LCOS FX 11.1

Addendum

12/2024

LANCOM SYSTEMS

Contents

Copyright

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 (*eay@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 1997-2023

LANCOM Systems GmbH

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Wuerselen

Germany

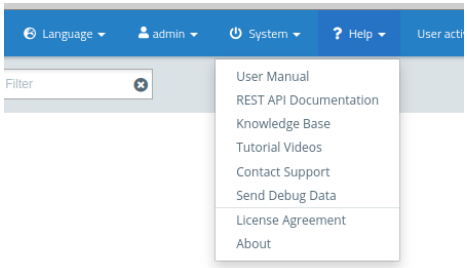
www.lancom-systems.com

1 Addendum to LCOS FX version 11.1

This document describes the changes and enhancements in LCOS FX version 11.1 since the previous version.

2 REST API Documentation

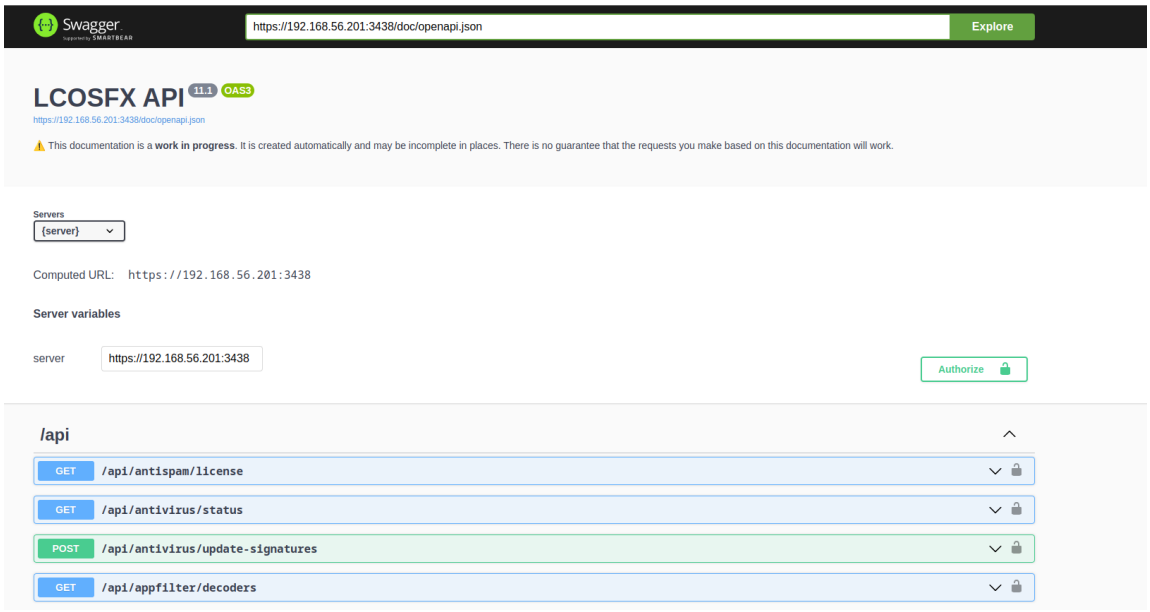
In the header under **Help** > **REST API Documentation**, you will find automatically generated documentation for the REST API.



The documentation is opened in a separate tab with the address currently used for web client access as the server.

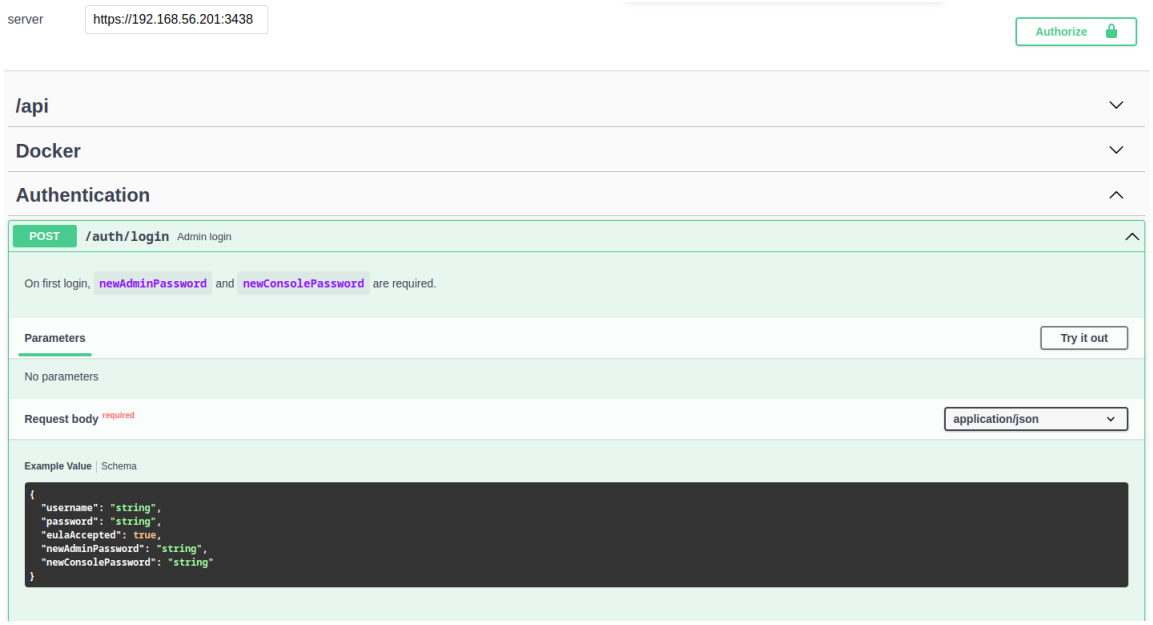
The API may change and the documentation may also be incomplete in parts.

You can also change the server variable and thus reference a different firewall. This is not recommended as different devices may be running different firmware versions and therefore provide different APIs

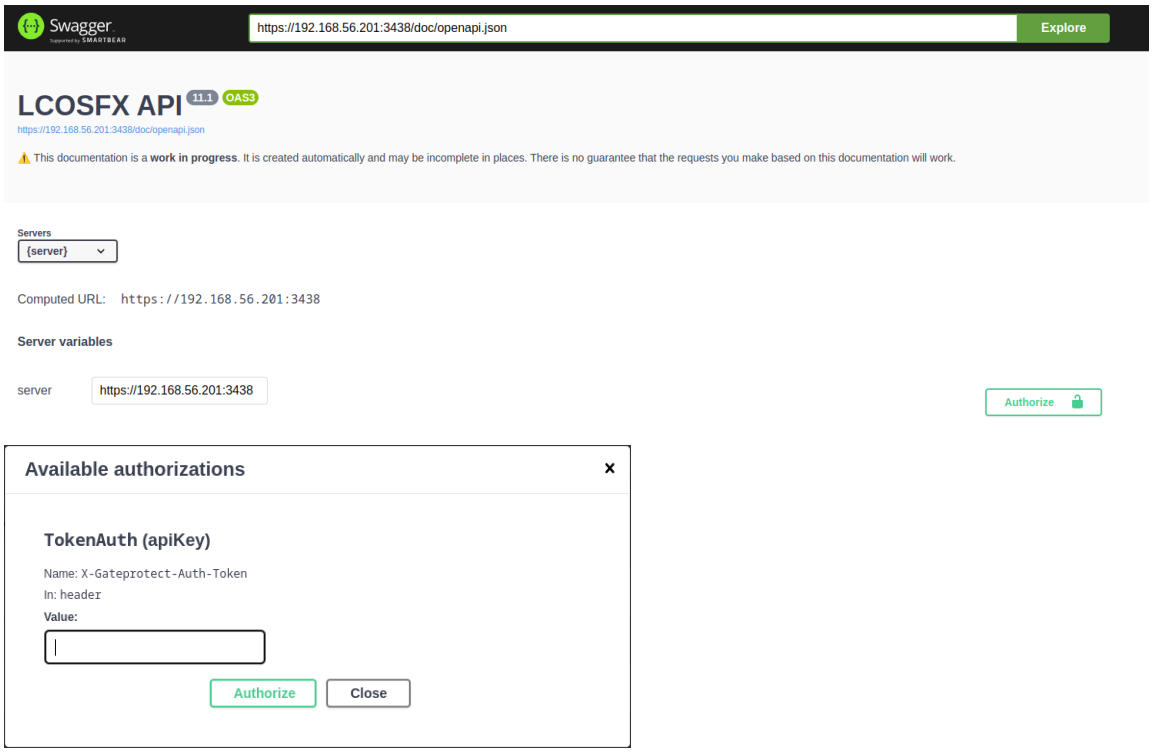


Executing an API request against a firewall requires an auth token, which the user receives after a successful login. This token can be obtained in the following way: Under the **Authentication** category of the API documentation, the login

endpoint is also included, in which you can perform a login with **Try it out** and thus obtain the auth token. The **token** field in the response after a successful login contains the token.



If the auth token is available, the value can now be entered via the **Authorize** button.



It should then be possible to execute all the requests listed in the documentation against the specified firewall.

3 TFTP

As of LCOS FX 11.1, a new option has been added to allow or deny access to the firewall via TFTP.

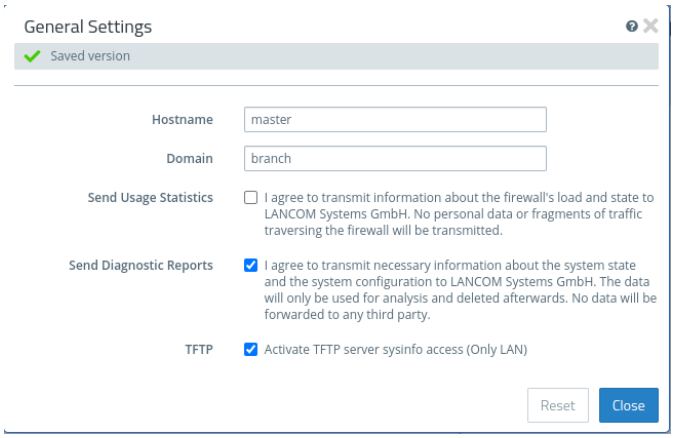


Figure 1: Firewall > General settings

Input box	Description
TFTP	Allow or deny access to the firewall via TFTP. TFTP is allowed by default. TFTP access is only enabled in the internal network for sysinfo access.

4 Ping Settings

As of LCOS FX 11.1, a distinction is made between IPv4 and IPv6 ping under **Firewall** > **Firewall Access** > **Ping Settings**.

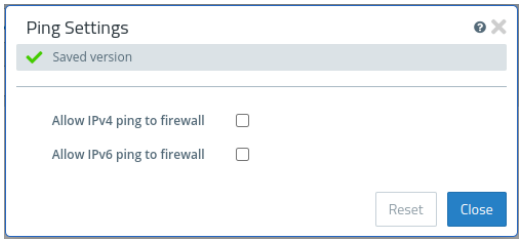


Figure 2: Firewall > Firewall Access > Ping Settings

Input field	Description
Allow IPv4 ping to firewall **Allow IPv6 ping to firewall**	Configure separately for IPv4 and IPv6 how your LANCOM R&S®Unified Firewall handles ICMP echo requests to the firewall from the internal network and the Internet. The option is set to “Deny” by default, but you can change this to “Allow” if required. › “Deny” – The LANCOM R&S®Unified Firewall does not respond to ICMP echo requests to the firewall from the internal network and the Internet. › “Allow” – The LANCOM R&S®Unified Firewall reponds to ICMP commands to the firewall from the internal network and the Internet. While blocking ICMP echo requests can improve the security of your LANCOM R&S®Unified Firewall, it also makes any troubleshooting in the network difficult. Therefore, if an error occurs in the network, we recommended setting this option to `Allow` before you start troubleshooting.

5 IPv6

As of LCOS FX 11.1, there is (limited) support for IPv6. IPsec connections can now be created on the basis of IPv6. Two new connection types have been added under **Network** > **Connections** > **Network Connections**: **Static IPv6** and **DHCPv6**.

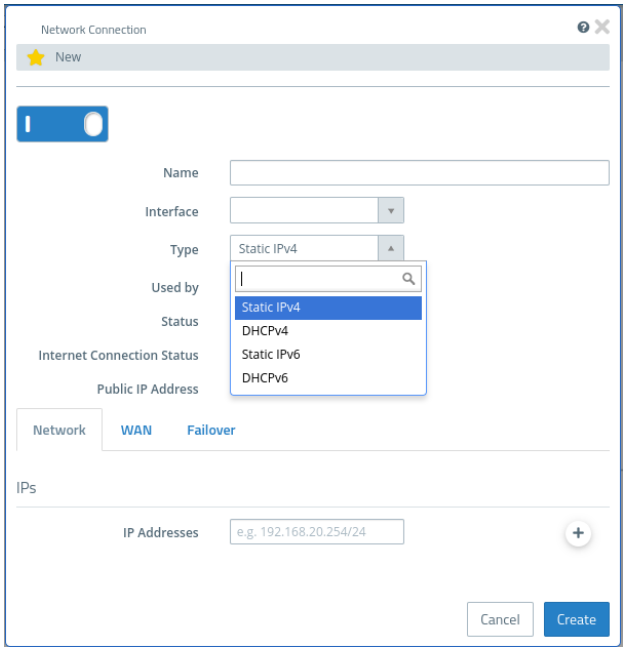


Figure 3: Network > Connections > Network Connections

Input field	Description
Type	From the drop-down list, select the connection type. This option is set to `Static IPv4` by default, but you can adjust the settings to one of the other values as necessary: › **Static IPv4** – This mode is used to specify a fixed IPv4 address for the connection. › **DHCPv4** – This mode is used to assign IPv4 addresses dynamically. › **Static IPv6** – This mode is used to specify a fixed IPv6 address for the connection. ⓘ These connections can only be used in IPsec connections. › **DHCPv6** – This mode is used to assign IPv6 addresses dynamically. ⓘ These connections can only be used in IPsec connections ❗ Once you click **Create** to establish the network connection, you will no longer be able to change the connection type. ⓘ The elements in the **Network** tab depend on the selected connection type.

ⓘ By selecting one of the two options **Static IPv6** or **DHCPv6**, only IPv6 values can be used in various fields:

- **IP Addresses**
- **Default Gateway**
- **Heartbeats**

IPsec connection

In an IPsec connection, the IPv6 connection can be selected or omitted as before for IPv4.

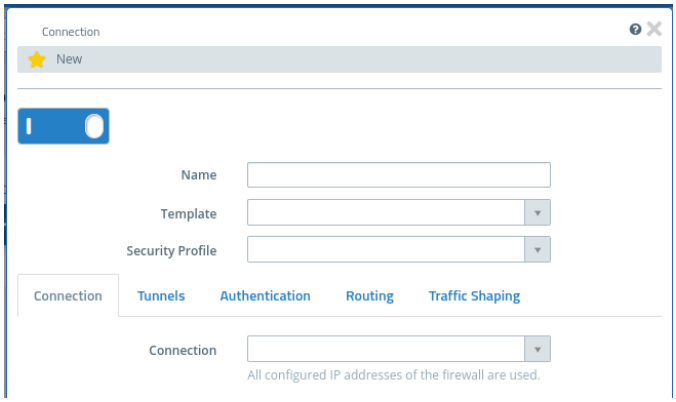


Figure 4: VPN > IPsec > Connections

If no connection is selected, both IPv4 and IPv6 addresses can be selected under **Listening IP addresses** and **Remote gateways**. Otherwise, these must correspond to the connection type.

Only IPv4 values, not IPv6 values, can be used under the **Tunnels** tab.

WireGuard

The connections between two peers can now use IPv6. Internal IPs are still restricted to IPv4.

External Portal

The External Portal can now also be accessed via IPv6.

Reverse Proxy

Reverse proxy front-ends can now also be reached via IPv6 and communicate with IPv6 reverse proxy back-ends.

DNS

IPv6 addresses can be specified as DNS server addresses.

6 Traffic Shaping

As of LCOS FX 11.1, in **Inbound Rules** and **Outbound Rules** of shaping configurations, not only traffic groups can be selected, but also interfaces to which the rule should apply. The relevant selection fields have been expanded under **Network** > **Traffic Shaping** > **Shaping Configurations**.

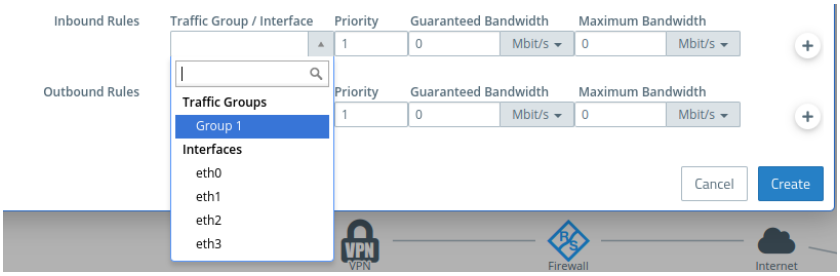


Figure 5: Network > Traffic Shaping > Shaping Configurations

Input Field	Description
Traffic Group / Interface	Select the traffic group or interface for which this rule should apply. Selectable interface types are Ethernet, VLAN, Bridge, and Bond.

7 Host and network object references in host group objects

As of LCOS FX 11.1, it is now possible to select host or network objects that have already been created in host group objects (**Desktop** > **Desktop Objects** > **Host/Network Groups**).

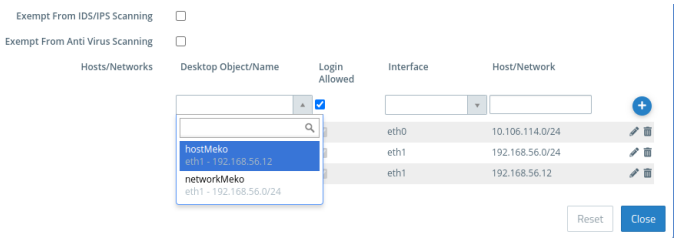


Figure 6: Desktop > Desktop Objects > Host/Network Groups

For **Hosts / Networks**, you can now alternatively select an already created host or network object under **Desktop Object/Name**. Changes to these referenced desktop objects are automatically applied to this host group when the rules are activated. Editing the existing host or network object from this dialog is only possible once it has been added to the list. In the info area, referenced objects are marked with a ⚙, so they can also be edited directly from there.

8 Source ports for user-defined services

As of LCOS FX 11.1 the option to restrict the source ports is offered under **Desktop** > **Services** > **User-defined Services**. For this purpose, the display dialog has been extended to show the source port settings.

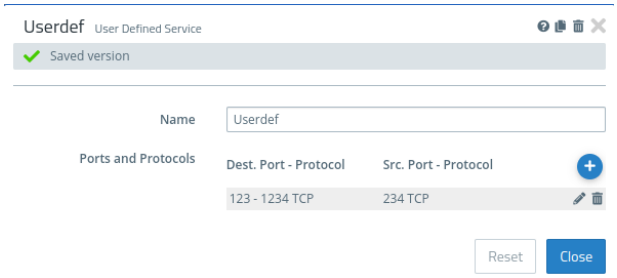


Abbildung 7: Desktop > Services > User-defined Services

In the **User-defined Services** editing window, the input options have been extended to allow the specification of the source port if necessary.

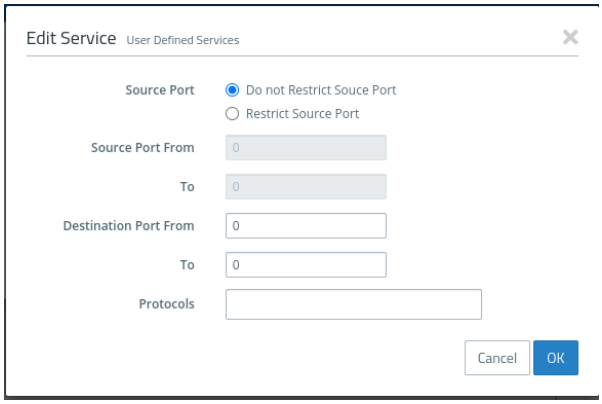


Abbildung 8: User-defined Services editing window

The **Source Port** can optionally be restricted for the TCP or UDP protocol. If you select the **Restrict Source Port** option, you can specify individual ports or ranges for TCP or UDP in order to apply the service to traffic that is transmitted from a source port. Use the **Source Port From** and **To** input fields to enter values. The value can be any integer from `1` to `65535`.

Source Port From and **To** form a port range. To specify a single port, use the same value for both fields or leave **To** blank.

9 Protocols

As of LCOS FX 11.1, the previously available protocols (ICMP, TCP, UDP, GRE, ESP, AH) have been extended by three additional protocols (IGMP, OSPF and VRRP) and, similar to the services, have been grouped together under Predefined protocols.

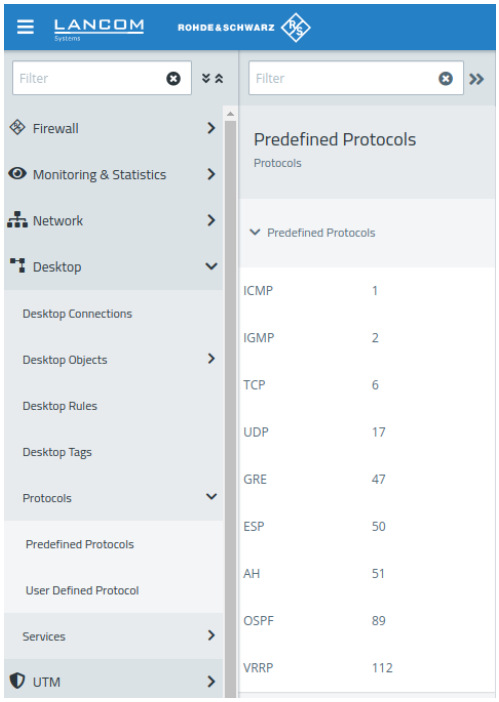


Figure 9: Desktop > Protocols > Predefined Protocols

Additional protocols or protocol numbers can be added under **User Defined Protocols**.

9.1 User Defined Protocols

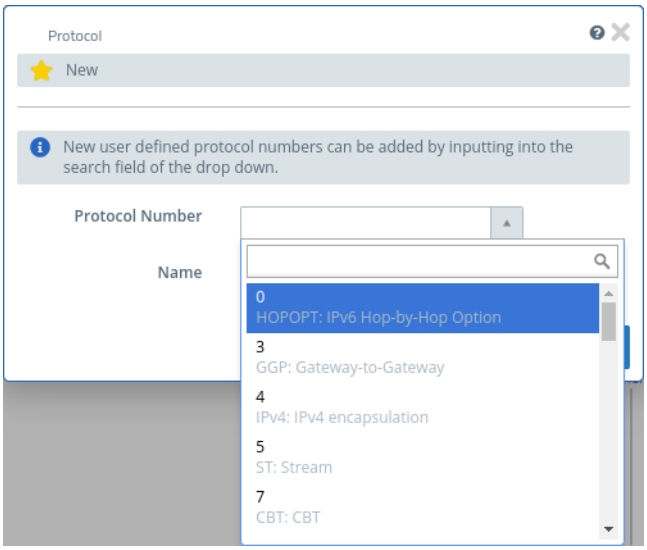
If you need a port or protocol that is not covered by one of the predefined protocols, you can create a custom protocol that can be used with a service.

Navigate to **Desktop** > **Protocols** > **User Defined Protocols** to display the list of user-defined protocols created in the system in the object list.

Here you can add a new user-defined protocol or edit an existing user-defined protocol.

You can configure the following elements in the **Protocol** editing window:

Input field	Description
Protocol Number	A protocol number from 0 to 255 can be selected. The suggested values correspond to those of the *IANA*. Protocol numbers that have already been used are not displayed. However, they can be used again by entering the number directly. If a known protocol is used, the name

Input field	Description
	is automatically suggested. All other protocol numbers are marked as user-defined protocols and the name is not automatically pre-filled.  **Figure 10: Desktop > Protocols > User Defined Protocols**
Name	Accept the suggested name or enter your own name for this user-defined protocol.

The buttons at the bottom right of the editing field depend on whether you are adding a new custom protocol or editing an existing one. For a newly configured custom protocol, click **Create** to add it to the list of available protocols or **Cancel** to discard your changes. To edit an existing custom protocol, click **Save** to save the custom protocol or **Reset** to discard your changes. You can click **Close** to close the editing window as long as no changes have been made in it.

The user-defined protocols defined here are available for use in user-defined services.

10 Reverse Proxy

Websockets

As of LCOS FX 11.1 a **Websocket** option has been added to the settings of the individual proxy paths of a reverse proxy frontend. The Websocket option must be enabled to allow a websocket provided by the backend to be proxied correctly. For TLS websockets, the SSL option must be activated in both the frontend and the backend.

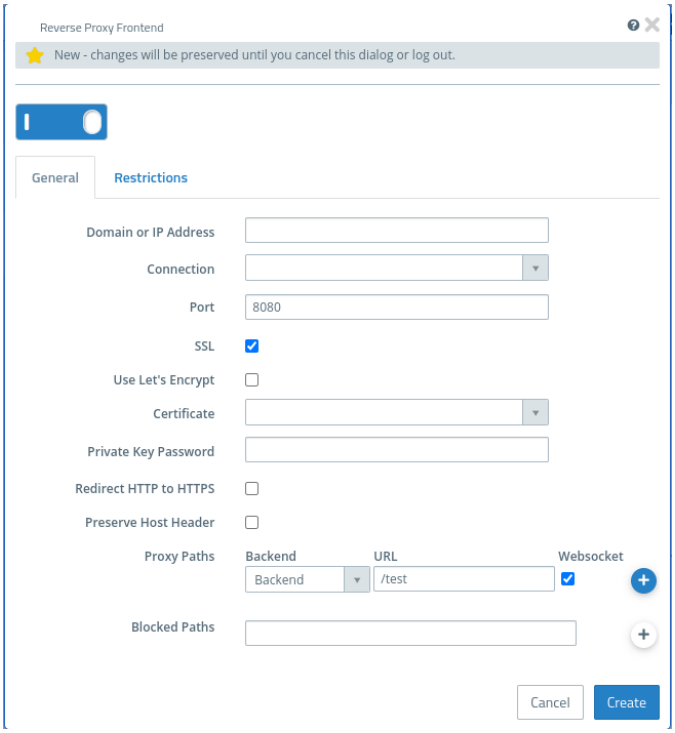


Figure 11: UTM > Reverse Proxy > Frontends > General

Preserve Host Header

In addition, a new option **Preserve Host Header** can be set to retain the host HTTP header when reverse proxying incoming HTTP requests. Depending on the application scenario, switching this option on or off can resolve problems in communication with the target server.

Access restrictions for reverse proxy front-ends

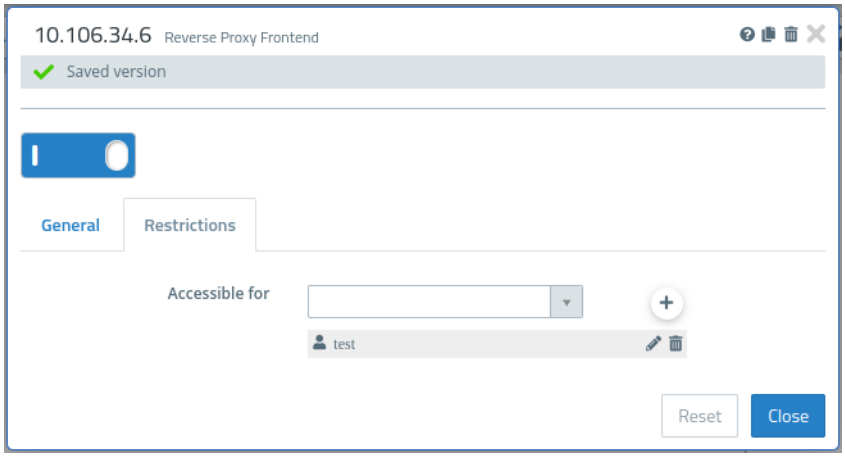


Figure 12: UTM > Reverse Proxy > Frontends > Restrictions

Table 1: Restrictions

Input field	Description
Accessible for	Individual reverse proxy front-ends can be provided with access restrictions here. If access restrictions are set up, then the reverse proxy front end is only accessible for the set users (or users who are members of a set group). A user is authenticated via the external portal. Local firewall users, LDAP users and groups, as well as users and groups of the identity provider set under **User Authentication** > **External Portal** > **SAML** are available for selection. If no restrictions are set up, the reverse proxy frontend can be used without prior authentication.

Wireguard

A previously defined wireguard connection can now also be selected from the selectable connections.

11 TCP Load Balancer

As of LCOS FX 11.1 RU1, the Reverse Proxy has been extended with a TCP Load Balancer.

Navigate to **UTM** > **Reverse Proxy** > **TCP Load Balancer** to create a TCP Load Balancer. You can create multiple Load Balancers.

In the **TCP Load Balancer** window, you can view the following information and configure the following elements:

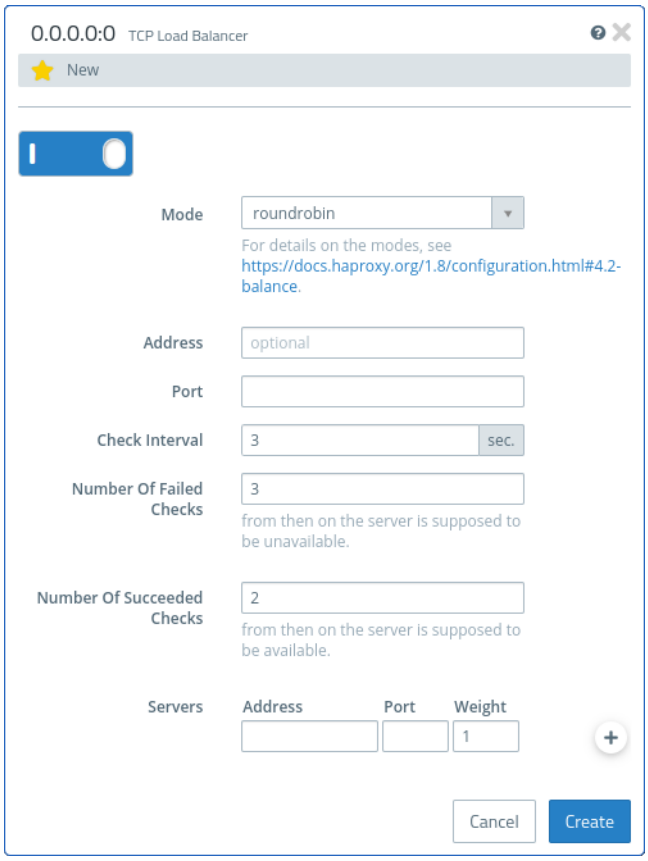


Figure 13: UTM > Reverse Proxy > TCP Load Balancer

Input Field	Description
Mode	The mode determines how the load is distributed.
Address	Optional IP address to which the Load Balancer is bound. The default is 0.0.0.0, which includes all IP addresses of the Unified Firewall.
Port	Port to which the Load Balancer is bound.
Check Interval	Interval in seconds after which checks on the availability of the addresses specified under Server are performed.
Number of Failed Checks	The number of failed checks after which a server is considered unavailable.
Number of Succeeded Checks	The number of successful checks after which a server previously considered unavailable is deemed available again.

Input Field	Description
Server	The **Address** and **Port** of a server for load balancing. The **Weight** can control its usage. The higher the value, the more likely the server will be used.

Use the buttons at the bottom right of the editing window to discard your changes (**Cancel**), or to create a new load balancer (**Create**).

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

12 External Portal

Cookies are used for reverse proxy authentication. In order for this cookie to be sent from the browser to the server under the correct conditions, it may be necessary to set the domain attribute of the cookie accordingly. For this purpose, the **Reverse Proxy Auth Cookie Domain** field has been added to the settings under **User Authentication** > **External Portal** > **Settings**.

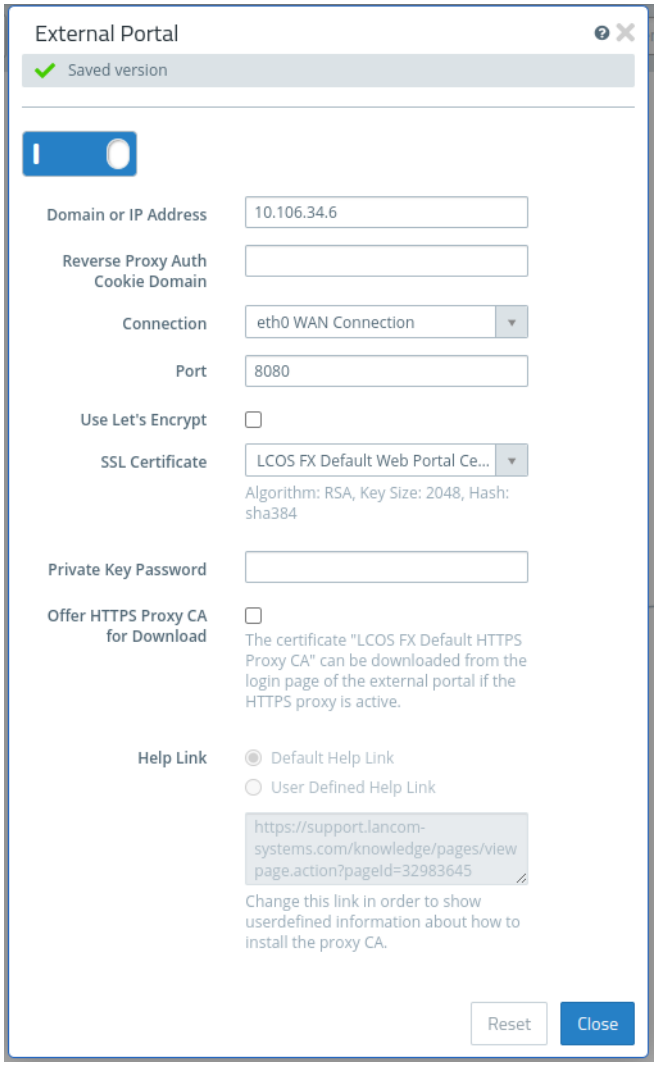


Figure 14: User Authentication > External Portal > Settings

Input field	Description
Reverse Proxy Auth Cookie Domain	Cookies are used for reverse proxy authentication. To ensure that these cookies are sent from the browser to the server under the correct conditions, it may be necessary to set the domain attribute of the cookie accordingly. If this field is empty, the cookie domain is not explicitly set and corresponds to the domain or IP specification of the external portal. If the value has not been adjusted by the user, a sensible default value is used: › No cookie domain when specifying an IP address

Input field	Description
	› The specified domain, if it is a second level domain (i.e. it is directly below a TLD, such as example.com) › The next higher domain, if it is a subdomain. So for portal.example.com then e.g. example.com. The cookie domain is important so that successful authentication on the external portal hosted at portal.example.com, for example, is also effective for other services on other subdomains, such as webmail.example.com or intranet.example.com. For special cases, the cookie domain can be manually set to a custom value. **Important safety information:** Setting a cookie domain causes the browser to send this cookie to the target server for requests to the specified domain. The cookie for reverse proxy authentication is sensitive information that enables the owner to access resources shared via reverse proxy. Only cookie domains that are fully trustworthy should be specified.

Wireguard

A previously defined wireguard connection can now also be selected from the selectable connections.

13 SAML / Single Sign-On

The internal and external portal now support single sign-on to selected identity providers (IdP) using SAML. Microsoft Azure and Keycloak are supported. The settings for this are made independently of each other for the external portal and the internal portal.

13.1 SAML / Single Sign-On (Internal Portal)

The internal portal supports single sign-on to selected identity providers (IdP) using SAML. Microsoft Azure and Keycloak are supported.

Navigate to **User Authentication** > **Internal Portal** > **SAML** to open an editing window in which you can customize the settings for SAML.

You can configure the following elements in the **SAML** editing window:

IdP Synchronization

These settings are necessary for connecting the firewall to the IdP. Lists of users and groups known to the IdP can then be queried via this connection.

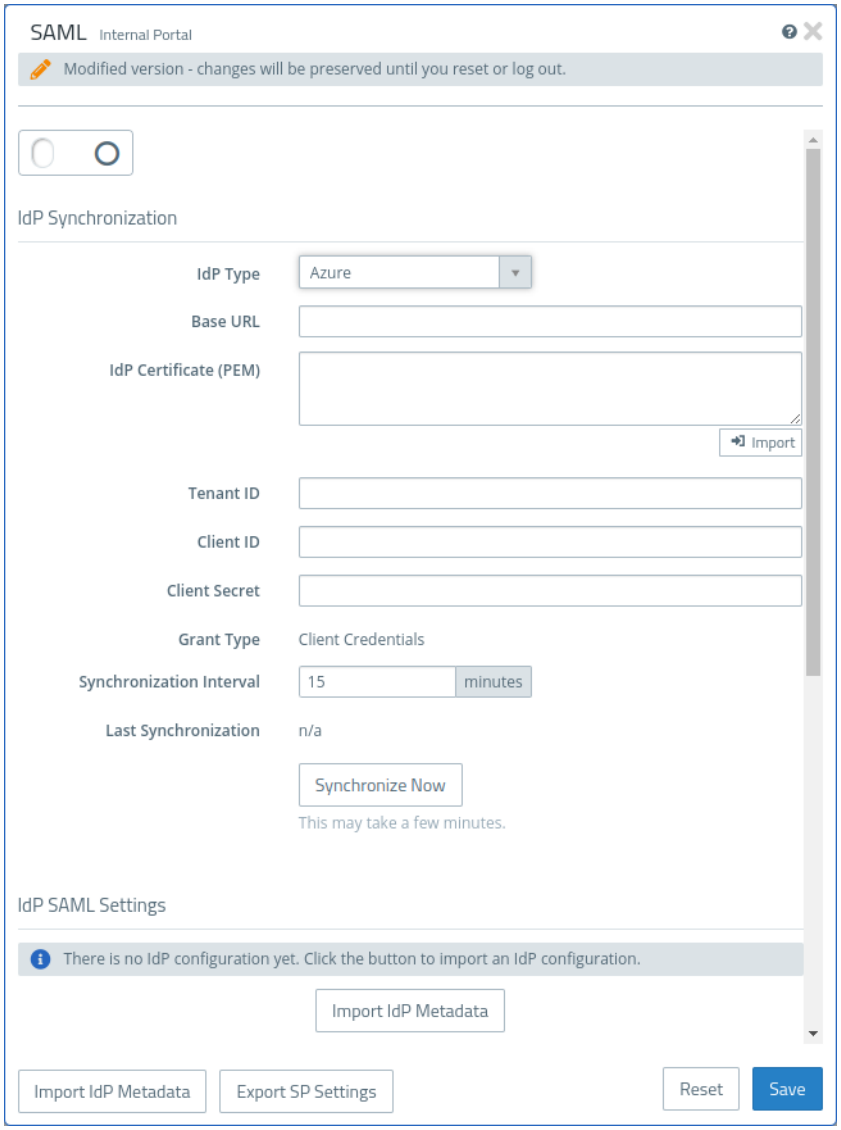


Figure 15: IdP Synchronization (Microsoft Azure)

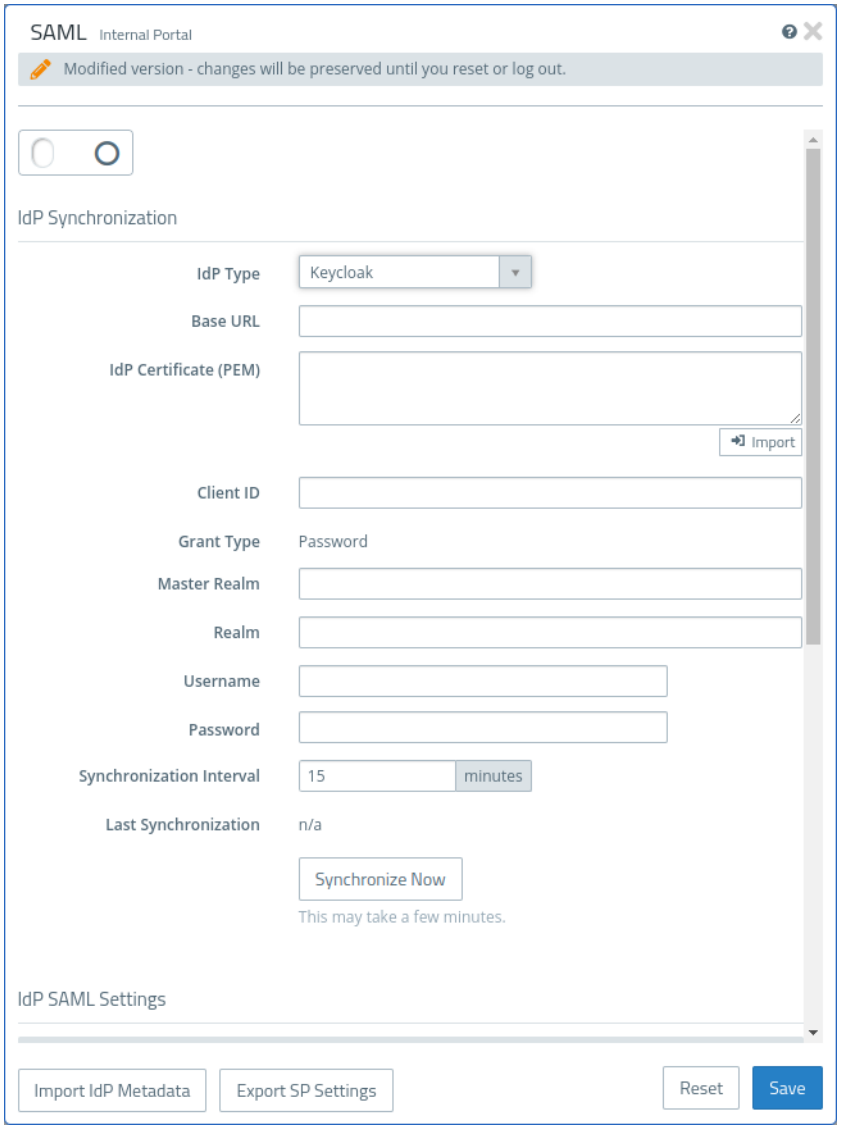


Figure 16: IdP Synchronization (Keycloak)

Input field	Description
I/**O**	A slide switch indicates whether the SAML connection is currently active (**I**) or inactive (**O**). You can change the status by clicking on the slide switch. The SAML connection is deactivated by default.
IdP Type	Azure or Keycloak. The details vary depending on the type.
Base URL	The URL under which the IdP API can be reached. For Keycloak, this is the host name or IP address and the port of the Keycloak server. With Azure, the URL is made up of the host name (e.g. “https://sts.windows.net/”) and the tenant ID. E.g. “https://sts.windows.net/ac564d8f-3367-c9a1-31dd-68e35de484ac”
IdP Certificate (PEM)	Optional. If the firewall connection to the IdP uses a certificate that the firewall does not trust, this can be stored here so that a secure connection can be established. This is helpful for self-signed certificates, for example. It can be entered in text form or imported from a file.
IdP Type Azure	
Tenant ID	Azure tenant ID.

Input field	Description
Client ID	ID of the client configured on the IdP under which the queries are carried out.
Client Secret	Azure client secret.
Grant Type	Always “Client Credentials”.
IdP Type Keycloak	
Client ID	ID of the client configured on the IdP under which the queries are carried out.
Grant Type	Always “Password”.
Master Realm	The Keycloak Master Realm.
Realm	The realm for which the users and groups are to be queried.
Username	User name for logging in to the Keycloak API.
Password	Password for logging in to the Keycloak API.
Synchronization Interval	Interval between the start of two synchronization processes. A synchronization process is only started if the previous synchronization process has been completed. If it is still running, nothing is done. After the interval has elapsed again, this check is repeated and a new synchronization process is started if necessary.
Last Synchronization	Time of the last synchronization process. A synchronization process can be started manually in the background via **Synchronize Now**.

IdP SAML Settings

The IdP SAML settings are imported from the so-called “Federation Metadata” XML file. This file can be exported from the IdP. Its content depends on the respective settings in the IdP. If no metadata has been imported yet, the form displays the **Import IdP Metadata** button provided for this purpose. After the import, the transferred settings are displayed here. Changed IdP metadata can also be imported later using the **Import IdP Metadata** button at the bottom of the editor window.

SP SAML Settings

The SP-SAML settings describe where and how the service provider running on the firewall can be reached for SAML authentication. The service provider settings can be exported as an XML file. This XML file can then be imported into the IdP to apply the relevant settings.

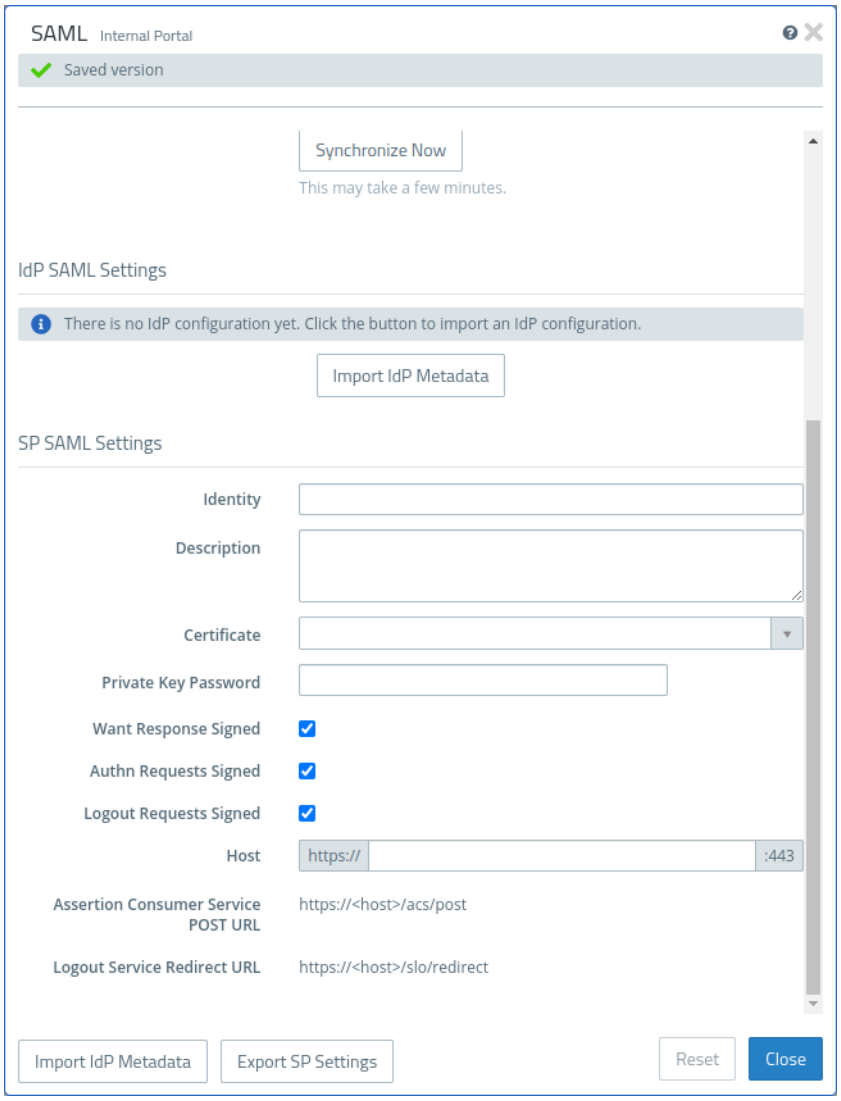


Figure 17: SP SAML Settings

Input field	Description
Identity	A freely selectable identifier for the service provider. E.g. the firewall name.
Description	An optional description.
Certificate	The certificate. Azure only supports certificates with a key size of 2048 bits due to a limitation of Azure.
Private Key Password	The password for the private key of the certificate used.
Want Response Signed	If this option is activated, responses from the firewall are signed.
Authn Requests Signed	If this option is activated, only correctly signed Authn requests are accepted.
Logout Requests Signed	If this option is activated, only correctly signed logout requests are accepted.

Input field	Description
Host	Host address at which the client can reach the service provider. The port always corresponds to the **Web Login Port** of the internal portal (**User Authentication** > **Internal Portal** > **Settings**). The host part can be freely selected. An IP address or an appropriately resolving host name that belongs to an intranet interface of the firewall should be specified here. The internal portal and the service provider can only be accessed on these interfaces.
Assertion Consumer Service POST URL	URL to which the client browser is redirected as part of the login process. Results from the host address.
Logout Service Redircect URL	URL to which the client browser is redirected as part of the logout process. Results from the host address.

Users of the IdP for the internal portal

The users and groups loaded by the IdP set up for the internal portal can be used to log in to the firewall's internal portal. Accordingly, these users and groups can be used for

- the administration of content filter override codes (**UTM** > **URL/Content Filter** > **Settings**),
- the set of rules on the desktop (user and group objects, both simple and VPN variants) and
- the Wake on LAN function (**User Authentication** > **Internal Portal** > **Wake on LAN**).

13.2 SAML / Single Sign-On (External Portal)

The external portal supports single sign-on to selected identity providers (IdP) using SAML. Microsoft Azure and Keycloak are supported.

Navigate to **User Authentication** > **External Portal** > **SAML** to open an editing window in which you can customize the settings for SAML.

You can configure the following elements in the **SAML** editing window:

IdP Synchronization

These settings are necessary for connecting the firewall to the IdP. Lists of users and groups known to the IdP can then be called up via this connection.

Input field	Description
I/**0**	A slide switch indicates whether the SAML connection is currently active (**I**) or inactive (**0**). You can change the status by clicking on the slide switch. The SAML connection is deactivated by default.
IdP Type	Azure or Keycloak. The details vary depending on the type.
Base URL	The URL under which the IdP API can be reached. For Keycloak, this is the host name or IP address and the port of the Keycloak server. With Azure, the URL is made up of the host name (e.g. “https://sts.windows.net/”) and the tenant ID. E.g. “https://sts.windows.net/ac564d8f-3367-c9a1-31dd-68e35de484ac”
IdP Certificate (PEM)	Optional. If the firewall connection to the IdP uses a certificate that the firewall does not trust, this can be stored here so that a secure connection can be established. This is helpful for self-signed certificates, for example. It can be entered in text form or imported from a file.
IdP Type Azure	
Tenant ID	Azure tenant ID.

Input field	Description
Client ID	ID of the client configured on the IdP under which the queries are carried out.
Client Secret	Azure client secret.
Grant Type	Always “Client Credentials”.
IdP Type Keycloak	
Client ID	ID of the client configured on the IdP under which the queries are carried out.
Grant Type	Always “Password”.
Master Realm	The Keycloak Master Realm.
Realm	The realm for which the users and groups are to be queried.
Username	User name for logging in to the Keycloak API.
Password	Password for logging in to the Keycloak API.
Synchronization Interval	Interval between the start of two synchronization processes. A synchronization process is only started if the previous synchronization process has been completed. If it is still running, nothing is done. After the interval has elapsed again, this check is repeated and a new synchronization process is started if necessary.
Last Synchronization	Time of the last synchronization process. A synchronization process can be started manually in the background via **Synchronize Now**.

IdP SAML Settings

The IdP SAML settings are imported from the so-called “Federation Metadata” XML file. This file can be exported from the IdP. Its content depends on the respective settings in the IdP. If no metadata has been imported yet, the form displays the **Import IdP Metadata** button provided for this purpose. After the import, the transferred settings are displayed here. Changed IdP metadata can also be imported later using the **Import IdP Metadata** button at the bottom of the editor window.

SP SAML Settings

The SP-SAML settings describe where and how the service provider running on the firewall can be reached for SAML authentication. The service provider settings can be exported as an XML file. This XML file can then be imported into the IdP to apply the relevant settings.

Input field	Description
Identity	A freely selectable identifier for the service provider. E.g. the firewall name.
Description	An optional description.
Certificate	The certificate. ⓘ Azure only supports certificates with a key size of 2048 bits due to a limitation of Azure.
Private Key Password	The password for the private key of the certificate used.
Want Response Signed	If this option is activated, responses from the firewall are signed.
Authn Requests Signed	If this option is activated, only correctly signed Authn requests are accepted.
Logout Requests Signed	If this option is activated, only correctly signed logout requests are accepted.
Host	Host address at which the client can reach the service provider. The host specification and the port correspond to the settings for the external portal (**User Authentication** > **External Portal** > **Settings**, **Domain or IP address** and **Port**). Adjustments are not possible.

Input field	Description
Assertion Consumer Service POST URL	URL to which the client browser is redirected as part of the login process. Results from the host address.
Logout Service Redircect URL	URL to which the client browser is redirected as part of the logout process. Results from the host address.

Users of the IdP for the external portal

The users and groups loaded by the IdP set up for the external portal can be used to log in to the external portal of the firewall. Accordingly, these users and groups can be used for

- VPN profiles (**User Authentication** > **External Portal** > **VPN Profiles**) and
- access restrictions to reverse proxy frontends (**UTM** > **Reverse Proxy** > **HTTP(S)Frontends**).

14 Let's Encrypt Server

As of LCOS FX 11.1, there are further options for configuring a separate address for the Let's Encrypt server in the settings.

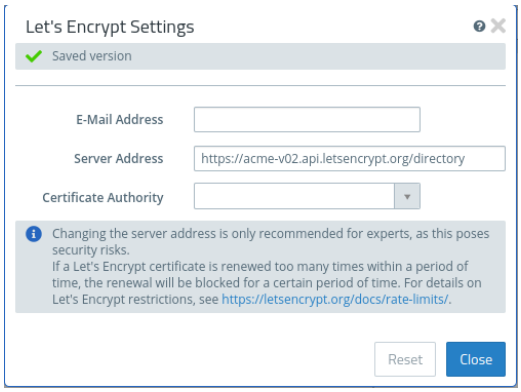


Figure 18: Certificate Management > Let's Encrypt

Input field	Description
Server Address	Optionally, enter an URL for the Let's Encrypt server. If the server's certificate is not globally trusted, the corresponding certificate authority must be imported in the certificate management and then selected here.
Certificate Authority	If the URL for the Let's Encrypt server has changed, enter the certificate authority here if it is not globally trusted.

15 Changes to antivirus

As of LCOS FX 11.1, the **Heuristic Analysis** option has been removed as part of the switch to Bitdefender's antivirus engine. The heuristic analysis is always active from now on.

In addition, the option Scan archive files can now be set separately for **Mail** or **HTTP(s) and FTP**.

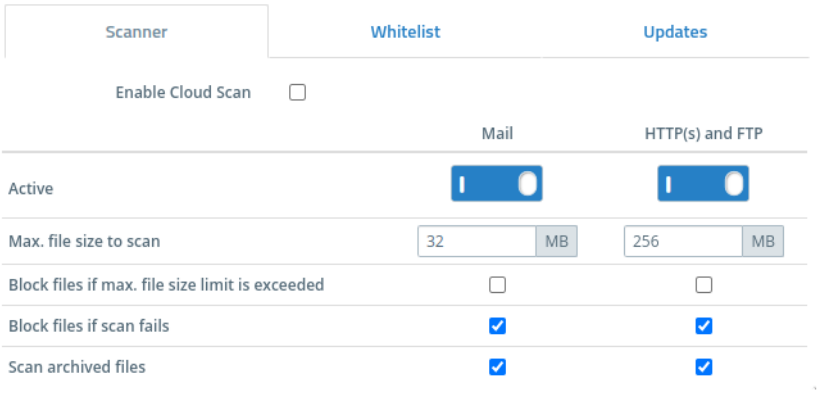


Figure 19: UTM > Antivirus Settings > Scanner