Administration Guide for Labris MNG

Administration Guide for Labris Centralized Management
Version 3.4.2

http://labrisnetworks.com/support-training/
Tel: +90 850 455 4555

Copyright

Disclaimer

Neither the author nor the publisher makes any representation or warranty of any kind with regard to the information contained in the book. No liability shall be accepted for any actions caused, or alleged to have been caused, directly or indirectly from using the information contained in this book.

Table of Contents

About Labris Networks Inc.

Since 2002, Labris Networks Inc. has been an R&D focused and rapidly-growing provider of network security solutions through its globally-proven products. Labris ensures ultimate network security through its extensive product line including Firewall/VPN, Web Security, E-Mail Security, Lawful Interception and Availability Protection solutions on LABRIS UTM, Labris LOG and Harpp DDoS Mitigator appliances. Next-generation solutions are developed to detect, identify all kinds of real-time threats, applications providing a smart shield against intrusions, viruses, spam, malware and availability attacks.

Labris products protect networks of all sizes with a variety of topologies and deployment scenarios. Through Labris FLEX firmware options, the customers have privileges to get the security software they need as well as extra modules such as Wireless Guest Authentication, Detailed Internet Reporting, Lawful Interception and Logging. Having a customer-focused, future-oriented and flexible approach, Labris also offers its state-of-the-art security software as a Cloud Service.

Having operations in a rapidly growing global network of more than 20 countries, Labris products protect enterprises, brands, government entities, service providers and mission-critical infrastructures.

Labris with its worldwide partners is committed to the highest levels of customer satisfaction and loyalty, providing the best after-sales support by the multilingual Global Support Center. Being one of the Common Criteria EAL4+ certified security gateway brands in the world and rapidly growing global player, Labris provides its customers the top-level security with optimum cost. Labris, headquartered in Ankara, Turkey, has offices serving Europe, Middle East, North Africa, Caucasus and Southeast Asia.

About LABRIS UTM

Labris UTM is an Identity-based UTM Appliance. Labris UTM's solution is purpose-built to meet the security needs of corporates, government organizations, and educational institutions. Labris UTM's perfect blend of best-of-breed solutions includes Identity based Firewall, Content filtering, Anti Virus, Anti Spam, Intrusion Detection and Prevention (IDP), and VPN.

Labris UTM provides increased LAN security by providing separate port for connecting to the publicly accessible servers like Web server, Mail server, FTP server etc. hosted in DMZ which are visible to the external world and still have firewall protection. It also provides assistance in improving bandwidth management, increasing employee productivity and reducing legal liability associated with undesirable Internet content access.

Labris UTM is available for Small Enterprises , Medium Enterprises as well as Large Enterprises

Labris UTM Web Security provides further control to block inappropriate and illegal web sites as well as instant messaging and peer-to-peer applications while Labris UTM Application Intelligence and Control broadens control over inefficient web applications such as social media platforms (Facebook, twitter, etc.), online trading, IM/chat, peer-to-peer sharing and streaming video sites. Labris Email Security completes the offering with effective protection against spam and phishing attacks so employees only read legitimate emails and are not exposed to fake emails. Labris UTM's intelligent solutions simplify the centralized management of local and remote network services while protecting your precious information and communications resources with low TCO.

How to Purchase LABRIS UTM

To purchase LABRIS UTM, Visit - http://labrisnetworks.com/products/product/lbrlog-series

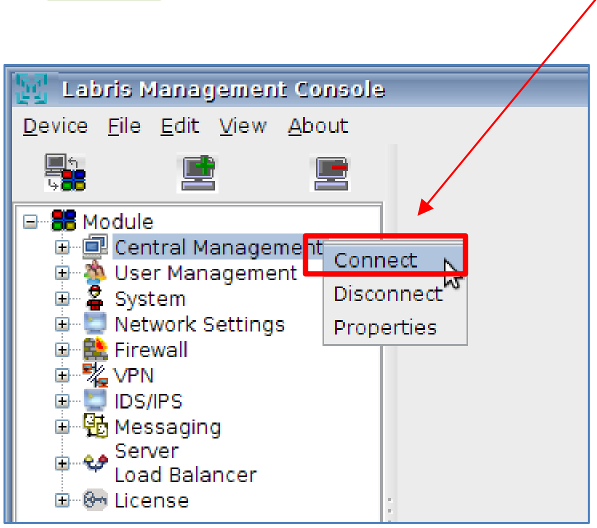
You can purchase through authorized distributors http://labrisnetworks.com/authorized-distributors/

Centralized Management

Central Management system provides administrators the ability to effectively manage remote Labris UTM devices. Administrators can monitor health status of remote Labris UTM devices and also manage these devices.

Note

- *You can also change your prefered language even after you login to the appliance as shown in following image*



Viewing Options in Central Management

When we Right click on “**Central Management Tab**” we find following options

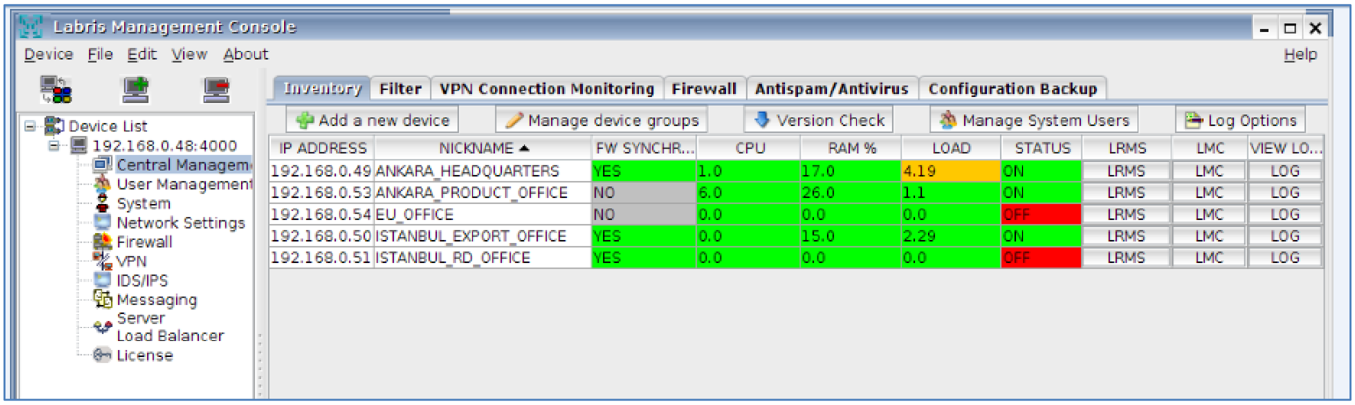
1 – Connect	Connects to Central Management module of Labris UTM
2 – Disconnect	Disconnects from Central Management module of Labris UTM
3 – Properties	Opens Central Management module properties window

Inventory

Inventory Tab in **Central Management** allows administrators to administer and monitor remote Labris UTM devices.

Inventory Table

Inventory table lists remote devices with their statuses. Administrators can edit, delete, enable/disable, restore these devices from inventory table. Also administrators can connect to LRMS dashboard and Labris Management Console of these remote Labris UTM devices' by clicking their LRMS and LMC buttons. Using inventory table administrators easily can view remote Labris UTM devices' logs by clicking LOG button.



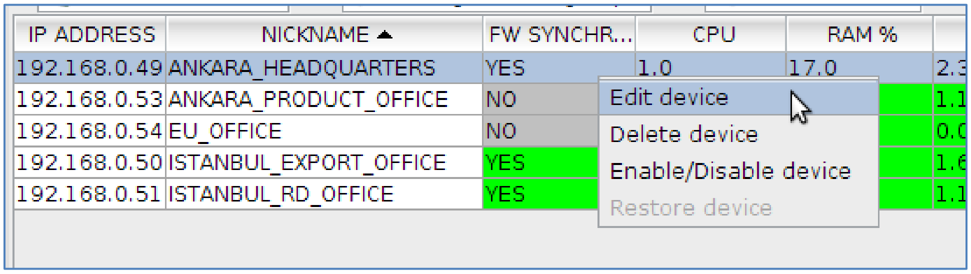
IP ADDRESS	NICKNAME ▲	FW SYNCHR...	CPU	RAM %	LOAD	STATUS	LRMS	LMC	VIEW LO...
192.168.0.49	ANKARA_HEADQUARTERS	YES	1.0	17.0	4.19	ON	LRMS	LMC	LOG
192.168.0.53	ANKARA_PRODUCT_OFFICE	NO	6.0	26.0	1.1	ON	LRMS	LMC	LOG
192.168.0.54	EU_OFFICE	NO	0.0	0.0	0.0	OFF	LRMS	LMC	LOG
192.168.0.50	ISTANBUL_EXPORT_OFFICE	YES	0.0	15.0	2.29	ON	LRMS	LMC	LOG
192.168.0.51	ISTANBUL_RD_OFFICE	YES	0.0	0.0	0.0	OFF	LRMS	LMC	LOG

Inventory table has 10 columns which are described below:

IP Address	Shows remote Labris UTM device's IP address
Nickname	Shows remote Labris UTM device's name
FW Syncronized	Shows whether firewall policy running on remote Labris UTM device is installed by Central Management system(YES) or firewall policy is installed locally by remote Labris UTM(NO).
CPU	Shows remote Labris UTM device's CPU usage
RAM	Shows remote Labris UTM device's RAM usage
LOAD	Shows remote Labris UTM device's load average
STATUS	Shows whether remote Labris UTM device is reachable
LRMS	By clicking this button administrators can connect to remote Labris UTM device's LRMS dashboard
LMC	By clicking this button administrators can connect to remote Labris UTM device's LMC
LOG	By clicking this button administrators can view remote Labris UTM device's logs

By clicking refresh button data on inventory table can be refreshed with the latest updates from remote Labris UTM devices.

Manage Device



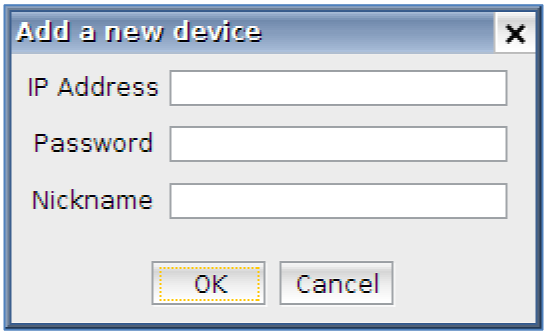
IP ADDRESS	NICKNAME ▲	FW SYNCHR...	CPU	RAM %	
192.168.0.49	ANKARA_HEADQUARTERS	YES	1.0	17.0	2.3
192.168.0.53	ANKARA_PRODUCT_OFFICE	NO			1.1
192.168.0.54	EU_OFFICE	NO			0.0
192.168.0.50	ISTANBUL_EXPORT_OFFICE	YES			1.6
192.168.0.51	ISTANBUL_RD_OFFICE	YES			1.1

By right clicking on an entry in inventory table administrators get a 4 row menu which is described below:

Edit device	Enables administrators to change remote Labris UTM device's connection IP and remote Labris UTM device's nickname
Delete device	Removes remote Labris UTM device from central management.
Enable/Disable device	Disables policy installations from Central Management to remote Labris UTM device
Restore device	Restores Central Management configurations on remote Labris UTM device

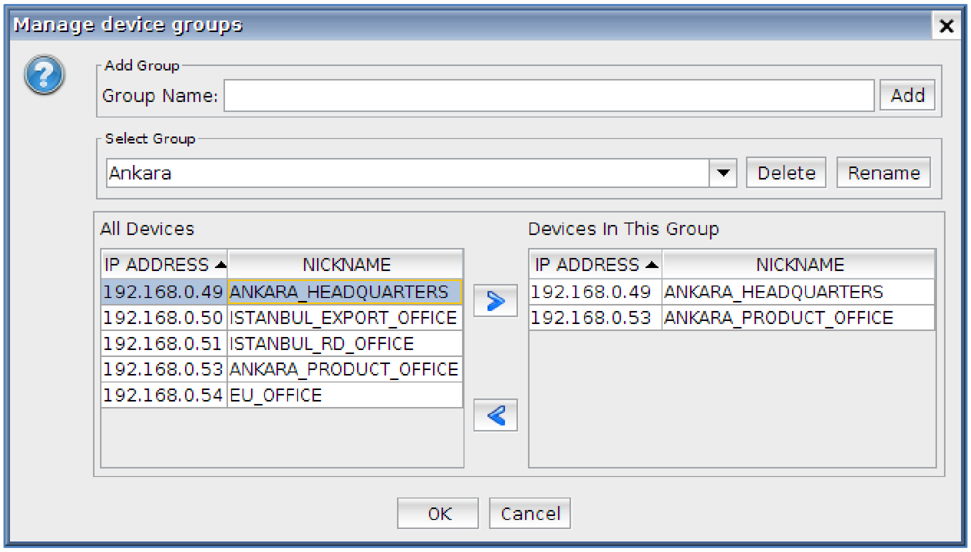
Adding a New Device

By clicking "Add a new device" button administrators can add a new remote Labris UTM device to central management system. After clicking "Add a new device" button opens a window. In "Add a new device" window administrators set IP Address, Password and Nickname of the remote device.



Manage Device Groups

By clicking "Manage device groups" button administrators can create, rename and delete remote device groups. Remote Labris UTM devices can be added and removed from device groups. These device groups can be used as policy installation destinations.



Manage device groups

Add Group

Group Name:

Select Group

Ankara

All Devices

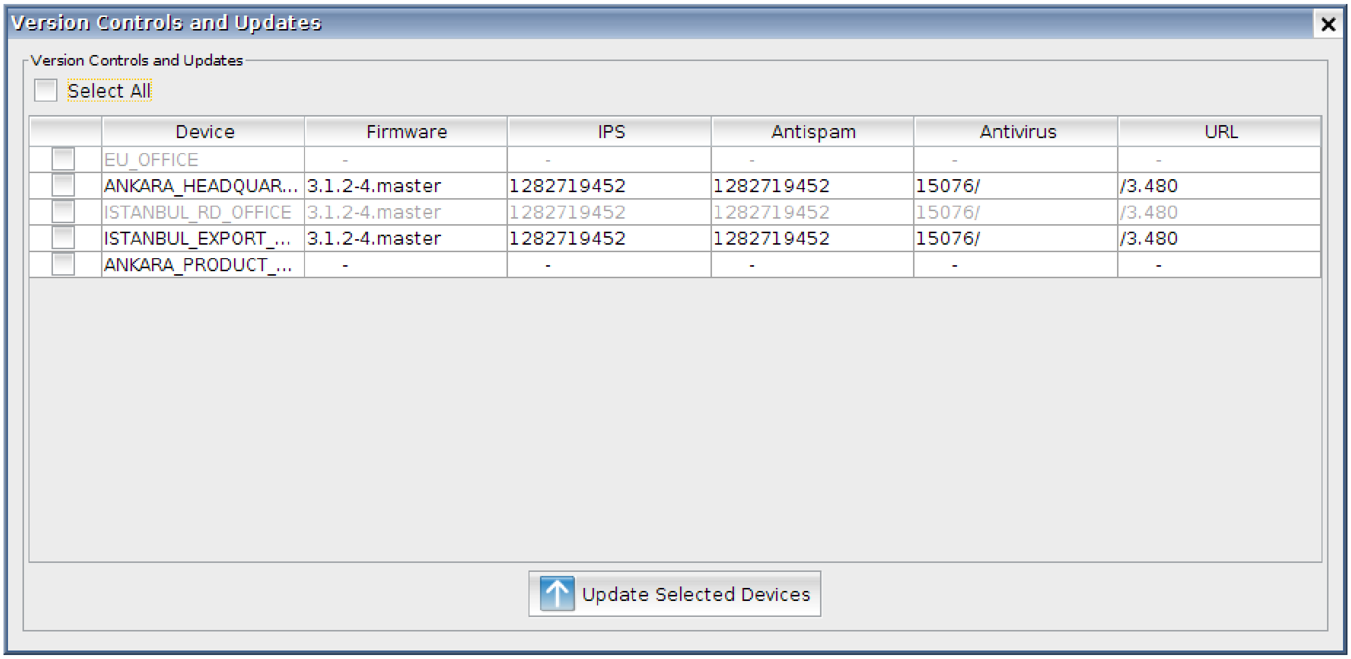
IP ADDRESS ▲	NICKNAME
192.168.0.49	ANKARA_HEADQUARTERS
192.168.0.50	ISTANBUL_EXPORT_OFFICE
192.168.0.51	ISTANBUL_RD_OFFICE
192.168.0.53	ANKARA_PRODUCT_OFFICE
192.168.0.54	EU_OFFICE

Devices In This Group

IP ADDRESS ▲	NICKNAME
192.168.0.49	ANKARA_HEADQUARTERS
192.168.0.53	ANKARA_PRODUCT_OFFICE

Version Controls and Updates

By clicking "Manage device groups" button administrators can check version information of remote Labris UTM devices. In addition to this administrators can update selected remote Labris UTM devices' IPS, antispam, antivirus and webfilter url databases by clicking "Update Selected Devices" button.



Version Controls and Updates

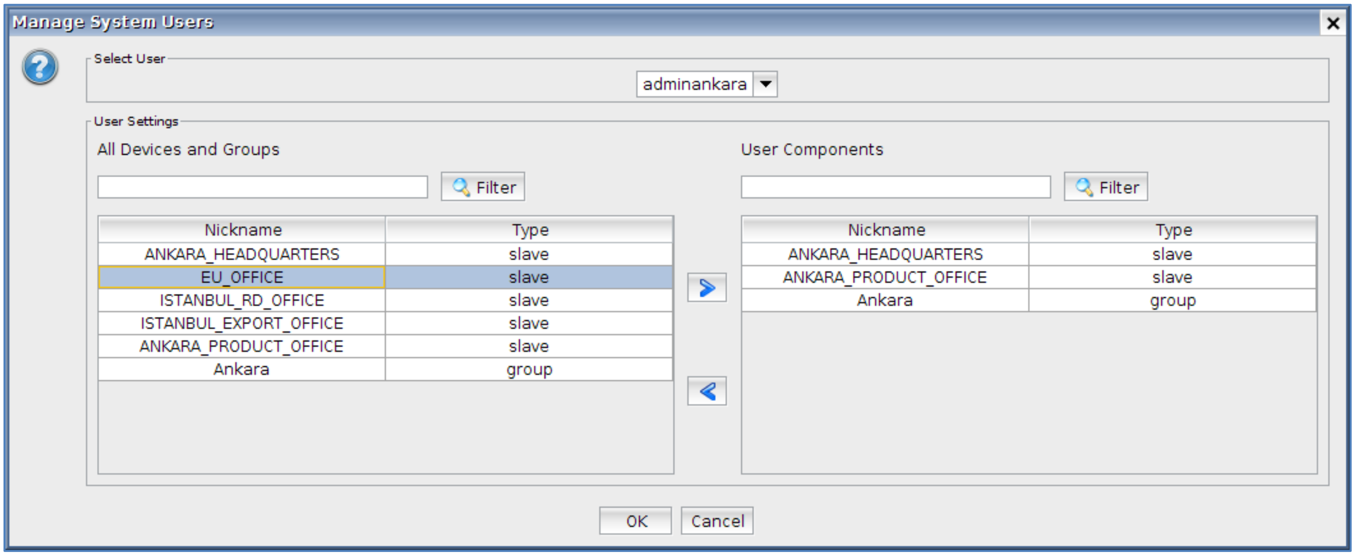
Version Controls and Updates

□ Select All

	Device	Firmware	IPS	Antispam	Antivirus	URL
□	EU_OFFICE	-	-	-	-	-
□	ANKARA_HEADQUAR...	3.1.2-4.master	1282719452	1282719452	15076/	/3.480
□	ISTANBUL_RD_OFFICE	3.1.2-4.master	1282719452	1282719452	15076/	/3.480
□	ISTANBUL_EXPORT_...	3.1.2-4.master	1282719452	1282719452	15076/	/3.480
□	ANKARA_PRODUCT_...	-	-	-	-	-

Manage System Users

By clicking "Manage System Users" button administrators can permit system users to manage selected remote Labris UTM devices.



Select User: adminankara

All Devices and Groups

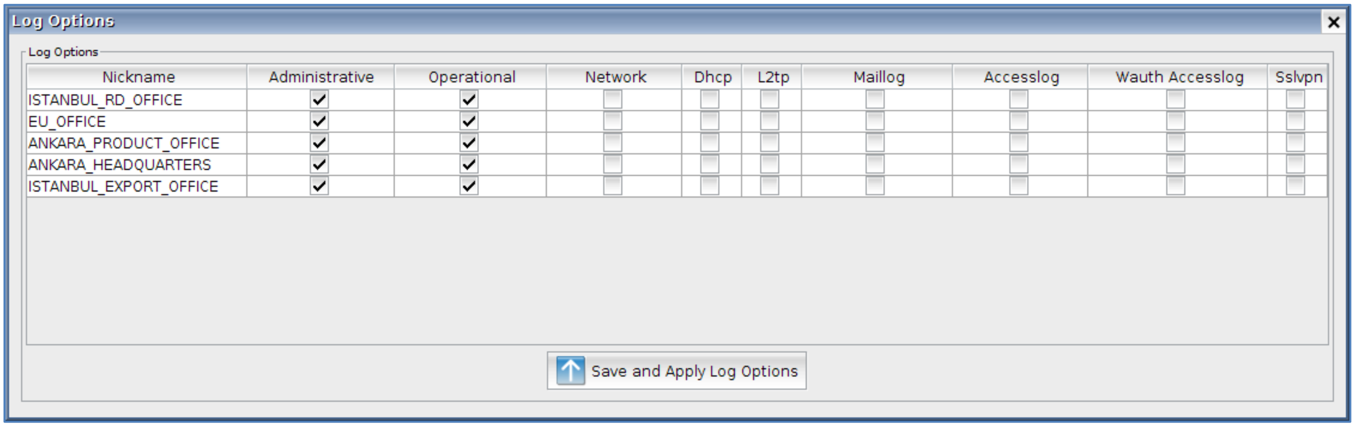
Nickname	Type
ANKARA_HEADQUARTERS	slave
EU_OFFICE	slave
ISTANBUL_RD_OFFICE	slave
ISTANBUL_EXPORT_OFFICE	slave
ANKARA_PRODUCT_OFFICE	slave
Ankara	group

User Components

Nickname	Type
ANKARA_HEADQUARTERS	slave
ANKARA_PRODUCT_OFFICE	slave
Ankara	group

Log Options

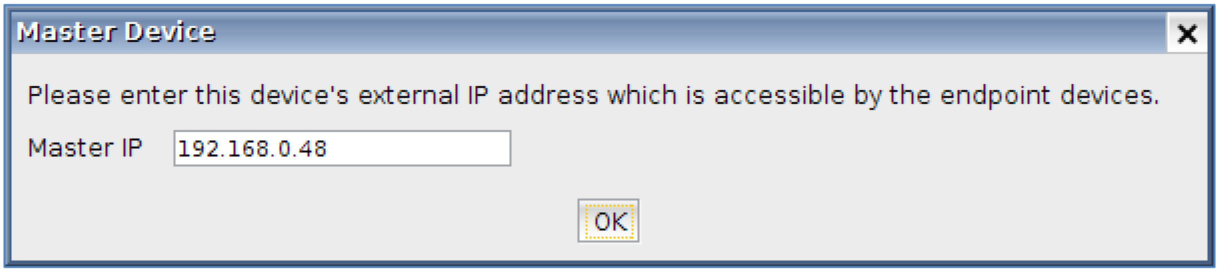
By clicking "Log Options" button administrators can select which logs to be received from remote Labris UTM devices. These logs can be viewed by clicking "LOG" button in inventory table.



Nickname	Administrative	Operational	Network	Dhcp	L2tp	Maillog	Accesslog	Wauth Accesslog	Sslvpn
ISTANBUL_RD_OFFICE	☑	☑	□	□	□	□	□	□	□
EU_OFFICE	☑	☑	□	□	□	□	□	□	□
ANKARA_PRODUCT_OFFICE	☑	☑	□	□	□	□	□	□	□
ANKARA_HEADQUARTERS	☑	☑	□	□	□	□	□	□	□
ISTANBUL_EXPORT_OFFICE	☑	☑	□	□	□	□	□	□	□

Edit Central Management IP Address

By clicking "Edit Central Management IP Address" button administrators can update Central Management device's IP address. This IP address is used when connecting to remote Labris UTM devices and when receiving data from remote Labris UTM devices. So this IP address must be routable from remote Labris UTM devices.



Master Device

Please enter this device's external IP address which is accessible by the endpoint devices.

Master IP: 192.168.0.48

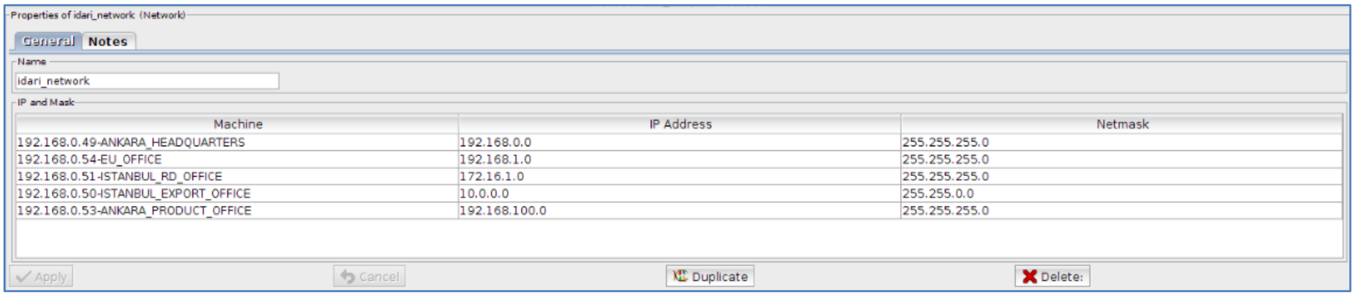
Firewall

Firewall tab in **Central Management** module allows administrators to manage firewall rules of remote Labris UTM devices.

Important Note: An initial firewall policy must be installed from the local LMC of remote Labris UTM devices. Only after installing an initial policy, firewall rules can be installed from Central Management.

The differences of the Firewall Module in Central Management from the standard UTM firewall modules are listed below:

1) Dynamic Network Objects in Objects Folder: When creating a dynamic network object, the object's value should be set for every remote Labris UTM devices. As seen in the picture below, when the firewall policy is installed on remote Labris UTM devices, the dynamic network objects will be seen and used as standard network objects with their respective values.



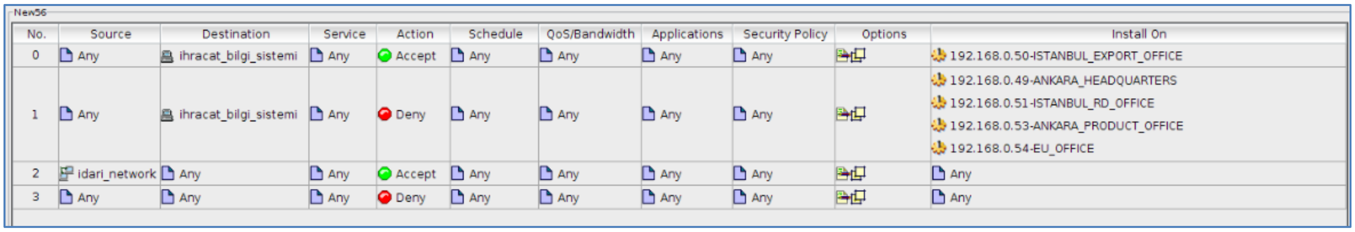
Properties of idari_network (Network)

Name: idari_network

IP and Mask

Machine	IP Address	Netmask
192.168.0.49-ANKARA_HEADQUARTERS	192.168.0.0	255.255.255.0
192.168.0.54-EU_OFFICE	192.168.1.0	255.255.255.0
192.168.0.51-ISTANBUL_RD_OFFICE	172.16.1.0	255.255.255.0
192.168.0.50-ISTANBUL_EXPORT_OFFICE	10.0.0.0	255.255.0.0
192.168.0.53-ANKARA_PRODUCT_OFFICE	192.168.100.0	255.255.255.0

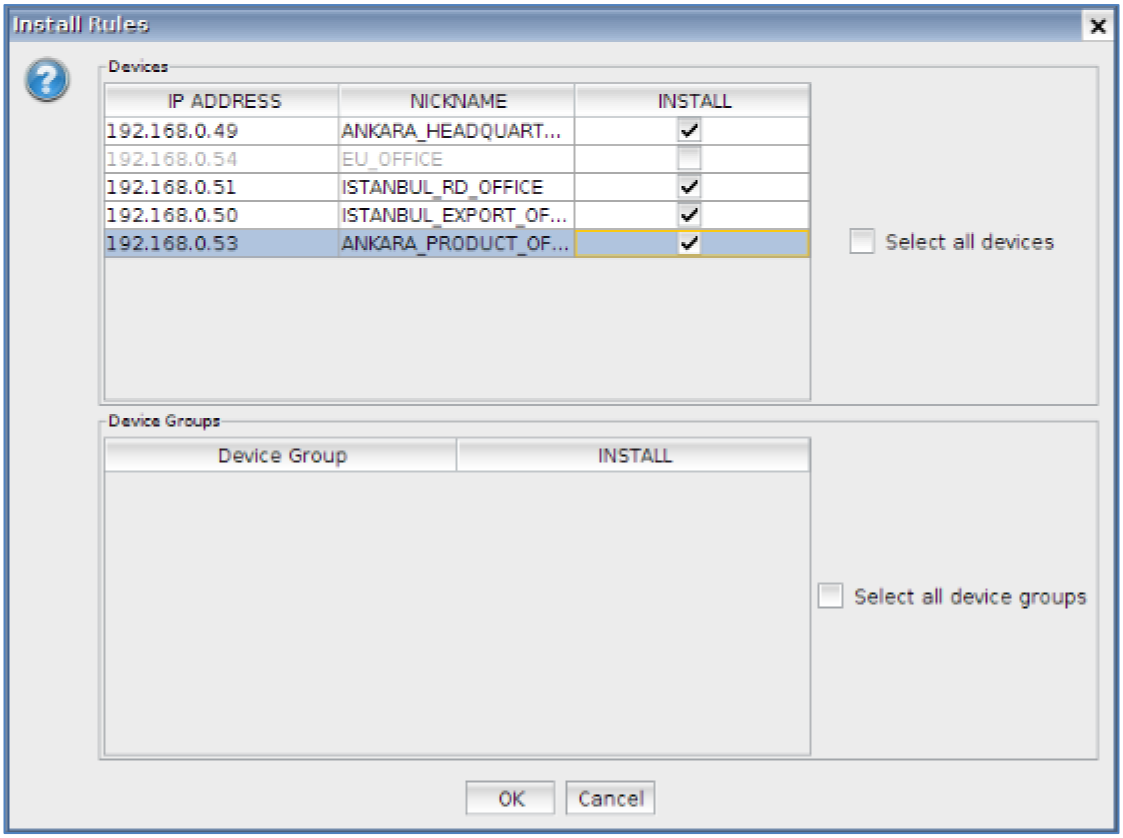
2) Install On Column in Policy Table: Devices and Device Groups can be used in this column. Each rule will be installed to the devices in this column. With this column you can install different rules to different remote Labris UTM devices.



New56

No.	Source	Destination	Service	Action	Schedule	QoS/Bandwidth	Applications	Security Policy	Options	Install On
0	Any	ihracat_bilgi_sistemi	Any	● Accept	Any	Any	Any	Any		192.168.0.50-ISTANBUL_EXPORT_OFFICE
1	Any	ihracat_bilgi_sistemi	Any	● Deny	Any	Any	Any	Any		192.168.0.49-ANKARA_HEADQUARTERS 192.168.0.51-ISTANBUL_RD_OFFICE 192.168.0.53-ANKARA_PRODUCT_OFFICE 192.168.0.54-EU_OFFICE
2	idari_network	Any	Any	● Accept	Any	Any	Any	Any		Any
3	Any	Any	Any	● Deny	Any	Any	Any	Any		Any

3) Install Policy button: This button opens a new pop-up to select which device or device groups will receive the firewall policy.



Install Rules

Devices

IP ADDRESS	NICKNAME	INSTALL
192.168.0.49	ANKARA_HEADQUART...	☑
192.168.0.54	EU_OFFICE	☐
192.168.0.51	ISTANBUL_RD_OFFICE	☑
192.168.0.50	ISTANBUL_EXPORT_OF...	☑
192.168.0.53	ANKARA_PRODUCT_OF...	☑

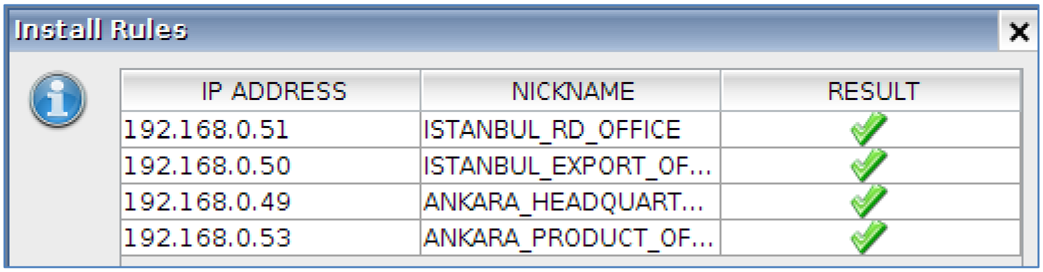
☐ Select all devices

Device Groups

Device Group	INSTALL

☐ Select all device groups

And the results are shown as below:



Install Rules

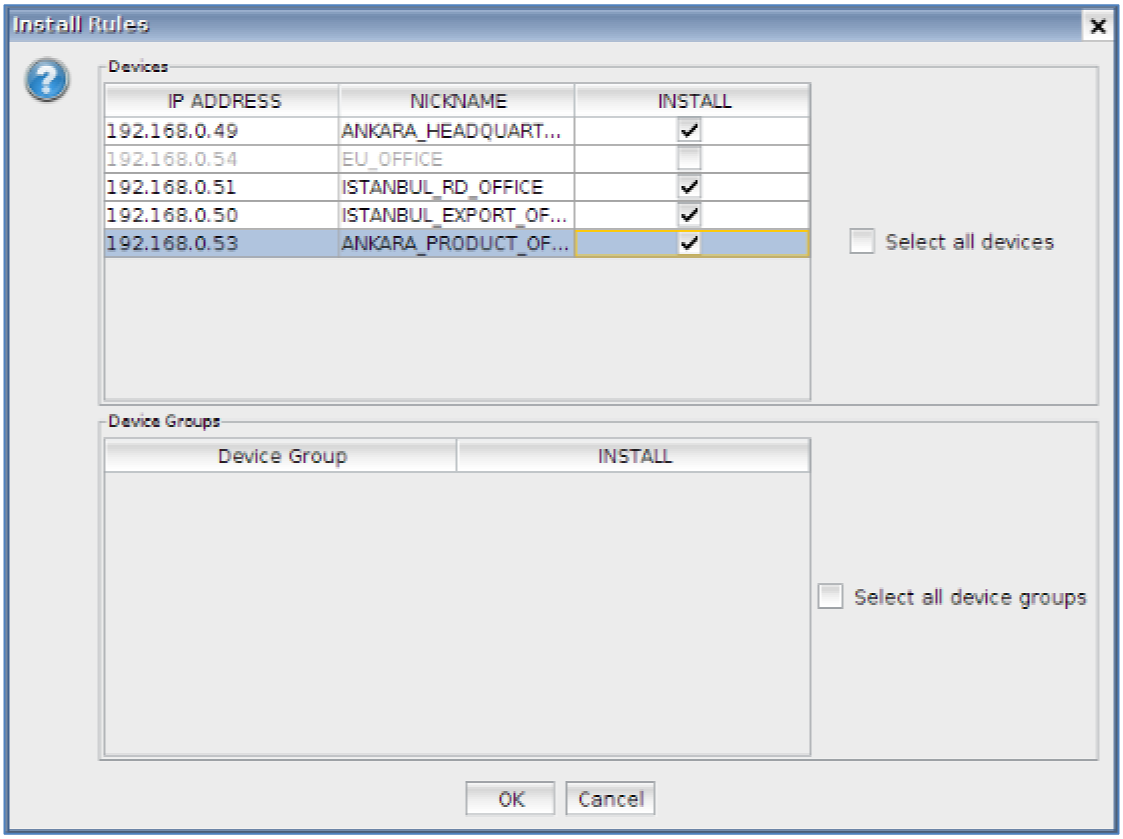
IP ADDRESS	NICKNAME	RESULT
192.168.0.51	ISTANBUL_RD_OFFICE	✓
192.168.0.50	ISTANBUL_EXPORT_OF...	✓
192.168.0.49	ANKARA_HEADQUART...	✓
192.168.0.53	ANKARA_PRODUCT_OF...	✓

Antispam/Antivirus

Antispam/Antivirus tab in **Central Management** module allows administrators to manage antispam, whitelist and blacklist and antivirus options of remote Labris UTM devices. Detailed usage of this module is explained in its own section.

To send antispam/antivirus configurations to remote Labris UTM devices click save and then Install button.

Install button opens a new pop-up to select which device or device groups will receive the antispam/antivirus configuration.

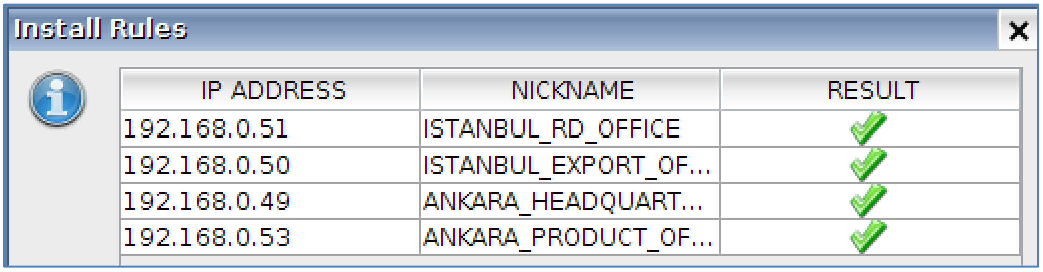


IP ADDRESS	NICKNAME	INSTALL
192.168.0.49	ANKARA_HEADQUART...	☑
192.168.0.54	EU_OFFICE	☐
192.168.0.51	ISTANBUL_RD_OFFICE	☑
192.168.0.50	ISTANBUL_EXPORT_OF...	☑
192.168.0.53	ANKARA_PRODUCT_OF...	☑

☐ Select all devices

Device Group	INSTALL

☐ Select all device groups



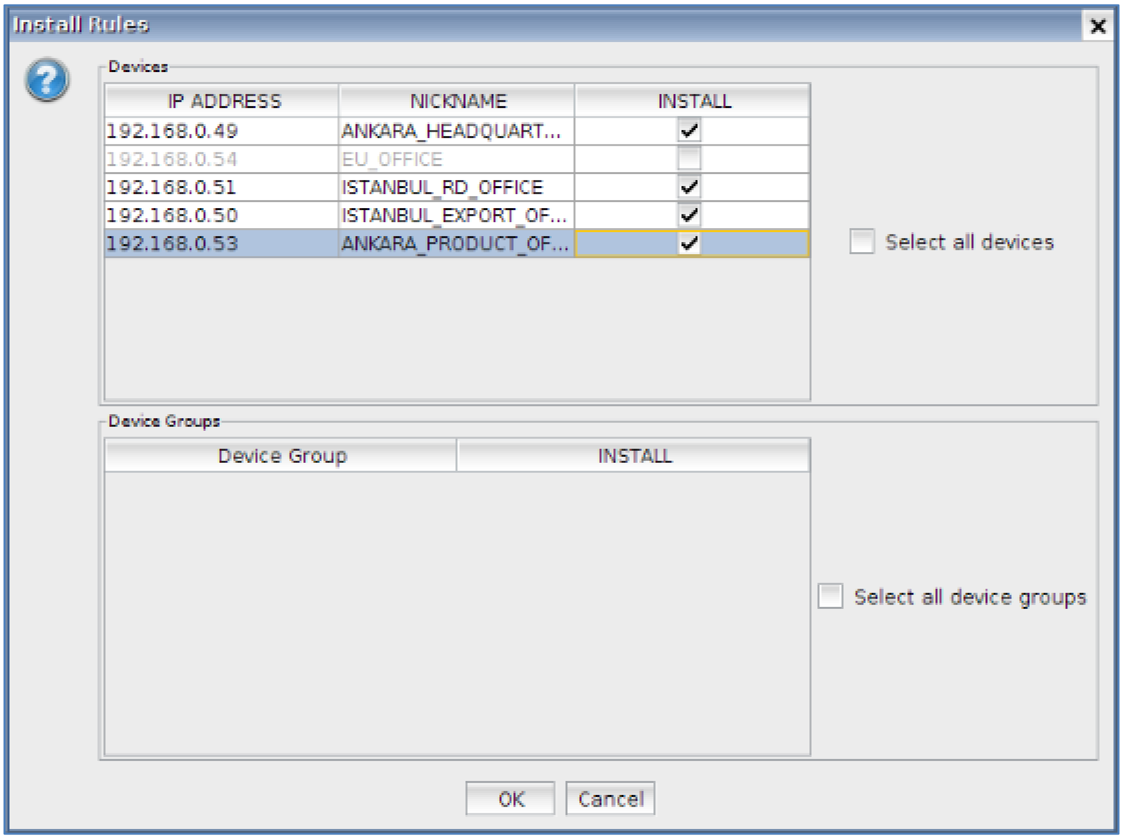
IP ADDRESS	NICKNAME	RESULT
192.168.0.51	ISTANBUL_RD_OFFICE	✓
192.168.0.50	ISTANBUL_EXPORT_OF...	✓
192.168.0.49	ANKARA_HEADQUART...	✓
192.168.0.53	ANKARA_PRODUCT_OF...	✓

Filter

Filter tab in **Central Management** module allows administrators to manage filter configuration of remote Labris UTM devices. Detailed usage of **Filter Groups**, **Banned Filters**, **Exception Filters** and **Configuration** tabs is explained in their own sections.

Only **Central Management** specific option is **Install** button in **Filter Groups** tab.

Install button opens a new pop-up to select which device or device groups will receive the filter configuration.

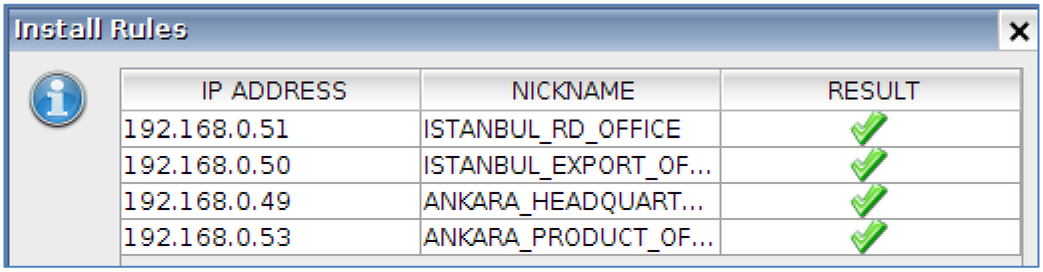


IP ADDRESS	NICKNAME	INSTALL
192.168.0.49	ANKARA_HEADQUART...	☑
192.168.0.54	EU_OFFICE	□
192.168.0.51	ISTANBUL_RD_OFFICE	☑
192.168.0.50	ISTANBUL_EXPORT_OF...	☑
192.168.0.53	ANKARA_PRODUCT_OF...	☑

□ Select all devices

Device Group	INSTALL

□ Select all device groups



IP ADDRESS	NICKNAME	RESULT
192.168.0.51	ISTANBUL_RD_OFFICE	✓
192.168.0.50	ISTANBUL_EXPORT_OF...	✓
192.168.0.49	ANKARA_HEADQUART...	✓
192.168.0.53	ANKARA_PRODUCT_OF...	✓

NTLM Authentication Note:

If Active Directory(AD) integration will be used, Central Management Device and remote Labris UTM devices cannot join different AD Servers. Additionally, Active Directory credentials are not shared across Labris devices. Each device must join AD Server seperately if it will use AD users.

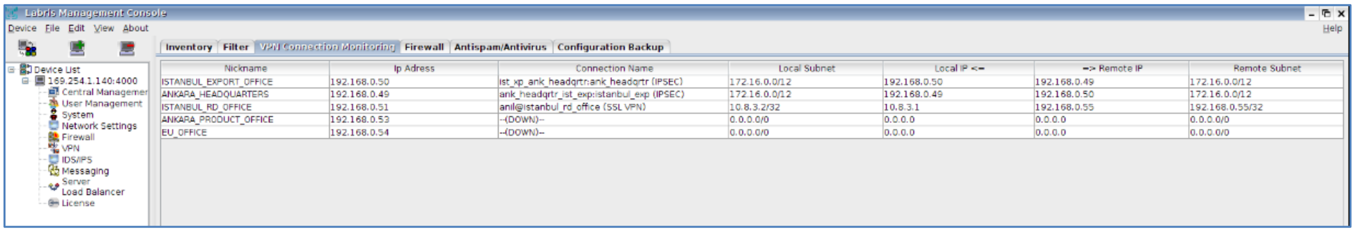
VPN Connection Monitoring

VPN Connection Monitoring tab in **Central Management** module allows administrators to monitor status of VPN connection in remote Labris UTM devices in a uniformed way. Each VPN connection is presented in a separate row with extra info about connection. Connection status is refreshed every 5 minutes. **Refresh** button on the lower left triggers a status update for all VPN connections.

Columns and their meanings

Nickname: Name of the remote Labris UTM device as in **Inventory** tab.
Ip Address: IP address of remote Labris UTM device as in **Inventory** tab.
Connection Name: Name and status of the VPN connection.
Local Subnet: Local subnet shared in this VPN connection.
Local IP: Local IP address used in this VPN connection.
Remote IP: Connected remote IP address in this VPN connection.
Remote Subnet: Remote subnet shared in this VPN connection.

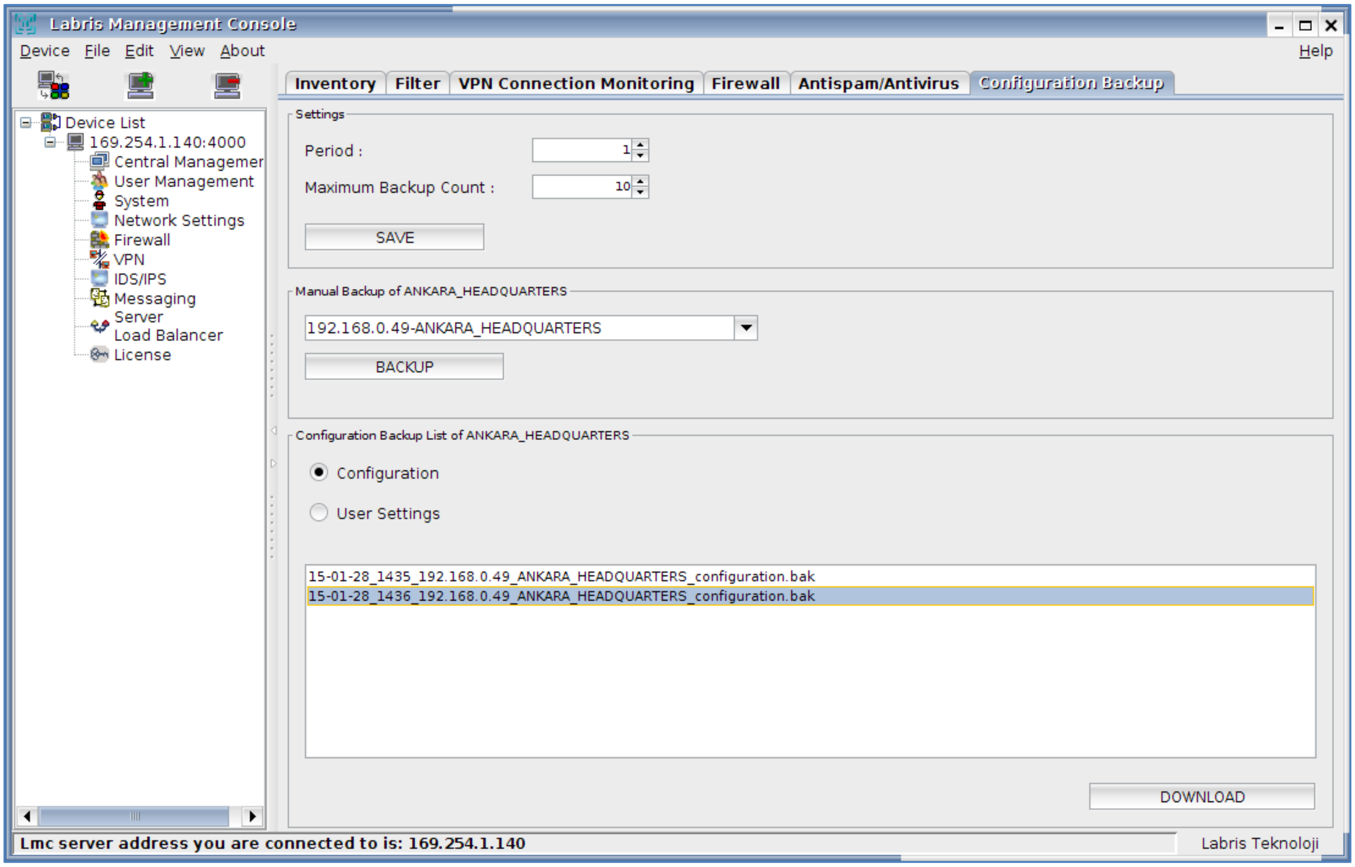
An example of the screen is shown as below:



Nickname	Ip Adress	Connection Name	Local Subnet	Local IP <--	--> Remote IP	Remote Subnet
ISTANBUL_EXPORT_OFFICE	192.168.0.50	ist_xp_ank_headqrtr:ank_headqrtr (IPSEC)	172.16.0.0/12	192.168.0.50	192.168.0.49	172.16.0.0/12
ANKARA_HEADQUARTERS	192.168.0.49	ank_headqrtr_ist_exp:istanbul_exp (IPSEC)	172.16.0.0/12	192.168.0.49	192.168.0.50	172.16.0.0/12
ISTANBUL_RD_OFFICE	192.168.0.51	anil@istanbul_rd_office (SSL VPN)	10.8.3.2/32	10.8.3.1	192.168.0.55	192.168.0.55/32
ANKARA_PRODUCT_OFFICE	192.168.0.53	--(DOWN)--	0.0.0.0/0	0.0.0.0	0.0.0.0	0.0.0.0/0
EU_OFFICE	192.168.0.54	--(DOWN)--	0.0.0.0/0	0.0.0.0	0.0.0.0	0.0.0.0/0

Configuration Backup

Configuration Backup tab in **Central Management** module allows administrators to create and save backups of remote Labris UTM devices. The central management device automatically creates backup of every Labris UTM device at specific time intervals. The administrator can set the backup frequency on the basis of days and the maximum backup count per remote Labris UTM device.



Settings

Period : 1

Maximum Backup Count : 10

Manual Backup of ANKARA_HEADQUARTERS

192.168.0.49-ANKARA_HEADQUARTERS

Configuration Backup List of ANKARA_HEADQUARTERS

● Configuration

○ User Settings

15-01-28_1435_192.168.0.49_ANKARA_HEADQUARTERS_configuration.bak
15-01-28_1436_192.168.0.49_ANKARA_HEADQUARTERS_configuration.bak

Lmc server address you are connected to is: 169.254.1.140

Backup-Restore policy is different for devices joined to Central Management. For devices joined Central Management restore stage is same with single Labris UTM device except user, group and domain restore process. In Central Management system, remote Labris UTM devices' user, group and domain data is not restored from backup file.

User, group and domain data is only restored when backup is restored on Central Management device. In this case all user, group and domain data in remote Labris UTM devices' is overwritten by the restore user, group and domain data.

User Management

Users, groups and domains are shared between Central Management devices and remote Labris UTM devices. This feature allows writing policies for same users and groups among all remote Labris UTM devices.

Remote Labris UTM devices can only edit users and groups which belong to that device's domain or that device's Active Directory domain, other users, groups and domains are read-only for that device.

Labris
NETWORKS