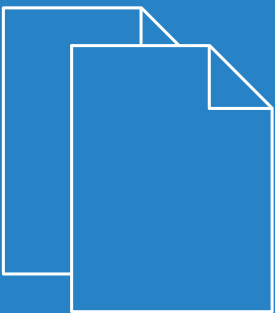


LCOS FX 10.5

Addendum



Contents

1 Addendum to LCOS FX version 10.5	4
2 Information panel	5
3 Executive Report	6
4 HTTP(S) Proxy Whitelists	10
5 Recovery points	11
6 Multiple administrators logged in	12
7 Desktop search	13
8 IMAP proxy	14
9 Content filter codes	15
9.1 Managing URL/content filter codes.....	15
10 Application-based routing	20
10.1 Routing Profiles.....	20
11 Creating rules from the log	22
12 VPN-SSL bridging	23
13 User Authentication	25
13.1 Technical background and preparations.....	25
13.2 Logging in.....	26
13.3 LDAP/AD.....	31
13.4 External portal.....	32
13.4.1 Settings.....	33
13.4.2 VPN profiles.....	33
13.5 Internal portal.....	34
13.5.1 Settings.....	34
13.5.2 Wake-on-LAN.....	34
13.6 Users.....	35
13.7 LDAP users.....	35
13.8 LDAP groups.....	35
13.9 Local users.....	36
13.10 Unassigned users.....	36
13.11 Example applications.....	37

Copyright

© 2020 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 (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.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom-systems.com

1 Addendum to LCOS FX version 10.5

This document describes the changes and enhancements in LCOS FX version 10.5 since the previous version.

2 Information panel

The information area is located on the right-hand side of the desktop.

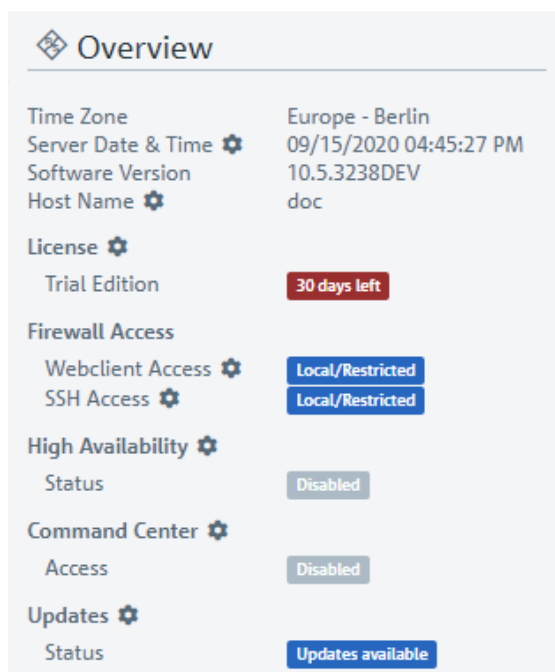


Figure 1: Information panel of the LANCOM R&S® Unified Firewall web client

As of LCOS FX version 10.5 RU2, you can click on entries with  to open a corresponding settings dialog.

3 Executive Report

From LCOS FX version 10.5 RU2, the **Desktop > Export** feature is being replaced and expanded by the feature described below.

By navigating to **Firewall > Executive Report**, you can generate a report on your current desktop configuration and various statistics, and transfer these to your computer.

In the **Executive Report** window you can choose between the file formats PDF and HTML by selecting the appropriate radio button.

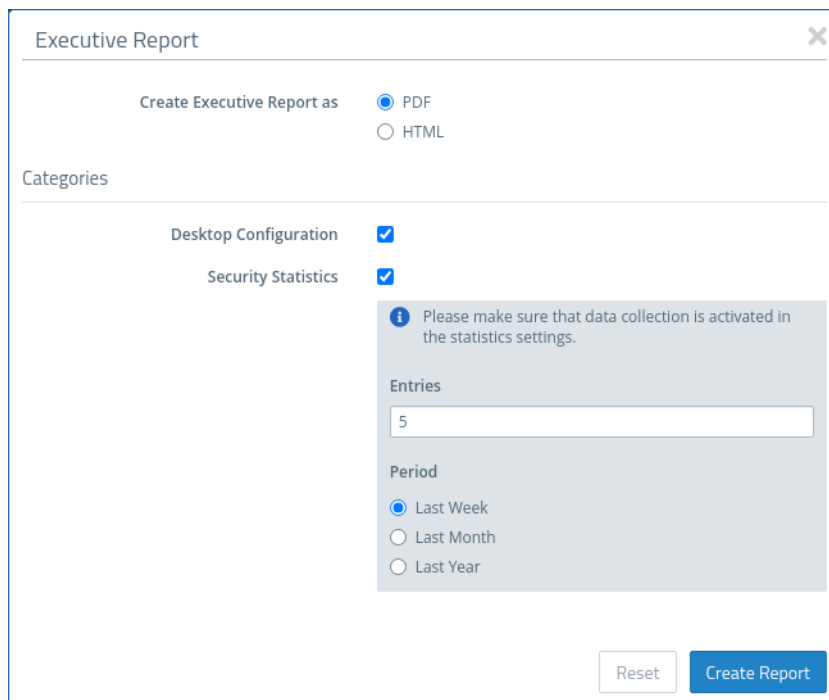




Figure 2: Executive Report – settings

In the **Categories** section you can configure the following elements:

Input box	Description
<p>Desktop configuration</p>	<p>The export file contains an image of the current desktop and a table with all of the configured firewall rules, including additional information such as NAT, DMZ, IP addresses of the host objects and the content of the description fields for the configured desktop objects and connections.</p> <hr/> <p> Desktop objects are only included if they are linked to other desktop objects.</p>
<p>Security statistics</p>	<p> In order for statistics to be generated, the value under Monitoring & Statistics > Settings must at least be set to "Create Statistics" for the event types.</p> <p>Contains the statistics that are also available under the menu item Monitoring & Statistics > Statistics > Overview, both as a graph and as a table:</p> <ul style="list-style-type: none"> > Blocked connections

Input box	Description
	<ul style="list-style-type: none">> Blocked content> Top viewed domains> Top blocked domains> Top traffic per source <p>If security statistics are activated, further settings are available:</p> <ul style="list-style-type: none">> Number of entries (this setting applies to the top lists only)> Period, definition of the period to be recorded starting with the current point in time

Click on **Create Report** if you want to create and transfer the export file. Your settings are saved and a file name with a date prefix (YYYY-MM-DD_HH-mm) is suggested. Otherwise click **Reset** to reset the settings to the last saved settings.

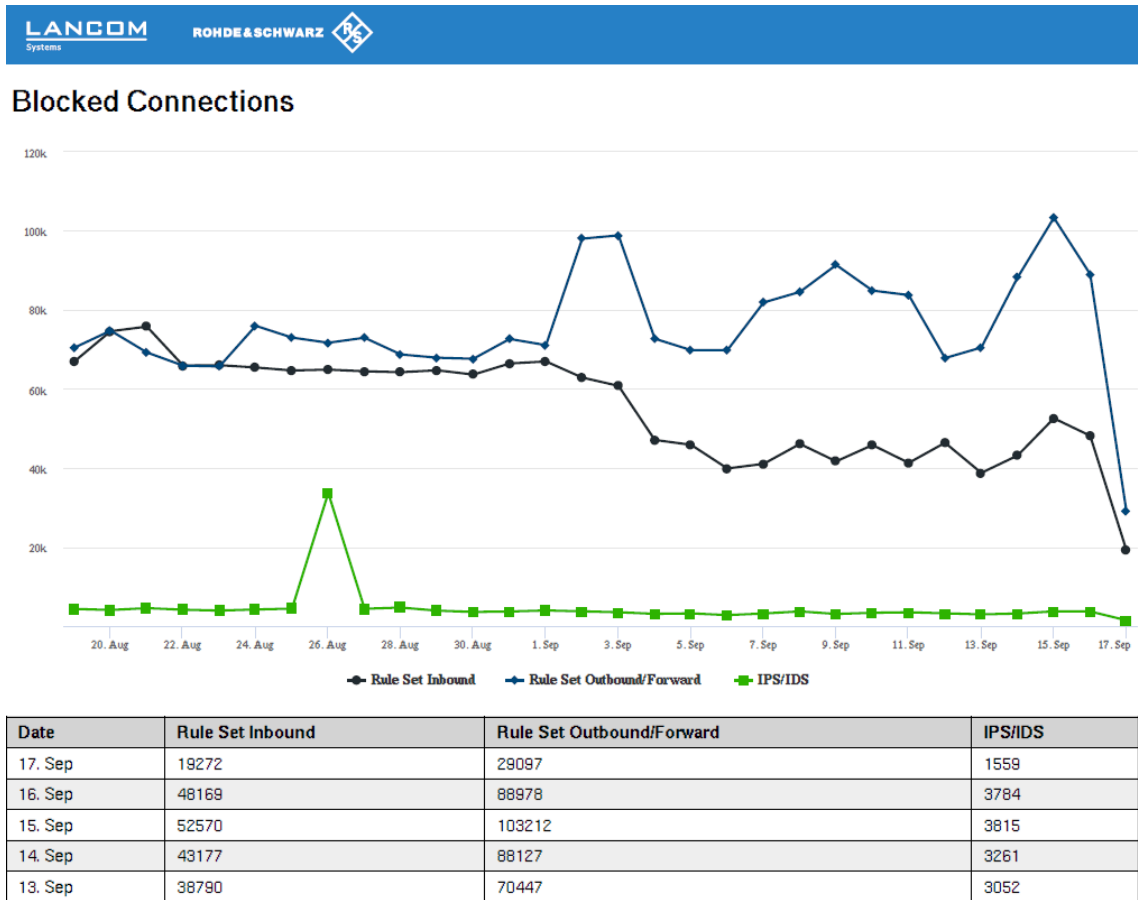
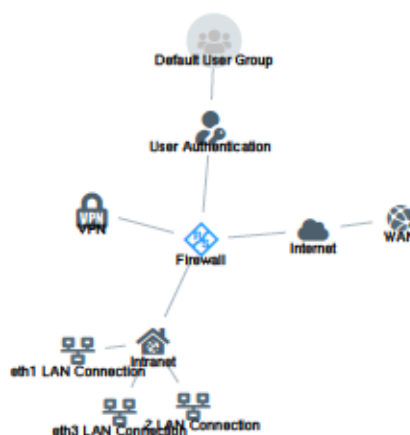


Figure 3: Sample from an Executive Report



Desktop Configuration





Source	Action	NAT	Destination	Service	Rule Settings	Connection Settings
eth2 LAN Connection 10.10.21.0/24	→	→	WAN eth0 WAN Connection	IMAP4 143 TCP	Proxy: IMAP4	Webfilter: Sex: Content Filter Kriminelles: Content Filter Werbung: Content Filter
	→	→		POP3s 995 TCP	Proxy: POP3S	
	→	→		SMTP 25 TCP	Proxy: SMTP	
	→	→		IMAP4s 993 TCP	Proxy: IMAP4S	
	→	→		POP3 110 TCP	Proxy: POP3	
	→	→		SMTPs 465 TCP	Proxy: SMTPS	
	→	→		HTTPS 443 TCP	Proxy: HTTPS	
	→	→		HTTP 80 TCP	Proxy: HTTP	
eth1 LAN Connection 10.10.20.0/24	→	→	WAN eth0 WAN Connection	HTTPS 443 TCP	Proxy: HTTPS	Webfilter: Sex: Content Filter Kriminelles: Content Filter Werbung: Content Filter
	→	→		HTTP 80 TCP	Proxy: HTTP	

Figure 4: Sample from an Executive Report

4 HTTP(S) Proxy Whitelists

With LCOS FX version 10.5 RU2, the whitelists for the HTTP(S) proxy have been changed from the previous flat list of domains to a URL list based on domain groups. This allows individual groups of domains to be quickly prohibited or permitted.

You can edit the domain groups under **UTM > Proxy > HTTP Proxy Settings**.

Eingabefeld	Beschreibung
<p>Whitelists</p>	<p>You can define separate whitelists for individual domain groups.</p> <p>A domain group consists of a name, an optional description and a list of URLs (domains) that should be excluded from SSL interception, virus scanning and URL filtering. You can add any number of domains to a domain group. Enter a domain and click  to add it to the list.</p> <p>Domains in the whitelist are accepted by the HTTP(S) proxy without analysis and become directly available to the users' browser. No certificates are created. This is necessary for services which employ strict Certificate Pinning, such as Windows Update (<i>windowsupdate.com</i>).</p> <p>You can edit or delete a domain group by clicking on the corresponding button next to an entry. Select or deselect the checkbox to the left of a domain group to enable or disable its use.</p> <hr/> <p> To unblock a domain „example.com“ including all subdomains like „www.example.com“, write „example.com“ with a dot at the beginning. To unblock only the domain „example.com“ without subdomains, write „example.com“ without a dot at the beginning.</p>

5 Recovery points

With LCOS FX version 10.4 RU3, LANCOM R&S® Unified Firewalls was prepared for the recovery functionality. Therefore, immediately before the upgrade to the LCOS FX version 10.5, for the first time a recovery point is created for the outgoing version (10.4 RU3).

Recovery points can be displayed using the System menu and executed if necessary.

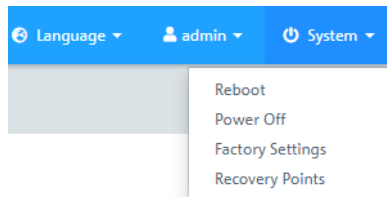


Figure 5: System menu with recovery points

- ⚠ A recovery is also possible in a high-availability scenario, although the recovery is limited to the main firewall only. The backup firewall can no longer be operated and must be installed anew.

6 Multiple administrators logged in

Multiple administrators can be logged in to the LANCOM R&S® Unified Firewall web client at the same time. However, only one of these administrators can have write access, i.e. make changes to the configuration. This is always the administrator who logged in first; the others all have read access only. If the administrator with write access then logs off, these privileges are passed on to the next administrator in line, i.e. who logged in earliest. This administrator receives a corresponding message.

When you log in, you will be informed that a session with write access is already active. If you have read permissions for the administrator settings, you will also see a list of the other administrators who are currently logged on. If you log in with an account that already has another privileged session active, you can terminate that session and start a new one. This is useful if you just closed a browser window without logging off.

The header shows whether you have reduced privileges.



An administrator with write access is also informed in the header if additional administrators log in.



Clicking the warning will bring up the same warning message that was also displayed when you logged in.

7 Desktop search

As of LCOS FX version 10.5 the Desktop Tags filter has been enhanced with the Desktop Filter. The input field now displays **Filter** instead of the previous **Tags**.

You can use the **Filter** input field at the end of the toolbar to quickly identify desktop objects based on the following criteria:

- > Name of the desktop object
- > Description
- > Tags
- > Interface used, including "any" and "Internet" interface
- > IP addresses, IP networks and IP ranges
- > User or user group names
- > Internet connections
- > IPsec and VPN SSL connection names
- > Local and remote networks used in IPsec connections

You can also filter for desktop connections, but due to the way the desktop works, connections can only be viewed indirectly by displaying the related desktop objects. Values that can be used for filtering:

- > Service name
- > Ports (for port ranges, a search is conducted in addition to the text filter to see whether the search string is a number and lies within the port range)
- > Protocol used (TCP, UDP, ICMP ...)
- > Activated DMZ, external IP address used for the DMZ
- > Activated proxy

Click in the input field to open a drop-down list with the names of the possible inputs. You can either select an element from the list to include it in the filter input, or search for a specific element. Pseudo elements are used to display the connections and are added to find connections with an activated proxy and DMZ. As you type your input into the search field, your LANCOM R&S[®] Unified Firewall will show only the drop-down list items that contain the characters you entered. You can add any number of entries to the filter input, all of which are combined with an "Or" operator. Input is not case sensitive.

Your LANCOM R&S[®] Unified Firewall limits the displayed desktop objects to those that match the selected filter criteria. Desktop nodes along the path from the **Firewall** root node to a node that matches the filter criteria are always displayed, even if intermediate objects do not match the search criteria.


Click on  in the input field to delete the search input and return to the unfiltered list view.

8 IMAP proxy


Starting with LCOS FX version 10.5 the complete e-mail security is also available for the IMAP protocol. Both IMAP with StartTLS and IMAPS are supported. This means that even smaller end customers who do not host their e-mails themselves can use the usual e-mail security with anti-malware and antispam.

9 Content filter codes

Content filter management has been improved to include codes that allow users to view blocked pages despite the filter by entering the respective code at certain times. The settings for URL/Content Filters have been adjusted for this change. The override mode can now be set under **UTM > URL/Content Filter > Settings** and there is a new option **Allow override by code**.

Input box	Description
Override Mode for Categories	<p>If a website has been blocked, you can control the behavior of your firewall here:</p> <ul style="list-style-type: none"> > Disabled Do not allow overrides. > Allow Override If a webpage is blocked, you can override the Content Filter for a set period of time. Enter the duration in minutes for disabling the category profile of the Content Filter. <hr/> <p> Only the current category of a URL/Content Filter profile is unblocked for a certain period.</p> <ul style="list-style-type: none"> > Allow Override by Code If a website has been blocked, your users can override the Content Filter by entering a short numerical code. Specify the users who are allowed to manage the codes here. From the perspective of your LANCOM R&S® Unified Firewall, these can be local users, LDAP users or LDAP groups.

Edit the profiles in the overview of the URL/Content Filter under **UTM > URL/Content Filter > URL/Content Filter**. The option **Override by user** takes on a changed meaning depending on the above setting.

Input box	Description
Override by user	<p>Check this box to allow overrides for this Content Filter profile. Depending on your settings, a code may have to be entered here. Learn more about managing the codes under Managing URL/content filter codes on page 15</p> <hr/> <p> This option is only available for profiles that are non-standard profiles.</p>

9.1 Managing URL/content filter codes

If a website has been blocked, your users can override the blocking mechanisms of the content filter—optionally by entering a short numerical code on the block page. The user has to be permitted to manage these codes and must be logged on to the LANCOM R&S® Unified Firewall. See the section “User Authentication” in the User Manual.

The administrator must have entered the users authorized to set up codes in the configuration of the content filter under **Override Mode for Categories**. These users then connect via HTTPS to one of the local firewall interfaces. With the appropriate DNS configuration in the network, for example, simply enter `https://firewall` or the IP address (`https://<IP address>`) in the web browser. These web pages are created in a responsive design so that they adapt to the capabilities of the device and can also be operated from a smartphone. For example, if the administrator has set up an LDAP connection of the firewall to Active Directory, log on with the access data of your Windows account.

Once logged in to the firewall, the management interface is visible at the bottom left. This displays the active codes that have been set up previously. "Active" means that these codes are available for use, but not necessarily that they are currently being used.

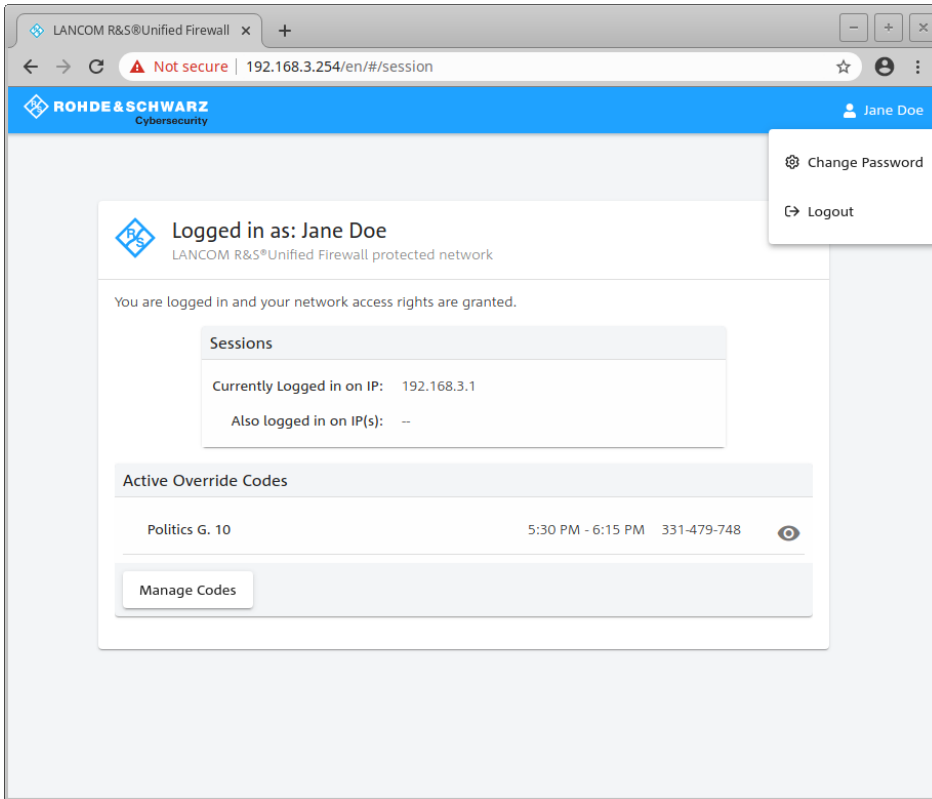


Figure 6: Override code: Accessing the management

If you click the eye symbol next to an active code, the code will be displayed as it will be shown to the intended users. Users can then enter the code on the block page.

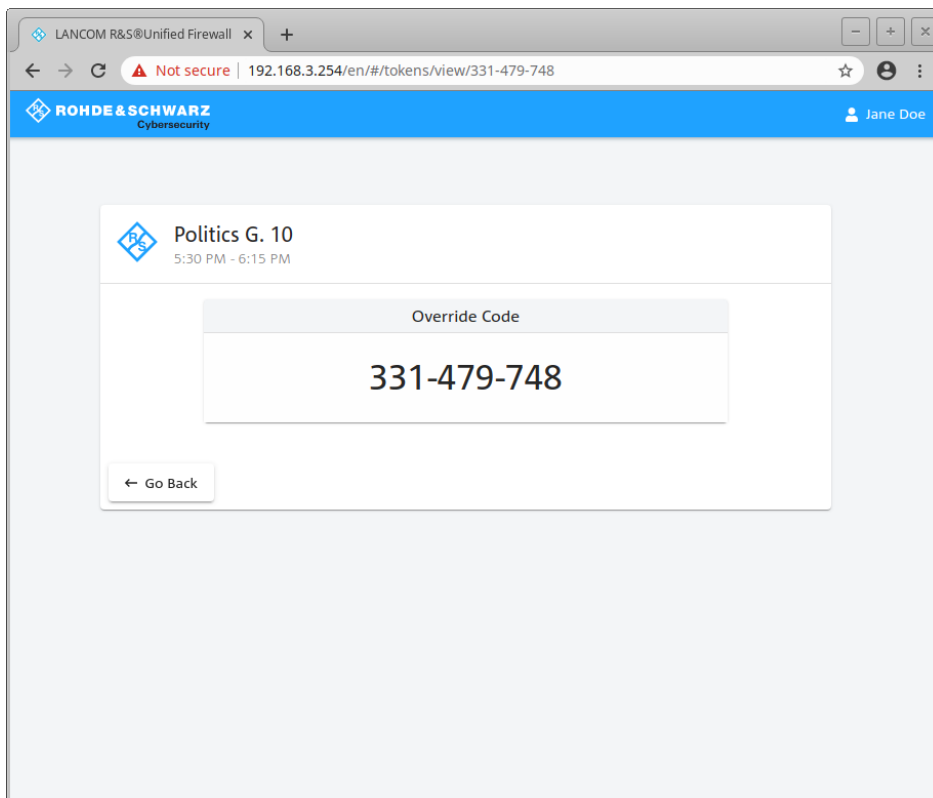


Figure 7: Override code: Presentation mode

The button **Manage codes** on the main page displays the interface for managing the codes. All of the codes are displayed here, including those that have expired and those ready for future use.

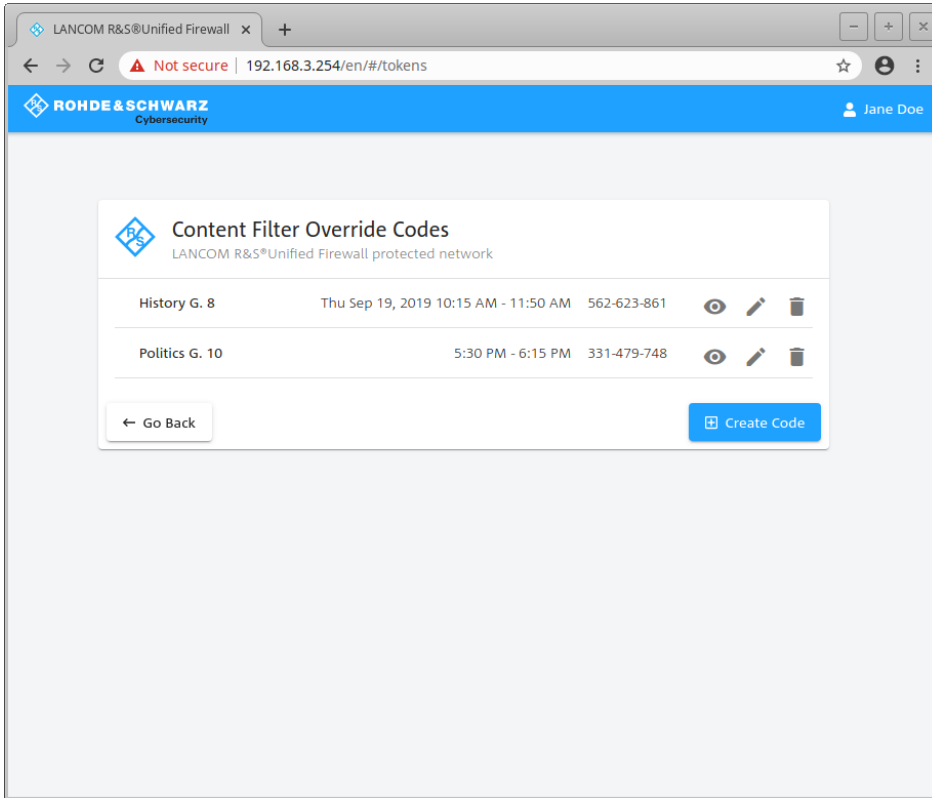


Figure 8: Override code: Management mode

You can use the icons to display a code in presentation mode (eye), edit it (pen) or delete it (trash can). New codes are generated by using the button **Create code**. You configure the following options here:

Input box	Description
Code Name	The name that refers to and is displayed with the code.
Code	The code itself. This cannot be changed.
Valid on	Date the code is valid.
Valid from	The time of day when the code becomes valid and can be used to bypass a filter.
Valid until	The time of day when the codes becomes invalid and can no longer be used to bypass a filter.

The screenshot shows a web browser window with the URL `192.168.3.254/en/#/tokens/edit/331-479-748`. The page header includes the LANCOM R&S logo and the user name 'Jane Doe'. The main content area displays a form for creating a new code:

- Code Name ***: Politics G. 10
- Code**: 331-479-748
- Valid on ***: 4/9/2020
- Valid from ***: 5:30 PM
- Valid until ***: 6:15 PM

At the bottom of the form are two buttons: 'Save' and 'Cancel'.

Figure 9: Override code: Create code

Save your new or changed code by clicking **Save**, or discard your entries with **Cancel**.

- ⚠ If you change a code's validity periods, this change does not apply to users who are already using this code. These overrides will end at their original end time. Users will then have to enter the code again to continue using the override.

A call to a blocked page is then displayed with a message on which a valid code can be entered.

The screenshot shows a notification message from the LANCOM R&S Unified Firewall. The message is titled 'URL FILTER MESSAGE' and contains the following information:

- URL BLOCKED !**
- User **michi** (IP:192.168.2.1) is not allowed to view following page
- <https://www.tripadvisor.com/>
- URL FILTERING:** URL or part of it is blacklisted in **Communication & Lifestyle**
- Override Code**

At the bottom of the message is a text input field and a 'Submit' button.

Figure 10: Override code: Blocked page notification

10 Application-based routing

As of LCOS FX version 10.5, application-based routing can be used for connections. The Application Filter section was renamed Application Management and expanded to include routing profiles.

Like the application-filter profiles, routing profiles are used in the desktop connections. The Connection dialog now features the new tab "Application-based routing", which can be used to add the configured routing profiles from the list on the right.




In contrast to the filter profiles, there is no mode setting for the routing profiles.

10.1 Routing Profiles

Navigate to **UTM > Application Management > Routing Profiles** to display the list of Routing Profiles in the object bar.

In the expanded view, the table columns show the **Name** of the profile and the number of protocols and applications selected for it. Use the buttons in the last column to view and modify the settings for an existing routing profile, create a new profile based on a copy of an existing profile, or delete a profile from the system.

Use the settings for **Routing Profiles** to configure the following options:

Input box	Description
Name	Enter a name for the routing profile.
Internet connection	Configures the Internet connection over which the traffic is to be routed.
Bypass proxy	Set a check mark in the check box to bypass the proxy. The traffic will then not be routed through the proxy. In particular, this makes it possible to exclude certain applications from the proxy, for example applications for mobile devices that enforce certificate pinning.
Bypass IPsec	Set a check mark in the check box to bypass an IPsec tunnel, meaning that the traffic is not routed through IPsec tunnels. Among other things, this feature can be used for branches that route all of their Internet traffic via IPsec to their headquarters. For certain trusted applications that need low latency, such as Microsoft Office 365, it often makes sense to exclude this traffic from being redirected to the headquarters.
Rules	<p>Select the protocols and applications you want to add to the profile. The protocols and applications are listed in the table by Category.</p> <p>Use the Filter input field to filter the list of protocols and applications and display only the entries that match your search input. Click  to show the unfiltered list of protocols and applications.</p> <p>Click the  button next to a category to view the protocols and applications that it contains, along with a brief description. You can select entire categories or individual protocols or applications by placing a checkmark in the appropriate box. Uncheck the box next to a category, protocol, or application to remove it from the Application Filter profile. To hide protocols and applications, click the  button next to the category.</p>

The buttons available at the bottom right of the edit box depend on whether you are adding a new router profile or editing an existing profile. For a new profile, click **Create** to add it to the list of profiles, or **Cancel** to discard your changes.

If you have made changes, you can use the buttons at the bottom right of the edit window to save them (**Save**) or discard them (**Reset**). Otherwise you can close the window (**Close**).

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

The routing profiles defined here can be used in user-defined firewall rules to implement application-based routing.

11 Creating rules from the log

You can create rules for denied access attempts directly from the alert and system logs. The alert log (**Monitoring & Statistics > Logs > Alert Log**) is preferred, since you can filter directly for Connection Blocked entries.

To use this functionality, the firewall must be configured accordingly:

1. Under **Monitoring & Statistics > Settings**, the setting for **Blocked Forwarded Traffic** has to be set to **Save Raw Data Locally** in order for the firewall to access the necessary data.
2. An Internet connection has to be defined if there is no data traffic between internal networks on different interfaces of the firewall.

As soon as data traffic is blocked, entries of the "Connection Blocked" category should appear in the alert log.

On the right-hand side of each of these entries, the user can use the action menu to **Create a new rule**. A new dialog is then displayed where you can define a rule (with fewer options than the Connection dialog).


Range / input field	Description
Log information	Information about the selected entry is listed here. Example: Data should be sent from a host (192.168.3.3) on the internal network via the interface "eth3" using "ICMP" and sent to the destination 192.168.5.5.
Service	In the "Service" section, the user can decide whether to use a predefined or custom service or to create a new custom service. The only services to be displayed relate to the port and protocol corresponding to the blocked access. This example is ICMP with (port 0/No port) and the ICMP protocol. The newly created service takes on the same port and protocol settings. A user-defined name can be entered.
Source, Action and Destination	<p>Any missing data for creating the desktop connection must be entered in the lower area. Here, too, you decide whether the source and destination are existing desktop objects, or whether new desktop objects should be created. It is also possible to connect a new object to an existing one.</p> <p>The available desktop objects include all Internet objects and desktop objects with a matching IP address and interface. This can also apply to VPN desktop objects. Any available desktop object that is selected by default is the one that most closely matches the interface and the IP address. In our example, a host object with 192.168.3.3 and eth3 takes priority over a network object with 192.168.3.0/24. If there is no suitable desktop object for selection, an Internet object is used instead.</p> <p>If you want to create a new desktop object, you are limited to one host or network object to make creating a rule quick and easy. The interface and the IP address are preselected according to the blocked entry. All you have to enter is a name. For the interface you can, if necessary, choose from any of the available interfaces without restriction. The address must either match the blocked access attempt or at least be from a network that contains its IP address, e.g. 192.168.3.0/24, 192.168.0.0/16. Depending on the selected address, a host or a network object is created.</p> <p>After selecting the source and destination you can still, if necessary, change the type of access or the NAT by clicking on the corresponding icons, similar to the rules for a desktop connection. Typically, the access should be source-to-destination or two-way. As NAT is usually used to access an Internet address, NAT is always preselected in the direction of the Internet object. If no Internet object is selected, NAT is deactivated by default.</p>

After the rule is created, you can use the Log dialog to create further rules or you can close the dialog. If you have created new rules, you will be asked to activate the rules after closing the Log dialog.



12 VPN-SSL bridging

From LCOS FX version 10.5 it is possible to use the bridging mode with VPN SSL. The VPN SSL settings dialog under **VPN > VPN SSL > VPN SSL Settings** now has an extra tab for Bridging.

On the **Bridging** tab you specify the settings for the VPN SSL server connection:

Input box	Description
Protocol	Select the protocol with the appropriate radio button.
Port	Specify the number of the VPN SSL listening port to be used for bridging.  The same port number must be specified at the remote end of the connection.
Encryption algorithm	Use the drop-down list to select the encryption algorithm to use for bridging over VPN SSL.
Key renegotiation	To increase security, a VPN SSL connection renegotiates the session key while the connection is in progress. Enter the interval for key renegotiation in seconds.
Compression	Optional: Uncheck this box to disable LZO (Lempel-Ziv-Oberhumer, an algorithm for lossless data compression). This checkbox is enabled by default.

Under **VPN > VPN SSL > VPN SSL Connections** you can add a VPN SSL connection or edit an existing connection. In the settings under **VPN SSL Connections** the following elements have been added for bridging:

Input box	Description
Connection type	Select the connection type and the function of the LANCOM R&S [®] Unified Firewall by selecting the appropriate radio button. From LCOS FX version 10.5 you can also choose from the following types: <ul style="list-style-type: none"> > Bridge (Server) – A bridge server connection is established.  You can create several bridge server connections; however, all connections must use the same bridge so that, for example, several locations can be combined into one network. No other settings are required. > Bridge (Client) – A bridge client connection is established.  As soon as a connection has been established, an automatically generated TAP interface appears in the port list for the bridge. This TAP interface cannot be removed from the bridge, but it can be used in desktop connections like any other interface in order to help to define rules.


The items displayed in the settings depend on the connection type selected:

You can configure the following items for bridge-server connections:

Input box	Description
Bridge	Select a bridge from the preconfigured bridges.

You can configure the following items for bridge-client connections:

Input box	Description
Bridge	Select a bridge from the preconfigured bridges.
Remote Addresses	Enter the IP address where the remote end of the connection can be reached.

Input box	Description
	<p>Click on Add to add an IP address to the list. If you add more than one network, an automatic failover will be triggered if the first network becomes unreachable. In this case, your LANCOM RGS[®] Unified Firewall will try to reach the other networks in the list one by one until a network is found.</p> <p>You can edit or delete any entry in the list by clicking on the appropriate icon.</p> <hr/> <p> When you edit an entry, a checkmark will appear to the right of the entry. Click the checkmark to accept the change.</p>
Remote Port	Enter the port number used at the remote end of this connection.
Try establishing connection for	Specify the timeout in minutes after which no further connection attempts will be made. If this option is set to 0, the connection attempts will continue without interruption.

13 User Authentication

As of LCOS FX version 10.5 RU1, an externally accessible portal was added to the user authentication. This is able to provide VPN profiles for the LANCOM Advanced VPN Client. For this purpose, user authentication has been moved one level higher in the menu and the previous settings have been relocated to **User Authentication > LDAP/AD** and **User Authentication > Internal Portal**. In addition to the new menu item **User Authentication > External Portal**, another new addition is the option to start a user's device by means of a Wake-on-LAN packet when the user logs in.

In the settings for **User Authentication** you set the list of users who are authorized to use your network resources (e.g. Internet access, content-filter override and VPN tunnels). You can use these settings to configure local users and connect your LANCOM R&S® Unified Firewall to an external directory service for accessing information about individual users and user groups. This allows you to create firewall rules not only for computers, but also for individual users. You can also provide VPN profiles for individual users of the LANCOM Advanced VPN Client.

Navigate to **User Authentication** to display the list of users available on the system in the object bar.

The following sections contain information about user authentication.

13.1 Technical background and preparations

The purpose of user authentication

User authentication can be used to assign firewall rules to users when they log in. Only one user can be logged in per IP address. If a user logs in from an IP address that is already being used for a session, the previously logged in user is logged out and the new user is logged in.

Logging in to the firewall

The LANCOM R&S® Unified Firewall operates a separate web server for the exclusive purpose of user logins. This receives the user name and password. A local user database created on your LANCOM R&S® Unified Firewall is used by an authentication service to verify the user name and password. If this login fails and a Microsoft Active Directory server or an OpenLDAP server are configured in the LANCOM R&S® Unified Firewall, the authentication service additionally contacts these directory servers via the Kerberos protocol and tries to authenticate the user. If authentication succeeds, the firewall rules for this user are assigned to the IP addresses where the request was sent from.

Users registered in the local database of your LANCOM R&S® Unified Firewall can change their passwords via the web server. The password can consist of up to 248 characters. Longer passwords can be accepted but are truncated automatically.

Some computers can be excluded from user authentication, for example terminal servers used by many users concurrently or servers that only administrators can login to. In these cases, the web server and authentication service do not accept user logins from the IP addresses of these computers.

Since all users of a terminal server have the same IP address, your LANCOM R&S® Unified Firewall cannot identify the individual users on the network. To get around this problem, Microsoft offers Remote Desktop IP virtualization for Server 2008 R2 and newer versions. With this application, each user gets their own IP address from a pool of IP addresses, similar to DHCP.

Authentication server

Your LANCOM R&S® Unified Firewall provides the option of local user administration, which is ideal for smaller organizations that do not use central user administration. The local user database can be used at any time. However,

you can also use an external directory service such as the Microsoft Active Directory server or an OpenLDAP server. Both Microsoft Active Directory and OpenLDAP use the Kerberos protocol to verify login information provided by user authentication clients.

Active Directory groups

If you use a Microsoft Active Directory server for authentication, the Active Directory groups are also listed in the object bar under User Authentication. Active Directory groups are an effective way to set up and maintain security settings for individual users. For example, you can add Active Directory users to specific Active Directory groups and use your LANCOM R&S® Unified Firewall to set firewall rules for specific groups.

13.2 Logging in

There are three different ways to login to the LANCOM R&S® Unified Firewalls:

- > [Login via web browser](#)
- > [Login via the LANCOM R&S® Unified Firewall User Authentication Client](#)
- > [Login via the LANCOM R&S® Unified Firewall Single Sign-On Client](#)

Login via web browser

If users have been set up as desktop objects and firewall rules have been configured for them, using the landing page will enable them to act in compliance with the rules. Logging in is possible with any browser and is SSL encrypted.

Follow these steps to login to your LANCOM R&S® Unified Firewall by web browser:

1. Start a web browser.
2. Check that cookies are enabled.
3. Enter the IP address of your LANCOM R&S® Unified Firewall, e.g. `https://192.168.12.1` (default port 443) into the address bar.

A web site with the LANCOM R&S® Unified Firewall landing page is displayed.

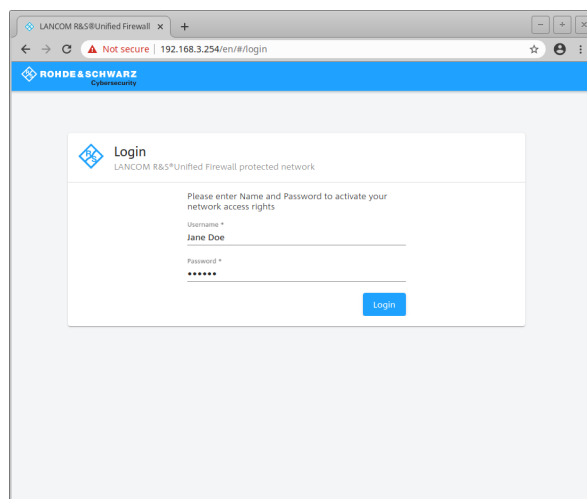


Figure 11: User authentication via web browser

4. Enter your username into the field **Name**.

-
- ❗ If the user is an LDAP user, the login name of the user must exactly match the name in the user's sAMAccountName attribute. Otherwise, the name in the user-specific firewall rules will not match the name of the user logging in to the client, and the rules will not match.

5. Enter the **Password**.

6. Click on **Login**.

Authentication is performed.

-
- ⚡ For security reasons, the browser window used to log in must remain open throughout the session. Otherwise, the user is automatically logged out after one minute. This prevents unauthorized persons from gaining access to the firewall if a user forgets to log out.

Login via the LANCOM R&S[®] Unified Firewall User Authentication Client

The Windows-based LANCOM R&S[®] Unified Firewall User Authentication Client is located in the directory `UA_Client` on the USB flash drive.

Follow these steps to use the LANCOM R&S[®] Unified Firewall User Authentication Client to login to your LANCOM R&S[®] Unified Firewall:

1. Install the LANCOM R&S[®] Unified Firewall User Authentication Client.
2. Start the LANCOM R&S[®] Unified Firewall User Authentication Client.



Figure 12: LANCOM R&S[®] Unified Firewall User Authentication Client

3. Under **Server Address**, enter the IP address of your LANCOM R&S[®] Unified Firewall.
4. Enter your username into the field **User Name**.

-
- ❗ If the user is an LDAP user, the login name of the user must exactly match the name in the user's sAMAccountName attribute. Otherwise, the name in the user-specific firewall rules will not match the name of the user logging in to the client, and the rules will not match.

5. Enter the **Password**.

6. Optional: Check the **Remember password** box to save the password for future logins.

7. Optional: Adjust the time window for the new connection under **Settings** by right-clicking on the icon in the notification area of the Windows task bar.

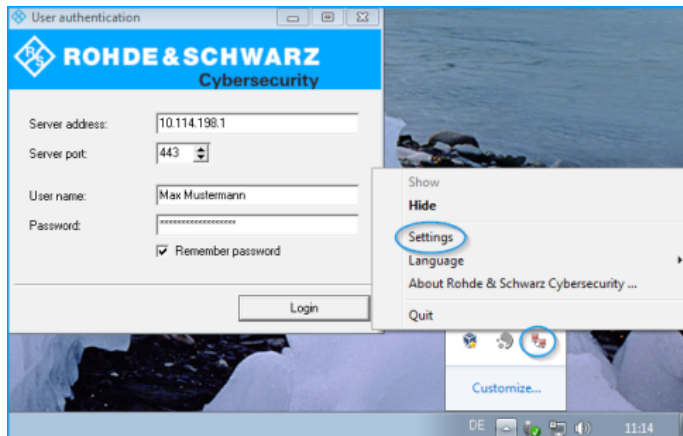


Figure 13: LANCOM R&S® Unified Firewall User Authentication Client settings

8. Click on **Login**.

Authentication is performed.



For security reasons we recommend that the LANCOM R&S® Unified Firewall User Authentication Client should always be updated to the latest available version. However, there is a compatibility mode that allows older versions of the LANCOM R&S® Unified Firewall User Authentication Client to work with LCOS FX of version 10 and higher. Please refer to [Settings](#) on page 34 for further information.

Login via the LANCOM R&S® Unified Firewall Single Sign-On Client

When using single sign-on (SSO), Active Directory domain users login to a Windows client. The rules configured on your LANCOM R&S® Unified Firewall that are relevant to these users are then applied automatically.

The following requirements must be met to operate SSO with a LANCOM R&S® Unified Firewall in an Active Directory environment:

1. Since Kerberos is time-based, make sure that for all SSO components (domain controller, Windows client and LANCOM R&S® Unified Firewall) are all set with the same time and the same NTP server.
2. Create the user `gpLogin`

In the user administration of Active Directory, a normal domain user needs to be created under "CN=Users". This user is then assigned a Service Principal Name (SPN), which is necessary to authenticate your LANCOM R&S® Unified Firewall at the server. The user does not need any special rights.

- a. Open the domain controller.

Figure 14: Create a user

- b. Under **First name** enter `gpLogin`.

This name makes it easier to find the user in the user overview later.

- c. Under **User logon name** enter `gpLogin/<firewall name>`.

In the example above, the host name (`<firewall name>`) is that of your LANCOM R&S® Unified Firewall `rsuf`, hence the logon name of the user is `gpLogin/rsuf`.

- d. Under **User logon name (pre-Windows 2000)** enter `gpLogin`.

- e. Click on **Next**.

- f. Enter a password for the user and confirm this.

Figure 15: Enter a user password

- g. Check the **Password never expires** box.
- h. Click on **Next**.
- i. To check the details of the new user, click **Finish**.

This creates the user `gpLogin`.

3. Login with the user `gpLogin` to query the Active Directory.

In the input box **User Name** under **Authentication Server**, enter `gpLogin`.

4. Configure the Service Principal Name (SPN).

Assign an SPN to the newly created user so that your LANCOM R&S® Unified Firewall recognizes the domain controller as trustworthy. To do this, execute the following command on the domain controller: `setspn -A gpLogin/rsuf gpLogin`

5. Generate a Kerberos key

With the help of the LANCOM R&S® Unified Firewall Single Sign-On Client, a user login to the Windows domain can be redirected to your LANCOM R&S® Unified Firewall. Your LANCOM R&S® Unified Firewall uses the Kerberos key to check the forwarded information and activate the user-specific firewall rules. Proceed as follows to generate a Kerberos key:

- a. Login to your LANCOM R&S® Unified Firewall.
- b. Navigate to **User Authentication > LDAP/AP**.
- c. On the **Kerberos** tab, click the **Create Kerberos Key** button to generate the Kerberos key.

The Active Directory is queried to validate the specified AD user and to obtain relevant information such as the version number of the Kerberos key. Your LANCOM R&S® Unified Firewall can use this information to generate a valid Kerberos key locally.

6. Enable SSO on your LANCOM R&S® Unified Firewall

Proceed as follows to enable SSO on your LANCOM R&S® Unified Firewall:

- a. Set a checkmark in the **Active** check box on the **Kerberos** tab.
- b. Click **Save** to store your settings.

7. Prepare the Windows client.

The ZIP archive with the Windows Installer for the Single Sign-On Client can be found at:

<https://www.lancom-systems.de/downloads/>

There are three ways to install the LANCOM R&S® Unified Firewall Single Sign-On Client:

- > Copy the standalone application `UAClientSSO.exe` to the desired location.
- > Run the setup program `UAClientSSOSetup.exe` and install the standalone application `UAClientSSO.exe` to the following path:
`C:\Program Files\R&S Cybersecurity\UA Client\3.0\`
- > Install the client via the domain using the Microsoft installer `UAClientSSO.msi` in a group policy object (GPO).



All of these methods install the independent application `UAClientSSO.exe` on the Windows PC. It can then be executed by specifying the following parameters:

- > Hostname of the LANCOM R&S® Unified Firewall (for further information see [Settings](#) on page 34).
- > IP address of the LANCOM R&S® Unified Firewall in the network of the client computer.

Example: Your LANCOM R&S® Unified Firewall has the hostname "rsuf". The IP address of the client computer on the network is 192.168.0.1. The target path for installing the LANCOM R&S® Unified Firewall Single Sign-On Client is therefore:



```
C:\Program Files\R&S Cybersecurity\UA Client\3.0\UAClientSSO.exe rsuf 192.168.0.1.
```

13.3 LDAP/AD

Here you can specify the connection parameters for the directory server used to manage the LDAP users on your network.



The tab **Authentication Server** allows you to specify which database type you want to use. You can use the local user database in the LANCOM R&S® Unified Firewall either independently or in combination with an external user database such as Microsoft Active Directory Server or the OpenLDAP server with Kerberos.

If you select `Microsoft Active Directory Server` you can configure the following items:

Input box	Description
Host	Enter the host name or the IP address of the directory server.  If you enter the host name of the directory server, you must configure the DNS settings. Otherwise, the name cannot be resolved.
Port	Enter the port number of the directory server to be used for communication. You can also select the port number with the up/down arrow.
User Name	Enter the name of a read-only user to retrieve the list of domain users from Active Directory. This input field must match the user attribute <code>sAMAccountName</code> . The user must be listed in "CN=Users". Please refer to Login via the LANCOM R&S® Unified Firewall Single Sign-On Client on page 28 for further information.
Password	Enter the password of the read-only user.  We recommend that you create a dedicated user for this purpose.
Domain Name	Enter the domain name of the Active Directory.
StartTLS	You can use the StartTLS protocol to secure the connection to the OpenLDAP or Microsoft Active Directory server. In this case, you also enter the Server CA to be used.

To check the settings configured for Microsoft Active Directory Server, click **Test AD Settings**.

If you select `OpenLDAP Server` you can configure the following items:

Input box	Description
Server Address	Enter the host name or the IP address of the directory server.  If you enter the host name of the directory server, you must configure the DNS settings. Otherwise, the name cannot be resolved.
Port	Enter the port number of the directory server to be used for communication. You can also select the port number with the up/down arrow.
User DN	Enter the user domain name of a read-only account.  You do not have to enter the complete user domain name. If you click Save , the system automatically adds the domain components from the Base DN entry.
Password	Enter the password of the read-only user.
Base DN	Enter a unique name (Base-DN) together with Relative Distinguished Names (RDN) separated by commas. For example, three domain components: <code>dc=ldap,dc=example,dc=com</code> specify the location in the directory where you want to start the directory search.
User Query	Optional: Specify the filter to be used to retrieve the list of users.

Input box	Description
User ID	Optional: Set the attributes from which the user identifier is retrieved. The user name displayed in the web client is derived from this LDAP-user attribute. By default, the user identifier is taken from the attribute <code>sAMAccountName</code> .
User name	Optional: Set the attribute from which the user name is retrieved.
User group	Optional: Set the attribute from which the user group is retrieved.
User Primary Group	Optional: Set the attribute from which the user primary group is retrieved.
Mail Query	Optional: Specify the filter to be used to retrieve the e-mail list.
Mail Name	Optional: Set the attribute from which the e-mail name is retrieved.
Group Query	Optional: Specify the filter to be used to retrieve the list of groups.
Group Name	Optional: Set the attribute from which the e-mail name is retrieved.
Group ID	Optional: Set the attribute from which the group ID is retrieved.
Group Primary ID	Optional: Set the attribute from which the group primary ID is retrieved.
Group Parent	Optional: Set the attribute from which the parent group is retrieved.
StartTLS	You can use the StartTLS protocol to secure the connection to the OpenLDAP or Microsoft Active Directory server. In this case, you also enter the Server CA to be used.

If you click **Save**, the system adds default values to any optional fields which you have not filled.

If you want to operate single-sign-on with Kerberos, the username must be `gpLogin`. The host name and domain of your firewall is taken from the general settings. Please refer to [Logging in](#) on page 26 for further information.

On tab **Kerberos**:


Input box	Description
Active	Select this checkbox to enable the Kerberos service.
Kerberos Key	Displays the service name, host name, and domain name for the userPrincipalName of the most recently created Kerberos key, also called a keytab. Please refer to Logging in on page 26 for further information.

13.4 External portal

With the external user portal, the administrator can allow individual or multiple users to have limited access to the firewall. This gives them the option to directly receive provided files or information. These may include the IPsec configuration required for the LANCOM Advanced VPN Client to establish a VPN connection to your LANCOM R&S® Unified Firewall.

The following steps are necessary for this:

- > Create a certificate for access via HTTPS.

 For the external portal, a certificate from a trustworthy certification authority is recommended!

- > Create local users or configure access to a directory server (OpenLDAP or Microsoft Active Directory).
- > Create an IPsec client-to-site connection.
- > Configure the external portal under **User Authentication > External Portal > Settings**.
- > Create a new profile under **User authentication > External portal > VPN profiles** and assign the VPN connection to the users.

The users can then log in to the firewall using the configured address.

13.4.1 Settings

The **User Authentication Settings** for the external portal allow you to activate or deactivate user authentication for external users.

The external portal uses the reverse proxy system to provide web access, and the settings are analogous to the settings for a reverse-proxy front end, with the following differences:

- > SSL is always activated
- > No "Outlook Anywhere", proxy paths or blocked paths
- > A separate reverse-proxy back end is created for the external portal in the back end, but it is not included in the list of back ends.
- > Also, the settings for the external portal do not appear in the list of front ends, but they are treated like a front end when validating settings.

Navigate to **User Authentication > External Portal > Settings** to open an editing window where you can create the general settings for the user authentication.

In the **External Portal** editing window you can modify the following parameters:

Input box	Description
I/O	A slider button indicates whether the external portal is enabled (I) or disabled (O). You can change the status of the user authentication by clicking the slider button. User authentication is disabled by default.
Domain or IP address	Enter the name of the domain or the IP address assigned to the external portal.
Connection	Select a connection. You can choose both a network connection and a PPP connection.
Port	Configure the externally accessible listen port for the external portal.
SSL certificate	Select a certificate with a private key.

13.4.2 VPN profiles

The purpose of the VPN profiles is to create and provide the VPN configuration files for the configured users. The VPN configuration files are similar to the zip files that users receive when they create an IPsec connection using the export button, except that these configuration files are not password-protected.

In the **VPN Profiles** editing window you can adjust the following parameters:

Input box	Description
Name	Give the template a descriptive name.
IPsec connection	This item selects the IPsec connection that is to be provided to the user as a configuration file in the external portal.
Gateway	The LANCOM Advanced VPN Client connects to this address.
Remote certificate	Certificate of the remote site.
Key password	Enter the password used to decrypt the private key of the client certificate.
Transport password	Enter the password used to decrypt the p12 transport container.
Users	Specify the users to whom this profile should apply. Assigning several users to a single IPsec connection only functions properly in combination with XAuth or EAP. In the portal, users only see the profiles assigned to them.

13.5 Internal portal

The internal user portal enables firewall rules to be assigned to users when they log in. It is also used to provide and manage content-filter codes to allow exemptions/overrides.


Only one user can be logged in per IP address. If a user logs in from an IP address that is already being used for a session, the previously logged in user is logged out and the new user is logged in.


13.5.1 Settings

The **User Authentication Settings** for the internal portal allow you to activate or deactivate user authentication for internal users.

Navigate to **User Authentication > Internal Portal > Settings** to open an editing window where you can create the general settings for the user authentication.

In the **Internal Portal** editing window you can modify the following parameters:

Input box	Description
I/O	A slider button indicates whether the user authentication is enabled (I) or disabled (O). You can change the status of the user authentication by clicking the slider button. User authentication is disabled by default.
Log Logins	Activate this checkbox if you want to log every authentication on the LANCOM R&S® Unified Firewall. You can view the login events under Monitoring & Statistics > Logs > System Log .
Login Mode	Choose one of the following four options: <ul style="list-style-type: none"> > Single Login (deny new login) – No user can login from more than one IP address at a time. > Single Login (disconnect old login) – All previous logins are logged off when the user logs in from a different IP address. > Multiple Logins – Users can login from up to 254 different IP addresses simultaneously. > Multiple Logins (with warning in report) – Users can log in from up to 254 different IP addresses simultaneously, and alerts are displayed in the report.
Web Login Port	Specify the HTTPS port for the web login by navigating up/down using the arrow key or by entering the port number. The default is port 443.
Compatibility Mode	Enable this checkbox if you want to log in to the LANCOM R&S® Unified Firewall with user authentication clients older than version 3.0.0.  Enabling this checkbox puts your network security at risk. Please refer to User Authentication on page 25 for further information.
Show Landing Page	Optional: Enable this checkbox to display a landing page when an unauthorized user attempts to access the Internet.

 Each individual IP address supports just one user login, even if the mode **Multiple Logins** is activated.

13.5.2 Wake-on-LAN

Start devices as soon as a user logs on to the internal portal in order to activate firewall rules.

In the **Wake on LAN** editing window you can modify the following parameters:

Input box	Description
User	Select a user in the left pane.
MAC address	Enter one or more MAC addresses in the right pane. As soon as the user logs in to the internal portal to activate firewall rules, wake-on-LAN packets are sent to this MAC address to start the corresponding device.

Click **Export** to export your user MAC addresses to the file system. Click **Import** to import user MAC addresses.

13.6 Users

Like computers, users and LDAP groups can be set up on the desktop as individual users or user groups.

You can then define rules for these desktop objects that are assigned to the users as soon as they log in. When a user logs in from a computer that certain rules are assigned to, the user is assigned the rules for this computer as well as their own user-specific rules. You can select users and LDAP groups from the local user database of your LANCOM R&S® Unified Firewall and from the OpenLDAP or Active Directory authentication server and add them to the user groups on the desktop. There is also a special **Default User Group** that can be selected on the desktop. Users cannot be added to this user group. It includes all of those users who can login but have not yet been set up as individual users or as members of another user group on the desktop. If a default user group has been set up on the desktop and you have assigned rules to it, users who are subsequently created on the Active Directory server are automatically added to this default user group. After logging in, these new users are automatically assigned the default rules without any further administrative work.

13.7 LDAP users

It is possible to connect your LANCOM R&S® Unified Firewall to an external directory server and access users using the Lightweight Directory Access Protocol (LDAP). These users can then be integrated into user-specific firewall rules.

You can also use LDAP to access directory services and to manage user data.

Connect to a directory server as described under [LDAP/AD](#) on page 31.

Navigate to **User Authentication > LDAP Users** to display the list of LDAP users on the directory server in the object bar.

To make the LDAP users listed here available for connections and group-specific firewall rules, the groups must be assigned to a user desktop object.

13.8 LDAP groups

It is possible to connect your LANCOM R&S® Unified Firewall to an external directory server and access user groups using the Lightweight Directory Access Protocol (LDAP). You can integrate these user groups into group-specific firewall rules.

You can also use LDAP to access directory services and to manage user data.

Connect to a directory server as described under [LDAP/AD](#) on page 31.

Navigate to **User Authentication > LDAP Groups** to display the list of LDAP groups on the directory server in the object bar.

To make the LDAP groups listed here available for connections and group-specific firewall rules, the groups must be assigned to a user-group desktop object.

13.9 Local users


Your LANCOM R&S® Unified Firewall offers local user administration for smaller installations without central administration. Use the settings under **Local User** to enter usernames and passwords. In this way you can define and manage users.

Navigate to **User Authentication > Local Users** to display the list of local users available on the system in the object bar.

In the expanded view, the table columns show the **Name** of the local user and also a **Description**, if one has been entered. Use the buttons in the last column to view and modify the settings of a local user, create a new user based on a copy of the existing local user, or delete a user from the system.

Under **User Authentication > Local Users** you can add a new user or edit an existing local user.

In the **Local User Authentication** editing window you can modify the following parameters:

Input box	Description
User Name	Specify a unique name for the local user. This name is the login name.  The user's login name must match the User Name (case sensitive). Otherwise, the name in the user-specific firewall rules will not match the name of the user logging in to the client, and the rules will not match.
Description	Optional: The information provided here is for internal use by the administrator only.
Password	Enter a password for the user and confirm this. The password must contain at least six characters.
Show Password	Optional: Set a check mark in the check box to verify the password.
Require password change after next login	Optional: If you check this box, the user will have to change their password after the next login. The web server will redirect the user from the login page to a page where the password can be changed.

The buttons available at the bottom right of the edit box depend on whether you are adding a new local user or editing an existing one. For a newly configured local user, click **Create** to add the new user to the list of local users, or **Cancel** to discard the entry.

If you have made changes, you can use the buttons at the bottom right of the edit window to save them (**Save**) or discard them (**Reset**). Otherwise you can close the window (**Close**).

The local users defined here are available for use in desktop objects such as the VPN users.

13.10 Unassigned users

Navigate to **User Authentication > Unassigned Users** to display LDAP users who are assigned to user objects on the desktop but can no longer be accessed on the directory service.

13.11 Example applications

In a Windows domain

If you operate a Windows domain, you can perform user authentication by means of the Windows domain controller. Proceed as follows to enable user authentication by the Windows domain controller:

1. Navigate to **User Authentication > Settings**.
2. Click on **Authentication Server**.
3. Enter the data for your domain controller.

All users in the specified domain are displayed in the user list.

4. Drag the user icons onto the configuration desktop and assign rules to them.

To log in, users enter the URL including `https://` and the IP address of the firewall into the address bar of their browser. A login page is displayed. After a successful login, the firewall rules of the user are assigned to the specified IP addresses. When the browser window is closed, the session cookie expires and the rules are no longer valid.

Excluding the terminal server from user authentication

If you use a terminal server, you should exclude it from user authentication. Otherwise, all current users will be logged out when a new user logs in.

Proceed as follows to exclude the terminal server from user authentication.

1. Click the host group icon on the toolbar at the top of the desktop.
2. Uncheck the box in the **Login Allowed** column.

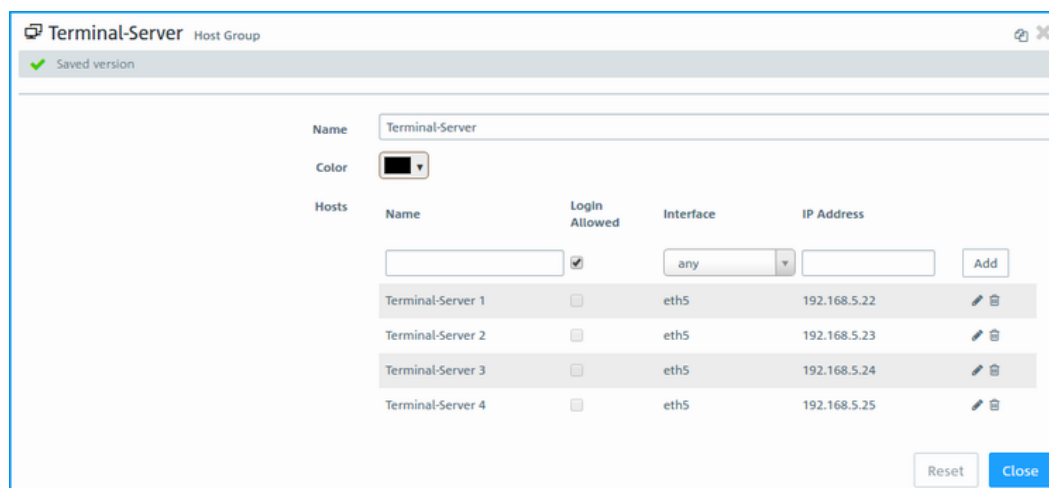


Figure 16: Object settings – terminal server



If your users require authentication in the terminal server, you can activate Remote Desktop IP Virtualization in the terminal server. This assigns a unique IP address to each user during a session.