

LCOS FX 11.2

Addendum

11/2025



LANCOM
SYSTEMS

Contents

- 1 Addendum to LCOS FX version 11.2.....4**
- 2 Changes in BGP settings.....5**
- 3 Renaming of “Proxy CAs”6**
- 4 Changes in the SAML Settings.....7**
- 5 Let's Encrypt Key Type.....9**

Copyright

© 2025 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, LANCOM Service LANcare, LANCOM Active Radio Control, and AirLancer 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.

Bitdefender SDK © Bitdefender 1997-2025

LANCOM Systems GmbH

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom-systems.com

1 Addendum to LCOS FX version 11.2

This document describes the changes and enhancements in LCOS FX version 11.2 since the previous version.

2 Changes in BGP settings

As of LCOS FX 11.2, the option **R. Table** (Destination routing table) was added to the individual neighbors in the BGP settings.

BGP Routing

✓ Saved version

☐ ☐

Own Name wizard

Domain v11-1

AS Number 1

Neighbors	Name	Address	AS Number	Password	R. Table

+

Figure 1: Network > Routing > BGP

Input field	Description
R. Table	Specify the optional destination routing table for the BGP peer. If set to 0 or left empty, the globally configured destination routing table will be used. Other valid values are 254 or the range from 512 to 65535.

3 Renaming of "Proxy CAs"

As of LCOS FX 11.2, the menu item  **Certificate Management** > **Proxy CAs** was renamed to **Truststore**.

Since the certification authorities (CAs) managed here are not only relevant for the proxy but also for other parts of the system—such as access to the IdP API used for SAML functions—the old name was no longer appropriate.

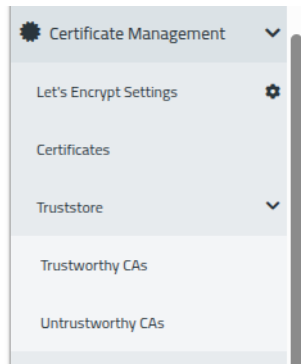


Figure 2:  **Certificate Management** > **Truststore**

4 Changes in the SAML Settings

As of LCOS FX 11.2, the following changes to the SAML settings have been introduced for both the internal and external portal. New options are now available for using the certificate truststore, selecting an optional IdP certificate (formerly "IdP Certificate (PEM)"), and specifying a base group ID.

In earlier versions, a certificate in PEM format had to be copied or imported into a text field. This procedure has been changed. The desired certificate must now first be imported into the certificate management. The imported certificate can then be selected via **IdP Certificate**. Alternatively, the new option **Use Certificate Truststore** can be enabled. In this case, the server certificate is validated against the system certificate truststore, and no separate certificate needs to be specified.

After updating to LCOS FX 11.2, a certificate previously stored in PEM format is automatically imported into the certificate management and selected, provided the text field contained exactly one certificate. If the PEM data contained multiple certificates, automatic selection is not possible, as only a single certificate can be specified now. Following an update, a message will appear prompting you to complete the configuration (see below).

SAML External Portal

✓ Saved version

☐ ☒

IdP Synchronization

IdP Type: [dropdown]

Base URL: [text field]

Use Certificate Truststore: ☐

IdP Certificate: [dropdown]

Client ID: [text field]

Base Group ID: [text field]

Grant Type: n/a

Synchronization Interval: 15 minutes

Last Synchronization: n/a

Synchronize Now

This may take a few minutes.

IdP SAML Settings

There is no IdP configuration yet. Click the button to import an IdP configuration.

Import IdP Metadata Export SP Settings Reset Close

Figure 3: User Authentication > External or Internal Portal > SAML

4 Changes in the SAML Settings

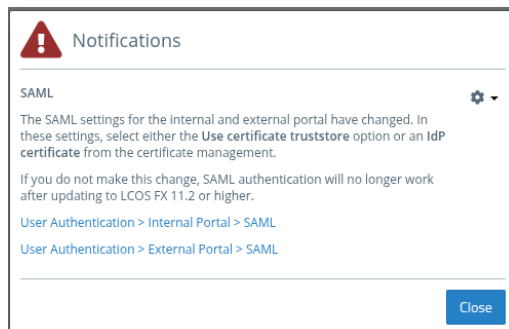
Input field	Description
Use Certificate Truststore	Instead of specifying a certificate under IdP Certificate , this option can be enabled. In this case, the verification of the server certificate is performed against the system certificate truststore. No certificate needs to be specified.
IdP Certificate	Optional. If the connection between the firewall and the IdP uses a certificate that the firewall does not trust, it can be selected here so that a secure connection can be established. This is useful, for example, for self-signed certificates. The certificate must be imported into the certificate management beforehand. Alternatively, instead of specifying a certificate, the option Use Certificate Truststore can be enabled. In this case, the verification of the server certificate is performed against the system certificate truststore. No certificate needs to be specified.
Base Group ID	Optional. Specify this ID to synchronize only a specific group (and its subgroups). This option can be used to reduce the scope of the IdP synchronization. It is particularly useful when a large number of groups exist and synchronization takes a long time.

Notifications

A new notification is displayed in the client after upgrades or when restoring a backup if

- > the SAML settings are enabled,
- > no IdP certificate has been selected,
- > and the option **Use Certificate Truststore** is not enabled.

These last two conditions may occur in particular after upgrading to LCOS FX 11.2 or when restoring older backups.



5 Let's Encrypt Key Type

As of LCOS FX 11.2, a new field has been added to the Let's Encrypt settings that allows you to specify the key type used for generating Let's Encrypt certificates. Previously, the default value was RSA with a key length of 2048 bits.

Figure 4: Certificate Management > Let's Encrypt

Input field	Description
Key Type	<p>Select the key type to be used for generating the Let's Encrypt certificates. The available options are ECDSA (recommended), RSA 4096, and RSA 2048 (legacy).</p> <p>⚠ When changing the key type, a confirmation prompt will appear. After confirmation, all previously used certificates that do not match the new key type will be immediately renewed with the new type.</p>

Notifications

After

- > upgrading to LCOS FX 11.2,
- > restoring an older backup, and
- > when using RSA 2048,

a one-time notification is displayed indicating that the use of this key type is not recommended.