LANCOM SD-WAN Gateways

Security-Relevant Settings

06/2025

LANCOM SYSTEMS

Contents

1 LCOS Version and Syntax Description

This document describes the security-relevant settings of LCOS-based SD-WAN gateways. It serves as a reference for device administration and the secure operation of LANCOM SD-WAN gateways.

The described settings apply to devices with at least LCOS version 10.90. To ensure comprehensive protection, particularly in the area of central administrator management, the features of this LCOS version are required.

For all listed configuration parameters, the associated command-line path, the necessary commands to set the parameters, and an overview of the possible values are provided.

Example scripts are generally reduced to the columns relevant for understanding.

2 Management

2.1 Password Quality

The security of password protection largely depends on the complexity and randomness of the chosen password. LCOS allows passwords for local administrator accounts with a length of up to 128 characters.

The password should be randomly generated and consist of at least eight characters. It should include at least three of the following four character classes: lowercase letters, uppercase letters, digits, and special characters.

CLI Setting for Root Password

```
passwd                  change password
passwd -n new [old]     change password (no prompt)
```

2.2 Brute-Force Protection

Password protection for local authentication is further reinforced by brute-force protection. Repeated incorrect password entries result in the access being locked for a configurable duration.

Path

```
/Setup/Config
/Setup/Voice-Call-Manager/General
```

Command

```
set /Setup/Config/Login-Errors 5
set /Setup/Config/Lock-Minutes 5
set /Setup/Voice-Call-Manager/General/Login-Errors 5
set /Setup/Voice-Call-Manager/General/Lock-Minutes 5
```

Possible Entries

```
Login-Errors            : 2 chars from: 1234567890
Lock-Minutes            : 2 chars from: 1234567890
```

2.3 SSH Parameters

The following menu is used to configure the security-relevant parameters for SSH usage.

Path

```
/Setup/Config/SSH
```

Command

```
set cipher-algorithms aes128-cbc,aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr,chacha20-poly1305,
    aes128-gcm,aes256-gcm
set DH-Groups Group-14,Group-15,Group-16,Group-17,Group-18
set Elliptic-Curves nistp256,nistp384,nistp521
set Signing-Hostkey-Algorithms ssh-ed25519,ssh-ed448,ecdsa-sha2,rsa-sha2-256,rsa-sha2-512
```

```
set Key-Exchange-Algorithms diffie-hellman-group-exchange-sha256,ecdh-sha2,curve25519-sha256,curve448-sha512,
    sntrup761x25519-sha512,diffie-hellman-group14-sha256,diffie-hellman-group15-sha512,
    diffie-hellman-group16-sha512
set MAC-Algorithms hmac-sha2-256,hmac-sha2-512,hmac-sha2-256-etm,hmac-sha2-512-etm
set Max-Hostkey-Length 8192
set Min-Hostkey-Length 2048
```

Possible Entries

```
[  1] Cipher-Algorithms             : Bitmask: 3des-cbc (1), 3des-ctr (2), arcfour (4), arcfour128 (8),
                                               arcfour256 (16), blowfish-cbc (32), blowfish-ctr (64),
                                               aes128-cbc (128), aes192-cbc (256), aes256-cbc (512),
                                               aes128-ctr (1024), aes192-ctr (2048), aes256-ctr (4096),
                                               chacha20-poly1305 (8192), aes128-gcm (16384),
                                               aes256-gcm (32768)
[  2] MAC-Algorithms                : Bitmask: hmac-md5-96 (1), hmac-md5 (2), hmac-sha1-96 (4), hmac-sha1 (8),

                                               hmac-sha2-256-96 (16), hmac-sha2-256 (32),
                                               hmac-sha2-512-96 (64), hmac-sha2-512 (128),
                                               hmac-md5-96-etm (256), hmac-md5-etm (512),
                                               hmac-sha1-96-etm (1024), hmac-sha1-etm (2048),
                                               hmac-sha2-256-96-etm (4096), hmac-sha2-256-etm (8192),
                                               hmac-sha2-512-96-etm (16384), hmac-sha2-512-etm (32768)
[  3] Key-Exchange-Algorithms       : Bitmask: diffie-hellman-group1-sha1 (1),
                                               diffie-hellman-group14-sha1 (2),
                                               diffie-hellman-group-exchange-sha1 (4),
                                               diffie-hellman-group-exchange-sha256 (8), ecdh-sha2 (16),
                                               curve25519-sha256 (32), curve448-sha512 (64),
                                               sntrup761x25519-sha512 (128),
                                               diffie-hellman-group14-sha256 (256),
                                               diffie-hellman-group15-sha512 (2048),
                                               diffie-hellman-group16-sha512 (512),
                                               diffie-hellman-group17-sha512 (4096),
                                               diffie-hellman-group18-sha512 (8192),
                                               sntrup4591761x25519-sha512 (1024)
[  7] DH-Groups                     : Bitmask: Group-1 (1), Group-5 (2), Group-14 (4), Group-15 (8),
                                               Group-16 (16), Group-17 (32), Group-18 (64)
[  8] Compression                   : No (0), Yes (1)
[  9] Elliptic-Curves               : Bitmask: nistp256 (1), nistp384 (2), nistp521 (4)
[ 10] SFTP-Server                   : try 'set SFTP-Server ?'
[ 11] Keepalive-Interval            : 5 chars from 1234567890
[ 12] Operating                     : Bitmask: No (0), Yes (1)
[ 13] Port                          : 5 chars from 1234567890
[ 14] Authentication-Methods        : try 'set Authentication-Methods ?'
[ 15] Signing-Hostkey-Algorithms    : Bitmask: ssh-ed25519 (8), ssh-ed448 (64), ecdsa-sha2 (4), ssh-rsa (1),
                                               rsa-sha2-256 (16), rsa-sha2-512 (32), ssh-dss (2)
[ 16] Verifyable-Hostkey-Algorithms : Bitmask: ssh-ed25519 (8), ssh-ed448 (64), ecdsa-sha2 (4), ssh-rsa (1),
                                               rsa-sha2-256 (16), rsa-sha2-512 (32), ssh-dss (2)
[ 17] Min-RSA-Hostkey-Length        : 5 chars from 1234567890
[ 18] Max-RSA-Hostkey-Length        : 5 chars from 1234567890
[ 19] Nonauth-Disconnect-Time       : 5 chars from 1234567890
[ 20] Max-Auth-Tries                : 5 chars from 1234567890
```

2.3.1 SSH Key Generation under LCOS

To generate an individual key pair – consisting of a public and a private key – proceed as follows:

Command

```
sshkeygen [-q] [-t dsa|rsa|ecdsa|ed25519|ed448] [-b bits] [-f output-file]
```

Possible Parameters

```
[-t dsa|rsa|ecdsa|ed25519|ed448]
```

This parameter defines the type of key to be generated. SSH supports the following key types:

- **RSA** keys are the most widely used and can range in length from 512 to 16,384 bits. Use keys of 3,072 bits whenever possible.
- **DSA** keys follow the Digital Signature Standard (DSS) by the National Institute of Standards and Technology (NIST) and are used, for example, in environments requiring compliance with the Federal Information Processing Standard (FIPS). They always have a length of 1,024 bits but are slower than equivalent RSA keys.

- **ECDSA** keys are a variant of DSA keys that use Elliptic Curve Cryptography (ECC) for key generation. ECC is an alternative to classic signature and key exchange algorithms like RSA and Diffie-Hellman. Its main advantage is that the same level of security can be achieved with shorter key lengths, which improves performance on equivalent hardware. See *RFC 5656* and *RFC 4492* for more information.
- **Ed25519** is based on the Edwards-curve Digital Signature Algorithm (EdDSA), as described in *RFC 8709*.
- **Ed448** is another EdDSA-based method also relying on elliptic curves, specified in *RFC 8709*.

If you do not specify a key type, the command will generate an RSA key by default.

```
-b <Bits>
```

This parameter sets the key length in bits for RSA keys. If omitted, the command generates a 1,024-bit key.

```
-f <OutputFile>
```

This parameter sets the filename for the generated key file in the device's file system. The filename depends on the key type. You can choose from the following:

- `ssh_rsakey` for RSA keys
- `ssh_dsakey` for DSA keys
- `ssh_ecdsakey` for ECDSA keys
- `ssl_privkey` for SSL-RSA keys
- `ssh_ed25519key` for Ed25519 keys
- `ssh_ed448key` for Ed448 keys

```
-q
```

This parameter activates “quiet” mode for key generation. Existing RSA or DSA keys are overwritten without prompting, and no progress messages are displayed. Use this option in scripts to suppress interactive prompts.

2.4 Central Authentication

In installations with multiple responsible administrators, local management of administrator accounts should be avoided whenever possible.

When central authentication is enabled, no additional local accounts are available!

To ensure functional disaster recovery, an optional fallback to the local root account can be configured. In this case, special attention must be paid to the quality and security of the root password.

Path

```
/Setup/TACACS+
/Setup/TACACS+/Server
/Setup/Config/Authentication
```

Command

```
set /Setup/Config/Authentication
set /Setup/TACACS+/Shared-Secret "***"
set /Setup/TACACS+/Encryption activated
set /Setup/TACACS+/Connection-Timeout 5
set /Setup/TACACS+/Fallback-to-local-users allowed
```

Possible Entries

```
Authentication           : Intern (0), Radius (1), Tacacs+ (2)
Authorisation            : deactivated (0), activated (1)
Shared-Secret            : 31 chars from: #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789a
                                          bcdefghijklmnopqrstuvwxyz `
Encryption               : deactivated (0), activated (1)
Fallback-to-local-users  : allowed (0), prohibited (1)
```

Command

```
cd /Setup/Tacacs+/Server
tab Server-Address Loopback-Address Compatibility-Mode
add "10.2.3.4"     "INTRANET"       deactivated
cd /
```

Possible Entries

```
[1] Server-Address       : 31 chars from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+,/:;<=>?[\]^_.0123456789-
[2] Loopback-Address     : 16 chars from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+,/:;<=>?[\]^_.0123456789-
[3] Compatibility-Mode   : deactivated (0), activated (1)
```

2.5 Optional Exceptions from TACACS+ Authorization and Accounting

LCOS provides an option to exclude commands executed via the cron table (`/Setup/Config/Cron-Table`), the action table (`/Setup/WAN/Action-Table`), or the `beginscript` command from TACACS+ authorization and accounting functions.

When TACACS+ integration is enabled, access to this option—as well as access to the cron table, the action table, and the `beginscript` command when the switch state is set to `deactivated (0)`—must be handled with particular restriction. Otherwise, administrators could gain unintended workarounds for modifying the configuration.

It is recommended to restrict access to this mechanism exclusively to administrators or automated processes that already have root privileges.

Path

```
/Setup/TACACS+
```

Command

```
set /Setup/TACACS+/ Bypass-Tacacs-for-CRON/scripts/action-table activated
```

Possible Entries

```
Bypass-Tacacs-for-CRON/scripts/action-table: deactivated (0),activated (1)
```

2.6 Exclude SNMP Get Requests from TACACS+ Authorization and Accounting

The TACACS+ functions for authorization and accounting of SNMP GET REQUESTs can be restricted to the setup path or completely disabled in SNMP-monitored networks to reduce the load on TACACS+ servers.

The status path does not contain user-specific information. Nevertheless, a project-specific assessment of the harmlessness of these status data should be conducted.

Complete deactivation of monitoring functions for SNMP GET REQUESTs is not recommended.

To prevent unauthorized SNMP access, this setting should be strictly controlled and restricted to administrators with root privileges only.

Path

```
/Setup/TACACS+
```

Command

```
set /Setup/Tacacs+/ SNMP-GET-Requests-Authorisation only_for_SETUP_tree
set /Setup/Tacacs+/ SNMP-GET-Requests-Accounting only_for_SETUP_tree
```

Possible Entries

```
SNMP-GET-Requests-Authorisation: only_for_SETUP_tree (0), all (1), none (2)
SNMP-GET-Requests-Accounting: only_for_SETUP_tree (0), all (1), none (2)
```

2.7 SNMPv3

With version 3, the protocol structure of SNMP was fundamentally revised. SNMPv3 is divided into multiple modules with clearly defined interfaces that interact with each other.

The three central components of SNMPv3 are:

- "Message Processing and Dispatch (MPD)" – responsible for processing and forwarding SNMP messages.
- "User-based Security Model (USM)" – defines user-based authentication and encryption.
- "View-based Access Control Mechanism (VACM)" – controls access to MIB objects based on predefined views.

2.7.1 Allow Admins

By default, this option is enabled, allowing registered administrators to access the system via SNMPv3.

Path

```
/Setup/SNMP
```

Command

```
set /Setup/SNMP/Allow-Admins YES
```

2.7.2 Permitted Protocols

Enable the SNMP versions here that the device should support for SNMP requests and SNMP traps.

It is recommended to use SNMPv3 exclusively (default setting).

Path

```
/Setup/SNMP
```

Command

```
set /Setup/SNMP/Admitted-Protocols SNMPv3
```

2.7.3 SNMPv3 Admin Authentication

This parameter defines the authentication method for administrators using SNMPv3.

The method is fixed to **HMAC-SHA256** and cannot be changed.

2.7.4 SNMPv3 Admin Encryption

This parameter defines the encryption settings for administrators using SNMPv3.

The encryption is fixed to **AES256** and cannot be changed.

2.7.5 Users

If individual users—different from administrators—are to be granted SNMPv3 access, they can be added separately. For each user, authentication and encryption methods can be configured individually.

Path

```
/Setup/SNMP/Users
```

Command

```
cd /Setup/SNMP/Users
tab User-Name Authentication-Protocol Authentication-Password Privacy-Protocol Privacy-Password Status
set "User1" "HMAC-SHA256" "9kuufgz76zzh56hft54gjf7" "AES256" "9kuufgz76zzh56hft54gjf7" "active"
```

Possible Entries

```
[ 2] User-Name               : 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.012345678
                                             9abcdefghijklmnopqrstuvwxyz`
[ 5] Authentication-Protocol : None (1), HMAC-MD5 (2), HMAC-SHA (3), HMAC-SHA224 (4), HMAC-SHA256 (5),
                                HMAC-SHA384 (6), HMAC-SHA512 (7)
[ 6] Authentication-Password : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.012345
                                             6789abcdefghijklmnopqrstuvwxyz `
[14] Authentication-Key      : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.012345
                                             6789abcdefghijklmnopqrstuvwxyz `
[ 8] Privacy-Protocol        : None (1), DES (2), AES128 (4), AES192 (20), AES256 (21)
[ 9] Privacy-Password        : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.012345
                                             6789abcdefghijklmnopqrstuvwxyz `
[15] Privacy-Key             : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.012345
                                             6789abcdefghijklmnopqrstuvwxyz `
[13] Status                  : active (1), inactive (2)
```

2.7.6 Groups

In the group configuration, ReadOnly and ReadWrite communities can be defined for SNMPv3.

Path

```
/Setup/SNMP/Groups
```

Command

```
cd /Setup/SNMP/Groups
tab Security.Model Security-Name Group-Name Status
set "SNMPv3(USM)" "User1" "SNMPv3-ReadOnly" "active"
```

Possible Entries

```
[1] Security-Model       : SNMPv1 (1), SNMPv2 (2), SNMPv3(USM) (3)
[2] Security-Name        : 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+,/:;<=>?[\]^_.0123456789abcde
                                         fghijklmnopqrstuvwxyz`
[3] Group-Name           : 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcd
                                         efghijklmnopqrstuvwxyz`
[5] Status               : active (1), inactive (2)
```

2.8 Local Management of Configuration Protocols

LCOS supports a variety of protocols for managing and monitoring its integrated functions. The use of configuration protocols can be centrally configured for LAN, WAN, and optionally WLAN connections.

To protect configuration data from unauthorized access, only encrypted configuration protocols should be used. LCOS supports SSH, SSL, Telnet over SSL, and HTTPS for this purpose.

Unencrypted protocols such as Telnet, HTTP, and TFTP should be disabled or used only over trusted connections, such as IPSec VPN tunnels.

SNMPv1 and SNMPv2 (grouped under the setting “SNMP”) should be completely disabled.

2.8.1 IPv4

Path

```
/Setup/Config/Access-Table
```

Command

```
cd /Setup/Config/Access-Table
tab Ifc. Telnet TFTP HTTP SNMP HTTPS Telnet-SSL SSH Config-Sync SNMPv3
set LAN No No No No Yes Yes Yes Yes Yes
set WAN No No No No Yes Yes Yes No Yes
set WLAN No No No No Yes Yes Yes No Yes
cd /
```

Possible Entries for Columns in Access Table

```
[  1] Ifc.        : value fixed
[  2] Telnet      : VPN (16), Yes (1), Read (4), No (0)
[  3] TFTP        : VPN (16), Yes (1), Read (4), No (0)
[  4] HTTP        : VPN (16), Yes (1), Read (4), No (0)
[  5] SNMP        : VPN (16), Yes (1), Read (4), No (0)
[  6] HTTPS       : VPN (16), Yes (1), Read (4), No (0)
[  7] Telnet-SSL  : VPN (16), Yes (1), Read (4), No (0)
[  8] SSH         : VPN (16), Yes (1), Read (4), No (0)
[ 10] Config-Sync : VPN (16), Yes (1), Read (4), No (0)
[  9] SNMPv3      : VPN (16), Yes (1), Read (4), No (0)
```

2.8.2 IPv6

In the IPv6 inbound firewall, a rule called “DENYALL” exists that blocks all incoming traffic from external sources. Make sure this rule is enabled on your device.

Path

```
/Setup/IPv6/Firewall/Inbound-Rules
```

Command

```
cd /Setup/IPv6/Firewall/Inbound-Rules
tab  Name        Action         Services  Source-Stations  Active  Prio  Src-Tag  Comment
add  "DENY-ALL"  "REJECT-SNMP"  "ANY"     "ANYHOST"        Yes     0     0        "reject all communication
                                                                                   to the device"
cd /
```

Possible Entries

```
[ 1] Name            : 36 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                     case characters are converted to upper case)
[ 5] Action          : 64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                     case characters are converted to upper case)
[ 7] Services        : 64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                     case characters are converted to upper case)
[ 8] Source-Stations : 64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                     case characters are converted to upper case)
[ 2] Active          : Yes (0), No (1)
[ 3] Prio            : 4 chars from 1234567890
[11] Src-Tag         : 5 chars from 1234567890
[10] Comment         : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdef
                                     ghijklmnopqrstuvwxyz `
```

3 Define SSL Protocol Versions

3.1 SSL Protocol Version for HTTPS Connections

Path

```
/Setup/HTTP/SSL
```

Command

```
cd /Setup/HTTP/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[3] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.2 SSL Protocol Version for Telnet Connections

Path

```
/Setup/Config/Telnet-SSL
```

Command

```
cd /Setup/Config/Telnet-SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[2] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.3 SSL Protocol Version for the CPE WAN Management Protocol, TR-069

Path

```
/Setup/CWMP/SSL
```

Command

```
cd /Setup/CWMP/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1.2 (8), TLSv1.3 (16)
```

3.4 SSL Protocol Version for RADSEC

Path

```
/Setup/RADIUS/RADSEC
```

Command

```
cd /Setup/RADIUS/RADSEC
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.5 SSL Protocol Version for the Action Table

Path

```
/Setup/WAN/SSL-for-Action-Table
```

Command

```
cd /Setup/WAN/SSL-for-Action-Table
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.6 SSL Protocol Version for Page Table in the Public Spot Module

Path

```
/Setup/Public-Spot-Module/SSL-for-Page-Table
```

Command

```
cd /Setup/Public-Spot-Module/SSL-for-Page-Table
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.7 SSL Protocol Version for E-Mail2SMS Authentication

Path

```
/Setup/Public-Spot-Module/Authentication-Modules/e-mail2Sms-Authentication/SSL
```

Command

```
cd /Setup/Public-Spot-Module/Authentication-Modules/e-mail2Sms-Authentication/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.8 SSL Protocol Version for RADIUS Server Authentication

Path

```
/Setup/Public-Spot-Module/Authentication-Modules/Radius-Server/SSL
```

Command

```
cd /Setup/Public-Spot-Module/Authentication-Modules/Radius-Server/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.9 SSL Protocol Version for Loading Firmware, Configuration, or Scripts via the Network

Path

```
/Setup/Autoload/Network/SSL
```

Command

```
cd /Setup/Autoload/Network/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.10 SSL Protocol Version for Centralized Firmware Management

Path

```
/Setup/WLAN-Management/Central-Firmware-Management/SSL
```

Command

```
cd /Setup/WLAN-Management/Central-Firmware-Management/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.11 SSL Protocol Version for the Rollout Agent

Path

```
/Setup/Config/Rollout-Agent/SSL
```

Command

```
cd /Setup/Config/Rollout-Agent/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.12 SSL Protocol Version for the Rollout Wizard

Path

```
/Setup/HTTP/Rollout-Wizard/SSL
```

Command

```
cd /Setup/HTTP/Rollout-Wizard/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.13 SSL Protocol Version for the SYSLOG Server

Path

```
/Setup/SYSLOG/SSL
```

Command

```
cd /Setup/SYSLOG/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1.2 (8), TLSv1.3 (16)
```

3.14 SSL Protocol Version for the CRON Table

Path

```
/Setup/Config/SSL-for-Cron-Table
```

Command

```
cd /Setup/Config/SSL-for-Cron-Table
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.15 SSL Protocol Version for Mail

Path

```
/Setup/Mail/SSL
```

Command

```
cd /Setup/Mail/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.16 SSL Protocol Version for SCEP Client

Path

```
/Setup/Certificates/SCEP-Client/SSL
```

Command

```
cd /Setup/Certificates/SCEP-Client/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.17 SSL Protocol Version for ACME Client

Path

```
/Setup/Certificates/ACME-Client/SSL
```

Command

```
cd /Setup/Certificates/ACME-Client/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.18 SSL Protocol Version for IoT

Path

```
/Setup/IoT/Wireless-ePaper/SSL
```

Command

```
cd /Setup/IoT/Wireless-ePaper/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.19 SSL Protocol Version for WLAN Management

Path

```
/Setup/WLAN-Management/Central-Firmware-Management/SSL
```

Command

```
cd /Setup/WLAN-Management/Central-Firmware-Management/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Possible Entries

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.20 Resetting SSL Settings to Default Values

With the command-line instruction `ssldefaults`, SSL settings can be reset to their default values either in the respective configuration path (e.g., `/Setup/Public-Spot-Module/SSL-for-Page-Table`) or globally in the root path.

After the reset, the following protocols are enabled by default:

- TLS 1.2
- TLS 1.3

Command

```
ssldefaults
```

3.21 Local Management of Administrator and Functional Rights

With local rights management, additional administrators can be created alongside the root user to define administrators with different permission levels. These local administrators are available for all supported configuration protocols.

Path

```
/Setup/Config/Admins
```

Command

```
cd /Setup/Config/Admins
tab Administrator Password
add "admin"       "********!"
tab Encrypted-Password
add "$6$2x4/JZ0hJbbkPWgW$TrQ3.dplvHeE/yZQ9ohxDab4W0GfOJqx3M1mO0EsBnLYwUVMcymlzWqv5rCnDQDJlLonryzhLdCK0T.wOaozQ1"
tab Active Access-Rights  Function-Rights SNMP-Encrypted-Password
add Yes    Admin-RO-Limit 0               "7BAC1CBBEED062F29D5B5CDDC81D6D60EBDFBF6B03FB102300544D2D69691C96"
cd /
```

In the example script, an administrator is configured who has read-only access but is restricted from executing trace functions (Limit) and wizards (Functional Rights).

Read-only administrators are not permitted to read password fields within the configuration.

When using centralized authentication for administrators, no additional local administrator accounts can be used.

Possible Entries

```
[1] Administrator           : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/;<=>?[\]^_.0123456789ab
                                            cdefghijklmnopqrstuvwxyz`
[2] Password                : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.01234567
                                             89abcdefghijklmnopqrstuvwxyz `
[6] Encrypted-Password      : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.01234567
                                             89abcdefghijklmnopqrstuvwxyz `
[4] Active                  : No (1), Yes (0)
[5] Access-Rights           : none (0), Admin-RO-Limit (8388608), Admin-RW-Limit (8388864),
                              Admin-RO (16777216), Admin-RW (16777472), Supervisor (4294967295)
[3] Function-Rights         : Bitmask: Basic-Wizard (0x1), Security-Wizard (0x2), Internet-Wizard (0x4),
                                       RAS-Wizard (0x10), Provider-Selection (0x8), LANLAN-Wizard (0x20),
                                       Time-Setting (0x40), Device-Search (0x80), Rollout-Wizard (0x2000),
                                       Public-Spot-Wizard (0x800), Dynamic-DNS-Wizard (0x4000),
                                       VoIP-CallManager-Wizard (0x8000), SSH-Command (0x20000),
                                       CF-Profile-Wizard (0x40000), Public-Spot-Xml-Interface (0x80000),
                                       Public-Spot-User-Management-Wizard (0x100000),
                                       Public-Spot-Configuration-Wizard (0x200000),
                                       Prepare-VoIP-Provider-Access (0x800000), CA-Web-Interface (0x1000000),
                                       User-Wizard-1 (0x2000000), User-Wizard-2 (0x4000000),
                                       User-Wizard-3 (0x8000000), User-Wizard-4 (0x10000000),
                                       Telekom-Internet-Protect-Pro-Wizard (0x20000000)
[7] SNMP-Encrypted-Password : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.01234567
                                             89abcdefghijklmnopqrstuvwxyz `
```

3.22 IPv4 Access List

The TCP access list allows restriction of administrator source addresses per routing context (Rtg tag). Only trusted source networks within management networks should be allowed for configuration access.

Path

```
/Setup/TCP-IP/Access-List
```

Command

```
cd /Setup/TCP-IP/Access-List
tab IP-Address  IP-Netmask  Rtg-tag  Comment
add 10.0.0.0    255.0.0.0   1
cd /
```

If no addresses are defined in the access list, access is permitted from any source address!

Possible Entries

```
[1] Administrator           : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/;<=>?[\]^_.0123456789ab
                                            cdefghijklmnopqrstuvwxyz`
[2] Password                : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.01234567
                                             89abcdefghijklmnopqrstuvwxyz `
[6] Encrypted-Password      : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.01234567
                                             89abcdefghijklmnopqrstuvwxyz `
[4] Active                  : No (1), Yes (0)
[5] Access-Rights           : none (0), Admin-RO-Limit (8388608), Admin-RW-Limit (8388864),
                              Admin-RO (16777216), Admin-RW (16777472), Supervisor (4294967295)
[3] Function-Rights         : Bitmask: Basic-Wizard (0x1), Security-Wizard (0x2), Internet-Wizard (0x4),
                                       RAS-Wizard (0x10), Provider-Selection (0x8), LANLAN-Wizard (0x20),
                                       Time-Setting (0x40), Device-Search (0x80), Rollout-Wizard (0x2000),
                                       Public-Spot-Wizard (0x800), Dynamic-DNS-Wizard (0x4000),
                                       VoIP-CallManager-Wizard (0x8000), SSH-Command (0x20000),
                                       CF-Profile-Wizard (0x40000), Public-Spot-Xml-Interface (0x80000),
                                       Public-Spot-User-Management-Wizard (0x100000),
                                       Public-Spot-Configuration-Wizard (0x200000),
                                       Prepare-VoIP-Provider-Access (0x800000), CA-Web-Interface (0x1000000),
                                       User-Wizard-1 (0x2000000), User-Wizard-2 (0x4000000),
                                       User-Wizard-3 (0x8000000), User-Wizard-4 (0x10000000),
```

```
                                        Telekom-Internet-Protect-Pro-Wizard (0x20000000)
[7] SNMP-Encrypted-Password : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.01234567
                                        89abcdefghijklmnopqrstuvwxyz `
```

3.23 IPv6 Access List

Path

```
/Setup/IPv6/Firewall/Inbound-Rules
```

Command

```
cd /Setup/IPv6/Firewall/Inbound-Rules
tab Name       Action        Services Source-Stations Active Prio Src-Tag Comment
add "DENY-ALL" "REJECT-SNMP"  ANY"    "ANYHOST"       Yes    0    0       "reject all communication to the
                                                                           device"
cd /
```

Possible Entries

```
[ 1] Name            : 36 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                     case characters are converted to upper case)
[ 5] Action          : 64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                     case characters are converted to upper case)
[ 7] Services        : 64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                     case characters are converted to upper case)
[ 8] Source-Stations : 64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                     case characters are converted to upper case)
[ 2] Active          : Yes (0), No (1)
[ 3] Prio            : 4 chars from 1234567890
[11] Src-Tag         : 5 chars from 1234567890
[10] Comment         : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdef
                                     ghijklmnopqrstuvwxyz `
```

3.24 Session Management

To prevent configuration sessions from being taken over without authorization, the permissible idle time of a configuration session should be limited.

Path

```
/Setup/Config
```

Command

```
set /Setup/Config/Config-Aging-Minutes 15 (für TCP basierte Verbindungen)
set /Setup/Config/Outband-Aging-Minutes 5 (für serielle Verbindung)
```

4 Layer 2 Management

LCOS supports the LANCOM Layer 2 Management Protocol (LL2M) for disaster recovery scenarios, allowing devices to be reconfigured or reset to factory defaults via Ethernet without direct physical access.

If this function is not required, it should be disabled. If Layer 2 Management is enabled, it is recommended to restrict access to a configurable time period (in seconds) after the device has rebooted, during which Layer 2 Management access is permitted.

Path

```
/Setup/Config/LL2M
```

Command

```
set /Setup/Config/LL2M/Operating No
set /Setup/Config/LL2M/Time-Limit 0
```

Possible Entries

```
[1] Operating          : No (0), Yes (1), Client-Only (2)
[2] Time-Limit         : 10 chars from 1234567890
[3] Crypto-Algorithms : Bitmask: Simple (2), SHA256 (4), SHA512 (8)
```

5 Theft Protection

The operation of the IP router can be linked to a location check. This theft protection function restricts the operation of the LANCOM router to predefined locations.

The operation of a stolen LANCOM router is thereby significantly hindered or even completely prevented. Depending on the device type, GPS functionality is available for location verification, with varying levels of security.

Path

```
/Setup/Config/Anti-Theft-Protection
```

Command

```
set /Setup/Config/Anti-Theft-Protection/Enabled No
set /Setup/Config/Anti-Theft-Protection/Deviation 50
set /Setup/Config/Anti-Theft-Protection/Get-GPS-Position No
set /Setup/Config/Anti-Theft-Protection/Latitude 12.3456789
set /Setup/Config/Anti-Theft-Protection/Longitude 1.2345678
```

Possible Entries

```
[ 1] Enabled          : No (0), Yes (1)
[ 8] Deviation[m]     : 4 chars from 1234567890
[ 9] Longitude[deg]   : 12 chars from +-.0123456789
[10] Latitude[deg]    : 11 chars from +-.0123456789
[12] Get-GPS-position : No (0), Yes (1)
```

5.1 Offline Configurations

The configuration of LCOS-based devices can be retrieved for offline editing and archiving. Two formats are available for this purpose: the LANconfig configuration in ".lcf" format and the LANCOM Script configuration in ".lcs" format.

The LANconfig configuration represents a complete image of the device configuration. It notably contains the root configuration password in plain text unless the file was downloaded in encrypted form. It is therefore strongly recommended to always download LANconfig configuration files in encrypted form.

The LANCOM Script configurations contain all passwords in plain text after export, with the exception of the root configuration password.

Command

```
Readconfig (LANconfig File Format)
Readscript (LANCOM Script Format)
```

The commands can be executed via TFTP, serial console, HTTP, HTTPS, Telnet, Telnet SSL, and SSH.

Exporting full configurations via these commands is only permitted for administrators with supervisor rights.

All LANCOM configuration files must be considered security-relevant and archived accordingly in a protected manner!

6 Internal Services and Logging

6.1 Service Activation

LCOS provides a wide range of internal services. To prevent potential misuse, services that are not required should be consistently disabled. An overview of currently configured services can be found in the status tree.

Path

```
/Status/config/services
```

6.1.1 DHCP

If dynamic IP address assignment via the LCOS DHCP service is not required, this function can be deactivated separately for each ARF context.

Path

```
/Setup/DHCP/Network-list
```

Command

```
cd /Setup/DHCP/Network-list
tab Network-name Start-Address-Pool End-Address-Pool Netmask Broadcast-Address Gateway-Address DNS-Default
add "INTRANET"   172.16.0.1         172.16.0.254     0.0.0.0 0.0.0.0           0.0.0.0         0.0.0.0
tab DNS-Backup Operating Broadcast-Bit Master-Server 2nd-Master-Server 3rd-Master-Server 4th-Master-Server
add 0.0.0.0    Yes       No            0.0.0.0       0.0.0.0           0.0.0.0           0.0.0.0
tab Loopback-Address Cache Adaption Cluster Max.-Lease Def.-Lease Suppress-ARP-check
add ""               No    No       Yes     0          0          No
cd /
```

Possible Entries

```
[ 1] Network-name       : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789
                                  (lower case characters are converted to upper case)
[ 2] Start-Address-Pool : 15 chars from 1234567890.
[ 3] End-Address-Pool   : 15 chars from 1234567890.
[ 4] Netmask            : 15 chars from 1234567890.
[ 5] Broadcast-Address  : 15 chars from 1234567890.
[ 6] Gateway-Address    : 15 chars from 1234567890.
[ 7] DNS-Default        : 15 chars from 1234567890.
[ 8] DNS-Backup         : 15 chars from 1234567890.
[11] Operating          : No (0), Yes (1), Auto (2), Stateless-Relay (8), Relay (16), Client (4)
[12] Broadcast-Bit      : No (0), Yes (1)
[13] Master-Server      : 15 chars from 1234567890.
[17] 2nd-Master-Server  : 15 chars from 1234567890.
[18] 3rd-Master-Server  : 15 chars from 1234567890.
[19] 4th-Master-Server  : 15 chars from 1234567890.
[22] Loopback-Address   : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                   (lower case characters are converted to upper case)
[14] Cache              : No (0), Yes (1)
[15] Adaption           : No (0), Yes (1)
[16] Cluster            : No (0), Yes (1)
[20] Max.-Lease         : 5 chars from 1234567890
[21] Def.-Lease         : 5 chars from 1234567890
[23] Suppress-ARP-check : No (0), Yes (1)
```

6.1.2 DNS

The LCOS DNS server is capable of resolving both statically configured names and names learned via DHCP. If this function is not required, the service should be deactivated.

DNS forwarding to a defined DNS server is not affected by this setting.

Path

```
/Setup/DNS
```

Command

```
set /Setup/DNS/Operating No
```

Possible Entries

```
Operating : No (0), Yes (1)
```

6.2 Source Route Verification

The internal services in LCOS are capable of performing source route verification. By default, LCOS accepts access to internal services regardless of the source address.

This allows for remote administration of a LANCOM device even without a configured return route. If administration should only be possible from source networks explicitly defined in the routing configuration, source route verification for internal services must be enabled (Src-check: strict).

Path

```
/Setup/TCP-IP/Network-list
```

Command

```
cd /Setup/TCP-IP/Network-list
tab Network-name IP-Address IP-Netmask    VLAN-ID Interface Src-check Type     Rtg-tag Comment
add "INTRANET"   172.16.0.1 255.255.255.0 1       LAN-1     strict    Intranet 1       "local intranet"
cd /
```

Possible Entries

```
[1] Network-name : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower case
                                 characters are converted to upper case)
[2] IP-Address   : 15 chars from 1234567890.
[3] IP-Netmask   : 15 chars from 1234567890.
[4] VLAN-ID      : 4 chars from 1234567890
[5] Interface    : LAN-1 (256), LAN-2 (257), LAN-3 (258), LAN-4 (259), LAN-5 (260), LAN-6 (261), LAN-7 (262),
                   GRE-TUNNEL-1 (2304), GRE-TUNNEL-2 (2305), GRE-TUNNEL-3 (2306), GRE-TUNNEL-4 (2307),
                   GRE-TUNNEL-5 (2308), GRE-TUNNEL-6 (2309), GRE-TUNNEL-7 (2310), GRE-TUNNEL-8 (2311),
                   BUNDLE-1 (2048), BUNDLE-2 (2049), L2TP-ETHERNET-1 (2560), L2TP-ETHERNET-2 (2561),
                   L2TP-ETHERNET-3 (2562), L2TP-ETHERNET-4 (2563), L2TP-ETHERNET-5 (2564),
                   L2TP-ETHERNET-6 (2565), L2TP-ETHERNET-7 (2566), L2TP-ETHERNET-8 (2567),
                   L2TP-ETHERNET-9 (2568), L2TP-ETHERNET-10 (2569), L2TP-ETHERNET-11 (2570),
                   L2TP-ETHERNET-12 (2571), L2TP-ETHERNET-13 (2572), L2TP-ETHERNET-14 (2573),
                  L2TP-ETHERNET-15 (2574), L2TP-ETHERNET-16 (2575), BRG-1 (1536), BRG-2 (1537), BRG-3 (1538),

                   BRG-4 (1539), BRG-5 (1540), BRG-6 (1541), BRG-7 (1542), BRG-8 (1543), any (65535)
[6] Src-check    : strict (1), loose (0)
[7] Type         : Disabled (0), Intranet (1), DMZ (2)
[8] Rtg-tag      : 5 chars from 1234567890
[9] Comment      : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdefghij
                                 klmnopqrstuvwxyz `
```

6.3 Time Settings

In order to evaluate status information in a time-correlated manner, time synchronization via the NTP service should be configured on the device. If authentication is performed using digital certificates, a synchronized time on the LCOS is absolutely essential.

Path

```
/Setup/Time
/Setup/NTP
/Setup/NTP/RQ-Address
```

Command

```
cd /Setup/NTP/RQ-Address
tab RQ-Address                Loopback-Addr. Authentication-Enabled Key-ID
add "NTPS1-0.CS.TU-BERLIN.DE" "INTRANET"     No                     1
add "NTPS1-1.CS.TU-BERLIN.DE" "INTRANET"     No                     1
cd /
```

The LANCOM router can provide the time internally as a time server per network. If this service is not to be used, the time server must be disabled.

Path

```
/Setup/NTP/Networklist
```

Command

```
cd /Setup/NTP/Networklist
tab Network-name Server-Operating
add "INTRANET"   Yes
cd /
```

6.3.1 MD5 Authentication for NTP Server

Enables or disables MD5 authentication for the NTP server.

Path

```
/Setup/NTP
```

Command

```
set /Setup/NTP/Server-Authentication Yes
```

MD5 Keys

The entry contains the value of the key(s).

Path

```
/Setup/NTP/Authentication-Keys
```

Command

```
cd /Setup/NTP/Authentication-Keys
tab Key-ID Key               Key-Type
add 1      "dsajfndyjkvhfhgh" MD5
cd /
```

Possible Entries

```
[1] Key-ID   : 10 chars from 1234567890
[2] Key      : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdefghijklmn
                             opqrstuvwxyz `
[3] Key-Type : MD5 (0), AES-CMAC-128 (1)
```

Trusted Keys

Contains a comma-separated list of trusted keys (key numbers).

Path

```
/Setup/NTP/Server-Trusted_Keys
```

Command

```
set /Setup/NTP/Server-Trusted_Keys [0-9,..]
```

6.3.2 MD5 Authentication for NTP Client

Enables or disables MD5 authentication for the NTP client.

Path

```
/Setup/NTP/RQ-Address
```

Command

```
cd /Setup/NTP/RQ-Address
cd <List entry>
set Authentication-Enabled yes
```

Key Number

Identifies the key used for MD5 authentication by the NTP client.

Path

```
/Setup/NTP/RQ-Address
```

Command

```
cd /Setup/NTP/RQ-Address
cd <List entry>
set Key-ID [1…65535]
```

Possible Entries

```
[1] RQ-Address: 64 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+,/:;<=>?[\]^_.0123456789abcdefghijklmnop
                              qrstuvwxyz`
[2] Loopback-Addr.: 39 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+,/:;<=>?[\]^_.0123456789
[3] Authentication-Enabled: No (0), Yes (1)
[4] Key-ID: 10 chars from 1234567890
```

6.4 Internal and External Event Logging

To ensure comprehensive documentation of internal processes in LCOS, syslog events should be recorded both locally and on an external server. To keep the amount of information manageable, it is advisable to tailor sources and priorities to the specific use case.

The parameter `Log-CLI-Changes` enables logging of command line instructions. When this parameter is active, each command executed via the device's command line is automatically recorded in the internal syslog memory.

Path

```
/Setup/SYSLOG
/Setup/SYSLOG/Server
```

Command

```
set /Setup/SYSLOG/Operating Yes
set /Setup/SYSLOG/ Log-CLI-Changes Yes

cd /Setup/SYSLOG/Server
tab Idx.   IP-Address  Port Protocol RFC5424-Format Source Level Loopback-Addr. Filter-Policy Filter-Name
add "0002" "10.1.1.11" 514  UDP      No             ff     07    "INTRANET"     Allow         ""
add "0001" "127.0.0.1" 514  UDP      No             ff     07    "INTRANET"     Allow         ""
cd /
```

The example script enables syslog messages from all sources with a level of warning or higher, both internally (127.0.0.1) and externally (10.1.1.11).

7 IP and Routing

7.1 Loopback Addresses

If LANCOM routers are to be accessible via dedicated management IP addresses in addition to the interface-bound IP addresses, named loopback addresses can be configured. These can be used for both active and passive communication by the router.

The loopback addresses must be considered in the network's routing. They can be assigned to internal services of the router as sender addresses. The loopback addresses are assigned to the respective ARF contexts via the routing tag.

Path

```
/Setup/TCP-IP/Loopback-List
```

Command

```
cd /Setup/TCP-IP/Loopback-List
tab Name          Loopback-Addr.  Rtg-tag
add "MANAGEMENT"  10.1.2.3        1
cd /
```

Internal services that actively communicate can be assigned a loopback address as the sender address.

7.2 Definition of Virtual Routers

Depending on the device type, LCOS provides between two and up to 256 virtual routers, which can be separated by so-called routing tags.

These virtual routers – also referred to as ARF contexts – can be assigned to physical interfaces and/or VLANs. Identical routing tags allow routing between the associated networks, whereas different routing tags strictly separate the networks from one another.

The routing tag acts as a filter on the routing table and thus determines which routes are available to a specific ARF context.

Path

```
/Setup/TCP-IP/Network-list
```

Command

```
cd /Setup/TCP-IP/Network-list
tab Network-name IP-Address IP-Netmask  VLAN-ID Interface Src-check Type     Rtg-tag Comment
add "INTRANET-1" 10.1.1.11  255.255.0.0 1       LAN-1     loose     Intranet 1
add "INTRANET-2" 10.2.1.11  255.255.0.0 2       LAN-1     loose     Intranet 1
add "OFFICE"     10.5.1.11  255.255.0.0 5       LAN-1     loose     Intranet 5
cd /
```

The assignment of ARF networks to VLANs and interfaces can be verified using the following command:

```
Ifc.: LAN-1
INTRANET 10.1.1.11 255.255.0.0 1
OFFICE   10.5.1.11 255.255.0.0 5
```

In the example shown, three networks are configured. INTRANET-1 and INTRANET-2 share the same routing tag and can therefore be routed between each other. The OFFICE network, however, is logically separated by a different routing tag.

Ensure that networks which should remain isolated from each other are configured with **different** routing tags!

Routing tag 0 designates a supervisor network with unrestricted access to all other networks. Therefore, it should be used with particular caution!

7.3 Using Virtual Routers in Routing

Routing tags define which routes from the global routing table are available to an ARF context (virtual router). An ARF context can only use those routes that match its routing tag.

Additionally, routes with the routing tag **0** are globally visible and thus accessible to all contexts.

Path

```
/Setup/IP-Router/IP-Routing-Table
```

Command

```
cd /Setup/IP-Router/IP-Routing-Table
tab IP-Address IP-Netmask   Rtg-tag Admin-Distance Peer-or-IP     Distance Masquerade Active Comment
add 10.11.0.0  255.255.0.0  1       0              "VPN-INTRANET" 0        No         Yes
add 10.15.0.0  255.255.0.0  5       0              "VPN-OFFICE"   0        No         Yes
cd /
```

Ensure that the routing tag of the respective ARF context matches the routes assigned to it. Any discrepancies may result in unintended routing behavior.

IP packets received on the WAN side are assigned the routing tag **0** by default, making all local networks accessible.

When using dynamic routing, the routing tag of dynamically learned routes can be assigned automatically via the configuration of the peer.

Path

```
/Setup/IP-Router/Tag-Table
```

Command

```
cd /Setup/IP-Router/Tag-Table
tab Peer        Rtg-tag  Start-WAN-Pool  End-WAN-Pool  DNS-Default  DNS-Backup
add "OFFICE-*"  5        0.0.0.0         0.0.0.0       0.0.0.0      0.0.0.0
cd /
```

Possible Entries

```
[1] Peer           : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789 (lower
                                                    case characters are converted to upper case)
[2] Rtg-tag        : 5 chars from 1234567890
[3] Start-WAN-Pool : 15 chars from 1234567890.
[4] End-WAN-Pool   : 15 chars from 1234567890.
[5] DNS-Default    : 15 chars from 1234567890.
[6] DNS-Backup     : 15 chars from 1234567890.
```

The wildcard character * can be used to group multiple peers. Peers sharing the same name prefix will then receive the configured routing tag. This is particularly useful for VPN dial-in clients with individual address pools.

The ARF—defined by its interface, VLAN, and routing tag assignment—serves as the central element for logically separating or linking network segments. It must be ensured that ARF contexts are only associated with the intended routes and peers via the routing tag.

Routing tags can also be used in firewall rules for policy-based routing. Carefully review firewall configurations to ensure correct handling of routing tags and to maintain isolation between ARF contexts.

7.4 Dynamic Routing

LCOS supports RIPv2, OSPFv2, BGPv4, and LISP as dynamic routing protocols.

7.4.1 RIPv2

Since RIPv2 does not provide for authentication, dynamic routing must only be enabled within trusted local networks and with authorized peers.

To prevent unauthorized manipulation of routing information, it must be ensured that RIPv2 does not accept or distribute information from unauthorized participants.

In LAN environments, RIPv2 communication is multicast-based. Therefore, physical access to the Ethernet must be strictly limited to authorized network participants.

For WAN connections, RIPv2 should only be enabled for defined, trusted peers. It must be ensured that directed RIP unicasts are not forwarded across WAN connections.

LAN

Path

```
/Setup/IP-Router/RIP/LAN-Sites
```

Command

```
cd /Setup/IP-Router/RIP/LAN-Sites
tab Network-name RIP-Type RIP-Send RIP-Accept Propagate Poisoned-Reverse Dft-Rtg-Tag Rtg-Tag-List Ignore-Tags
add "OFFICE"     RIP-2    No       Yes        No        No               0           ""           No
tab Rx-Filter Tx-Filter
add ""        ""
cd /
```

Possible Entries

```
[ 1] Network-name     : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                      case characters are converted to upper case)
[ 2] RIP-Type         : Off (0), RIP-1 (1), R1-comp (2), RIP-2 (3)
[12] RIP-Send         : No (0), Yes (1)
[ 3] RIP-Accept       : No (0), Yes (1)
[ 4] Propagate        : No (0), Yes (1)
[ 7] Poisoned-Reverse : No (0), Yes (1)
[ 5] Dft-Rtg-Tag      : 5 chars from 1234567890
[ 6] Rtg-Tag-List     : 33 chars from  ,0123456789
[14] Ignore-Tags      : No (0), Yes (1)
[10] Rx-Filter        : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                      case characters are converted to upper case)
[11] Tx-Filter        : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                      case characters are converted to upper case)
```

WAN

Path

```
/Setup/IP-Router/RIP/WAN-Sites
```

Command

```
cd /Setup/IP-Router/RIP/WAN-Sites
add "OFFICE-WAN"  RIP-2  No  Yes  auto  No  No  0.0.0.0  ""  0  ""  No  ""  ""
cd /
```

Possible Entries

```
[ 1] Peer             : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789
                                      (lower case characters are converted to upper case)
[ 2] RIP-Type         : Off (0), RIP-1 (1), R1-comp (2), RIP-2 (3)
[12] RIP-Send         : No (0), Yes (1)
[ 3] RIP-Accept       : No (0), Yes (1)
[ 4] Masquerade       : auto (0), on (1), intranet (2)
[ 7] Poisoned-Reverse : No (0), Yes (1)
[ 8] RFC2091          : No (0), Yes (1)
[ 9] Gateway          : 15 chars from 1234567890.
[13] Loopback-Address : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                      case characters are converted to upper case)
[ 5] Dft-Rtg-Tag      : 5 chars from 1234567890
[ 6] Rtg-Tag-List     : 33 chars from  ,0123456789
[14] Ignore-Tags      : No (0), Yes (1)
[10] Rx-Filter        : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                      case characters are converted to upper case)
[11] Tx-Filter        : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                      case characters are converted to upper case)
```

7.4.2 OSPFv2

OSPF supports authentication at the interface level. It is recommended to use the authentication type “Cryptographic-MD5”. The password should be randomly generated and have a minimum length of eight characters.

Path

```
/Setup/Routing-Protocols/OSPF/Interfaces
```

Command

```
cd /Setup/Routing-Protocols/OSPF/Interfaces
add "INTRANET" "DEFAULT" 0.0.0.0 Broadcast 1 5 1 1 10 40 Cryptographic-MD5 "********" No No
cd /
```

Possible Entries for Interfaces

```
[ 1] Interface            : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                      (lower case characters are converted to upper case)
[ 2] OSPF-Instance        : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                      (lower case characters are converted to upper case)
[ 3] Area-ID              : 15 chars from 1234567890.
[ 4] Type                 : Broadcast (0), NBMA (2), Point-To-Point (1), Point-To-Multipoint (3)
[ 5] Output-Cost          : 10 chars from 1234567890
[ 6] Rxmt-Interval        : 10 chars from 1234567890
[ 7] Inf-Trans-Delay      : 10 chars from 1234567890
[ 8] Router-Priority      : 3 chars from 1234567890
[ 9] Hello-Interval       : 10 chars from 1234567890
[10] Router-Dead-Interval : 10 chars from 1234567890
[11] Authentication-Type  : Null (0), Simple-Password (1), Cryptographic-MD5 (2)
[12] Authentication-Key   : 16 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789a
                                      bcdefghijklmnopqrstuvwxyz `
[13] Passive              : No (0), Yes (1)
[14] MTU-Ignore           : No (0), Yes (1)
```

If virtual links (transit areas) are used to connect other areas with the backbone area, the authentication type “Cryptographic-MD5” should also be configured for the virtual link.

Path

```
/Setup/Routing-Protocols/OSPF/Virtual-Links
```

Command

```
cd /Setup/Routing-Protocols/OSPF/Virtual-Links
tab OSPF-Instance Transit-Area-ID Router-ID Rxmt-Interval Hello-Interval Router-Dead-Interval
add "DEFAULT"     1.2.3.4         1.1.1.1   5             10             40
tab Authentication-Type Authentication-Key
add Cryptographic-MD5   "********"
cd /
```

Possible Entries for Virtual Links

```
[1] OSPF-Instance        : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                         (lower case characters are converted to upper case)
[2] Transit-Area-ID      : 15 chars from 1234567890.
[3] Router-ID            : 15 chars from 1234567890.
[6] Rxmt-Interval        : 10 chars from 1234567890
[7] Hello-Interval       : 10 chars from 1234567890
[8] Router-Dead-Interval : 10 chars from 1234567890
[4] Authentication-Type  : Null (0), Simple-Password (1), Cryptographic-MD5 (2)
[5] Authentication-Key   : 16 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789ab
                                         cdefghijklmnopqrstuvwxyz `
```

7.4.3 BGPv4

You have the option to authenticate your BGP neighbors using a password. The password should be randomly generated and at least eight characters long.

Path

```
/Setup/Routing-Protocols/BGP/Neighbors
```

Command

```
cd /Setup/Routing-Protocols/BGP/Neighbors
tab IP-Address    Port Loopback-Address Rtg-tag Remote-AS Name Operating Password   Neighbor-Profile
add "10.10.10.10" 179  "65000"          0       0         ""   Yes       "********" "DEFAULT"
tab Connection-Mode Connection-Delay Instance-Name Inbound-Policy Outbound-Policy Route-Reflector-Client
add Active          120              "DEFAULT"     ""             ""              No
tab BFD-Profile Comment
add ""          ""
cd /
```

Possible Entries

```
[ 1] IP-Address             : 56 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                            (lower case characters are converted to upper case)
[ 2] Port                   : 5 chars from 1234567890
[ 3] Loopback-Address       : 56 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                            (lower case characters are converted to upper case)
[ 4] Rtg-tag                : 5 chars from 1234567890
[ 5] Remote-AS              : 10 chars from 1234567890
[ 6] Name                   : 16 chars from -0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz
[ 7] Operating              : No (0), Yes (1)
[ 8] Password               : 16 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.012345678
                                             9abcdefghijklmnopqrstuvwxyz `
[ 9] Neighbor-Profile       : 16 chars from -0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz
[10] Connection-Mode        : Active (0), Passive (1), Delayed (2)
[11] Connection-Delay       : 5 chars from 1234567890
[12] Instance-Name          : 16 chars from -0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz
[13] Inbound-Policy         : 16 chars from -0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz
[14] Outbound-Policy        : 16 chars from -0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz
[16] Route-Reflector-Client : No (0), Yes (1)
[17] BFD-Profile            : 16 chars from -0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz

[15] Comment                : 254 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.01234567
                                              89abcdefghijklmnopqrstuvwxyz`
```

7.5 Proxy ARP

The Proxy ARP mechanism is used to integrate remote networks and IP addresses that fall within a locally defined IP network via WAN connections.

Unless this mechanism is explicitly required and local IP addresses are to be used exclusively within the local Ethernet network, Proxy ARP should be disabled.

Path

```
/Setup/IP-Router
```

Command

```
set /Setup/IP-Router/Proxy-ARP No
```

Possible Entries

```
Proxy-ARP : No (0), Yes (1)
```

7.6 Stealth Mode

A frequently discussed method of increasing network security is the so-called “hiding” of a router, where the device ignores incoming TCP and UDP requests instead of rejecting them as specified by the standard (stealth mode).

This approach is controversial because even silence can reveal the presence of a device. If there is truly no destination device, the upstream router responds with a message such as “unreachable” because it cannot forward the packet. However, if the router does not respond with a rejection, the destination was apparently reachable for it. Regardless of whether the queried receiver responds, this allows its presence to be inferred.

The behavior of an upstream router cannot be simulated without taking the device completely offline—which also makes it unreachable for services requested by itself.

Path

```
/Setup/IP-Router/Firewall
```

Command

```
set /Setup/IP-Router/Firewall/Stealth-Mode WAN
```

Possible Entries

```
Stealth-Mode : off (0), always (1), WAN (2), default-route (3)
```

8 VPN and Firewall

8.1 IKEv2

IKEv2 provides various authentication methods:

- PSK – Authentication using a pre-shared key (secret key agreed upon in advance)
- RSA – Certificate-based authentication
- RSASSA-PSS – Certificate-based authentication using a probabilistic signature scheme
- ECDSA – Certificate-based authentication using elliptic curve cryptography (probabilistic signature scheme)
- EdDSA – Certificate-based authentication using a deterministic signature scheme
- EAP – Authentication via username/password or certificates

LANCOM routers also support the older probabilistic signature scheme according to the `rsassa-pkcs1-v1_5` standard. However, LANCOM recommends using more modern methods such as ECDSA or EdDSA.

Path

```
/Setup/VPN/IKEv2/Auth/Parameter/
/Setup/VPN/IKEv2/Auth/Addit.-Remote-IDs
```

Command

```
cd /Setup/VPN/IKEv2/Auth/Parameter/
tab Name  Local-Auth        Local-Dig-Sig-Profile Local-ID-Type Local-ID  Local-Password Remote-Auth
add "VPN" Digital-Signature DEFAULT-ECDSA         Domain-Name   "GATEWAY" ""             Digital-Signature
tab Remote-Dig-Sig-Profile Remote-EAP-Profile Remote-ID-Type Remote-ID Remote-Password PPK-ID
add DEFAULT-ECDSA          ""                 Domain-Name    "PEER"    ""              ""
tab Addit.-Remote-ID-List Local-Certificate Remote-Cert-ID-Check OCSP-Check CRL-Check
add ""                    ""                No                   No         Yes
cd /
```

Possible Entries for Parameters

```
[ 1] Name                   : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                              (lower case characters are converted to upper case)
[ 2] Local-Auth             : RSA-Signature (1), PSK (2), ECDSA-256 (9), ECDSA-384 (10), ECDSA-521 (11),
                              Digital-Signature (14)
[13] Local-Dig-Sig-Profile  : 20 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                              (lower case characters are converted to upper case)
[ 3] Local-ID-Type          : No-Identity (0), IPv4-Address (1), IPv6-Address (5), Domain-Name (2),
                              Email-Address (3), Distinguished-Name (9), Key-ID (11)
[ 4] Local-ID               : 254 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.0123456
                               789abcdefghijklmnopqrstuvwxyz `
[ 5] Local-Password         : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.012345678
                              9abcdefghijklmnopqrstuvwxyz `
[ 6] Remote-Auth            : RSA-Signature (1), PSK (2), ECDSA-256 (9), ECDSA-384 (10), ECDSA-521 (11),
                              Digital-Signature (14), EAP (201)
[14] Remote-Dig-Sig-Profile : 20 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                              (lower case characters are converted to upper case)
[16] Remote-EAP-Profile     : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                              (lower case characters are converted to upper case)
[ 7] Remote-ID-Type         : No-Identity (0), IPv4-Address (1), IPv6-Address (5), Domain-Name (2),
                              Email-Address (3), Distinguished-Name (9), Key-ID (11)
[ 8] Remote-ID              : 254 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.0123456
                               789abcdefghijklmnopqrstuvwxyz `
[ 9] Remote-Password        : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.012345678
                              9abcdefghijklmnopqrstuvwxyz `
[18] PPK-ID                 : 66 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789a
                              bcdefghijklmnopqrstuvwxyz`
[10] Addit.-Remote-ID-List  : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                              (lower case characters are converted to upper case)
```

```
[11] Local-Certificate      : 254 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.0123456
                                              789abcdefghijklmnopqrstuvwxyz `
[12] Remote-Cert-ID-Check   : No (0), Yes (1)
[15] OCSP-Check             : No (0), Yes (1)
[17] CRL-Check              : No (0), Yes (1)
```

The selected digital signature profile determines the method used and the hash algorithms available for negotiation.

Path

```
/Setup/VPN/IKEv2/Auth/Digital-Signature-Profiles
```

Command

```
cd /Setup/VPN/IKEv2/Auth/Digital-Signature-Profiles
tab  Name                  Auth-Method        Hash-Algorithms
add  "DEFAULT-RSA-PSS"     RSASSA-PSS         SHA-512,SHA-384,SHA-256
add  "DEFAULT-RSA-PKCS"    RSASSA-PKCS1-v1_5  SHA-512,SHA-384,SHA-256
add  "DEFAULT-ECDSA"       ECDSA              SHA-512,SHA-384,SHA-256
add  "DEFAULT-EDDSA25519"  EdDSA25519         IDENTITY
add  "DEFAULT-EDDSA448"    EdDSA448           IDENTITY
cd /
```

Possible Entries for Digital Signature Profiles

```
[1] Name            : 20 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                    (lower case characters are converted to upper case)
[2] Auth-Method     : RSASSA-PSS (1), RSASSA-PKCS1-v1_5 (2), ECDSA (4), EdDSA25519 (8), EdDSA448 (16)
[3] Hash-Algorithms : Bitmask: IDENTITY (16), SHA-512 (1), SHA-384 (2), SHA-256 (4), SHA1 (8)
```

8.1.1 IKEv2 Encryption

LANCOM recommends the use of current Diffie-Hellman groups (DH groups) for secure key exchange. For encryption and integrity validation of both the IKE_SA and Child_SA connections, the strongest and most modern algorithms available should be used.

Path

```
/Setup/VPN/IKEv2/Encryption
```

Command

```
cd /Setup/VPN/IKEv2/Encryption
tab Name      DH-Groups                          PFS IKE-SA-Cipher-List      IKE-SA-Integ-Alg-List
add "DEFAULT" DH30,DH29,DH28,DH21,DH20,DH19,DH16 Yes AES-CBC-256,AES-GCM-256 SHA-512,SHA-384,SHA-256
tab Child-SA-Cipher-List    Child-SA-Integ-Alg-List
add AES-CBC-256,AES-GCM-256 SHA-512,SHA-384,SHA-256
cd /
```

Possible Entries for Encryption

```
[1] Name                    : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                        (lower case characters are converted to upper case)
[2] DH-Groups               : Bitmask: DH32 (4096), DH31 (2048), DH30 (32), DH29 (64), DH28 (128),
                                       DH21 (256),DH20 (512), DH19 (1024), DH16 (1), DH15 (2), DH14 (4),
                                       DH5 (8), DH2 (16)
[3] PFS                     : No (0), Yes (1)
[4] IKE-SA-Cipher-List      : Bitmask: AES-CBC-256 (1), AES-CBC-192 (2), AES-CBC-128 (4), 3DES (8),
                                       AES-GCM-256 (16), AES-GCM-192 (32), AES-GCM-128 (64),
                                       Chacha20-Poly1305 (128)
[5] IKE-SA-Integ-Alg-List   : Bitmask: SHA-512 (1), SHA-384 (2), SHA-256 (4), SHA1 (8), MD5 (16)
[6] Child-SA-Cipher-List    : Bitmask: AES-CBC-256 (1), AES-CBC-192 (2), AES-CBC-128 (4), 3DES (8),
                                       AES-GCM-256 (16), AES-GCM-192 (32), AES-GCM-128 (64),
                                       Chacha20-Poly1305 (128), NULL (256)
[7] Child-SA-Integ-Alg-List : Bitmask: SHA-512 (1), SHA-384 (2), SHA-256 (4), SHA1 (8), MD5 (16)
```

When using certificates, an appropriate validity period should be ensured. It is recommended to use an automated certificate rollout process utilizing the SCEP protocol.

8.1.2 Certificate Management

LCOS enables certificate management either manually or through an automated certificate rollout process. The automatic rollout uses the SCEP protocol (Simple Certificate Enrollment Protocol).

Certificates can be retrieved automatically by the device both initially and within a defined period before their expiration. In addition to automated enrollment, SCEP provides the security advantage that the private key is generated directly on the device and never leaves it.

The private key is stored in a non-readable memory area of the device. In security-critical environments, the use of the SCEP protocol is recommended whenever possible.

Path

```
/Setup/Certificates/SCEP-Client
```

Command

```
set /Setup/Certificates/SCEP-Client/SCEP-Operating Yes
```

Possible Entries

```
SCEP-Operating : No (0), Yes (1)
```

Command

```
cd /Setup/Certificates/SCEP-Client/CAs
tab Name     URL                                        DN                                Enc-Alg Identifier
add "VPN_CA" "http://127.0.0.1/cgi-bin/pkiclient.exe" "/CN=SK CA/O=LANCOM SYSTEMS/C=DE" AES256  ""
tab RA-Autoapprove CA-Signature-Algorithm CA-Fingerprint-Algorithm CA-Fingerprint Loopback-Addr.
add Yes            SHA-256                SHA-256                  ""             ""
cd /
```

Possible Entries

```
[ 1] Name                     : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.012345678
                                              9 (lower case characters are converted to upper case)
[ 2] URL                      : 251 chars from abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
                                               /?.-;:@&=$_+!*'(),%
[ 3] DN                       : 251 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.01234
                                               56789abcdefghijklmnopqrstuvwxyz `
[ 4] Enc-Alg                  : DES (0), 3DES (1), BLOWFISH (2), AES128 (3), AES192 (4), AES256 (5)
[ 5] Identifier               : 251 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.01234
                                               56789abcdefghijklmnopqrstuvwxyz `
[ 7] RA-Autoapprove           : No (0), Yes (1)
[ 6] CA-Signature-Algorithm   : MD5 (0), SHA1 (1), SHA-256 (2), SHA-384 (3), SHA-512 (4)
[ 8] CA-Fingerprint-Algorithm : off (0), SHA1 (1), MD5 (2), SHA-256 (3), SHA-384 (4), SHA-512 (5)
[ 9] CA-Fingerprint           : 192 chars from 1234567890abcdef:-, (upper case characters are converted to
                                               lower case)
[11] Loopback-Addr.           : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.012345678
                                              9 (lower case characters are converted to upper case)
```

Command

```
cd /Setup/Certificates/SCEP-Client/Certificates
tab Name     CADN                                Subject      ChallengePwd SubjectAltName KeyUsage
add "VPN_CA" "/CN=VPN CA/O=LANCOM SYSTEMS/C=DE" "/CN=VPN_CA" "********"   ""            ""
tab Extended-KeyUsage                           Device-Certificate-Keylength Application
add "serverAuth, critical, 1.3.6.1.5.5.7.3.18" 4096                          VPN1
cd /
```

Possible Entries

```
[1] Name                      : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.012345
                                             6789 (lower case characters are converted to upper case)
[2] CADN                      : 251 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.01
                                              23456789abcdefghijklmnopqrstuvwxyz `
[3] Subject                   : 251 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.01
                                              23456789abcdefghijklmnopqrstuvwxyz `
[4] ChallengePwd              : 251 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.012
                                              3456789abcdefghijklmnopqrstuvwxyz `
```

```
[5] SubjectAltName               : 251 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.01
                                                  23456789abcdefghijklmnopqrstuvwxyz `
[6] KeyUsage                     : 251 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.01
                                                  23456789abcdefghijklmnopqrstuvwxyz `
[9] Extended-KeyUsage            : 251 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.01
                                                  23456789abcdefghijklmnopqrstuvwxyz `
[7] Device-Certificate-Keylength : 10 chars from 1234567890
[8] Application                  : VPN1 (0), VPN2 (5), VPN3 (6), VPN4 (7), VPN5 (8), VPN6 (9), VPN7 (10),
                                   VPN8 (11), VPN9 (12), WLan-Controller (1), EAP/TLS (3), Default (13),
                                   CA (14), ConfigSync (15), SYSLOG-PKCS12 (24), SYSLOG-CA (25),
                                   ProvSrv (17), OCSP (18), LBS (20), Wireless-ePaper (21), SCEP-TLS (22),
                                   RADSEC (23), WEBconfig (26), unconfigured (4294967295)
```

8.1.3 VPN Rules

Both manually and automatically generated VPN rules must be checked for correctness using the `show vpn` command.

```
> show vpn

VPN SPD and IKE configuration:

# of connections = 1

Rule #1          ikev2        0.0.0.0/0 ANY ANY <-> 0.0.0.0/0 ANY ANY
    Name:                       VPN-CONNECTION
    Unique Id:                  IPSEC-0-VPN-CONNECTION-PR0-L0-R0
    Local  Gateway:             IPV6_ADDR(any:0, 2001:4dd0:af17:8e5e:a0:57ff:fe9c:47fe)
    Remote Gateway:             IPV6_ADDR(any:0, 2003:cf:3fff:2243:a0:57ff:feff:9a44)
```

8.1.4 IPv4 Firewall Strategy

The LCOS IPv4 firewall uses an “allow all” strategy in its factory default configuration. To ensure the highest level of data security during data transfers, the firewall strategy should initially be changed to the restrictive “deny all” principle.

Only explicitly desired data communication should be allowed at the boundaries between trusted and untrusted networks.

Path

```
/Setup/IP-Router/Firewall/Rules
```

Command

```
cd /Setup/IP-Router/Firewall/Rules
tab Name      Prot. Source    Destination Action            Firewall
add "DENYALL" "ANY" "ANYHOST" "ANYHOST"   "%Lcds0 %R %Lcd0" Yes
cd /
```

Possible Entries

```
[ 1] Name          : 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                   case characters are converted to upper case)
[ 2] Prot.         : 10 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefgh
                                    ijklmnopqrstuvwxyz`
[ 3] Source        : 40 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefgh
                                    ijklmnopqrstuvwxyz`
[ 4] Destination   : 40 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefgh
                                    ijklmnopqrstuvwxyz`
[ 7] Action        : 40 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefgh
                                    ijklmnopqrstuvwxyz`
[16] LB-Policy     : 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                   case characters are converted to upper case)
[17] LB-Switchover : No (0), Yes (1)
[ 8] Linked        : No (0), Yes (1)
[ 9] Prio          : 4 chars from 1234567890
[10] Firewall-Rule : No (1), Yes (0)
[12] Stateful      : No (1), Yes (0)
[15] Src-Tag       : 5 chars from 1234567890
[14] Rtg-tag       : 5 chars from 1234567890
[13] Comment       : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdefgh
                                   ijklmnopqrstuvwxyz
```

8.1.5 IPv6 Firewall Strategy

The LCOS IPv6 firewall uses a “deny all” strategy in its factory default configuration to ensure the highest level of data security during data transfers.

Only explicitly desired data communication should be allowed at the boundaries between trusted and untrusted networks.

Path

```
/Setup/IPv6/Firewall/Forwarding-Rules
```

Command

```
cd /Setup/IPv6/Firewall/Forwarding-Rules
tab Name      Action        Services Source-Stations
add "DENYALL" "REJECT-SNMP" "ANY"    "ANYHOST"
cd /
```

Possible Entries

```
[ 1] Name                : 36 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                         (lower case characters are converted to upper case)
[ 5] Action              : 64 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                         (lower case characters are converted to upper case)
[ 7] Services            : 64 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                         (lower case characters are converted to upper case)
[ 8] Source-Stations     : 64 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                         (lower case characters are converted to upper case)
[ 9] Destination-Stations : 64 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                         (lower case characters are converted to upper case)
[12] LB-Policy           : 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                         (lower case characters are converted to upper case)
[ 2] Flags               : Bitmask: none (0), deactivated (1), linked (4), stateless (8), LB-Switchover (16)
[ 3] Prio                : 4 chars from 1234567890
[11] Src-Tag             : 5 chars from 1234567890
[ 4] Rtg-tag             : 5 chars from 1234567890
[10] Comment             : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789a
                                         bcdefghijklmnopqrstuvwxyz `
```

8.1.6 Firewall Session Management, IDS and DoS

The LCOS firewall operates as a stateful inspection firewall. To prevent potential attacks via allowed protocols, firewall rules should generally be defined as stateful.

Additionally, LCOS analyzes the current state of IP connections to detect and block port scans and denial-of-service (DoS) attacks. For this protection to be effective, the IDS and DoS module actions must be set to “Reject” or “Drop”.

The respective threshold values should be adapted to the specific network environment.

Path

```
/Setup/IP-Router/Firewall
/Setup/IP-Router/Firewall/Rules
```

Command

```
set /Setup/IP-Router/Firewall/Max.-Half-Open-Conns. 100
```

Possible Entries

```
Max.-Half-Open-Conns. : 4 chars from: 1234567890
```

Command

```
set /Setup/IP-Router/Firewall/DoS-Action "%d%n"
```

Possible Entries

```
DoS-Action : 29 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopq
                           rstuvwxyz`
```

Command

```
set /Setup/IP-Router/Firewall/Port-Scan-Threshold 50
```

Possible Entries

```
Port-Scan-Threshold : 4 chars from: 1234567890
```

Command

```
set /Setup/IP-Router/Firewall/IDS-Action "%d%n"
```

Possible Entries

```
IDS-Action : 29 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopq
                           rstuvwxyz`
```

Command

```
cd /Setup/IP-Router/Firewall/Rules
tab Name        Prot. Source Destination Action LB-Policy LB-Switchover Linked Prio Firewall-Rule Stateful
add "ALLOW-XYZ" ""    ""     ""          "%A"   ""        No            No     0    Yes           Yes
tab Src-Tag Rtg-tag Comment
add 0       0       ""
cd /
```

Possible Entries

```
[ 1] Name          : 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                   case characters are converted to upper case)
[ 2] Prot.         : 10 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefgh
                                    ijklmnopqrstuvwxyz`
[ 3] Source        : 40 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefgh
                                    ijklmnopqrstuvwxyz`
[ 4] Destination   : 40 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefgh
                                    ijklmnopqrstuvwxyz`
[ 7] Action        : 40 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefgh
                                    ijklmnopqrstuvwxyz`
[16] LB-Policy     : 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                   case characters are converted to upper case)
[17] LB-Switchover : No (0), Yes (1)
[ 8] Linked        : No (0), Yes (1)
[ 9] Prio          : 4 chars from 1234567890
[10] Firewall-Rule : No (1), Yes (0)
[12] Stateful      : No (1), Yes (0)
[15] Src-Tag       : 5 chars from 1234567890
[14] Rtg-tag       : 5 chars from 1234567890
[13] Comment       : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdefgh
                                   ijklmnopqrstuvwxyz `
```

The following basic parameters are available as actions:

```
ACCEPT %A
DROP   %D
REJECT %R
```

The firewall rules effectively evaluated by the router can be verified using the following tools:

Command

```
show filter

Filter 0001 from Rule DENYALL:
  Protocol: 0
  Src: 00:00:00:00:00:00 0.0.0.0 0.0.0.0 0-0
  Dst: 00:00:00:00:00:00 0.0.0.0 0.0.0.0 0-0
  use routing tag 0000
  Limit per conn.: after transmitting or receiving of 0 kilobits per second
  actions after exceeding the limit:
      reject
  Limit per conn.: after transmitting or receiving of 0 kilobits
  actions after exceeding the limit:
      accept
```

The correct operation of the filtering rules can be verified in the firewall's status information. To do this, the desired IP connections should be established deliberately. The overview of open IP connections in the firewall displays which firewall rule was applied to each connection.

Path

```
/Status/IP-Router/Connection-List
```

To prevent established IP connections from being misused, LCOS removes the corresponding entries from the connection list after the connection has been properly closed or after a defined idle timeout has expired. The IP connection must then be re-established in accordance with standard procedures.

The timeouts can be adjusted to match the respective applications using the following settings.

To prevent attacks using non-standard-compliant fragmented packets, IP fragmentations should be properly reassembled by LCOS.

Path

```
/Setup/IP-Router/1-N-NAT
```

Command

```
set /Setup/IP-Router/1-N-NAT/TCP-Aging-Seconds 300
set /Setup/IP-Router/1-N-NAT/UDP-Aging-Seconds 120
set /Setup/IP-Router/1-N-NAT/ICMP-Aging-Seconds 10
set /Setup/IP-Router/1-N-NAT/Fragments Reassemble
set /Setup/IP-Router/1-N-NAT/Fragment-Aging-Seconds 5
set /Setup/IP-Router/1-N-NAT/IPSec-Aging-Seconds 2000
```

The correct functioning of the filter rules can be verified in the firewall status information. To do this, the corresponding IP connections must be established. The overview of active IP connections shows which firewall rule was applied to each connection.

Possible Entries

```
TCP-Aging-Seconds      : 5 chars from: 1234567890
UDP-Aging-Seconds      : 5 chars from: 1234567890
ICMP-Aging-Seconds     : 5 chars from: 1234567890
Fragments              : Filter (0), Route (1), Reassemble (2)
Fragment-Aging-Seconds : 3 chars from: 1234567890
IPSec-Aging-Seconds    : 5 chars from: 1234567890
IPSec-Table            : try 'set IPSec-Table ?'
```