line

Command	Description
<code>readconfig [-h] [-s <password>]</code>	<p>Shows the complete configuration in the format of the device syntax.</p> <ul style="list-style-type: none">■ <code>-h</code>: Adds a checksum to the configuration file.■ <code>-s <password></code>: Encrypts the configuration file with the use of the specified password. <p>Access rights: Supervisor-Read</p>


Command	Description
<code>readscript [-n] [-d] [-i] [-c] [-m] [-h] [-s <password>]</code>	<p>The <code>readscript</code> command generates a text dump of all commands and parameters required to configure the device in its current state. You can use the following option switches for this:</p> <ul style="list-style-type: none"> ■ <code>-n</code>: The text output is only numerical without identifiers. The output only contains the current status values of the configuration as well as the associated SNMP IDs. ■ <code>-d</code>: The default values are included in the text output. ■ <code>-i</code>: The table designations are included in the text output. ■ <code>-c</code>: Includes any comments contained in the script file. ■ <code>-m</code>: The text is output to the screen in a compact but difficult to read format (no indentations). ■ <code>-h</code>: Adds a checksum to the script file. ■ <code>-s <password></code>: Encrypts the script file with the use of the specified password. <p>Access rights: Supervisor-Read</p>

5.2.1 Saving and loading device-configuration and script files


A device configuration file contains all of its settings. Script files are useful for managing the settings of a device automatically. To protect of these files against unauthorized access or transmission errors, it is possible to export them from or upload them to the device in an encrypted state and with a checksum.


There are three different file types:

- No checksum, no encryption: A text file with content readable by a text editor.
- Checksum: The text file contains information about the checksum and the hash algorithm for calculating this checksum. The contents of this text file is readable with a simple text editor.

 LANconfig prior to version 9.10 recognizes files with checksums.

- Encryption: Before the file is exported it is encrypted by the device using a password chosen by the administrator. The text file contains information about the encryption algorithm used, as well as a checksum. The contents of the text file is no longer decipherable by a text editor, with the exception of the file header.

 LANconfig prior to version 9.10 cannot read encrypted files.

 The file extensions of these files are `.lcf` for configuration files or `.lcs` for script files. The detection of a file that is encrypted and/or contains a checksum relies exclusively on the file header.

Configuration management with WEBconfig and the console

To export a configuration file from WEBconfig, navigate to the view **File management > Save configuration**.

Save Configuration

☐ Include checksum

Password:

Password (Repeat):

The following options are available:

No entries

By default, all options are disabled. A click on **Download** invokes the dialog for downloading an unencrypted configuration file without a checksum.

Include checksum

A click on **Download** invokes the dialog for downloading an unencrypted configuration file with a checksum.

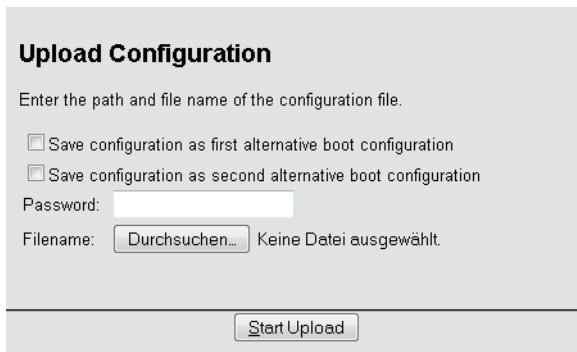
Password

Specify a password if you want to encrypt the configuration file before downloading it.

To save the configuration from the console, use the following parameters:

- `readconfig`: Backs up the configuration without checksum and encryption.
- `readconfig -h`: Adds a checksum to the configuration file.
- `readconfig -s <password>`: Encrypts the configuration file with the use of the specified password.

To upload a configuration file with WEBconfig, navigate to the view **File management > Upload configuration**.



If the configuration file is encrypted, enter the appropriate password and click on **Start upload**.



For more information about alternate boot configurations, see the chapter [Alternative boot config](#).

Script management with WEBconfig and the console

To export a script file from WEBconfig, navigate to the view **File management > Save configuration script**.

The following options are available:

Parameters

By default, all options are disabled. A click on **Download** invokes the dialog for downloading an unencrypted script file without a checksum.

Password

Specify a password if you want to encrypt the script file before downloading it.

To save the script file from the console, the following parameters are available:

- `readscript`: Backs up the configuration without checksum and encryption.
- `readscript -h`: Adds a checksum to the configuration file.
- `readscript -s <password>`: Encrypts the configuration file with the use of the specified password.



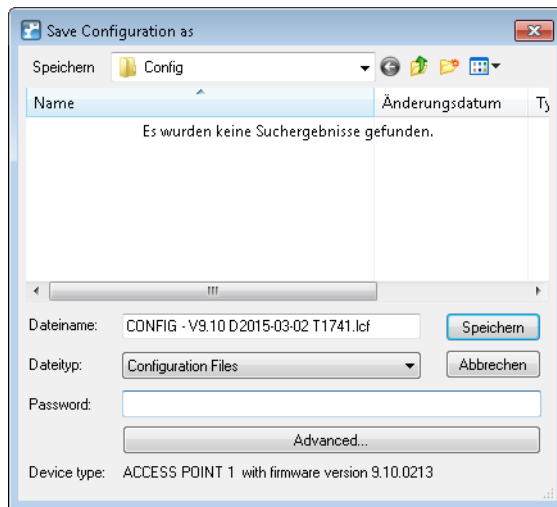
More information about the parameters, see the chapter [Commands for the console](#) in the section about `readscript`.

To upload a script file with WEBconfig, navigate to the view **File management > Execute configuration script**.

If the script file is encrypted, enter the appropriate password and click on **Start upload**.

Configuration management with LANconfig

You can use LANconfig to save a configuration file by right-clicking on the corresponding device in the list of devices. From the context dialog, open the save dialog under **Configuration management > Save as file**.



The following entries are available:

File name

LANconfig composes the file name from various pieces of information (including version number, date and time). Change the name to suit your needs.

File type

Choose whether this is a configuration file or something else.

Password

Specify a password if you want to encrypt the configuration file before downloading it.

Under **Advanced** you can set optional parameters that are processed by the device when a configuration file is loaded automatically (auto-load). Use this to customize the configuration.

You can use LANconfig to upload a configuration file to the device by right-clicking on the device where the configuration is to be uploaded. From the context dialog, open the restore dialog under **Configuration management > Restore from file**.

Select the required configuration file, enter the password (if applicable) and click **Open** to upload the configuration to the device.

5.2.2 Additions to the Status menu

Script log

This table provides an overview of the executed scripts.

SNMP ID:

1.11.23

Telnet path:

Status > Config

Index

Shows the index of this entry.

SNMP ID:

1.11.23.1

Telnet path:

Status > Config > Script-Log

Time

Shows the time of this entry.

SNMP ID:

1.11.23.2

Telnet path:

Status > Config > Script-Log

Comment

Shows the comment for this entry.

SNMP ID:

1.11.23.3

Telnet path:

Status > Config > Script-Log

Successful

Shows whether the script was successfully completed.

SNMP ID:

1.11.23.4

Telnet path:

Status > Config > Script-Log

Error line

In the event of an error, this shows which line of the script caused the abort.

SNMP ID:

1.11.23.5

Telnet path:**Status > Config > Script-Log**

5.3 Each device has its own SSL key & changes to the default SSL settings

As of LCOS version 9.10, after a configuration reset each device generates its own SSL RSA key of 2048-bit length.

Further, "RC4-128" is no longer set as the default for HTTPS connections.


5.3.1 Automatic generation of device-specific SSH/SSL keys

If you have a device with LCOS 8.84 or higher and you have not loaded an individual key into the device, then resetting the configuration will prompt the internal SSH server to try and compile its own device-specific SSH keys directly at the system startup. These include:

- an SSH-2-RSA key with 2048 bit length;
- an SSH-2-DSS key with 1024 bit length (as per FIPS 186-2);
- an SSH-2-ECDSA key with 256, 384 or 521 bit length;
- an SSL-RSA key with 2048 bit length;

which the device stores in its internal file system as `ssh_rsakey`, `ssh_dsakey`, `ssl_privkey` or `ssh_ecdsakey`.

If key generation is successful, the entry `SSH ... host key generated` is entered into the SYSLOG as a "notice"; If it fails, the entry `SSH: host key generation failed, try later again with '...'` is entered as an "alert". The failure to generate a key, for example if there is too little entropy, causes the system to revert to the factory implemented cryptographic key.

 When you an update from an older LCOS version to 8.84 or higher without subsequently doing a configuration reset, the device does not generate a device-specific SSH/SSL key. This maintains compatibility with existing installations. However, you can trigger the key generation manually. Enter the following commands in the console:

```
sshkeygen -t rsa -b 2048 -f ssh_rsakey
sshkeygen -t dsa -b 1024 -f ssh_dsakey
sshkeygen -t ecdsa -b 256 -f ssh_ecdsakey
sshkeygen -t rsa -b 2048 -f ssl_privkey
```

5.3.2 Manually create custom SSH keys

You have the option to replace the factory installed and automatically generated SSH/SSL keys with your own RSA, DSA or DSS keys, in order to achieve stronger encryption. A number of alternatives are available here:

- You can generate the individual keys on the console using LCOS.
- Using an external program, you can create an OpenSSH private key and then upload this key to the device as `SSH-DSS-key [...]` or `SSH-RSA key (*.key [BASE64 unencrypted])`.

The use of an external program is an option if your device has insufficient entropy, so causing key creation with LCOS to fail.

SSH key generation with LCOS

To generate a key pair consisting of a public and a private key, you enter the following command at the console:

```
sshkeygen [-?|-h] [-t (dsa|rsa|ecdsa)] [-b <Bits>] -f <OutputFile> [-q]
```

-?, -h

Displays a brief help text about the available parameters

-t (dsa|rsa|ecdsa)

This parameter specifies what type of key is generated. SSH supports the following types of keys:

- 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.
- DSA keys follow the Digital Signature Standard (DSS) 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). DSA or DSS keys are always 1024 bits long, but they are slower to process than a corresponding RSA key.
- ECDSA keys are a variant of DSA keys, whereby the device uses elliptic curves for key generation (elliptic curve cryptography, ECC). ECC is an alternative to the conventional signature and key exchange techniques such as RSA and Diffie-Hellman. The main advantage of elliptic curves is that their mathematical properties offer the same key strength as RSA or Diffie-Hellman but with a significantly shorter key length. This provides for better hardware performance. ECC and its integration in SSL and TLS are described in RFCs 5656 and 4492.

If no type is specified, the command generates an RSA key by default.

-b <bits>

This parameter sets the length of the RSA key in bits. If you do not specify a length, the command produces a key with a length of 1024 bits by default.

-f <OutputFile>

These parameters specify the mounting point of the generated key file in the device file system. The choice of mounting point depends on what type key you are generating. The choices available to you are:

- `ssh_rsakey` for RSA keys
- `ssh_dsakey` for DSA keys
- `ssh_ecdsakey` for ECDSA keys
- `ssl_privkey` for SSL-RSA keys

-q

This parameter enables the 'quiet' mode for the key generation. If you set this parameter, LCOS overwrites any existing RSA or DSA keys without asking; there is no information about the progress of the operation. You can, for example, use this parameter in a script to suppress any security prompts for the users.

SSH key generation with Linux systems

Many Linux distributions already feature the OpenSSH package. All you have to do to generate the key file is to enter a simple command into the shell. The syntax corresponds to the LCOS command `sshkeygen`:

```
ssh-keygen [-t (dsa|rsa)] [-b <Bits>] [-f <OutputFile>]
```

The command `ssh-keygen -t rsa -b 4096 -f hostkey` creates an RSA key of 4096 bits in length, which consists of the private component 'hostkey' and the public component 'hostkey.pub'.

SSH key generation with Windows systems

Windows systems are not inherently capable of compiling SSH keys. You should instead use a suitable utility program such as the free software PuTTYgen.

A guide on how to create an individual key with PuTTYgen is available in the section [Generating an SSH keypair with PuTTY](#). After following the various steps to generate the key, do **not** use the buttons **Save public key** and **Save private key**, but instead choose **Conversions > Export OpenSSH key**. The resulting OpenSSH private key can then be uploaded into the device without further processing.

5.3.3 Additions to the Setup menu

Crypto algorithms

This bitmask specifies which cryptographic algorithms are allowed.

SNMP ID:

2.21.40.5

Telnet path:

Setup > HTTP > SSL

Possible values:

**RC4-40
RC4-56
RC4-128
DES40
DES
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256**

Default:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

6 Diagnosis

6.1 Advanced config version information under Status

As of LCOS version 9.10, you will find additional information about your current configuration (date, hash, version) in WEBconfig and via the console under **Status > Config**.

6.1.1 Additions to the Status menu

Configuration date

This entry indicates when you last changed the configuration of the device.



The time is displayed in UTC format.

SNMP ID:

1.11.20

Telnet path:

Status > Config

Configuration hash

This entry shows you the hash value of the current configuration.



The displayed value is a SHA1 hash.

SNMP ID:

1.11.21

Telnet path:

Status > Config

Configuration version

This entry shows you the current version of the device configuration.

SNMP ID:

1.11.22

Telnet path:

Status > Config

6.2 SSH identifier in the event log

As of LCOS version 9.10, the device displays the SSH identifier in the event log for connections encrypted by SSH.

6.2.1 Additions to the Status menu

Event log

This log table is an overview of all of the logged event messages that affect the configuration of the device, such as failed logins or firmware update history.

SNMP ID:

1.11.12

Telnet path:

Status > Config

Possible values:

Idx.

Index number of the event

System time

Time of the event

Event

Event message in abbreviated form

Access

Access protocol used, e.g. SSH or HTTPS

IP address

IP address that was used to access the device

Info1

Event code

Info2

Description of the event code

Info3

SSH identifier

7 LCMS

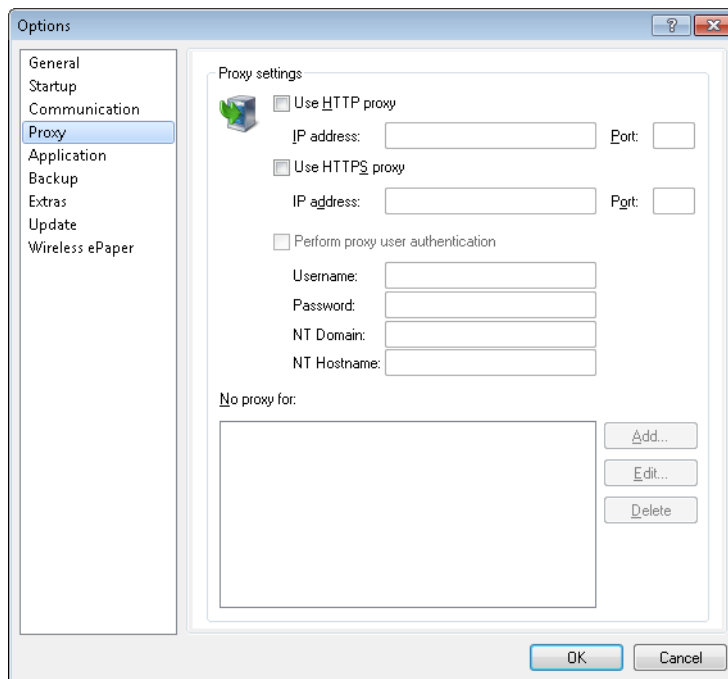
7.1 Proxy authentication via NTLM

As of LCOS version 9.10, proxy authentication of LANconfig via NT LAN Manager (NTLM) is now possible.

7.1.1 Proxy

If you wish to use a proxy server for access to your device, you can configure this here. Activate the required protocol and enter the address and port for accessing the proxy server.

Depending on the protocol, it may be possible to specify a list of networks or individual hosts for which the proxy settings do not apply.



Use HTTP proxy

Enables the use of an HTTP proxy.

- **Address:** Enter the IP address of the the HTTP proxy server.
- **Port:** Enter the port used by the HTTP proxy server.

Use HTTPS proxy

Enables the use of an HTTPS proxy.

- **Address:** Enter the IP address of the the HTTPS proxy server.
- **Port:** Enter the port used by the HTTPS proxy server.

Perform proxy user authentication

If the proxy server requires authentication, enter the user name and password here. If the NT LAN Manager (NTLM) is to carry out the authentication, you additionally enter the NT domain and computer name.

! This option is available only if the proxy setting is enabled.

No proxy for

Enter the IP addresses and the corresponding netmask to which the proxy settings do not apply.

! This option is available only if the proxy setting is enabled.

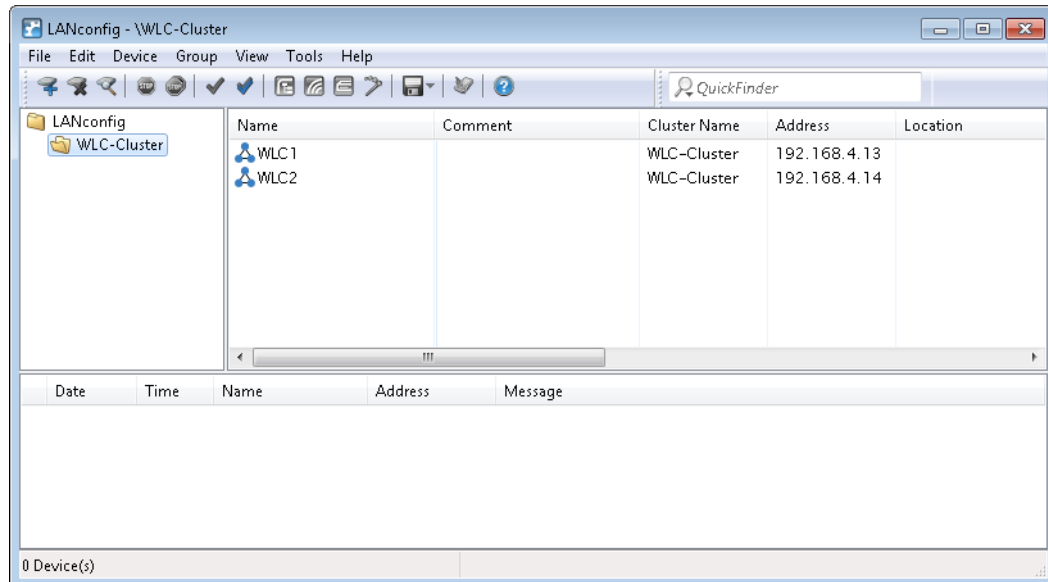
7.2 Special LANconfig icon for devices in a cluster or using Config Sync

LANconfig has a specific icon to mark devices that share their configuration via Config Sync. Furthermore, the **Config Cluster** column shows the configuration group for each device. LANconfig is thus able to sort and edit the device listing according to cluster name.

If you try to make changes to the configuration of a cluster member, you will receive following warning:

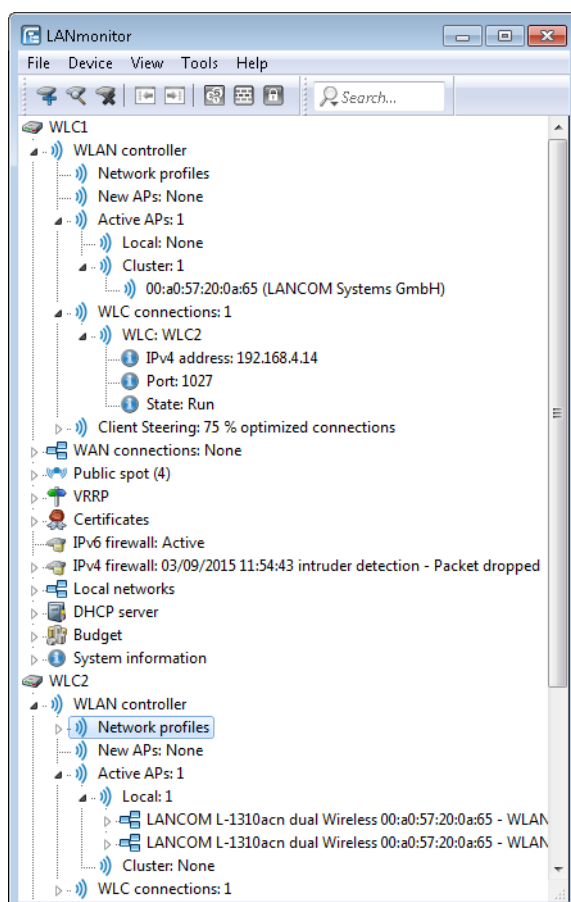
"This device belongs to the Config Cluster: [cluster name]. Editing this configuration also affects the following devices: [Listing of all devices in the same cluster]"

You can bypass this message if necessary. To do this, enable the option **Don't show again** in the displayed window.



7.3 Special LANmonitor icon for devices in a cluster or using Config Sync

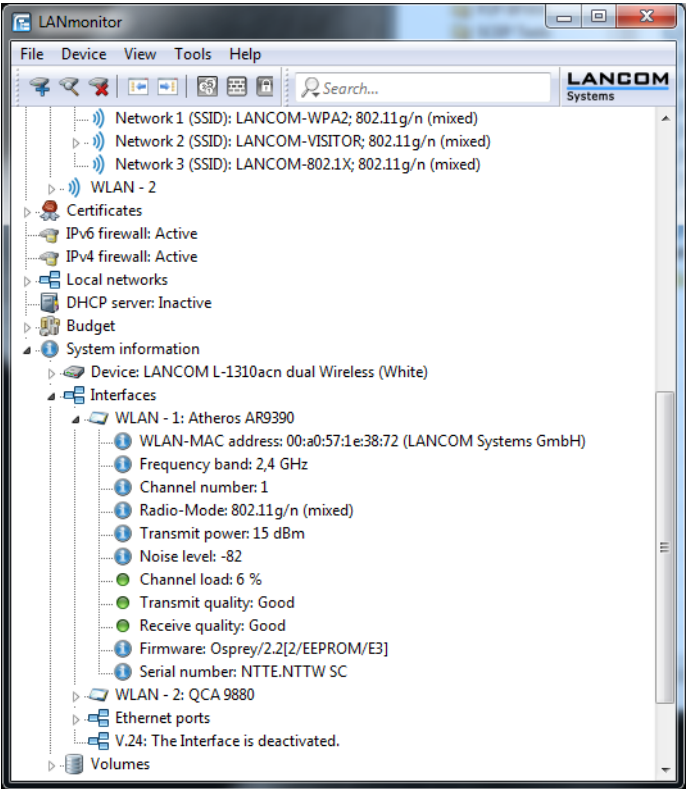
LANmonitor has a specific icon to mark devices that share their configuration via Config Sync. Also, the name of the configuration group (cluster name) is shown after the device name. LANmonitor thus makes it easier to see which devices share the same configuration.



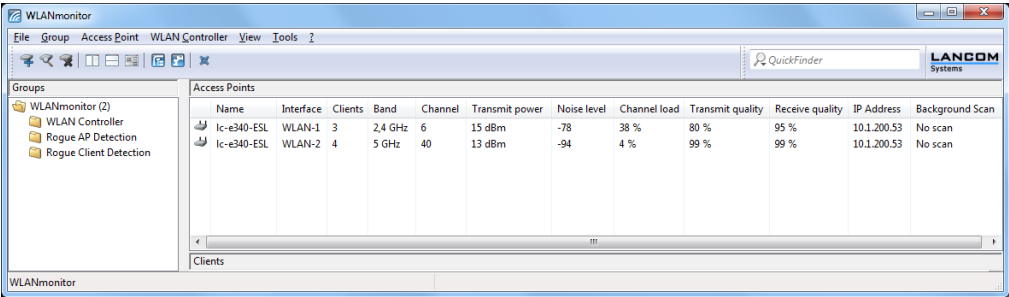
7.4 LANCOM "Wireless Quality Indicators" (WQI)

LANmonitor optionally displays the signal quality of the individual interfaces with the **Wireless Quality Indicators**. This representation of reception and transmission quality (RX and TX) helps you to make a quick assessment of signal

quality. To display this information in LANmonitor, open the section **System information** for the device. The indicators are displayed under **Interfaces**.



The WLANmonitor also displays the **Wireless quality indicators**. To do this click on the main folder for the group.



7.5 Extended number of characters for device names

The current release of LCOS allows you to assign longer device names in LANconfig and WEBconfig. The number of characters allowed is now 64 instead of 16.

7.6 Different notations for MAC addresses

As of LCOS version 9.10, LANconfig allows MAC addresses to be entered in other formats.

7.6.1 Different notations for MAC addresses

To make it easier to enter MAC addresses by using copy and paste from other applications into LANconfig, the following formats can be used when entering MAC addresses:

- 000000000000
- 00:00:00:00:00:00
- 00-00-00-00-00-00
- 000000-000000

The input is then automatically converted into the form 00 : 00 : 00 : 00 : 00 : 00.

7.7 LANconfig: Text corrections relating to access rights

As of LCOS version 9.10, the descriptions of the access rights in the configuration menu **Management > Admin** in the section **Configuration access ways** have been corrected:

- From a LAN interface
- From a WLAN interface
- From a WAN interface

LANconfig also used the new names in the section **Access to web-server services > Access rights**.

8 IPv6

8.1 Prefix-exclude option for DHCPv6 prefix delegation

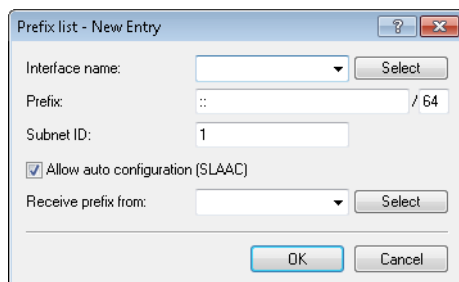
As of LCOS version 9.10, the DHCPv6 client of the device supports the prefix exclude option for DHCPv6-based prefix delegation according to RFC 6603.

8.1.1 Prefix-exclude option for DHCPv6 prefix delegation

The DHCPv6 client of the device supports the prefix exclude option for DHCPv6-based prefix delegation according to RFC 6603.

Providers use this mechanism with DHCPv6 prefix delegation in order to exclude a prefix from the delegated prefix set from being used on the customer LAN. This means that the device does not require an additional prefix for the WAN link, but instead it uses the prefix that was excluded from the delegated DHCPv6 prefix set. This prefix is no longer available for the LAN on the customer site.

If a device is configured to use the excluded prefix for the LAN, a syslog message is issued and the prefix is not advertised on the LAN. To resolve this conflict, you configure a different subnet ID for this LAN under **IPv6 > Router advertisement > Prefix list**.



The screenshot shows a configuration window titled "Prefix list - New Entry". It contains the following fields and controls:

- Interface name:** A dropdown menu with a "Select" button to its right.
- Prefix:** A text field containing "::" followed by a "/ 64" suffix.
- Subnet ID:** A text field containing the value "1".
- Allow auto configuration (SLAAC):** A checked checkbox.
- Receive prefix from:** A dropdown menu with a "Select" button to its right.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

9 ISDN

9.1 Additions to the Status menu

9.1.1 PCM-SYNC-SOURCE

This value indicates which ISDN interface provides the clock signal for the PCM bus. The PCM bus transfers the internal calls between the various interfaces (ISDN, analog and SIP).

SNMP ID:

1.33.2.2

Telnet path:

Status > ISDN > Framing

9.1.2 PCM-Switch

This menu contains the status values for the PCM switch.

SNMP ID:

1.33.20

Telnet path:

Status > ISDN

PCM connection

This table maps the switching of internal telephone calls. Under certain circumstances, this information can be relevant to troubleshooting by LANCOM Support.

SNMP ID:

1.33.20.1

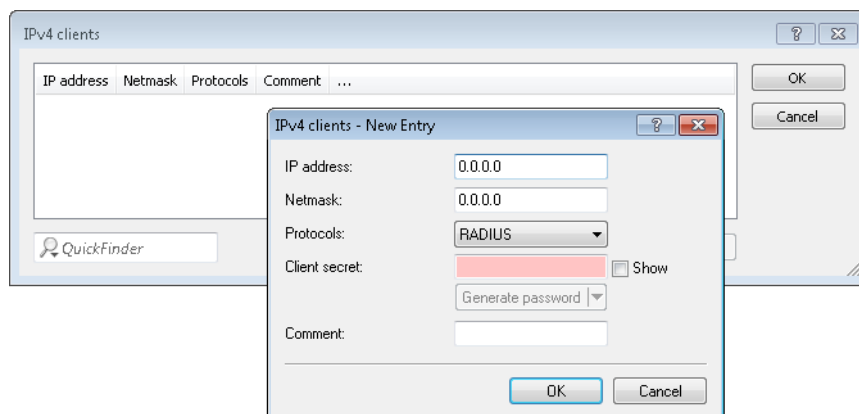
Telnet path:

Status > ISDN > PCM-Switch

10 RADIUS

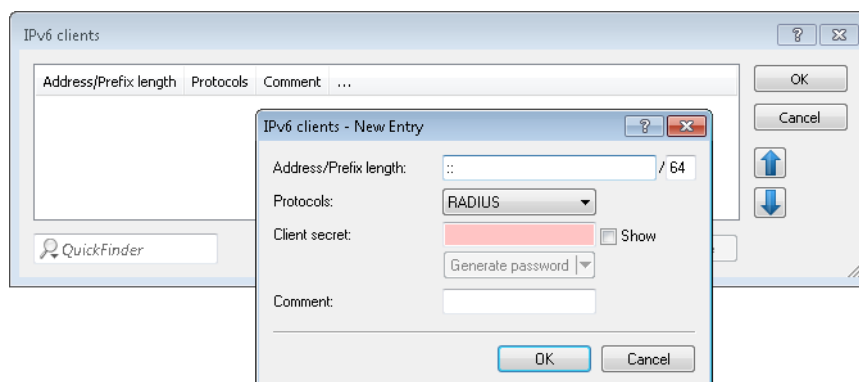
10.1 Comment field for RADIUS clients

As of LCOS version 9.10 it is possible to store a comment for each RADIUS client (IPv4 and IPv6) in the RADIUS table.



Comment

Comment on this entry.



Comment

Comment on this entry.

10.1.1 Additions to the Setup menu

Clients

Here you enter the clients that are to communicate with the RADIUS server.

SNMP ID:

2.25.10.2

Telnet path:

Setup > RADIUS > Server

Comment

Comment on this entry.

SNMP ID:

2.25.10.2.5

Telnet path:

Setup > RADIUS > Server > Clients

Possible values:

Max. 251 characters from [A-Z][a-z][0-9]@{ }~!\$%&'()*+,-./:;<=>?[\]^_`~

Default:

empty

IPv6 clients

Here you specify the RADIUS access data for IPv6 clients.

SNMP ID:

2.25.10.16

Telnet path:

Setup > RADIUS > Server

Comment

Comment on this entry.

SNMP ID:

2.25.10.16.5

Telnet path:

Setup > RADIUS > Server > IPv6-Clients

Possible values:

Max. 251 characters from [A-Z][a-z][0-9]@{ }~!\$%&'()*+,-./:;<=>?[\]^_`~

Default:

empty

10.2 More attributes for RADIUS requests

As of LCOS version 9.10 the device supports additional RADIUS attributes for the Public Spot, see chapter [Public Spot](#).

Table 6: The device transmits the following attributes in the access request:

ID	Name	Meaning	Possible values in LCOS
1	User name	The name entered by the user.	Used with 802.1X WLAN, PPPoE server, L2TP, PPTP, VPN
2	User-Password	The password entered by the user.	Used with 802.1X WLAN, PPPoE server, L2TP, PPTP, VPN
4	NAS-IP-Address	Specifies the IPv4 address of the device requesting access for a user.	<IPv4 address of the device>
6	Service-Type	Specifies the type of service that the device requests or expects as a response.	<ul style="list-style-type: none"> ■ Authenticate-Only ■ Framed
7	Framed-Protocol	Specifies the protocol to be used.	PPP
30	Called-Station-Id	Specifies the identifier of the called station (e.g. the VPN server).	<ul style="list-style-type: none"> ■ Server IP address (for VPN connections via PPTP or L2TP) ■ Service name (for PPPoE) ■ BSSID:SSID (for WLAN) ■ MAC address of the device (for Public Spot)
31	Calling-Station-Id	Specifies the identifier of the calling station (e.g. the VPN client).	<ul style="list-style-type: none"> ■ Client IP address (for VPN connections via PPTP or L2TP) ■ Client MAC address (for PPPoE, WLAN and Public Spot)
32	NAS identifier	Specifies the name of the device being managed by the RADIUS server.	<Device-Name>
61	NAS-Port-Type	Specifies the physical port through which the device authenticates the user.	<ul style="list-style-type: none"> ■ Virtual (for VPN connections via PPTP or L2TP) ■ Ethernet (with PPPoE) ■ Wireless 802.11 (for WLAN)
95	NAS-IPv6-Address	Specifies the IPv6 address of the device requesting access for a user.	<IPv6-address of the device>
64	Tunnel-Type	Defines the tunneling protocol which will be used for the session.	<ul style="list-style-type: none"> ■ 13 (VLAN; for Public Spot)
65	Tunnel-Medium-Type	Defines the transport medium over which the tunneled session will be established.	<ul style="list-style-type: none"> ■ 6 (802; for Public Spot)
81	Tunnel-Private-Group-ID	Defines the group ID if the session is tunneled.	<ul style="list-style-type: none"> ■ 1-4096 (for Public Spot)
177	Mobility-Domain-ID	Identifies the mobility domain where the client is located.	

ID	Name	Meaning	Possible values in LCOS
181	WLAN-HESSID	Contains the HESSID of the 802.11u SSID.	
182	WLAN-Venue-Info	Contains information about the category of the site.	This is configured under Wireless-LAN > 802.11u > Venue information .
183	WLAN-Venue-Language	Contains information about the language of the site.	This is configured under Wireless-LAN > 802.11u > Venue information .
184	WLAN-Venue-Name	Contains the name of the site (venue name).	This is configured under Wireless-LAN > 802.11u > Venue information .
186	WLAN-Pairwise-Cipher	Contains information about the pairwise key used by the client and AP.	
187	WLAN-Group-Cipher	Contains information about the group key used by the client and AP.	
188	WLAN-AKM-Suite	Contains information about the access management (authentication and key management) between the client and AP.	
189	WLAN-Group-Mgmt-Cipher	Contains information about the group management key/cipher used to secure a connection via RSNA (robust security network association) between an AP and mobile client.	
190	WLAN-RF-Band	Contains information about the frequency band used by the client.	

The following vendor-specific RADIUS attributes use the IANA Private Enterprise Number "3561" of the Broadband Forum. The remaining entries are LANCOM-specific attributes!

Table 7: Overview of all supported manufacturer-specific RADIUS attributes in the access request

ID	Name	Meaning	Possible values in LCOS
1	ADSL-Agent-Circuit-Id, Vendor 3561	Specifies the interface of the device being managed by the RADIUS server. Only transmitted if agent-relay info is included in the PPPoED packet (see PPPoE snooping).	<Device interface>
2	ADSL-Agent-Remote-Id, Vendor 3561	Specifies the identifier of the device being managed by the RADIUS server. Only transmitted if agent-relay info is included in the PPPoED packet (see PPPoE snooping).	<Device identifier>
16	LCS-Orig-NAS-Identifier, Vendor 2356	NAS-identifier of the original access point in WLC mode.	<Device-Name>
17	LCS-Orig-NAS-IP-Address, Vendor 2356	NAS IP address of the original access point in WLC mode.	<IPv4 address of the device>
18	LCS-Orig-NAS-IPv6-Address, Vendor 2356	NAS IPv6 address of the original access point in WLC mode.	<IPv6-address of the device>

10.3 Accounting status types "Accounting On" and "Accounting Off"

As of LCOS version 9.10, devices that use RADIUS for WLAN and Public Spots now also process the RADIUS accounting status types "Accounting-On" and "Accounting-Off".

10.3.1 Accounting status types "Accounting On" and "Accounting Off"

The RADIUS server and an AP exchange status information, such as the start, end, or update of client sessions at the AP. These data packets are characterized by the behavior of the logged-on clients.

With the status types "Accounting-On" and "Accounting-Off", the AP informs the RADIUS server about its general ability to perform RADIUS accounting:

Accounting-On


When the device switches to an operating state where it can exchange accounting information with a RADIUS server, it sends an "Accounting-On".

Accounting-Off

When the device switches to an operating state where it cannot exchange accounting information with a RADIUS server, it sends an "Accounting-Off".

The following conditions trigger the transmission of an "Accounting-On" or "Accounting-Off":


- The device activates or deactivates a physical WLAN interface with the appropriate SSID.

 Deactivation can also be the result of overheating, loss of connection or incorrect link detection.

- The WLAN interface switches into a non-AP mode (i.e. neither managed nor stand-alone-AP) or back.
- In P2P mode, the device switches into "exclusive" mode, which disables all SSIDs.
- The device activates or deactivates an SSID.
- The device activates or deactivates the RADIUS accounting for an SSID.

10.4 Larger volume budgets in the RADIUS server and Public Spot

As of LCOS version 9.10, the RADIUS server is capable of managing volume budgets in excess of 4GByte.

 The RADIUS server now interprets existing volume budgets as a value in MBytes (previously in bytes). By updating to LCOS version 9.10, the device converts existing values and rounds them up to full MBytes. For example, the entry "1000000" (byte) converts to "1" (MByte).

This extension affects the Public Spot module. The specification of the volume budget via the Public Spot web API can also include a unit:

volumebudget

Volume budget

The following entries are allowed:

- **k** or **K**: Specified in kilobytes (kB), e.g. `volumebudget=1000k`.
- **m** or **M**: Specified in megabytes (MB), e.g. `volumebudget=1000m`.
- **g** or **G**: Specified in gigabytes (GB), e.g. `volumebudget=1g`.

Without a unit, the specification corresponds to a value in bytes (B).

If this parameter is omitted completely, the wizard uses the default value.

This extension affects the XML interface. The specification of the volume budget at the login request and the login response can also include a unit:

TRAFFICEXPIRE

The maximum data volume for a user account. The user can use this data volume until a relative or absolute expiry time (if set) is reached.

The following entries are allowed:

- **k** or **K**: Specified in kilobytes (kB), e.g. <TRAFFICEXPIRE>1000k</TRAFFICEXPIRE>.
- **m** or **M**: Specified in megabytes (MB), e.g. <TRAFFICEXPIRE>100m</TRAFFICEXPIRE>.
- **g** or **G**: Specified in gigabytes (GB), e.g. <TRAFFICEXPIRE>1g</TRAFFICEXPIRE>.

Without a unit, the specification corresponds to a value in bytes (B).

10.4.1 Additions to the Setup menu

Volume budget

The maximum data volume in MBytes for this user account. The user can use this data volume until a relative or absolute expiry time (if set) is reached.

SNMP ID:

2.25.10.7.12

Telnet path:

Setup > RADIUS > Server

Possible values:

Max. 10 characters from 0123456789

Default:

0

Special values:

0

switches off the monitoring of data volume.

Volume budget MByte

This entry enables you to set the budget volume of the RADIUS user in megabytes.

SNMP ID:

2.25.10.7.22

Telnet path:

Setup > RADIUS > Server > Users

Possible values:

Max. 10 characters from [0–9]

Default:

0

Special values:

0

The volume budget is deactivated.

Volume budget

With this entry you specify the volume budget in MBytes assigned to automatically created users. The value 0 deactivates the function.

SNMP ID:

2.24.41.3.3

Telnet path:**Setup > Public-Spot-Module > Authentication-Modules > User-Template****Possible values:**

Max. 4 characters from 0123456789

Default:

0

Special values:

0

switches off the monitoring of data volume.

10.5 RADIUS server: Realm discovery for computer authentication

As of LCOS version 9.10, the RADIUS server additionally determines the realm of a RADIUS request from a computer authentication.

The device considers the parts of a user name that follow to be the realm:

user@company.com

company.com is the realm and is separated from the name of the user by an @ character.

company\user

company is the realm and is separated from the name of the user by a backslash (""). This form of authentication is used for a Windows login, for example.

host/user.company.com

If the user name starts with the string host / and the rest of the name contains at least one dot/period, the device considers everything after the first dot to be the realm (in this case company.com).

10.5.1 Additions to the Setup menu

Realm types

Specify how the RADIUS server determines the realm of a RADIUS request.

SNMP ID:

2.25.10.17

Telnet path:

Setup > RADIUS > Server

Possible values:**Mail domain**

`user@company.com`: `company.com` is the realm and is separated from the name of the user by an @ character.

MS domain

`company\user`: `company` is the realm and is separated from the name of the user by a backslash (""). This form of authentication is used for a Windows login, for example.

MS-CompAuth

`host/user.company.com`: If the user name starts with the string `host/` and the rest of the name contains at least one dot/period, the device considers everything after the first dot to be the realm (in this case `company.com`).

Default:

Mail domain

MS domain

10.6 RADIUS client: Additional source ports for requests when necessary

As of LCOS version 9.10, the RADIUS client opens additional source ports for access requests if necessary.

10.6.1 Additional source ports for access requests

The RADIUS client uses a source port (UDP listener) for negotiating access requests with the RADIUS server. This port allows the simultaneous negotiation of up to 256 IDs. If a client is processing a large number of requests at the same time and the RADIUS server is far away, it is possible for all 256 access requests to be open at the same time, causing the RADIUS client to be unable to handle any further requests. This can happen, for example, in extensive Eduroam environments.

In this case, the RADIUS client opens the next highest source port to enable the access request negotiation for additional IDs. This is automatic and is not configurable.

10.7 User-defined RADIUS attributes

As of LCOS version 9.10 the RADIUS attributes are configurable.

10.7.1 RADIUS attributes configurable

LCOS allows the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified by means of a semicolon-separated list of attribute numbers or names (as per [RFC 2865](#), [RFC 3162](#), [RFC 4679](#), [RFC 4818](#), [RFC 7268](#)) and a corresponding value in the form
`<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device, the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks ("`<Value>`") allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (`\`), as does the backslash itself (`\\`).

The following variables are permitted as values:

%n

Device name

%e

Serial number of the device

%%

Percent sign

%{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

10.7.2 Additions to the Setup menu

Attribute-Values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to [RFC 2865](#), [RFC 3162](#), [RFC 4679](#), [RFC 4818](#), [RFC 7268](#)) and a corresponding value in the form
`<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>`.

Variables can also be used as values (such as %n for the device name). Example: `NAS-Identifier=%n`.

SNMP ID:

2.2.22.12

Telnet path:

Setup > WAN > RADIUS

Possible values:

Max. 128 characters from `[A-Z][a-z][0-9]#@[|]~!$%&'()*+,-./:;<=>?[\]^_`~`

Default:

empty

L2TP attribute values

With this entry you configure the RADIUS attributes for the tunnel end point of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to [RFC 2865](#), [RFC 3162](#), [RFC 4679](#), [RFC 4818](#), [RFC 7268](#)) and a corresponding value in the form
`<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>.`

Variables can also be used as values (such as %n for the device name). Example: `NAS-Identifier=%n`.

SNMP ID:

2.2.22.27

Telnet path:

Setup > WAN > RADIUS

Possible values:

Max. 128 characters from `[A-Z][a-z][0-9]#@[|]~!$%&'()*+,-./:;<=>?[\]^_`~`

Default:

empty

Attribute-Values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to [RFC 2865](#), [RFC 3162](#), [RFC 4679](#), [RFC 4818](#), [RFC 7268](#)) and a corresponding value in the form
`<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>.`

Variables can also be used as values (such as %n for the device name). Example: `NAS-Identifier=%n`.

SNMP ID:

2.11.81.1.9

Telnet path:

Setup > Config > Radius > Server

Possible values:

Max. 128 characters from `[A-Z][a-z][0-9]#@[|]~!$%&'()*+,-./:;<=>?[\]^_`~`

Default:

empty

Attribute-Values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to [RFC 2865](#), [RFC 3162](#), [RFC 4679](#), [RFC 4818](#), [RFC 7268](#)) and a corresponding value in the form
`<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>.`

Variables can also be used as values (such as %n for the device name). Example: NAS-Identifier=%n.

SNMP ID:

2.12.29.18

Telnet path:

Setup > WLAN > RADIUS-Access-Check

Possible values:

Max. 128 characters from [A-Z][a-z][0-9]#@{ }~!\$%&'()*+,-./:;<=>?[\]^_`~

Default:

empty

Backup attribute values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to [RFC 2865](#), [RFC 3162](#), [RFC 4679](#), [RFC 4818](#), [RFC 7268](#)) and a corresponding value in the form

<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>.

Variables can also be used as values (such as %n for the device name). Example: NAS-Identifier=%n.

SNMP ID:

2.12.29.19

Telnet path:

Setup > WLAN > RADIUS-Access-Check

Possible values:

Max. 128 characters from [A-Z][a-z][0-9]#@{ }~!\$%&'()*+,-./:;<=>?[\]^_`~

Default:

empty

Attribute-Values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to [RFC 2865](#), [RFC 3162](#), [RFC 4679](#), [RFC 4818](#), [RFC 7268](#)) and a corresponding value in the form

<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>.

Variables can also be used as values (such as %n for the device name). Example: NAS-Identifier=%n.

SNMP ID:

2.12.45.17.9

Telnet path:

Setup > WLAN > RADIUS-Accounting > Servers

Possible values:

Max. 128 characters from [A-Z][a-z][0-9]#@[]~!\$%&'()*+,-./:;<=>?[\]^_`~

Default:

empty

Auth.-Attribute-Values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to [RFC 2865](#), [RFC 3162](#), [RFC 4679](#), [RFC 4818](#), [RFC 7268](#)) and a corresponding value in the form
<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>.

Variables can also be used as values (such as %n for the device name). Example: NAS-Identifier=%n.

SNMP ID:

2.24.3.15

Telnet path:

Setup > Public-Spot-Module > Provider-Table > Server

Possible values:

Max. 128 characters from [A-Z][a-z][0-9]#@[]~!\$%&'()*+,-./:;<=>?[\]^_`~

Default:

empty

Acc.-Attribute-Values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to [RFC 2865](#), [RFC 3162](#), [RFC 4679](#), [RFC 4818](#), [RFC 7268](#)) and a corresponding value in the form
<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>.

Variables can also be used as values (such as %n for the device name). Example: NAS-Identifier=%n.

SNMP ID:

2.24.3.16

Telnet path:

Setup > Public-Spot-Module > Provider-Table > Server

Possible values:

Max. 128 characters from [A-Z][a-z][0-9]#@[]~!\$%&'()*+,-./:;<=>?[\]^_`~

Default:*empty***Attribute-Values**

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to [RFC 2865](#), [RFC 3162](#), [RFC 4679](#), [RFC 4818](#), [RFC 7268](#)) and a corresponding value in the form

<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>.

Variables can also be used as values (such as %n for the device name). Example: NAS-Identifier=%n.

SNMP ID:

2.25.10.3.15

Telnet path:**Setup > RADIUS > Server > Forward-Servers****Possible values:**

Max. 128 characters from [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~

Default:*empty***Accnt.-Attribute-Values**

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to [RFC 2865](#), [RFC 3162](#), [RFC 4679](#), [RFC 4818](#), [RFC 7268](#)) and a corresponding value in the form

<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>.

Variables can also be used as values (such as %n for the device name). Example: NAS-Identifier=%n.

SNMP ID:

2.25.10.3.16

Telnet path:**Setup > RADIUS > Server > Forward-Servers****Possible values:**

Max. 128 characters from [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~

Default:*empty*

Attribute-Values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to [RFC 2865](#), [RFC 3162](#), [RFC 4679](#), [RFC 4818](#), [RFC 7268](#)) and a corresponding value in the form
<Attribute_1>=<Value_1>, <Attribute_2>=<Value_2>.

Variables can also be used as values (such as %n for the device name). Example: NAS-Identifier=%n.

SNMP ID:

2.30.3.9

Telnet path:

Setup > IEEE802.1x > RADIUS-Server

Possible values:

Max. 128 characters from [A-Z][a-z][0-9]#@[| } ~ ! \$ % & ' () * + - , / : ; < = > ? [\] ^ _ . ~

Default:

empty

11 Public Spot

11.1 Restricting administrators to voucher output only

If in LCOS you have created an administrator who is restricted to the function rights of the **Public Spot Wizard (create account)** only, then this administrator now has access only to the input mask of the add user wizard. The navigation toolbar in WEBconfig remains concealed.

11.1.1 Wizard for creating and managing users

Using the setup wizard **Create Public Spot account** you can use WEBconfig to create temporary accesses to the Public Spot network with just a few clicks of the mouse. In the simplest case, you only need to enter the duration of access, the wizard assigns the username and password automatically and stores the credentials in the user database of the internal RADIUS server. The user receives a printed, personalized voucher, which the user can immediately use to login to the Public Spot network for the specified period.

Alternatively, a stock of vouchers can be created and printed out to speed up the voucher issue at peak times or to allow employees without access to the device to issue vouchers. In this case the Public Spot account is created with an online time duration that starts when the user logs in for the first time. You also set a maximum validity period for the access. After this time, the Public Spot automatically deletes the access account, even if the online time was not used up yet.

The setup wizard **Manage Public Spot account** displays all registered Public-Spot access accounts in a table on a web page. This gives you an overview of your most important user data, as well as a user-friendly way to extend or reduce the validity of an access account with a single click, or even delete user accounts completely. In addition, the administrator can call up information about the user account using the wizard, such as the password in cleartext, the authentication status, the IP address, the sent/received data volume or any restrictions that apply to the user account.

If several administrators are involved with the management of Public Spot accounts, you have the option of restricting the accounts that are displayed to those created by the respective administrator. As a result, the overview table only displays those accounts that were created by the administrator who is currently logged-on.



This restriction has no effect if an administrator account has a full name that is a part of the other administrator account names. "PSpot_Admin" for example sees the entries made by "PSpot_Admin1" and "PSpot_Admin2". "PSpot_Admin" acts as a super-admin in this scenario. All other administrators ("PSpot_AdminX"), however, do not see the entries made by the others.

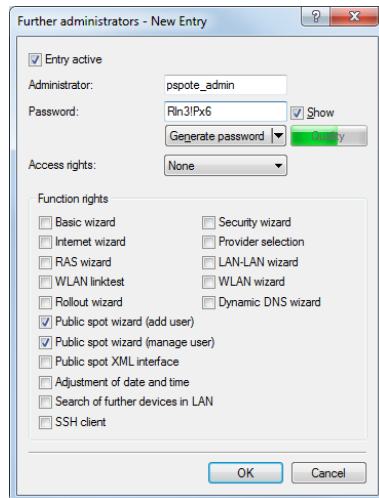
11.1.2 Setting up limited administrator rights for Public Spot managers

It is possible to allow employees to create and manage user accounts even though they do not have access rights to the device configuration. This is done by setting up a limited administrator, who only has the right to use the [Public Spot Wizard](#). This tutorial describes the steps and the necessary access rights and privileges to do this in LANconfig.

The rights to use the Public Spot Wizards are configurable separately from one another, so it is possible to restrict a limited administrator to any single Wizard. In the case of the Public Spot setup wizard, the restricted administrator logging in to WEBconfig is automatically forwarded to the corresponding input mask.

1. In LANconfig, open the configuration dialog for the device you want to add a Public Spot administrator to. The Public Spot option has to be enabled on this device.
2. Navigate to the item **Management > Admin**. In the section **Device configuration**, click **Further administrators** and then click **Add**.

To allow an existing user to perform Public Spot management, you instead select the user's entry in the table and click on **Change**.



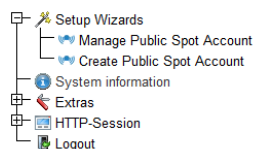
3. You activate the profile by checking the **Entry active** box.
4. Assign a descriptive name in the field **Administrator**.
5. Enter a **Password** and repeat it as a check.
6. Set the **Access rights** to **None**.
7. In the section **Function rights** enable the options **Public Spot wizard (add user)**, and **Public Spot wizard (manage user)** for the Public Spot setup wizard.



The function right **Public Spot XML interface** is not required by a Public Spot administrator. The right is only relevant if you use the XML interface and should not be combined with the function rights described above for security reasons.

8. Save the new or modified administrator profile by clicking on **OK**.

If you have granted the feature rights to several Wizards, the limited administrator can navigate between these using the navigation bar in WEBconfig.



If you have set the function right for the **Public Spot Wizard (create user)** only, then a limited administrator can only navigate within this Wizard, and the navigation bar is hidden. In this case it is not possible to logout of WEBconfig manually. For security reasons, this means that the lifetime of the WEBconfig session is very short. In case of inactivity, the device automatically logs out the limited administrator.



For technical reasons, the Create Public Spot Account wizard does not update automatically after use of the **Create and CSV export** button. A limited administrator who wishes to set up additional users and print vouchers must invoke the Wizard again (e.g. via a URL or by refreshing the web page if the navigation bar is hidden).

11.2 Specify volume budget on vouchers

LCOS9.10 now enables you to use the placeholder tag `<pbelem vollimit>` in the voucher template, so as to inform Public Spot users of the data volume assigned to them.

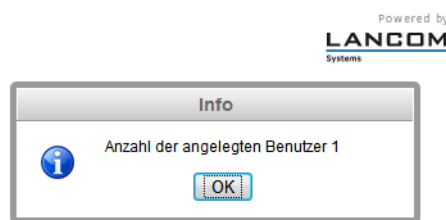
VOLLIMIT

Valid for: <pbe1em><pbcond>

This identifier contains the amount of data, expressed in bytes, that the client is still allowed to transfer before the device terminates the current session. This identifier is zero for a session with no data limit.

Zugangsdaten Public-Spot

Benutzername/Username: user47874
 Passwort/Password: e83sc1
 Gültig bis/Valid until: 12.01.2016 11:52:00
 Dauer/Duration: 1 Stunde(n)
 Volumen-Budget/Volume budget: 12 MByte





11.3 XML interface: Enhanced VLAN handling

As of LCOS version 9.10, you have the option to communicate the user's source VLAN to the Public Spot via an external gateway, and to forward the VLAN-ID dependent authentication to an external RADIUS server.

SOURCE_VLAN (optional, only in conjunction with authentication by RADIUS server)

The VLAN ID of the network from which a Public Spot user attempts to login (source VLAN). The Public Spot forwards the source VLAN in its access request to the internal or external RADIUS server. The Public Spot uses the RADIUS attribute 81 (**tunnel-private-group-ID**) together with the RADIUS attributes 64 (**tunnel-type**) and 65 (**tunnel-medium-type**). The RADIUS server uses the source VLAN to decide whether to accept or decline the access request from the Public Spot.

If the RADIUS server accepts the request, it returns an access-accept with the RADIUS attributes mentioned above to the Public Spot. The Public Spot then saves the source VLAN for the client and its station list and allows the user to access the Public Spot network.


-  Use the source VLAN in conjunction with the setup parameter 2.24.47. This prevents Public Spot users in VLAN-separated Public Spot networks/SSIDs from authenticating once at the RADIUS server and then accessing all of the managed Public Spot networks/SSIDs.
-  The SOURCE_VLAN should not be confused with the VLAN_ID. The VLAN_ID is not sent to the RADIUS server. However, the Public Spot uses it to assign a VLAN ID provided by the gateway to a successfully authenticated user.

For internal checking, the Public Spot stores the source VLAN to its station table as soon as the external RADIUS server has accepted the authentication request. If a user then switches to a different Public Spot network/SSID with a VLAN-ID which is different to that stored, then the Public Spot sets the user to "unauthenticated" and displays the login page again at the next opportunity.

11.3.1 Additions to the Setup menu

Check origin VLAN

Use this parameter to specify whether the VLAN ID of the network where a user is authenticated is used by the XML interface to verify user requests. This is relevant, for example, in scenarios where several Public Spot SSIDs are separated by means of VLAN and a one-time authentication at one of these SSIDs should not automatically entitle the user to access the other SSIDs.

 The parameter requires that you have also enabled the setup parameters 2.24.40.1 (the XML interface itself) and 2.24.40.2 (authentication by the XML interface via an internal or an external RADIUS server) .

SNMP ID:

2.24.47

Telnet path:

Setup > Public-Spot-Module

Possible values:

No

The Public Spot does not take the VLAN ID into account when verifying users. A one-time authentication entitles a user to access all of the SSIDs managed by the Public Spot. As long as the user account is valid, authentication is automatic.

Yes

The Public Spot takes the VLAN ID into account when verifying users. The Public Spot stores the VLAN ID to the column of the same name in the station table, assuming that the authentication by the RADIUS server was successful. This VLAN ID is the value for `SOURCE_VLAN` in the login request from the external gateway. If the Public Spot user moves to a network with a different VLAN ID, the Public Spot updates their station-table entry to "unauthenticated" and prompts the user to authenticate at the RADIUS server again. In this case, the user receives the sign-in page to authenticate again.

 To learn more about the request and response types, as well as the `SOURCE_VLAN` element, refer to the Reference Manual.

Default:

No

VLANs

This parameter optionally defines a list of VLAN IDs which control the approved site(s) that are available to the corresponding host name. Only users who have the VLAN ID stored in the station table are able to access this host without having to authenticate. Use this parameter, for example, in application scenarios where Public Spot networks/SSIDs are separated by VLAN and you wish to set different access restrictions for different user groups.

SNMP ID:

2.24.31.3

Telnet path:

Setup > Public-Spot-Module > Free-Networks > VLans

Possible values:**Default:***empty*

Comma-separated list, max. 16 characters from [0-9],

Special values:*empty, 0*

Access to the host entered here is possible from all VLANs.

11.3.2 Messages to and from the authentication server

Transferred attributes

As previously mentioned, your device transmits far more than just the username and password in a RADIUS request. RADIUS servers might choose to completely ignore these additional attributes, or only use a subset of these attributes. Many of these attributes are used for access to the server using dial-in, and are defined as standard attributes in the RADIUS RFCs. However, some important information for hotspot operation can not be represented with standard attributes. These additional attributes are manufacturer-specific with the manufacturer code 2356 (LANCOM Systems GmbH).

Table 8: Overview of the RADIUS attributes transmitted by the device to the authentication server

ID	Name	Meaning	Possible values in LCOS
1	User name	The name entered by the user.	
2	User-Password	The password entered by the user.	
4	NAS-IP-Address	IP address of your device	<IPv4 address of the device>
6	Service-Type	Type of service that the user requested. The value "1" stands for Login.	
8	Framed-IP-Address	Specifies the IP address that is assigned to the client.	<IP address of the client>
30	Called-Station-Id	MAC address of your device	<nn:nn:nn:nn:nn:nn>
31	Calling-Station-Id	MAC address of the client The address is given byte-wise in hexadecimal notation with separators.	<nn:nn:nn:nn:nn:nn>
32	NAS identifier	Name of your device, if configured.	<Device-Name>
61	NAS-Port-Type	Type of physical port over which a user had requested authentication.	<ul style="list-style-type: none"> ■ ID 19 denotes clients from WLAN. ■ ID 15 denotes clients from Ethernet.
87	NAS-Port-Id	Description of the interface over which the client is connected to your device. This may be a physical and a logical interface.	For example <ul style="list-style-type: none"> ■ LAN-1 ■ WLAN-1-5 ■ WLC-TUNNEL-27



Consider that more than one client may be connected to one interface at a time, so that, unlike dial-in servers, port numbers are not unique for clients.


Processed attributes

Your device evaluates the authentication response of a RADIUS server for attributes that it may possibly process further. Most attributes however only have a meaning if the authentication response was positive, so that they influence the subsequent session:

Table 9: Overview of the supported RADIUS attributes

ID	Name	Meaning	Possible values in LCOS
18	Reply-Message	An arbitrary string from the RADIUS server that may transport either a login failure reason or a user welcome message. This message may be integrated into user-defined start or error pages via the <code>SEVERMSG</code> element.	
25	Class	An arbitrary octet string that may contain data provided by the authentication/accounting backend. Whenever the device sends RADIUS accounting requests, they will contain this attribute as-is. Within an authentication response, this attribute can occur multiple times in order, for example, to transmit a string that is longer than 255 bytes. The device processes all occurrences in accounting requests in the order they appeared in the authentication response.	
26	Vendor 2356, Id 1 LCS-Traffic-Limit	Defines the data volume in bytes after which the device automatically ends the session. This value is useful for volume-limited accounts. If this attribute is missing in the authentication response, it is assumed that no volume limit applies. A traffic limit of 0 is interpreted as an account which is principally valid, however with a used-up volume budget. The device does not start a session in this case.	
26	Vendor 2356, Id 3 LCS-Redirection-URL	This can contain any URL that is offered as an additional link on the start page. This can be the start page of the user or a page with additional information about the user account.	
26	Vendor 2356, Id 5 LCS-Account-End	Defines an absolute point in time (measured in seconds since January 1, 1970 0:00:00) after which the account becomes invalid. If this attribute is missing, an unlimited account is assumed. The device does not start a session if its internal clock has not been set, or the given point in time is in the past.	
26	Vendor 2356, Id 7 LCS-Public-Spot-Username	Contains the name of a Public Spot user for auto-login. Auto-login refers to the table of MAC authenticated users who are automatically assigned usernames by the server.	
26	Vendor 2356, Id 8 LCS-TxRateLimit	Defines the maximum downstream rate in kbps. This restriction may be combined with the corresponding Public Spot function.	
26	Vendor 2356, Id 9 LCS-RxRateLimit	Defines the maximum upstream rate in kbps. This restriction may be combined with the corresponding Public Spot function.	
26	Vendor 2356, Id 13 LCS-Advertisement-URL	Specifies a comma-separated list of advertisement URLs.	
26	Vendor 2356, Id 14 LCS-Advertisement-Interval	Specifies the interval in minutes after which the Public Spot reroutes a user to an advertisement URL. With an interval of 0 forwarding occurs directly after login.	
27	Session-Timeout	Defines an optional maximum duration of the session, measured in seconds. If this attribute is missing in the response, an unlimited account is assumed. A Session timeout of zero seconds is interpreted as an account which is principally valid, however with a used-up time budget. The device does not start a session in this case.	
28	Idle timeout	Defines a time period in seconds after which the device will terminate the session if no packets were received from the	

ID	Name	Meaning	Possible values in LCOS
		client. This value may possibly overwrite the idle timeout that is defined locally under Public Spot > Server > Idle timeout .	
64	Tunnel-Type	Defines the tunneling protocol which will be used for the session.	
65	Tunnel-Medium-Type	Defines the transport medium over which the tunneled session will be established.	
81	Tunnel-Private-Group-ID	Defines the group ID if the session is tunneled.	
85	Acct-Interim-Interval	Defines the amount of time between subsequent RADIUS accounting updates. This value is only evaluated if the RADIUS client does not have a local accounting interval defined, i.e. if you have not set an Accounting update cycle for the Public Spot module.	

 Note that the LCS-Account-End and Session-Timeout attributes are mutually exclusive, and it therefore does not make sense to include both in the response. If both attributes are included in a response, the attribute that appears as the last one in the attribute list will define the session's time limit.

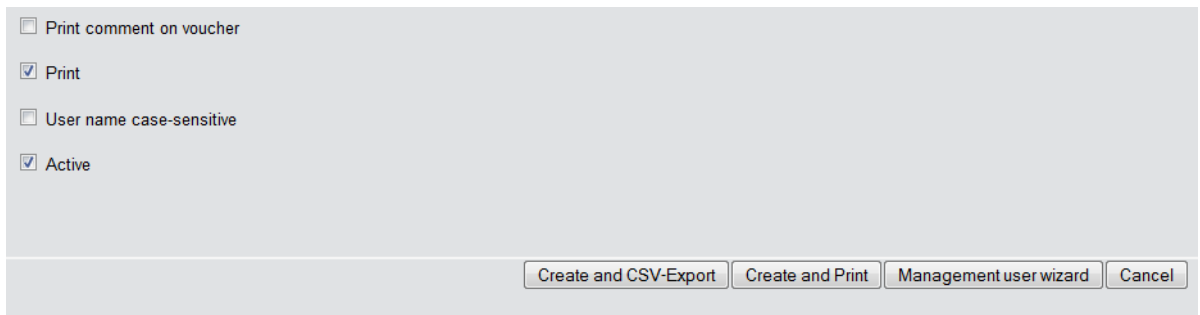
11.4 "Small header image": Optimized display for 19" devices


As of LCOS version 9.10, 19-inch devices also have a login page with a customizable header image for narrow screens. This improves the way the Public Spot appears on mobile devices.

11.5 New button "Manage user wizard"

As of LCOS version 9.10 you have the option in the Setup Wizard **Create Public Spot account** to display the additional button **Manage user wizard**.

The button **Manage User Wizard** button takes you to the **Manage Public Spot Account** Setup Wizard.



 You have the option to either show or hide this button. It is displayed by default.

11.5.1 Additions to the Setup menu

Hide-User-Management-Button

This parameter gives you the option to hide the **Manage user wizard** button in the Setup Wizard.

SNMP ID:

2.24.19.20

Telnet path:

Setup > Public-Spot-Module > Add-User-Wizard

Possible values:

Yes

The **Create Public Spot account** Setup Wizard hides the **Manage user wizard** button.

No

The Setup Wizard displays the **Manage user button**.

Default:

No

11.6 Only show user accounts generated by the currently logged-on administrator

As of LCOS version 9.10, the Setup Wizard **Manage Public Spot account** gives you have the option to hide accounts that were created by other administrators.

If several administrators are involved with the management of Public Spot accounts, you have the option of restricting the accounts that are displayed to those created by the respective administrator. As a result, the overview table only displays those accounts that were created by the administrator who is currently logged-on.



This restriction has no effect if an administrator account has a full name that is a part of the other administrator account names. "PSpot_Admin" for example sees the entries made by "PSpot_Admin1" and "PSpot_Admin2". "PSpot_Admin" acts as a super-admin in this scenario. All other administrators ("PSpot_AdminX"), however, do not see the entries made by the others.

11.6.1 Additions to the Setup menu

show-all-users-admin-independent

This entry allows you to display only those user accounts in the Setup Wizard that were created by the currently logged-in administrator.

SNMP ID:

2.24.44.11

Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

Possible values:**Yes**

The Setup Wizard displays all Public Spot accounts.

No

The Setup Wizard only displays the Public Spot accounts created by the currently logged-on administrator.

Default:

Yes

11.7 Evaluation of DHCP option 82 in RADIUS and Public Spot

As of LCOS version 9.10, RADIUS client and Public Spot devices evaluate the DHCP option 82.

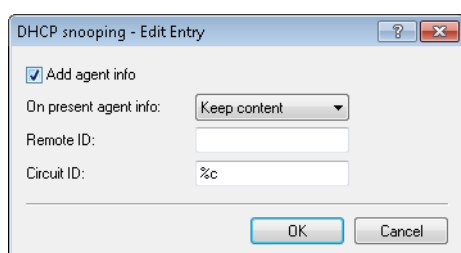
11.7.1 AP-specific login to a central Public Spot

A central WLC manages a Public Spot in a distributed infrastructure. Accordingly, the configuration of the Public Spot (Public Spot SSID, security standards) is identical on all of the participating APs. This allows a Public Spot provider to offer an identical Public Spot at all of the different locations.

After receiving a voucher, customers would have access to this Public Spot at any branch. In order to limit access to the branch where the customer has received the voucher, the AP transmits its own identifier in addition to the user name and password. This identifier enables the voucher to be associated with this AP. To transfer the identifier, the AP attaches the circuit ID (DHCP option 82) to the DHCP requests. These DHCP packets pass through the central Public Spot, which checks the identifier based on the entries in the RADIUS user table.

The Public Spot only allows a request if the voucher in the RADIUS user table is associated with this AP. Customers who have received a voucher at branch A cannot login to the same Public Spot at branch B, since the two APs transmit different identifiers.

The AP identifier is configured as the circuit ID for the corresponding interface under **Interfaces > Snooping > DHCP snooping**.



You can use the following variables:

- %%: Inserts a percent sign.
- %c: Inserts the MAC address of the interface used by the Public Spot user to authenticate. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- %c: Inserts the name of the interface used by the Public Spot user to authenticate.
- %n: Inserts the name of the AP as specified under **Management > General**.
- %v: Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.

- **%p**: Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, **%p** and **%i** are identical.
- **%s**: Inserts the WLAN SSID if a WLAN client is used for the authentication. For other clients, this variable contains an empty string.
- **%e**: Inserts the serial number of the AP, to be found for example under **Management > General**.

On the WLC, you configure this identifier in the RADIUS user table under **RADIUS server > General > User table**.

As the "Called station", you add the ID of the AP that should enable access by means of the corresponding voucher.

When setting up new Public Spot users, the Public Spot Setup Wizard automatically uses the ID of the device if this is configured under **Public Spot > Wizard > Circuit IDs**.

When you create a new Public Spot account, the setup wizard checks to see whether this table contains an entry for the logged-in **administrator**. If this is the case, the setup wizard inserts the **circuit ID** into the RADIUS user table as the "called station".

11.7.2 Additions to the Setup menu

Circuit-IDs

When a user authenticates at a Public Spot, the circuit ID configured in this table is an additional identifier sent by the AP to the WLC along with the user name and password.

When you create a new Public Spot account, the Public Spot setup wizard checks to see whether this table contains an entry for the logged-in administrator. If this is the case, the setup wizard inserts the circuit ID into the RADIUS user table as the "called station".

SNMP ID:

2.24.48

Telnet path:**Setup > Public Spot****Administrator**

Contains the name of the administrator who is entitled to assign this circuit ID.

SNMP ID:

2.24.48.1

Telnet path:**Setup > Public-Spot > Circuit-IDs****Possible values:**

Max. 16 characters from `[A-Z][a-z][0-9]@{ | }~!$%&'()+- , / ; < = > ? [\] ^ _ . ``

Default:*empty***Circuit ID**

Contains the circuit ID sent by the AP to the WLC as an additional identifier along with the user name and password when a user authenticates at a Public Spot.

SNMP ID:

2.24.48.2

Telnet path:**Setup > Public-Spot > Circuit-IDs****Possible values:**

Max. 64 characters from `[A-Z][a-z][0-9]#@{ | }~!$%&'()*+ - , / : ; < = > ? [\] ^ _ . ``

Default:*empty*

11.8 Additions to the Status menu

11.8.1 Max. no. users

This entry indicates the maximum number of users that may be authenticated with the Public Spot at the same time.

SNMP ID:

1.44.11

Telnet path:**Status > Public-Spot**

11.8.2 PbSpot authenticated users

This entry displays the number of Public Spot users who are currently authenticated via the Public Spot itself.

SNMP ID:

1.44.12

Telnet path:**Status > Public-Spot**

11.8.3 PMS authenticated users

This entry displays the number of Public Spot users who are currently authenticated via the PMS interface.

SNMP ID:

1.44.13

Telnet path:**Status > Public-Spot**

11.8.4 Local configured users

This entry indicates how many Public Spot users are currently setup locally on the device.

SNMP ID:

1.44.14

Telnet path:**Status > Public-Spot**

11.9 Additions to the Setup menu

11.9.1 Password input set

This setting specifies the character set used by the **Create Public Spot Account** wizard to create passwords for new users.

SNMP ID:

2.24.19.18

Telnet path:

Setup > Public-Spot-Module > Add-User-Wizard

Possible values:

Character+digits
Characters
Digits

11.9.2 Hide CSV export

This parameter determines whether or not to display the button for exporting information to a CSV file in the Wizard for creating new Public Spot accounts.

SNMP ID:

2.24.19.19

Telnet path:

Setup > Public-Spot-Module > Add-User-Wizard

Possible values:

No
Yes

Default:

No

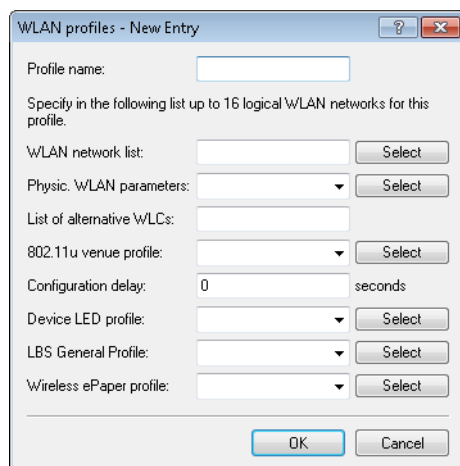
12 WLAN

12.1 Upgrade to 16 SSIDs per WLAN module

As of LCOS version 9.10 IEEE 802.11n WLAN modules support up to 16 SSIDs and IEEE 802.11ac WLAN modules support 15 SSIDs.

WLCs with the LCOS version 9.10 manage up to 16 SSIDs per AP profile.

For each WLAN profile you can specify the following parameters under **WLAN controller > Profiles > WLAN profiles**:




12.2 WLAN disabled by default

As of LCOS version 9.10, all of the WLAN interfaces of the WLAN routers are disabled by default.


12.3 Wildcards for MAC address and SSID filters

As of LCOS version 9.10 wildcards (* and ?) can be used to specify MAC addresses. You can also restrict access by WLAN clients to specific SSIDs.

 In WEBconfig, the new station list replaces the previous station list under **Setup > WLAN > Access-list** (APs) or **Setup > WLAN-management > Access-list** (WLCs).


When updating to the new version, LCOS takes the available values from the existing station list.

Table 10: Overview of all possible traces

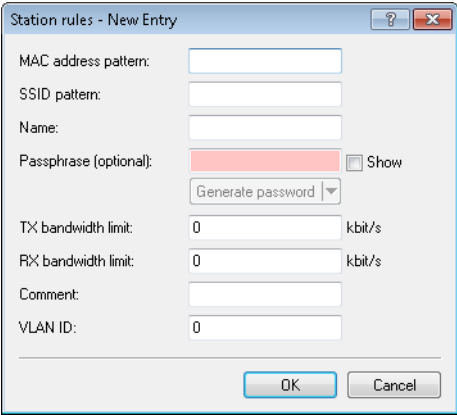
This parametercauses the following message in the trace:
WLAN-ACL	Status messages about MAC filtering rules. <div><div></div><div>The display depends on how the WLAN data trace is configured. If a MAC address is specified there, the trace shows only the filter results relating to that specific MAC address.</div></div>

12.3.1 Access-control list

With the **Access Control List (ACL)** you can permit or prevent individual WLAN clients accessing your WLAN. The decision is based on the MAC address that is permanently programmed into WLAN adapters.

 If you are centrally managing your LANCOM WLAN routers and LANCOM APs with a WLC, you will find the station table under **WLAN controller > Stations** under the button **Stations**.

Check under **Wireless LAN > Stations** to see if the setting **Filter out data from the listed stations, transfer all other** is activated. New stations to be included in your wireless network are added with the button **Stations**.



MAC address pattern

MAC address of the WLAN client for this entry. The following entries are possible:

Individual MAC address


A MAC address in the format 00a057112233, 00-a0-57-11-22-33 or 00:a0:57:11:22:33.

Wildcards

The wildcards '*' and '?' uses to specify MAC address ranges, e.g. 00a057*, 00-a0-57-11-??-?? or 00:a0:?:?:11:.*.

Vendor ID

The device contains a list of the major manufacturer OUIs (organizationally unique identifier). The MAC address range is valid if this entry matches the first three bytes of the MAC address of the WLAN client.

 It is possible to use wildcards.

SSID pattern

WLAN clients with the corresponding MAC addresses have access that is limited to this SSID.



The use of wildcards makes it possible to allow access to multiple SSIDs.

Name

You can enter any name you wish and a comment for any WLAN client. This enables you to assign MAC addresses more easily to specific stations or users.

Passphrase

Here you may enter a separate passphrase for each physical address (MAC address) that is used in a 802.11i/WPA/AES-PSK-secured network. If no separate passphrase is specified for this MAC address, the passphrases stored in the **802.11i/WEP** area will be used for each logical wireless LAN network.

TX bandwidth limit

Transmission-bandwidth restriction for WLAN clients currently authenticating themselves. A WLAN device in client mode communicates its setting to the AP when logging on. This then uses these two values to set the minimum bandwidth.

RX bandwidth limit

Reception-bandwidth restriction for WLAN clients currently authenticating themselves. A WLAN device in client mode communicates its setting to the AP when logging on. This then uses these two values to set the minimum bandwidth.



The RX bandwidth restriction is only active for WLAN devices in client mode. For value is not used by normal WLAN clients.

VLAN-ID

This VLAN ID is assigned to packets that are received from the client with the MAC address entered here. In case of VLAN-ID '0', the station is not assigned a specific VLAN ID. Instead, the VLAN ID of the radio cell (SSID) applies.

If filter rules contradict, the individual rule has a higher priority: A rule without wildcards in the MAC address or SSID takes precedence over a rule with wildcards. When creating these entries, the user should ensure that filter rules do not contradict. The definitions in the filters can be checked in a Telnet session with the trace command `trace WLAN-ACL`.



The filter criteria in the station list either allow or deny WLAN clients to access your wireless network. The entries **Name**, **Bandwidth limit**, **VLAN ID** and **Passphrase** are meaningless if the device uses valid filter criteria to deny access to the WLAN.

12.3.2 Additions to the Setup menu

Access rules

You can limit the data traffic between the wireless LAN and its local network by excluding certain stations from transferring data, or you can approve specific stations only.

SNMP ID:


2.12.89

Telnet path:

Setup > WLAN

MAC address pattern

Enter the MAC address of a station.

 It is possible to use wildcards.

SNMP ID:

2.12.89.1

Telnet path:

Setup > WLAN > Access rules

Possible values:

Max. 20 characters from `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_`~`

Possible arguments:**MAC address**

MAC address of the WLAN client for this entry. The following entries are possible:

Individual MAC address


A MAC address in the format 00a057112233, 00-a0-57-11-22-33 or 00:a0:57:11:22:33.

Wildcards

The wildcards '*' and '?' uses to specify MAC address ranges, e.g. 00a057*, 00-a0-57-11-??-?? or 00:a0:?:?:11:.*.

Vendor ID

The device contains a list of the major manufacturer OUIs (organizationally unique identifier). The MAC address range is valid if this entry matches the first three bytes of the MAC address of the WLAN client.

 It is possible to use wildcards.

Name

You can enter any name you wish for any station. This enables you to assign MAC addresses more easily to specific stations or users.

SNMP ID:

2.12.89.2

Telnet path:

Setup > WLAN > Access rules

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_`~`

Comment

You can enter any comment you wish for any station. This enables you to assign MAC addresses more easily to specific stations or users.

SNMP ID:

2.12.89.3

Telnet path:


Setup > WLAN > Access rules


Possible values:

Max. 30 characters from `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_`~`

WPA passphrase

Here you may enter a separate passphrase for each entry that is used in a 802.11i/WPA/AES-PSK-secured network. If no separate passphrase is specified for this MAC address, the passphrases stored in the **802.11i/WEP** area will be used for each logical wireless LAN network.

 The passphrases should consist of a random string at least 22 characters long, corresponding to a cryptographic strength of 128 bits.

 This field has no significance for networks secured by WEP.

SNMP ID:

2.12.89.4

Telnet path:


Setup > WLAN > Access rules

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_`~`

Tx-Limit

Bandwidth restriction for registering WLAN clients. A client communicates its setting to the AP when logging on. This then uses these two values to set the minimum bandwidth.

 The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an AP Rx stands for "Send data" and Tx stands for "Receive data".

SNMP ID:

2.12.89.5

Telnet path:

Setup > WLAN > Access rules

Possible values:

Max. 9 characters from 0123456789

0 ... 999999999

Default:

0

Special values:

0

No limit

Rx-Limit

Bandwidth restriction for registering WLAN clients. A client communicates its setting to the AP when logging on. This then uses these two values to set the minimum bandwidth.



The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an AP Rx stands for "Send data" and Tx stands for "Receive data".

SNMP ID:

2.12.89.6

Telnet path:**Setup > WLAN > Access rules****Possible values:**

Max. 9 characters from 0123456789

0 ... 999999999

Default:

0

Special values:

0

No limit

VLAN-ID

The device assigns this VLAN ID to packets received by the WLAN client and containing the MAC address entered here.

SNMP ID:

2.12.89.7

Telnet path:**Setup > WLAN > Access rules****Possible values:**

Max. 4 characters from 0123456789

0 ... 4096

Default:

0

Special values:

0

No limit

SSID pattern

For WLAN clients with the appropriate MAC addresses, this entry allows them to access this SSID or it restricts them to it.



The use of wildcards makes it possible to allow access to multiple SSIDs.

SNMP ID:

2.12.89.9

Telnet path:

Setup > WLAN > Access rules

Possible values:

Max. 40 characters from `[A-Z][a-z][0-9]#@{ | } ~ ! $ % & ' () * + - , / : ; < = > ? [\] ^ _ . ``

Special values:

*

Placeholder for any number of characters

?

Placeholder for exactly one character

Default:

empty

Access rules

You can limit the data traffic between the wireless LAN and its local network by excluding certain stations from transferring data, or you can approve specific stations only.

SNMP ID:

2.37.21

Telnet path:

Setup > WLAN-Management

MAC address pattern

Enter the MAC address of a station.



It is possible to use wildcards.

SNMP ID:

2.37.21.1

Telnet path:

Setup > WLAN-Management > Access rules

Possible values:

Max. 20 characters from `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_``

Possible arguments:**MAC address**

MAC address of the WLAN client for this entry. The following entries are possible:

Individual MAC address

A MAC address in the format 00a057112233, 00-a0-57-11-22-33 or 00:a0:57:11:22:33.

Wildcards

The wildcards '*' and '?' uses to specify MAC address ranges, e.g. 00a057*, 00-a0-57-11-??-?? or 00:a0:?:?:11:.*.

Vendor ID

The device contains a list of the major manufacturer OUIs (organizationally unique identifier). The MAC address range is valid if this entry matches the first three bytes of the MAC address of the WLAN client.



It is possible to use wildcards.

Name

You can enter any name you wish for any station. This enables you to assign MAC addresses more easily to specific stations or users.

SNMP ID:

2.37.21.2

Telnet path:

Setup > WLAN-Management > Access rules

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_``

Comment

You can enter any comment you wish for any station. This enables you to assign MAC addresses more easily to specific stations or users.

SNMP ID:

2.37.21.3

Telnet path:

Setup > WLAN-Management > Access rules

Possible values:

Max. 30 characters from `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_`~`

WPA passphrase

Here you may enter a separate passphrase for each entry that is used in a 802.11i/WPA/AES-PSK-secured network. If no separate passphrase is specified for this MAC address, the passphrases stored in the **802.11i/WEP** area will be used for each logical wireless LAN network.



The passphrases should consist of a random string at least 22 characters long, corresponding to a cryptographic strength of 128 bits.



This field has no significance for networks secured by WEP.

SNMP ID:

2.37.21.4

Telnet path:

Setup > WLAN-Management > Access rules

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_`~`

Tx-Limit

Bandwidth restriction for registering WLAN clients. A client communicates its setting to the AP when logging on. This then uses these two values to set the minimum bandwidth.



The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an AP Rx stands for "Send data" and Tx stands for "Receive data".

SNMP ID:

2.37.21.5

Telnet path:

Setup > WLAN-Management > Access rules

Possible values:

Max. 9 characters from 0123456789

0 ... 999999999

Default:

0

Special values:

0

No limit

Rx-Limit

Bandwidth restriction for registering WLAN clients. A client communicates its setting to the AP when logging on. This then uses these two values to set the minimum bandwidth.



The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an AP Rx stands for "Send data" and Tx stands for "Receive data".

SNMP ID:

2.37.21.6

Telnet path:**Setup > WLAN-Management > Access rules****Possible values:**

Max. 9 characters from 0123456789

0 ... 999999999

Default:

0

Special values:

0

No limit

VLAN-ID

The device assigns this VLAN ID to packets received by the WLAN client and containing the MAC address entered here.

SNMP ID:

2.37.21.7

Telnet path:**Setup > WLAN-Management > Access rules****Possible values:**

Max. 4 characters from 0123456789

0 ... 4096

Default:

0

Special values:

0

No limit

SSID pattern

For WLAN clients with the appropriate MAC addresses, this entry allows them to access this SSID or it restricts them to it.



The use of wildcards makes it possible to allow access to multiple SSIDs.

SNMP ID:

2.37.21.9

Telnet path:

Setup > WLAN-Management > Access rules

Possible values:

Max. 40 characters from `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_``

Special values:

*

Placeholder for any number of characters

?

Placeholder for exactly one character

Default:

empty

12.4 Conformity with current ETSI radio standards in the 2.4GHz/5GHz bands

As of LCOS version 9.10, the AP additionally supports the radio standards ETSI EN 300328-V1.7.1, ETSI EN 300328-V1.8.1 and ETSI EN 301893-V1.7.1.

12.4.1 DFS configuration

In LANconfig you access the DFS settings under **Wireless LAN > General**, then click **Physical WLAN settings** and select the **Radio** tab.

Time of DFS rescan

This entry determines at what time (0 - 24h) the device deletes the DFS database and performs a DFS rescan. If this item is left empty, the device only performs a DFS rescan when no further free channel is available. This is the case when the number of channels determined during the initial DFS scan falls below the minimum number of free channels.



The cron command options can be used to define the time: The entry '1,6,13' starts the rescan at 01:00h, 06:00h and 13:00h. The entry '0-23/4' starts a rescan every four hours between 00:00h and 23:00h.

Number of channels to scan

This entry determines the minimum number of free channels that a DFS scan has to achieve. The default value of '2' means that the device performs a DFS scan for as long as it takes to detect 2 free channels. If the device has to switch channels, for example if it detects an active radar pattern, the second channel is immediately available for the change.

A value of '0' disables the restriction. The physical WLAN interface performs a DFS scan on all available channels.

Rescan free channels

With this item you select whether, following the completion of a DFS rescan, the physical WLAN interface deletes occupied channels or saves them for subsequent DFS rescans.

- **Yes:** The physical WLAN interface deletes occupied channels after completing a DFS rescan so that they are available again for a new DFS rescan.
- **No:** The device saves occupied channels after completing a DFS rescan and so that the device immediately skips them during a new DFS rescan.

12.4.2 Additions to the Setup menu

Preferred DFS scheme

In order to operate the WLAN device in accordance with current ETSI radio standards, select the corresponding standard here.



When upgrading a LCOS version to a current radio standard, the previous setting is retained.

SNMP ID:

2.23.20.8.20

Telnet path:

Setup > Interfaces > WLAN > Radio settings > Preferred DFS scheme

Possible values:

EN 301 893-V1.3

EN 301 893-V1.5

EN 301 893-V1.6

EN 301 893-V1.7

Default:

EN 301 893-V1.7

Preferred 2.4 scheme

This parameter sets the version of the EN 300 328 standard operated by the device in the 2.4-GHz band.



Should you carry out a firmware update, the current version is retained. New devices and devices subject to a configuration reset operate version 1.8 by default.

SNMP ID:

2.23.20.8.28

Telnet path:

Setup > Interfaces > WLAN > Radio-settings

Possible values:

EN300328-V1.7

EN300328-V1.8

Default:

EN300328-V1.8

12.5 Time of the DFS rescan configurable via LANconfig

As of LCOS version 9.10, the time for a DFS rescan can be configured in LANconfig.

12.6 P2P support for 802.11ac

As of LCOS version 9.10, 802.11ac modules are also able to establish P2P connections. The distance between two access points can be up to one kilometer (1 km).



The maximum range depends on the antenna system used.

12.7 Client mode for 802.11ac

As of LCOS version 9.10, 802.11ac modules are also able to operate in client mode.

12.8 Bandwidth limit for each WLAN client per SSID

As of LCOS version 9.10, a general bandwidth limit can be applied to all WLAN clients in each SSID.

Client TX bandwidth limit

Here, you set the transmit-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

Client RX bandwidth limit

Here, you set the receive-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

12.8.1 Additions to the Setup menu

Per-Client-Tx-Limit

Here, you set the transmit-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

SNMP ID:

2.23.20.1.23

Telnet path:

Setup > Interfaces > WLAN > Network

Possible values:

Max. 10 characters from 0123456789

Default:

0

Special values:

0

Disables the limit.

Per-Client-Rx-Limit

Here, you set the receive-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

SNMP ID:

2.23.20.1.24

Telnet path:**Setup > Interfaces > WLAN > Network****Possible values:**

Max. 10 characters from 0123456789

Default:

0

Special values:

0

Disables the limit.

12.9 Opportunistic key caching (OKC) adjustable on the client side

As of LCOS version 9.10, the OKC can also be adjusted for devices in client mode.

12.9.1 Additions to the Setup menu

OKC

This option enables or disables the opportunistic key caching (OKC).

The device uses this value only if the interface works in client mode. The interface is in AP mode, the enabling or disabling of OKC is only possible by means of profile management with a WLC.

In the PMK caching status under **Status > WLAN > PMK-Caching > Contents**, OKC PMKs can be identified by the authenticator address `ff:ff:ff:ff:ff:n`, where `n` is the assigned profile number (e.g. 0 for "WLAN-1", 1 for "WLAN1-2", etc.).

SNMP ID:

2.23.20.3.17

Telnet path:**Setup > Interfaces > WLAN > Encryption****Possible values:****Yes****No****Default:****Yes**

12.10 Counter for WPA login attempts

As of LCOS version 9.10, the device stores the number of successful and failed WPA login attempts on each interface.

12.10.1 Additions to the Status menu

Ports

This table provides an overview of the accepted or rejected connection requests for each logical interface.

SNMP ID:**1.46.3****Telnet path:****Status > IEEE802.1x****Port**

Displays the name of the interface.

SNMP ID:**1.46.3.1****Telnet path:****Status > IEEE802.1x > Ports****Num-accept**

Displays the number of successful WPA requests on this interface.

SNMP ID:**1.46.3.2**

Telnet path:**Status > IEEE802.1x > Ports****Num-reject**

Displays the number of failed WPA requests on this interface.

SNMP ID:

1.46.3.3

Telnet path:**Status > IEEE802.1x > Ports****WPA-PSK-Num-Wrong-Passphrase**

Displays the number of WPA requests on this interface that were rejected due to an incorrect passphrase.

SNMP ID:

1.3.64.20

Telnet path:**Status > WLAN > Encryption****WPA-PSK-Num-Success**

Displays the number of successful WPA requests on this interface.

SNMP ID:

1.3.64.21

Telnet path:**Status > WLAN > Encryption****WPA-PSK-Num-Failures**

Displays the number of failed WPA requests on this interface.

SNMP ID:

1.3.64.22

Telnet path:**Status > WLAN > Encryption**

12.11 Point-to-point links via 802.11ac

As of LCOS version 9.10, point-to point links can be established using 802.11ac WLAN modules.



This extension only works if all of the P2P APs involved have LCOS version 9.10. When updating from LCOS to LCOS version 9.10 you should first update the APs that are connected via WLAN (starting with the farthest away and finishing with the update of the nearest) and only then should you update the devices connected by cable.

12.12 Additions to the Setup menu

12.12.1 Channel change delay

Here you specify how long an access point, which has detected a radar, waits until it changes to a different channel.

SNMP ID:

2.12.130.9

Telnet path:

Setup > WLAN > DFS

Possible values:

Max. 3 characters from [0–9]

Default:

0

Special values:

0

The value 0 disables this function.

12.13 Additions to the Status menu

12.13.1 Delete values

SNMP ID:

1.46.99

Telnet path:

Status > IEEE802.1x

13 WLAN management

13.1 AutoWDS operation

13.1.1 Additions to the Status menu

CAPWAP up

Indicates whether CAPWAP is active.

SNMP ID:

1.59.109.2

Telnet path:

Status > WLAN Management > AutoWDS-operation

Possible values:

No
Yes

CAPWAP up again after config

Indicates whether CAPWAP is active again after a successful configuration.

SNMP ID:

1.59.109.3

Telnet path:

Status > WLAN Management > AutoWDS-operation

Possible values:

No
Yes

AutoWDS fallback timer

Displays the value of the AutoWDS fallback timer.

SNMP ID:

1.59.109.4

Telnet path:

Status > WLAN Management > AutoWDS-operation

AutoWDS fallback force deassoc timer

Displays the value of the AutoWDS force deassoc timer.

SNMP ID:

1.59.109.5

Telnet path:

Status > WLAN Management > AutoWDS-operation

CAPWAP continuation timer

Displays the value of the CAPWAP continuation timer.

SNMP ID:

1.59.109.6

Telnet path:

Status > WLAN Management > AutoWDS-operation

CAPWAP silent timer

Displays the value of the CAPWAP silent timer.

SNMP ID:

1.59.109.7

Telnet path:

Status > WLAN Management > AutoWDS-operation

13.2 Disable responses to CAPWAP requests from a WAN connection

As of LCOS version 9.10 it is possible to disable responses to CAPWAP requests from a WAN remote station.

13.2.1 Protection against unauthorized CAPWAP access from the WAN

The WLC or LANCOM router with activated WLC option handles CAPWAP requests from the LAN and the WAN in the same way. In the case of requests from WAN remote stations, it accepts the APs into its AP management and, under certain circumstances, it sends a default configuration. If configured appropriately, the CAPWAP service is no longer available to WAN remote stations, meaning that for WAN remote stations, APs are no longer accepted and configurations are not provisioned.

The configuration is done under **WLAN Controller > General** in the section **Wireless LAN controller**. If the automatic acceptance of new APs is enabled, you can use the feature **Accept new AP over WAN connection** to control whether the CAPWAP service is available to WAN remote stations.

Wireless LAN controller

Here you define the basic parameters for your wireless LAN controller (WLC).

☐ Wireless LAN controller enabled

☒ Automatically accept new APs (Autoaccept)

Accept new AP over WAN connection: No

☐ Automatically provide APs with a default configuration

☐ Synchronize main device password

No
Only via VPN
Yes

No

The device accepts no new APs over the WAN connection.

Only via VPN

The device only accepts new APs if the WAN connection is via VPN.

Yes

The device accepts all new APs over the WAN connection.

13.2.2 Additions to the Setup menu

Allow WAN connections

This item configures the way that the WLC handles requests from the WAN. For example, it is desirable to prevent CAPWAP requests from unknown WAN peers from accidentally assigning a default configuration with internal network settings to these APs.

SNMP ID:

2.37.29

Telnet path:

Setup > WLAN-Management

Possible values:

Yes

When an AP sends a request from the WAN, the WLC includes it into the AP management and, with the appropriate setting, it sends a default configuration.

VPN

When an AP sends a request from the WAN, the WLC includes it into the AP management and, with the appropriate setting, it sends a default configuration only if the WAN connection uses a VPN tunnel.

No

When an AP sends a request from the WAN, the WLC does not include it into the AP management.

Default:

No

13.3 Additional date information for central firmware management

As of LCOS version 9.10, the table for central firmware management by the WLC now contains date information.

13.3.1 Firmware management table

This table is used to store information about which firmware versions are to be operated with which devices (MAC address) and device types.

Device types

Select here the type of device that the firmware version specified here is to be used for.

- Possible values: All or a selection from the list of available devices.
- Default: All

MAC address

Select here the device (identified by its MAC address) that the firmware version specified here is to be used for.

- Possible values: Valid MAC address
- Default: Blank

Version

Firmware version that is to be used for the devices or device types specified here.

- Possible values: Firmware version in the form x.x.x
- Default: Blank

Date

The date allows you to downgrade to a specific firmware version within a release, for example from a Release Upgrade (RU) on an earlier upgrade.

- Possible values: 8 characters from 0123456789 The entry must match the format of the UPX header, e.g. "01092014" for the September 01, 2014.
- Default: Blank

13.3.2 Additions to the Setup menu

Date

Date of the corresponding firmware version.

SNMP ID:

2.37.27.15.5

Telnet path:

Setup > WLAN-Management > Central-Firmware-Management > Firmware-Version-Management

Possible values:

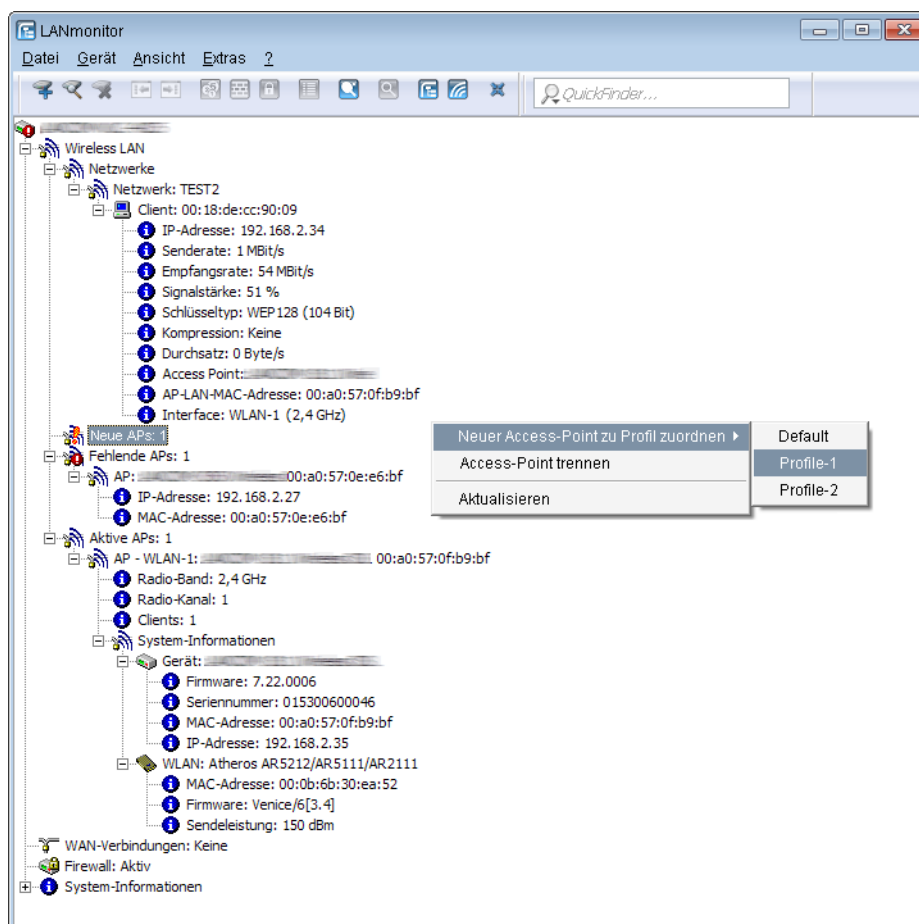
Max. 8 characters from [0-9]

Default:

Corresponds to the UPX header of the firmware (such as "01072014" for the July 01, 2014)

13.4 Display of channel and frequency of clients logged on to the AP

As of LCOS version 9.10, the station table in the WLC additionally displays the channel and frequency of clients logged on to active WLAN networks.



i For APs with an older firmware version and unable to transmit this data, the WLC takes the channel and frequency information from the **Active radios** status table under **Status > Active-Radios > WLAN-Management > AP-Status**.

13.4.1 Additions to the Status menu

Radio band

This value displays the radio band used by the client that is logged in to the AP.

SNMP ID:

1.73.100.27

Telnet path:**Status > WLAN-Management > Station-table****Possible values:****0**

Unknown

2.4GHz

The client is using the 2.4GHz band.

5GHz

The client is using the 5GHz band.

Radio channel

This value displays the radio channel used by the client that is logged in to the AP.

SNMP ID:

1.73.100.28

Telnet path:**Status > WLAN-Management > Station-table****Possible values:**

1 ... 140

13.5 Using LANconfig to backup certificates

As of LCOS version 9.10, LANconfig is fully able to backup and upload certificates.

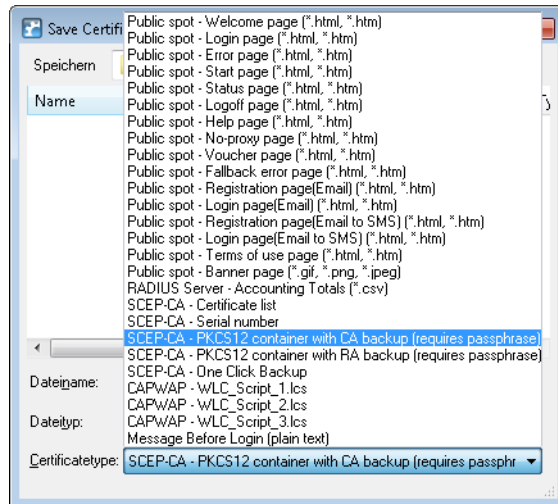
13.5.1 Using LANconfig to backup and restore certificates

Certificates are stored and uploaded with LANconfig as follows:

Save

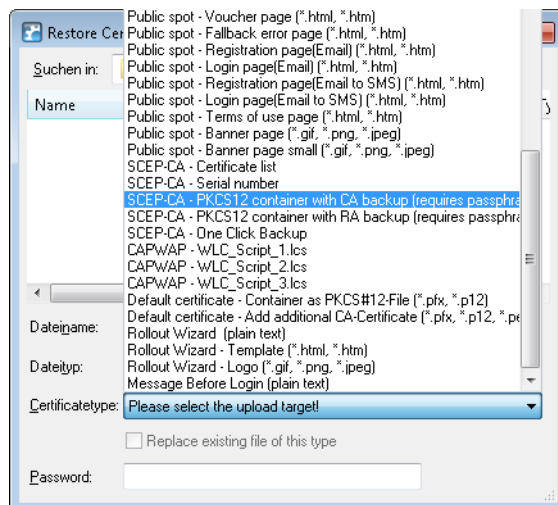
1. Highlight the WLC in the device view section and in the menu select **Device > Configuration management** and the item **Save certificate as file**.

2. Set the **Certificate type** to PKCS12 container and click **Save**.



Upload

1. Highlight the WLC in the device view section and in the menu select **Device > Configuration management** and the item **Upload certificate or file**.
2. Set the **Certificate type** to PKCS12 container.
3. Now navigate to the desired file, enter the password if necessary and click **Open**.



One Click Backup

For the One Click Backup, select the entry "SCEP-CA - One Click Backup" from the dialog list.

13.6 Displaying the certificate status of an AP

As of LCOS version 9.10, an AP transmits its certificate status to the WLC.

13.6.1 Additions to the Status menu

Certificate status

Displays the status of the APs.

SNMP ID:

1.73.9.3.9

Telnet path:

Status > WLAN-Management > AP-Status > New-AP

Possible values:

0

Unknown (default for APs with older firmware)

1

Missing

2

Expired

3

Incompatible (certificate does not match the CA chain of the WLC)

4

Still not valid (e.g. if clocks in the WLC and AP are not synchronized)

5

Valid

13.7 On/off switch for AP LEDs per WLC

As of LCOS version 9.10, the device LEDs of every AP in a multi-AP environments can be separately configured on a WLC.

For each WLAN profile you can specify the following parameters under **WLAN controller > Profiles > WLAN profiles**:

WLAN profiles - New Entry

Profile name:

Specify in the following list up to 16 logical WLAN networks for this profile.

WLAN network list:

Physic. WLAN parameters:

List of alternative WLCs:

802.11u venue profile:

Configuration delay: seconds

Device LED profile:

LBS General Profile:

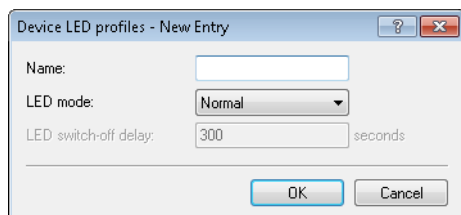
Wireless ePaper profile:

Device LED profile

The device LED profile selected here applies to the WLAN profile. To manage the devices LED profiles, see **WLAN controller > Profiles > Device LED profiles**.

13.7.1 Device LED profiles

The LEDs on the device are configurable so that you can, for instance, operate an AP while drawing a minimum of attention to it. In order to perform this configuration by WLC, you need to create the corresponding profile under **WLAN Controller > Profiles > Device LED profiles** and assign this to a WLAN profile.



Name

Give a name to the device LED profile here.

LED mode

The following options are available:

- **Normal:** The LEDs are always enabled, also after rebooting the device.
- **Timed off:** After a reboot, the LEDs are enabled for a certain period of time and are then turned off. This is useful for the LEDs to indicate critical errors during the restart process.
- **All off:** The LEDs are all off. Even after restarting the device, the LEDs remain off.

LED switch-off delay

The **Timed off** option uses the setting in the field **LED switch-off delay** in seconds to control the time before the LEDs are disabled after a restart.

13.7.2 Additions to the Setup menu

LED profiles

The LEDs on the device are configurable so that you can, for instance, operate an AP while drawing a minimum of attention to it. In order to perform this configuration by WLC, you need to create the corresponding profile and assign this to a WLAN profile.

SNMP ID:

2.37.1.21

Telnet path:

Setup > WLAN-Management > AP-Configuration

Name

Give a name to the device LED profile here.

SNMP ID:

2.37.1.21.1

Telnet path:**Setup > WLAN-Management > AP-Configuration > LED-Profiles****Possible values:**

Max. 31 characters from [A-Z][a-z][0-9]

Default:*empty***LED mode**

Set the operating mode for the LEDs here.

SNMP ID:

2.37.1.21.4

Telnet path:**Setup > WLAN-Management > AP-Configuration > LED-Profiles****Possible values:****On**

The LEDs are always enabled, also after rebooting the device.

Off

The LEDs are all off. Even after restarting the device, the LEDs remain off.

Timed off

After a reboot, the LEDs are enabled for a certain period of time and are then turned off. This is useful for the LEDs to indicate critical errors during the restart process.

Default:

On

LED off secondsIn the operating mode **Timed off** you can specify the delay in seconds after which the LEDs are disabled following a restart. This is useful for the LEDs to indicate critical errors during the restart process.**SNMP ID:**

2.37.1.21.5

Telnet path:**Setup > WLAN-Management > AP-Configuration > LED-Profiles**

Possible values:

Max. 4 characters from [0–9]

Default:

300

LED profiles

The device LED profile selected here applies to the WLAN profile.

SNMP ID:

2.37.1.3.8

Telnet path:

Setup > WLAN-Management > AP-Configuration > Commonprofiles

Possible values:

Max. 31 characters from [A–Z] [a–z] [0–9]

Default:

empty

13.7.3 Additions to the Status menu

LED profiles

This entry displays the existing LED profiles.

SNMP ID:

1.59.110

Telnet path:

Status > WLAN-Management

LED profiles

Displays information about the LED profiles.

SNMP ID:

1.73.2.23

Telnet path:

Status > WLAN-Management > AP-Configuration

Name

Contains the name of the LED profile.

SNMP ID:

1.73.2.23.1

Telnet path:

Status > WLAN-Management > LED-Profiles >

Possible values:

Max. 31 characters from [A-Z][a-z][0-9]

Default:

empty

LED mode

Indicates the LED mode.

SNMP ID:

1.73.2.23.4

Telnet path:

Status > WLAN-Management > LED-Profiles >

Possible values:**On**

The LEDs are always enabled, also after rebooting the device.

Off

The LEDs are all off. Even after restarting the device, the LEDs remain off.

Timed off

After a reboot, the LEDs are enabled for a certain period of time and are then turned off. This is useful for the LEDs to indicate critical errors during the restart process.

LED off seconds

In the operating mode **Timed off** this column indicates after how many seconds the device disables the LEDs after a restart.

SNMP ID:

1.73.2.23.5

Telnet path:

Status > WLAN-Management > LED-Profiles >

Possible values:

Max. 4 characters from [0–9]

Default:

300

LED profiles

This column indicates the assigned LED profile.

SNMP ID:

1.73.2.3.8

Telnet path:

Status > WLAN-Management > AP-Configuration > Commonprofiles

Possible values:

Max. 31 characters from [A–Z] [a–z] [0–9]

Default:

empty

LED prof. errors

Contains the error codes displayed by the device LEDs.

SNMP ID:

1.73.2.22

Telnet path:

Status > WLAN-Management > AP-Configuration

Index

Contains the sequential index of the error messages.

SNMP ID:

1.73.2.22.1

Telnet path:

Status > WLAN-Management > AP-Configuration > LED-Prof.-Errors

Index

Contains the name of the LED profile.

SNMP ID:

1.73.2.22.2

Telnet path:

Status > WLAN-Management > AP-Configuration > LED-Prof.-Errors

Error

Contains the error that occurred.

SNMP ID:

1.73.2.22.3

Telnet path:

Status > WLAN-Management > AP-Configuration > LED-Prof.-Errors

Possible values:**None**

No error

Inheritance error

No profile

Profile not found

No memory

SSID missing

Network not found

AP parameters not found

AP intranet not found

RADIUS profile not found

AutoWDS profile not found

Master equal to slave

No profile either Group found

Info profiles WINS group

Group wrong defined

SSID WLC tunnel missing

SSID inter-station traffic allowed

Too many networks for AutoWDS

Reported by AP

13.8 Managing Wireless-ePaper and iBeacon profiles with WLCs

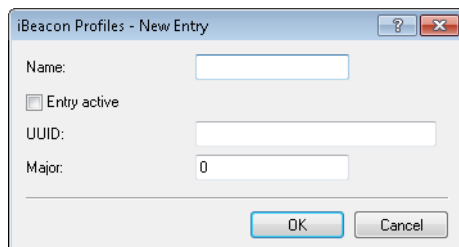
As of LCOS version 9.10, it is possible to create and distribute Wireless-ePaper and iBeacon profiles for E-series access points.

13.8.1 ESL- and iBeacon profiles

In order to use a WLC to manage the settings of the Wireless ePaper information and iBeacon information of the individual APs, you create the corresponding profiles for Wireless ePaper and iBeacon via **WLAN-Controller > AP-Configuration** with the button **Extended settings**.



The button **iBeacon profiles** is used to create iBeacon profiles for the assignment groups and the AP table, which specify the iBeacon information to be broadcast by the individual APs.



Name

Name of the profile

Entry active

Activates or deactivates this profile.

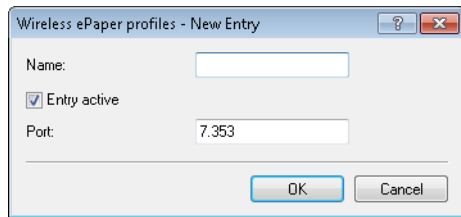
UUID

Unique identification of the transmitter

Major

Specifies the Major value of the iBeacon.

The button **Wireless ePaper profiles** is used to create Wireless ePaper profiles for the WLAN-profiles table, which specify the Wireless ePaper information to be broadcast by the individual APs.



Name

Name of the profile

Entry active

Activates or deactivates this profile.

Port

Specifies the port.

13.8.2 Additions to the Setup menu

iBeacon

This entry allows you to configure the iBeacon module.

SNMP ID:

2.23.90.1

Telnet path:

Setup > Interfaces > Bluetooth

UUID

This entry allows you to assign a "universally unique identifier" (UUID) to the iBeacon module.

SNMP ID:

2.23.90.1.2

Telnet path:

Setup > Interfaces > Bluetooth > iBeacon

Possible values:

Max. 36 characters from `[0-9][a-f][A-F]-`

Default:

00000000-0000-0000-0000-000000000000

Major

Assign a unique major ID to the iBeacon module.

SNMP ID:

2.23.90.1.3

Telnet path:

Setup > Interfaces > Bluetooth > iBeacon

Possible values:

Max. 5 characters from [0–9]

1 ... 65535 Integer value

Default:

2002

Minor

Assign a unique minor ID to the iBeacon module.

SNMP ID:

2.23.90.1.4

Telnet path:

Setup > Interfaces > Bluetooth > iBeacon

Possible values:

Max. 5 characters from [0–9]

1 ... 65535 Integer value

Default:

1001

Reception power shift

Specify the reception power shift.

SNMP ID:

2.23.90.1.5

Telnet path:

Setup > Interfaces > Bluetooth > iBeacon

Possible values:

Max. 4 characters from [0–9] –

-128 ... 127

Default:

0

Transmission power

Set the transmission power of the iBeacon module.

SNMP ID:

2.23.90.1.6

Telnet path:**Setup > Interfaces > Bluetooth > iBeacon****Possible values:****Low**

The module sends with minimum power.

Medium

The module sends with medium power.

High

The module sends with maximum power.

Default:

High

Channel/channels

Set which channels the iBeacon module should use to transmit.

SNMP ID:

2.23.90.1.7

Telnet path:**Setup > Interfaces > Bluetooth > iBeacon****Possible values:****2402MHz**

The module transmits on channel 2402.

2426MHz

The module transmits on channel 2426.

2480MHz

The module transmits on channel 2480.

2402MHz, 2426MHz, 2480MHz

The module transmits on all channels.

Default:

2402MHz, 2426MHz, 2480MHz

Coexistence

Specify here whether iBeacon is to be operated in parallel with the Wireless ePaper service.

SNMP ID:

2.23.90.1.8

Telnet path:

Setup > Interfaces > Bluetooth > iBeacon

Possible values:

No
Yes

Default:

Yes

Wireless ePaper

Configure the settings for the Wireless ePaper module here.

SNMP ID:

2.88

Telnet path:

Setup

Port

Assign a port to the Wireless ePaper module.

SNMP ID:

2.88.2

Telnet path:

Setup > Wireless-ePaper

Possible values:

Max. 5 characters from [0-9]

Default:

2002

Channel

Set which channel the Wireless ePaper module should use.

SNMP ID:

2.88.3

Telnet path:**Setup > Wireless-ePaper****Possible values:**

2404MHz
2410MHz
2422MHz
2425MHz
2442MHz
2450MHz
2462MHz
2470MHz
2474MHz
2477MHz
2480MHz
Auto

Default:

2425MHz

13.9 The modules iBeacon and Wireless ePaper have an additional "Managed" mode

As of LCOS version 9.10 you can operate the iBeacon/BLE and Wireless ePaper modules in "Managed" mode.



Existing configurations continue to run in the "Manual" mode and the corresponding module uses the local configuration. New configurations start in the "Managed" mode. In this case it is necessary for the configuration to be carried out by a WLAN controller.

13.9.1 Additions to the Setup menu

iBeacon

This entry allows you to configure the iBeacon module.

SNMP ID:

2.23.90.1

Telnet path:**Setup > Interfaces > Bluetooth****Operating**

This entry allows you to set the operating mode of the module.

SNMP ID:

2.23.90.1.1

Telnet path:**Setup > Interfaces > Bluetooth > iBeacon****Possible values:****Off**

The module is not enabled.

Manual

iBeacon configurations are done manually.

Managed

The module is managed by a WLAN controller.

Default:

Managed

Wireless ePaper

Configure the settings for the Wireless ePaper module here.

SNMP ID:

2.88

Telnet path:**Setup****Operating**

This entry allows you to set the operating mode of the module.

SNMP ID:

2.88.1

Telnet path:**Setup > Wireless-ePaper****Possible values:****Off**

The module is not enabled.

Manual

Wireless ePaper configurations are done manually.

Managed

The module is managed by a WLAN controller.

Default:

Manual

13.10 WLAN profiles divided into basic and advanced profiles

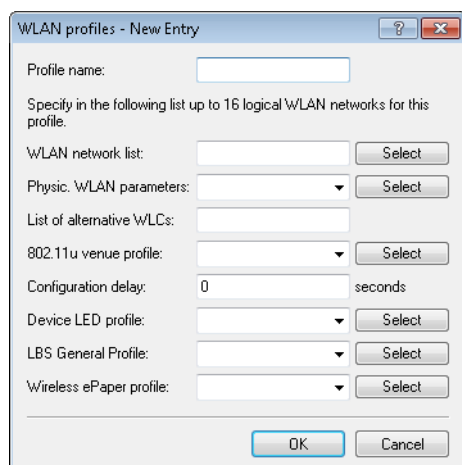
As of LCOS version 9.10, LANconfig can be used to configure advanced profiles of a WLC under **WLAN controller > Profiles**, for example to manage profiles for the location-based services (LBS).

13.11 General LBS profile and device location profile

As of LCOS version 9.10, you can create and map LBS servers and device location profiles for WLAN profiles on WLCs.

These profiles are mapped to WLAN profiles as follows:

For each WLAN profile you can specify the following parameters under **WLAN controller > Profiles > WLAN profiles**:

**LBS general profile**

The general LBS profile selected here applies to the WLAN profile. You select the general LBS profile under **WLAN Controller > Profiles > Advanced profiles** with the button **LBS - General**.

The AP table is a central element of the configuration for WLCs. Here, the WLC assigns WLAN profiles (i.e. the combinations of logical and physical WLAN parameters) to the APs via their MAC addresses. Furthermore, the existence of an entry in the AP table for a specific AP affects its ability to connect to a WLC. Under **WLAN Controller > AP Configuration > Access Point Table** you can define the following parameters for each AP:

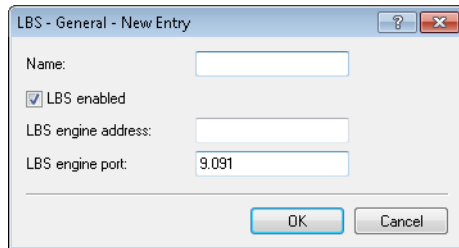
LBS AP location profile

LBS location profile from the list of defined profiles.

13.11.1 General LBS profile and device location profile

In order to conveniently manage the settings for location-based services servers (LBS) and the AP locations by means of a WLC, you create the appropriate profiles for LBS servers and AP device locations via the menu **WLAN Controller > Profiles** and the button **Advanced profiles**.

The button **LBS - General** opens the dialog for creating a general LBS server profile.

**Name**

Enter a descriptive name for the profile.

LBS enabled

Enable or disable LBS.

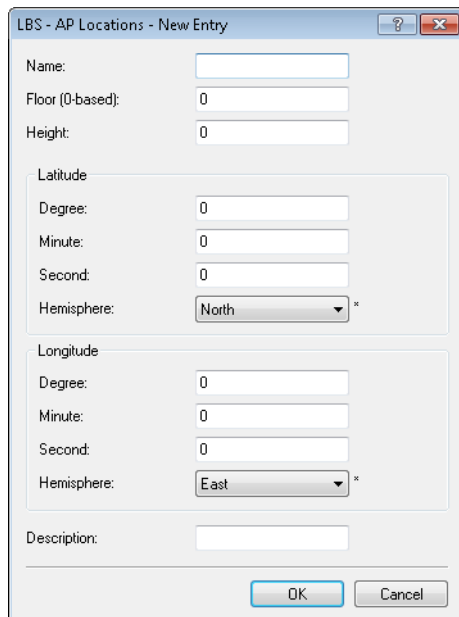
LBS server address

Enter the address of the LBS server.

LBS server port

Enter the port used by the LBS server (default: 9091).

The button **LBS - AP locations** opens the dialog for creating a location profile for the LBS APs.

**Name**

Enter a descriptive name for the profile.

Floor (0-based)

Here you enter the floor on which the device is located. This allows you to differentiate between the top floor and bottom floor, for example.

Height

Here you enter the height of the device installation. It is possible to specify a negative value so that you can differentiate between a location above and below sea level.

Degrees (latitude)

This field specifies the angle in degrees of the geographic coordinate system.

Minutes (latitude)

This field specifies the minutes of the geographic coordinate system.

Seconds (latitude)

This field specifies the seconds of the geographic coordinate system.

Hemisphere (latitude)

This field specifies the orientation of the geographic coordinate system. The following values are possible for geographical latitude:

- North: Northerly latitude
- South: Southerly latitude

Degrees (longitude)

This field specifies the angle in degrees of the geographic coordinate system.

Minutes (longitude)

This field specifies the minutes of the geographic coordinate system.

Seconds (longitude)

This field specifies the seconds of the geographic coordinate system.

Hemisphere (longitude)

This field specifies the orientation of the geographic coordinate system. The following values are possible for geographical longitude:

- East: Easterly longitude
- West: Westerly longitude

Description

Enter a description of the device.

13.11.2 Additions to the Status menu

Common profiles

This column indicates the assigned LBS general profile.

SNMP ID:

1.73.2.3

Telnet path:

Status > WLAN-Management > AP-Configuration > Commonprofiles

13.11.3 Additions to the Setup menu

LBS general profile

The LBS general profile selected here applies to the WLAN profile.

SNMP ID:

2.37.1.3.9

Telnet path:**Setup > WLAN-Management > AP-Configuration > Commonprofiles****Possible values:**Max. 31 characters from `[A-Z][a-z][0-9]`**Default:***empty*

13.12 Additions to the Status menu

13.12.1 Acquire statistical data

This entry indicates whether the device collects statistical data.

SNMP ID:

1.73.123.9

Telnet path:**Status > WLAN-Management > Client-Steering****Possible values:****Yes**

The device collects statistical data.

No

The device does not collect statistical data.

13.13 WLC Clustering Wizard

As of LCOS version 9.10 it is possible to use the Clustering Wizard in LANconfig to configure the WLCs all at once.



With WLCs equipped with the "WLC High Availability Clustering XL option" you are able to select all of the listed WLCs and configure them all in one go using the WLC Clustering Wizard (see [1-Click WLC High Availability Clustering Wizard](#)).

14 VPN

14.1 SCEP-CA function in VPN environments

As of LCOS version 9.10, it is possible to use the existing CA with SCEP function in the VPN environment.

14.2 SCEP algorithms updated

As of LCOS version 9.10, the SCEP client and server additionally support AES192 and AES256 and also SHA256, SHA384, and SHA512.



The default entries remain unchanged so as to maintain compatibility with the remote stations in the event of a firmware update. Only use the latest algorithms when the remote stations have also been updated accordingly.

14.2.1 Configuring the CAs

The configuration is carried out with LANconfig under **Certificates > SCEP client** with the button **CA table**.

Name

Configuration name of the CA.

URL

URL of the CA.

Distinguished name

Distinguished name of the CA. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration.

You can also use reserved characters by using a preceding backslash ("\"). The supported reserved characters are:

- Comma (",")
- Slash ("/")
- Plus ("+")
- Semicolon (";")
- Equals ("=")

You can also use the following internal firmware variables:

- %% inserts a percent sign.
- %f inserts the version and the date of the firmware currently active in the device.
- %r inserts the hardware release of the device.
- %v inserts the version of the loader currently active in the device.
- %m inserts the MAC address of the device.
- %s inserts the serial number of the device.
- %n inserts the name of the device.
- %l inserts the location of the device.
- %d inserts the type of the device.

Identifier

CA identifier (as required by some web server to identify the CA).

Encryption algorithm

This algorithm encrypts the payload of the certificate request. Possible values are:

- DES (Default)
- 3-DES
- Blowfish
- AES128
- AES192
- AES256

Signature algorithm

The certificate request is signed with this algorithm. Possible values are:

- MD5 (default)
- SHA1
- SHA256
- SHA384
- SHA512

Fingerprint algorithm

Algorithm for signing the fingerprint. This determines whether the CA certificate is to be checked by means of fingerprint, and which algorithm is used for this. The CA fingerprint has to agree with the checksum which results when this algorithm is applied. Possible values are:

- Off (default)
- MD5
- SHA1
- SHA256
- SHA384
- SHA512

Fingerprint

The authenticity of a received CA certificate can be checked by means of the the checksum (fingerprint) entered here (corresponding to the set CA fingerprint algorithm).

Usage type

Indicates the intended application of the specified CA. The CA entered here is only queried for the corresponding application. Possible values are:

- VPN
- EAP/TLS
- WLAN controller
- General



If a general CA exists no further CAs can be configured. Otherwise the choice of CA would be unclear.

RA autoapprove

Some CAs provide the option of using an earlier certificate issued by this CA as proof of authenticity for future requests. This option defines whether an existing system certificate should be used to sign new requests. Possible values are:

- Yes
- No (Default)

Source address

This is where you configure an optional source address to be used instead of the one otherwise automatically selected for the source address. If you have configured loopback addresses, you can specify them here as source address.

You can enter an address in various forms:

- Name of the IP network (ARF network), whose address should be used.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ (Note: If there is an interface named "DMZ", its address will be taken).
- LB0 ... LBF for one of the 16 loopback addresses or its name
- Furthermore, any IP address can be entered in the form x.x.x.x.



If the source address set here is a loopback address, these will be used unmasked on the remote client.

14.2.2 Additions to the Setup menu

Enc-Alg

The encryption algorithm is specified here as used by the SCEP protocol (Simple Certificate Enrollment Protocol). Both the certification authority (CA) and the certificate holder (client) must support the algorithm. A number of methods are available:



If possible you should employ one of the last methods (3DES, BLOWFISH, AES) if the certification authority (CA) and all the clients support it. The default value here is DES encryption to ensure interoperability.

SNMP ID:

2.39.1.14.4

Telnet path:**Setup > Certificates > SCEP-Client > CAs****Possible values:****DES**

Data Encryption Standard: The DES algorithm uses a 64-bit key. This is the SCEP standard encryption. DES is an algorithm developed by the National Bureau of Standards (NBS) in the USA. The DES algorithm uses a 64-bit key which allows combinations of a substitution cipher, transposition cipher and exclusive-OR (XOR) operations. The 64-bit block size consists of an effective key length of 56 bits and 8 parity bits. The algorithm is based on the Lucifer cipher.

3DES

Triple-DES: This is an improved method of DES encryption using two keys of 64-bits in length.

BLOWFISH

The BLOWFISH algorithm works with a variable key length of between 32 and 448 bits. It is a fast and highly secure algorithm. It has major advantages over other symmetrical methods such as DES and 3DES.

AES

Advanced Encryption Standard: The AES algorithm has a variable block size of 128, 192 or 256 bits and a variable key length of 128, 192 or 256 bits, providing a very high level of security.

Default:

DES

CA signature algorithm

Here you select the signature algorithm used by the Certificate Authority (CA) to sign the certificate. This method must be supported by the certification authority (CA) and the certificate recipient (client) as the client uses this signature to check the integrity of the certificate. Two cryptographic hash functions are relatively widespread.

SNMP ID:

2.39.1.14.6

Telnet path:**Setup > Certificates > SCEP-Client > CAs****Possible values:****MD5**

Message Digest Algorithm 5: The MD5 algorithm generates a 128-bit hash value. MD5 was developed in 1991 by Ronald L. Rivest. The results reveal no conclusive information about the key. This method takes a message of any length to generate a 128-bit message digest, which is attached to the unencrypted message. The recipient compares the message digest with that determined from the information.

SHA1

Secure Hash Algorithm 1: The SHA1 algorithm generates a 160-bit hash value. This is used to calculate a unique checksum for any data. Generally this data makes up messages. It is practically impossible to come across two messages with exactly the same SHA value.

SHA256

Like SHA1 but with a 256-bit hash value.

SHA384

Like SHA1 but with a 384-bit hash value.

SHA512

Like SHA1 but with a 512-bit hash value.

Default:

MD5

CA fingerprint algorithm

Here you select the fingerprint algorithm that the Certificate Authority (CA) uses to calculate the signature's fingerprint. Both the certification authority (CA) and the certificate holder (client) must support the algorithm.

The fingerprint is a hash value of data (key, certificate, etc.), i.e. a short number string that can be used to check the integrity of the data.

SNMP ID:

2.39.1.14.8

Telnet path:

Setup > Certificates > SCEP-Client > CAs

Possible values:

Off

MD5

Message Digest Algorithm 5: The MD5 algorithm generates a 128-bit hash value. MD5 was developed in 1991 by Ronald L. Rivest. The results reveal no conclusive information about the key. This method takes a message of any length to generate a 128-bit message digest, which is attached to the unencrypted message. The recipient compares the message digest with that determined from the information.

SHA1

Secure Hash Algorithm 1: The SHA1 algorithm generates a 160-bit hash value. This is used to calculate a unique checksum for any data. Generally this data makes up messages. It is practically impossible to come across two messages with exactly the same SHA value.

SHA256

Like SHA1 but with a 256-bit hash value.

SHA384

Like SHA1 but with a 384-bit hash value.

SHA512

Like SHA1 but with a 512-bit hash value.

Default:

MD5

Encryption algorithm

The encryption algorithm is specified here as used by the SCEP protocol (Simple Certificate Enrollment Protocol). Both the certification authority (CA) and the certificate holder (client) must support the algorithm. A number of methods are available:



If possible you should employ one of the last methods (3DES, BLOWFISH, AES) if the certification authority (CA) and all the clients support it. The default value here is DES encryption to ensure interoperability.

SNMP ID:

2.39.2.3

Telnet path:**Setup > Certificates > SCEP-CA****Possible values:****DES**

Data Encryption Standard: The DES algorithm uses a 64-bit key. This is the SCEP standard encryption. DES is an algorithm developed by the National Bureau of Standards (NBS) in the USA. The DES algorithm uses a 64-bit key which allows combinations of a substitution cipher, transposition cipher and exclusive-OR (XOR) operations. The 64-bit block size consists of an effective key length of 56 bits and 8 parity bits. The algorithm is based on the Lucifer cipher.

3DES

Triple-DES: This is an improved method of DES encryption using two keys of 64-bits in length.

BLOWFISH

The BLOWFISH algorithm works with a variable key length of between 32 and 448 bits. It is a fast and highly secure algorithm. It has major advantages over other symmetrical methods such as DES and 3DES.

AES

Advanced Encryption Standard: The AES algorithm has a variable block size of 128, 192 or 256 bits and a variable key length of 128, 192 or 256 bits, providing a very high level of security.

Default:

DES

Signature algorithm

Here you select the signature algorithm used by the Certificate Authority (CA) to sign the certificate. This method must be supported by the certification authority (CA) and the certificate recipient (client) as the client uses this signature to check the integrity of the certificate. Two cryptographic hash functions are relatively widespread.

SNMP ID:

2.39.2.6

Telnet path:**Setup > Certificates > SCEP-CA****Possible values:****MD5**

Message Digest Algorithm 5: The MD5 algorithm generates a 128-bit hash value. MD5 was developed in 1991 by Ronald L. Rivest. The results reveal no conclusive information about the key. This method takes a message of any length to generate a 128-bit message digest, which is attached to the unencrypted message. The recipient compares the message digest with that determined from the information.

SHA1

Secure Hash Algorithm 1: The SHA1 algorithm generates a 160-bit hash value. This is used to calculate a unique checksum for any data. Generally this data makes up messages. It is practically impossible to come across two messages with exactly the same SHA value.

SHA256

Like SHA1 but with a 256-bit hash value.

SHA384

Like SHA1 but with a 384-bit hash value.

SHA512

Like SHA1 but with a 512-bit hash value.

Default:

MD5

Fingerprint algorithm

Here you select the fingerprint algorithm that the Certificate Authority (CA) uses to calculate the signature's fingerprint. Both the certification authority (CA) and the certificate holder (client) must support the algorithm.

The fingerprint is a hash value of data (key, certificate, etc.), i.e. a short number string that can be used to check the integrity of the data.

SNMP ID:

2.39.2.7

Telnet path:**Setup > Certificates > SCEP-CA****Possible values:****MD5**

Message Digest Algorithm 5: The MD5 algorithm generates a 128-bit hash value. MD5 was developed in 1991 by Ronald L. Rivest. The results reveal no conclusive information about the key. This method

takes a message of any length to generate a 128-bit message digest, which is attached to the unencrypted message. The recipient compares the message digest with that determined from the information.

SHA1

Secure Hash Algorithm 1: The SHA1 algorithm generates a 160-bit hash value. This is used to calculate a unique checksum for any data. Generally this data makes up messages. It is practically impossible to come across two messages with exactly the same SHA value.

SHA256

Like SHA1 but with a 256-bit hash value.

SHA384

Like SHA1 but with a 384-bit hash value.

SHA512

Like SHA1 but with a 512-bit hash value.

Default:

MD5

14.3 Loopback address for L2TP connections

As of LCOS version 9.10 it is possible to specify a loopback address for L2TP connections.



If a loopback address is entered as the source address and the routing tag has a value of "0", the device uses the routing tag of the loopback address.

14.3.1 Additions to the Setup menu

Source address

Here you can optionally specify a loopback address for the device to use as the target address instead of the one that would normally be selected automatically.



If the list of IP networks or source addresses contains an entry named 'DMZ', then the associated IP address will be used.



If the source address set here is a loopback address, this will be used unmasked even on masked remote clients.

SNMP ID:

2.2.35.10

Telnet path:

Setup > WAN > L2TP-Endpoints

Possible values:**Valid entry from the list of possible addresses.**

Name of the IP networks whose addresses are to be used.

"INT" for the address of the first intranet

"DMZ" for the address of the first DMZ
 LBO to LBF for the 16 loopback addresses
 Any valid IP address
empty

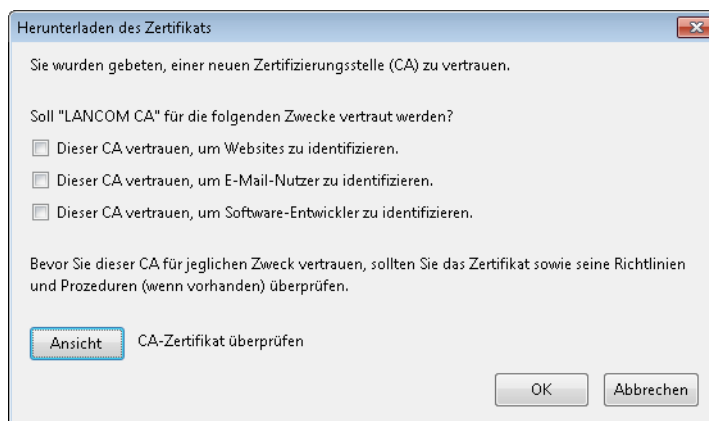
Default:


14.4 Download link for the public portion of the CA certificate

As of LCOS version 9.10, the public part of the CA certificate is available by means of a download link.

14.4.1 Download link for the public portion of the CA certificate

You can download the public part of the CA certificate without having to authenticate by using the link `http://<URL>/getcacert/cacert.crt`. The transmission uses the MIME type `application/x-x509-ca-cert`, so that software with the appropriate functionality will immediately offer to install the certificate.



 The download is only possible if the CA is enabled. An error message appears if the CA is disabled.

If the CA is enabled, WEBconfig is also able to download the certificate under **Extras > Download current CA certificate**.

14.5 Configurable one-time password (OTP) for SCEP-CA

As of LCOS version 9.10, it is also possible to create one-time passwords (OTP) for SCEP-CA.

14.5.1 Configuring challenge passwords

In LANconfig, you configure the certificate parameters under **Certificates > Certificate handling** in the section **Certificate issuing**.

Certificate issuing

Here you set the certificate parameters as used by the CA for the SCEP client.

Validity period: days

General challenge password:

This table can be used for setting further parameters for the challenge password.

Here you set the security features employed by the CA.

Validity period

Here you specify the validity period of the certificate in days.

General challenge password

An additional "Password" can be entered here, which is transmitted to the CA. This can be used by default to authenticate revocation requests. If CAs operate Microsoft-SCEP (mscep), the one-time passwords issued by the CA can be entered here for the authentication of requests.

The **Challenge table** contains the certificate recipients' (clients') own passwords.

Challenge table - New Entry

Distinguished name:

MAC address:

Challenge:

Validity:

Distinguished name

The "Distinguished name" must be entered here. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration. Separated by commas or forward slashes, this is a list where the name, department, state and country can be specified for the gateway. The following are examples of how an entry might appear: CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE

MAC address

Enter the MAC address of the client whose password is to be managed by the challenge-password table.

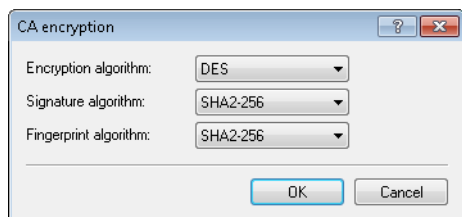
Challenge

Enter the challenge (password) for the client here.

Validity

Enter the validity period of the password here. By selecting "one-time" the password becomes a one-time password (OTP) so that, for example, it can only be used for authentication once.

Under **CA encryption** you configure the security parameters for the CA encryption.



Encryption algorithm

The encryption algorithm is specified here as used by the SCEP protocol. Both the certification authority (CA) and the certificate holder (client) must support the algorithm. The following methods are available:

- DES
- 3DES
- BLOWFISH
- AES128
- DES192
- DES256

Signature algorithm

Here you select the signature algorithm used by the Certificate Authority (CA) to sign the certificate. This method must be supported by the CA and the certificate recipient (client) as the client uses this signature to check the integrity of the certificate. The following cryptographic hash functions are available for selection:

- MD5
- SHA1
- SHA2-256
- SHA2-384
- SHA2-512

Fingerprint algorithm

Here you select the fingerprint algorithm that the Certificate Authority (CA) uses to calculate the signature's fingerprint. Both the CA and the certificate recipient (client) must support the method.

The fingerprint is a hash value of data (key, certificate, etc.), i.e. a short number string that can be used to check the integrity of the data. The following cryptographic hash functions are available for selection:

- MD5
- SHA1
- SHA2-256
- SHA2-384
- SHA2-512

14.5.2 Additions to the Setup menu

Challenge

Enter the validity period of the password here. By selecting "one-time" the password becomes a one-time password (OTP), so it can only be used for authentication once.

SNMP ID:

2.39.2.5.3.5

Telnet path:

Setup > Certificates > SCEP-CA > CA-certificates > Challenge-Passwords

Possible values:

One-time
Permanent

Default:

Permanent

14.6 Deleting VPN error messages in the status table

As of LCOS version 9.10 the device automatically deletes VPN-connection error messages from the status table after a defined period. By default, this option is disabled (time = 0 minutes).

By default, the device retains the VPN error messages in the status table. Depending on the installation LANmonitor may display a large number of open error messages, which clutters the display. For this reason the WEBconfig setting under **Setup > Config > Error-Aging-Minutes** enables you to define a period of time in minutes after which the device automatically deletes these error messages from the status table.



To document sporadic errors, disable this option with the entry 0.

14.6.1 Additions to the Setup menu

Error aging minutes

Here you set the length of time in minutes after which the device deletes VPN errors from the status table.



To document sporadic errors, disable this option with the entry 0.

SNMP ID:

2.11.65

Telnet path:

Setup > Config

Possible values:

Max. 4 characters from 0123456789

Default:

0

Special values:

0

Disables this option. Errors will remain in the status table.

14.7 IPv4 addresses for VPN tunnels in the IP parameter list

As of LCOS version 9.10, devices supporting VPN manage the IPv4 addresses for VPN tunnels in the IP parameter list.

14.7.1 Additions to the Setup menu

IP-List

If certain remote sites do not automatically transmit the IP parameters needed for a connection, then enter these values here.

Use this table to configure the extranet address of a VPN tunnel, for example.

SNMP ID:

2.2.20

Telnet path:

Setup > WAN

Remote site

Enter the name for the remote station here.

When configuring a VPN tunnel, this entry corresponds to the appropriate service under **Setup > VPN > VPN-Peers** or **Setup > VPN > IKEv2 > Connections**.

SNMP ID:

2.2.20.1

Telnet path:

Setup > WAN > IP-List

Possible values:

Select from the list of defined peers.

Max. 16 characters from `[A-Z][0-9]{ | }~!$%&'()+-./:;<=>?[\]^_.`

Default:

empty

Masq.-IP-Addr.

Almost all Internet providers usually have the remote device assign a dynamic IP address to your router when it establishes the connection. If your Internet provider has assigned you static IP addresses, or if you wish to operate masquerading for your VPN network, you assign it to the respective connection here. If the masquerading IP address is not set, then the address assigned when the connection was established is used for masquerading.



You need to set a masquerading address for a VPN connection if you wish to mask a private network behind this address in the VPN network.



This setting is also necessary if a private address (172.16.x.x) is assigned during PPP negotiation. Normal masquerading is thus impossible as this type of address is filtered in the Internet.

SNMP ID:

2.2.20.9

Telnet path:

Setup > WAN > IP-List

Possible values:

Valid IPv4 address, max. 15 characters from [0–9] .

Default:

0.0.0.0

Masquerading

You can use IP masquerading to hide a logical network behind a single address (that of the router). If, for example, you have an Internet connection, you can use it to connect your entire network to the Internet.

Almost all Internet providers usually have the remote device assign a dynamic IP address to your router when it establishes the connection. If your Internet provider has assigned fixed IP addresses, you can assign them to the relevant connection in the IP parameter list.

Select "on" to enable IP masquerading for all LAN interfaces. If you wish to assign fixed IP addresses to computers in the demilitarized zone (DMZ) and yet you still wish to activate IP masquerading for the computers on the other LAN interfaces (intranet), then select "Intranet".

If you want this entry to mask a VPN connection, select "on".

SNMP ID:

2.8.2.5

Telnet path:

Setup > IP-Router > IP-Routing-Table

Possible values:**No**

IP masking off

On

Intranet and DMZ masquerading

Intranet

Intranet - Intranet masquerading only

Default:

No

Extranet address

In LCOS versions before 9.10, this field contained the IPv4 address used by the local stations to mask their own IP address in certain scenarios.

As of LCOS version 9.10, masquerading uses the entry under **Setup > WAN > IP-List** in the field **Masq.-IP-Addr.**

SNMP ID:

2.19.9.2

Telnet path:

Setup > VPN > VPN-Peers

Possible values:

Max. 15 characters from [0–9] .

Default:

empty

15 Routing and WAN connections

15.1 Client binding

As of LCOS version 9.10, load balancing additionally features client binding.

15.1.1 Client binding

The use of load balancing leads to problems for servers that use an IP address to identify a logged-on user. If a user is logged in to a web site, for example, and the load balancer then takes a different Internet connection, then the server interprets this as a connection attempt by a user who is not logged on. In the best case the user sees a new login dialog, but not the desired web page.

One possible workaround would be to use a firewall rule (policy based routing) to direct the traffic to this server over a specific Internet connection. However, this would limit all of the traffic to that server to the bandwidth of a single connection. What's more, there is no way to establish a backup if the first connection should fail.

In contrast to this, client binding does not monitor the individual TCP/IP sessions but the client that opened an Internet connection in the initial session. It directs all subsequent sessions through this Internet connection, which corresponds in principle to the policy-based routing mentioned above. How this is done depends on the protocol, i.e. it transports only data of the same protocol type (e.g. HTTPS) over this Internet connection. If the client loads additional data via an HTTP connection, it probably does this with a different connection.

To prevent data from being bottle-necked into this one Internet connection when it could easily be transferred via parallel connections, a timer ensures that the load balancer distributes additional sessions between the available Internet connections for a specified period. After the timer expires, the client binding forces a new session over the original Internet connection and the timer is restarted. The server thus continues to recognize the login status for the user due to the current IP address.

15.1.2 Load balancing with client binding

In LANconfig, client binding is configured under **IP router > Routing** in the section **Load balancing**.

The screenshot shows a configuration window titled "Load balancing". It contains the following elements:

- A text box: "If your Internet provider does not support real channel bundling, it is possible to combine several connections with a load balancer."
- A checkbox labeled "Load balancing enabled" which is currently unchecked.
- A button labeled "Load balancing..."
- A horizontal separator line.
- A text box: "For connections that fit certain protocol/port criteria, client binding ensures that only a single WAN connection is used for each target address. This avoids the occurrence of multiple source addresses."
- Two input fields: "Binding minutes:" with the value "30" and "Balance seconds:" with the value "10".
- A button labeled "Client binding protocols..."

Binding minutes

Here you specify the time in minutes for the binding entries to be valid for a client.

Balance seconds

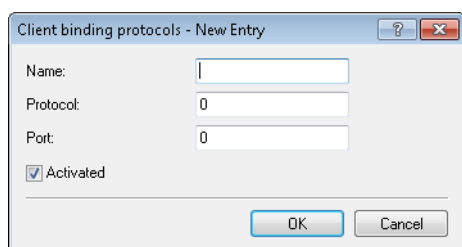
To prevent data from flowing the this main-session Internet connection when it could easily be transferred via parallel connections, a timer ensures that the load balancer distributes additional sessions between the

available Internet connections for a specified period. After the timer expires, the client binding forces a new session over the original Internet connection and the timer is restarted. The server thus continues to recognize the login status for the user due to the current IP address.

Here you specify the time in seconds, following the start of the main session, during which the load balancer is free to distribute new sessions to other Internet connections.

Client binding is protocol-oriented. You set the corresponding protocols under **Client binding protocols**. The table already contains the default entries

- HTTPS
- HTTP
- ANY



Name

Contains a descriptive name for this entry.

Protocol

Contains the IP protocol number.



Learn more about IP protocol numbers in the IANA [Online database](#).

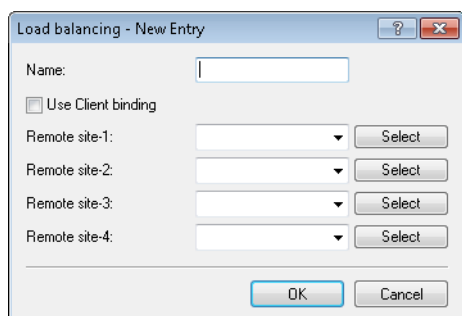
Port

Contains the port of the IP protocol.

Activated

Activates or deactivates this entry.

Client binding can be activated or deactivated for each of the entries under **Load balancing**.



15.1.3 Enhancements in the menu system

Additions to the Setup menu

Client binding

In this menu, you can configure the client binding.

The use of load balancing leads to problems for servers that use an IP address to identify a logged-on user. If a user is logged in to a web site, for example, and the load balancer then takes a different Internet connection, then the server interprets this as a connection attempt by a user who is not logged on. In the best case the user sees a new login dialog, but not the desired web page.

One possible workaround would be to use a firewall rule (policy based routing) to direct the traffic to this server over a specific Internet connection. However, this would limit all of the traffic to that server to the bandwidth of a single connection. What's more, there is no way to establish a backup if the first connection should fail.

In contrast to this, client binding does not monitor the individual TCP/IP sessions but the client that opened an Internet connection in the initial session. It directs all subsequent sessions through this Internet connection, which corresponds in principle to the policy-based routing mentioned above. How this is done depends on the protocol, i.e. it transports only data of the same protocol type (e.g. HTTPS) over this Internet connection. If the client loads additional data via an HTTP connection, it probably does this with a different connection.

To prevent data from being bottle-necked into this one Internet connection when it could easily be transferred via parallel connections, a timer ensures that the load balancer distributes additional sessions between the available Internet connections for a specified period. After the timer expires, the client binding forces a new session over the original Internet connection and the timer is restarted. The server thus continues to recognize the login status for the user due to the current IP address.

SNMP ID:

2.8.20.3

Telnet path:

Setup > IP-Router > Load-Balancer

Protocols

In this table, you specify the protocols and the associated ports for monitoring by the client binding.



The table already contains the default entries

- HTTPS
- HTTP
- ANY

SNMP ID:

2.8.20.3.1

Telnet path:

Status > IP-Router > Load-Balancer > Client-Binding

Name

Enter a descriptive name for this entry.

SNMP ID:

2.8.20.3.1.1

Telnet path:

Setup > IP-Router > Load-Balancer > Client-Binding > Protocols

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]`

Default:

empty

Protocol

Select the IP protocol number.



Learn more about IP protocol numbers in the [online database](#) of the IANA.

SNMP ID:

2.8.20.3.1.2

Telnet path:

Setup > IP-Router > Load-Balancer > Client-Binding > Protocols

Possible values:

Max. 3 characters from `[0-255]`

Special values:

0

All protocols

Default:

0

Port

Select the port.

SNMP ID:

2.8.20.3.1.3

Telnet path:

Setup > IP-Router > Load-Balancer > Client-Binding > Protocols

Possible values:

Max. 5 characters from [0–65535]

Special values:

0

All ports

Default:

0

Operating

Here you enable or disable the client binding for this entry.

SNMP ID:

2.8.20.3.1.4

Telnet path:**Setup > IP-Router > Load-Balancer > Client-Binding > Protocols****Possible values:****Yes**

Enables the entry

No

Disables the entry

Default:

Yes

Binding minutes

Specify the time in minutes for the binding entries to be valid for a client.

SNMP ID:

2.8.20.3.2

Telnet path:**Status > IP-Router > Load-Balancer > Client-Binding****Possible values:**

Max. 3 characters from [0–999]

Special values:

0

Default:

30

Balance seconds

To prevent data from flowing through this main-session Internet connection when it could easily be transferred via parallel connections, a timer ensures that the load balancer distributes additional sessions between the available Internet connections for a specified period. After the timer expires, the client binding forces a new session over the original Internet connection and the timer is restarted. The server thus continues to recognize the login status for the user due to the current IP address.

Here you specify the time in seconds, following the start of the main session, during which the load balancer is free to distribute new sessions to other Internet connections.

SNMP ID:

2.8.20.3.3

Telnet path:**Status > IP-Router > Load-Balancer > Client-Binding****Possible values:**

Max. 3 characters from [0–999]

Special values:

0

The timer is deactivated. All sessions are bound to the existing Internet connection.

Default:

10

Client binding

Here you enable or disable the client binding for each load balancer.

SNMP ID:

2.8.20.2.10

Telnet path:**Setup > IP-Router > Load-Balancer > Bundle-Peers****Possible values:****Yes**

Client binding is enabled.

No

Client binding is disabled.

Default:

No

Additions to the Status menu**Client binding**

This table shows the details of current client bindings.

SNMP ID:

1.10.32.3

Telnet path:**Status > IP-Router > Load-Balancer****Source-IP**

This entry shows the source IP addresses of the client.

SNMP ID:

1.10.32.3.1

Telnet path:**Status > IP-Router > Load-Balancer > Client-Binding****Bundle-Peer**

This entry shows the name of the selected Internet connection.

SNMP ID:

1.10.32.3.2

Telnet path:**Status > IP-Router > Load-Balancer > Client-Binding****Timeout**

This entry indicates the remaining time until the load balancer deletes this entry.

SNMP ID:

1.10.32.3.3

Telnet path:**Status > IP-Router > Load-Balancer > Client-Binding**

Balance

This entry indicates whether the timer is enabled for allowing further Internet connections.

SNMP ID:

1.10.32.3.4

Telnet path:

Status > IP-Router > Load-Balancer > Client-Binding

15.2 Interface binding "Any" removed in IPv4

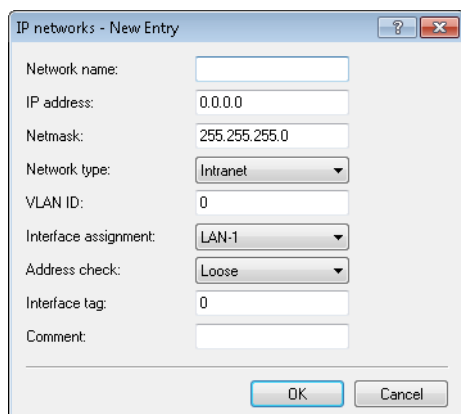
As of LCOS version 9.10 it is no longer possible to select "Any" when assigning interfaces to IPv4 networks.

 The new default setting is "LAN-1" or "BRG-1".

15.2.1 Defining networks and assigning interfaces

When defining a network, the first setting is for the IP address range which is to be valid for a certain local interface on the router. "Local interfaces" are logical interfaces which are assigned either to a physical Ethernet port (LAN) or to a wireless port (WLAN). To realize the scenarios outlined above, it is possible for several networks to be active on one interface: Conversely, a network can also be active on multiple interfaces (via bridge groups or with the interface assignment 'Any').


The networks are defined in a table under **IPv4 > General > IP networks**. A unique name for the networks is set along with definitions for the address range and interface assignment. The network name allows the identification of networks in other modules (DHCP server, RIP, NetBIOS, etc.) and to enable control over which services are available in which networks.



15.2.2 Additions to the Setup menu

Interface

Here you select the interface that is to be allocated to the network.

 The values for 'x' in the list vary per model.

SNMP ID:

2.7.30.5

Telnet path:**Setup > TCP-IP > Network-List****Possible values:****LAN-1****LAN-x****WLAN-x-x****P2P-x-x****BRG-x****Default:**

LAN-1

15.3 Generic routing encapsulation (GRE)

As of LCOS version 9.10 it is possible to transmit data packets of any transmission protocol as IP packets within GRE tunnels.

The trace command has an additional parameter in case of issues with GRE tunnels:

Table 11: Overview of all possible traces

This parametercauses the following message in the trace:
GRE	Messages to GRE tunnels

15.3.1 Understanding the generic routing encapsulation (GRE) protocol

GRE is a tunneling protocol that encapsulates any layer-3 data packets (including IP, IPSec, ICMP, etc.) into virtual point-to-point network connections. This is very useful, among other things, when the two communication partners wish to use a particular transport protocol (for example, IPSec) that is unavailable on the transmission path. Since GRE itself does not encrypt the tunneled data, the two communication partners themselves must ensure that the data is protected.

Configuring a GRE tunnel

To configure a GRE tunnel with LANconfig, navigate to **Communication > Remote sites > GRE tunnel** and click **GRE tunnel**.

The screenshot shows a dialog box titled "GRE tunnel - New Entry". It contains the following fields and controls:

- Remote site: [Text input field]
- Server address: [Text input field]
- Routing tag: [Text input field with value 0]
- Checksum: ☐
- Key present: ☐
- Key: [Text input field with value 0]
- Source address: [Dropdown menu] [Select button]
- Packet sequence: ☐
- OK button
- Cancel button

Remote site

The name of the remote station for this GRE tunnel. Use this name in the routing table in order to send data through this GRE tunnel.

Server address

Address of the GRE tunnel endpoint (valid IPv4 or IPv6 address or FQDN).

Routing-Tag

Routing tag for the connection to the GRE tunnel endpoint. The device maps data packets to this GRE tunnel by means of the routing tag.

Checksum

Here you specify whether the GRE header should contain a check sum.

With the check sum function enabled, the device calculates a checksum for the transmitted data and attaches this to the GRE tunnel header. If the GRE header of incoming data contains a checksum, the device checks this against the transmitted data. The device discards any data received with an erroneous or missing check sum.

With the checksum function disabled, the device sends all tunnel data without a checksum and it expected data packets without a checksum. Incoming data packets with a checksum in the GRE header are discarded.

Key present

Here you specify whether the GRE header should contain a key for data-flow control.

If you enable this feature, the device inserts the value set in the **key** field into the GRE header for this GRE tunnel. The device only maps incoming data packets to this GRE tunnel if their GRE header contains an identical key value.

With this feature disabled, the GRE header of outgoing data packets does not contain a key value. The device only maps incoming data packets to this GRE tunnel if their GRE header similarly does not contain a key value.

Key

The key that assures data-flow control in this GRE tunnel. Two devices connected via several GRE tunnels use this key to map the data packets to the appropriate GRE tunnel.

Sequencing

Here you specify whether the GRE header contains information about the sequence of the data packets.

With this feature enabled, the device includes a counter in the GRE header of outgoing data packets in order to communicate the sequence of the data packets to the GRE tunnel endpoint. The device analyses the sequence of incoming data packets and drops packets with an incorrect or missing packet sequence.

Source address

Here you can optionally specify a source address for the device to use as the target address instead of the one that would normally be selected automatically. Possible values are:

- Name of the IP networks whose addresses are to be used.
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address



If the list of IP networks or source addresses contains an entry named 'DMZ', then the associated IP address will be used.

To use IPv6 as the GRE tunnel transport protocol, navigate to **IPv6 > WAN interfaces** and create a new entry named "IPV6GRE", for example. When you subsequently configure the GRE tunnel, you set this interface as the **Remote site**.

If you need to specify an IP address for the tunnel interface, proceed as follows:

IPv4 address

Create a new entry under **Communication > Protocols > IP parameters** and set the name of the remote site as the name of the GRE tunnel remote site. Finally, enter the necessary values for the **IP address** and **Netmask**.

IPv6

Create a new entry under **IPv6 > General > IP addresses** and set the network name as the name of the GRE tunnel remote site. Finally, enter the necessary values for the **Address/Prefix length**.

15.3.2 Additions to the Setup menu

GRE-Tunnel

GRE is a tunneling protocol that encapsulates any layer-3 data packets (including IP, IPSec, ICMP, etc.) into virtual point-to-point network connections. You configure the various GRE tunnels here.

SNMP ID:

2.2.51

Telnet path:

Setup > WAN

Remote site

The name of the remote station for this GRE tunnel. Use this name in the routing table in order to send data through this GRE tunnel.

SNMP ID:

2.2.51.1

Telnet path:

Setup > WAN > GRE-Tunnel

IP address

Address of the GRE tunnel endpoint (valid IPv4 or IPv6 address or FQDN).

SNMP ID:

2.2.51.3

Telnet path:

Setup > WAN > GRE-Tunnel

Possible values:

Max. 64 characters from `[A-Z][0-9]@{ | }~!$%&'()+- , / : ; < = > ? [\] ^ _ .`

Default:

empty

Routing-Tag

Routing tag for the connection to the GRE tunnel endpoint.

SNMP ID:

2.2.51.4

Telnet path:

Setup > WAN > GRE-Tunnel

Possible values:

0 ... 65535

Default:

0

Key present

Here you specify whether the GRE header should contain a key for data-flow control.

If you enable this feature, the device inserts the value set in the **key** field into the GRE header for this GRE tunnel. The device only maps incoming data packets to this GRE tunnel if their GRE header contains an identical key value.

With this feature disabled, the GRE header of outgoing data packets does not contain a key value. The device only maps incoming data packets to this GRE tunnel if their GRE header similarly does not contain a key value.

SNMP ID:

2.2.51.5

Telnet path:

Setup > WAN > GRE-Tunnel

Possible values:

Yes
No

Default:

No

Key value

The key that assures data-flow control in this GRE tunnel.

SNMP ID:

2.2.51.6

Telnet path:

Setup > WAN > GRE-Tunnel

Possible values:

0 ... 4294967295

Default:

0

Checksum

Here you specify whether the GRE header should contain a check sum.

With the check sum function enabled, the device calculates a checksum for the transmitted data and attaches this to the GRE tunnel header. If the GRE header of incoming data contains a checksum, the device checks this against the transmitted data. The device discards any data received with an erroneous or missing check sum.

With the checksum function disabled, the device sends all tunnel data without a checksum and it expected data packets without a checksum. Incoming data packets with a checksum in the GRE header are discarded.

SNMP ID:

2.2.51.7

Telnet path:

Setup > WAN > GRE-Tunnel

Possible values:

Yes
No

Default:

No

Sequencing

Here you specify whether the GRE header contains information about the sequence of the data packets.

With this feature enabled, the device includes a counter in the GRE header of outgoing data packets in order to communicate the sequence of the data packets to the GRE tunnel endpoint. The device analyses the sequence of incoming data packets and drops packets with an incorrect or missing packet sequence.

SNMP ID:

2.2.51.8

Telnet path:**Setup > WAN > GRE-Tunnel****Possible values:****Yes****No****Default:**

No

Source address

Here you can optionally specify a source address for the device to use as the target address instead of the one that would normally be selected automatically.



If the list of IP networks or loopback addresses contains an entry named 'DMZ', then the associated IP address will be used.

SNMP ID:

2.2.51.9

Telnet path:**Setup > WAN > GRE-Tunnel****Possible values:****Valid entry from the list of possible addresses.**

Name of the IP networks whose addresses are to be used.

"INT" for the address of the first intranet

"DMZ" for the address of the first DMZ

LB0 to LBF for the 16 loopback addresses

Any valid IP address

empty

Default:

15.3.3 Additions to the Status menu

GRE-Tunnel

This table shows the status values of the GRE tunnel.

SNMP ID:

1.86

Telnet path:**Status****Remote site**

This column contains the name of each GRE tunnel remote station.

SNMP ID:

1.86.1

Telnet path:**Status > GRE-Tunnel****Server address**

This column contains the addresses of the GRE tunnel endpoints (valid IP address or FQDN).

SNMP ID:

1.86.3

Telnet path:**Status > GRE-Tunnel****Routing-Tag**

This column contains the routing tags for the connections to each of the GRE tunnel endpoints.

SNMP ID:

1.86.4

Telnet path:**Status > GRE-Tunnel****Key present**

This column indicates whether the GRE header of the respective tunnel contains a key.

SNMP ID:

1.86.5

Telnet path:**Status > GRE-Tunnel**

Key

This column contains the key if one is present in the GRE header of the corresponding tunnel.

SNMP ID:

1.86.6

Telnet path:

Status > GRE-Tunnel

Checksum

This column indicates whether the GRE header of the corresponding tunnel contains a checksum.

SNMP ID:

1.86.7

Telnet path:

Status > GRE-Tunnel

Sequencing

This column indicates whether the GRE header of the corresponding tunnel contains packet sequencing.

SNMP ID:

1.86.8

Telnet path:

Status > GRE-Tunnel

Source address

This column contains the source address specified for the respective GRE tunnel.

SNMP ID:

1.86.9

Telnet path:

Status > GRE-Tunnel

15.4 Ethernet-over-GRE tunnel (EoGRE)


As of LCOS version 9.10 it is possible to transmit Ethernet packets as IP packets within EoGRE tunnels.

The trace command has an additional parameter in case of issues with GRE tunnels:

Table 12: Overview of all possible traces

This parametercauses the following message in the trace:
GRE	Messages to GRE tunnels

15.4.1 Ethernet-over-GRE (EoGRE)

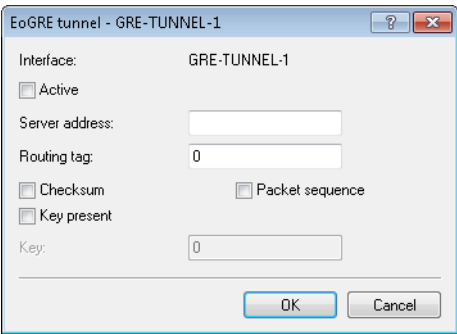
 For more information about the GRE protocol, see [Understanding the generic routing encapsulation protocol \(GRE\)](#).

The current version of LCOS provides a number of “Ethernet over GRE” tunnels (EoGRE) to transmit Ethernet packets via GRE. Since these Ethernet packets move on OSI layer 2 only, the EoGRE tunnel only functions as a bridge.

This can be used to implement L2VPN (VPN as a simple level-2 bridge) or a transparent Ethernet bridge over WAN.

Configuring an EoGRE tunnel

To configure an EoGRE tunnel with LANconfig, navigate to **Communication > Remote sites > GRE tunnel**, click **EoGRE tunnel** and select the appropriate tunnel.



Interface

Name of the selected EoGRE tunnel.

Operating

Activates or deactivates the EoGRE tunnel. Deactivated EoGRE tunnels do not send or receive any data.

Server address

Address of the EoGRE tunnel endpoint (valid IPv4 or IPv6 address or FQDN).

Routing-Tag

Routing tag for the connection to the EoGRE tunnel endpoint. The device maps data packets to this EoGRE tunnel by means of the routing tag.

Checksum

Here you specify whether the GRE header should contain a check sum.

With the check sum function enabled, the device calculates a checksum for the transmitted data and attaches this to the GRE tunnel header. If the GRE header of incoming data contains a checksum, the device checks this against the transmitted data. The device discards any data received with an erroneous or missing check sum.

With the checksum function disabled, the device sends all tunnel data without a checksum and it expected data packets without a checksum. Incoming data packets with a checksum in the GRE header are discarded.

Key present

Here you specify whether the GRE header should contain a key for data-flow control.

If you enable this feature, the device inserts the value set in the **key** field into the GRE header for this EoGRE tunnel. The device only maps incoming data packets to this EoGRE tunnel if their GRE header contains an identical key value.

With this feature disabled, the GRE header of outgoing data packets does not contain a key value. The device only maps incoming data packets to this EoGRE tunnel if their GRE header similarly does not contain a key value.

Key

The key that assures data-flow control in this EoGRE tunnel. Two devices connected via several EoGRE tunnels use this key to map the data packets to the appropriate EoGRE tunnel.

Sequencing

Here you specify whether the GRE header contains information about the sequence of the data packets.

With this feature enabled, the device includes a counter in the GRE header of outgoing data packets in order to communicate the sequence of the data packets to the EoGRE tunnel endpoint. The device analyses the sequence of incoming data packets and drops packets with an incorrect or missing packet sequence.

Connecting a local interface to an EoGRE tunnel

Connecting a local interface to an EoGRE tunnel involves the following steps:

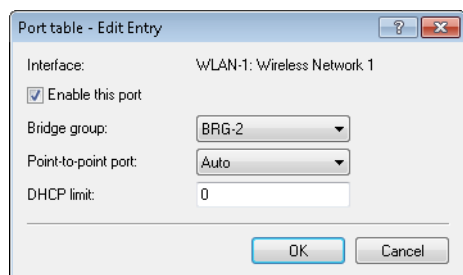
1. Create a new entry under **Communication > Remote sites > GRE tunnel > EoGRE tunnel**.

Activate the tunnel and, under **Server address**, enter the address of the remote device to which the EoGRE tunnel is to connect (IPv4 address, IPv6 address, or FQDN).

2. Add a bridge group for the activated EoGRE tunnel under **Interfaces > LAN > Port table**.

Enable the port and select the required bridge group.

3. Again under **Interfaces > LAN > Port table**, supplement the same bridge group with the local interface that you want to connect through the EoGRE tunnel (e.g. WLAN-1).



Enable the port and select from the list the bridge group that contains the EoGRE tunnel.

15.4.2 Additions to the Status menu

EoGRE-Tunnel

This table shows you information about the EoGRE tunnels.

SNMP ID:

1.87

Telnet path:

Status

15.4.3 Additions to the Setup menu

EoGRE-Tunnel

The current version of LCOS provides a number of "Ethernet over GRE" tunnels (EoGRE) to transmit Ethernet packets via GRE. You configure the various EoGRE tunnels here.

SNMP ID:

2.2.50

Telnet path:

Setup > WAN

Interface

Name of the selected EoGRE tunnel.

SNMP ID:

2.2.50.1

Telnet path:

Setup > WAN > EoGRE-Tunnel

Operating

Activates or deactivates the EoGRE tunnel. Deactivated EoGRE tunnels do not send or receive any data.

SNMP ID:

2.2.50.2

Telnet path:

Setup > WAN > EoGRE-Tunnel

Possible values:

Yes

No

Default:

No

IP address

Address of the EoGRE tunnel endpoint (valid IPv4 or IPv6 address or FQDN).

SNMP ID:

2.2.50.3

Telnet path:

Setup > WAN > EoGRE-Tunnel

Possible values:

Max. 64 characters from `[A-Z][0-9]@{ | }~!$%&' ()+-, / : ; <=> ? [\] ^ _ .`

Default:

empty

Routing-Tag

Routing tag for the connection to the EoGRE tunnel endpoint.

SNMP ID:

2.2.50.4

Telnet path:

Setup > WAN > EoGRE-Tunnel

Possible values:

0 ... 65535

Default:

0

Key present

Here you specify whether the GRE header should contain a key for data-flow control.

If you enable this feature, the device inserts the value set in the **key** field into the GRE header for this EoGRE tunnel. The device only maps incoming data packets to this EoGRE tunnel if their GRE header contains an identical key value.

With this feature disabled, the GRE header of outgoing data packets does not contain a key value. The device only maps incoming data packets to this EoGRE tunnel if their GRE header similarly does not contain a key value.

SNMP ID:

2.2.50.5

Telnet path:**Setup > WAN > EoGRE-Tunnel****Possible values:****Yes****No****Default:**

No

Key value

The key that assures data-flow control in this EoGRE tunnel.

SNMP ID:

2.2.50.6

Telnet path:**Setup > WAN > EoGRE-Tunnel****Possible values:**

0 ... 4294967295

Default:

0

Checksum

Here you specify whether the GRE header should contain a check sum.

With the check sum function enabled, the device calculates a checksum for the transmitted data and attaches this to the GRE tunnel header. If the GRE header of incoming data contains a checksum, the device checks this against the transmitted data. The device discards any data received with an erroneous or missing check sum.

With the checksum function disabled, the device sends all tunnel data without a checksum and it expected data packets without a checksum. Incoming data packets with a checksum in the GRE header are discarded.

SNMP ID:

2.2.50.7

Telnet path:**Setup > WAN > EoGRE-Tunnel****Possible values:****Yes****No****Default:**

No

Sequencing

Here you specify whether the GRE header contains information about the sequence of the data packets.

With this feature enabled, the device includes a counter in the GRE header of outgoing data packets in order to communicate the sequence of the data packets to the EoGRE tunnel endpoint. The device analyses the sequence of incoming data packets and drops packets with an incorrect or missing packet sequence.

SNMP ID:

2.2.50.8

Telnet path:**Setup > WAN > EoGRE-Tunnel****Possible values:****Yes****No****Default:**

No

15.5 Loopback addresses for RIP

As of LCOS version 9.10 it is possible to specify a loopback address for WAN RIP.

Source address (opt.)

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

If you have configured loopback addresses, you can specify them here as source address. You can enter an address in various forms:

- Name of the IP network (ARF network), whose address should be used.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ (Note: If there is an interface named "DMZ", its address will be taken).
- LB0...LBF for one of the 16 loopback addresses or its name.
- Furthermore, any IP address can be entered in the form x.x.x.x.



If the source address set here is a loopback address, these will be used unmasked on the remote client.

15.5.1 Additions to the Setup menu

Loopback address

Enter a loopback address here. Possible values are:

- The name of an ARF network
- Configured loopback address
- IPv4 address

SNMP ID:

2.8.8.4.13

Telnet path:**Setup > IP-Router > RIP > WAN-Table****Possible values:**

Specify a valid IPv4 address here. |

Default:*empty*

15.6 PPPoE snooping new

As of LCOS version 9.10 PPPoE snooping is also implemented.

15.6.1 PPPoE snooping

PPPoE snooping enables devices that receive and forward PPPoE discovery (PPPoED) packets to analyze these packets and to supplement them with additional information. This information can be used by a PPPoE access concentrator (AC) to process the PPPoED data packets accordingly. This role is called the "PPPoE-Intermediate-Agent".

PPPoE snooping in the LCOS processes the following PPPoED packets:

- PADI (PPPoE Active Discovery Indication)
- PADR (PPPoE Active Discovery Request)
- PADT (PPPoE Active Discovery Terminate)

The PPPoE intermediate agent, which is responsible for the PPPoE snooping, supplements the PPPoED packet with manufacturer-specific attributes (circuit ID and remote ID), and any existing IDs in received packets are replaced with its own values.

- The remote ID: Uniquely identifies the client making a PPPoE request.
- Circuit ID: Uniquely identifies the interface used by a client to make a PPPoE request.

PPPoE snooping is configured for each LAN/WLAN interface.

15.6.2 Additions to the Setup menu

PPPoE snooping

Here you configure PPPoE snooping for each interface.

SNMP ID:

2.20.43

Telnet path:**Setup > LAN-Bridge****Port**

Indicates the physical or logical interface to which this PPPoE-snooping configuration applies.

SNMP ID:

2.20.43.1

Telnet path:**Setup > LAN-Bridge > PPPoE-Snooping****Possible values:****LAN-x**

All physical LAN interfaces

WLAN-x

All physical WLAN interfaces

WLAN-x-x

All logical WLAN interfaces

P2P-x-x

All logical P2P interfaces

WLC-TUNNEL-x

All virtual WLC tunnels

GRE-TUNNEL-x

All virtual GRE tunnels

Add agent info

Here you decide whether the PPPoE intermediate agent gives incoming PPPoE packets a manufacturer-specific PPPoE tag with the vendor ID "3561" before forwarding the request to a PPPoE server.

This option allows the PPPoE intermediate agent to deliver additional information to the PPPoE server about the interface used by the client to make the request.

The PPPoE tag is composed of values for the **Remote ID** and the **Circuit ID**.



If these two fields are empty, the PPPoE intermediate agent does not add a PPPoE tag to the data packets.

SNMP ID:

2.20.43.2

Telnet path:**Setup > LAN-Bridge > PPPoE-Snooping****Possible values:****Yes**

Adds "relay agent info" to the PPPoE packets.

No

This setting disables PPPoE snooping for this interface.

Default:

No

Remote ID

The remote ID is a sub-option of the PPPoE intermediate agent option. It uniquely identifies the client making a PPPoE request.

You can use the following variables:

- `%`: Inserts a percent sign.
- `%c`: Inserts the MAC address of the interface where the PPPoE intermediate agent received the PPPoE request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- `%C`: Inserts the name of the interface where the PPPoE intermediate agent received the PPPoE request.
- `%n`: Inserts the name of the PPPoE intermediate agent as specified under **Setup > Name**.
- `%v`: Inserts the VLAN ID of the PPPoE request packet. This VLAN ID is sourced either from the VLAN header of the PPPoE data packet or from the VLAN ID mapping for this interface.
- `%p`: Inserts the name of the Ethernet interface that received the PPPoE data packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, `%p` and `%i` are identical.
- `%s`: Inserts the WLAN SSID if the PPPoE packet originates from a WLAN client. For other clients, this variable contains an empty string.
- `%e`: Inserts the serial number of the PPPoE relay agent, to be found for example under **Status > Hardware-Info > Serial number**.

SNMP ID:

2.20.43.3

Telnet path:

Setup > LAN-Bridge > PPPoE-Snooping

Possible values:

Max. 30 characters from `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_.`

Default:

empty

Circuit ID

The circuit ID is a sub-option of the PPPoE intermediate agent info option. It uniquely identifies the interface used by the client to make a PPPoE request.

You can use the following variables:

- `%`: Inserts a percent sign.
- `%c`: Inserts the MAC address of the interface where the PPPoE intermediate agent received the PPPoE request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- `%C`: Inserts the name of the interface where the PPPoE intermediate agent received the PPPoE request.
- `%n`: Inserts the name of the PPPoE intermediate agent as specified under **Setup > Name**.
- `%v`: Inserts the VLAN ID of the PPPoE request packet. This VLAN ID is sourced either from the VLAN header of the PPPoE data packet or from the VLAN ID mapping for this interface.
- `%p`: Inserts the name of the Ethernet interface that received the PPPoE data packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, `%p` and `%i` are identical.
- `%s`: Inserts the WLAN SSID if the PPPoE packet originates from a WLAN client. For other clients, this variable contains an empty string.

- %e: Inserts the serial number of the PPPoE relay agent, to be found for example under **Status > Hardware-Info > Serial number**.

SNMP ID:

2.20.43.4

Telnet path:**Setup > LAN-Bridge > PPPoE-Snooping****Possible values:**Max. 30 characters from `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_.`**Default:***empty***Discard server packets**

Here you decide whether the PPPoE intermediate agent retains or discards any existing PPPoE tags.

SNMP ID:

2.20.43.5

Telnet path:**Setup > LAN-Bridge > PPPoE-Snooping****Possible values:****Yes**

The PPPoE intermediate Agent removes existing PPPoE tags and leaves both the "Circuit ID" and the "Remote ID" empty.

No

The PPPoE intermediate agent takes over any existing PPPoE tags.

Default:

No

15.7 Default settings in the access table for WAN connections

As of LCOS version 9.10, all protocols for WAN connections are disabled in the access table.

15.7.1 Additions to the Setup menu

Telnet

Use this option to set the access rights for configuring the device via the TELNET protocol. This protocol is required for text-based configuration of the device with the Telnet console, which is independent of the operating system.

SNMP ID:

2.11.15.2

Telnet path:**Setup > Config > Access-Table****Possible values:****VPN**

Access is only possible via VPN.



VPN-capable devices only.

Yes

Access is generally possible.



By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.



Default setting for the WAN interface.

Default:

Yes

No

TFTP

Use this option to set the access rights for configuring the device via the TFTP protocol (Trivial File Transfer Protocol). This protocol is required, for example, for configuration using the LANconfig application.

SNMP ID:

2.11.15.3

Telnet path:**Setup > Config > Access-Table****Possible values:****VPN**

Access is only possible via VPN.



VPN-capable devices only.

Yes

Access is generally possible.



By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.



Default setting for the WAN interface.

Default:

Yes

No

HTTP

Use this option to set the access rights for configuring the device via the HTTP protocol (Hypertext Transfer Protocol). This protocol is required for configuring the device via the implemented web-based browser interface independent of the operating system.

SNMP ID:

2.11.15.4

Telnet path:

Setup > Config > Access-Table

Possible values:**VPN**

Access is only possible via VPN.



VPN-capable devices only.

Yes

Access is generally possible.




By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

 Default setting for the WAN interface.

Default:

Yes

No

SNMP

Use this option to set the access rights for configuring the device via the SNMP protocol (Simple Network Management Protocol). This protocol is required, for example, for configuring the device using the LANmonitor application.

SNMP ID:

2.11.15.5


Telnet path:**Setup > Config > Access-Table****Possible values:****VPN**

Access is only possible via VPN.

 VPN-capable devices only.

Yes

Access is generally possible.


 By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

 Default setting for the WAN interface.

Default:

Yes

No

HTTPS

Use this option to set the access rights for configuring the device via the HTTPS protocol (Hypertext Transfer Protocol Secure or HTTP via SSL). This protocol is required for configuring the device via the implemented web-browser interface independent of the operating system.

SNMP ID:

2.11.15.6

Telnet path:

Setup > Config > Access-Table

Possible values:

VPN

Access is only possible via VPN.



VPN-capable devices only.

Yes

Access is generally possible.



By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.



Default setting for the WAN interface.

Default:

Yes

No

Telnet-SSL

Use this option to set the access rights for configuring the device via the TELNET protocol. This protocol is required for text-based configuration of the device with the Telnet console, which is independent of the operating system.

SNMP ID:

2.11.15.7

Telnet path:

Setup > Config > Access-Table


Possible values:**VPN**

Access is only possible via VPN.

 VPN-capable devices only.

Yes

Access is generally possible.

 By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

 Default setting for the WAN interface.

Default:

Yes

No

SSH

Use this option to set the access rights for configuring the device via the TELNET/SSH protocol. This protocol is required for configuring the device securely via the implemented Telnet console from text-based systems independent of the operating system.

SNMP ID:

2.11.15.8

Telnet path:

Setup > Config > Access-Table


Possible values:**VPN**

Access is only possible via VPN.

 VPN-capable devices only.

Yes

Access is generally possible.

 By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.



Default setting for the WAN interface.

Default:

Yes

No

Config Sync

Indicates whether a config sync is possible (restricted) via this interface.

SNMP ID:

2.11.15.10

Telnet path:

Setup > Config > Access-Table

Possible values:**VPN**

Access is only possible via VPN.



VPN-capable devices only.

Yes

Access is generally possible.



By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.



Default setting for the WAN interface.

Default:

Yes

No

16 Backup solutions

16.1 Backup connections for dual-SIM devices

As of LCOS version 9.10, dual-SIM devices also support backup connections if the primary connection is based on a cellular connection. You can also explicitly specify the time until the device returns to the primary connection.

16.1.1 Configuration of the backup connection

The following steps are necessary to define a backup connection:

1. The backup connection requires the appropriate WAN interface to be set up so that the remote site can be reached via this alternative route. If, for example, the ISDN line is to serve as the backup connection, then the remote site is set up as an ISDN remote site (along with the necessary entries in the communications layers and in the PPP list).
2. If the connection to the remote site cannot be checked with LCP requests, the monitoring of the connection should be initiated with an entry in the polling table.
3. Assignment of the new backup connection to the remote site which is to be backed up. This entry is made in the backup table. Dedicated entries in the routing table are not required for a backup connection. The backup connection automatically takes over the source and target networks from the remote site that routes the data under normal operating conditions.

A remote site can be assigned with multiple backup lines in the backup table. In the case of backup, the system decides which backup line is to be used first:

- The last remote site that was reached successfully
- The first remote site in the list

The **maximum backup time** specifies the maximum amount of time in minutes that the backup state is maintained. If a time is specified here, the backup connection is disconnected after this time and the backup state is terminated.

For backup scenarios via a cellular connection (multi-SIM), where for technical reasons the cellular module can only maintain one connection at a time, it is only the termination of the backup state that triggers the main connection to attempt to reconnect.

Regardless of the scenario, the backup event occurs again if the main connection cannot be re-established by the time the backup time delay (set elsewhere than this dialog) expires.

The backup table in LANconfig is located under **Communication > Call management** under **Backup table**.

Backup table - New Entry

Remote site: Select

Backup list: Select

Begin with:

☒ the last successfully reached remote site

☐ the first remote site

Maximum backup time: minutes

OK Cancel

16.1.2 Additions to the Setup menu

Fallback minutes

Specifies the maximum amount of time in minutes that the backup state is maintained. If a time is specified here, the backup connection is disconnected after this time and the backup state is terminated.

For backup scenarios via a cellular connection (multi-SIM), where for technical reasons the cellular module can only maintain one connection at a time, it is only the termination of the backup state that triggers the main connection to attempt to reconnect.

Regardless of the scenario, the backup event occurs again if the main connection cannot be re-established by the time the backup time delay (set elsewhere than this dialog) expires.

SNMP ID:

2.2.24.4

Telnet path:

Setup > WAN > Backup-Peers

Possible values:

Max. 4 characters from 0123456789

Default:

0

Special values:

0

The backup connection remains active permanently.

17 Other services

A single device offers a range of services for the PCs on the LAN. These are essential functions for use by the workstations. In particular these are:

- Automatic address management with DHCP
- Name administration of computers and networks by DNS
- Network traffic logging with SYSLOG
- Charging
- Office communications with LANCAPI
- Time server

17.1 Prefer perfect forward secrecy (PFS) for connections

As of LCOS version 9.10 it is possible to enter a PFS encryption method (cipher suite) irrespective of whether the client has a different setting.

17.1.1 Additions to the Setup menu

Prefer PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

SNMP ID:

2.11.29.6

Telnet path:

Setup > Config > Telnet-SSL

Possible values:

On
Off

Default:

On

Prefer PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

SNMP ID:

2.21.40.7

Telnet path:

Setup > HTTP > SSL

Possible values:

On
Off

Default:

On

Prefer PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

SNMP ID:

2.25.10.10.19.6

Telnet path:

Setup > RADIUS > Server > EAP > EAP-TLS

Possible values:

On
Off

Default:

On

Prefer PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

SNMP ID:

2.25.20.5

Telnet path:

Setup > RADIUS > RADSEC

Possible values:

On
Off

Default:

On

17.2 E-mail notification from the Content Filter

As of LCOS version 9.10, it is possible to send e-mail notifications about the causes of content-filter events, either immediately or daily depending on the cause.

17.2.1 Options for the LANCOM Content Filter

Under **Content Filter > Options** you determine whether you wish to be notified of events and where LANCOM Content Filter information is to be stored.

Event notification

Here you may define how to be informed about particular events.

Events...

E-Mail recipient:

Save information

Specify whether the device should regularly store an content filter snapshot.

☐ Content filter snapshot activated

Interval: monthly

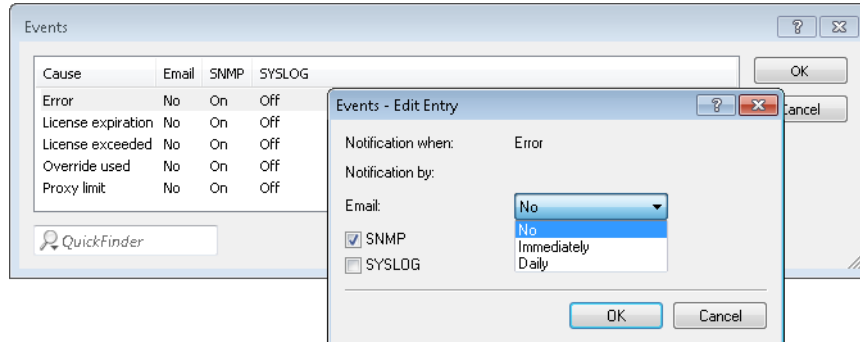
Day of month: 1

Day of week: Monday

Time of day: 00 : 00

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. For different event types you can specify whether messages should be output and, if so, how many.



E-mail

Here, you specify if and how e-mail notification takes place:

No

No e-mail notification is issued for this event.

Immediately

Notification occurs when the event occurs.

Daily

The notification occurs once per day.

Notifications can be sent for the following events:

Error

For SYSLOG: Source „System“, priority „Alert“.

Default: SNMP notification

License expiry

For SYSLOG: Source „Admin“, priority „Alert“.

Default: SNMP notification

License exceeded

For SYSLOG: Source „Admin“, priority „Alert“.

Default: SNMP notification

Override applied

For SYSLOG: Source „Router“, priority „Alert“.

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 specified.

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.

Day of week

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 of day:

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
- Default: 00:00

17.2.2 Additions to the Setup menu

E-mail

Here you specify whether you want to receive notifications by e-mail.

The option presettings differ depending on the cause.

SNMP ID:

2.41.2.2.9.2

Telnet path:

Setup > UTM > Content Filter > Global settings > Notifications

Possible values:

Off
Immediate
Daily

17.3 TACACS+ extension for the passwd command

As of LCOS version 9.10, a user password can additionally be changed using the console command `passwd` even with TACACS+ authentication enabled.

Table 13: Overview of all commands available at the command line

Command	Description
<code>setpass passwd [-u <User>] [-n <new> <old>]</code>	<p>Changes the password of the current user account.</p> <p>In order to change the password without a subsequent input prompt, use the option switch <code>-n</code> while entering the new and old password.</p> <p>In order to change the password of the local user account when authentication by TACACS+ is enabled, use the option switch <code>-u</code> with the name of the corresponding user. If the local user does not exist or the user name is missing, the command aborts. The user must also have supervisor rights, or authorization by TACACS must be enabled.</p>


17.4 Input field for DHCP options extended to 251 characters

As of LCOS version 9.10, it is possible to enter 251 characters when specifying DHCP options.

17.4.1 Additions to the Setup menu

Option value

This field defines the contents of the DHCP option. IP addresses are normally specified using the conventional IPv4 notation, e.g. `123.123.123.100`. Integer tapes are usually entered in decimal digits and string types as simple text. Multiple values in a single field are separated with commas, e.g. `123.123.123.100, 123.123.123.200`.

 The maximum possible length value depends on the selected option number. RFC 2132 lists the maximum length allowed for each option.

SNMP ID:

2.10.21.3

Telnet path:

Setup > DHCP > Additional-Options

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_``

Default:

empty

18 Other parameters

18.1 Profile

Displays the profile of the cellular modem.

SNMP ID:

1.49.45

Telnet path:

Status > Modem-Mobile

18.2 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

SNMP ID:

2.11.29.7

Telnet path:

Setup > Config > Telnet-SSL

Possible values:

Forbidden

The device disconnects from the remote station if this requests a renegotiation.

Allowed

The device permits renegotiations with the remote station.

Ignored

The device ignores the request to renegotiate sent by the remote station.

Default:

Allowed

18.3 TLS connections

In this directory, you specify the address and port to be used by the device to accept incoming configuration changes.

SNMP ID:

2.11.51.3

Telnet path:

Setup > Config > Sync

18.3.1 Port

Specify the port to be used by the device to receive incoming configuration changes.

SNMP ID:

2.11.51.3.1

Telnet path:

Setup > Config > Sync > TLS-Connections

Possible values:

Max. 5 characters from [0–9]

0 ... 65535

Default:

1941

18.4 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

SNMP ID:

2.21.40.8

Telnet path:

Setup > HTTP > SSL

Possible values:

Forbidden

The device disconnects from the remote station if this requests a renegotiation.

Allowed

The device permits renegotiations with the remote station.

Ignored

The device ignores the request to renegotiate sent by the remote station.

Default:

Allowed

18.5 LBS-Tracking

This entry enables or disables the LBS tracking for this SSID.

SNMP ID:

2.23.20.1.25

Telnet path:

Setup > Interfaces > WLAN > Network

Possible values:**No**

LBS tracking is disabled.

Yes

LBS tracking is enabled.

18.6 LBS-Tracking-List

With this entry, you set the list name for the LBS tracking. When a client successfully associates with this SSID, the client transfers the specified list name, the MAC address of the access point, and its own MAC address to the LBS server.

SNMP ID:

2.23.20.1.26

Telnet path:

Setup > Interfaces > WLAN > Network

Possible values:

Name from Setup > WLAN > Network > LBS-Tracking

Max. 16 characters from `[A-Z][0-9]@{ }~!$%&'()+-,:;<=>?[\]^_.`

Default:*empty*

18.7 OKC

This option enables or disables the opportunistic key caching (OKC).

The device uses this value only if the interface works in client mode. The interface is in AP mode, the enabling or disabling of OKC is only possible by means of profile management with a WLC.

In the PMK caching status under **Status > WLAN > PMK-Caching > Contents**, OKC PMKs can be identified by the authenticator address `ff:ff:ff:ff:ff:n`, where `n` is the assigned profile number (e.g. 0 for "WLAN-1", 1 for "WLAN1-2", etc.).

SNMP ID:

2.23.20.3.17

Telnet path:**Setup > Interfaces > WLAN > Encryption****Possible values:****Yes****No****Default:**

Yes

18.8 Network name

Enter a unique name for the network where this WLAN interface is located.

SNMP ID:

2.23.20.5.15

Telnet path:**Setup > Interfaces > WLAN > Interpoint-Settings****Possible values:**Max. 32 characters from `[A-Z][0-9]{ | }~!$%&'()+-./:;<=>?[\]^_.`**Default:***empty*

18.9 Manage user wizard

In this entry, you will find the advanced settings for the **Public Spot Manage Users** wizard.

SNMP ID:

2.24.44

Telnet path:

Setup > Public-Spot-Module

18.9.1 Show status information

This entry gives you the option to hide status information in the Setup Wizard.

SNMP ID:

2.24.44.10

Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

Possible values:

No

The Setup Wizard hides the following columns: **Online-Time**, **Traffic**, **Status**, **MAC-Address**, **IP-Address**.

Yes

The Setup Wizard displays all status information.

18.10 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

SNMP ID:

2.25.20.6

Telnet path:

Setup > RADIUS > RADSEC

Possible values:

Forbidden

The device disconnects from the remote station if this requests a renegotiation.

Allowed

The device permits renegotiations with the remote station.

Ignored

The device ignores the request to renegotiate sent by the remote station.

Default:

Allowed

18.11 LBS-Tracking-List

With this entry, you set the list name for the LBS tracking. When a client successfully associates with this SSID, the client transfers the specified list name, the MAC address of the AP, and its own MAC address to the LBS server.

SNMP ID:

2.37.1.1.47

Telnet path:

Setup > WLAN-Management > AP-Configuration

Possible values:

Name from **Setup > WLAN-Management > AP-Configuration > LBS-Tracking**

Max. 16 characters from `[A-Z][0-9]@{ | }~!$%&'()+- , / : ; < = > ? [\] ^ _ .`

Default:

empty

18.12 Max. number of concurrent updates

Here you specify how many firmware updates the WLC may perform at the same time.

SNMP ID:

2.37.27.38

Telnet path:

Setup > WLAN-Management > Central-Firmware-Management

Possible values:

1-30
10

Default:

10

18.13 CAPWAP-Port

In this entry, you specify the CAPWAP port for the WLAN controller.

SNMP ID:

2.59.5

Telnet path:

Setup > WLAN-Management

Possible values:

Max. 5 characters from [0–9]
0 ... 65535

Default:

1027

18.14 RS count

Configures the number of IPv6 router solicitations that the device should send after the IPv6 LAN interface is started.

SNMP ID:

2.70.6.13

Telnet path:

Setup > IPv6 > LAN-Interfaces

Possible values:

Max. 1 characters from [0–9]

Default:

3

18.15 RS count

Configures the number of IPv6 router solicitations that the device should send after the IPv6 WAN interface is started.

SNMP ID:

2.70.7.11

Telnet path:

Setup > IPv6 > WAN-Interfaces

Possible values:

Max. 1 characters from [0–9]

Default:

3

18.16 Flash restore

With the device in test mode, you can restore the configuration from the Flash memory. You do this from the command-line interface with the command `do/Other/Flash-Restore`. This command restores the original configuration that was active before executing the command "Flash No" from the Flash memory.

SNMP ID:

4.7

Telnet path:

Other > Flash-Restore

18.17 Additions to the Status menu

18.17.1 DSLAM chipset manufacturer dump

Displays additional information provided by the manufacturer of the DSLAM chipset. The content is variable and depends on the manufacturer.

SNMP ID:

1.41.25.47

Telnet path:

Status > ADSL > Advanced

18.17.2 DSLAM manufacturer dump

Displays additional information provided by the manufacturer of the DSLAM. The content is variable and depends on the manufacturer.

SNMP ID:

1.41.25.48

Telnet path:

Status > ADSL > Advanced

18.17.3 DSLAM chipset manufacturer dump

Displays additional information provided by the manufacturer of the DSLAM chipset. The content is variable and depends on the manufacturer.

SNMP ID:

1.75.25.47

Telnet path:

Status > VDSL > Advanced

18.17.4 DSLAM manufacturer dump

Displays additional information provided by the manufacturer of the DSLAM. The content is variable and depends on the manufacturer.

SNMP ID:

1.75.25.48

Telnet path:

Status > VDSL > Advanced