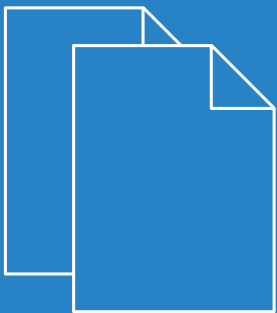


LCOS FX 10.7

Addendum



Contents

1 Addendum to LCOS FX version 10.7.....	4
2 Netmap.....	5
3 Certificate Management.....	8
3.1 Certificates.....	8
3.1.1 Overview of certificates.....	8
3.1.2 Private key password.....	15
3.2 Templates.....	16
3.2.1 Templates overview.....	16
3.2.2 Settings for templates.....	16
3.3 Proxy CAs.....	17
3.3.1 Trusted proxy CAs.....	17
3.3.2 Untrusted proxy CAs.....	17
4 WWAN.....	18
4.1 WWAN Connections.....	18
4.1.1 WWAN Connections Overview.....	18
4.1.2 WWAN Connections Settings.....	18
4.2 WWAN Interfaces.....	20
4.2.1 WWAN Interfaces Overview.....	20
4.2.2 WWAN Interfaces Settings.....	20

Copyright

© 2022 LANCOM Systems GmbH, Würselen (Germany). All rights reserved.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from LANCOM Systems. We reserve the right to make any alterations that arise as the result of technical development.

Windows® and Microsoft® are registered trademarks of Microsoft, Corp.

LANCOM, LANCOM Systems, LCOS, LANcommunity and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions.

This product contains separate open-source software components which are subject to their own licenses, in particular the General Public License (GPL). If the respective license demands, the source files for the corresponding software components will be provided on request. Please send an e-mail to gpl@lancom.de.

Products from LANCOM Systems include software developed by the "OpenSSL Project" for use in the "OpenSSL Toolkit" (www.openssl.org).

Products from LANCOM Systems include cryptographic software written by Eric Young (ey@cryptsoft.com).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Germany

www.lancom-systems.com

1 Addendum to LCOS FX version 10.7

This document describes the changes and enhancements in LCOS FX version 10.7 since the previous version.

2 Netmap

From LCOS FX version 10.7 it is possible to make SNAT and DNAT settings for entire networks. The previous option of NAT for individual services is of course still available.

For this purpose, the new tab **NAT** was added to in the Connection dialog:

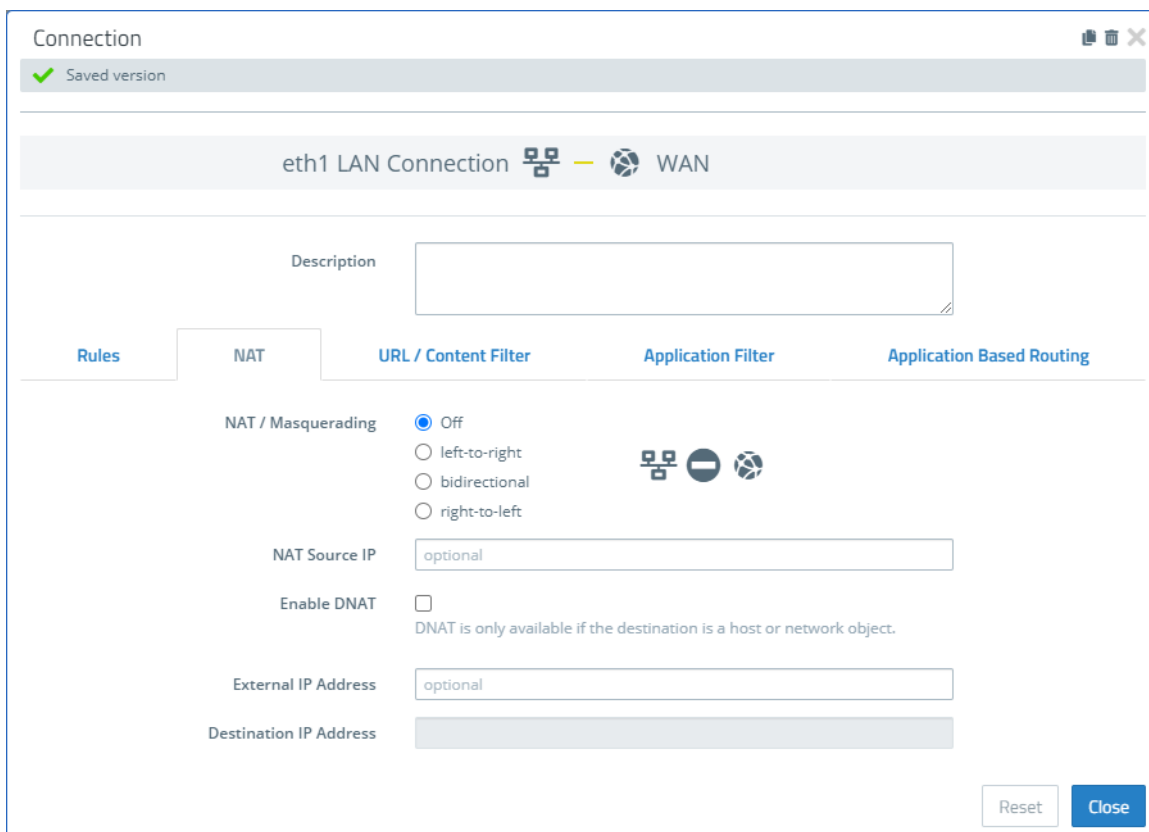



Figure 1: Connection dialog > NAT

Using the **NAT** tab it is possible to configure SNAT and DNAT for entire networks. The settings correspond to those for individual services except for the destination port, which is omitted from the NAT settings for the connection.

Input box	Description
NAT / Masquerading	Specify the desired direction for NAT/masquerading (bidirectional , left-to-right , or right-to-left), or disable the function for that rule (Off) by selecting the appropriate radio button. The default setting depends on the source and destination objects selected for the connection.
NAT Source IP	Optional: If you have multiple outgoing IP addresses, specify the IP address to use for the source NAT. If no IP address is specified, the system automatically selects the main IP address of the outgoing interface.  If a connected object is a network, you can also enter a network here, provided that it has the same size as the object's network.
Enable DNAT	If a single host or network object is the destination, you can mark this check box to activate DNAT.

Input box	Description
External IP address	Optional: Enter the destination IP address of the data being processed. DNAT is applied to this data traffic only. This IP address has to be one of the IP addresses of the firewall. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> i If a connected object is a network, you can also enter a network here, provided that it has the same size as the object's network. </div>
Destination IP address	Optional: Enter the destination IP address of the data being processed.

The tab **Rules** now has an additional column **Connection NAT** to make it easier to switch NAT settings from connection-based to service-based and vice versa. By default, newly added services use the option to use the NAT settings for the connection. If you wish to use the service-specific settings described below, you must remove the checkmark here.

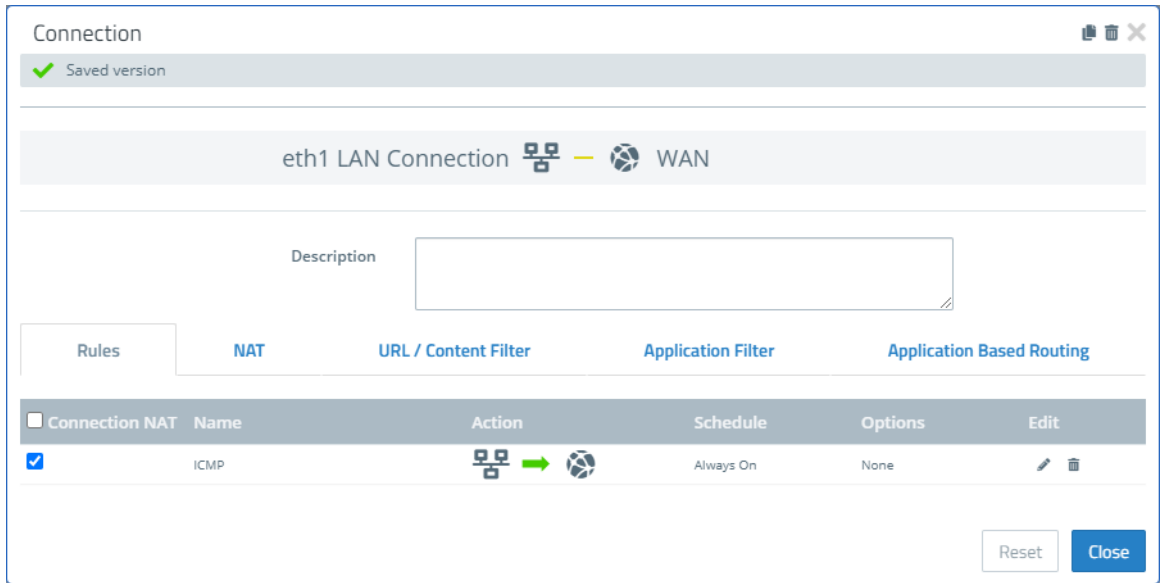


Figure 2: Connection dialog > Rules

In order to preserve the previous service-specific settings, you have to edit the rule and, in the dialog, use the tab **Advanced** to switch from the option **Use Connection Settings** to **Use Service Specific Settings**. In this way the familiar settings are displayed for editing again:

ICMP eth1 LAN Connection WAN

Description

Ports/Protocols Schedule **Advanced**

Proxy Enable proxy for this service

NAT Use Connection Settings
 Use Service Specific Settings

NAT / Masquerading

Off
 left-to-right
 bidirectional
 right-to-left

NAT Source IP
optional

Enable DMZ / Port Forwarding for this service

Port forwarding is only available if the destination is a host object.

External IP Address
optional

External Port

Reset Cancel **OK**

Figure 3: Service dialog > Advanced

3 Certificate Management

As of LCOS FX version 10.7, modifications to the **Certificate Management** resulted in, among other things, changes to the menu structure under Certificate Management. The items **Certificates** and **Templates** have retained their enhanced functionality, while the **Trustworthy CAs** have been supplemented by **Untrustworthy CAs**. The item **OCSP/CRL** has been removed completely. The certificate requests are now created under the item **Certificates**.

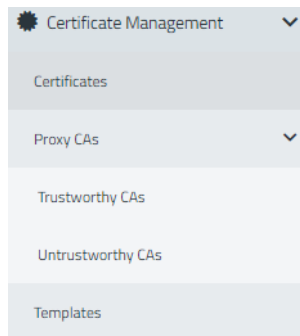


Figure 4: Certificate Management menu

The following is a full description of the modifications, making reference to modified or discontinued features where applicable.

3.1 Certificates

The **Certificates** configuration dialog allows you to manage the certificates used by the LANCOM R&S® Unified Firewall web client, the built-in SSL proxy and the OpenVPN server.

To secure encrypted connections, your LANCOM R&S® Unified Firewall uses digital certificates as per the X.509 standard.

The LANCOM R&S® Unified Firewall itself acts as a certification authority. Therefore, a so-called CA certificate is required. To centralize the management of the certificates, it is advisable to create a CA certificate on a central firewall and use it to sign every certificate used for the application directly. This is called a single-staged certification chain.

All certificates for applications have to be signed by the central firewall. If a certificate is needed for another firewall, you have to create a request on it. This request has to be signed by the central firewall. The signed request which you created has to be imported by the other firewalls to use it.

If the other firewalls require the ability to create certificates for mostly local purposes which are however recognized as valid to your whole organization, you can use multi-staged certification chains. Therefore, you need a so-called root CA certificate on your central firewall with which you sign the secondary CA certificates. You need to create requests for these secondary CA certificates on your other firewalls. After importing the signed CA certificates, the other firewalls themselves are able to sign certificates for applications. To display these hierarchies clearly, your LANCOM R&S® Unified Firewall shows them in a tree view.

3.1.1 Overview of certificates

Navigate to **Certificate Management > Certificates** to display a tree diagram listing the certificates available on the system as organized by certificate authority.

Use the buttons above the list to expand or collapse the branches, import a certificate from a file (→), sign a certificate signing request, or create a new certificate.

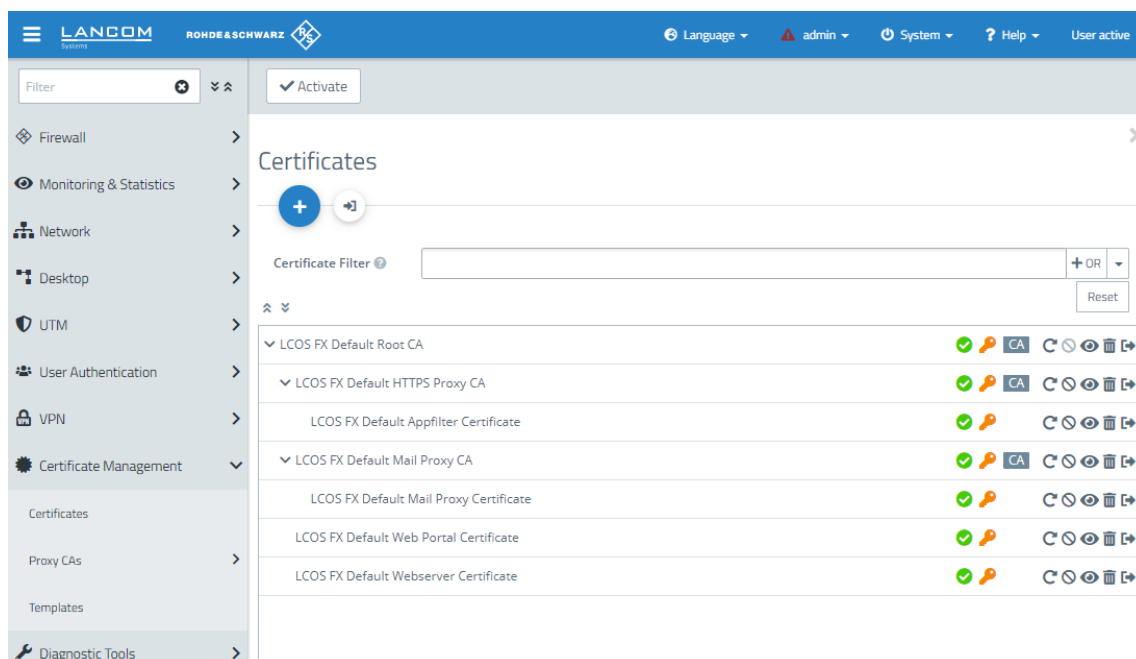


Figure 5: Certificate Management > Certificates



After the initial boot-up and following a new installation, the following certificates are created by default, although occasionally they first have to be selected in the setup wizard:







Table 1: Previously created certificates

Certificate name	Description
LCOS FX default root CA	Top-level certification authority used to create subordinate certification authorities and certificates.
LCOS FX default HTTPS proxy CA	Certification authority for creating subordinated certificates for use by the HTTPS proxy.
LCOS FX default app-filter certificate	Preconfigured certificate for application management.
LCOS FX default mail proxy CA	Certification authority for creating subordinated certificates for use by the mail proxy.
LCOS FX default mail proxy certificate	Preconfigured certificate for the mail proxy.
LCOS FX default web portal certificate	Preconfigured certificate for the web portal.
LCOS FX default web server certificate	Preconfigured certificate for the web server.

This list displays the name of the respective certificate and its dependencies as shown by the tree structure. The button behind each certificate indicate its validity:

- > – certificate is valid
- > – certificate expires in 8 to 30 days
- > – certificate expires in one to 7 days
- > -- certificate has expired

- >  – certificate has been revoked
- >  – certificate has been replaced

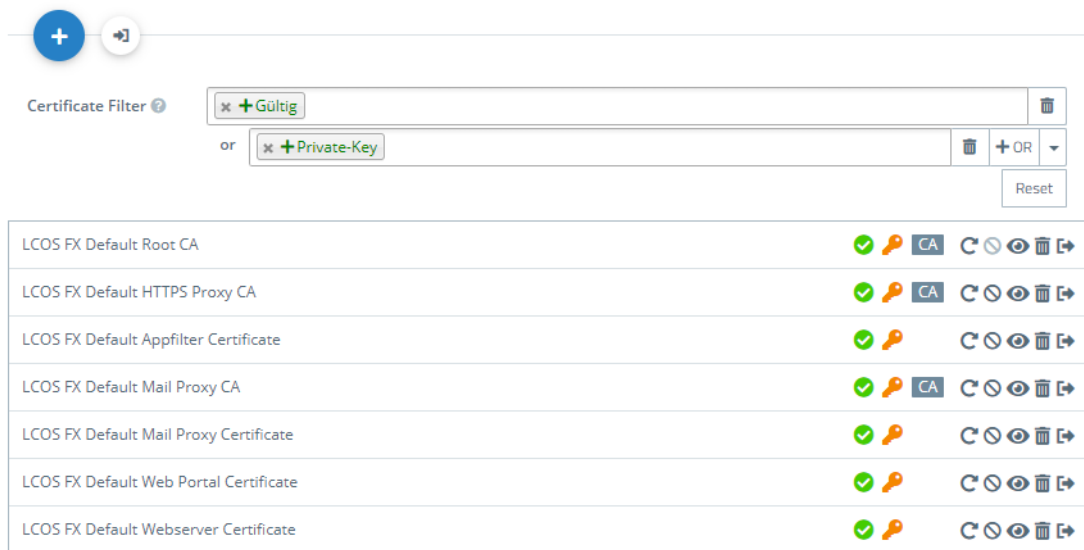
Also displayed is the availability of a private key for the certificate () and a “CA” shows whether the certificate is a certification authority. You can also use the buttons to display details of each certificate () , export a certificate () , renew the validity of a certificate () , revoke the certificate () , and delete the certificate or just its private key () .

Filtering the certificate overview

From LCOS FX version 10.7 the former simple text filter has been replaced by a filter similar to the one used for the alert log.

You can use **Certificate Filter** in the input field to narrow down the results by using different search criteria and options.

Certificates



The screenshot shows the 'Certificates' management interface. At the top, there are two circular buttons: a blue one with a plus sign and a grey one with a refresh icon. Below them is a 'Certificate Filter' section with a search input field containing 'Gültig' and a dropdown menu showing 'Private-Key'. To the right of the input field are icons for deleting the filter, adding an 'OR' condition, and a 'Reset' button. Below the filter is a table listing certificates with their respective icons for status, private key availability, and CA status.


















































LCOS FX Default Root CA			CA					
LCOS FX Default HTTPS Proxy CA			CA					
LCOS FX Default Appfilter Certificate								
LCOS FX Default Mail Proxy CA			CA					
LCOS FX Default Mail Proxy Certificate								
LCOS FX Default Web Portal Certificate								
LCOS FX Default Webserver Certificate								

Figure 6: Certificates with applied filter




Proceed as follows to create a filter:

1. Click in the input field.
The web client displays suggested filters.
2. Select one of the suggested filters from the drop-down list, or enter any search text to receive further suggestions. Predefined filters are:
 - > Status
 - > Valid certificates
 - > Expired certificates
 - > Revoked Certificates
 - > Certificates valid for less than a week
 - > Certificates valid for less than a month
 - > Certificates not yet valid
 - > Property
 - > With private key
 - > Is a certificate authority
 - > Is a request

- > Was generated using one of the following key algorithms: RSA, NIST curves, ED448, ED25519
- > NIST curve types: secp224r1, secp256r1, secp384r1, secp521r1, secp256k1
- > Key size 1024, 1536, 2048, 3072, 4096, 6144 and 8192
- > Key usage: Content commitment, CRL signature, data encryption, decryption only, digital signature, encryption only, key agreement, key certificate signature, key encryption
- > Extended key usage: Any advanced key usage, client authentication, code signature, e-mail protection, OCSP signature, server authentication, time stamp
- > Hash algorithms: sha1, sha224, sha256, sha384, sha512
- > Reasons for revocation: Unspecified, key compromised, CA compromised, affiliation changed, replaced, business discontinuation, rights revoked, attribute authority compromised

Entering text shows new filter properties:

- > Text
 - > Common Name contains entered text
 - > Subject contains entered text
 - > Subject of the issuer contains entered text
- > Hexadecimal notation (hyphens and colons are ignored, i.e. you can enter "dddd", "dd-dd" or "dd: dd", and all are considered valid)
 - > Fingerprint contains entered text
 - > Signature contains entered text


 For each suggestion, you can specify whether to use this as an inclusion filter ( / AND) or exclusion filter ( / AND-NOT).

After selection, the suggested filter is inserted into the input field as a search criterion.

The list of certificates is adapted to the search query.

Repeat the above steps until you have added the desired filter criteria to your query.


 Only entries that match all filter criteria are displayed.


To delete a filter criterion in a search query, click on .






You can add multiple lines to your search by clicking on **+ OR** next to the input field. You can choose to insert a new blank line or to copy the last created line. Each line is a separate search query, which is ORed with the other lines.






Delete the line by clicking  next to the line.

Creating a certificate or certificate request

With the plus button  above the list with the elements you can create new certificates and signing requests. You can configure the following elements:

Input box	Description
Certificate Type	Choose between the options Certificate to create a certificate or a certification authority (CA) and a Certificate Signing Request . With the latter, you create a certification request for a certificate or for a subordinate CA, which then has to be signed by a higher-level CA to become valid.  When selecting the option Certificate Signing Request , neither the Validity nor the Signing CA can be selected as these are specified when the certificate is signed.

Input box	Description
	<p>The created request appears under the certificates in a separate branch of the certificate tree, Outstanding Certificate Signing Requests.</p>
Common Name (CN)	Specify a name for this certificate.
Private Key Password	Required: Enter a password to secure the private key.
Show Password	Optional: Set a check mark in the check box to view the password.
Validity	<p>Set the starting time for the certificate’s validity period. The input boxes are already filled out with the current date as the creation date and the expiry date set to the same day one year later in the case of a certificate or 5 years later in the case of a certificate authority. To specify a different period, select one of the options provided or select the start and end date in the calendar that is displayed.</p> <p>The start and end dates are displayed in the following format: MM/DD/YYYY – MM/DD/YYYY (e.g. 04/18/2021 – 04/18/2031).</p>
Template	<p>Optional: Choose one of the Templates on page 16 to fill-out the boxes in the section “Options” and “Subject and SAN” with values from the template.</p> <hr/> <p> If you select a template, any settings you made previously are overwritten!</p>
Signing CA	Select the signing CA.
CA Password	<p>With a CA is selected this field is mandatory, unless it is one of the LCOS FX CAs listed in Table 1: Previously created certificates on page 9. Enter a password for the private key of the signing certification authority. The password is required because the public key of the new certificate is signed with the private key of the signing CA.</p>
Show CA Password	Optional: Set a check mark in the check box to view the password.
Certificate Authority	<p>This option determines whether or not the certificate being created can also be used as a certification authority to sign other certificates.</p> <hr/> <p> Caution: There are different default periods of validity for certificates (1 year) and Certificate Authorities (5 years). Changing this property causes the validity period to be adjusted.</p>
Path Length	<p>Only available if Certificate Authority is selected. Here you determine how many sub-CA levels can be created with this CA. With a value of 0, no sub-CAs can be signed with this CA, i.e. only “normal” certificates can be signed with this CA. If the field is left blank, there is no limit.</p>
Key Usage	Click in the box for a choice of preset property values, e.g. data encryption.
Encryption algorithm	<p> The algorithm “DSA” was deprecated as of LCOS FX version 10.7. It was replaced with the “NIST curves”, “ed448” and “ed25519” elliptic curve methods.</p> <p>Select the algorithm you require from the list of results.</p> <hr/> <p> If you select the option “NIST curves”, you have to select the type of NIST curve from the Curve field.</p> <hr/> <p> However, the new algorithms <i>NIST Curves</i>, <i>ed448</i> and <i>ed25519</i> are only partially supported or not yet supported at all by some services, e.g. in the reverse proxy.</p>
Curve	If you selected the option “NIST curves” under Encryption algorithm , you select the type of NIST curve here.
Key Size	If you selected the option “RSA” under Encryption algorithm , you select the key size here.

Input box	Description
	<p> Note that key sizes below 2048 are no longer accepted by some services on the firewall, such as mail and HTTPS proxy.</p>
Hash Algorithm	Select one of the available hash algorithms.
Extended Key Usage	Here you can click in the box to add further predefined property values from a list, such as the timestamp, for example.
Subject	<p>Optional: From the drop-down list you can choose any number of subjects, such as Country (C), State (ST), Organization (O), or Organizational Unit (OU), and enter the content in the input box to the right. Click on  on the right-hand side to add an entry to the list. You can edit or delete any entry in the lists by clicking on the appropriate icon.</p> <p> When you edit a Subject, a checkmark will appear to the right of the entry. You first have to confirm your change with this checkmark before you can save the certificate settings.</p>
Subject Alternative Name (SAN)	<p>Optional: You can enter any number of custom names for different uses and select the appropriate types from the drop-down list. The following types are available: E-Mail, DNS, DirName, URI, IP and RegID. Click on  on the right-hand side to add a Subject Alternative Name (SAN) to the list. You can edit or delete any entry in the lists by clicking on the appropriate icon.</p> <p> When you edit a Subject Alternative Name (SAN), a checkmark will appear to the right of the entry. You first have to confirm your change with this checkmark before you can save the certificate settings.</p>

With the buttons in the lower right corner of the editing field, you can create a new certificate and add it to the list of available certificates, or cancel the creation of a new certificate (**Cancel**).

Importing a certificate or signing a certificate signing request

The  button above the list allows you to import a certificate from a file or to sign a certificate signing request.

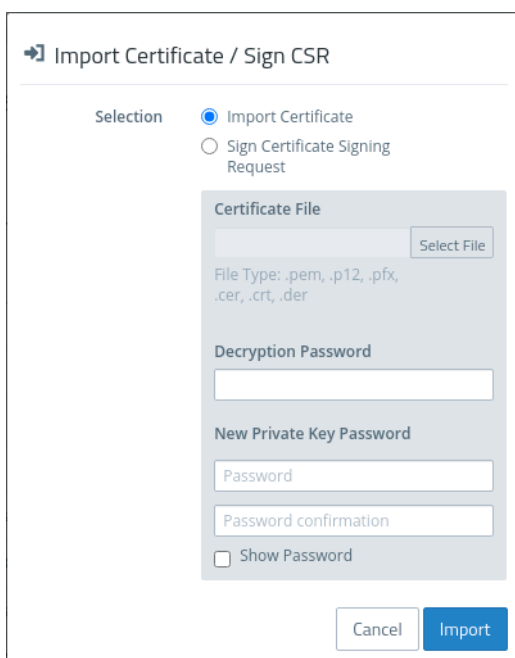


Figure 7: Importing a certificate / signing a certificate signing request

The radio buttons at the top allow you to choose between importing a certificate or signing a certificate signing request.

The import function supports certificate files in various formats (*.pem, *.p12, *.pfx, *.cer, *.crt, *.der). If the file contains a private key, a password must be entered to decrypt the private key, and a password must be entered to encrypt the private key again. You can optionally display the password.

In the case of a certificate signing request, select the associated file. The following file types are supported: *.pem, *.crt, *.cer, *.der. You select a signing CA and enter the associated password. The validity period must also be selected. Once signed successfully, the certificate is offered for download as a PEM.

With the buttons in the lower right corner of the editing field, you can import the selected certificate file and add it to the list of available certificates, sign the certificate signing request, or cancel the dialog (**Cancel**).


Renew certificate

The **C** button for a certificate in the list prompts a new certificate to be created with a new validity period.

In the case of a simple certificate, select the new period under **Validity** and enter the **CA Password** of the relevant CA certificate. For certificates that are not self-signed, a completely different CA can be selected when renewing. This is not limited to the current CA. For certificates that are not self-signed, two passwords must be entered; the CA password and the private-key password of the certificate being renewed.

With a Certificate Authority (CA) you can also change the Common Name and assign a new validity period to the certificates signed by this CA.

 Derived sub-CAs and certificates must be renewed manually.

 The certificates due for renewal are no longer revoked automatically. You can optionally carry out the revocation after the renewal.

Use the buttons at the bottom right in the editing box to renew the validity period of the selected certificate or CA and, if necessary, the certificates signed by it, or to cancel the dialog (**Cancel**).

Revoke certificate


With the **R** button you can revoke a listed certificate. To do this, you must select a reason and enter the password of the private key of the certificate's parent CA.

Certificates cannot be revoked if

- > the certificate was revoked already,
- > the certificate does not have a CA (first-level CA) or
- > the CA of the certificate does not have a private key.


Use the buttons in the lower right-hand corner of the editing window to revoke the selected certificate or to cancel the dialog (**Cancel**).

Viewing certificate details

The button  is used to view the details of a certificate in the list.


You can use the buttons in the lower right corner of the edit box to copy the public key and the certificate's fingerprint to the clipboard, or to close the dialog (**Close**).

Deleting a certificate or private key

The  button next to a certificate in the list allows you to delete the certificate or the private key that belongs to it. Unlike a revoked certificate, a deleted certificate is also removed from the certificate tree. No password is required to do this.

Use the buttons in the lower right-hand corner of the editing window to delete the certificate or the private key only, or to cancel the dialog (**Cancel**).

Exporting a certificate

The  button next to a certificate in the list allows you to export the certificate in the format PEM, PKCS, or DER.

PEM

An export in the PEM format usually exports the public portion of the certificate only. Optionally, the related CAs can also be included in the PEM file. If available, the private key can be exported as well. This requires the current password to decrypt the private key and a new password to encrypt the exported private key. If the certificate has no private key, this option is not available.

PKCS

The PKCS format is only available for exporting certificates that have a private key. As with the PEM export, this requires the current password to decrypt the private key and a new password to encrypt the exported private key. Unlike PEM, the password is required to encrypt the entire container and not the private key.

DER

An export in the DER format involves the certificate being exported in the PEM format, in which case the PEM is Base64 coded. Here too the private key can optionally be exported by using the passwords. Since the DER format supports one certificate only, the certificate and the private key are stored separately and collected into a ZIP file. The private key is saved in the pkcs8 format.

Use the buttons in the lower right-hand corner of the editing window to export the certificate or to cancel the dialog (**Cancel**).

3.1.2 Private key password

From LCOS FX version 10.7, whenever a certificate with a private key is required, you must enter this password to decrypt the key if:

- > the relevant settings are activated or
- > the certificate is changed.

This behavior affects the following dialogs and settings:

- > Command Center settings
- > Web client settings
- > Application Management settings
- > HTTP proxy settings
- > Mail proxy settings
- > Reverse proxy front-end settings
- > Settings for the external portal
- > VPN profiles
- > Settings for the internal portal
- > IPsec connections with cert. or CA authentication
- > VPN SSL settings



By contrast, there is no need to enter a private key password if it is one of the LCOS FX CAs listed in [Table 1: Previously created certificates](#) on page 9.

3.2 Templates

To simplify the creation of new certificates, you can use templates to automatically fill out the input boxes for a range of optional fields, e.g. the **Distinguished Name** and the **Subject Alternative Names**.

3.2.1 Templates overview




Navigate to **Certificate Management > Templates** to display the list of templates available on the system in the object bar. Two templates for certificates and certificate authorities are available after installing the LANCOM R&S® Unified Firewall.




In the expanded view, the table columns show the name and settings of the template. Use the buttons in the last column to view and modify a template’s settings, create a new template based on a copy of an existing one, or delete a template from the system.

 The two default templates cannot be deleted.

3.2.2 Settings for templates

In the **Templates** editing window you can specify additional certificate options, which can be used automatically when a certificate is created. The following elements can be specified:

Input box	Description
Name	Enter a name for this template. You can use this name to select the template when creating the certificate.
Certificate Authority	This option determines whether or not the certificate being created can also be used as a certification authority to sign other certificates.  Caution: There are different default periods of validity for certificates (1 year) and Certificate Authorities (5 years). Changing this property causes the validity period to be adjusted.
Path Length	Only available if Certificate Authority is selected. Here you determine how many sub-CA levels can be created with this CA. With a value of 0, no sub-CAs can be signed with this CA, i.e. only “normal” certificates can be signed with this CA. If the field is left blank, there is no limit.
Key Usage	Click in the box for a choice of preset property values, e.g. data encryption.
Encryption algorithm	Select the algorithm you require from the list.  If you select the option “NIST curves”, you have to select the type of NIST curve from the Curve field.
Curve	If you selected the option “NIST curves” under Encryption algorithm , you select the type of NIST curve here.
Key Size	If you selected the option “RSA” under Encryption algorithm , you select the key size here.
Hash Algorithm	Select one of the available hash algorithms.
Extended Key Usage	Here you can click in the box to add further predefined property values from a list, such as the timestamp, for example.
Subject	Optional: From the drop-down list you can choose any number of subjects, such as Country (C) , State (ST) , Organization (O) , or Organizational Unit (OU) , and enter the content in the input box to the right. Click on  on the right-hand side to add an entry to the list. You can edit or delete any entry in the lists by clicking on the appropriate icon.

Input box	Description
	 When you edit a Subject , a checkmark will appear to the right of the entry. You first have to confirm your change with this checkmark before you can save the certificate settings.
Subject Alternative Name (SAN)	Optional: You can enter any number of custom names for different uses and select the appropriate types from the drop-down list. The following types are available: E-Mail, DNS, DirName, URI, IP and RegID. Click on  on the right-hand side to add a Subject Alternative Name (SAN) to the list. You can edit or delete any entry in the lists by clicking on the appropriate icon.  When you edit a Subject Alternative Name (SAN) , a checkmark will appear to the right of the entry. You first have to confirm your change with this checkmark before you can save the certificate settings.

The buttons available at the bottom right of the edit box depend on whether you are adding a new template or editing an existing one. For a newly configured template, click **Create** to add it to the list of available templates, or **Cancel** to discard your changes. To edit an existing template, click **Save** to save the newly configured template, or **Reset** to discard your changes.


3.3 Proxy CAs

The settings under **Proxy CA** are used to manage your CA certificates: For this purpose, they are arranged in trusted and untrusted lists.

3.3.1 Trusted proxy CAs

Navigate to **Certificate Management > Proxy CAs > Trustworthy CAs** for the object bar to display a list of the custom and system certificate authorities currently created in the system and that are trusted by the SSL proxy for external connections.

In the expanded view, the **Common Name** of the CA certificate is displayed in the first column of the table. Use the buttons in the last column to view the settings for a CA certificate or to mark a CA certificate as untrusted. This will place it in the list under **Certificate Management > Proxy CAs > Untrustworthy CAs**. You can also delete user-defined CA certificates.

To send a user-defined CA to your LANCOM R&S[®] Unified Firewall, click the  (Import) button in the header of the object bar, select the desired PEM/CRT file, open it, and click **Import**. The imported user-defined certificate is added to the list of available trusted proxy CAs. Use the option **Show User Defined CAs Only** to reduce the displayed list to the Certificate Authorities you have added.

3.3.2 Untrusted proxy CAs

Navigate to **Certificate Management > Proxy CAs > Untrustworthy CAs** for the object bar to display a list of user-defined and system certification authorities currently created in the system and that are **not** trusted by the SSL proxy for external connections.

In the expanded view, the **Common Name** of the CA certificate is displayed in the first column of the table. Use the buttons in the last column to view the settings for a CA certificate or to mark a CA certificate as trusted. This will place it in the list under **Certificate Management > Proxy CAs > Trustworthy CAs**. You can also delete user-defined CA certificates.

Use the option **Show User Defined CAs Only** to reduce the displayed list to the Certificate Authorities you have added.

4 WWAN

As of LCOS FX version 10.7, WWAN connections and interfaces are supported. The prerequisite is a corresponding mobile radio module in your LANCOM R&S® Unified Firewall.

4.1 WWAN Connections

The settings under **WWAN Connections** allow you to configure connections that use a **WWAN Interface** and add new ones.

The following sections provide more detailed information about WWAN connections.

4.1.1 WWAN Connections Overview

Navigate to **Network > Connections > WWAN Connections**, to view the list of WWAN connections currently created in the system in the item list bar.

The view first displays the **Name** of the connection and whether it is **Active** or not. The buttons in the last column allow you to view and adjust the settings for an existing WWAN connection, create a new connection based on a copy of an existing WWAN connection, or delete a WWAN connection from the system.

4.1.2 WWAN Connections Settings

Under **Network > Connections > WWAN Connections** you can add a new network connection or edit an existing one.

The settings under **WWAN Connection** contain the following elements:

Input field	Description
I/O	A slider switch indicates whether the WWAN connection is active (I) or inactive (O). Click the slider switch to change the status of the connection. A new connection is active by default.
Name	Enter a name for the network connection.
Interface	Assign an interface to the connection. You can only select a WWAN interface that is not being used by another connection.
Status	Displays the status of the connection (up, disconnected or disabled).

On the **WWAN** tab:

Input field	Description
APN	Stands for Access Point Name. This is what makes it possible to access the Internet in the mobile network. The APN is a type of address that the LANCOM R&S® Unified Firewall uses to contact the mobile network. Some common APNs of the major ISPs can be selected directly by clicking in the empty input field. However, you can also specify your own.
Username	Enter the username required to connect to your mobile service provider.
Password	Enter the password required to connect to your mobile service provider.
SIM PIN	Enter the PIN required to access your SIM card. To change the PIN if necessary, use the Change PIN button at the bottom left.

Input field	Description
	<p>If the SIM card is inserted, the PIN entered will be checked as soon as the dialog is saved. If an incorrect PIN is entered, an error message appears below the input field indicating the number of remaining attempts.</p> <p>Since the SIM card can be changed at any time, regardless of the configuration, or can be inserted later, this error message may also be displayed directly as soon as a connection is opened for editing. If the PIN has been rejected once, then the device will not try to use this PIN again during reboots or similar, in order to prevent the SIM card from being blocked.</p> <p>If the SIM card is already locked, the Unlock SIM button appears at the bottom left of the editor. Clicking on this button opens a window in which the PUK (Personal Unblocking Key) and a new PIN must be entered instead of the old PIN.</p>
Allow Roaming	Allow roaming if necessary.

On the **WAN** tab:

Input field	Description
Time Restrictions	<p>Select this check box if you want to set a time limit for which the connection is enabled.</p> <p>Click Edit to open the Time Restrictions editor panel which provides the following options:</p> <ul style="list-style-type: none"> > Set specific times and weekdays using the sliders. > Always On - The connection is always enabled. > Always Off - The connection is always disabled.
Multi WAN Weight	Specify how much of the Internet traffic is routed through this connection by entering a value from 1 to 256. The higher the set value, the higher the percentage of Internet traffic routed through the connection. Setting the same value for all connections results in equal traffic distribution across all connections.
Desktop Object	From the drop-down list, select an Internet object that is used in firewall rules for this connection.

On the **Failover** tab:

Input field	Description
Heartbeats	<p>Specify how you want to test the state of the connection by adding ping tests.</p> <p>The default settings contain a ping test with the Google server (8.8.8.8). Click Add to add another test to the list. For more information on configuring the reachability test, see Heartbeat Settings on page 19.</p> <p>You can edit or delete individual entries in the list by clicking the corresponding button next to an entry.</p>
Use as backup connection	Select this check box to configure this connection as a backup Internet connection.
Backup connections	<p>Select any backup connection you wish to assign to the connection and specify its Priority. If the current connection fails, your LANCOM R&S[®] Unified Firewall switches to the available backup connection with the highest priority. Click Add to add the backup connection to the list.</p> <p>You can edit or delete individual entries in the list by clicking the corresponding button next to an entry.</p>

Heartbeat Settings

The **Heartbeats** panel allows you to configure automatic heartbeat tests. The editor panel contains the following elements:

Input field	Description
Type	From the drop-down list, select the type of reachability test you want to run: > <code>ping</code> - This mode sends ping signals to the target. > <code>tcp_probe</code> - This mode tests the capacity of a TCP connection.
Timeout	Specify the timeout for the test in seconds.
Number of tries	Set the overall number of tries to be performed.
Number of successful tries	Set the number of successful tries required for a successful heartbeat.
Arguments	Specify the arguments to be used in the test, e. g. IP addresses that you want to ping.

Click **Test** to run the connection test manually. Click **OK** to save your settings and to return to the **Network Connection** panel.

The buttons at the bottom right of the editor panel depend on whether you add a new WWAN connection or edit an existing one. For a newly configured connection, click **Create** to add it to the list of available WWAN connections or **Cancel** to discard your changes. To edit an existing PPP connection, click **Save** to store the reconfigured connection or **Reset** to discard your changes. You can click **Close** to shut the editor panel as long as no changes have been made on it.

Click **Activate** in the toolbar at the top of the desktop to apply your configuration changes.

4.2 WWAN Interfaces

You can use the settings under **WWAN Interfaces** to activate or deactivate any existing WWAN interface, such as a cellular connection.

The following sections provide more detailed information on WWAN interfaces.

4.2.1 WWAN Interfaces Overview

Navigate to **Network > Interfaces > WWAN Interfaces**, to display the list of WWAN interfaces currently created in the system in the item list bar.

The first column of the table displays the **Name** of the WWAN interface. The next column displays the current signal strength.

4.2.2 WWAN Interfaces Settings

Under **Network > Interfaces > WWAN Interfaces**, you can enable or disable a WWAN interface and view information about the interface.


In the **WWAN Interface** edit window, you can view the following information and configure the following items:

Input field	Description
I/O	A slider switch indicates whether the WWAN connection is active (I) or inactive (O). Click the slider switch to change the status of the connection.
Name	Displays the name of the WWAN interface.
IMEI	The International Mobile Equipment Identity (IMEI) is a unique 15-digit serial number that can be used to uniquely identify cell phones or comparable devices worldwide.
Used by	Connection that uses this interface.

Input field	Description
Status	Status of the connection.
Signal	Signal strength of the connection.
Radio Bands	Radio bands used.
RSSI	Received Signal Strength Indicator
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
SNR	Signal to Noise Ratio
MTU	The Maximum Transmission Unit (MTU) describes the maximum size of the user data that can be transmitted in a single data packet.

Click on **Network Scan** to retrieve a list of the different radio cells whose signals can be received. Generating this list may take several minutes. The more data is being transmitted over the module at the time of the scan, the slower the scan will be. A scan cannot be aborted and no interaction with the firewall web client is possible during the scan. Before the start of the scan, a warning appears with the option to cancel.

To edit an existing WWAN interface, click **Save** to store the reconfigured connection or **Reset** to discard your changes. You can click **Close** to shut the editor panel as long as no changes have been made on it.

Click  **Activate** in the toolbar at the top of the desktop to apply your configuration changes.