

Administration Guide for Labris UTM

Unified Threat Management Appliances and Software

Version 3.4.2

<http://labrisnetworks.com/support-training/>

Tel: +90 850 455 4555



Labris
NETWORKS

1. Copyright

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission in writing of the author/publisher.

2. 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.

© Copyright 2013-2014. All rights reserved.

3. Document Revision History

#	Document modified by	Description	Authorized by
1			
2			
3			
4			

Table of Contents

Copyright.....	1
Disclaimer.....	1
Document Revision History.....	1
About Labris Networks Inc.....	12
About LABRIS UTM.....	13
How to Purchase LABRIS UTM ?	13
LABRIS UTM Appliance deployment Architecture	14
Connecting Appliance	14
Accessing the Web Admin Console.....	15
LRMS into the LABRIS UTM Appliance	15
Wizard Installation	19
How to use Wizard Installation?.....	20
A – Gateway Mode Network Configuration This is the section where the hostname and working mode settings of the device can be made.	22
B - DNS Configuration This is the section where DNS IP address settings can be made.	24
C - DHCP Configuration This is the section where we can activate or deactivate DHCP server in which the interface and IP settings of the IP addresses to be distributed to our DHCP Local users, are made.	24
Accessing LABRIS UTM through LMC.....	27
LMC Interface.....	27
Menu.....	28
File Menu	29
Edit Menu.....	31
View Menu	34
Device Menu	35
Add Modules from Server Menu	36
User Management	39
Users	39
Adding User.....	39
Deleting User.....	42
Changing password / Editing User	43
Groups.....	44
Adding Group	44
Deleting Group.....	48

Editing Group	49
WAUTH.....	56
Deleting WAUTH policy.....	60
Editing WAUTH Policy	61
Adding WAUTH Authentication and User	62
Login.....	82
Change User Password.....	83
Obtain Password	87
Registering with SMS	87
GSM number and common key	87
System.....	105
System LMC Module	105
Users	106
Adding User.....	106
Deleting User.....	108
Change Password / Editing User	109
DHCP	112
DNS.....	129
HA - High Availability Appliance Deployment Architecture.....	134
Configuration Backup / Restore.....	146
Update	157
Automatic Update.....	157
Record	158
Date / Time Settings.....	159
Console Access Settings.....	159
General Settings.....	162
Trusted Time Stamp.....	163
Restart.....	165
Shutdown.....	165
Network Settings.....	165
IP Configuration	166
IP Alias (ADD, Edit, Delete, Status, Enable/disable).....	166
ADSL (Add, Edit, Delete, Status, Enable/Disable).....	174
Bridge(Add ,Edit, Delete, Status , Enable/disable).....	179

3G (ADD, Edit, Delete, Status, Enable/disable)	182
Vlan (Add , Edit, Delete, Status , Enable/disable)	185
Routes	189
Default Gateway	190
Static Route	190
Add (Static Route)	191
Delete (Static Route)	192
Load Balance	192
Add (Load Balance Route)	199
Edit (Load Balance Route)	200
Delete (Load Balance Route)	201
Advanced/ Policy Based Routing	201
Link Configuration	202
Decision Table	203
WAN failover (WAN Backup)	207
Firewall	214
Make a new firewall object	215
Objects	220
Network Objects	221
Hosts	222
Networks	227
Address Ranges	229
Object Groups	232
Users	235
Services	237
ICMP	238
IP	240
TCP	244
UDP	247
Service Groups	249
DoS/DDoS	253
General	254
SYN Flood	254
UDP Flood	255

CONN Flood.....	256
ICMP Flood	256
ICMPv6 Flood	256
Notes.....	257
QoS/Bandwidth.....	259
General.....	259
Notes.....	260
Schedule.....	261
Standard.....	262
User Defined	263
General.....	263
Start.....	264
Stop.....	265
Notes.....	265
Application Control	267
User Defined	267
Firewall.....	270
Labris Firewall Management.....	270
Install, Save (create a new policy object for first setup), Install Policy.....	270
Add Next Generation Firewall.....	272
Firewall Properties	274
Global Policy table.....	278
NAT (Network Address Translate) Policy table.....	282
Interfaces	286
Firewall Application.....	289
SSH Inspection.....	289
Network Address Translate (NAT)	291
What is the NAT?	291
Why it is made?.....	291
NAT Types	292
SNAT.....	292
DNAT	292
PAT	292
Port Forwarding/Port Mapping.....	292

Reverse Proxy engine.....	292
Sample configuration:.....	294
VPN.....	295
IPSEC VPN Configuration.....	296
Profile Administration;.....	296
Add Profile	296
Identity Confirmation RSA; RSA (Rivest Shamir Adleman) It is the section where common security key, used in the stage of establishing connection with the remote network with which IPSEC VPN will be made, is defined. RSA is an internet encryption and authentication system.....	297
Add Local Networks (Manuel);	298
Add Remote Networks;.....	298
Policy;.....	299
Add Policy.....	300
Add PHASE-1;	300
Add PHASE-2;	301
Add Global Policy For Remote Network access permissions in cases where Generate Firewall Rule Automatically option is not selected, Step 3 and Step 4 must be applied.	303
Add NAT policy.....	303
Delete Profile	303
Connection Tracking;	304
SSL VPN Configuration using CLI	304
Create a new global policy	305
Create a new NAT Policy	306
Add a user on policy.....	307
SSL VPN CLIENT - User Administration.....	307
SSLVPN Client	308
Add	308
Edit	310
Delete.....	311
Settings.....	312
L2TP.....	313
Add	315
Edit	316
Delete.....	318
Service Management	318

FILTER	319
Filter Groups	320
Add/Edit Filter Group.....	321
Delete Filter Group	324
Time limit	325
Add Time	325
Delete Time.....	327
Add Users	328
Add Groups	329
Add IP/ IP Range.....	331
Delete.....	332
Banned Filters	334
Domain/ Category Filtering.....	334
Add.....	335
Add More	336
Delete.....	337
URL/Category Filtering.....	338
Add.....	338
Add More	340
Delete.....	341
Regex URL Filtering	341
Add.....	342
Add More	343
Delete.....	345
Phrases.....	347
Add.....	347
Delete.....	348
Content Change	349
Add.....	349
Delete.....	351
Extension Filter	353
Add.....	353
Delete.....	355
Application Types Filter (MIME)	357

Add	357
Add More	358
Delete	359
Exception Filters.....	361
Domain.....	362
Add	362
Add Multiple	363
Delete	365
URL.....	366
Add	366
Delete	367
Phrases.....	368
Add	368
Delete	369
Grey Site.....	370
Add	370
Add Multiple	372
Delete	373
Grey URL	374
Add	374
Add More	375
Delete	377
Settings.....	378
Reporting Options.....	378
Authentication	379
NTLM Authentication.....	379
NTLM Authentication AD Configuration	415
General View.....	415
Prerequisite.....	415
Scenario.....	416
Configuration	416
Logging Options	424
Network Settings.....	424
Weighted Phrase Settings.....	425

Cache Settings	425
Fork Pool Settings	425
Log Monitoring.....	426
Show.....	427
Filter	427
Start.....	427
Clear	428
ANTISPAM/ANTIVIRUS.....	429
Spam Mail Box	429
Search Criterions.....	429
Virus Mail Box	430
Search Criterions.....	430
Antispam-Antivirus Options.....	431
Domain Control.....	431
Settings.....	434
Antispam Options	436
Check Options	436
Report Options.....	440
Whitelist Blacklist.....	440
Enable White List	440
Enable black List.....	444
Antivirus Options	447
Antivirus Options	447
Report Options.....	451
IDS/IPS.....	452
Sensor Settings.....	452
Intrusion Detection System.....	452
Settings.....	453
Network Settings.....	453
Interface.....	458
Rule sets	461
Alert Settings.....	469
Mail Alert Settings.....	469
Report Mails.....	470

Alerts	470
MESSAGING.....	470
Domains	471
Domain.....	471
All Users	474
Aliases	479
Groups.....	482
Services	484
Configuration	486
Load Balancer.....	488
Configuration	489
Externally Advertised Services	489
Internal Servers for Selected External Service	493
Internal Address.....	493
Service	495
Global	496
Global Settings	496
Monitor	497
Service Monitor.....	497
License.....	498
New License	498
Install License	500
Glossary.....	500
Labris Firewall Messages.....	501
1. Labris Logview User Guide	505
1. Introduction	505
2. Parts & Tools	507
3. Instructions	511
4. Records Table.....	511
4.1. Real-time Monitoring.....	514
5. Utilities	517
5.1. Settings.....	517
5.2. Save Screen	518
5.3. Load Screen.....	518

6. Regional Settings.....	520
7. Service Monitoring.....	521
8. Layout Options.....	522
8.1. Single Widget View	522
8.2. Column View	523
8.3. List View	523
8.4. Grid View.....	523

4. 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.

5. 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.

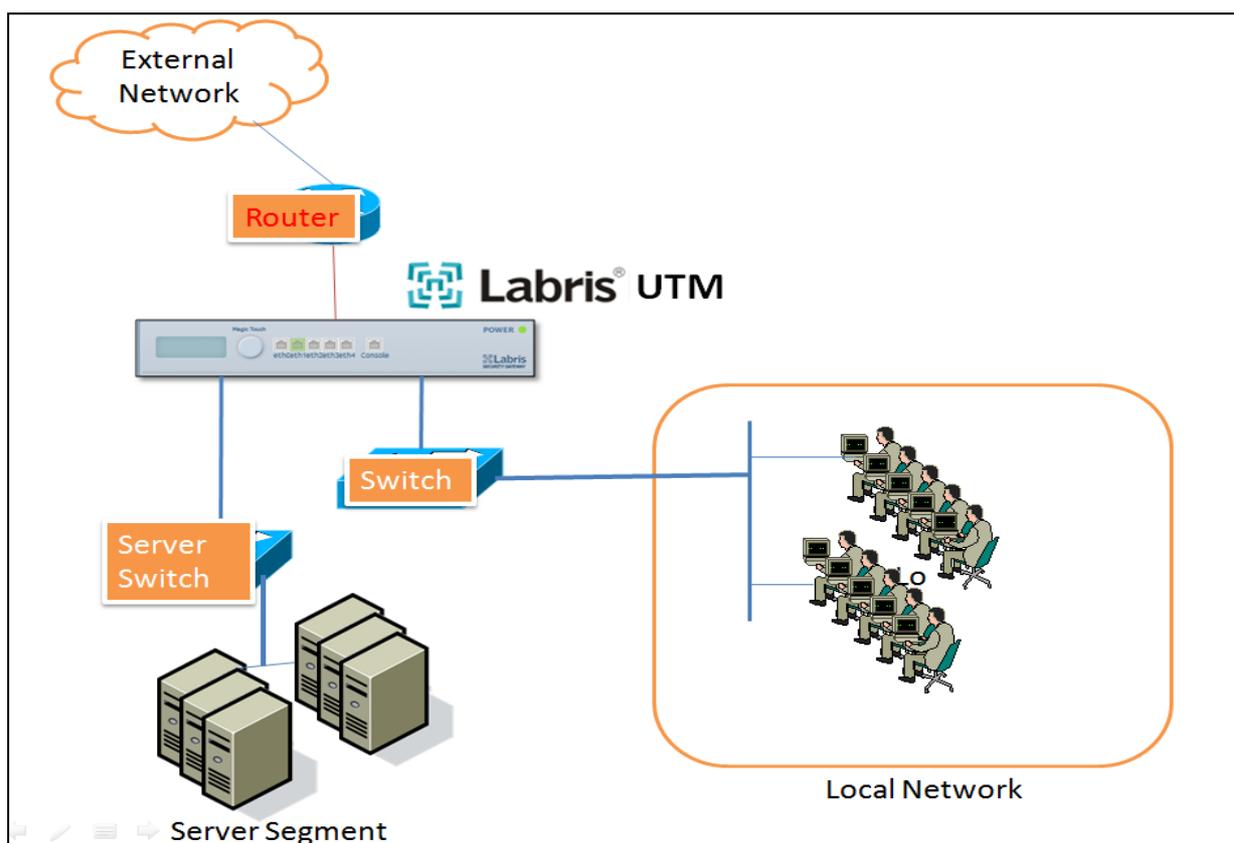
6. How to Purchase LABRIS UTM ?

To purchase LABRIS UTM, Visit - <http://labrisnetworks.com/products/product/lbrutm-series-appliances/>

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

7. LABRIS UTM Appliance deployment Architecture

This section provides information about the logical and physical design for the prescribed deployment architecture. LABRIS UTM Appliance deployment architecture consists of software processes called servers, topological units referenced as nodes and the security device known as Labris UTM. In the below deployment architecture, all the Servers and LAN users are connected to the Labris UTM through L2 switches. Labris UTM Appliance is connected to external network through Router.



8. Connecting Appliance

Connect appliance to a management computer's Ethernet interface. You can use a cross-over Ethernet cable to connect directly or use straight-through Ethernet cable to connect through the hub or switch. Both the cables are provided along with the appliance. Connect Ethernet cable one end to Labris UTM device in eth0 and other end to computer.

Note

• Labris UTM Device will provide default IP address

9. Accessing the Web Admin Console

Labris Default Management Port = eth0/Port1/Net0/Mgt (first port to device)

Labris Default IP Address: 169.254.1.1

Labris Default Username: admin

Labris Default Password:labris

Connect your computer to the first port on the Labris and then open computer's network settings section and assign IP address **169.254.1.2** and subnet **255.255.0.0**. Open your browser and browse <https://169.254.1.1:81>(Here IP address is the IP address of your device) to access **LABRIS UTM** Web Console (GUI). Login page is displayed and you are prompted to enter login credentials. Use default username and password to log on.

Note

•Latest versions of Browsers like **Internet Explorer** or **Mozilla Firefox** are required to access web Admin Console

10.LRMS into the LABRIS UTM Appliance

LRMS – Labris Report and Monitoring Service

Once you set and install LABRIS UTM Appliance properly this is how you will login in to the LABRIS UTM Appliance

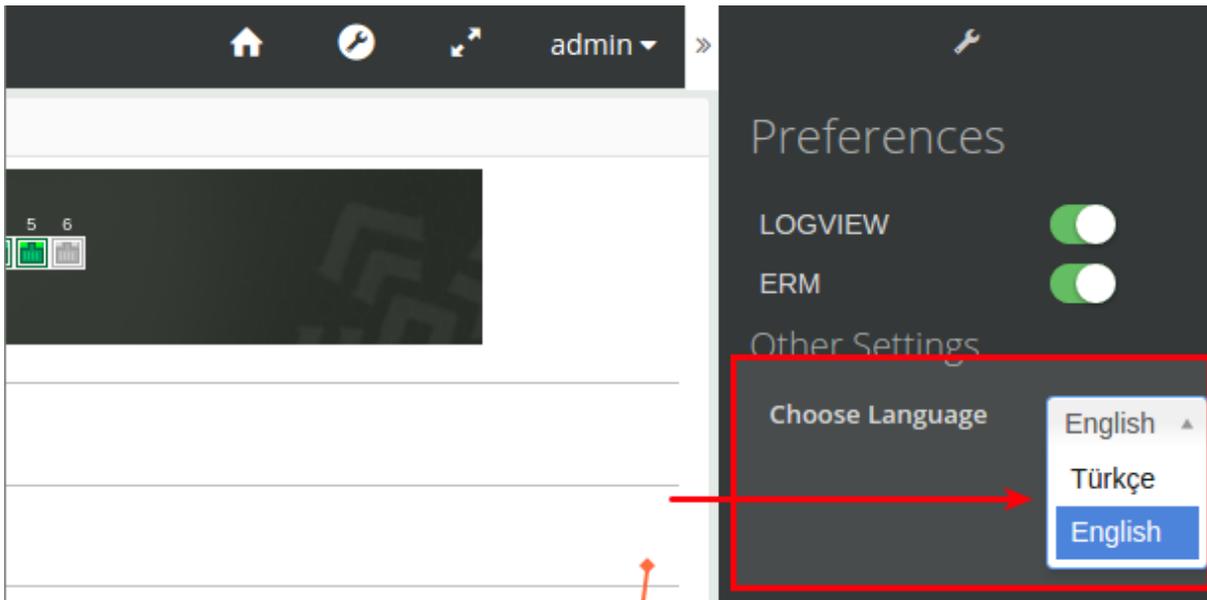
It has a login screen as well as languages selection screen

These are the inputs for LABRIS UTM Login screen

1	Username	Type in your valid Default username . This username is the one which you have given during the installation
2	Password	Type in your valid Default password . This password is the one which you have given during the installation.A good password is a mix of alphabets , numericals , special characters with a minimum length of 8
3	Warm Me	Warm Me before logging me into other sites.
4	Clear	Clear all Input
5	Login	Click on " Login " button to login to your appliance
6	Languages	Select your preferred language before logging into your appliance .Currently available languages are English and Turkish

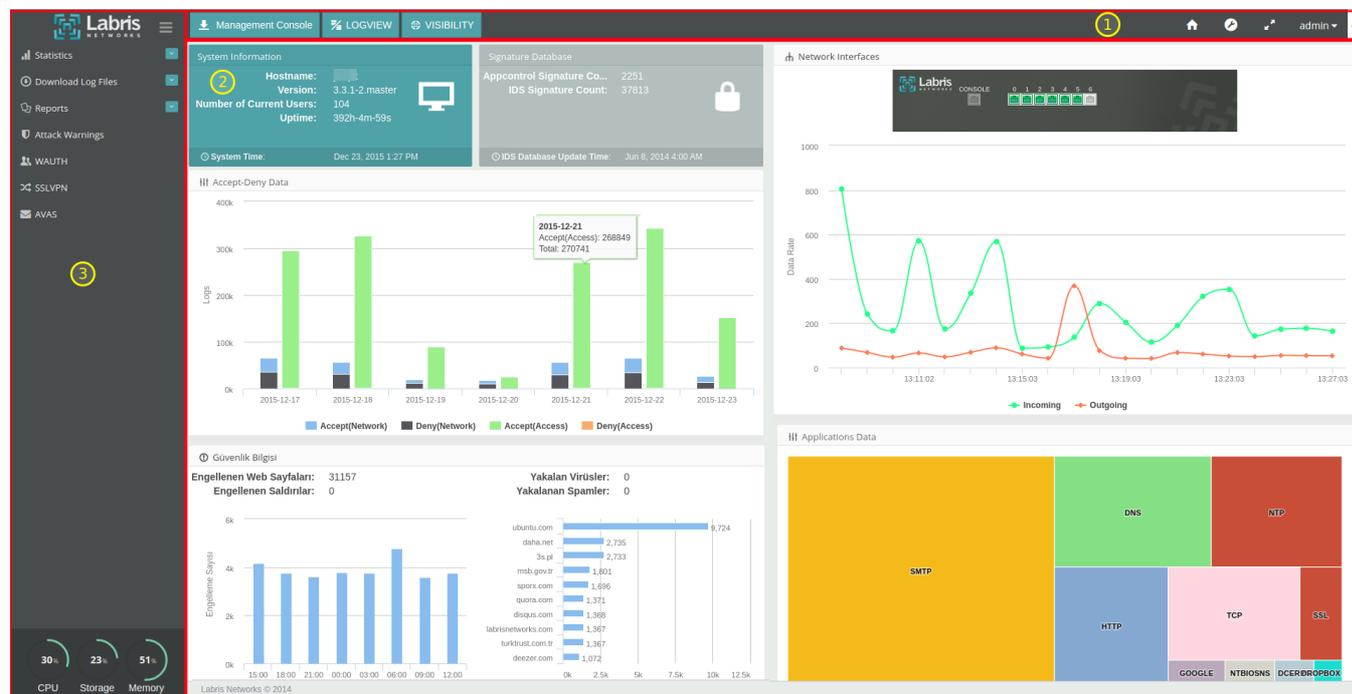
The image shows the Labris Central Authentication Service login page. It features the Labris Networks logo at the top. Below the logo, the text "Labris Central Authentication Service" is displayed. The page contains a "Username:" field (callout 1), a "Password:" field (callout 2), and a checkbox labeled "Warn me before logging me into other sites." (callout 3). There are two buttons: "CLEAR" (callout 4) and "Login" (callout 5). At the bottom, there is a language selection menu (callout 6) with "English | Turkish" options. A security notice at the bottom reads: "For security reasons, please Log Out and Exit your web browser when you are done accessing services that require authentication!"

Note • You can also change your preferred language even after you login to the appliance as shown in following image



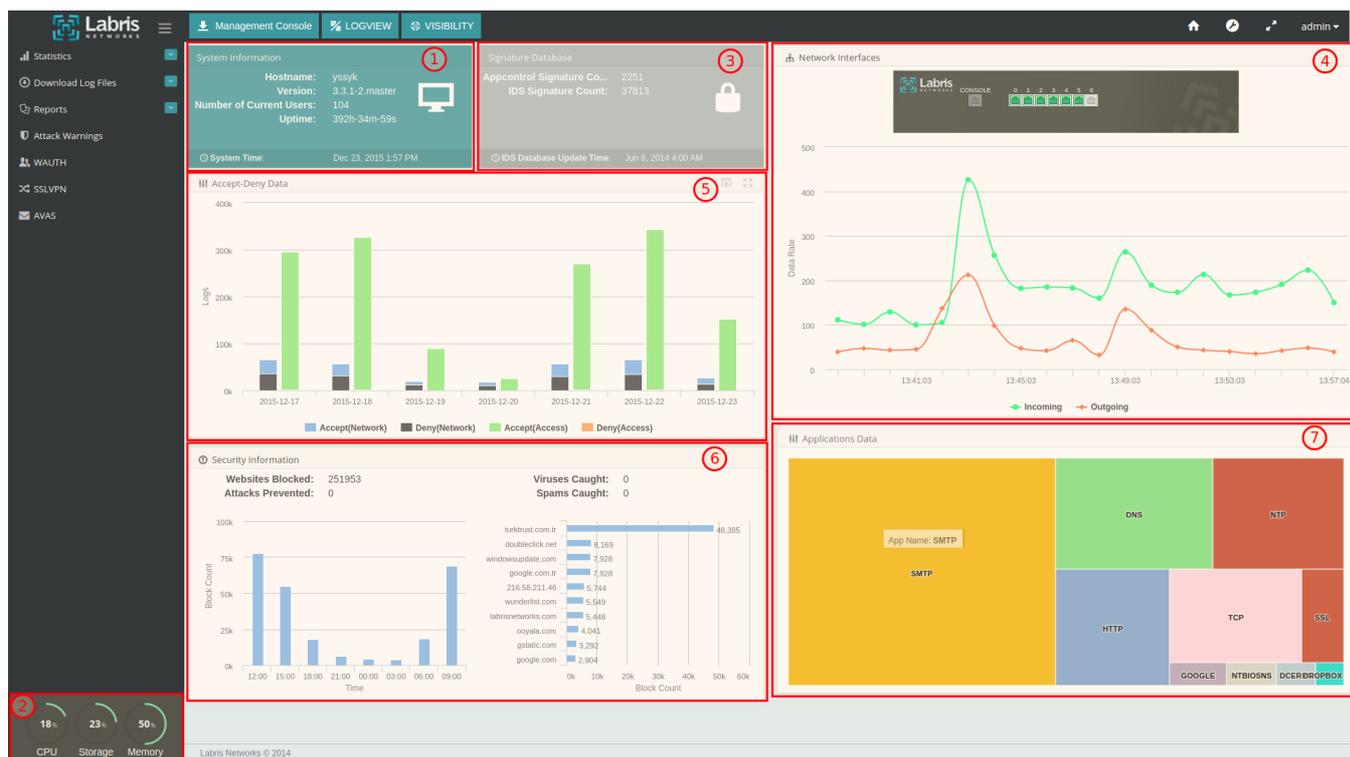
Understanding your landing page or home screen

In this section you will understand various sections of **LABRIS UTM** appliance's home screen after the initial login.



1	Page Header Section	In this section, you will find links to LMC, Logview, Visibility, Wizard, Authentication and Settings toggle, Help and Logout . Notice the right hand top corner for Help and Logout .
2	Main Dashboard	After the initial login, you will be landed on to your Labris Security Gateway Software Dashboard . Main dashboard will show you System Information and various historical & real time statistics.
3	Navigation	You can navigate to various sections such as. In addition to these you will also find options to change your preferred language.

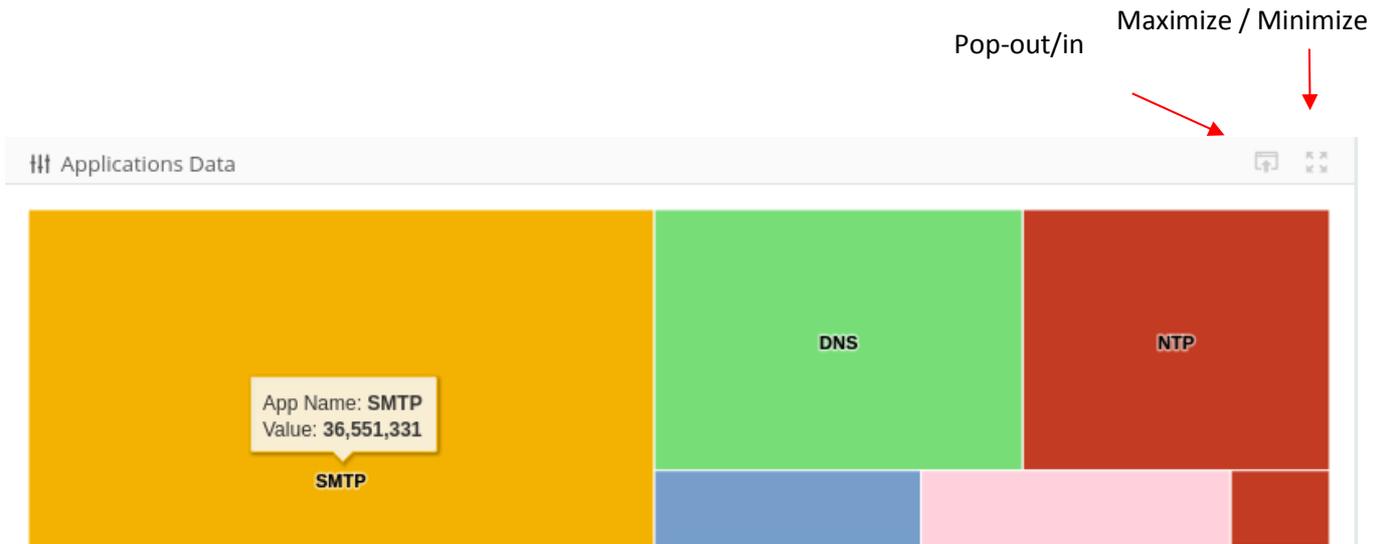
On Dashboard, You will find widgets such as **System Information, Network Interfaces, Resources, Protection Information, Application Data** and **Signature Databases**.



1	System Information	System Information field in the dashboard displays information on the No.of users , Host Name , Labris Version , System Time and Uptime
2	Resources	Resources field displays information on resources(Processors , Memory , Disk) and their utilization levels with diagrams which makes us to understand easily.
3	Signature Databases	Signature Databases displays information which is related to the UTM device
4	Network Interfaces	Network Interfaces field displays information like Ip Address , NetMask , Status and Error Information . We can also find a chart which gives pictorial representation of the Ethernet utilization .
5	Accept-Deny Data	Accept-Deny Data widget summarizes Accepted and Denied traffics count by a single date from Firewall(Network) and Webfilter(Access) data.
6	Protection Information	Protection field displays information related to the virus / spams caught and also the No.of websites blocked and Attacks prevented .
7	Application Data	Application Data widget shows a treemap graph for most used application along the whole network.

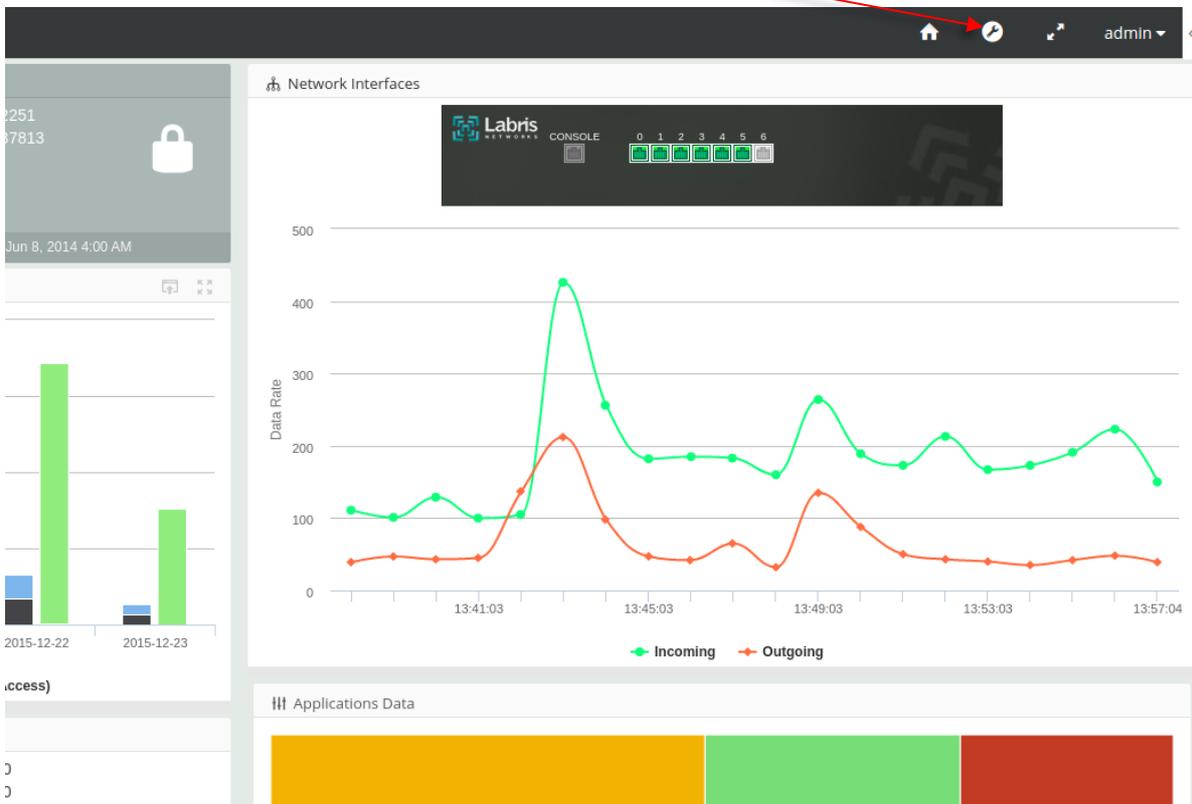
How to Pop-in/out and Maximize/Minimize widgets on the Main Dashboard

You can pop-out/in and maximize/minimize these widgets on the main dashboard by clicking icons which, are shown as below based on your need.



Wizard Installation

Installation wizard enables simple configuration of Labris UTM products by users in just a few steps. Installation wizard can be accessed via product's web interface. The wizard is fixed at the top right corner of the web interface.



11. How to use Wizard Installation?

The product configuration can be started by clicking the Wizard icon on the web interface. The product configuration can be made in five steps in total.

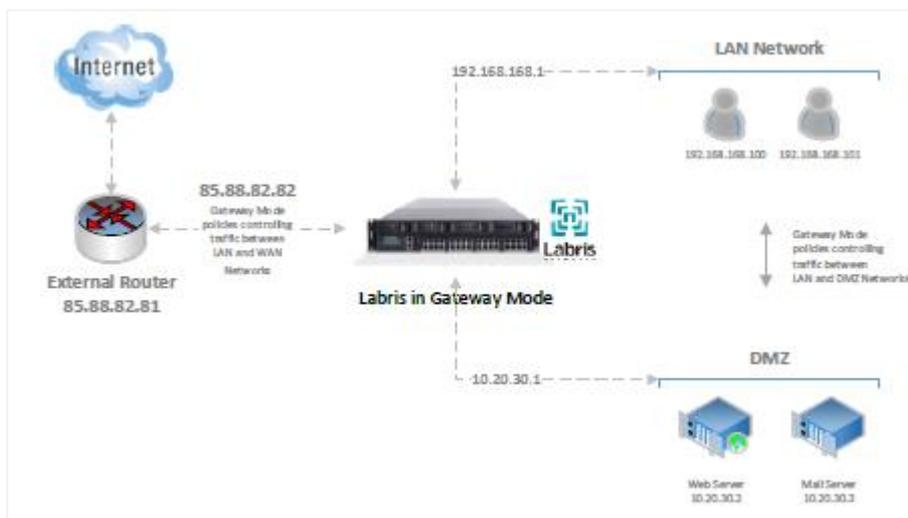
1. Hostname and Gateway Mode Configuration
 - a. Gateway Mode Network Configuration
 - i. Network Configuration for LAN or DMZ
 1. Network Configuration for HotSpot and Web Filter on the LAN or DMZ interface
 - ii. Network Configuration for IP Type DHCP
 - iii. Network Configuration for IP Type Static
 - iv. Network Configuration for IP Type PPPoE
 - b. DNS Configuration
 - c. DHCP Server Configuration
2. Hostname and Bridge Mode Configuration
 - a. Bridge Mode Network Configuration

1. Hostname and Gateway Mode Configuration

Configure as Gateway if you want to use Labris UTM as

- A firewall or replace an existing Firewall
- A gateway for routing traffic
- Link load balancer and implement gateway failover functionality

Apart from configuration Gateway IP address (IP address through which all the traffic will be routed), you must also configure LAN and WAN IP addresses.



Hostname and Working Mode;

The screenshot shows the Labris Installation Wizard at the 'Hostname and Working Mode Configuration (1/4)' step. The form has two main sections: '1 Hostname' with a text input field containing 'slave', and '2 Working Mode' with a dropdown menu set to 'Gateway'. Below these are navigation buttons: '3 < Back', 'Next >', and '5 Apply & Next'. A '6 Jump to Selected Section' dropdown menu is open, showing options: 'jump to selected section', 'Hostname Configuration', 'Network Configuration', 'Bridge Configuration', 'DNS Configuration', 'DHCP Server Configuration', and 'jump to selected section'.

1	Hostname	Device Hostname
2	Working Mode	Select a Working Mode. Gateway or Bridge
3	Back	The Back Step Now
4	Next	The Next Step Now
5	Apply & Next	Apply Changes and goto Next Step
6	Jump to Selected Section	Connect The Desired Step

12. A – Gateway Mode Network Configuration

This is the section where the hostname and working mode settings of the device can be made.

i - Network Configuration for LAN or DMZ;

Network Configuration - (eth2) (2/4)

1	Interface	Select Interface
2	Interface Type	Select Network Type for WAN,LAN or DMZ
3	Interface Name	Name for Network
4	NAT	Network Address Translate ON or OFF

ii - Network Configuration for IP Type DHCP;

6	IP Type	Select IP Type for DHCP, Static or PPPoE
7	IP Address	IP Address for Network LAN,WAN or DMZ
8	Netmask	Netmask for Network LAN,WAN or DMZ
9	Default Gateway	Gateway for Network WAN

iii - Network Configuration for IP Type Static

6	IP Type	Select IP Type for DHCP, Static or PPPoE
7	IP Address	IP Address for Network LAN,WAN or DMZ
8	Netmask	Netmask for Network LAN,WAN or DMZ
9	Default Gateway	Gateway for Network WAN

The screenshot shows two configuration fields. The first field is labeled '10 VLAN' and contains a blue button with the text 'ON'. The second field is labeled '11 VLAN ID' and contains a text input box with the number '1' inside.

10	VLAN	VLAN ON or OFF for Network
11	VLAN ID	ID for VLAN

iv - Network Configuration for IP Type PPPoE

The screenshot shows two rows of configuration fields. The first row contains: '6 IP Type' with a dropdown menu showing 'PPPoE', '7 IP Address' with an empty text box, '8 Netmask' with an empty text box, and '9 Default Gateway' with an empty text box. The second row contains: '10 DSL Username' with a text box containing 'labris', '11 DSL Password' with a masked text box (dots), and '12 Verify DSL Password' with a masked text box (dots).

6	IP Type	Select IP Type for DHCP, Static or PPPoE
7	IP Address	IP Address for Network LAN,WAN or DMZ
8	Netmask	Netmask for Network LAN,WAN or DMZ
9	Default Gateway	Gateway for Network WAN
10	DSL Username	Username for DSL Authentication
11	DSL Password	Password for DSL Authentication
12	Verify DSL Password	Again Password for DSL Authentication

1 - Network Configuration for HotSpot and Web Filter on the LAN or DMZ interface;

The screenshot shows two rows of configuration fields. The first row contains: '13 WAUTH' with a blue button labeled 'ON', and '14 WAUTH SSL Connection' with a blue button labeled 'ON'. The second row contains: '15 HTTP Filtering' with a blue button labeled 'ON', and '16 HTTPS Filtering' with a blue button labeled 'ON'.

13	WAUTH	Wireless Authentication enable or disable for Network LAN or DMZ
14	WAUTH SSL Connection	Connect with SSL on the WAUTH Management Page
15	HTTP Filtering	Web Filtering enable or disable HTTP Protocol for Network LAN or DMZ
16	HTTPS Filtering	Web Filtering enable or disable HTTPS Protocol for Network LAN or DMZ

13. B - DNS Configuration

This is the section where DNS IP address settings can be made.

The screenshot shows the 'DNS Configuration (3/4)' section of a web interface. It contains two rows of configuration fields. The first row has three input boxes for 'DNS 1 IP', 'DNS 2 IP', and 'DNS 3 IP', with values 192.168.168.10, 8.8.8.8, and 4.4.2.2 respectively. The second row has an input box for 'Internal DNS Domain Name' with the value 'labrisDNS.local' and a dropdown menu for 'Time Zone' set to 'Europe/Istanbul'.

1	DNS 1 IP	First DNS Server for IP Address
2	DNS 2 IP	Second DNS Server for IP Address
3	DNS 3 IP	Third DNS Server for IP Address
4	Internal DNS Domain Name	Internal DNS Server Domain Name
5	Time Zone	Select a Time Zone

14. C - DHCP Configuration

This is the section where we can activate or deactivate DHCP server in which the interface and IP settings of the IP addresses to be distributed to our DHCP Local users, are made.

DHCP OFF

The screenshot shows the 'DHCP Configuration (4/4)' section of a web interface. It contains two fields: 'DHCP Server for LAN' with a radio button set to 'OFF', and 'DHCP Interface' with a dropdown menu set to 'eth0'.

1	DHCP Server for LAN	Select DHCP Server Active or Passive
2	DHCP Interface	Interface list for DHCP Server or Relay

DHCP ON

DHCP Configuration (4/4)

1 DHCP Server for LAN

2 DHCP Interface

3 DHCP IP Start

4 DHCP IP End

5 DHCP Netmask

6 DHCP Gateway

7 DNS 1 IP

8 DNS 2 IP

1	DHCP Server for LAN	Select DHCP Server Active or Passive
2	DHCP Interface	Select DHCP Interface
3	DHCP IP Start	DHCP IP Start Address
4	DHCP IP End	DHCP IP End Address
5	DHCP Netmask	Netmask for IP Address
6	DHCP Gateway	Gateway IP Address for Client s
7	DNS 1 IP	First DNS IP Address for Clients
8	DNS 2 IP	Second DNS IP Address for Clients

2. Hostname and Bridge Mode Configuration

Configure as Bridge if

- You have a private network behind an existing firewall or behind a router and you do not want to replace the firewall.
- You are already masquerading outgoing traffic.



A - Bridge Mode Network Configuration

Labris NETWORKS Installation Wizard

Hostname and Working Mode Configuration (1/4)

1 Hostname: slave

2 Working Mode: Bridge

3 < Back Next > Apply & Next 5

4

1	Hostname	Device Hostname
2	Working Mode	Select a Working Mode. Gateway or Bridge
3	Back	The Back Step Now
4	Next	The Next Step Now
5	Apply & Next	Apply Changes and goto Next Step

Bridge Configuration (2/4)

1 Bridge Name: br0

2 Left Bridge Interface: em2

3 Right Bridge Interface: em3

4 Bridge IP: 192.168.168.2

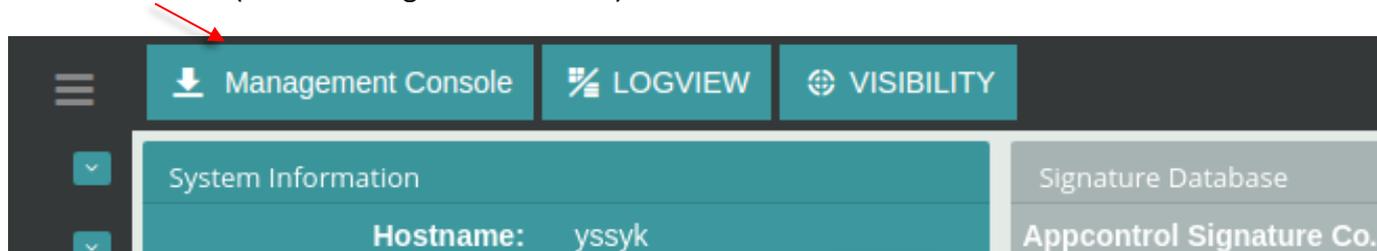
5 Bridge Netmask: 255.255.255.0

6 Submit

1	Bridge Name	Name for Bridge
2	Left Bridge Interface	Select Bridge Interface for Left
3	Right Bridge	Select Bridge Interface for Right
4	Bridge IP	Bridge IP for Management
5	Bridge Netmask	Bridge IP Netmask for Management
6	Submit	Apply Changes

Accessing LABRIS UTM through LMC

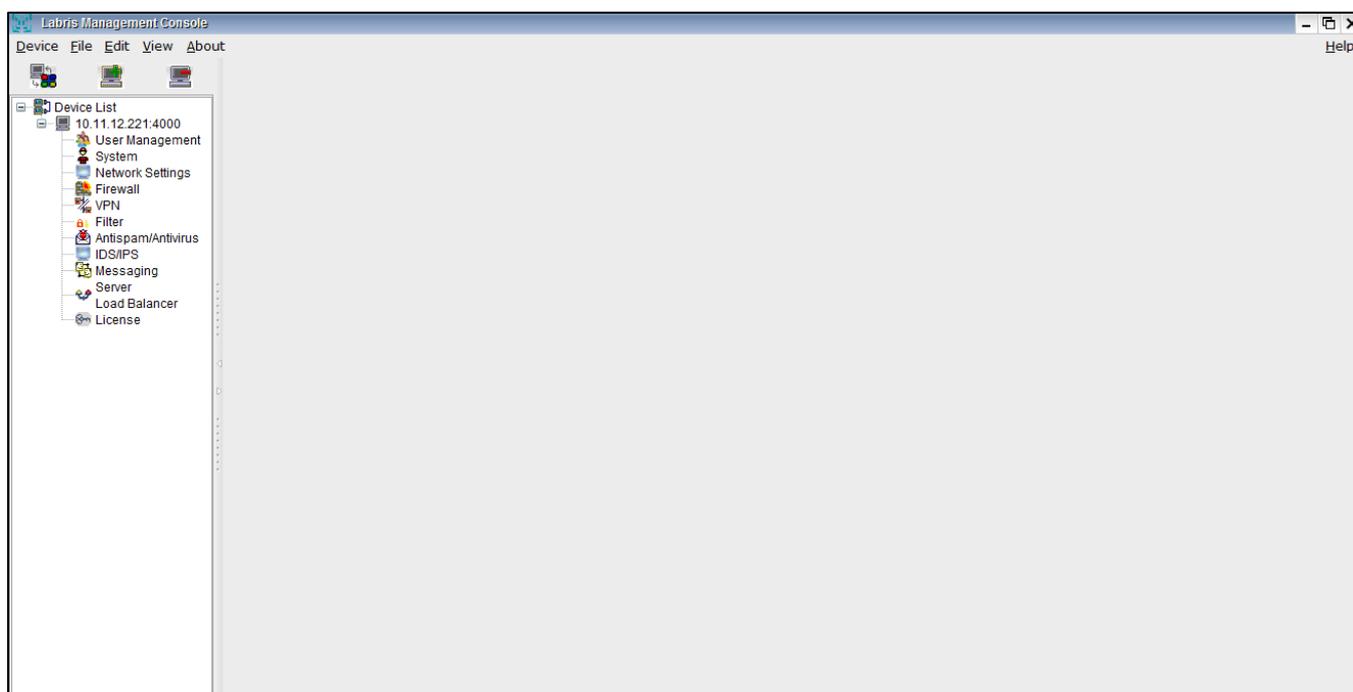
Click on **LMC** tab (Labris Management Console) from the Dashboard.



Note

• LMC requires JAVA addon. While opening the LMC, you will be offered certificate and security related information. Please accept the information and proceed as appropriate

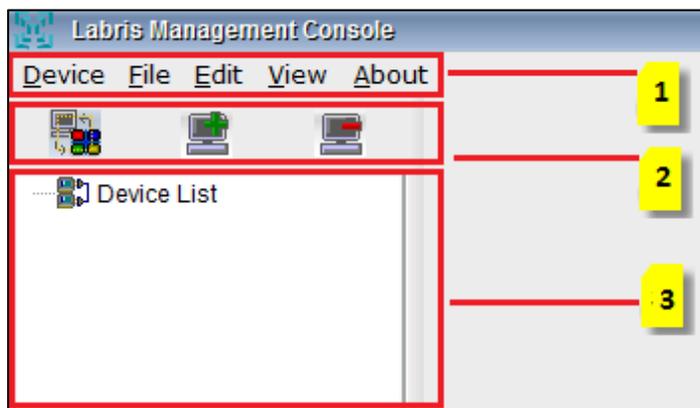
After all the validation and verification, the following LMC screen appears.



Now, we are ready to get connected to our appliance for further activities.

LMC Interface

This is the default LMC interface we get when we connect to the Labris Management Console



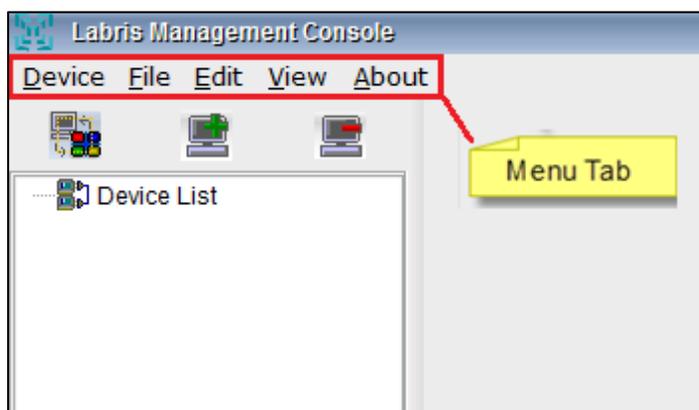
In Labris Management Console we will find three sections.

Section 1	Menu Tab	Menu Tab is a horizontal strip that contains lists of available menus
Section 2	Module	Module Tab consists of three short cut icons for Change view, Add module, Delete Module
Section 3	Server List	Server List consists of list of servers added to LMC

Menu

A **Menu Tab** is a region of a screen or application interface where drop down menus are displayed. A **Menu tab** is an integral graphical user interface (GUI) component in LMC.

In **Menu Tab** we will find **Device**, **File Menu**, **Edit Menu**, **View Menu** and **About Menu**.



Brief Summary about each of the parameters in Menu tab:

1	Device	Device helps to manage the server with different options
2	File Menu	File Menu offers commands for closing windows and exiting the current program. It contains commands relating to the handling of files, such as New, open, save, exit
3	Edit Menu	Edit Menu consists of LMC options and Certificates. We can manage Certificates by using this Menu
4	View Menu	View Menu provides two different options like Sort and GUI templates to view the content in different modes
5	About	About Menu gives information about LMC

File Menu

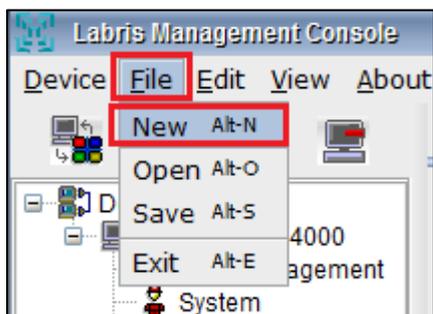
File Menu enables us to connect to new LMC, Open a file, save a file and Exit from the LMC

Under **File Menu** we find the following options

1	New	This option enables to connect to the New LMC
2	Open	This option enables to open an existing document which is located in the local machine
3	Save	This option enables to save the contents of a Files
4	Exit	This option enables to close and exit from the LMC

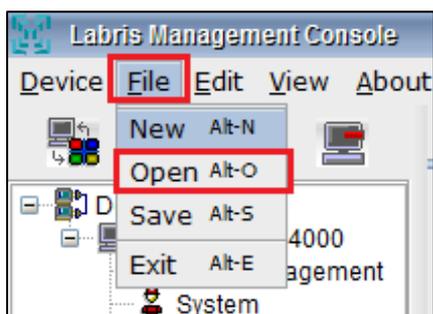
To open New Labris management console

1. Go to **File>New**
2. **New** Options helps us to connect to the **New** Labris Management Console (LMC).
When we click on New the following screen appears.

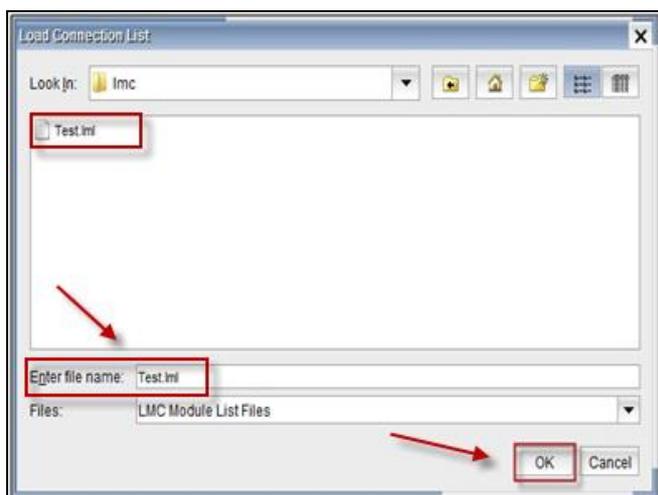


Opening an existing file using LMC

1. Go to **File>Open**
2. Using **Open** option we can open an existing file in LMC

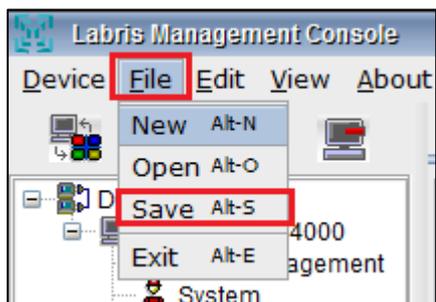


3. Browse the path of the file, Select the **File** and click **Ok**



Saving the files in LMC

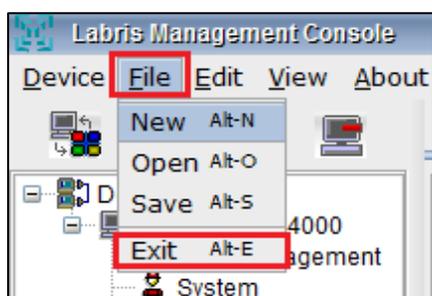
1. Go to **File>Save**



2. Using **Save** option we can save the files in LMC

Exiting from LMC console

1. Go to **File>Exit**
2. When we click on **Exit** it prompts us with a message **“Do you really want to exit?”**
3. Click on **“Yes”** to exit, or click on **“No”** to remain in the same LMC



Edit Menu

Edit Menu helps us to manage LMC options like change of Language (English & Turkish), settings etc. Certificate details can also be viewed and managed from Edit Menu

Under **Edit Menu** we find the following options

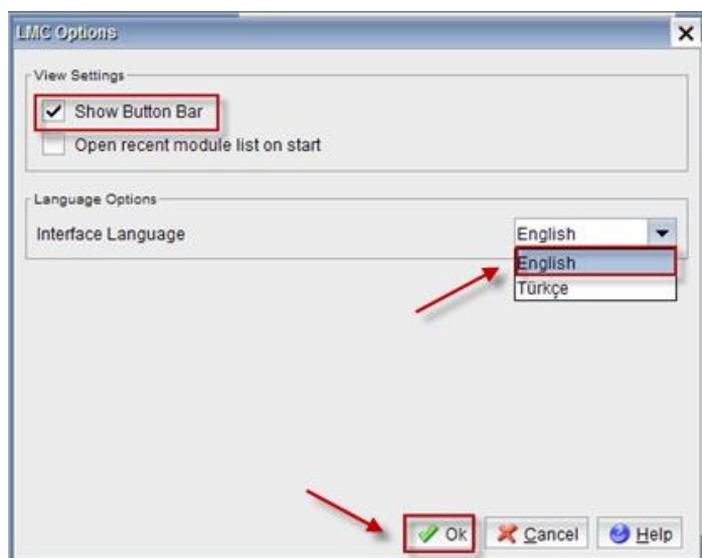
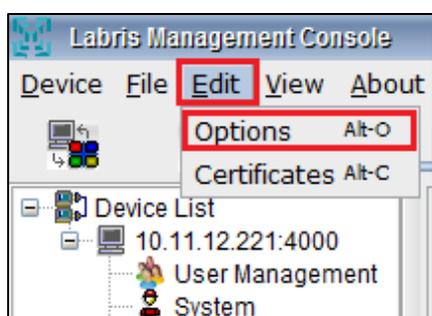
1	Options	This option helps us manage LMC options
2	Certificates	This option helps us to View details and manage certificates in LMC

Editing options in LMC

1. Go to **Edit>Options**

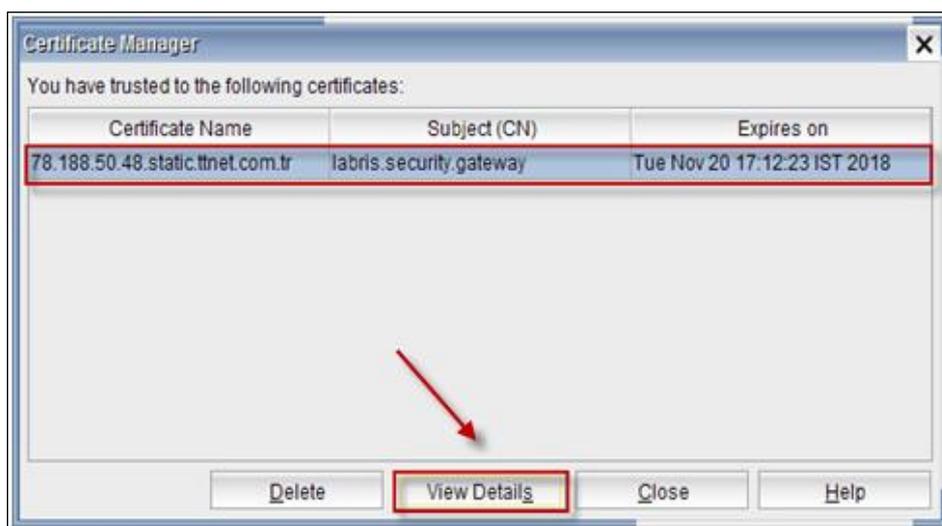
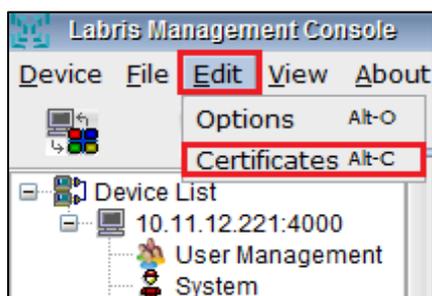
2. Using **Options** we can view settings and select interface language in LMC and click “**Ok**” to apply settings.

1	View settings	View Settings consists of show button bar and open module list on start. Choose appropriate option
2	Language options	This option enables us to choose preferred language either English or Turkish
3	OK	Select OK to apply the settings
4	Cancel	Select Cancel if we don't want to apply these settings
5	Help	Help options gives the related information about LMC options. It provides online help.



Certificates details in LMC

1. Go to **Edit>Certificates**
2. When we click on “**Certificates**” the Certificate manager console gets opened, where we can manage the Certificate using options like Delete, View Details, Close, Help



3. If we want to view the certificate details click on “**View Details**”. A screen appears as below with all necessary details of the certificate

1	Delete	Delete options helps us to delete the selected certificate from LMC
2	Close	Close option helps us to close the Certificate manager window
3	Help	Help Options gives information about the certificates and its related options



1	View public Key	This option helps us to view the public key
2	Cancel	This option helps us to close the Certificate details window

View Menu

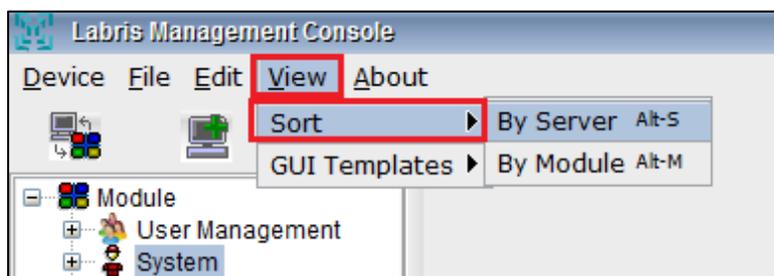
View Menu is one of the option in Menu Tab. **View Menu** helps us to view the contents in different modes depending on the options available in LMC.

Under **View Menu** we find the following options

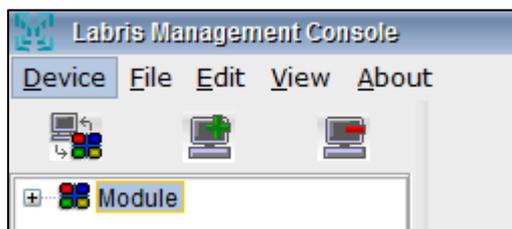
1	Sort	This option helps to sort by server or module
2	GUI Templates	This option helps to change the view of LMC to Aero mode or MacWin mode

Sorting Labris management console

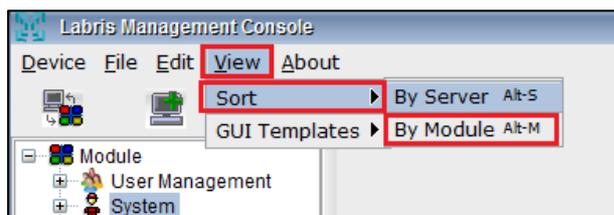
1. Go to **View>Sort> By Server**



2. When we sort **By Module** the view of the LMC appears as below

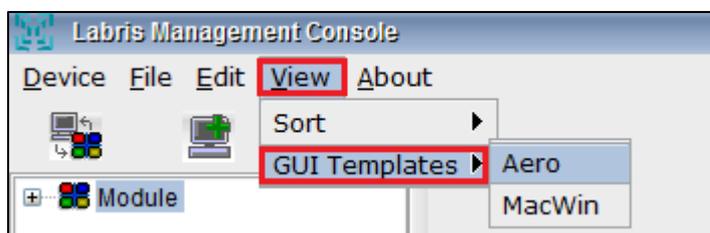


1. Go to **View>Sort> BY Module**
2. When we sort by module the view of the LMC changes as below



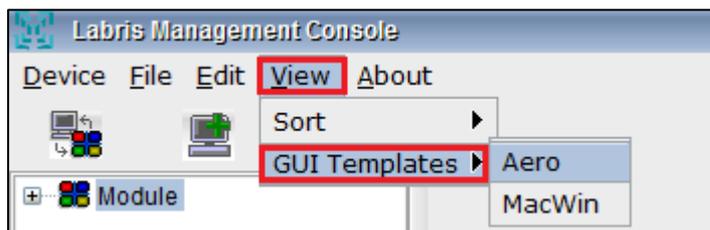
View using GUI Templates option in Aero Mode

1. Go to **View>GUI Templates> Aero**
2. When we click on Aero the view of the LMC appears as below



View using GUI Templates option in MacWin Mode

1. Go to **View>GUI Templates>MacWin**
2. When we click on **MacWin** the view of the LMC appears as below



Device Menu

Device Menu provides us with different options like Add, Remove, Connect, Disconnect server from LMC. We can manage the server using the options in **Device Menu**

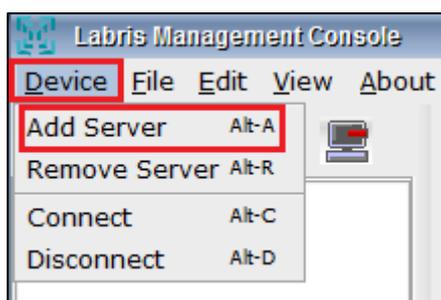
Under **Device Menu** we find the following options

1	Add Server	This option helps to Add server to the LMC
2	Remove Server	This option helps us to Remove server from the LMC
3	Connect	This option helps to Connect the server to the LMC
4	Disconnect	This option helps to Disconnect the server from LMC

Add Modules from Server Menu

To manage and configure the appliances we will add Server to the LMC.

1. Go to **Device>Add server**

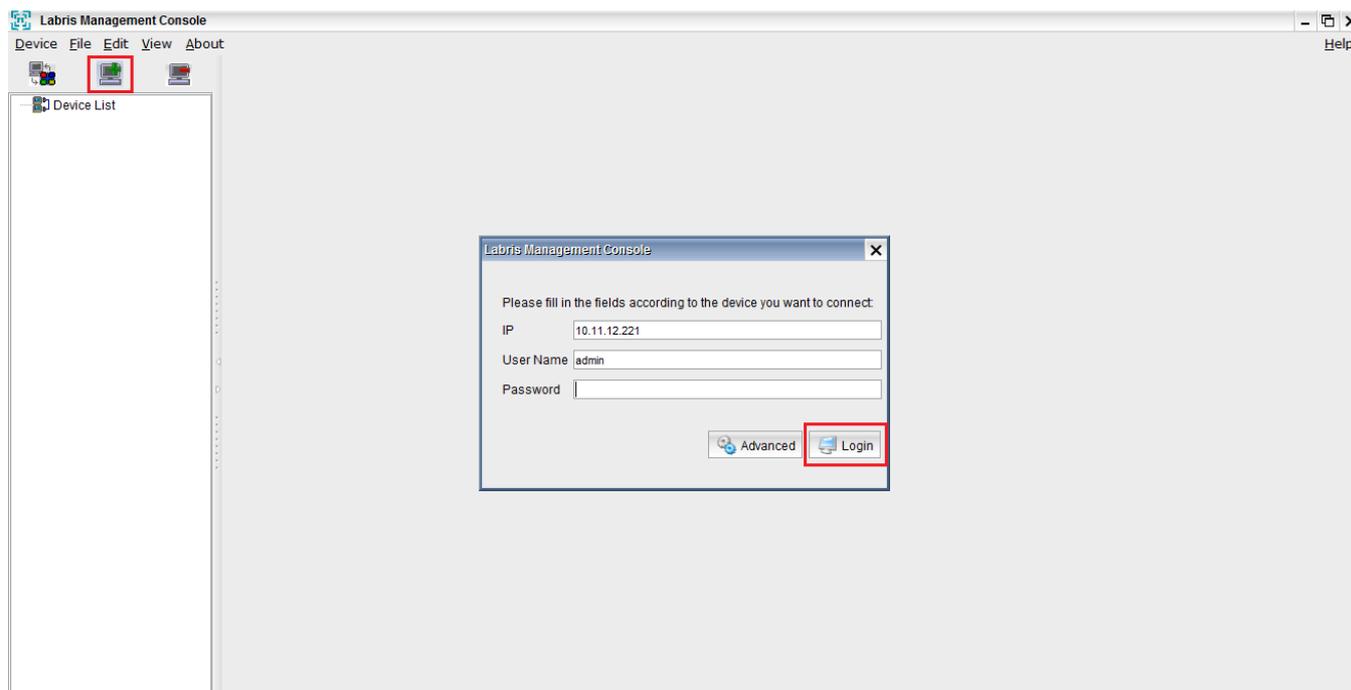


Note

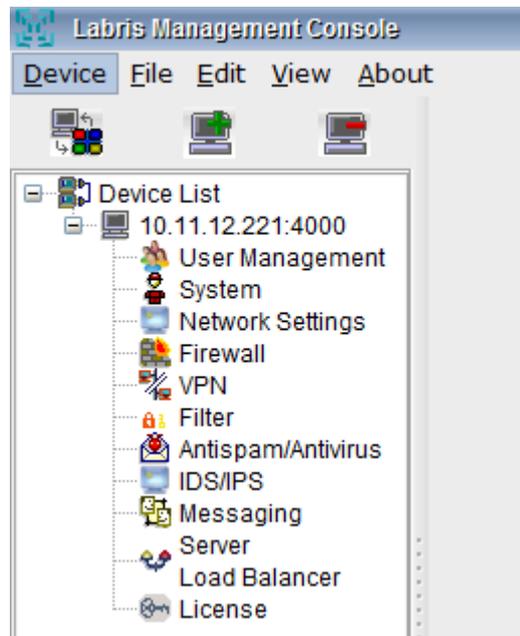
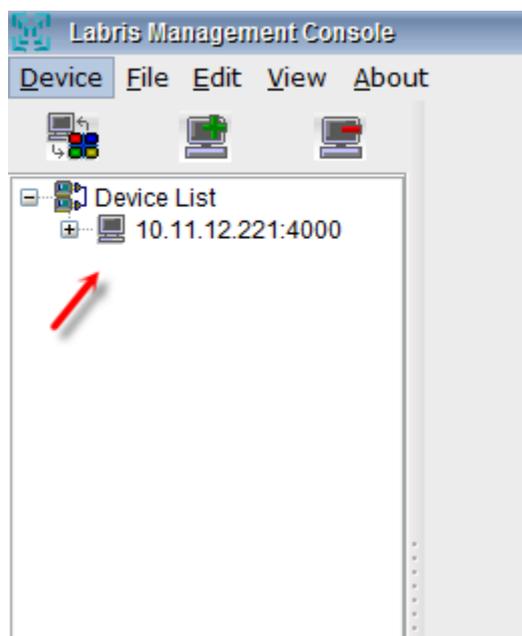
- We can even choose a short cut icon under Module to **Add server**

After clicking on the “**Add Server**”, you will see the “**Add Devices from Server**” menu. . Type in the appropriate Default **Username** and Default **Password** and click on “**Authenticate**” button.

Notice & verify your appliance’s IP address in the “**Add Devices from Server**” menu and click on the “**Login**” button as shown below



2. After successful authentication process, you will notice your new appliance appearing on LMC's Server list as shown in the following images.



User Management

User Management system providing administrators with the ability to effectively manage users on the network. It is an authentication feature that provides administrators with the ability to identify and control the state of users logged into the network.

It is not limited to, the ability to query and filter users that are currently logged into the network, but also manually log out users, and control users login counts and login times.



Viewing Options in User Management

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

1	Connect	It enables Users, Groups & WAUTH to connect to the LMC
2	Disconnect	It enables Users, Groups & WAUTH to disconnect from LMC
3	Properties	It helps us to view properties of User Management in LMC

15. Users

Users Tab in LMC enables us to **Add** new User, **Edit** existing Users, **Delete** User in User Management Section in LMC.

When we click on Users tab all the existing Users are displayed with fields **User Name, Name Surname, Source, Domain, Global and Note**

Adding User

Add tab in user management helps us to **Add a new user** to the LMC Appliance

Click on **Add tab** to add a New User

Users						
Users Groups Identity Integration WAUTH Quota						
Select All <input type="checkbox"/> Delete <input type="checkbox"/> Edit <input type="checkbox"/> Add <input type="button" value="Add"/>						
	User Name	Name Surname	Source	Domain	Global	Note
<input type="checkbox"/>	testuser2745	testuser2745	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser7610	testuser7610	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser486	testuser486	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser4500	testuser4500	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser3983	testuser3983	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser9446	testuser9446	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser2633	testuser2633	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser7236	testuser7236	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser9795	testuser9795	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser8720	testuser8720	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser3928	testuser3928	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser7577	testuser7577	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	

Add User ✕

1

2

3

4

5

6 Global

7

Select Group 8

Quota Policy 9

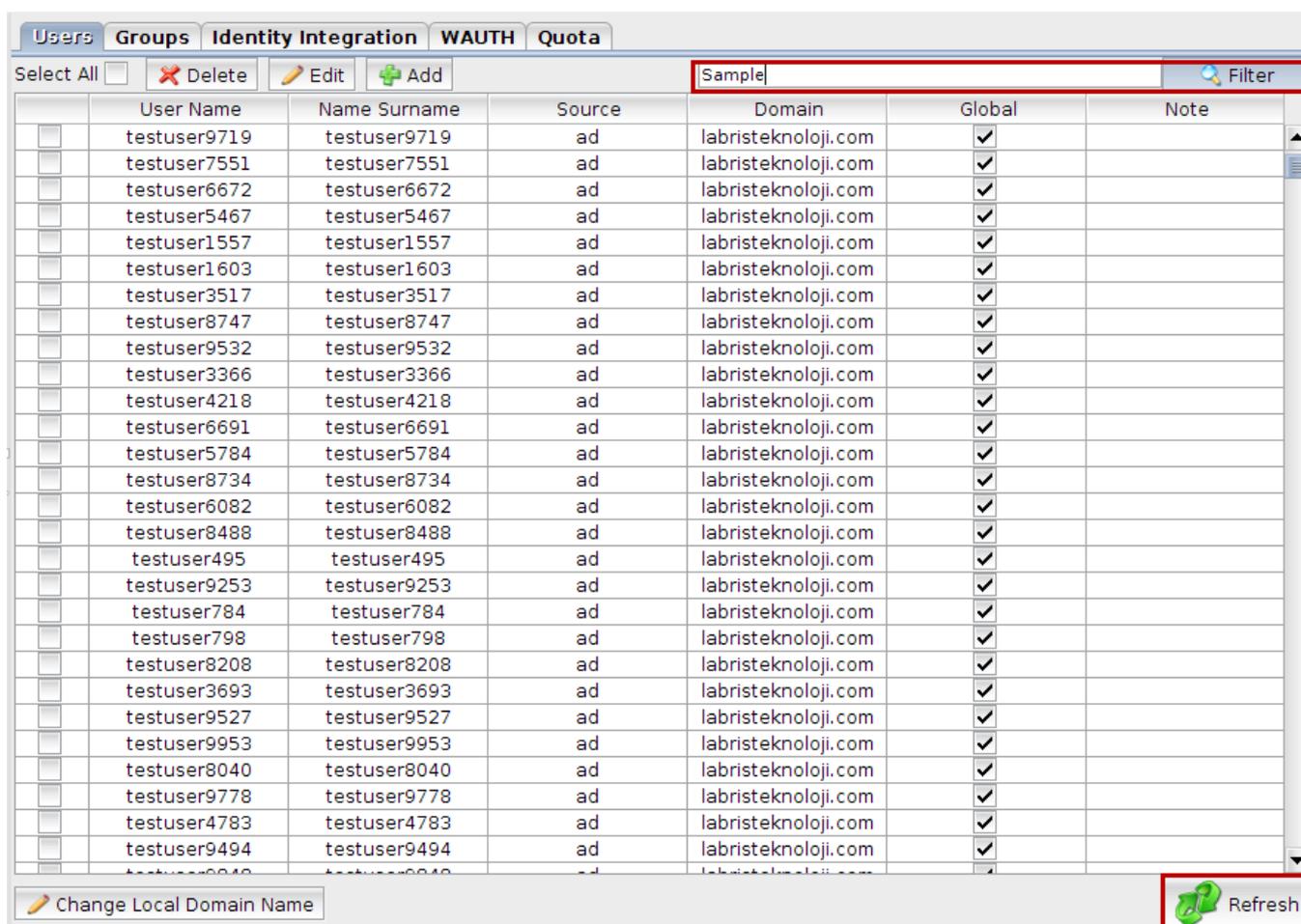
These are the inputs for adding New User

1	User Name	Type the name of the new User
2	Name Surname	Type the Surname of the new User
3	Password	Type Password of the new User s
4	Password Again	Re type the same Password for confirmation
5	Domain	By default Slave is being selected in Domain
6	Global	It is deemed central management. In the case of the device is the same as the firm's global projects marking more than one user is deemed to be used every time a user was created in the location is achievable UTM device.
7	Comment	Type reason for the User creation (Optional)
8	Select Group	You can make a user, member of a group
9	Select Quota Policy	You can choose a quota policy for user

Global, Comment and Select Group fields can be selected according to the User requirement and click on **OK** to apply these settings.



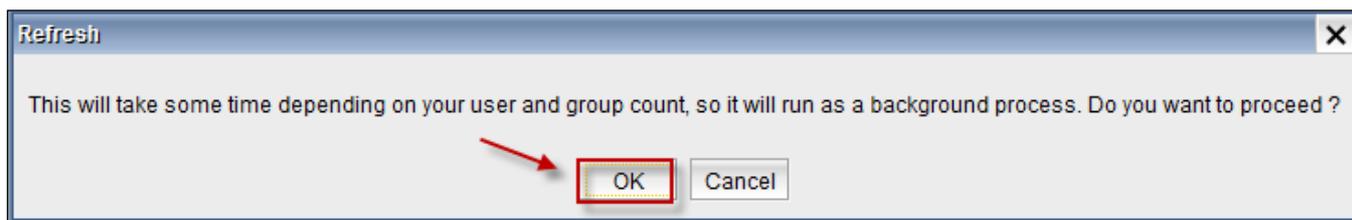
Type the name of the User in the **Filter Tab** to check whether the user is added to the list or not. If the user is not added click on **Refresh Tab**



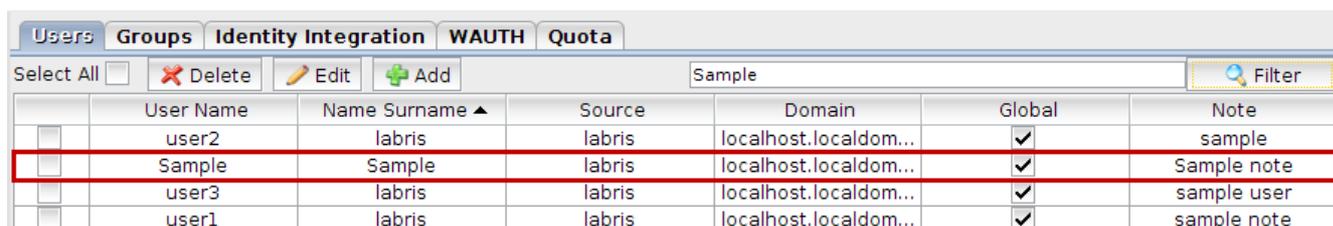
The screenshot shows the 'Users' management interface. At the top, there are tabs for 'Users', 'Groups', 'Identity Integration', 'WAUTH', and 'Quota'. Below the tabs are buttons for 'Select All', 'Delete', 'Edit', and 'Add'. A search bar labeled 'Sample' is next to a 'Filter' button. The main area is a table with columns: 'User Name', 'Name Surname', 'Source', 'Domain', 'Global', and 'Note'. The table contains 25 rows of test users, all with 'ad' as the source and 'labristeknoloji.com' as the domain. A 'Refresh' button with a green circular arrow icon is located at the bottom right of the interface.

	User Name	Name Surname	Source	Domain	Global	Note
<input type="checkbox"/>	testuser9719	testuser9719	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser7551	testuser7551	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser6672	testuser6672	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser5467	testuser5467	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser1557	testuser1557	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser1603	testuser1603	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser3517	testuser3517	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser8747	testuser8747	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser9532	testuser9532	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser3366	testuser3366	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser4218	testuser4218	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser6691	testuser6691	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser5784	testuser5784	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser8734	testuser8734	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser6082	testuser6082	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser8488	testuser8488	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser495	testuser495	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser9253	testuser9253	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser784	testuser784	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser798	testuser798	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser8208	testuser8208	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser3693	testuser3693	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser9527	testuser9527	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser9953	testuser9953	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser8040	testuser8040	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser9778	testuser9778	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser4783	testuser4783	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser9494	testuser9494	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	

Below screen appears stating that it takes some time to Refresh, click **OK** to continue the **Refresh** process



After completing Refresh process type the name of the User in the **Filter tab**, then you can notice the **New User** displaying in the User's list



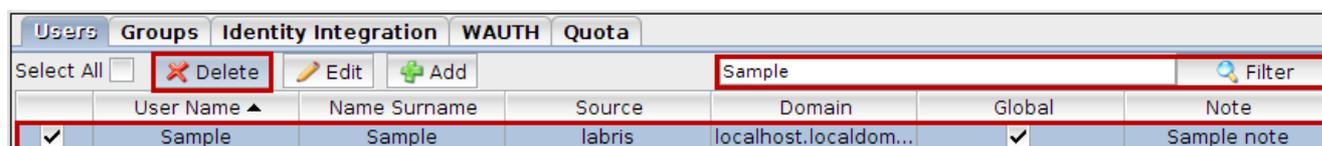
The screenshot shows the "Users" tab in a management interface. At the top, there are tabs for "Users", "Groups", "Identity Integration", "WAUTH", and "Quota". Below the tabs are buttons for "Select All", "Delete", "Edit", and "Add". A search box contains the text "Sample" and a "Filter" button. Below this is a table with columns: "User Name", "Name Surname", "Source", "Domain", "Global", and "Note".

	User Name	Name Surname ▲	Source	Domain	Global	Note
<input type="checkbox"/>	user2	labris	labris	localhost.localdom...	<input checked="" type="checkbox"/>	sample
<input checked="" type="checkbox"/>	Sample	Sample	labris	localhost.localdom...	<input checked="" type="checkbox"/>	Sample note
<input type="checkbox"/>	user3	labris	labris	localhost.localdom...	<input checked="" type="checkbox"/>	sample user
<input type="checkbox"/>	user1	labris	labris	localhost.localdom...	<input checked="" type="checkbox"/>	sample note

Deleting User

Delete Tab in user management helps us to **delete** the **user** permanently from the LMC Appliance

Type the name of the User which you want to delete in the Filter tab, Select the User and click on **Delete Tab**



The screenshot shows the "Users" tab in a management interface. The "Delete" button is highlighted with a red box. The search box contains the text "Sample" and a "Filter" button. Below this is a table with columns: "User Name", "Name Surname", "Source", "Domain", "Global", and "Note".

	User Name ▲	Name Surname	Source	Domain	Global	Note
<input checked="" type="checkbox"/>	Sample	Sample	labris	localhost.localdom...	<input checked="" type="checkbox"/>	Sample note

Then the below screen appears, Click **OK** to delete a User in User Management in LMC



It takes some time to **Delete** an **User** from User's list



Below screen gives information that the selected User is deleted successfully. Click **OK**



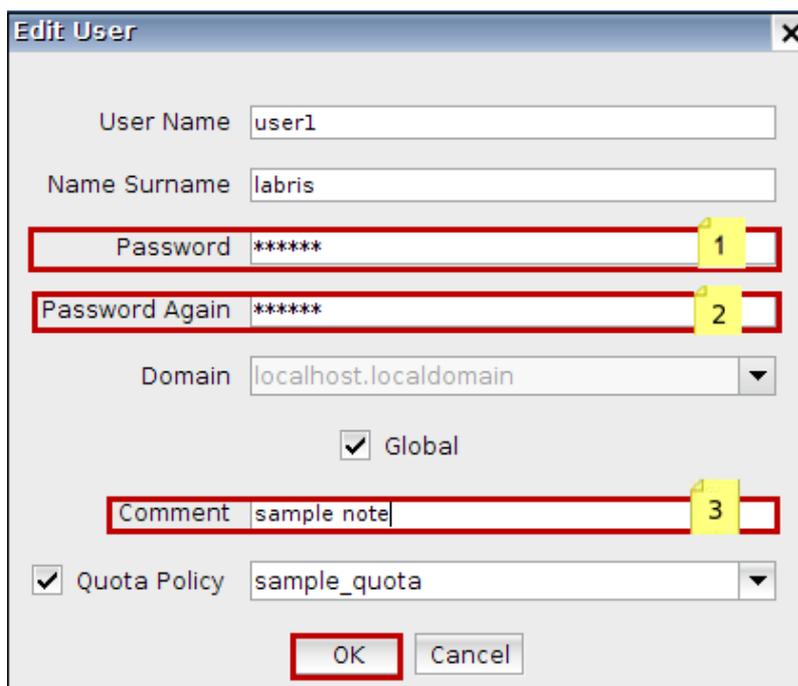
Changing password / Editing User

Select a User from the User's list and click on

Edit Tab

Users						
Users Groups Identity Integration WAUTH Quota						
Select All <input type="checkbox"/> Delete <input type="checkbox"/> Edit <input type="checkbox"/> Add <input type="checkbox"/> Filter <input type="text"/>						
	User Name	Name Surname	Source	Domain	Global	Note
<input type="checkbox"/>	user3	labris	labris	localhost.localdo...	<input checked="" type="checkbox"/>	sample user
<input type="checkbox"/>	user2	labris	labris	localhost.localdo...	<input checked="" type="checkbox"/>	sample
<input checked="" type="checkbox"/>	user1	labris	labris	localhost.localdo...	<input checked="" type="checkbox"/>	sample note
<input type="checkbox"/>	testuser9999	testuser9999	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser9998	testuser9998	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	testuser9997	testuser9997	ad	labristeknoloji.com	<input checked="" type="checkbox"/>	

Edit option helps us to change the password of the existing User and edit the comment.



User Name: user1
Name Surname: labris
Password: ***** (1)
Password Again: ***** (2)
Domain: localhost.localdomain
 Global
Comment: sample note (3)
 Quota Policy: sample_quota
OK Cancel

1	Password	Type new Password of the User
2	Password Again	Re Type new Password again for confirmation
3	Comment	Type reason for the User creation (Optional)

Click **OK** to apply these settings.

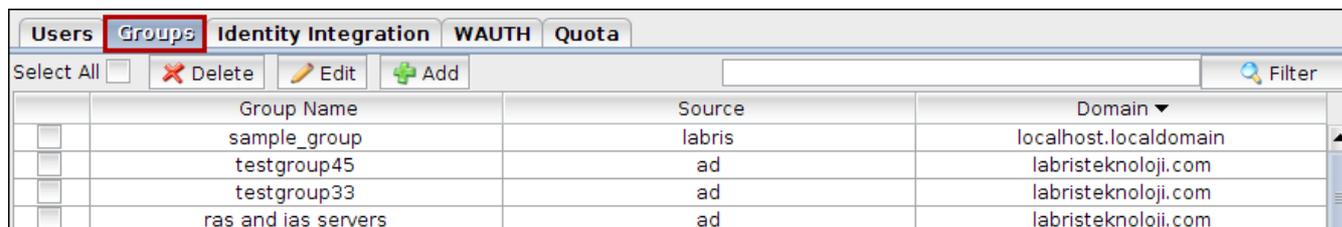


16. Groups

Groups permit us to easily assign to all members of a group abilities in a space that are specified to that Group. After creating a Group we are able to manage its membership by adding or deleting Users to that Group. All the created Users may be a member of any Group with Guest abilities. We can have same Users in multiple Groups.

Groups Tab in LMC enables us to **Add New Group**, **Edit existing Groups**, **Delete Groups** in User Management Section in LMC.

When we click on **Groups Tab** all the existing groups are displayed with the fields **Group Name**, **Source**, **Domain**.

A screenshot of the LMC Groups Tab interface. The "Groups" tab is selected and highlighted with a red box. The interface includes a toolbar with "Delete", "Edit", and "Add" buttons, and a search filter. Below is a table with columns for Group Name, Source, and Domain.

	Group Name	Source	Domain
<input type="checkbox"/>	sample_group	labris	localhost.localdomain
<input type="checkbox"/>	testgroup45	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup33	ad	labristeknoloji.com
<input type="checkbox"/>	ras and ias servers	ad	labristeknoloji.com

Adding Group

Users Groups Identity Integration WAUTH Quota				
Select All <input type="checkbox"/>	Delete	Edit	Add	Filter
	Group Name	Source	Domain ▼	
<input type="checkbox"/>	sample_group	labris	localhost.localdomain	
<input type="checkbox"/>	testgroup45	ad	labristeknoloji.com	
<input type="checkbox"/>	testgroup33	ad	labristeknoloji.com	
<input type="checkbox"/>	ras and ias servers	ad	labristeknoloji.com	
<input type="checkbox"/>	incoming forest trust builders	ad	labristeknoloji.com	
<input type="checkbox"/>	testgroup46	ad	labristeknoloji.com	
<input type="checkbox"/>	enterprise admins	ad	labristeknoloji.com	
<input type="checkbox"/>	testgroup43	ad	labristeknoloji.com	

Click on **Add Tab** to add **New Group** to the Groups in User Management

Below screen appears with **Group Name & Group Configuration**.

Add Group

Group Name
 Domain: Quota Policy

Group Configuration

All Users and Groups 1

Name	Type	Source	Domain
testuser2745	user	ad	labristeknoloji...
testuser7610	user	ad	labristeknoloji...
testuser486	user	ad	labristeknoloji...
testuser4500	user	ad	labristeknoloji...
testuser3983	user	ad	labristeknoloji...
testuser9446	user	ad	labristeknoloji...
testuser2633	user	ad	labristeknoloji...
testuser7236	user	ad	labristeknoloji...
testuser9795	user	ad	labristeknoloji...
testuser8720	user	ad	labristeknoloji...

3

4

Group Components 2

Name	Type	Source	Domain

Group Name consists of two fields **Group Name & Domain**.

1	Group Name	Type name of the New Group
2	Domain	In this field slave is selected by default

Group Configuration consists of two fields **All Users and Groups** and **Group Components**.

1	All Users and Groups	All the users and groups are displayed in this field
2	Group Components	Users in specific Group are displayed in this field
3		Click this icon to add Users in to Group Components

4		Click this icon to delete Users from the Group Components
---	---	---

Click **OK** to add New Group to the Group's list.

It takes some time to apply changes.



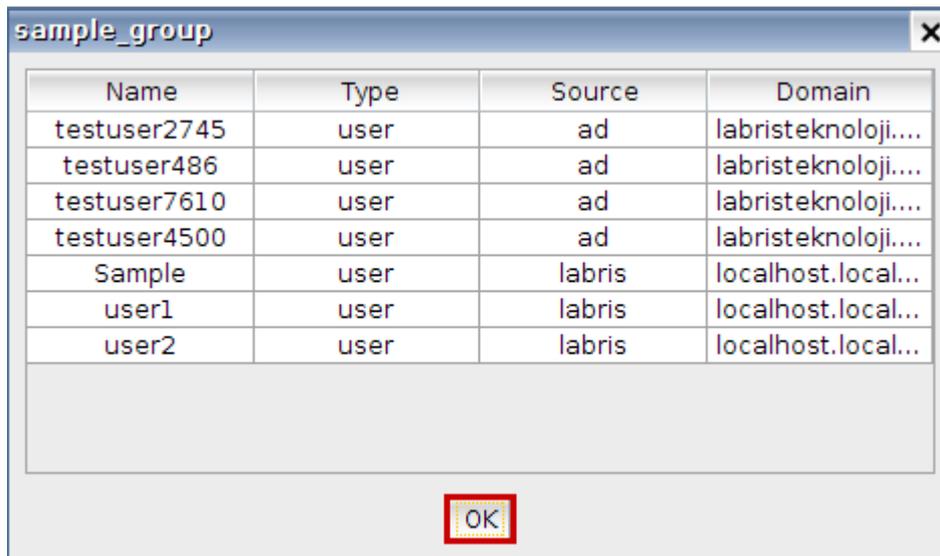
Type the **New Group name** in the **Filter tab** and click **Refresh** to find out the **New Group** in the **Group's** list is added or not.

	Group Name	Source	Domain
<input type="checkbox"/>	testgroup11	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup12	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup13	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup14	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup15	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup16	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup17	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup18	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup19	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup2	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup20	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup21	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup22	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup23	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup24	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup25	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup26	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup27	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup28	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup29	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup3	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup30	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup31	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup32	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup33	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup34	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup35	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup36	ad	labristeknoloji.com

Now you can notice the **newly added Group** in the **Group's** list. Right click on the **Group** and select **Show Group**.

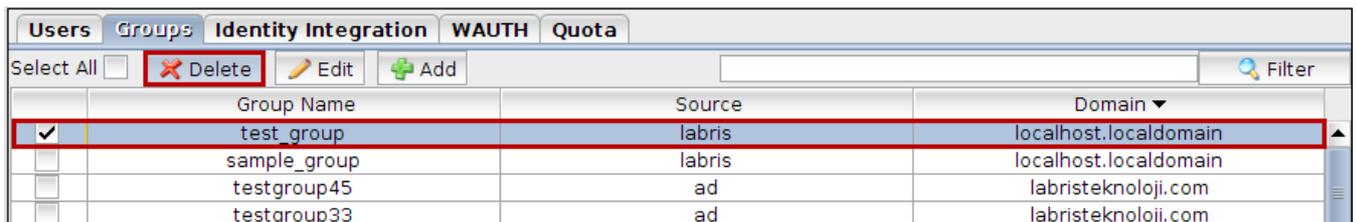
	Group Name	Source	Domain
<input type="checkbox"/>	sample_group	labris	localhost.localdomain
<input type="checkbox"/>	windows authorization access group	ad	labristeknoloji.com
<input type="checkbox"/>	users	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup99	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup98	ad	labristeknoloji.com

When you click on **Show Group**, Users in that **group** are displayed. Click **OK** to close the current tab.

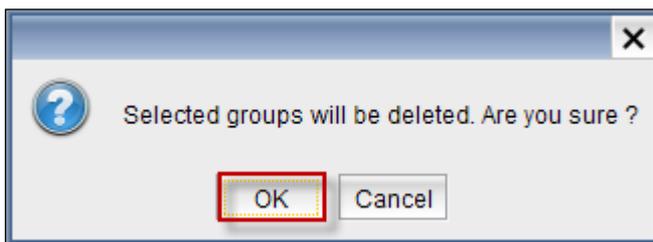


Deleting Group

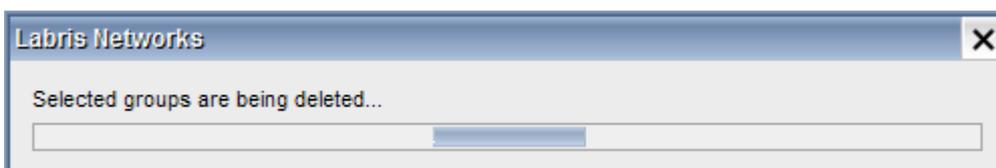
Select the Group from the Group's list and click on **Delete** Tab.



Warning screen is displayed; Click **OK** to delete a Group from the LMC.



Deleting process is in progress.

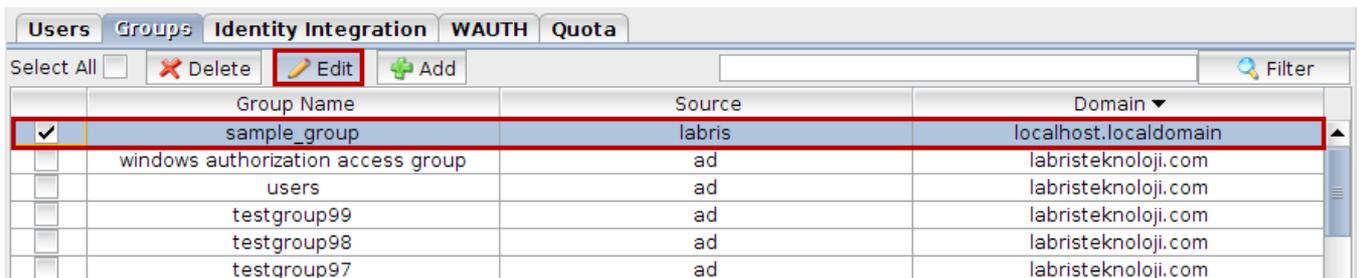


Below screen appears stating that the selected Group is **Deleted** successfully & click **OK** to close the current tab



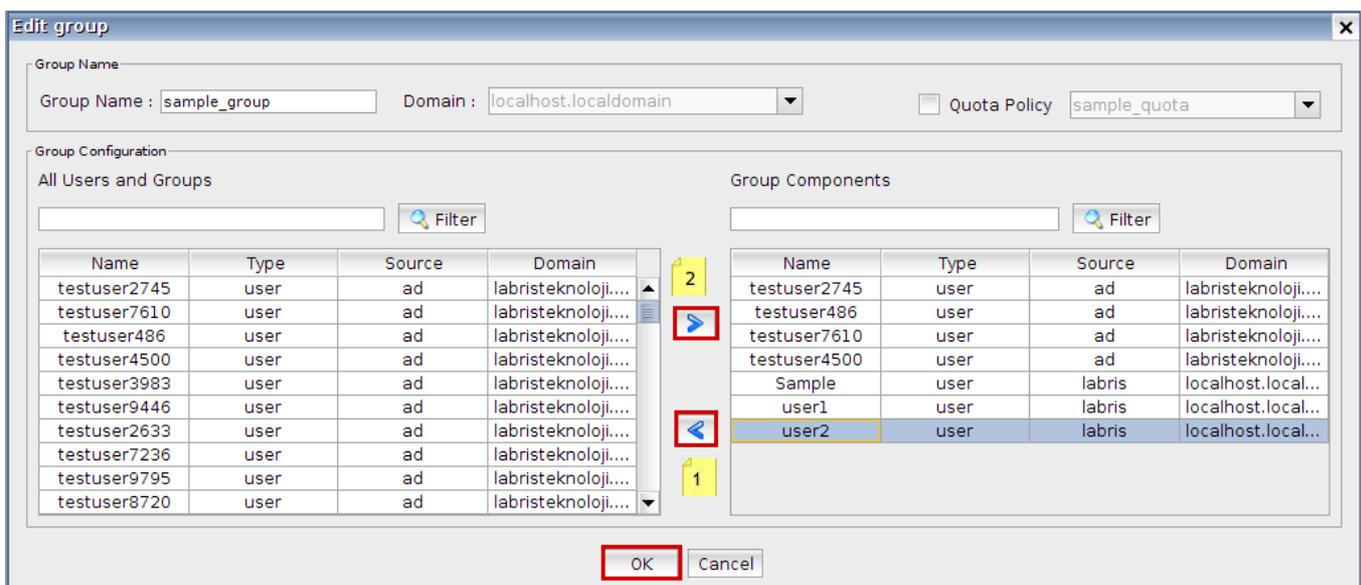
Editing Group

Select the **Group** which you want to edit from the list and click on **Edit Tab**.

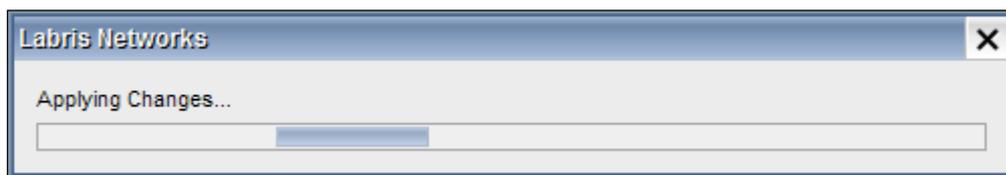


Select the User from the **Group** components list and click on the **icon 1** to remove User from the **Group** Components and click **OK**

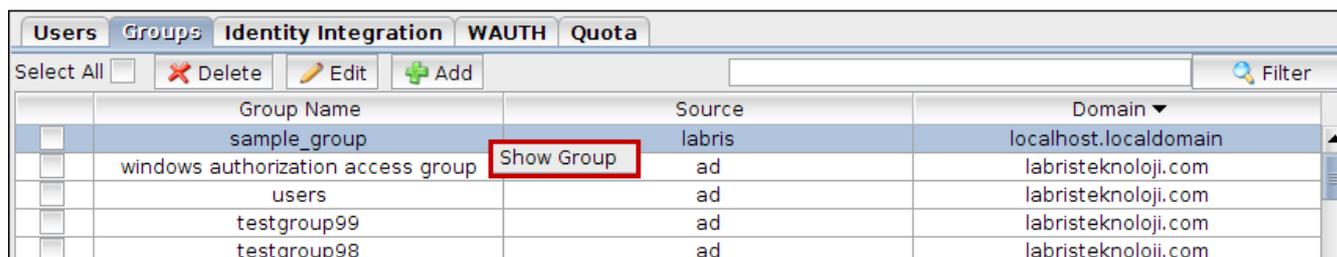
Select the **User** from All Users and **Groups** field and click on the **icon 2** to add Users in to Group Components list and click **OK**



It takes some time to apply the changes.

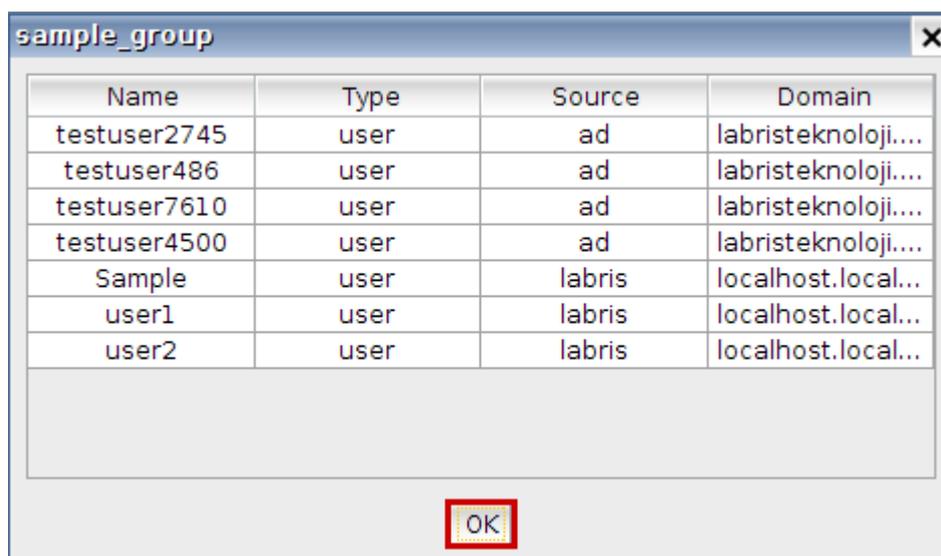


To notice changes made to the **Group** right click on the User and select **Show Group**



	Group Name	Source	Domain
<input type="checkbox"/>	sample_group	labris	localhost.localdomain
<input type="checkbox"/>	windows authorization access group	ad	labristeknoloji.com
<input type="checkbox"/>	users	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup99	ad	labristeknoloji.com
<input type="checkbox"/>	testgroup98	ad	labristeknoloji.com

Then information about **Group** Components are displayed and click **OK** to close the current tab.

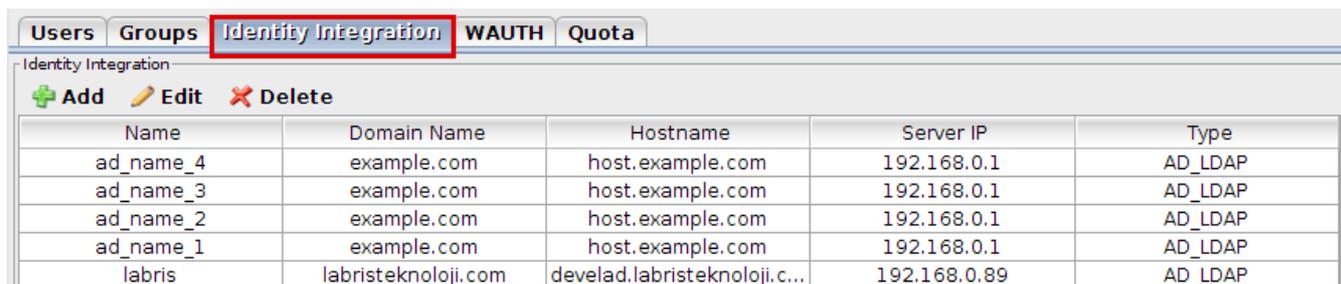


Name	Type	Source	Domain
testuser2745	user	ad	labristeknoloji....
testuser486	user	ad	labristeknoloji....
testuser7610	user	ad	labristeknoloji....
testuser4500	user	ad	labristeknoloji....
Sample	user	labris	localhost.local...
user1	user	labris	localhost.local...
user2	user	labris	localhost.local...

17. Identity Integration

Identity Integration Tab in LMC enables us to **Add** new Identity, **Edit** existing Identities, **Delete** Identity in User Management Section in LMC.

When we click on Identity Integration tab all the existing Identity Integrations are displayed with fields **Name, Domain Name, Hostname, Server IP, Type**.



Name	Domain Name	Hostname	Server IP	Type
ad_name_4	example.com	host.example.com	192.168.0.1	AD_LDAP
ad_name_3	example.com	host.example.com	192.168.0.1	AD_LDAP
ad_name_2	example.com	host.example.com	192.168.0.1	AD_LDAP
ad_name_1	example.com	host.example.com	192.168.0.1	AD_LDAP
labris	labristeknoloji.com	develad.labristeknoloji.c...	192.168.0.89	AD_LDAP

Adding Identity

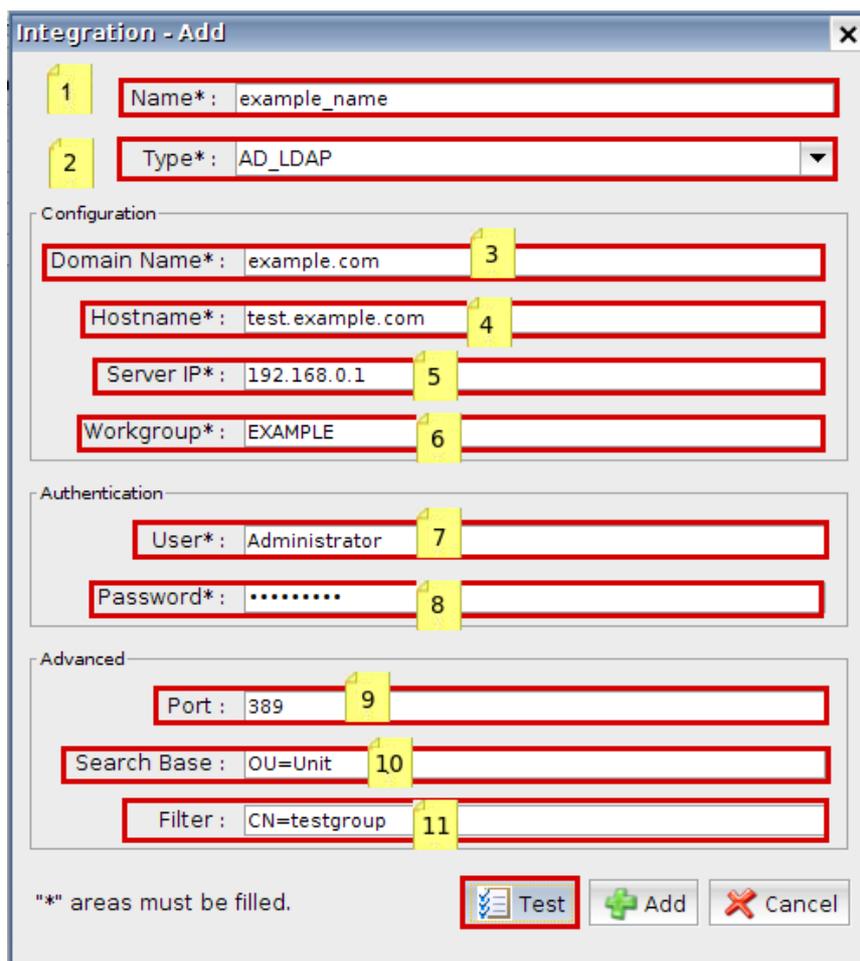
Add tab in identity integration helps us to **Add** a **new integration** to the LMC Appliance

Click on **Add tab** to add a New Identity Integration.



Name	Domain Name	Hostname	Server IP	Type
ad_name_4	example.com	host.example.com	192.168.0.1	AD_LDAP
ad_name_3	example.com	host.example.com	192.168.0.1	AD_LDAP
ad_name_2	example.com	host.example.com	192.168.0.1	AD_LDAP
ad_name_1	example.com	host.example.com	192.168.0.1	AD_LDAP
labris	labristeknoloji.com	develad.labristeknoloji.c...	192.168.0.89	AD_LDAP

You can type credentials and test without integration using **Test** button below.



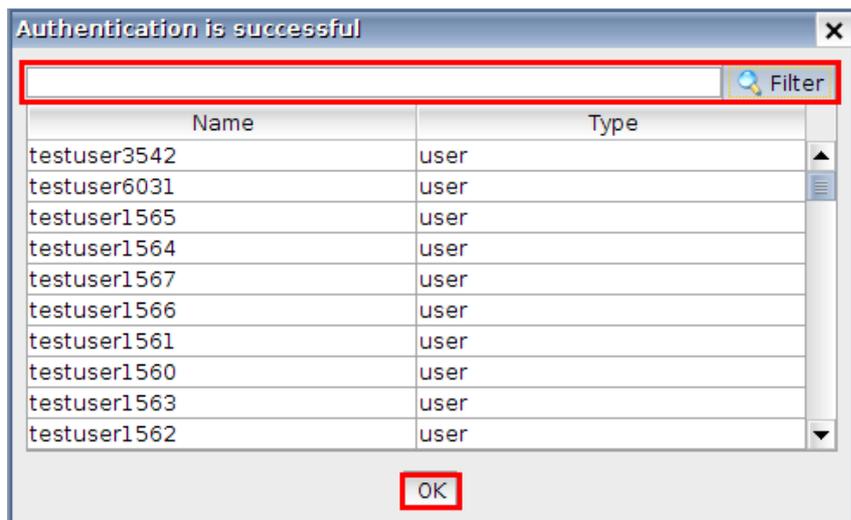
"*\" areas must be filled.

Test Add Cancel

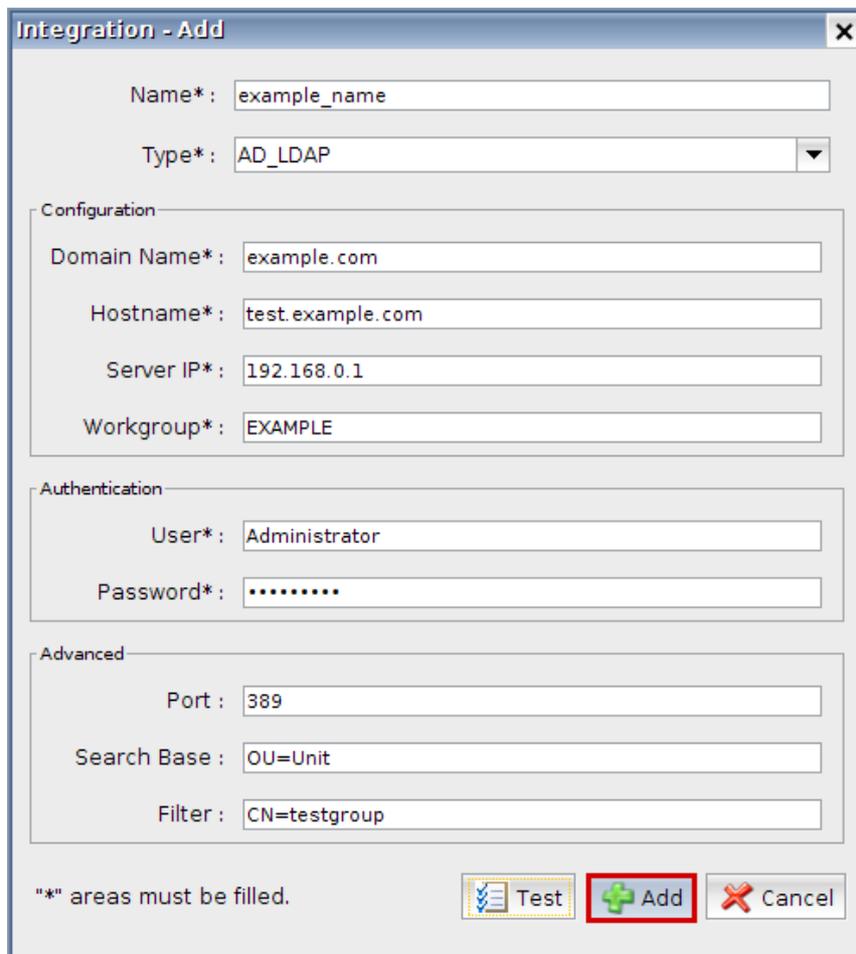
These are the inputs for New Integration:

1	Name	Unique name for integration
2	Type	Server configuration type
3	Domain Name	Domain Name
4	Hostname	Hostname of Server
5	Server IP	IP Address of Server
6	Workgroup	Workgroup of User
7	User	Username
8	Password	Password
9	Port	Connection port
10	Search Base	Starting point for the search instead of the default
11	Filter	Conditions for entries

If credentials are correct, you can see queried users. Using **Filter** button, you can filter queried users.

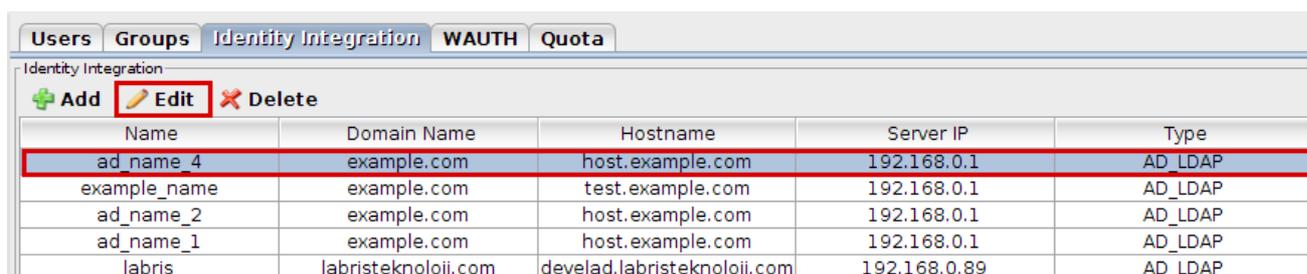


After writing necessary configurations, you can add integration with the **Add** button below.



Editing Identity

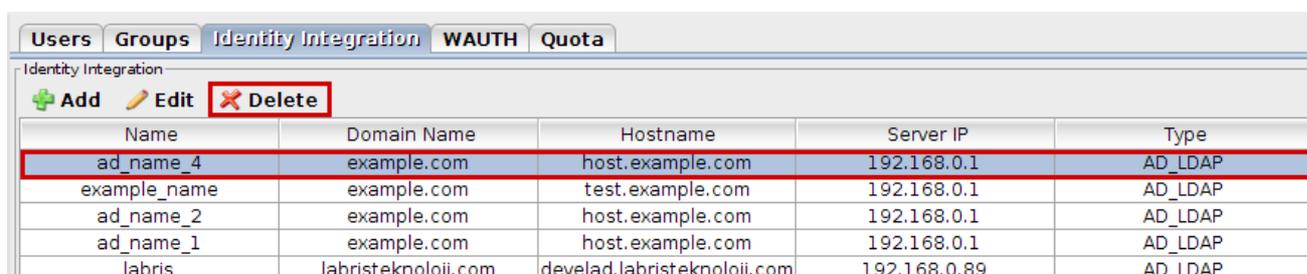
A previously added Integration can be edited by choosing it and clicking the **Edit Button**.



Name	Domain Name	Hostname	Server IP	Type
ad_name_4	example.com	host.example.com	192.168.0.1	AD_LDAP
example_name	example.com	test.example.com	192.168.0.1	AD_LDAP
ad_name_2	example.com	host.example.com	192.168.0.1	AD_LDAP
ad_name_1	example.com	host.example.com	192.168.0.1	AD_LDAP
labris	labristeknoloji.com	develad.labristeknoloji.com	192.168.0.89	AD_LDAP

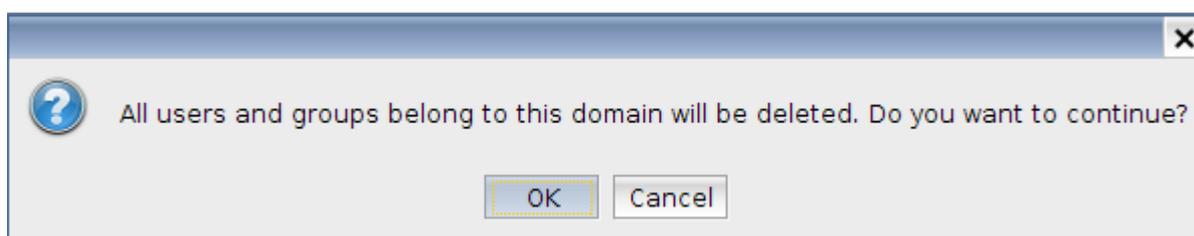
Deleting Identity

Select the Integration from the Integrations list and click on **Delete Tab**.



Name	Domain Name	Hostname	Server IP	Type
ad_name_4	example.com	host.example.com	192.168.0.1	AD_LDAP
example_name	example.com	test.example.com	192.168.0.1	AD_LDAP
ad_name_2	example.com	host.example.com	192.168.0.1	AD_LDAP
ad_name_1	example.com	host.example.com	192.168.0.1	AD_LDAP
labris	labristeknoloji.com	develad.labristeknoloji.com	192.168.0.89	AD_LDAP

Warning will be shown after clicking delete button.



If you press **OK** progress bar will be shown. This might take some time.



Advanced Options for Identity Integration

The screenshot shows an 'Advanced' configuration panel with three input fields:

- Port :** A text box containing the value '0'.
- Search Base :** A text box containing the value 'OU=Ankara, OU=istanbul'.
- Filter :** A text box containing the value 'memberOf=CN=testgroup,OU=test,DC=domain,DC=com'.

Port: Port number between 0-65535 which will be used to connect to the server. Default value is 0 which is actually translated into default port of Server.

Search base: The starting point for the search of the users and groups. If it is empty, default search base which consists of domain name will be used. If not, it is concatenated to the default search base.

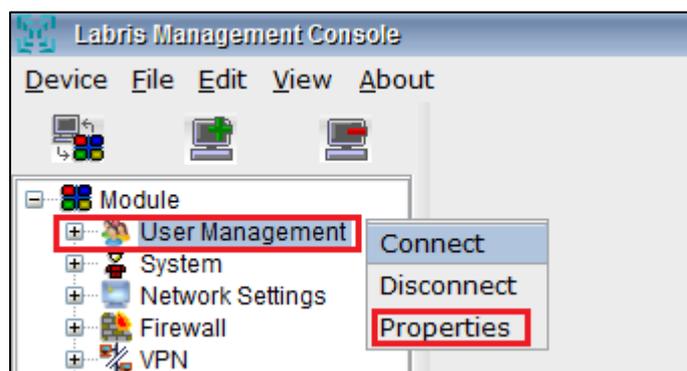
For example if "OU=Ankara" is written on the search base and domain name is "example.com", it will be translated into "OU=Ankara, DC=example, DC=com".

Filter: Conditions for searching users and groups which should conform to the string representation for search filters as defined in RFC 4515.

For example: "&(objectClass=Person)(primaryGroupId=513)".

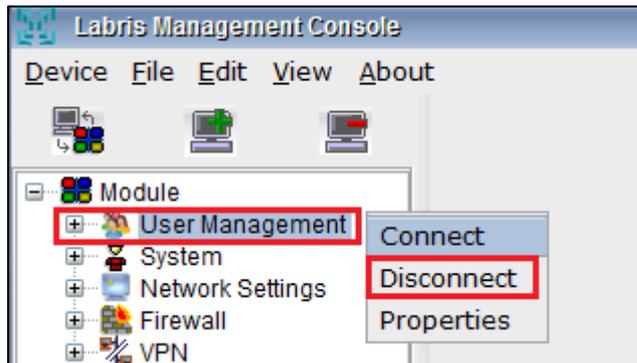
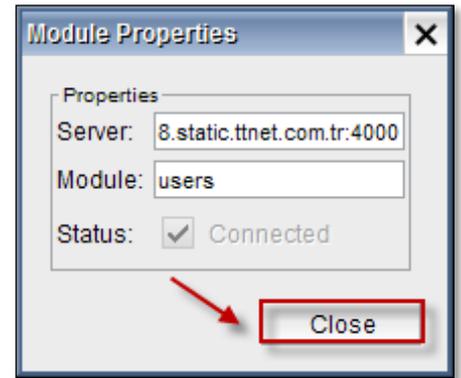
Other Options in User Management

Right click on the **User Management** and select **Properties**.



All the properties of the module are displayed in this screen.
Click **Close** to move out of this tab.

Give right click on the **User Management** Tab and select **Disconnect** to disconnect from the **User Management**.



WAUTH

WAuth is the module used for user authentication and guest authentication. WAuth is enabled by interface and supports specific exceptions.

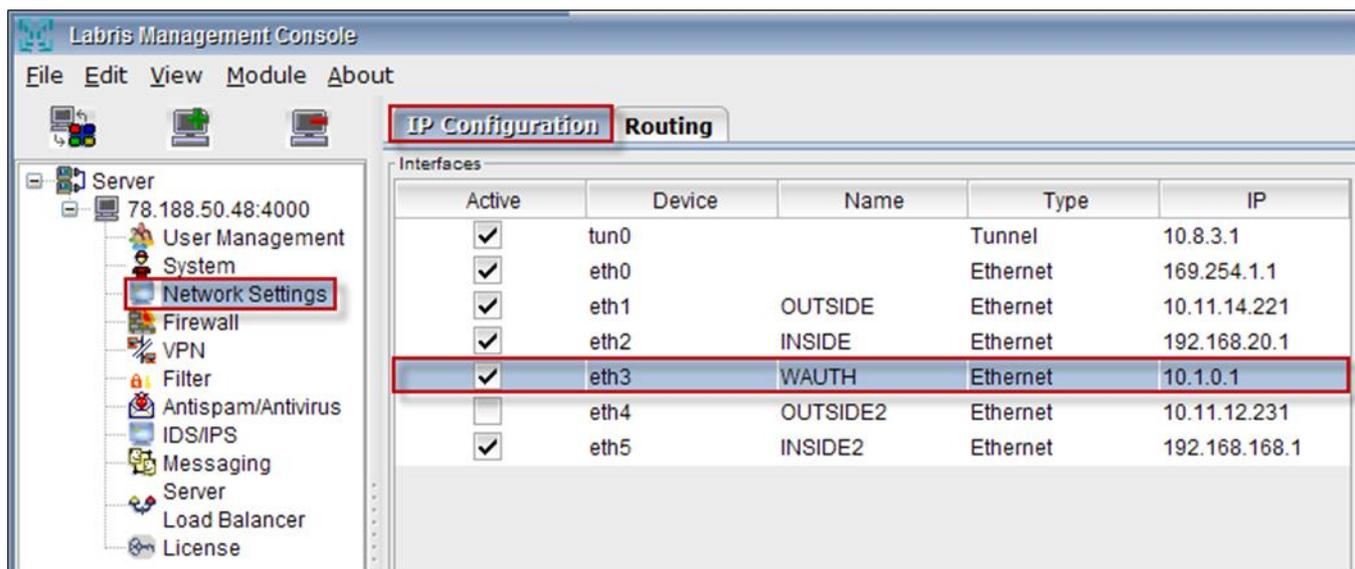
WAuth (Wireless Authentication) in LMC enables us to **Add New WAuth Interface, Edit existing WAuth Interface, and Delete WAuth Interface** in User Management Section in LMC.

Your device configuration for WAUTH

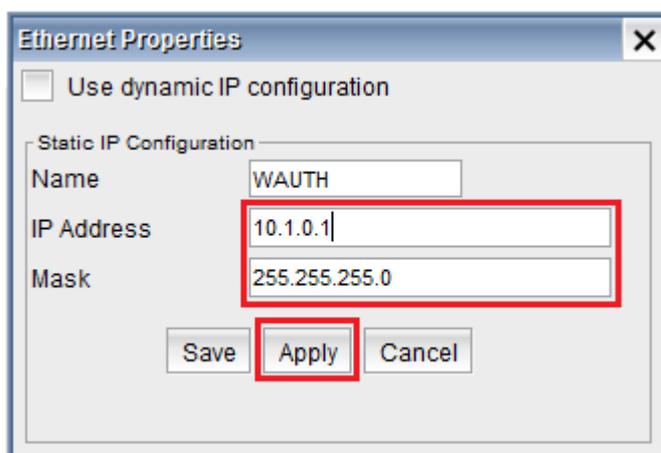
First Step:

Add a separate Network for WAuth in the Network settings module. Select Network settings for selected interface.

Choose the interface you want to choose for enabling WAuth.



- Edit Interface IP address or Name;



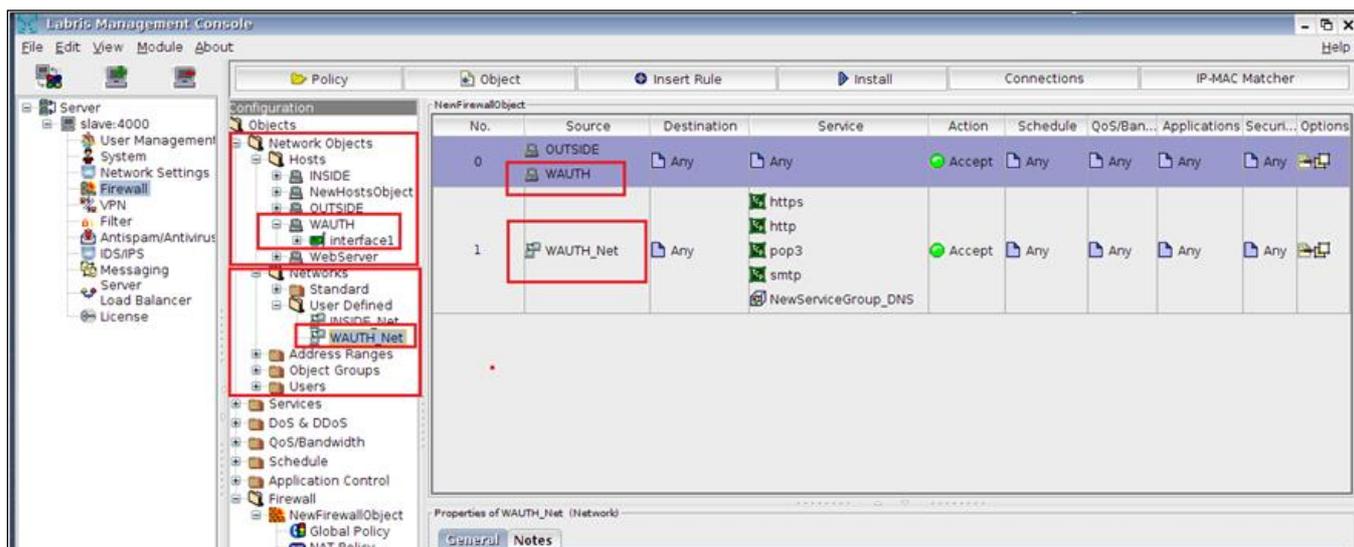
Second Step:

Create a DHCP Server for WAUTH;

[Click for DHCP configuration.](#)

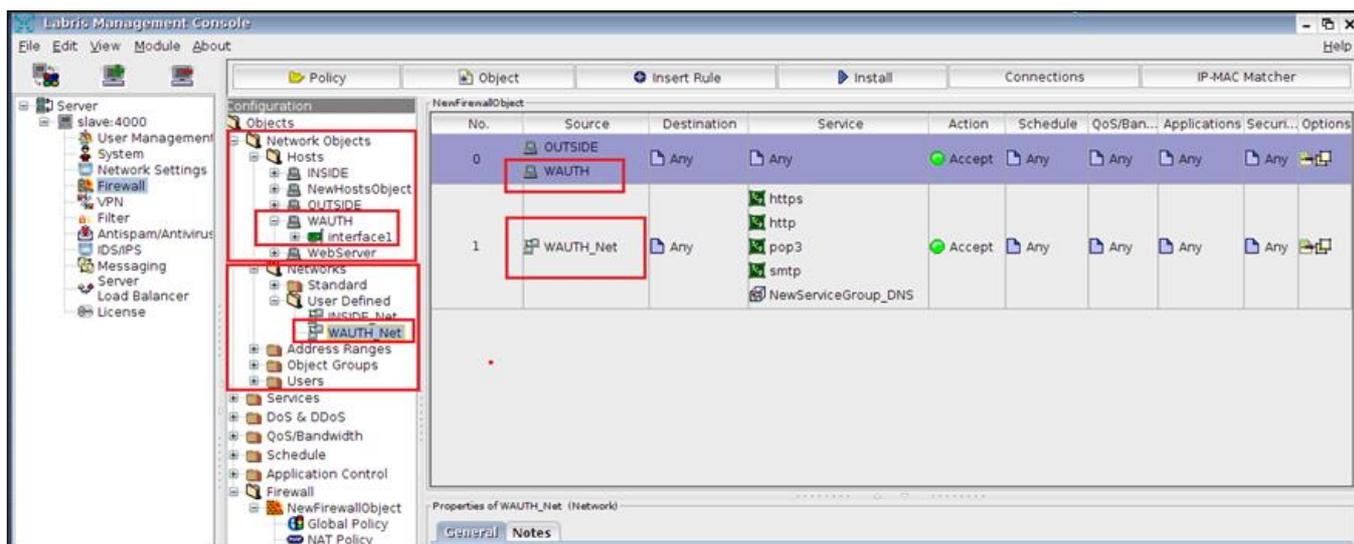
Third Step:

Create a **Network object** in firewall for WAUTH host and **Network** WAUTH_Net. (For Creating Network Object, please refer to **Hosts** under Network Objects section in Make a new Firewall object)



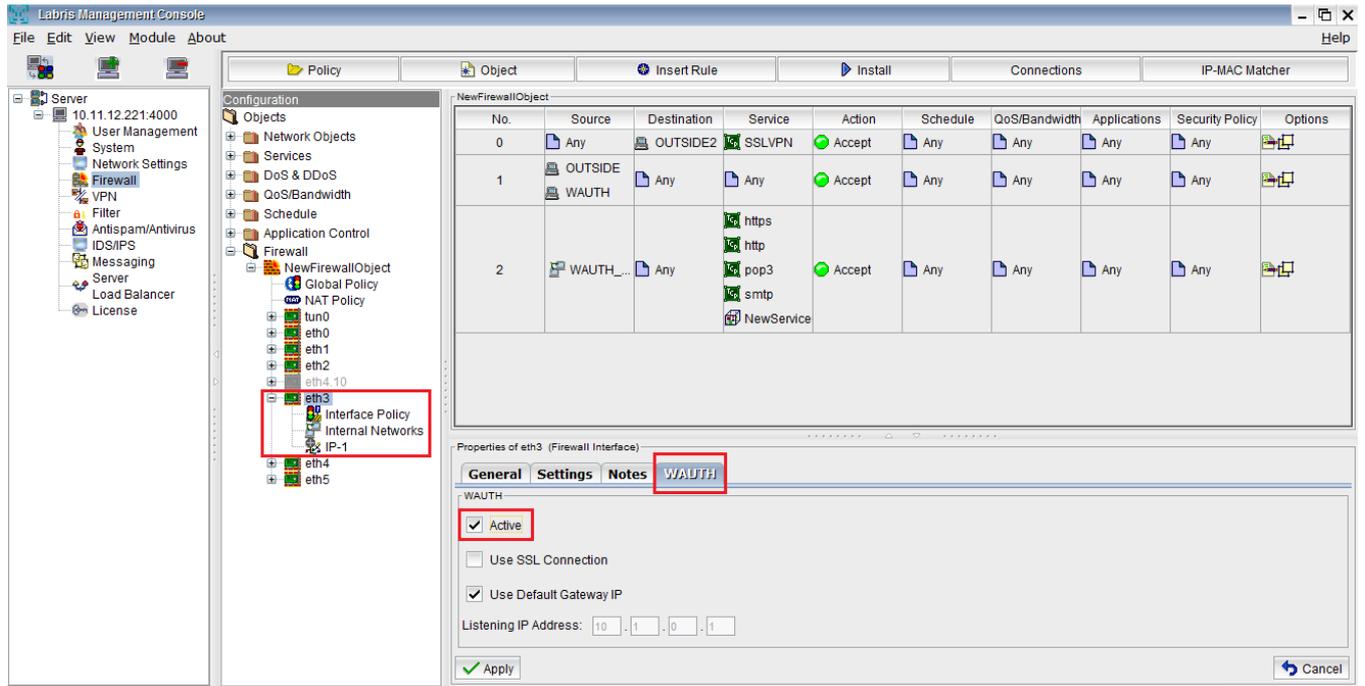
Fourth Step:

Add a policy (For Creating a **new policy** firewall object please refer to **Labris Firewall Management**)



Fifth Step:

Enable Wauth for the selected interface by configuring in interface WAUTH tab in Firewall module.



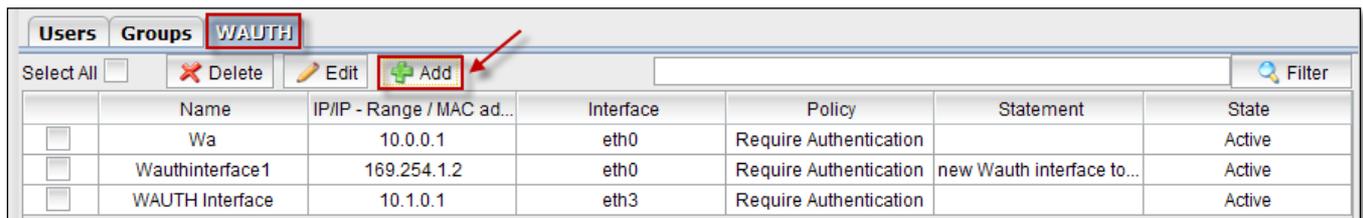
Sixth Step:

Add a user for WAUTH.

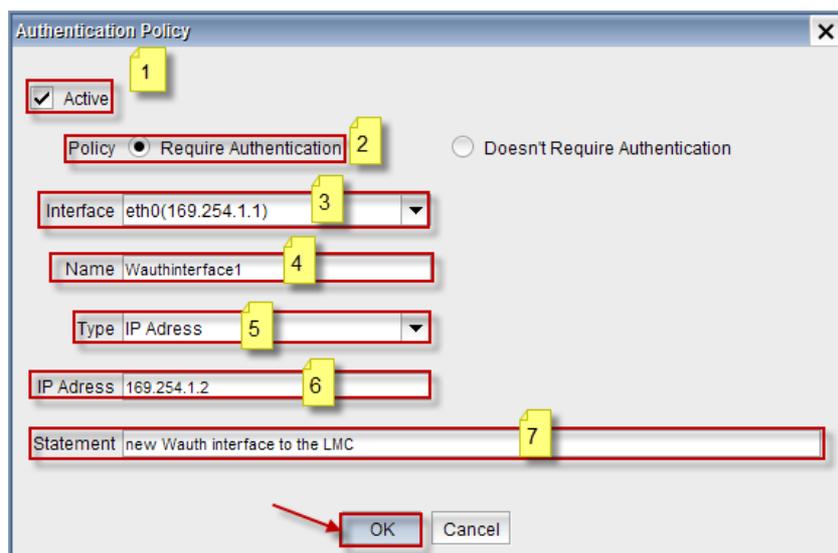
[Click for User Management.](#)

Configuring WAUTH policy

Click on **Add Tab** to add **Interface** to the **WAUTH** in User Management.



Below screen appears.



These are the inputs for the **Authentication Policy**.

1	Active	Enable this option to activate the interface
2	Policy	Choose required Policy
3	Interface	Choose interface from the drop down list
4	Name	Type name of the Interface
5	Type	Choose type of Interface from drop down list
6	IP Address	Give the IP Address
7	Statement	Type the Statement if any required (Optional)

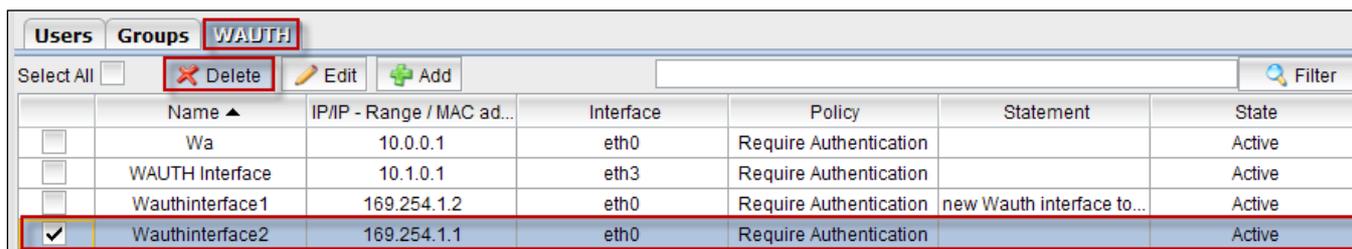
Click **Ok**.

Notice Interface added to the **WAUTH** in the below screen.

Users		Groups		WAUTH		
Name	IP/IP - Range / MAC ad...	Interface	Policy	Statement	State	
Wa	10.0.0.1	eth0	Require Authentication		Active	
Wauthinterface1	169.254.1.2	eth0	Require Authentication	new Wauth interface to...	Active	
Wauthinterface2	169.254.1.1	eth0	Require Authentication		Active	
WAUTH Interface	10.1.0.1	eth3	Require Authentication		Active	

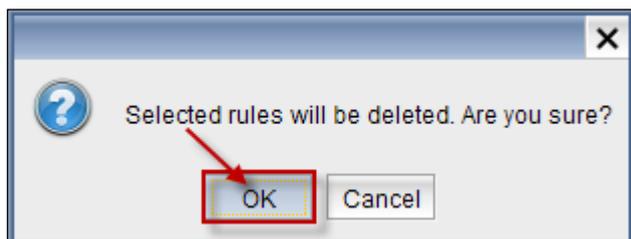
Deleting WAUTH policy

Select the Interface from the **WAUTH** list and click on **Delete** Tab



	Name ▲	IP/IP - Range / MAC ad...	Interface	Policy	Statement	State
<input type="checkbox"/>	Wa	10.0.0.1	eth0	Require Authentication		Active
<input type="checkbox"/>	WAUTH Interface	10.1.0.1	eth3	Require Authentication		Active
<input type="checkbox"/>	Wauthinterface1	169.254.1.2	eth0	Require Authentication	new Wauth interface to...	Active
<input checked="" type="checkbox"/>	Wauthinterface2	169.254.1.1	eth0	Require Authentication		Active

Warning screen is displayed, Click **OK** to delete the Interface



Deleting process is in progress.

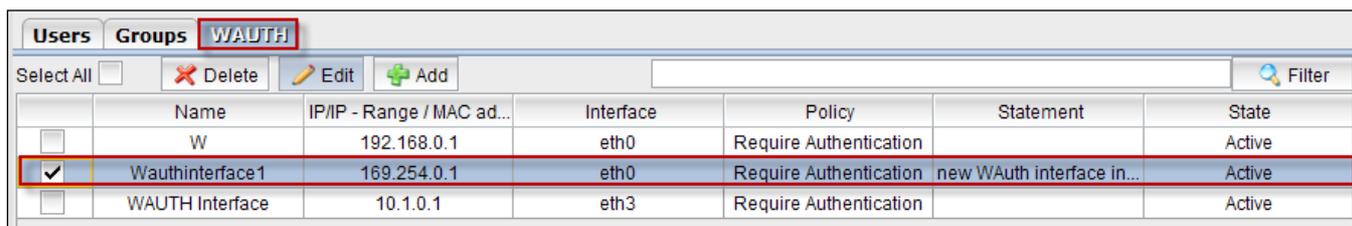


Below screen appears stating that **Deleted** successfully & click **OK** to close the current tab.



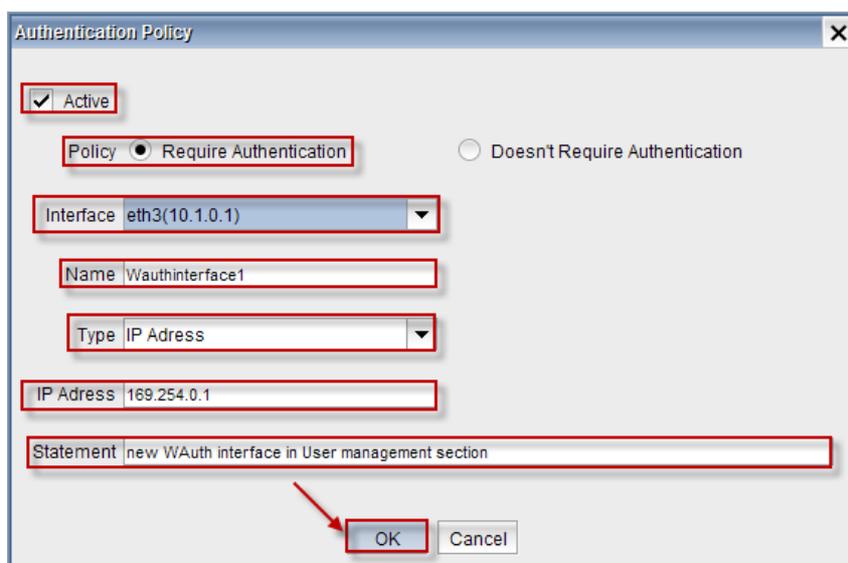
Editing WAUTH Policy

Select the **Group** which you want to edit from the list and click on **Edit Tab**.



	Name	IP/IP - Range / MAC ad...	Interface	Policy	Statement	State
<input type="checkbox"/>	W	192.168.0.1	eth0	Require Authentication		Active
<input checked="" type="checkbox"/>	Wauthinterface1	169.254.0.1	eth0	Require Authentication	new WAuth interface in...	Active
<input type="checkbox"/>	WAUTH Interface	10.1.0.1	eth3	Require Authentication		Active

We can edit any of the fields in the Authentication policy.



Authentication Policy

Active

Policy Require Authentication Doesn't Require Authentication

Interface eth3(10.1.0.1)

Name Wauthinterface1

Type IP Adress

IP Adress 169.254.0.1

Statement new WAuth interface in User management section

OK Cancel

Click **Ok**.

Adding WAUTH Authentication and User

Click on **WAUTH** tab from the dashboard and select Settings

Subnet Rules

Select **Subnet Rules** tab to view and change Subnet Rule specific settings. You can use subnet rules to enable/disable specific settings for specific networks. To illustrate, your internal network may not offer any sign up methods in Wauth Welcome screen but your guest network may offer TCKN Sign Up method. You can also set how the login screen should look using for different networks (different Company Logo's etc.). Combined with Access Control List (ACL) you can allow only specific users/groups to login from your internal network.

Note: Subnet independent configurations (like Hotel and AD configuration). Should be made on **Default** subnet rule.

Subnet Rules - Adding New Subnet Rule

Settings - Default

Setting Rule: Default

Subnet Rules | ACL | TCKN Wauth

Add new rule

Subnet list: 0.0.0.0/0.0.0.0

Save

Subnet Rules - Editing Subnet Rule

Settings - subnet-based-rule 2

Setting Rule: subnet-based-rule 2

Subnet Rules | General | UI | ACL

Rule name: subnet-based-rule 2

Subnet list: 192.168.0.0/255.255.255.0

Save Delete

1	Setting Rule	Current subnet rule choice. This affects all configuration data in all tabs (General, UI, ACL)
2	Rule Name	Name of this subnet rule
3	Subnet List	Comma separated list of networks that this subnet rule should apply to.
4	Save	Save changes to subnet rule.
5	Delete	Delete this subnet rule. Warning: This also deletes all configuration choices for this rule on other tabs (General, UI, TCKN, SMS, ACL etc.)

Subnet Rules - Default

Default subnet rule can't be deleted and its networks can't be edited. This ensures that if no other subnet rules matches the user, **Default** subnet rule will be applied for user.

Settings - Default

Setting Rule:

Subnet Rules | **General** | UI | ACL | TCKN Wauth

Rule name:

Subnet list:

General Settings

Select **General tab** to view and change the General settings.

Authentication methods in WAUTH is configured in General tab.

Common Key:

Common key provides an effective mechanism to prevent unauthorized users from registering. During registration, user must provide the common key if authentication method requires it.

Example scenario:

TCKN Wauth with common key (Assuming TCKN Wauth is already configured)

- In General tab;
 - Set CK Option to Manual.
 - Set Common Key to the desired value.
 - Click Save.
- In TCKN Wauth tab:
 - Activate common key

You can also set CK Option to Automatic and provide a CK period. If you do this, common key will be changed at the end of this period automatically.

If you want unauthorized users (users who cannot login to web admin panel) to view common key, you can set a username and password for this.

- Set CK Username and CK Password values.

- For wauth listening ip 192.168.0.1, as unauthorized user go to:
192.168.0.1:85/wauth/show_ck/
- Enter values from CK Username and CK Password.
- Current common key will be shown.

Important Note: Common keys are different for each subnet rule. If you have multiple subnet rules, you should provide matching subnet rule's CK Username and CK Password. Otherwise you will get an error.

Network Authentication System

- Create User
- Online Users
- All Users
- Settings

Settings - Default

Setting Rule:

Subnet Rules | General | UI | ACL | TCKN Wauth

Welcome message: 1

Welcome message (EN): 2

Local Authn. Format: 3

SMS Wauth: 4

Active Directory Authn. 5

Hotel Integration: 6

TC Identity NVI Confirmation: 7

Passport Wauth: 8

Agreement Enable/Disable: 9

Agreement: [Show Agreement](#) 10

Agreement (EN): [Show Agreement \(EN\)](#) 11

Timeout Enable/Disable: 12

Timeout Period: (minutes) 13

Authentication Type: 14

Ingress Session Enable/Disable: 15

Reference Emails/Domains: Add 16

Reference Timeout (seconds): 17

Smtp Server Address: 18

Smtp Mode: 19

Smtp Port: 20

Smtp Username: 21

Smtp Password: 22

Smtp Mail From: 23

CK Option: Automatic 24

CK Period: 1 (mins) 25

Common Key: SPWUY5 26

CK Username: common 27

CK Password: 28

CK Instructions: Kayıt olabilmek için lütfen danışmadan ortak anahtarı temin ediniz. 29

CK Instructions (EN): Please get the common key from advisory. 30

These are the inputs for the General Settings.

1	Welcome message	Welcome message is displayed in Turkish
2	Welcome message (EN)	Welcome message is displayed in English
3	Local Authent format	Choose Authentication format from the drop down list
4	SMS Wauth	We can enable or disable this option
5	Active Directory Authent	We can enable or disable this option
6	Hotel Integration	We can enable or disable this option
7	TC Identity NVI Confirmation	We can enable or disable option
8	Passport Wauth	We can enable or disable option
9	Agreement	We can enable or disable this option
10	Agreement [TR]	This option displays information regarding agreement in Turkish.
11	Agreement (EN)	This option displays information regarding agreement in english
12	Time out	We can enable or disable this option
13	Time period	Mention time period in minutes
14	Authentication Type	Choose Authentication type from the drop down list
15	Ingress session	We can enable or disable this option
16	Reference Emails/Domains	We can add or delete reference emails/domains from this field
17	Reference Timeout	We can set reference email timeout (seconds)
18	Smtip Server Address	We can set smtp server address
19	Smtip Mode	We can choose smtp mode (TLS, SSL, Normal)
20	Smtip Port	We can set port number for smtp protocol
21	Smtip Username	We can set username for smtp server

22	Smtplib Password	We can set password for smtp server
23	Smtplib Mail From	We can set mail from field in sent mail
24	CK Option	Common key will be set manually or generated automatically.
25	CK Period	Common key regeneration period when common key is generated automatically.
26	Common Key	Current common key (will be regenerated on save if it's automatically generated)
27	CK Username	Username to get current common key for unprivileged user
28	CK Password	Password to get current common key for unprivileged user
29	CK Instructions	Instructions to show user on sign-up screen.
30	CK Instructions (EN)	Instructions to show user on sign-up screen (english)

Click on **Save** to save the changes

Settings of Hotel Authentication

Select **Hotel** tab

These are the inputs for the Hotel Authentication.

1	Default	Select User Group
2	Hotel Name	Type the Name of the Hotel
3	Product type	Choose product type
4	MAC Address	Type MAC Address (optional)

5	Machine Port	Type Machine port (optional)
6	Real Name	Type the name of the Database
7	Real Name	Type the name of the table (optional)
8	User Name	Type the Username
9	Password	Type the password
10	User Name Field Name	Type Username Field Name (optional)
11	Password Field Name	Type Password Field Name (optional)
12	Name Field Name	Type Name of the Field Name (optional)
13	Surname Field Name	Type Surname of the Field Name (optional)
14	Departure Date	Mention Departure Date (optional)
15	Timeout	Mention Timeout in minutes
16	Infinite timeout	We can enable or disable this option
17	Multiple Login	We can enable or disable this option

Click on Test to test the details and then select **save** to save the changes

Settings of SMS Authentication

Select **SMS Authentication**

These are the inputs for the SMS Authentication.

Subnet Rules General SMSWauth UI ACL TCKN Wauth Passport

Default Group: Default 1

Multiple Login: 2

Account Quota: 1440 (mins) 3

Account Expiration Date: 24 (hours) 4

Timeout: 1440 (mins) 5

Cust. Serv. Tel: 1111111111 6

Comp. Mobile***: 1111111111 7

Cust. Serv. Email: example@labrisnetworks.cor 8

Help page for SMS authentication: 9

Title of SMS authentication help page: Labris Networks 10

Subtitle of SMS authentication help page: Wauth Ağ Yetkilendirme Sist 11

Message of SMS authentication help page: 12
 Giriş için Kullanıcı adı ve şifreniz var ise Şifrem Var butonuna basıp bilgilerinizi girip internette gezinmeye başlayabilirsiniz.

Giriş bilgileriniz yok ise Şifrem Yok butonuna basarak cep telefonu numaranızı girip, SMS ile giriş bilgilerinizi alabilir ve bu bilgilerle giriş yapıp internette gezinmeye başlayabilirsiniz.

Enable Common Key: 13

SMS sending will be afforded by the company*: 14

Use Custom SMS Api: 15

Remained Token**: 500 16

Custom SMS Service Configuration 17

Buy tokens 18

Show Common Key 19

Save 20

1	Default Group	Users authenticated with SMS will be a member of this group.
2	Multiple Login	SMS users will be allowed to login from different devices simultaneously.
3	Account Quota	Account Quota
4	Account Expr. Date	Users authenticated with SMS will be expired after this period of time.
5	Timeout	Mention Timeout Period
6	Cust. Serv. Tel	Type Customer Service Telephone number
7	Comp. Mobile	Type Company Mobile Name
8	Cust. Serv. Email	Type Customer Service Email address
9	Help page for SMS authentication	Show a help page to user for SMS authentication.
10	Title of SMS auth. help page	Title of SMS authentication help page
11	Subtitle of SMS auth. help page	Subtitle of SMS authentication help page
12	Message of SMS auth. help page	Message to show in SMS authentication help page
13	Enable Common Key	Require common key for new user sign-up.

14	SMS sending will be afforded by the company	Cost of SMS sending will be afforded by the host.
15	Use Custom SMS Api	Use another SMS sending API. You need to configure this API via "Custom SMS Service Configuration" button
16	Remained Token	If SMS sending cost will be afforded by company and custom SMS API isn't used, these tokens will be used for new registrations.
17	Custom SMS Service Configuration	Configure custom (third-part) SMS service API.
18	Buy Tokens	Open token purchase page.
19	Show Common Key	Show common key query webpage.
20	Save	Save changes

Click on **Buy tokens** and select **Save** to save the changes.

Active Directory Authentication

Select **AD** (Active Directory tab)

Domain name and authenticating account information configuration is done in this tab.

These are the inputs for Active directory Authentication.

1	AD Domain Name	Type Active Directory Domain Name
2	Disable Group Name	Choose this option to Disable Group Name
3	AD Work Group	Type Active Directory Work Group Name

4	AD Group Name	Type Active Directory Group Name
5	AD Timeout	Mention Active Directory Timeout period
6	Infinite Timeout	We can enable or disable this option
7	AD Quota	Mention time period of Active Directory Quota
8	Infinite Quota	We can enable or disable this option
9	AD Expire Date	Mention time period of Active Directory Expire Date
10	Infinite Expr time	We can enable or disable this option

User Interface Customization

Select **UI** (Active Directory tab)

UI tab is used for customization of guest and user welcome screens.

Subnet Rules General **UI** ACL

Logo: No file chosen **1**

Delete Logo: **2**

Logo URL: **3**

Background Image: No file chosen **4**

Delete Background Image: **5**

Background Image Position: **6**

Background Image Repetition: **7**

Page Title: **8**

Page Title: **9**

Login Page Header: **10**

Login Page Header: **11**

Login Page Footer: **12**

Login Page Footer: **13**

Username Caption: **14**

Username Caption: **15**

Password Caption: **16**

Password Caption: **17**

Login Button Caption: **18**

Login Button Caption: **19**

Logout Button Caption: **20**

Logout Button Caption: **21**

Background Color: **22**

Header/Footer Font Color: **23**

Page Title Background Color: **24**

Page Title Font Color: **25**

Default Domain Choice: **26**

1	Logo	Add a company logo
2	Delete Logo	Delete default logo
3	Logo URL	Add a company logo on the web
4	Background Image	Add a image for background
5	Delete Background Image	Delete default background image
6	Background Image Position	Select position for background image
7	Background Image Repetition	Select repetition for background image
8	Page Title	Page Title Instructions is displayed in Turkish
9	Page Title-Eng	Page Title Instructions is displayed in English
10	Login Page Header	Login Page Header Instructions is displayed in Turkish
11	Login Page Header-Eng	Login Page Header Instructions is displayed in English
12	Login Page Footer	Login Page Footer Instructions is displayed in Turkish
13	Login Page Footer-Eng	Login Page Footer Instructions is displayed in English
14	Username Caption	Username Instructions is displayed in Turkish
15	Username Caption-Eng	Username Instructions is displayed in English
16	Password Caption	Password Instructions is displayed in Turkish
17	Password Caption-Eng	Password Instructions is displayed in English
18	Login Button Caption	Login Button Caption Instructions is displayed in Turkish
19	Login Button Caption-Eng	Login Button Caption Instructions is displayed in English
20	Logout Button Caption	Logout Button Caption Instructions is displayed in Turkish
21	Logout Button Caption-Eng	Logout Button Caption Instructions is displayed in English
22	Background Color	Select Background
23	Header/Footer Font Color	Select Header/Footer font color
24	Page Title Background Color	Select Page Title background color
25	Page Title Font Color	Select Page Title font color
26	Default Domain Choice	Select default domain choice for login screen

Turkish Citizen ID Number Authentication

Select TCKN Wauth tab (Turkish Citizen ID Number Tab)

You can set configuration options for Turkish Citizen ID Number authentication method in this tab.

1	Default Group	Users signed up with this method will be a member of this group
2	Multiple Login	TCKN users will be allowed to login from different devices simultaneously.
3	Infinite Quota	We can set enable or disable infinite quota
4	Account Quota	We can set time quota for user
5	Infinite Account	We can set enable or disable infinite account time
6	Timeout	We can set time for login time
7	Account Expiration Date	Users authenticated with SMS will be expired after this period of time.
8	Cust. Serv. Tel	Type customer service telephone number
9	Cust. Serv. Mail	Type customer service mail
10	Reference Approval	We can enable or disable reference approval
11	Request Mobile Number	We can require user's gsm no with this field.
12	Use GSM Number for Username	Checking this option will generate username from gsm no (instead of TCKN)
13	Send Password With SMS	Activating this will generate a random password for user and send it to user's mobile phone.
14	Enable Common Key	Require Common Key for new users.
15	Show Common Key	Show common key query webpage.
16	Save	Save changes.

Passport Number Authentication

Select Passport Wauth tab (Turkish Citizen ID Number Tab)

You can set configuration options for Passport Number authentication method in this tab.

The screenshot shows the 'SMSWauth' configuration page with the following numbered elements:

- Default Group: Default
- Multiple Login:
- Infinite Quota:
- Account Quota: 1440 (mins)
- Infinite Account:
- Timeout: 1440 (mins)
- Account Expiration Date: 24 (hours)
- Cust. Serv. Tel: 1111111111
- Cust. Serv. Email: example@labrisnetworks.co
- Reference Approval:
- Request Mobil Number:
- Use GSM Number for Username:
- Send Password With SMS:
- Enable Common Key:
- Show Common Key button
- Save button

1	Default Group	Users signed up with this method will be a member of this group.
2	Multiple Login	Passport users will be allowed to login from different devices simultaneously.
3	Infinite Quota	We can enable or disable infinite quota
4	Account Quota	We can set time quota for user
5	Infinite Account	We can set enable or disable infinite account time
6	Timeout	We can set time for login time
7	Account Expiration Date	Users authenticated with SMS will be expired after this period of time.
8	Cust. Serv. Tel	Type customer service telephone number
9	Cust. Serv. Mail	Type customer service mail
10	Reference Approval	We can enable or disable reference approval
11	Request Mobile Number	We can require user's gsm no with this field.
12	Use GSM Number for Username	Checking this option will generate username from GSM No (instead of Passport No)
13	Send Password With SMS	Activating this will generate a random password for user and send it to user's mobile phone.
14	Enable Common Key	Require Common Key for new users.
20	Show Common Key	Show common key query webpage.
21	Save	Save changes.

Access Control List

Select which users/groups/ip's are allowed to (or not allowed to) login Wauth.

Subnet Rules

General

UI

ACL

IP Addresses:

1

Rule choice:

2

Only allow given IPs,users and groups
 Deny given IPs,users and groups

Select Members:

Members

Filter

3

All Users

Filter

testuser3129@labristeknoloji.com
 testuser2754@labristeknoloji.com
 testuser7327@labristeknoloji.com
 testuser5861@labristeknoloji.com
 testuser7071@labristeknoloji.com
 testuser4161@labristeknoloji.com
 testuser2547@labristeknoloji.com
 testuser9728@labristeknoloji.com
 testuser7669@labristeknoloji.com

Remove Members

Add Members

« Prev Next »

Select Groups:

Member Groups

Filter

4

All Groups

Filter

testgroup98@labristeknoloji.com
 testgroup78@labristeknoloji.com
 testgroup66@labristeknoloji.com
 testgroup70@labristeknoloji.com
 testgroup31@labristeknoloji.com
 testgroup66@labristeknoloji.com
 testgroup29@labristeknoloji.com
 hasanlar@u9
 enterprise admins@labristeknoloji.com

Remove Groups

Add Groups

« Prev Next »

Save

1	Ip Addresses	Comma separated list of ips
2	Rule choice	Allow or deny these ip's, users and groups
3	Select Members	Choose users to apply this rule
4	Select Member Groups	Choose groups to apply this rule

Creating WAUTH User

User for WAUTH may be created in two ways. First is LMC. Local users can be created in LMC User Management module and directly be used in Wauth. Second is Wauth web based simple management screens. By Wauth web screen, one can create Wauth users.

Select **WAUTH tab** from the dashboard and click on **Create User tab**

The screenshot shows a 'Create User' form with the following fields and callouts:

- 1: Username: TestUser
- 2: Domain: slave
- 3: Group: Default
- 4: Real Name: Labris Test User
- 5: Expiration Date: Date: 2014-04-30, Time: 12:00:00
- 6: Quota (min):
- 7: Infinite quota:
- 8: MAC Address(Optional): 112233445566
- 9: Allow Multiple Logins:
- 10: Notes: Labris Test User
- 11: Password: [masked]

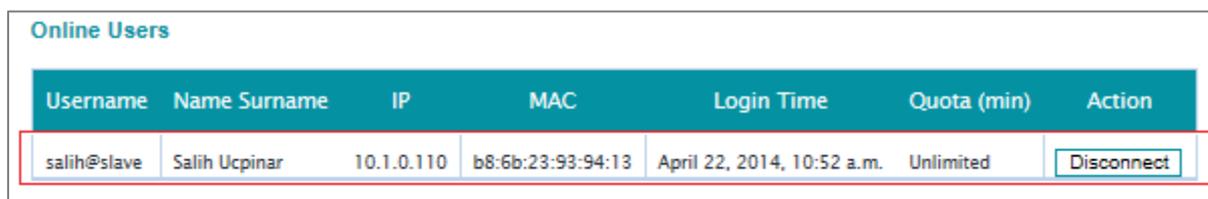
A 'Create User' button is located at the bottom of the form.

These are the inputs to Create User.

1	User Name	Type name of the User
2	Domain	Choose Domain Name
3	Group	Select Group for User
4	Real Name	Type Real Name of the User
5	Expiration Date	Select Expiration Date and Time of the User
6	Quota	Mention Quota
7	Infinite Quota	We can enable or disable this option
8	MAC Address (optional)	Type MAC Address (optional)
9	Allow multiple Logins	We can enable or disable this option
10	Notes	Type any notes regarding User (optional)
11	Password	Type Password of the User

Online Users

IP/MAC addresses and login time information is shown in Online Users screen. Also, this screen provides a function to disconnect the user.

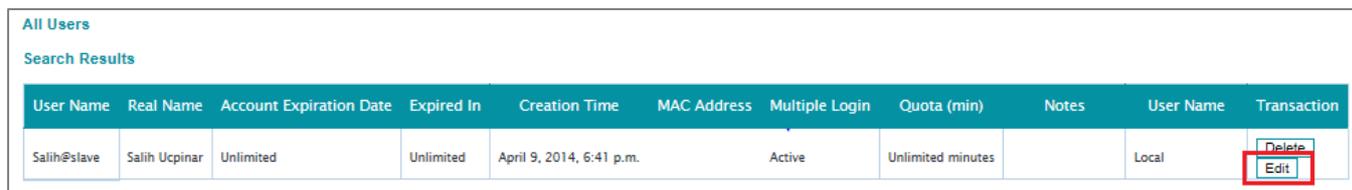


Username	Name Surname	IP	MAC	Login Time	Quota (min)	Action
salih@slave	Salih Ucpinar	10.1.0.110	b8:6b:23:93:94:13	April 22, 2014, 10:52 a.m.	Unlimited	Disconnect

All Users (User editing)

It is the screen that showing all users and information of users. Editing is easily done by clicking and opening Edit User window.

Note: If a user is online and his account is deleted, the user will be disconnected.



User Name	Real Name	Account Expiration Date	Expired In	Creation Time	MAC Address	Multiple Login	Quota (min)	Notes	User Name	Transaction
Salih@slave	Salih Ucpinar	Unlimited	Unlimited	April 9, 2014, 6:41 p.m.		Active	Unlimited minutes		Local	Delete Edit

This edit window can also be used for just password changing without any account information editing. If you do not touch any field other than password, no other information will be changed except for password. In the same way, this editing window may be used for prolonging account lifetime.

1	User Name	Show Username
2	Real Name	Edit Real Name
3	Expiration Date	Edit Expiration Date and Time of the User
4	MAC Address	Edit MAC Address
5	Allow Multiple Login	We can enable or disable this option
6	Quota	Edit Mention Quota
7	Infinite Quota	We can enable or disable this option
8	Notes	Type any notes regarding User (optional)
9	Password	Change User Password

WAUTH Welcome Screen

The guest or user is expected to authenticate him/herself to the system with given credential information, credential information they get through SMS messages, TCKN, Passport authentication.

Also, the system provides function for authenticating users of Active Directory with their AD credentials.

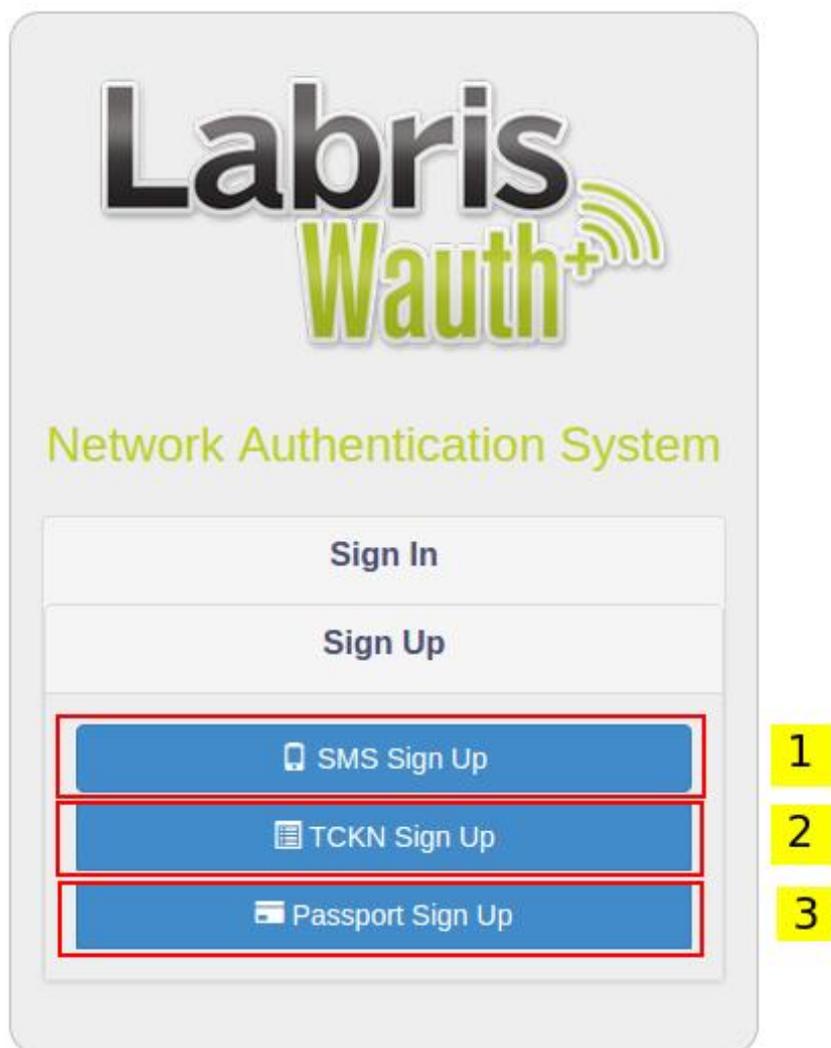
After account creation, user is expected to open an internet browser and will be welcomed with a welcome screen. Guest or user should enter the credentials on this stage.

This welcome screen can be shown in different languages according to internet browser's language settings.

For obtaining passwords, please follow next parts of the document.

1	User Name	Username Input
2	Password	Password Input
3	Domain	Select Domain Local or Domain Controller
4	Login	Login Button
5	Sign Up	Alternative Sign-up Methods
6	Reset Password	Reset forgot password

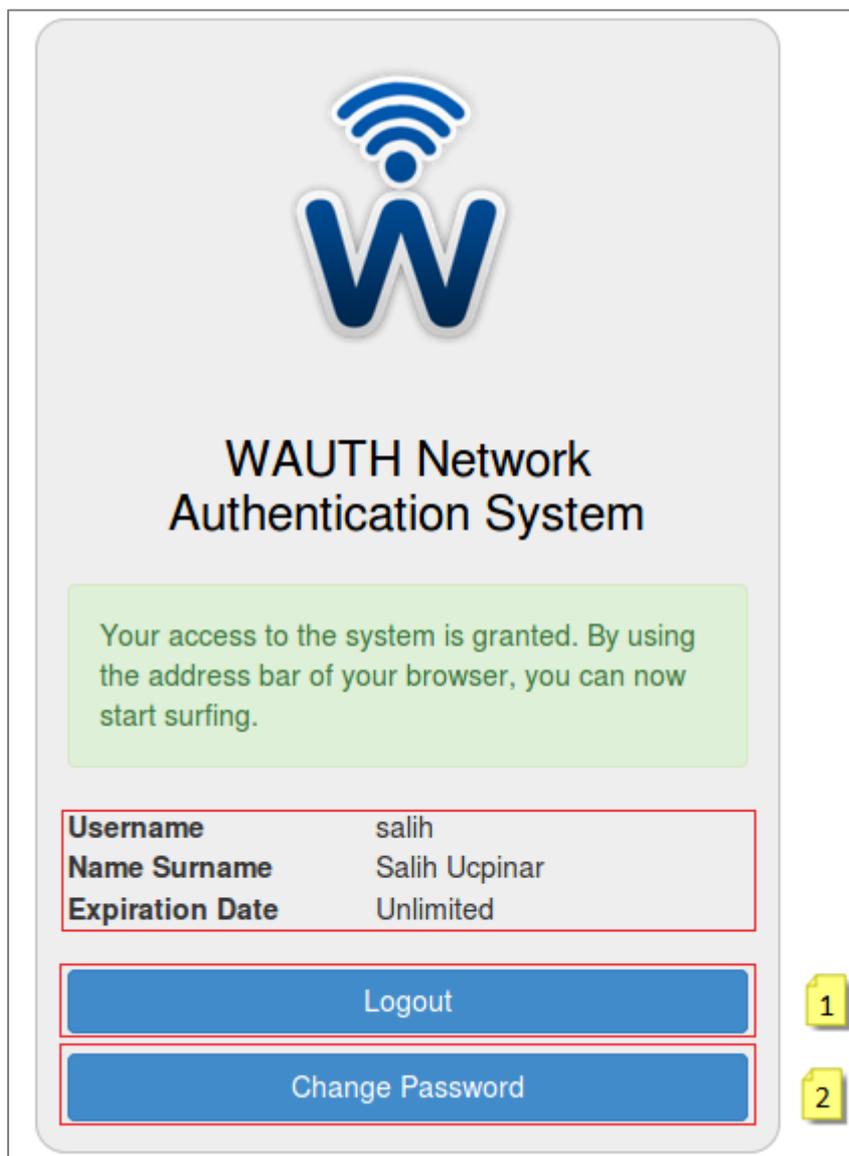
Alternative Sign Up Methods



1	SMS Sign Up	Sign up using mobile number
2	TCKN Sign Up	Sign up using your TC Identity Number
3	Passport Sign Up	Sign Up using passport number

18. Login

Post-entry Screen



1	Logout	Logout Button
2	Change Password	Change Password Button

19. Change User Password

User can change his password with “Change Password” button and Change Password window shown.

The image shows a 'Change Password' form. It has a title 'Change Password' at the top. Below the title are three input fields: 'Current password', 'New password', and 'Verify password'. Each field is highlighted with a red border and a yellow callout box containing a number (1, 2, and 3 respectively). Below the input fields are two blue buttons: 'Confirmation' and 'Back'.

1	Current Password	User Old Password
2	New Password	User New Password
3	Verify Password	New Password Again

20. Reset Password

Users who signed up with TCKN or Passport Number may reset their forgot passport.

Reset Password - Personal Info Validation Step

In this step, user provides the same information during sign up. This fields will be checked against the previous information of user and if they match, user will be allowed to reset their password.

The image shows a mobile application interface for 'Labris Wauth+' Network Authentication System. The title 'Labris Wauth+' is at the top in a stylized font, with 'Wauth+' in green and a Wi-Fi symbol. Below it, 'Network Authentication System' is written in green. The form consists of five input fields, each with a red border and a yellow number in the top right corner: 1. 'Name' (with an information icon), 2. 'Surname' (with an information icon), 3. 'Year of Birth' (with a clock icon), 4. 'E-Mail' (with an envelope icon), and 5. 'TC Identity Code' (with a person icon). At the bottom, there are two blue buttons: 'Back' and 'Next'.

1	Name	First Name
2	Surname	Last Name
3	Year of Birth	Year of birth
4	E-Mail	E-Mail
5	TC Identity Code	TC Identity Number

Reset Password - Set new password step

The screenshot shows the Labris Wauth+ Network Authentication System interface. At the top is the logo 'Labris Wauth+' with a Wi-Fi symbol. Below the logo is the text 'Network Authentication System'. There are two input fields, each with an information icon on the left and a yellow box with a number on the right. The first field is labeled 'New Password' with the number '1'. The second field is labeled 'Confirm Password' with the number '2'. Below the fields are two blue buttons: 'Back' and 'Next'.

1	New Password	New password for user
2	Confirm Password	Confirm new password for user

Reset Password - Password Changed Screen

After completing all steps user will see the screen below.

The screenshot shows the Labris Wauth+ Network Authentication System interface after a password change. At the top is the logo 'Labris Wauth+' with a Wi-Fi symbol. Below the logo is the text 'Network Authentication System'. Below that is a green message 'Password changed.' and a blue link 'Click here to login with your new password.'

21.

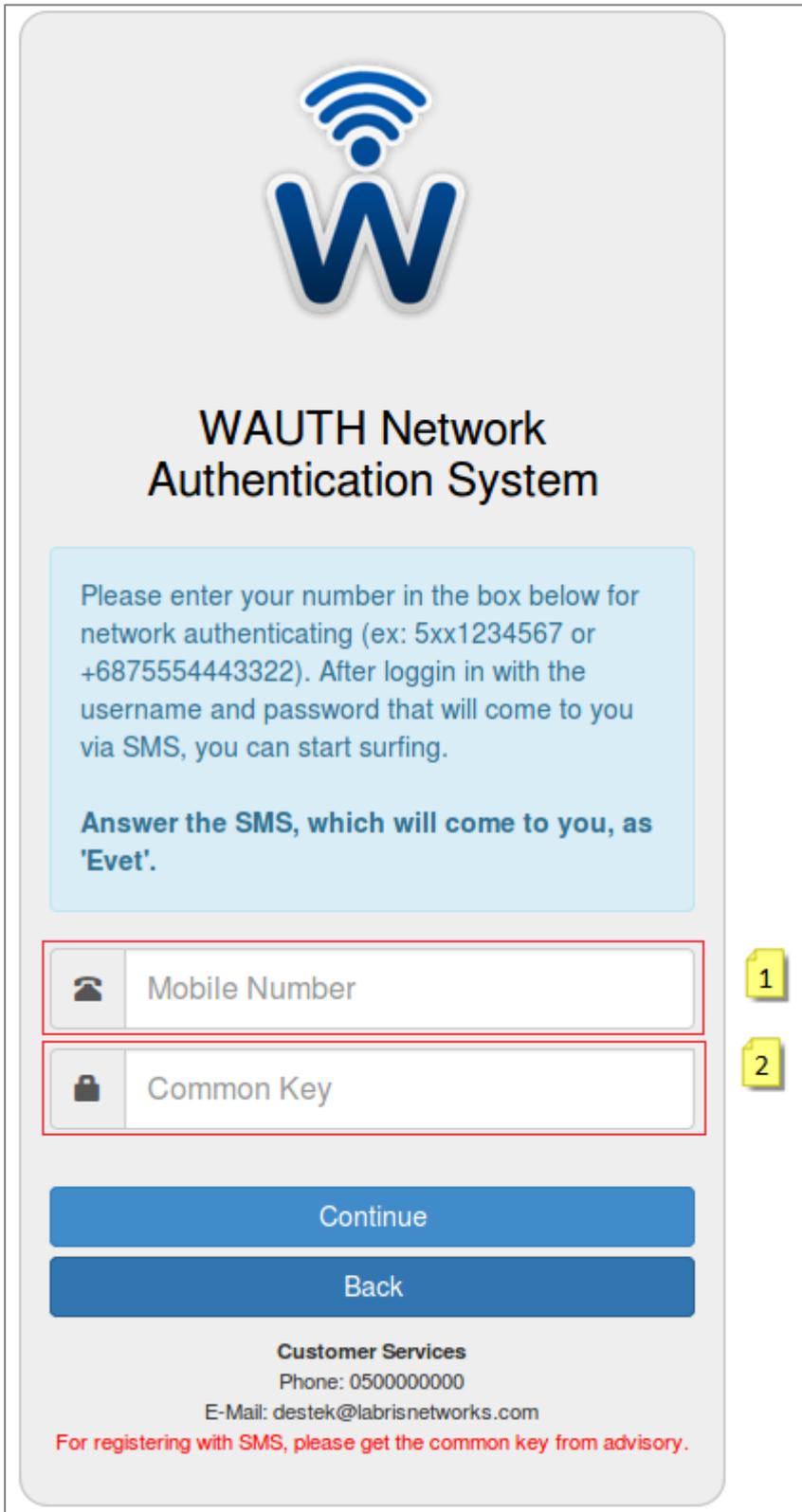
SMS Sign Up

22. Registering with SMS

Click to “Obtain Password” button. If SMS authentication is disabled, obtain password choice will not be shown. For enabling SMS authentication, enable SMS Wauth in Wauth General Settings tab.

GSM number and common key

Common key is a security solution for preventing unwanted guests to use the corporation’s wifi guest internet access. This common key is enabled and set in SMSWauth screen. If CK is enabled, guest is wanted to enter it.



The image shows a mobile application interface for the WAUTH Network Authentication System. At the top is a logo consisting of a blue 'W' with a Wi-Fi signal icon above it. Below the logo is the title 'WAUTH Network Authentication System'. A light blue box contains instructions: 'Please enter your number in the box below for network authenticating (ex: 5xx1234567 or +6875554443322). After login in with the username and password that will come to you via SMS, you can start surfing.' Below this is another instruction: 'Answer the SMS, which will come to you, as 'Evet''. There are two input fields: 'Mobile Number' with a phone icon and 'Common Key' with a lock icon. Both fields are highlighted with a red border and numbered '1' and '2' respectively. Below the input fields are two blue buttons: 'Continue' and 'Back'. At the bottom, there is contact information for 'Customer Services' including a phone number (0500000000) and an email address (destek@labrisnetworks.com). A red note at the bottom states: 'For registering with SMS, please get the common key from advisory.'

1	Mobile Number	Mobile Telephone Number
2	Common Key	Company Common Key

23. TCKN Sign Up

Users may sign up using their TC Identity Number. Validity of user-provided information (TC Identity Code, Name, Surname, Year of Birth) is checked against the records.

Labris Wauth+
Network Authentication System

1 | TC Identity Code

2 | Name

3 | Surname

4 | Year of Birth

5 | Mobile Number

6 | Reference Mail

7 | Common Key

Sign Up

Back

Customer Services
Phone: 3122101490
E-Mail: support@labrisnetworks.com

1	TC Identity Code	TC Identity Number of user
2	Name	Name of new user
3	Surname	Surname of new user
4	Year of Birth	Year of birth
5	Mobile Number	Only visible if Request Mobile Number is activated. Will be used for sending password via sms if Send Password with Sms is activated.
6	Reference Mail	Mail of the person who will approve this new user. This fields is visible if Reference Approval is activated. Reference mail should be one of the mails or member of a domain configured in General Settings->Reference Emails/Domains .
7	Common Key	We can fill common key

24. Passport Sign Up

Users may sign up using their Passport Number.

Labris Wauth+
Network Authentication System

1 Passport Number

2 Name

3 Surname

4 Year of Birth

5 Mobile Number

6 Reference Mail

7 Common Key

Sign Up

Back

Customer Services
Phone:
E-Mail:

1	Passport Number	Passport number of new user.
2	Name	Name of new user
3	Surname	Surname of new user
4	Year of Birth	Year of birth
5	Mobile Number	Only visible if Request Mobile Number is activated. Will be used for sending password via sms if Send Password with Sms is activated.
6	Reference Mail	Mail of the person who will approve this new user. This fields is visible if Reference Approval is activated. Reference mail should be one of the mails or member of a domain configured in General Settings->Reference Emails/Domains .
7	Common Key	We can fill common key

25. Quota

Labris UTM can measure internet usage of users in terms of byte count and elapsed time. This functionality is provided by Quota module. In this section, all information required to configure quota settings and monitor quota usage of users is provided. Quota module measures all the traffic which passes over Labris UTM. This means if you have multiple internal networks, you can measure and limit traffic between internal networks also.

Terminology

In order to simplify configuration and enable advanced configuration options, administrator can define Quota Policies and Quota Exceptions and use any combination of them for different users or groups.

Quota Policy

A Quota Policy is a set of rules which defines how much a user or members of a group can use the internet in a period.

Period: Defines when the usages will be cleared. In other words, it defines when the quota will be renewed. It's useful if you want to set the limits daily, weekly, monthly, yearly. If you don't want quota to reset and define final limits in the policy, you can choose non-periodic.

Note: Periods are completed at the end of specified unit. For example, if a new policy is created with 1 Month period on 15th November, usage will be reset on 30th November, not on 15th December.

Surfing Time: It allows limiting the quota by time. Time limit allows measuring surfing time of user and set limit for them. Surfing time is not measured directly, instead calculated by counting transferred bytes in the last minute. If user transferred at least 100 KB in the last minute, it is passed for a minute usage. This means minimum unit for surfing time is minute and for example ten seconds of usage may be calculated as one-minute usage.

If period is set, this usage will be reset at the end of period.

Data Quota: Download and upload limits can be defined here.

Quota Exception: Multiple Quota Exceptions can be attached to the policy. Order is important.

Quota Exception

A Quota Exception is a rule to measure a specific usage pattern and define limit for this pattern. For example, you may have a generic quota policy with 5 GB download limit. If you have an ftp server outside of your internal network or in a separate network (e.g. DMZ) you may want to set a separate limit for transfers between users and ftp server. In this case you need to define an exception and attach this exception to your quota policy.

Destination IP: Set the destination IP address for this exception. You may also specify a network in the CIDR form (e.g. 10.0.0.0/16).

Destination Port: Set the destination port for this exception. You may specify a single port here. Different use cases are possible here. For example, you may skip defining destination IP and set

destination port as 22. This allows all SSH traffic to match this exception regardless of the destination IP address.

Day of Week Range: Set a filter for week range.

Time Range: Set when the exception will match during day. Again, different use cases are possible here. For example, you may want that FTP exception match only during work hours. In this case, you can set Day of Week Range to Monday-Friday and Time Range to 08:00:00-17:00:00.

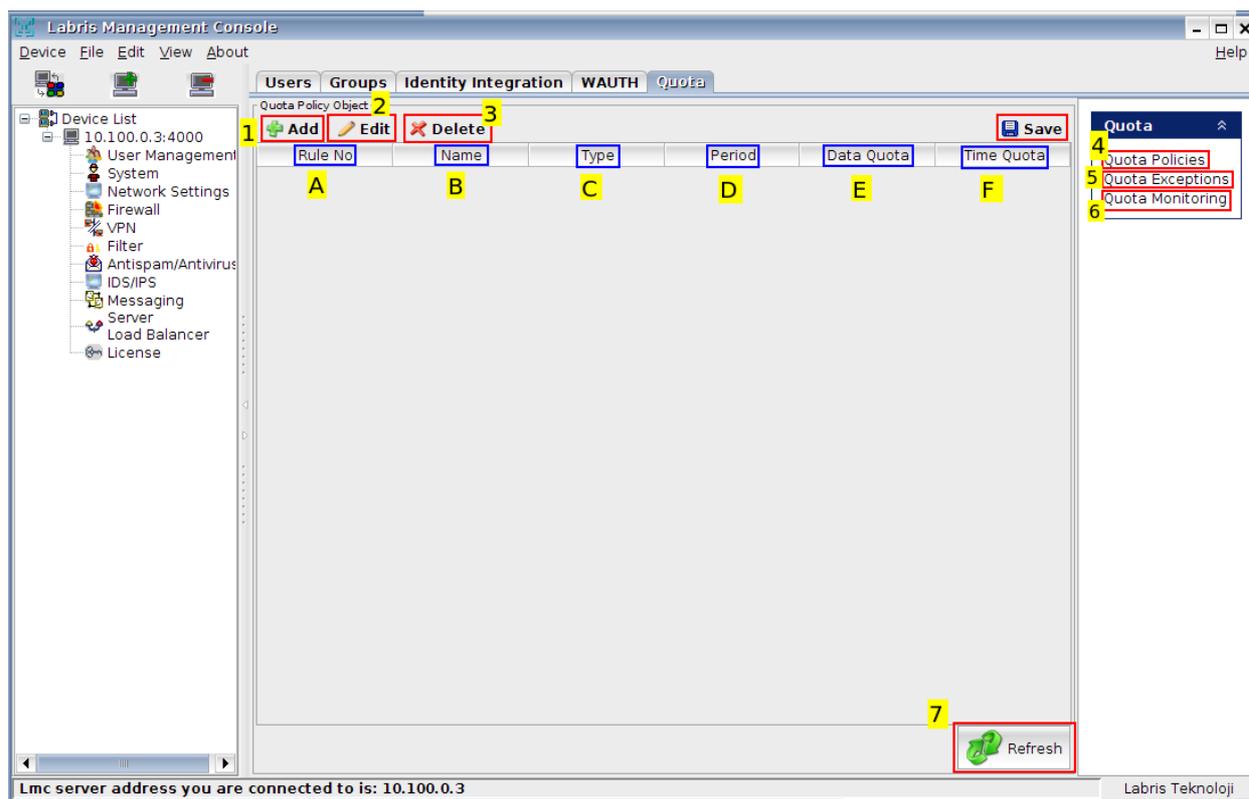
Creating a Simple Quota Policy with Single Quota Exception

This is a simple scenario with general 5 GB download limit, 20 GB download exception for SSH and 20 GB upload exception for SSH. SSH exception is defined for work hours. Both policy period and SSH exception period are set to one month.

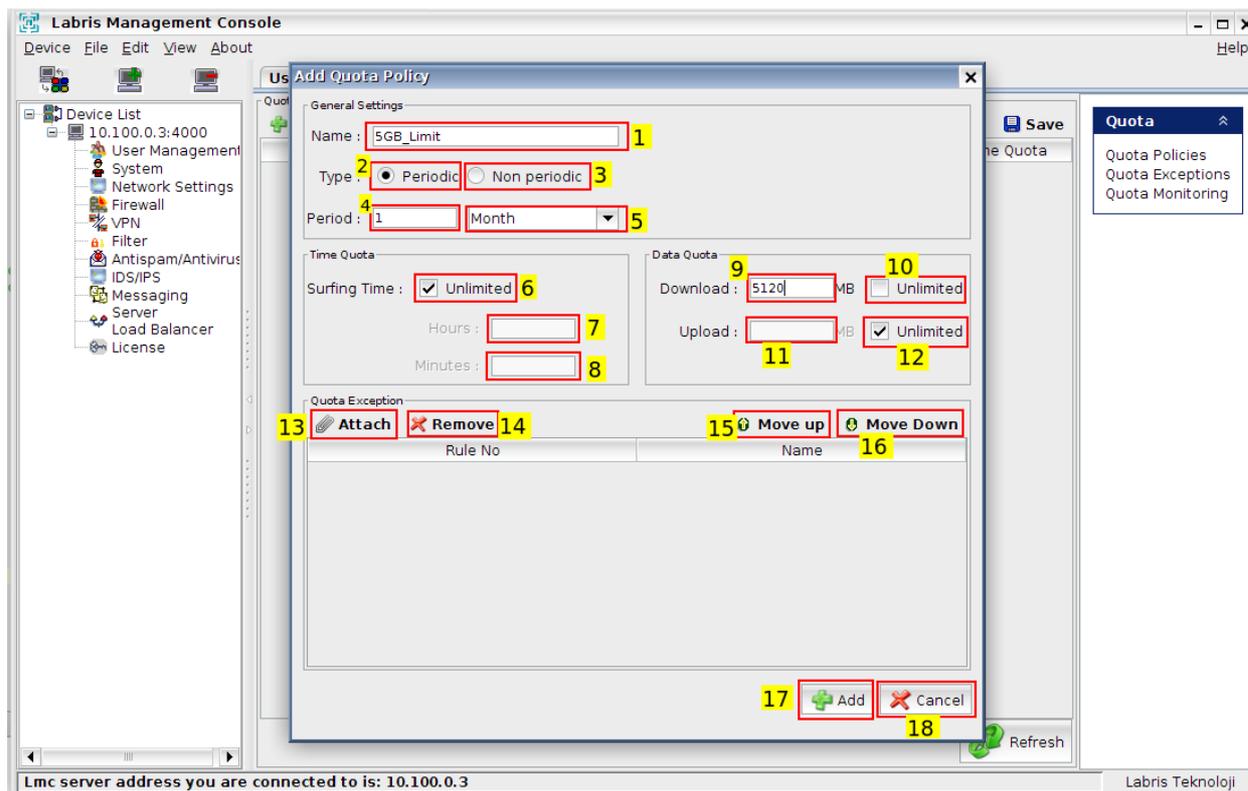
Quota Policy Creation

This is the main screen of quota. By default, Quota Policies screen is open. You can add new policy, edit or delete existing policies here. Right sidebar allows hopping to other screens: Quota Exceptions, Quota Monitoring.

Note: Do not forget pressing Save after adding/editing/deleting. Otherwise your changes will be lost.



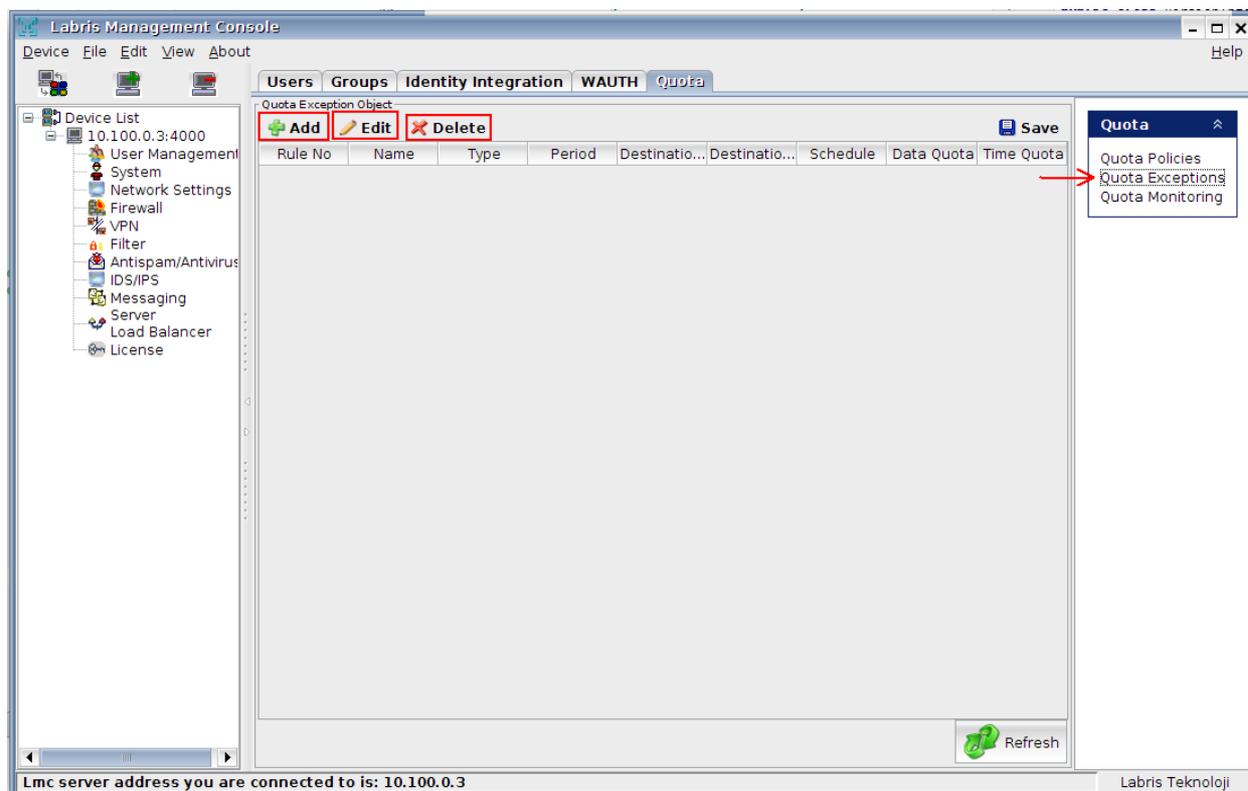
No	Name	Description
1	Add Policy	Create a new quota policy
2	Edit Policy	Edit an existing quota policy
3	Delete Policies	Delete existing quota policy
4	Quota Policies	Open Quota Policies screen
5	Quota Exceptions	Open Quota Exceptions screen
6	Quota Monitoring	Open Quota Monitoring screen
7	Refresh	Refresh policies exceptions and monitoring data (unsaved changes will be lost)
8	Save	Save Quota Policies to UTM. Omitting save step will cause changes to be lost
A	Rule No	Number of quota policy
B	Name	Name of quota policy
C	Type	Periodic or non-periodic
D	Period	Show if policy is periodic
E	Data Quota	Show data quota of policy
F	Time Quota	Show time quota of policy

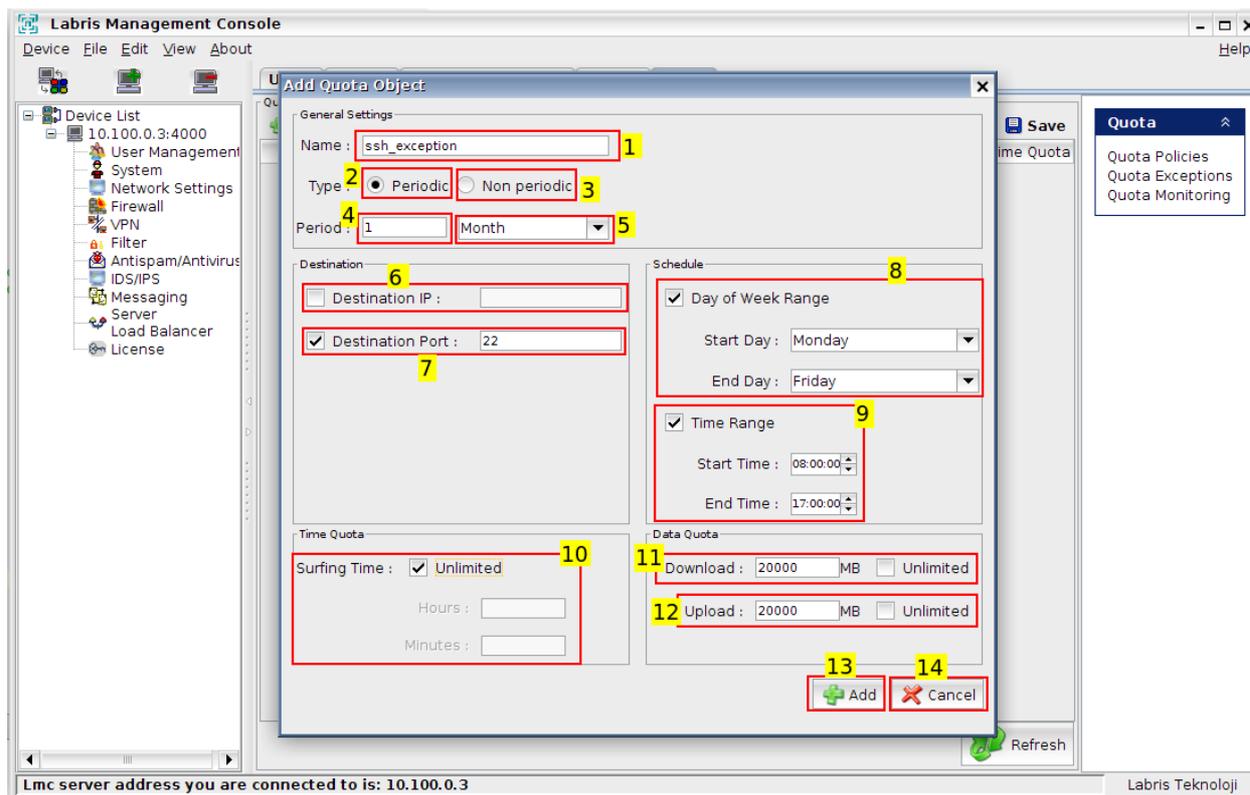


No	Name	Description
1	Policy Name	Name of the policy. This name will be used when assigning to users/groups.
2	Periodic	Usage will be zeroed at the end of period.
3	Non-periodic	Usage will not be reset. Limits are final.
4	Period count	Period count.
5	Period unit	Possible values are: Day, Week, Month, Year
6	Unlimited surfing time	Don't set a limit for surfing time. Disables Hours and Minutes fields.
7	Surfing Time Hour Limit	Set how many hours a user is allowed to surf. Combination with minutes field is possible.
8	Surfing Time Minute Limit	Set how many minutes a user is allowed to surf. Combination with hours field is possible.
9	Quota Download Limit	Set how many megabytes a user is allowed to download.
10	Unlimited Quota Download	Don't set a limit for download.
11	Quota Upload Limit	Set how many megabytes a user is allowed to upload.
12	Unlimited Quota Upload	Don't set a limit for upload.
13	Attach New Exception	Attach an existing quota exception to this policy.
14	Remove an Exception	Remove an already attached quota exception from this policy.
15	Move chosen exception up	Move attached exception up in the order.
16	Move chosen exception down	Move attached exception down in the order.
17	Add	Complete policy creation
18	Cancel	Cancel policy creation

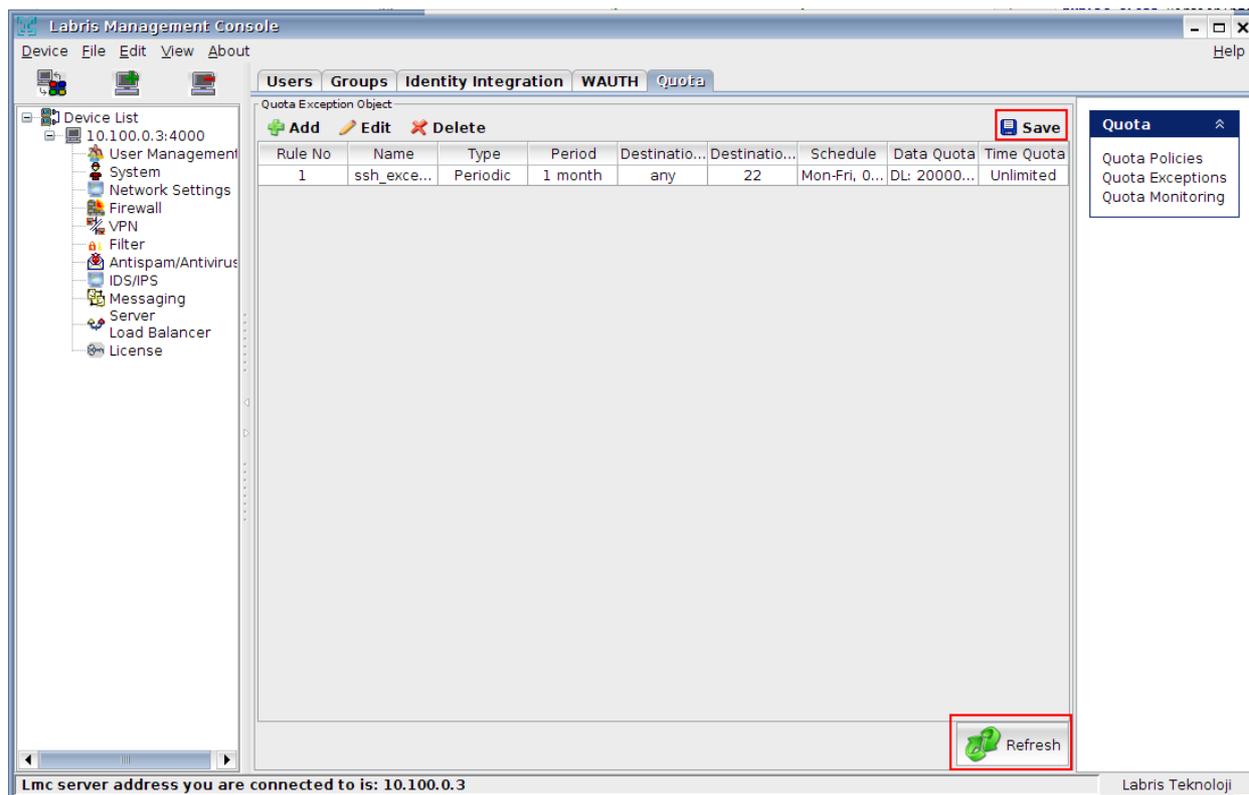
Quota Exception Creation

This is Quota Exceptions screen. Don't forget pressing save after exception create/edit/delete.

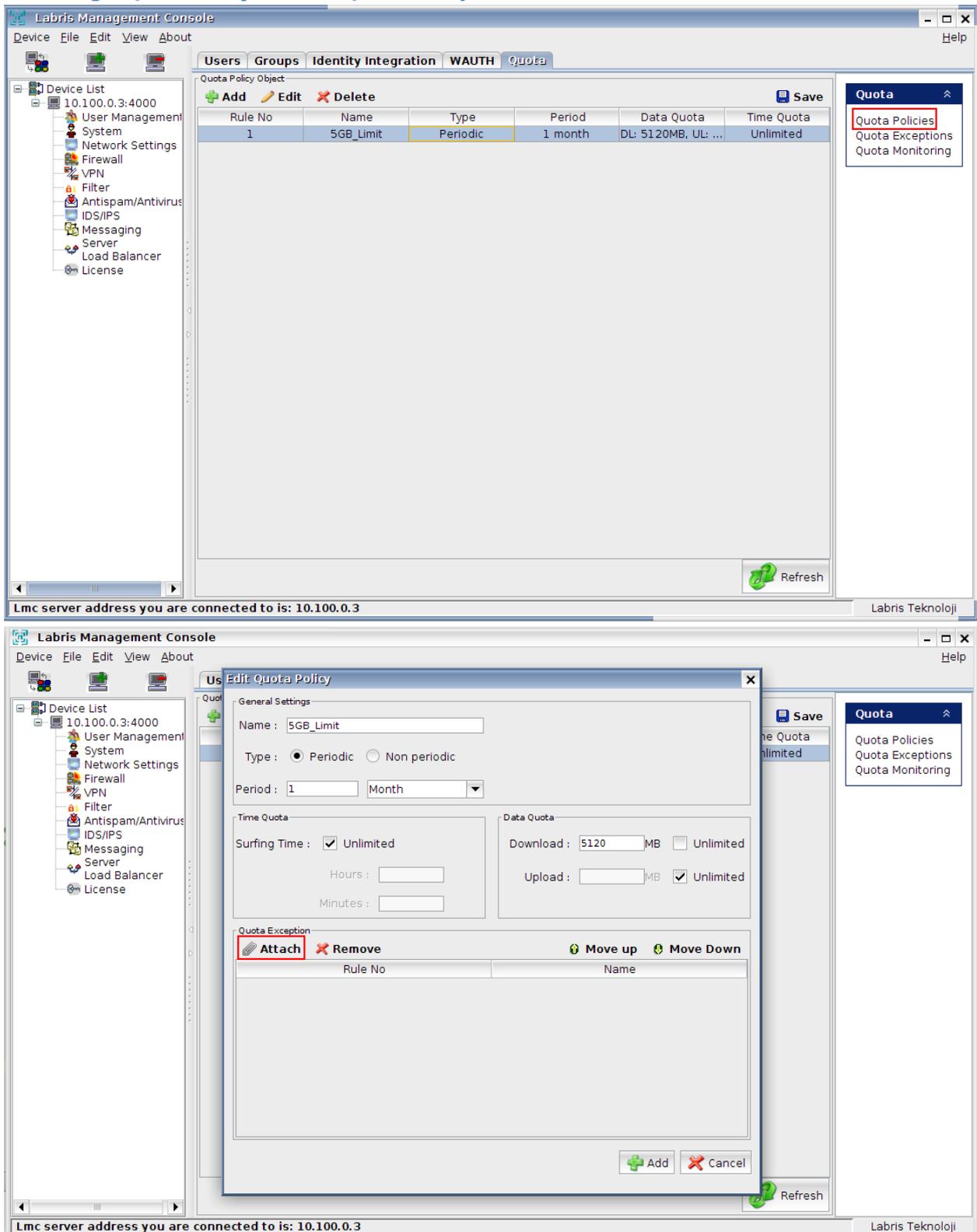


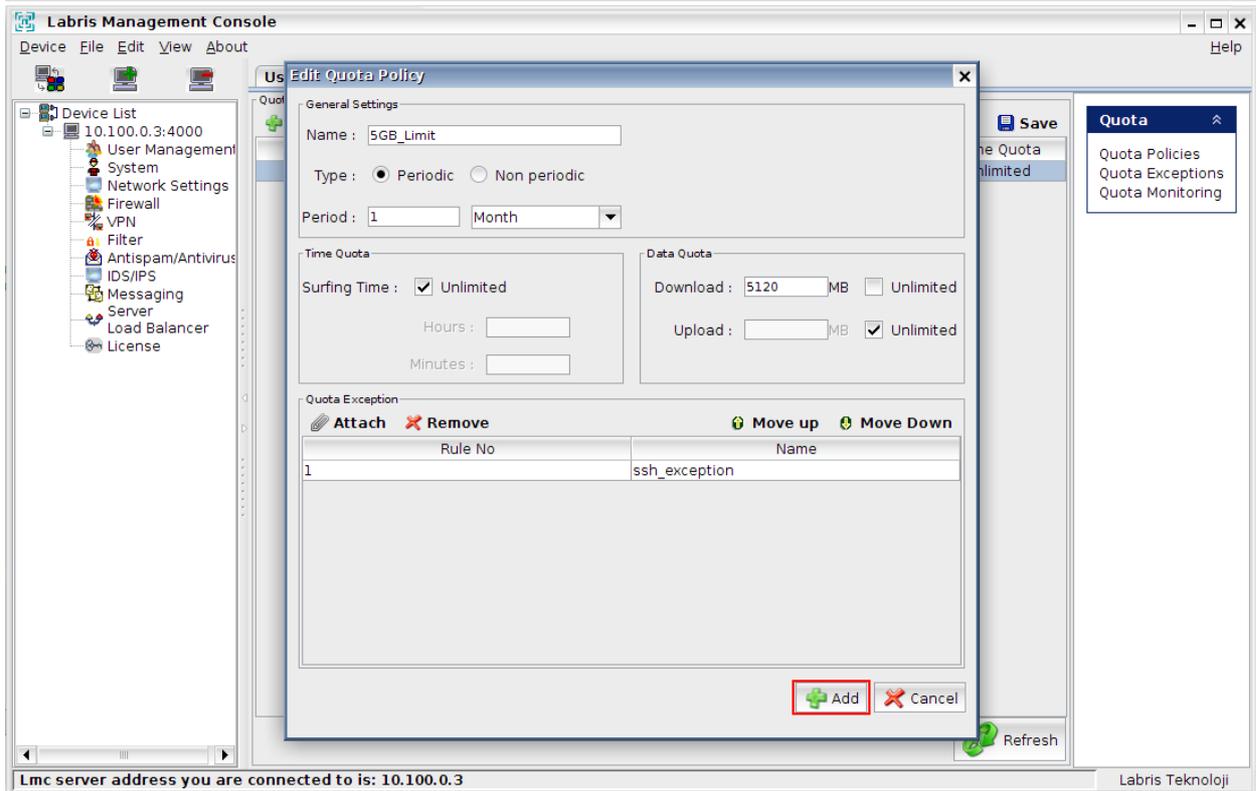
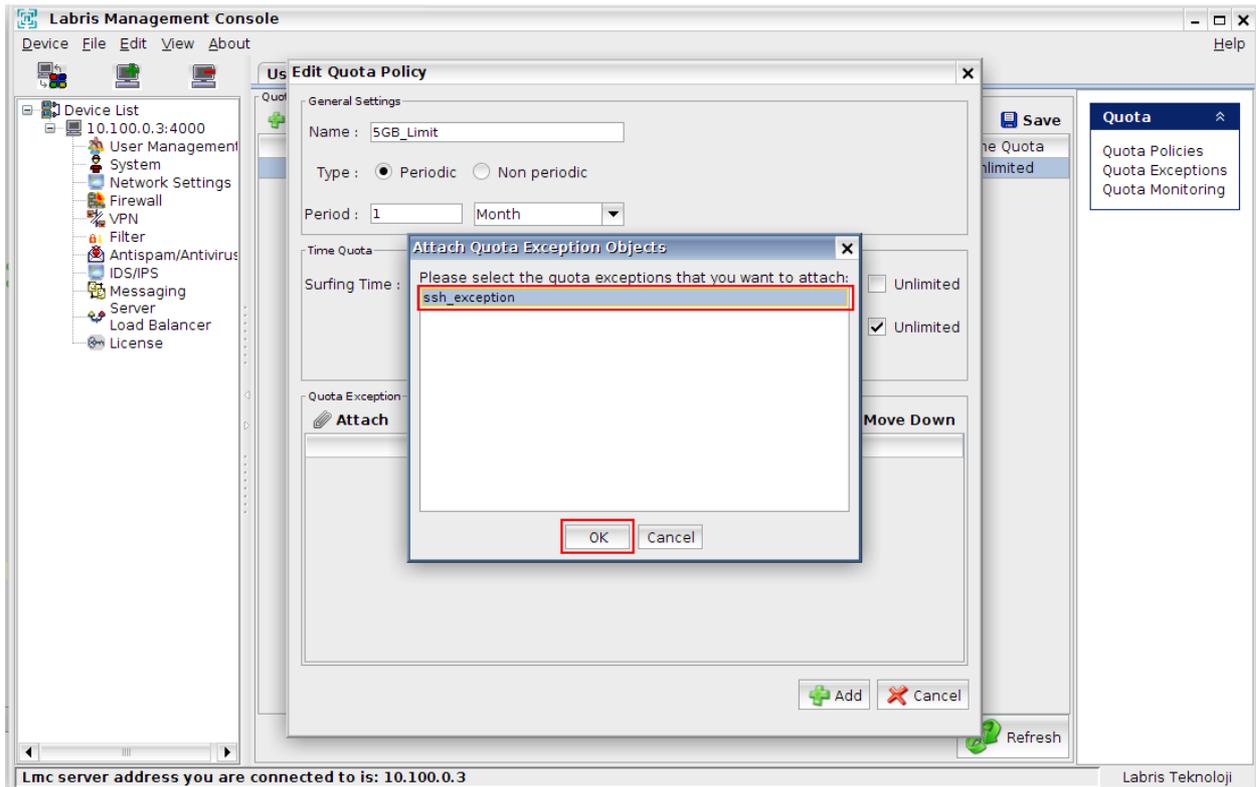


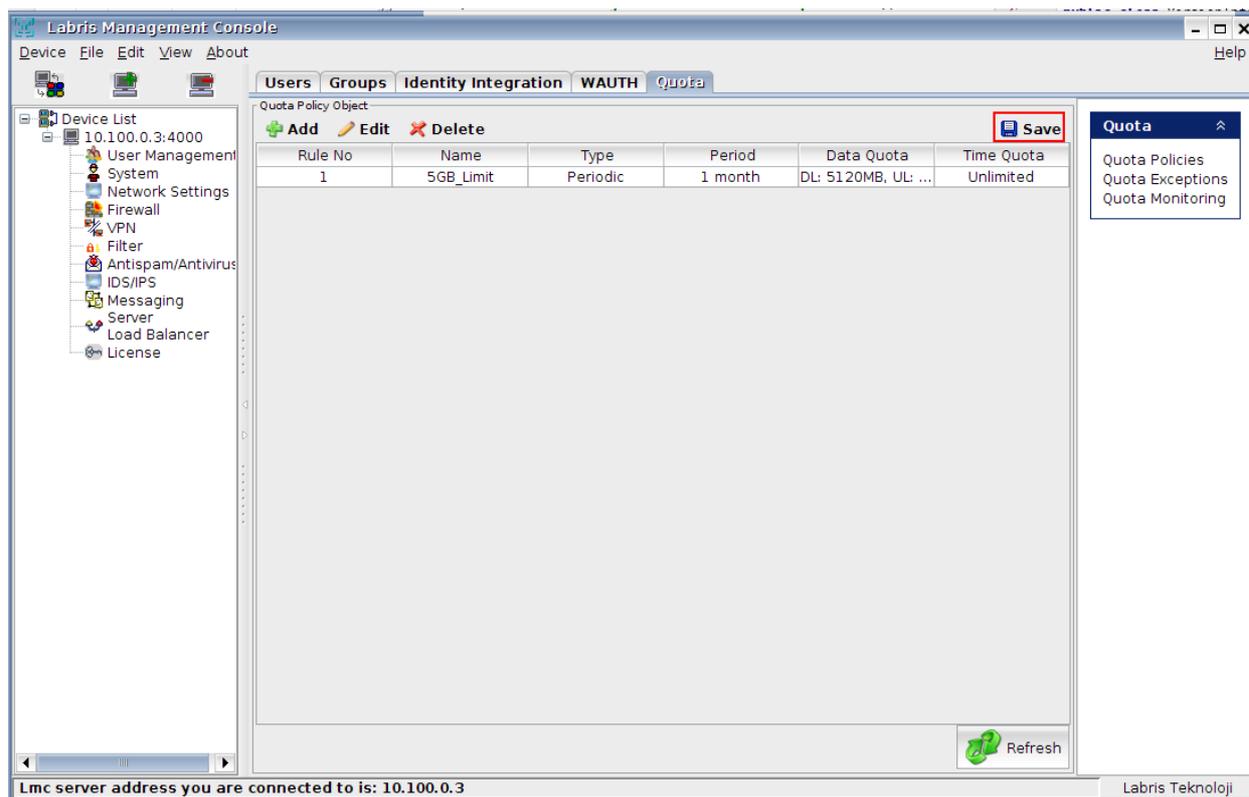
No	Name	Description
1	Exception Name	Name of the exception. This name will be used when attaching exception to a policy.
2	Periodic	Usage will be zeroed at the end of period.
3	Non-periodic	Usage will not be reset. Limits are final.
4	Period count	Period count.
5	Period unit	Possible values are: Day, Week, Month, Year.
6	Destination IP/Net	Destination IP Address or Network (CIDR) for this exception.
7	Destination Port	Destination port for this exception (only one port).
8	Day of Week Range	Which days this exception will match.
9	Time Range	Which hours this exception will match.
10	Surfing time	Set time limits for this exception.
11	Download Limit	Set download limit for this exception.
12	Upload Limit	Set upload limit for this exception.
13	Add	Complete exception creation.
14	Cancel	Cancel exception creation.



Attaching a Quota Exception to a Quota Policy



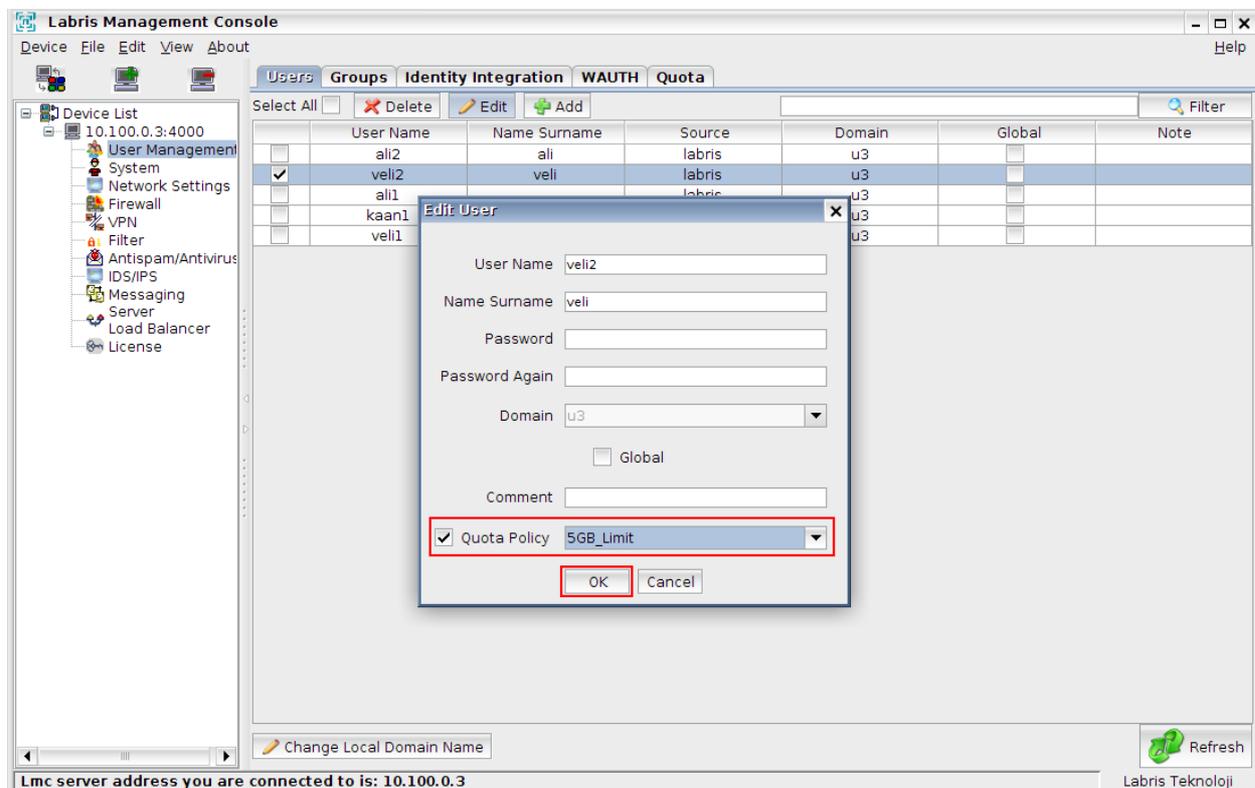
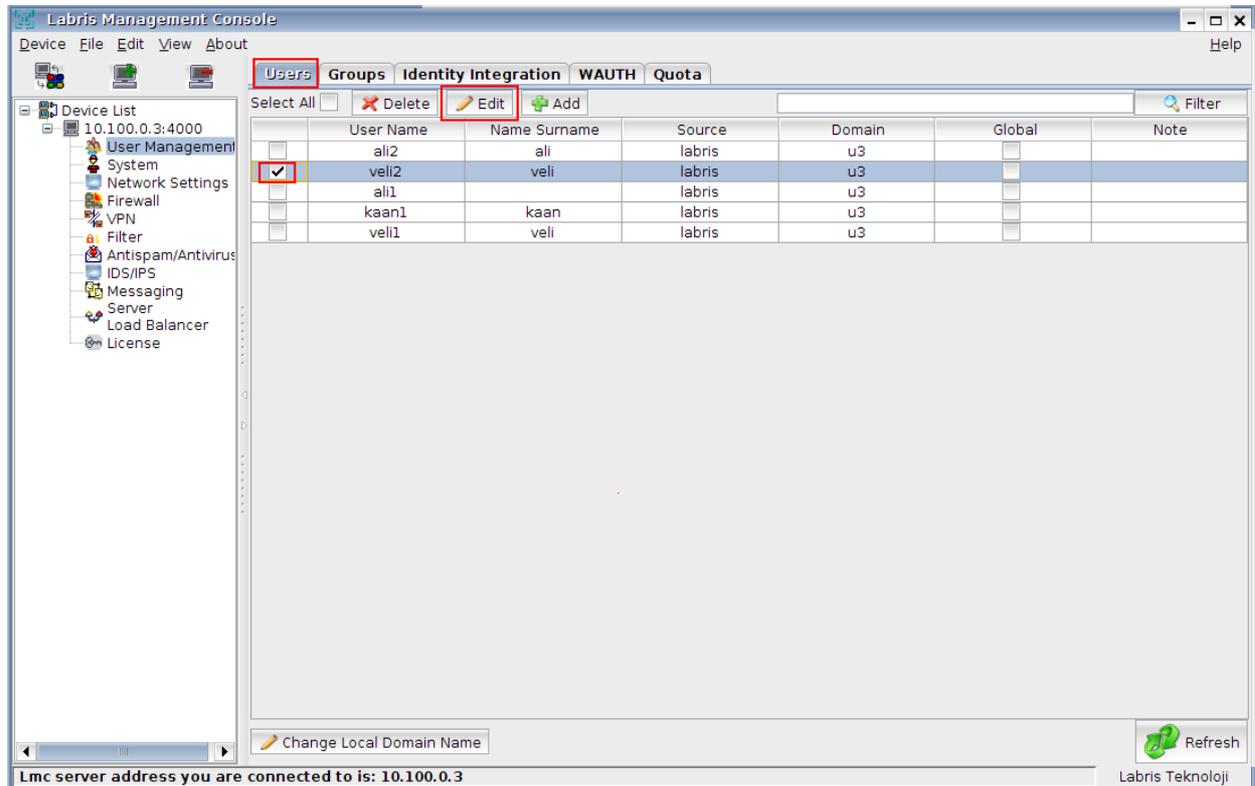


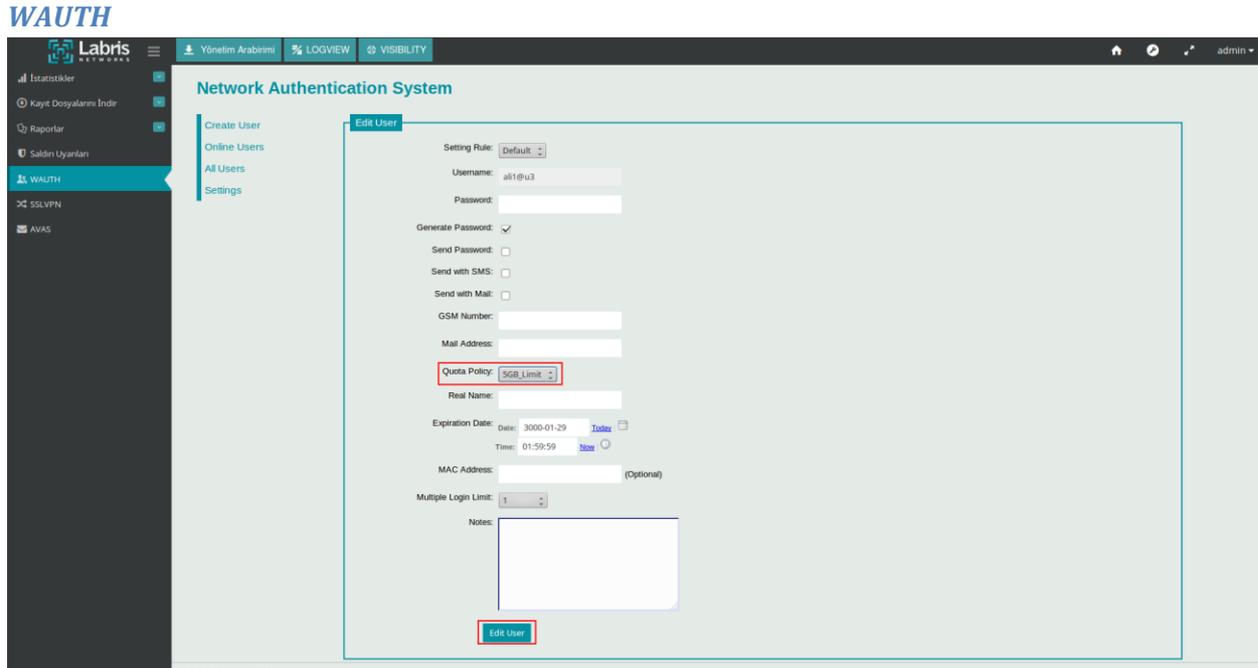


Assigning a Quota Policy to User

After defining a policy (and exceptions), you need to assign users to this policy. This is possible in both LMC and WAUTH.

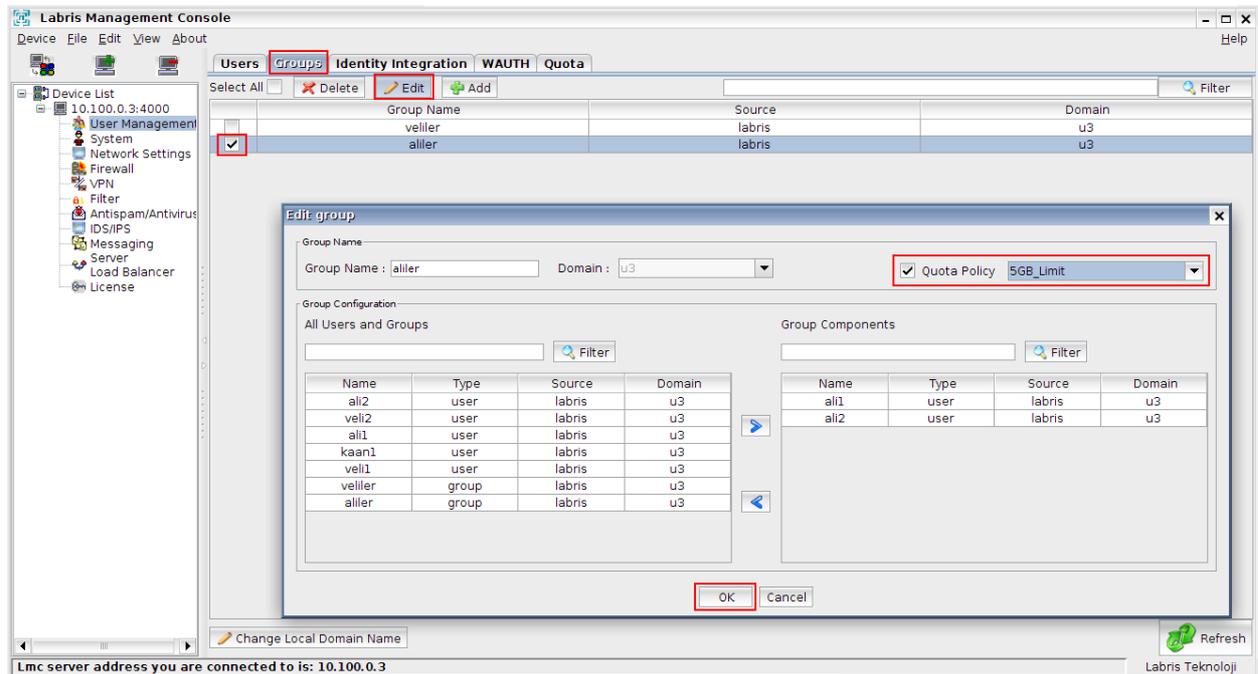
LMC





Assigning a Quota Policy to Group

Assignment to groups are only possible in LMC. When you assign a policy to group, all users not having a quota policy before are associated with new quota policy. If a user is specifically assigned a quota policy before, policy of this user will not be changed with group quota assignment.

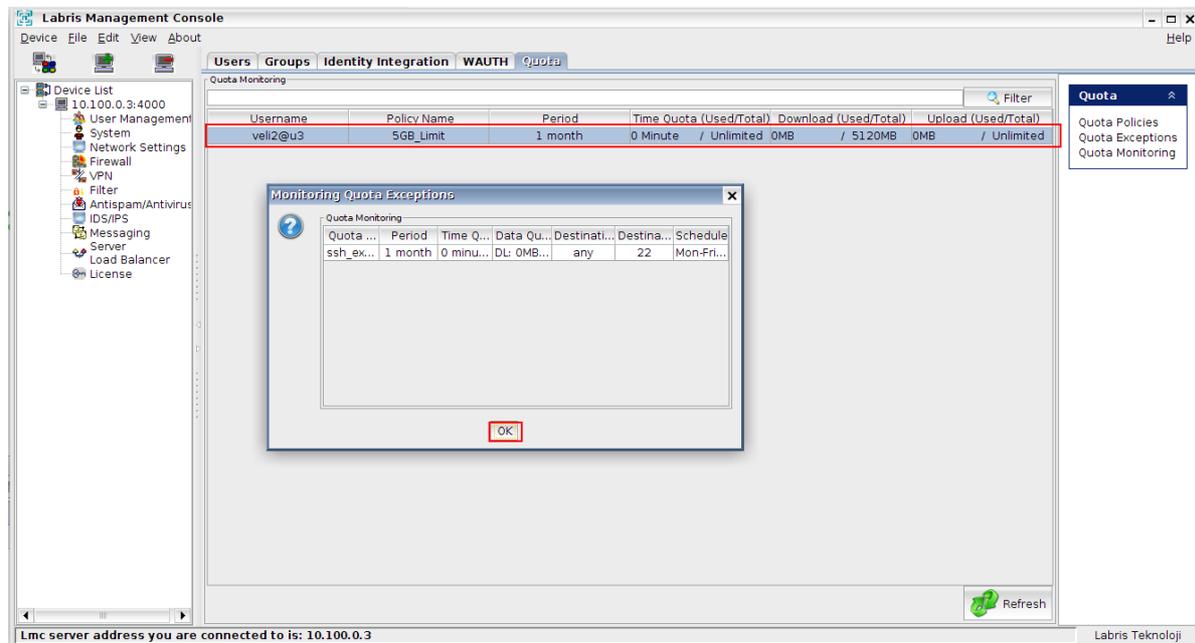
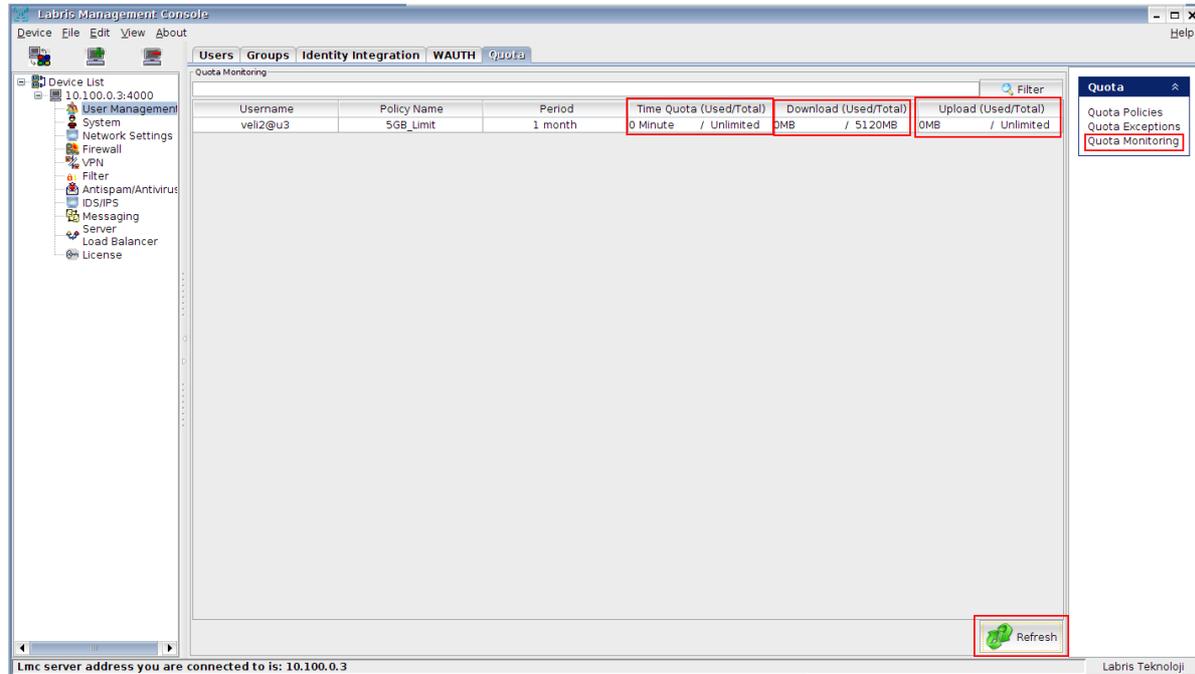


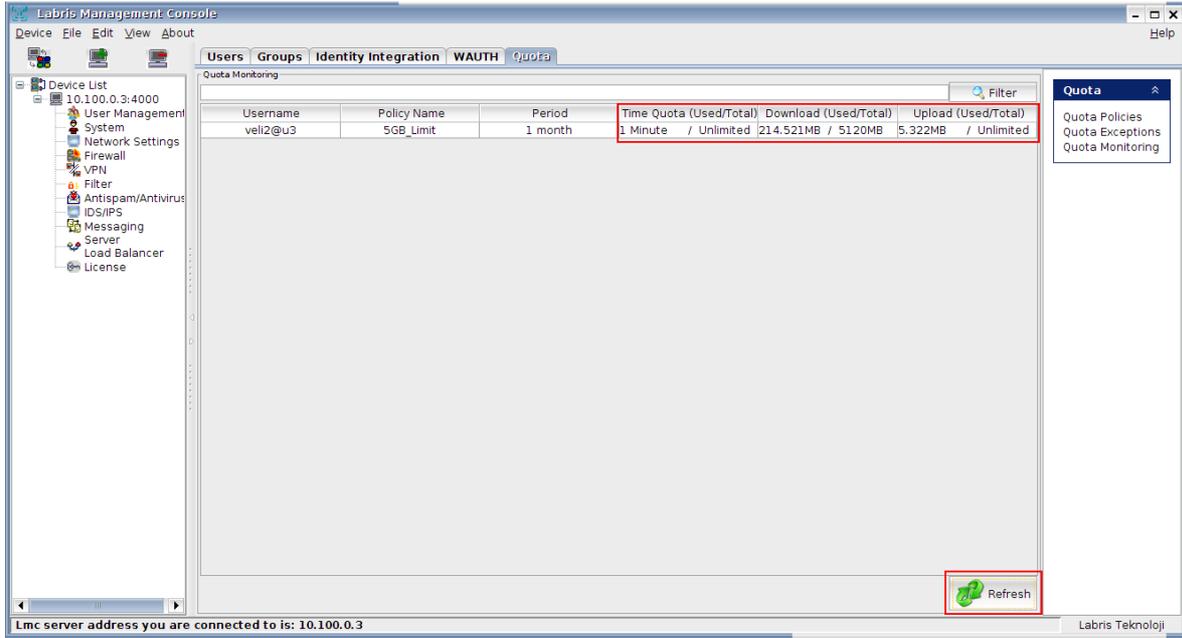
Monitoring Quota Usage

Usages of all users can be monitored in LMC. Additionally, a single user can see own usage in WAUTH Welcome screen. Monitoring in LMC is more detailed since you can examine by policy and see all exception usages also. On the other hand, a user can only see only policy usage in welcome screen. Exceptions and usages belong to them are not listed.

LMC

Double clicking on a usage shows exception usage.





WAUTH Welcome Screen

Labris Wauth+

Ağ Yetkilendirme Sistemi

Sisteme erişiminiz kabul edildi. Tarayıcınızın adres çubuğunu kullanarak gezintinize başlayabilirsiniz.

Bu pencereyi kapatmayınız

Kullanıcı Adı	veli2
Ad Soyad	veli
Silinme tarihi	Silinme Yok
İndirme Kotası	0 MB / 5120 MB
Gönderme Kotası	0 MB / Sınırsız
Zaman Kotası	Kullanım Yok / Sınırsız

Çıkış

Şifre Değiştir

Labris Wauth+

Ağ Yetkilendirme Sistemi

Sisteme erişiminiz kabul edildi. Tarayıcınızın adres çubuğunu kullanarak gezintinize başlayabilirsiniz.

Bu pencereyi kapatmayınız

Kullanıcı Adı	veli2
Ad Soyad	veli
Silinme tarihi	Silinme Yok
İndirme Kotası	214 MB / 5120 MB
Gönderme Kotası	5 MB / Sınırsız
Zaman Kotası	1 dakika / Sınırsız

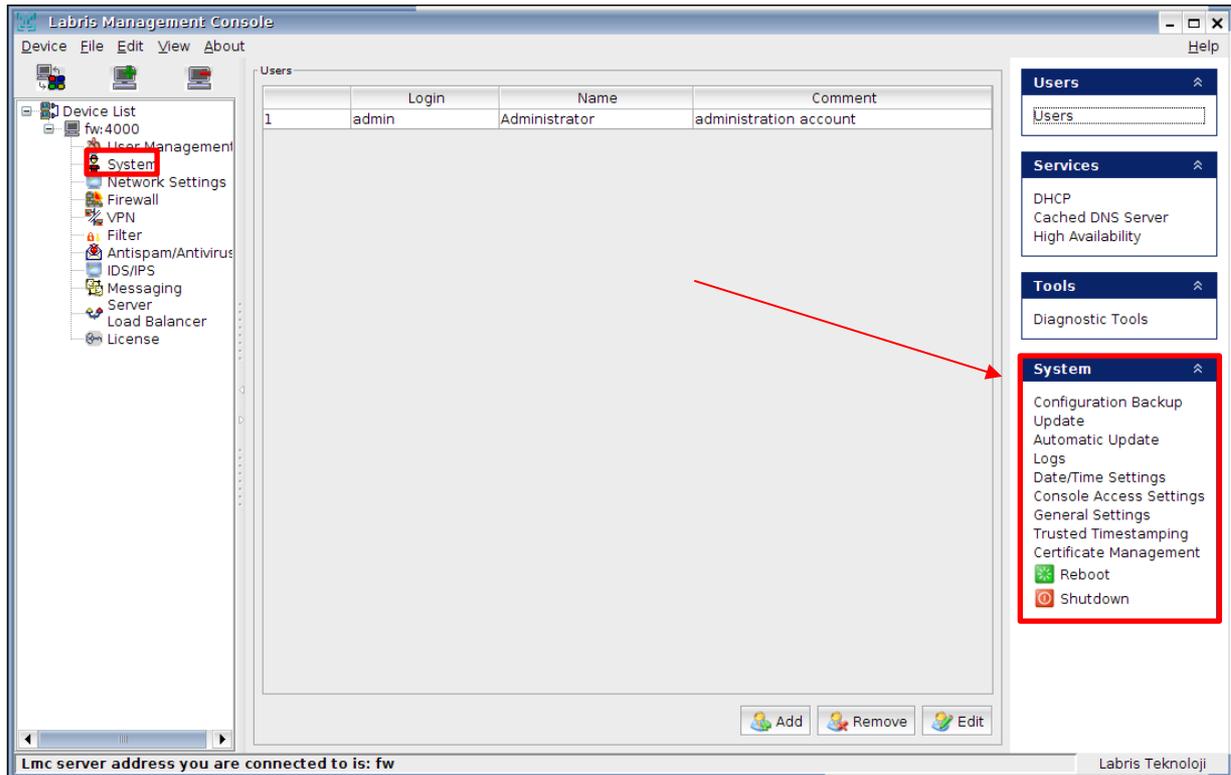
Çıkış

Şifre Değiştir

System

System Tab in the LMC provides us with different options like **DHCP , DNS , Date / Time settings , Configuring backup's , update , automatic updates , logs and general settings.**

All the above mentioned options can be **configured** under **System Module**. When we are connected to **System Module** below screen appears.

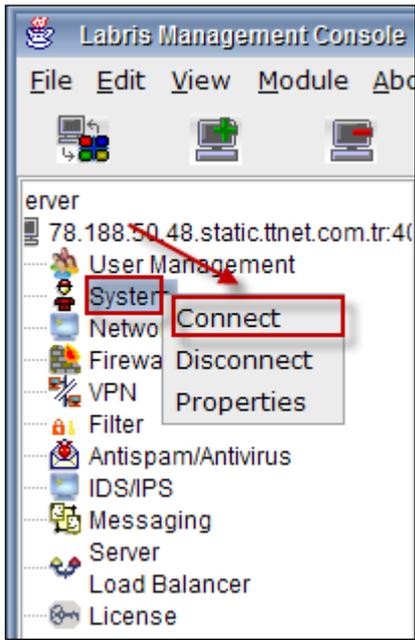


Viewing Options in System

When we Right click on **“System Tab”** we find following options.

1	Connect	It enables us to Connect to the System Module
2	Disconnect	It enables us to Disconnect from System Module
3	Properties	It helps us to view properties of System Module in LMC

26. System LMC Module

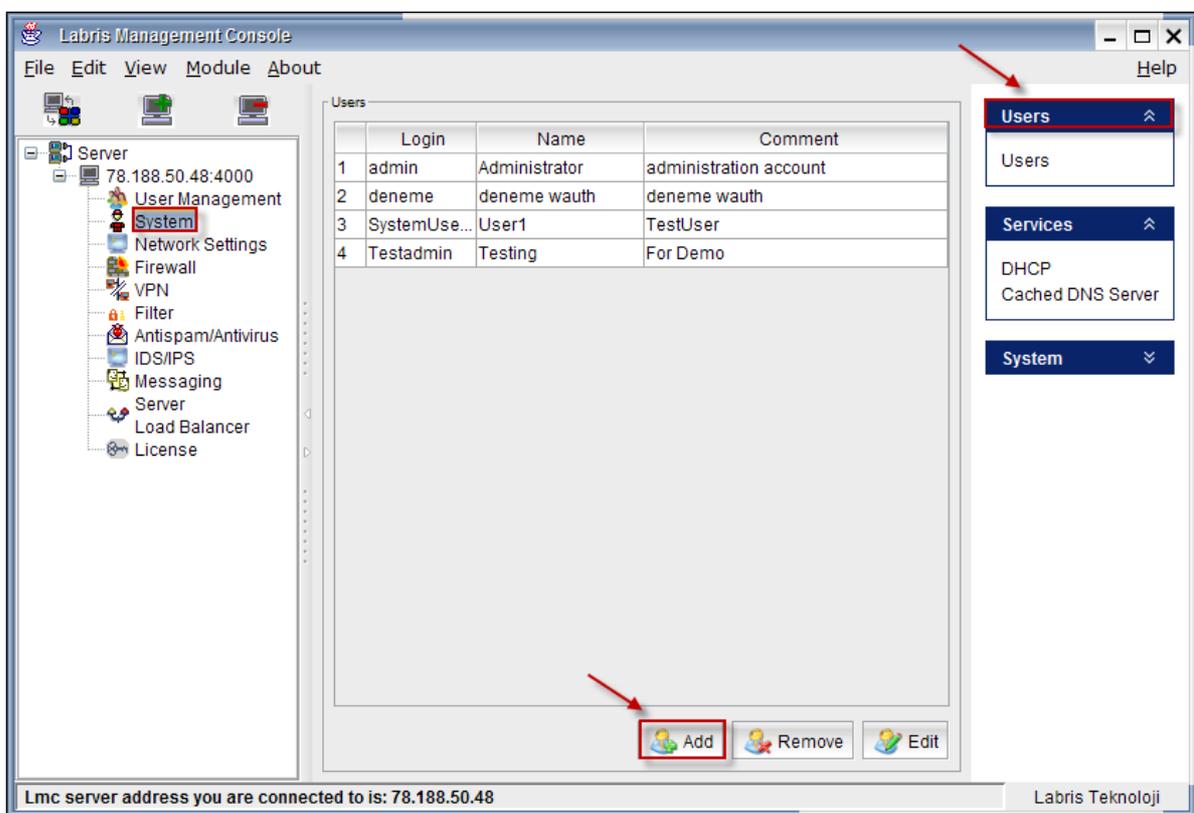


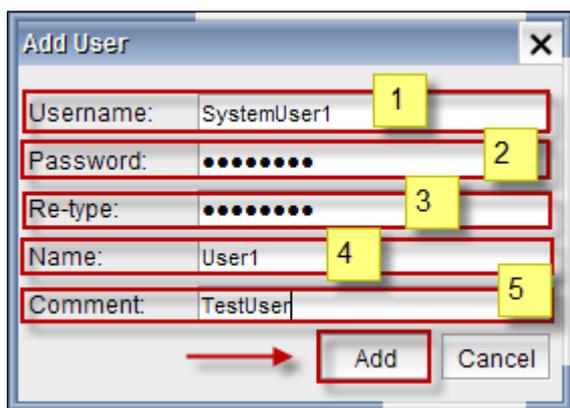
Users

In **System Module** on the right pane you can find **Users** tab in that click on **Users**

Adding User

Click on **Add** Tab to add a New User in **System** Module.

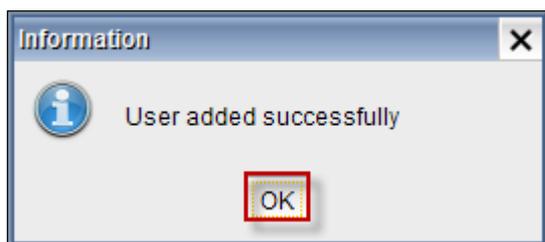




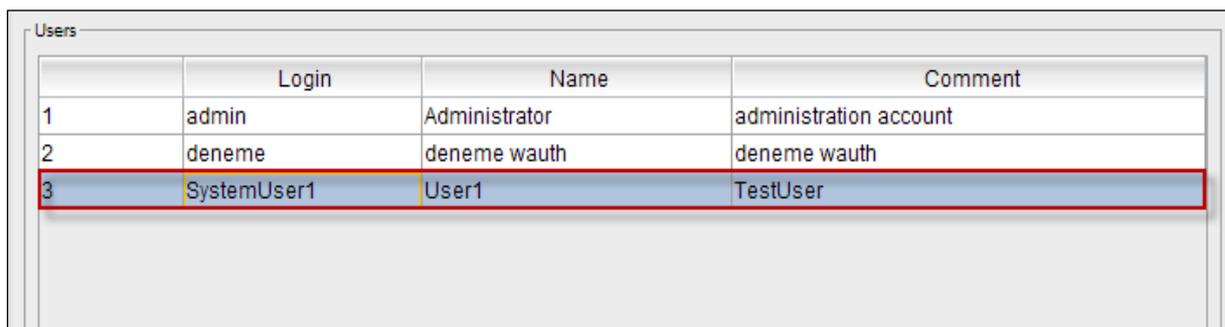
These are the inputs for adding a **New User**

1	Username	Type the name of the Username of the new User
2	Password	Type the Password of the new User
3	Re-type	Re-Type Password of the new User for confirmation
4	Name	Type the Name of the new User
5	Comment	Type reason for the User creation (Optional)

Below screen appears stating that **User added successfully**, click **OK** to close the current tab



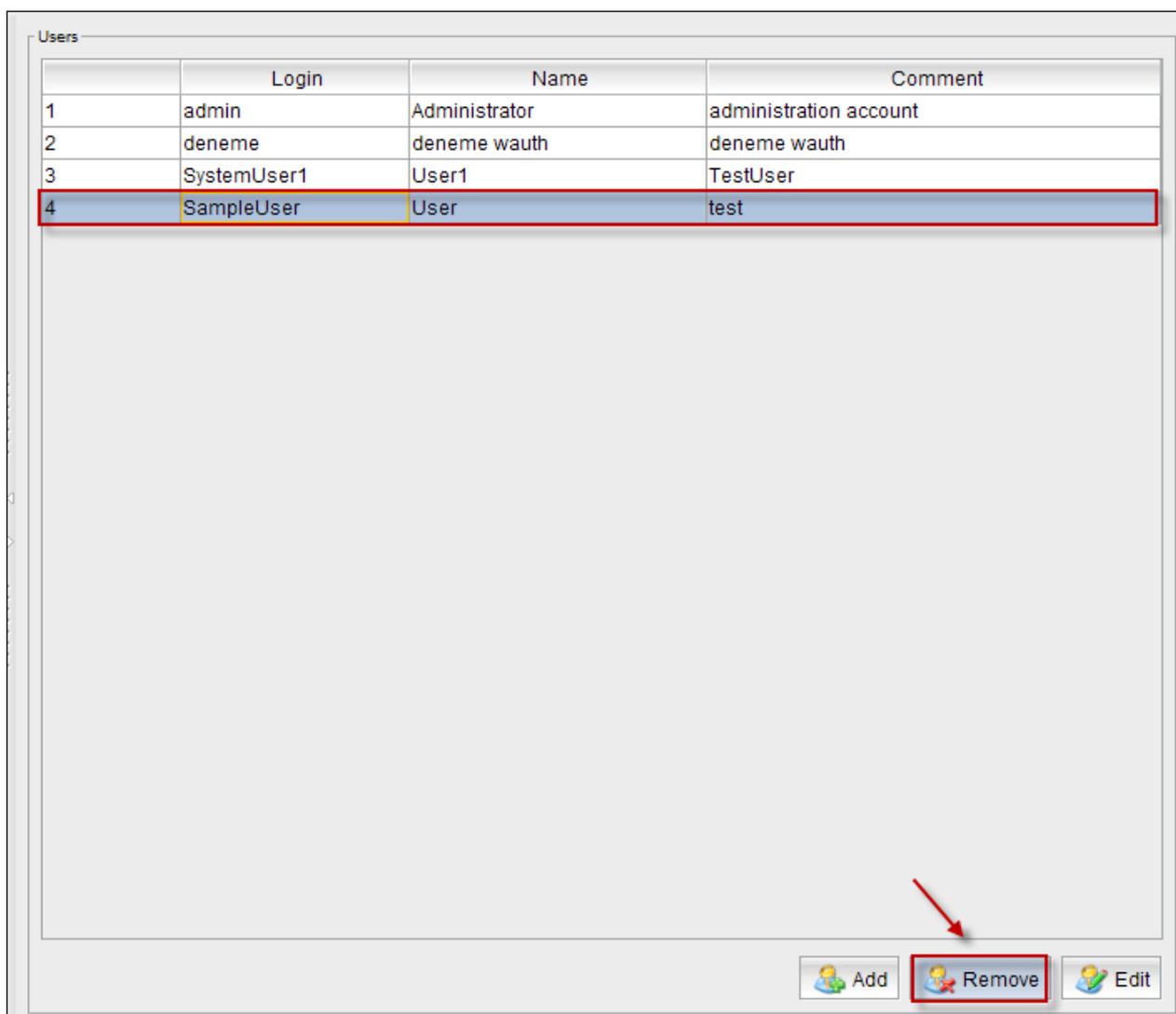
We can notice **new User** added in the **User's** list of **System Module**



	Login	Name	Comment
1	admin	Administrator	administration account
2	deneme	deneme wauth	deneme wauth
3	SystemUser1	User1	TestUser

Deleting User

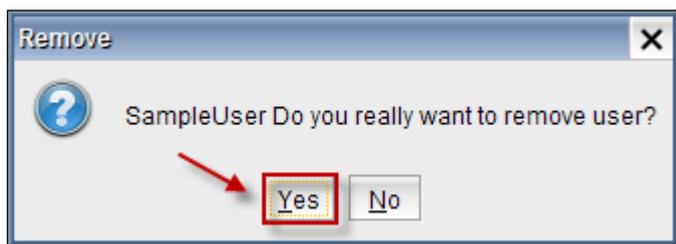
Select User and click on **Remove Tab** to delete an User.



	Login	Name	Comment
1	admin	Administrator	administration account
2	deneme	deneme wauth	deneme wauth
3	SystemUser1	User1	TestUser
4	SampleUser	User	test

At the bottom right of the interface, there are three buttons: Add, Remove, and Edit. A red arrow points to the Remove button.

When the below screen appears, click **Yes** to remove User.

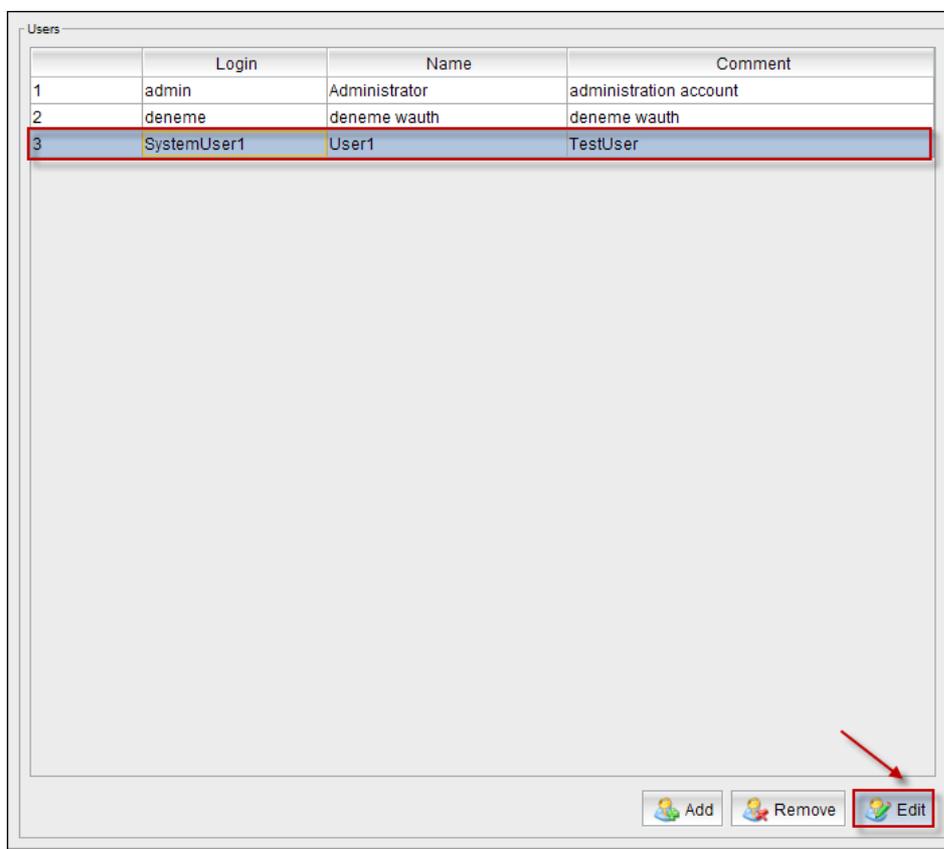


Alert screen appears displaying User removed successfully; click **Ok** to close the current tab.



Change Password / Editing User

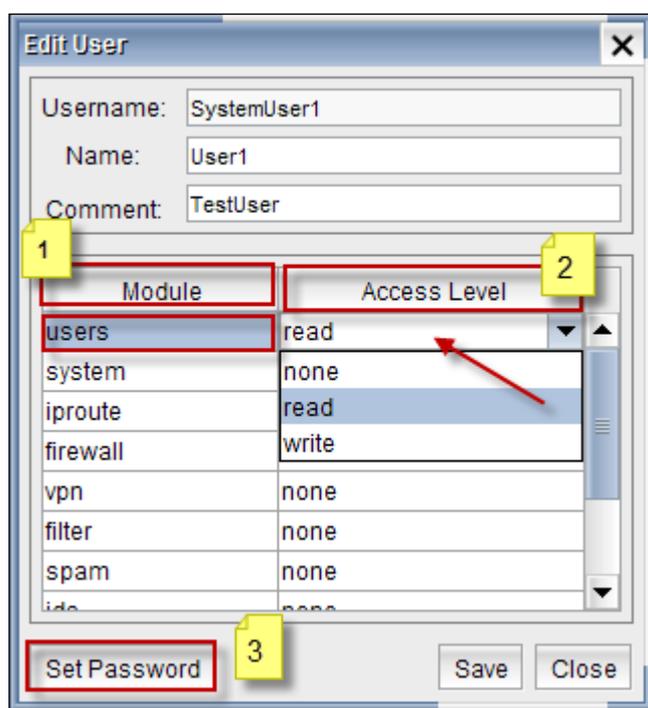
Select the user from the list and click on **Edit**



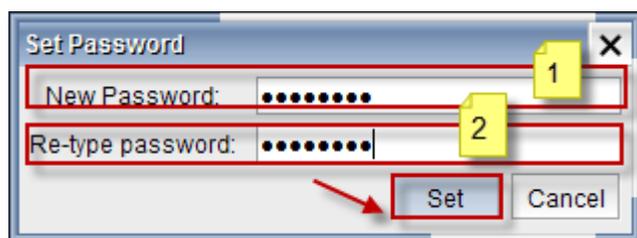
Viewing options in Edit User

1	Module	Displays all the Modules in LMC
2	Access level	Displays access level of each Module
3	Set Password	This option helps to Set Password to the User

Select the **Module** and choose **Access level** from the drop down menu as shown below



When we click on **Set Password**, below screen appears.



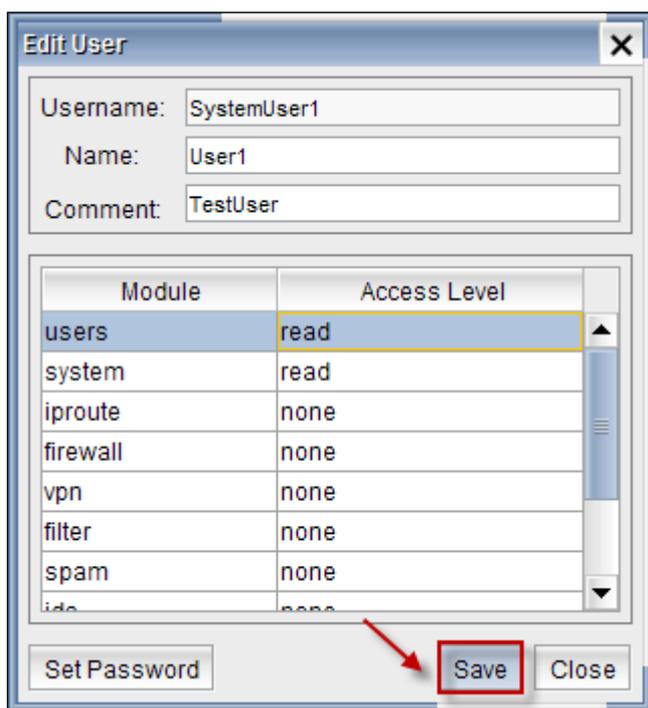
1	New Password	Type password of the User
2	Re-type Password	Re-type Password of the User for confirmation

Click on **Set Tab** to set New Password

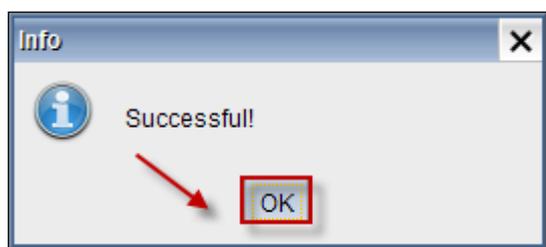
Below screen appears stating that password is changed successfully, Click **Ok** to close the current tab.



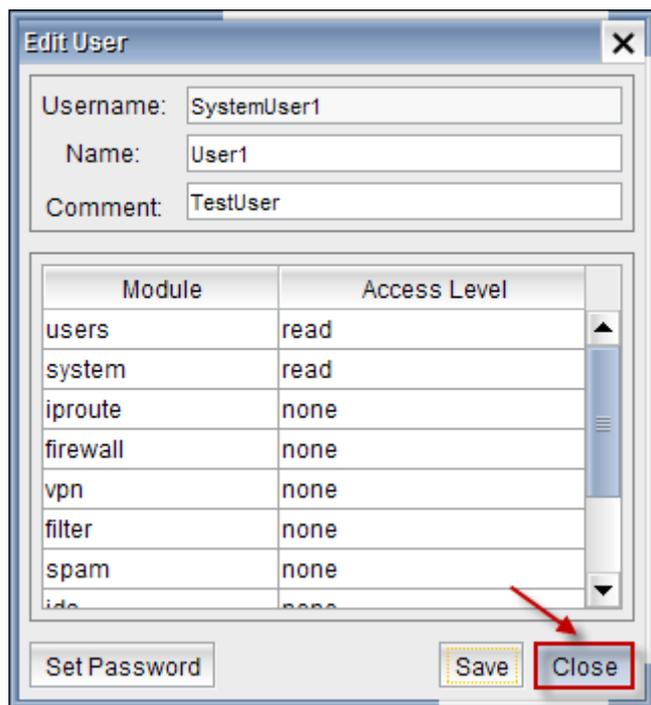
Click on **Save Tab** to save changes.



When the below screen appears, click **Ok**.



Click on **Close Tab**



27. DHCP

DHCP: DHCP stands for **Dynamic Host Configuration Protocol**

DHCP server provides IP address and other related configuration information like subnet mask and default gateway to the host systems within a LAN network. For every computer it will provide unique IP to identify the system.

By our configuration settings IP address will change certain period of time for the host systems

DHCP is useful in extremely larger networks where we want to centralize the IP management to reduce human errors.

ISP (Internet Service Provider)

Usually **ISP's** implement **DHCP** servers

DHCP is a server which assigns IPs automatically to the clients requested from a range of IPs.

IP leasing process:

1. **DHCP discover:** The client machine when turned on, broadcasts the network id, broadcast id and MAC address on Network for discovering **DHCP** server.
2. **Offer:** The **DHCP** server listening to the request made by the client offers a pool of IP addresses to the client machine.

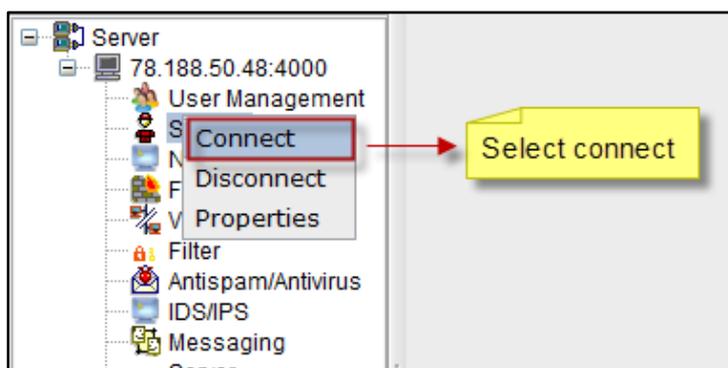
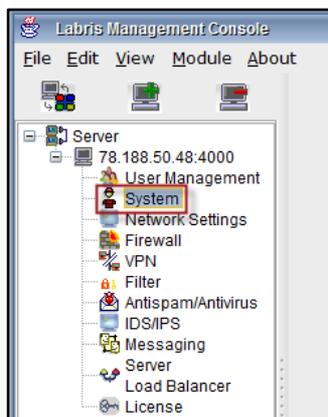
3. **Selection:** The client machine on receiving the pool of IP address selects an IP and requests the **DHCP** server to offer that IP.

4. **Acknowledgement:** The **DHCP** sends a confirmation about the allotment of the IP assigned to the client as an acknowledgement.

5. **IP lease:** If the client machine is not restarted for 8 days, exactly after 4days the client machine requests the **DHCP** server to extend the IP lease duration, on listening to this the **DHCP** server adds 8 more days for existing 4 days which is 12 days

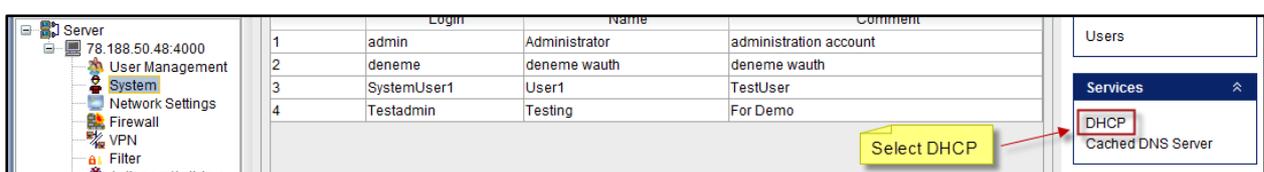
If the client machine is restarted again the **DHCP** lease process takes place and again the client gets an IP for 8 days.

Select **System** option from the Labris Management console

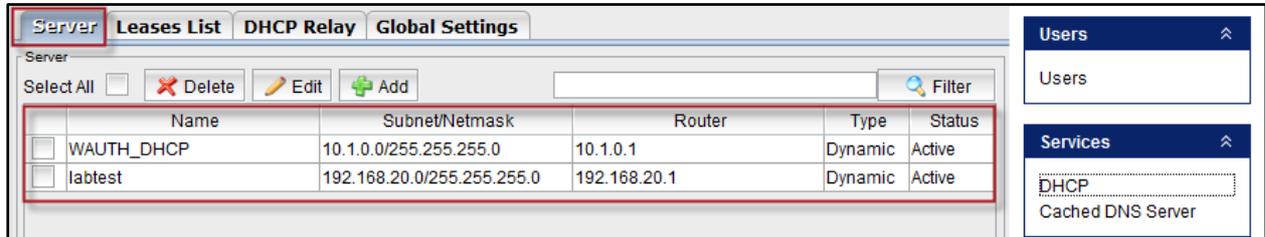


Right click on the System tab and click on **Connect** to get connected

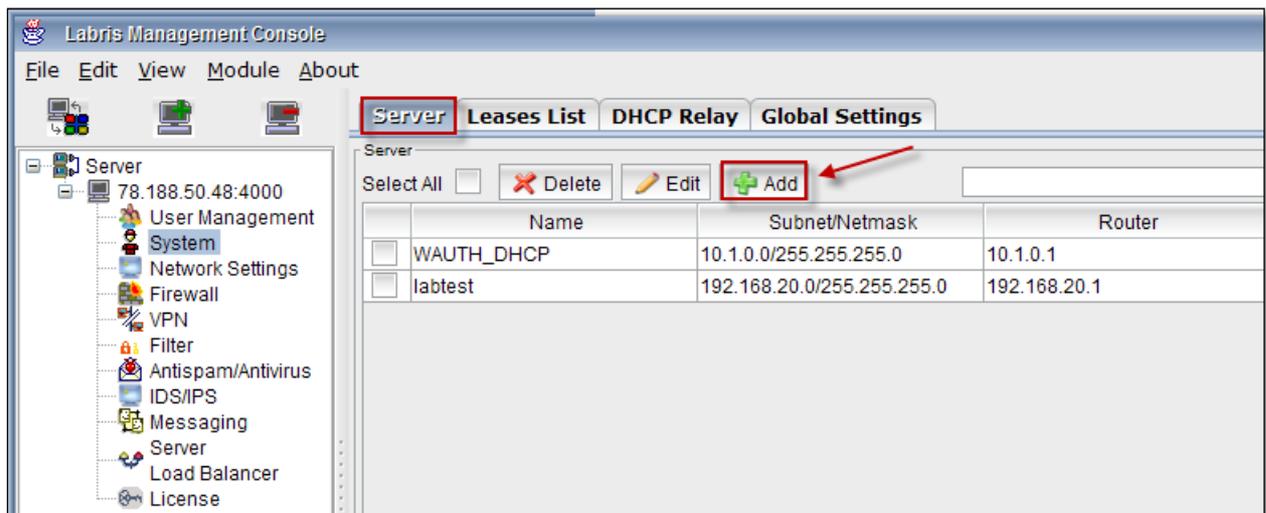
Select **DHCP** option under services.



Select **Server** tab to view the DHCP server details like **Name , Subnet , Router , Type and Status**.



Click on **Add** to Add the New DHCP Server details.



Make **DHCP** scope **Active** by enabling the **Active** checkbox. Select the **type** of the scope from the options mentioned here. In this screen we selected **Dynamic** option. Also Enable Use interface's IP address as router check box.

1	Scope Name	Type Scope name
2	Interface	Select Interface from drop down menu
3	IP Range	Mention Scope

Click on **Add Tab** to add an IP Range

The screenshot shows the 'Add Dhcp Scope' dialog box. The 'Settings' section is active, and the 'Dynamic' radio button is selected. The 'Scope Name' is 'TestScope', the 'Interface' is 'tun0 - 10.8.3.1', and the 'Netmask' is '/24 (255.255.255.0)'. The 'IP Address' field is checked to use the interface's IP address as the subnet. The 'Ip Range' is set to '10.8.3.10 - 10.8.3.80'. The 'Router' field is checked to use the interface's IP address as the router.

Continuation to the above screen, choose **Lease Time & Maximum Lease Time** from the scope and type **Domain Name**, Click on **Save** Tab.

Lease Time * 1440 5-144000 Minutes (100 Days)
Maximum Lease Time * 2880 5-144000 Minutes (100 Days)

Domain Name loak.com

DNS * Use router's IP address as DNS

Primary DNS
Secondary DNS

Advanced Settings Save

Saving changes is in progress.



Below screen appears stating that **Changes are saved and applied**, click **Ok** to close the current tab.



We can notice from the list that the Server is added

Server Leases List DHCP Relay Global Settings					
Server					
Select All <input type="checkbox"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Add"/> <input type="text"/> <input type="button" value="Filter"/>					
	Name	Subnet/Netmask	Router	Type	Status
<input type="checkbox"/>	WAUTH_DHCP	10.1.0.0/255.255.255.0	10.1.0.1	Dynamic	Active
<input type="checkbox"/>	labtest	192.168.20.0/255.255.255.0	192.168.20.1	Dynamic	Active
<input type="checkbox"/>	TestScope	10.8.3.0/255.255.255.0	10.8.3.1	Dynamic	Active

If we want to **Edit** the **IP Range**, Select IP Range and click on **Edit Tab**, modify the contents and Click **Ok** to apply changes

Add Dhcp Scope

Settings

Active Type Dynamic Static Ipsec

Scope Name *

Interface *

IP Address * Use interface's IP address as subnet

Netmask *

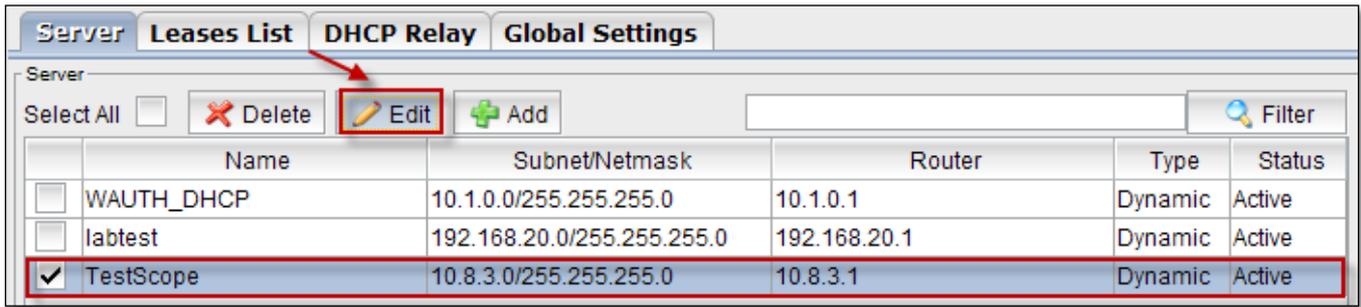
Ip Range * -

Edit

-

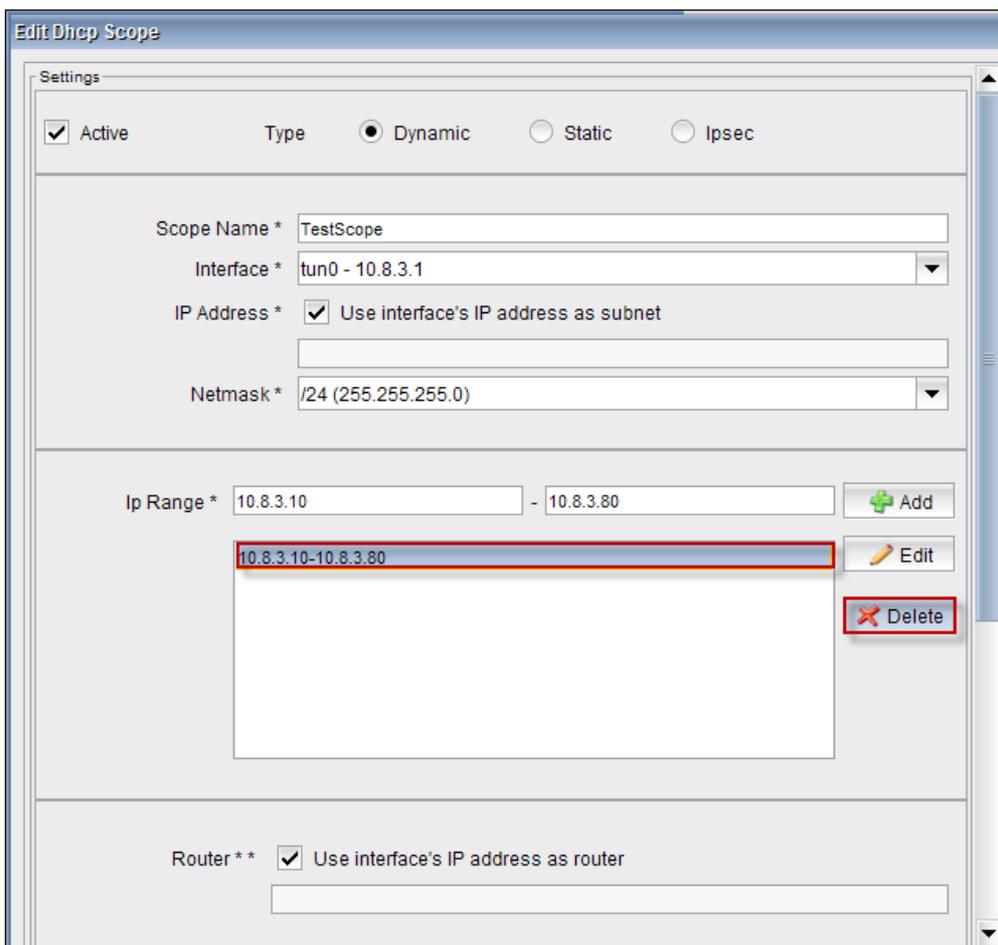
Router ** Use interface's IP address as router

Select the **Server** from the list and click on **Edit Tab**.



	Name	Subnet/Netmask	Router	Type	Status
<input type="checkbox"/>	WAUTH_DHCP	10.1.0.0/255.255.255.0	10.1.0.1	Dynamic	Active
<input type="checkbox"/>	labtest	192.168.20.0/255.255.255.0	192.168.20.1	Dynamic	Active
<input checked="" type="checkbox"/>	TestScope	10.8.3.0/255.255.255.0	10.8.3.1	Dynamic	Active

We can Edit **Scope Name, Interface and IP Range** in **Edit DHCP Scope**. At the same time we can even **Add, Edit, Delete IP Range** from the same tab. Select IP Range and click on **Delete** to delete the entire range.



Edit Dhcp Scope

Settings

Active Type Dynamic Static Ipsec

Scope Name *

Interface *

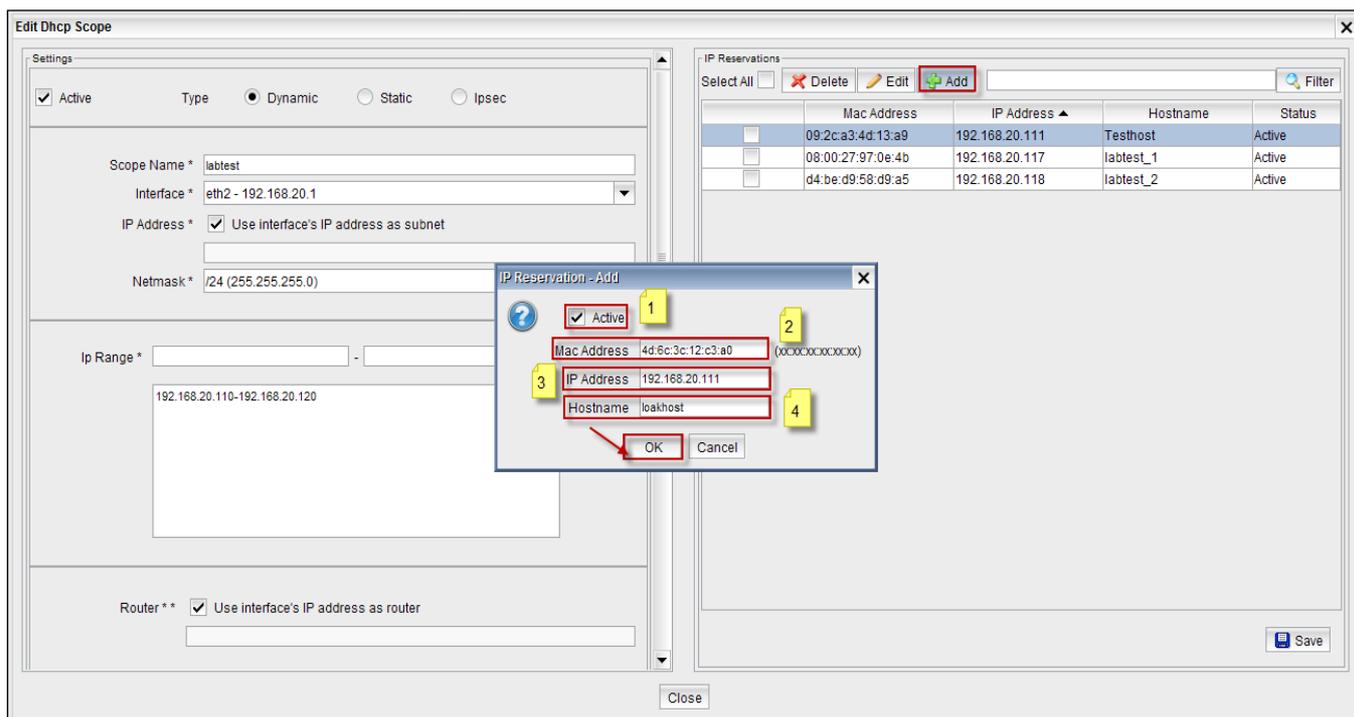
IP Address * Use interface's IP address as subnet

Netmask *

Ip Range * -

Router ** Use interface's IP address as router

Adding IP Reservation to DHCP scope

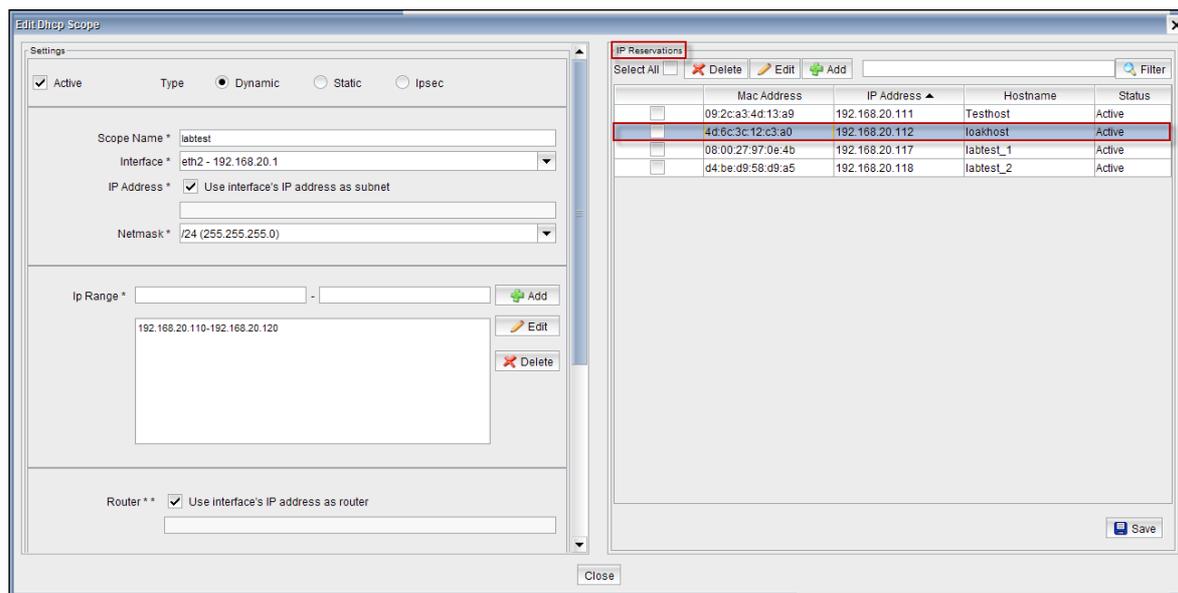


These are the inputs for adding IP Reservation

1	Active	We can enable or disable this option
2	Mac Address	Give Mac Address of the Host
3	IP Address	Give the IP Address within the scope of DHCP server
4	Hostname	Type the name of the Host

Click on **Ok**

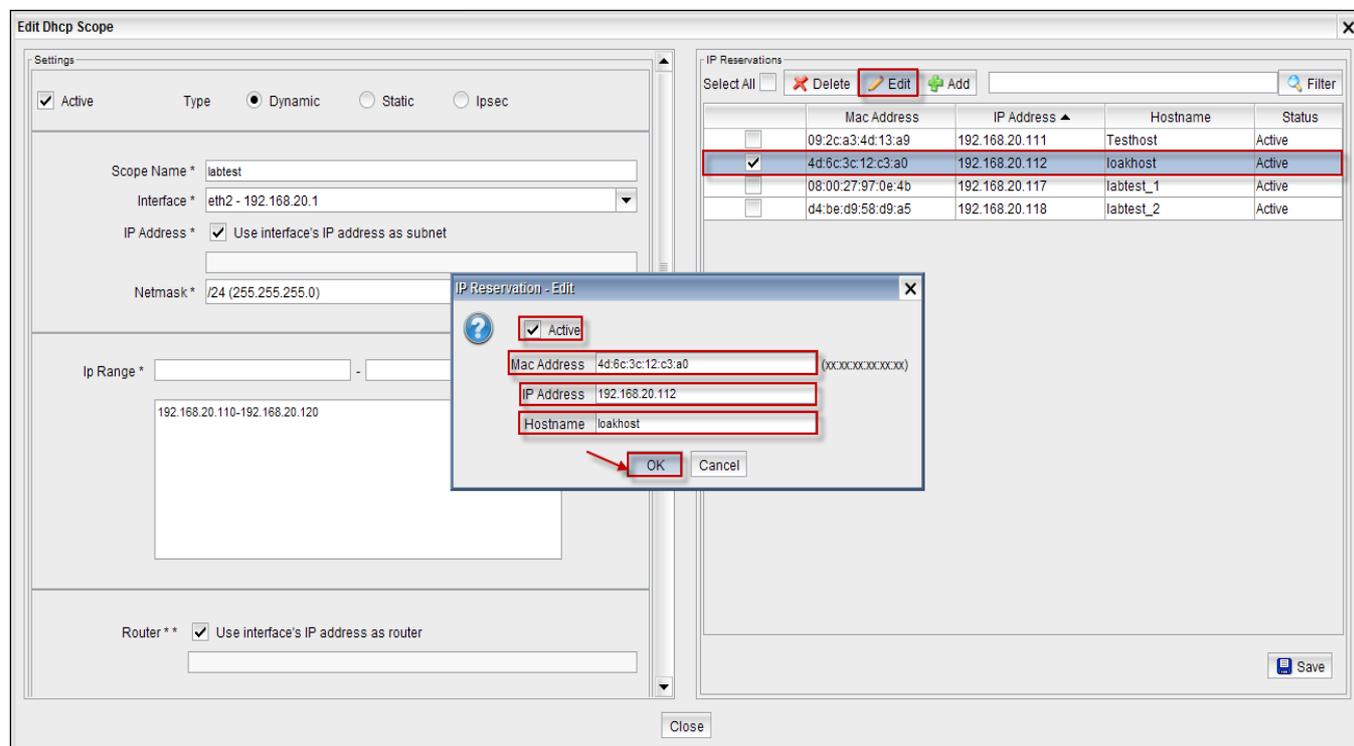
In the below screen we can notice **IP Reservation** added to the DHCP Server



Editing IP Reservation

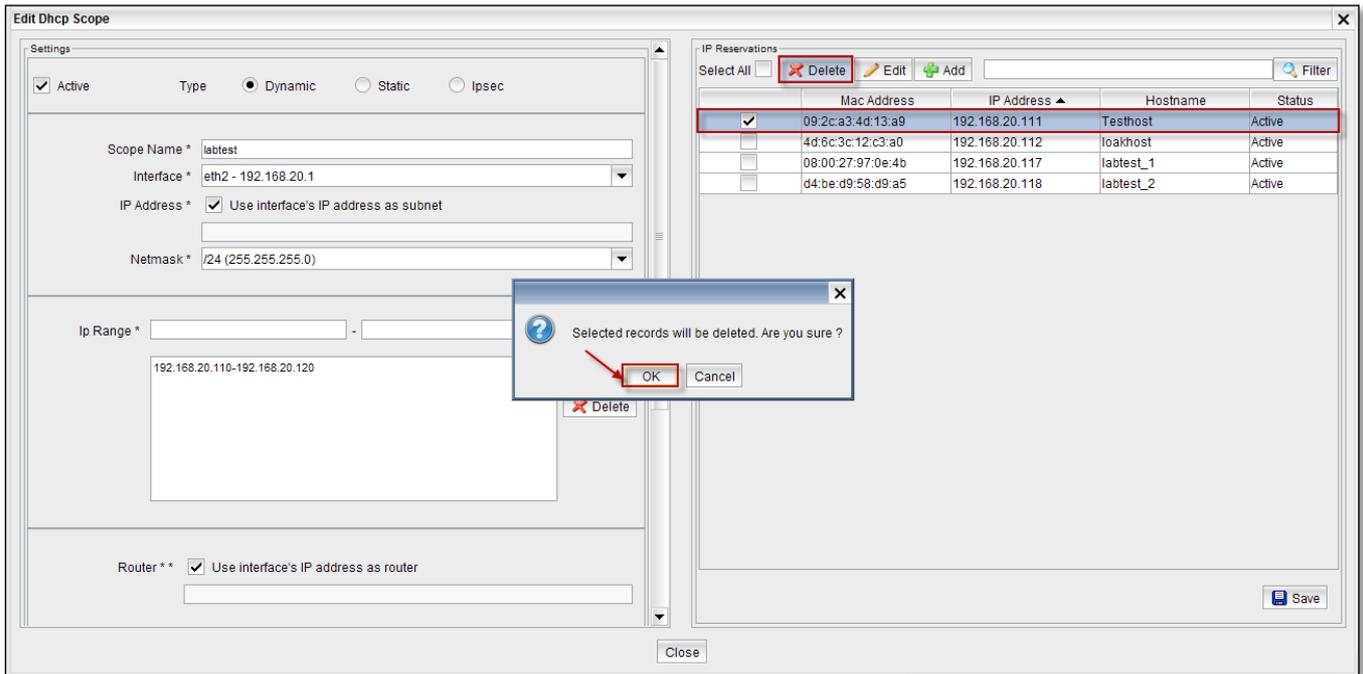
Select IP and click on **Edit tab**

We can edit all the fields in the Edit tab and click **Ok**



Deleting IP Reservation

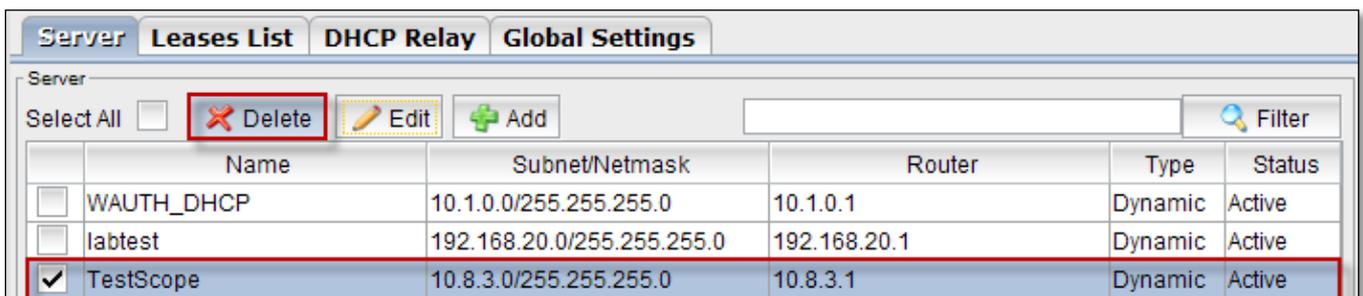
Select the IP and click on **Delete tab**, Click **Ok** to delete.



Below screen appears stating that selected records have been deleted. Click **Ok** to close the current tab.



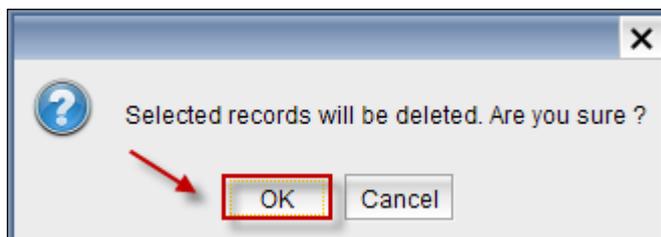
Select the **Server** from the list and click on **Delete Tab** to delete the **DHCP Server**.



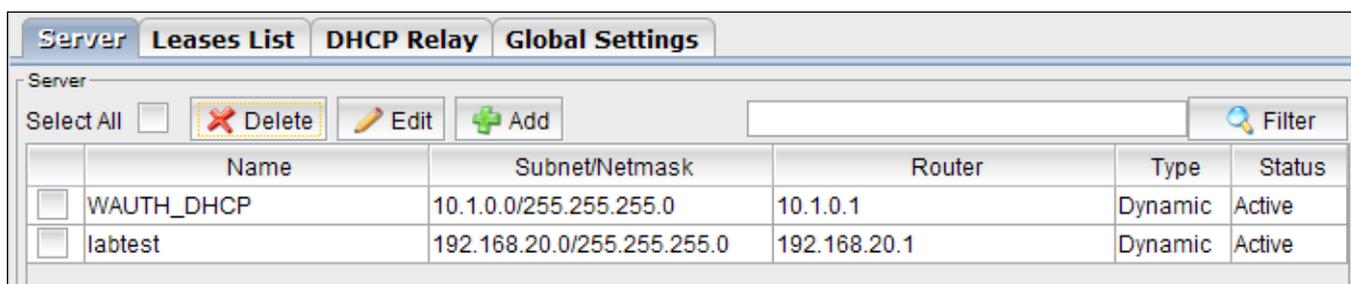
Deleting process is in progress.



When the below screen appears, click **Ok**.



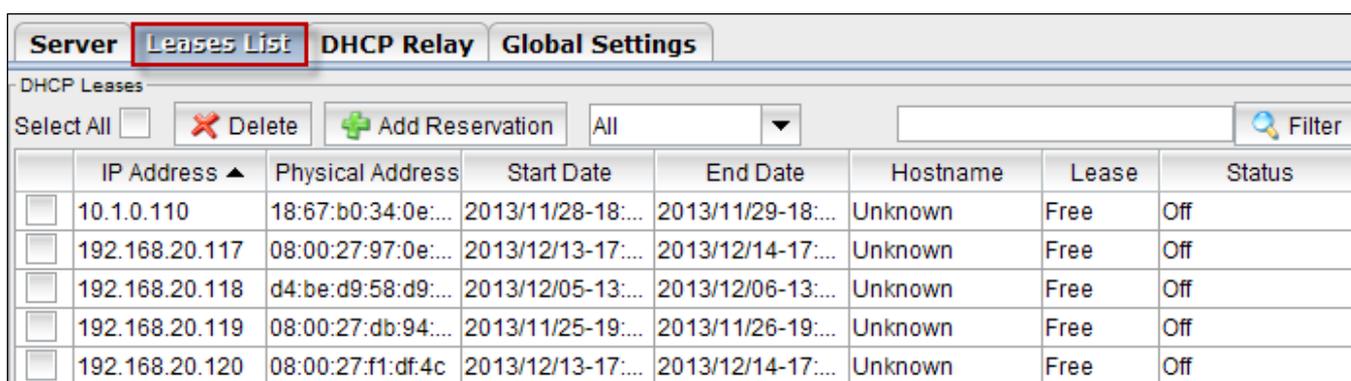
We can notice that the selected **Server** is **deleted** from the Servers list.



	Name	Subnet/Netmask	Router	Type	Status
<input type="checkbox"/>	WAUTH_DHCP	10.1.0.0/255.255.255.0	10.1.0.1	Dynamic	Active
<input type="checkbox"/>	labtest	192.168.20.0/255.255.255.0	192.168.20.1	Dynamic	Active

Lease list options

Select **Lease List** to display the details of **DHCP Lease List**.



	IP Address ▲	Physical Address	Start Date	End Date	Hostname	Lease	Status
<input type="checkbox"/>	10.1.0.110	18:67:b0:34:0e:...	2013/11/28-18:...	2013/11/29-18:...	Unknown	Free	Off
<input type="checkbox"/>	192.168.20.117	08:00:27:97:0e:...	2013/12/13-17:...	2013/12/14-17:...	Unknown	Free	Off
<input type="checkbox"/>	192.168.20.118	d4:be:d9:58:d9:...	2013/12/05-13:...	2013/12/06-13:...	Unknown	Free	Off
<input type="checkbox"/>	192.168.20.119	08:00:27:db:94:...	2013/11/25-19:...	2013/11/26-19:...	Unknown	Free	Off
<input type="checkbox"/>	192.168.20.120	08:00:27:f1:df:4c	2013/12/13-17:...	2013/12/14-17:...	Unknown	Free	Off

Choose **IP Address** and click on **Add Reservation Tab**.

	IP Address ▲	Physical Address	Start Date	End Date	Hostname	Lease	Status
<input type="checkbox"/>	10.1.0.110	18:67:b0:34:0e:...	2013/11/28-18:...	2013/11/29-18:...	Unknown	Free	Off
<input type="checkbox"/>	192.168.20.117	08:00:27:97:0e:...	2013/12/13-17:...	2013/12/14-17:...	Unknown	Free	Off
<input type="checkbox"/>	192.168.20.118	d4:be:d9:58:d9:...	2013/12/05-13:...	2013/12/06-13:...	Unknown	Free	Off
<input type="checkbox"/>	192.168.20.119	08:00:27:db:94:...	2013/11/25-19:...	2013/11/26-19:...	Unknown	Free	Off
<input checked="" type="checkbox"/>	192.168.20.120	08:00:27:f1:df:4c	2013/12/13-17:...	2013/12/14-17:...	Unknown	Free	Off

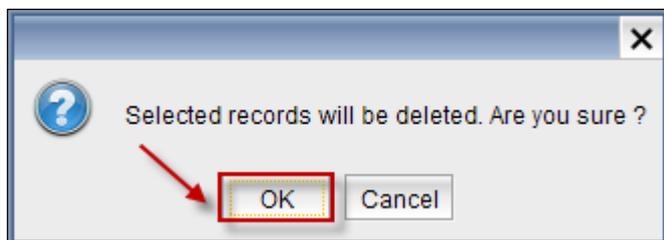
Click **Ok** to **Add reservation** for the selected **IP Address**.



Select the **IP Address** and click on **delete** tab to delete the selected lease list.

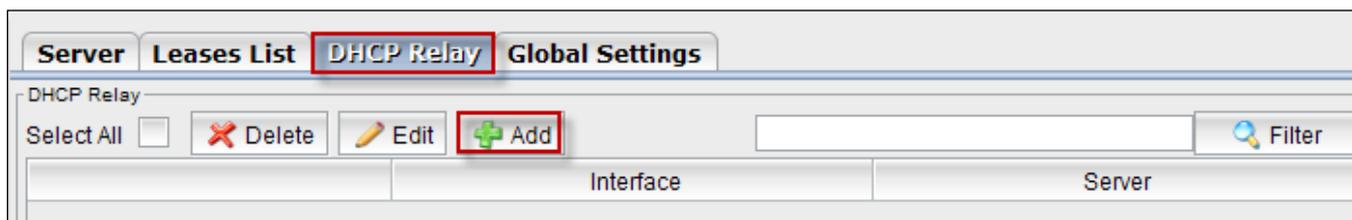
	IP Address ▲	Physical Address	Start Date	End Date	Hostname	Lease	Status
<input type="checkbox"/>	10.1.0.110	18:67:b0:34:0e:...	2013/11/28-18:...	2013/11/29-18:...	Unknown	Free	Off
<input type="checkbox"/>	192.168.20.117	08:00:27:97:0e:...	2013/12/13-17:...	2013/12/14-17:...	Unknown	Free	Off
<input type="checkbox"/>	192.168.20.118	d4:be:d9:58:d9:...	2013/12/05-13:...	2013/12/06-13:...	Unknown	Free	Off
<input type="checkbox"/>	192.168.20.119	08:00:27:db:94:...	2013/11/25-19:...	2013/11/26-19:...	Unknown	Free	Off
<input checked="" type="checkbox"/>	192.168.20.120	08:00:27:f1:df:4c	2013/12/13-17:...	2013/12/14-17:...	Unknown	Free	Off

Click **Ok** to delete the selected lease list

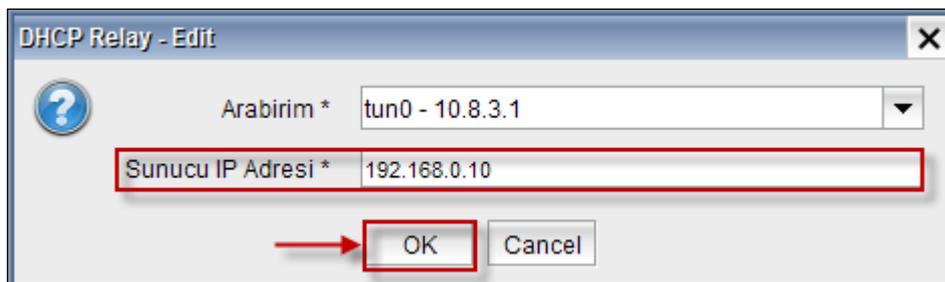


DHCP Relay options

Select **DHCP Relay** and click on **Add Tab**.



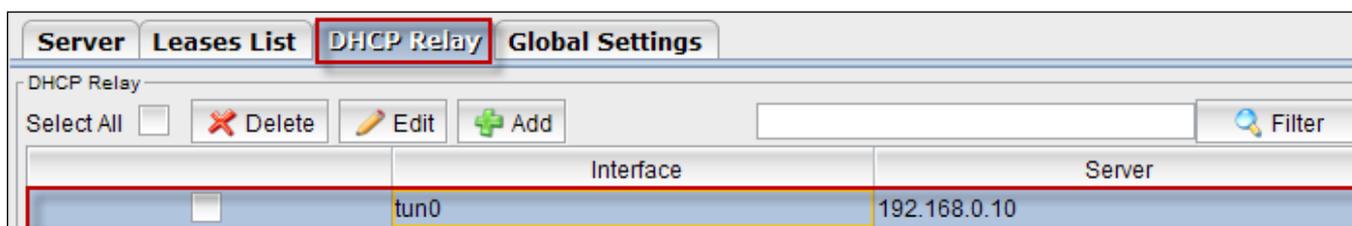
Give the server IP Address and click **OK**.



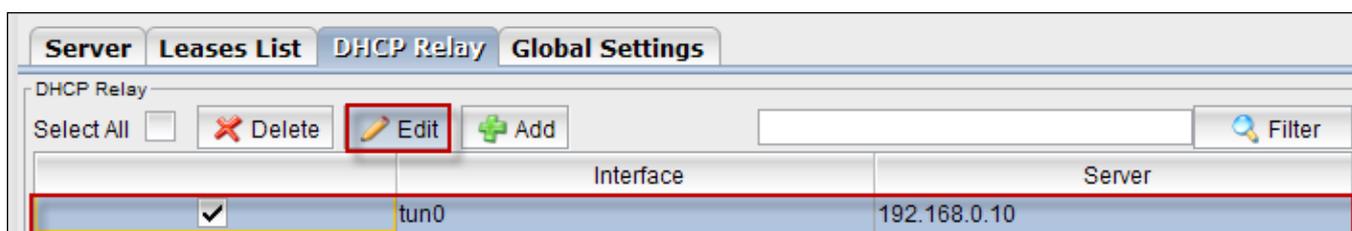
We can notice that **Server** is added in the **DHCP Relay**.

To set up the **DHCP Relay** with one **Server** and more than one interfaces, each interface should be added separately with **Server**.

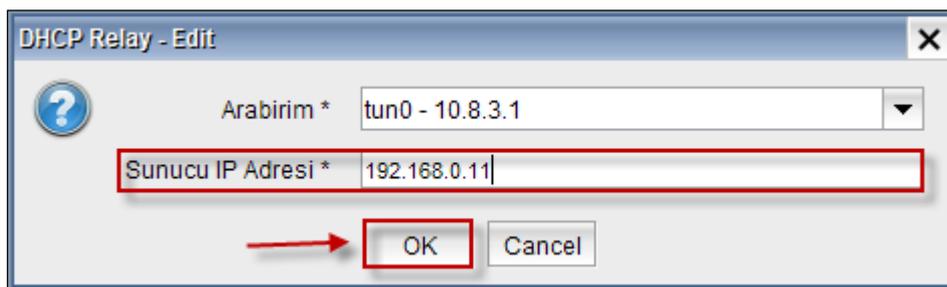
After add operation, a route which is from **DHCP Server** to **DHCP Relay** should be added.



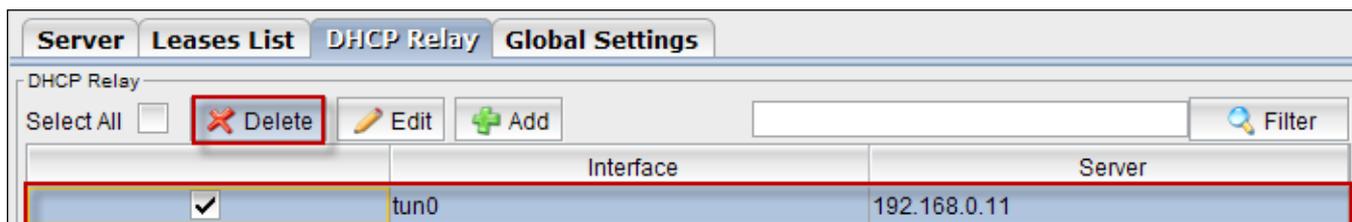
Select the **Server** and click on **Edit Tab**.



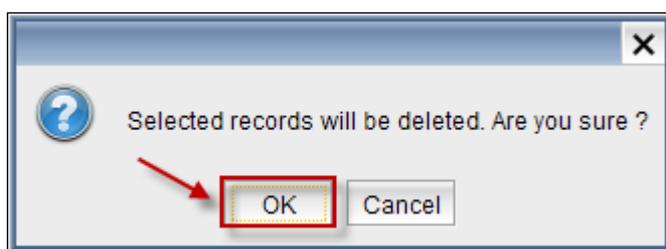
Edit the **Server IP Address** and click **OK**.



Select the **Server** and click on **Delete Tab** to delete server from the DHCP Relay.



Click **OK** to delete the server from DHCP Relay.



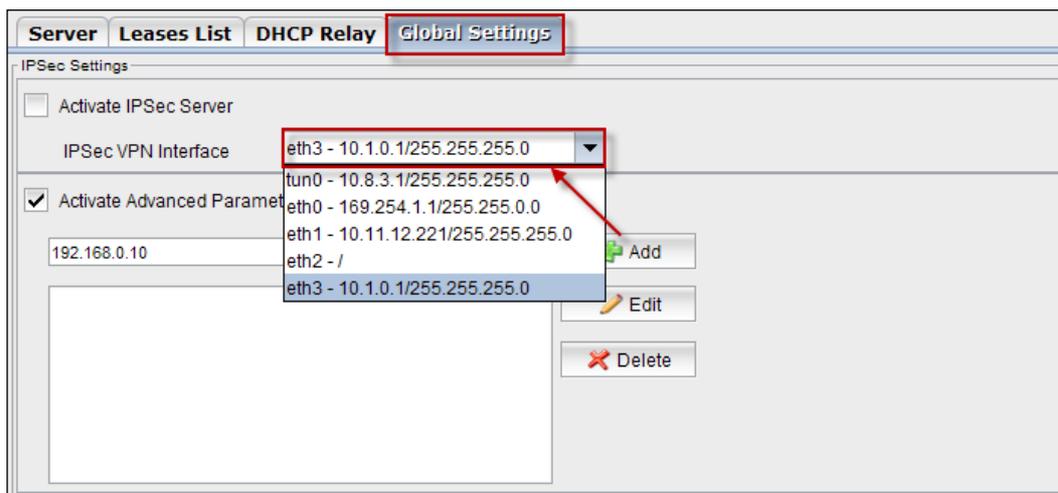
Below screen appears stating that Selected **Records** have been deleted, click **Ok** to close the current tab.



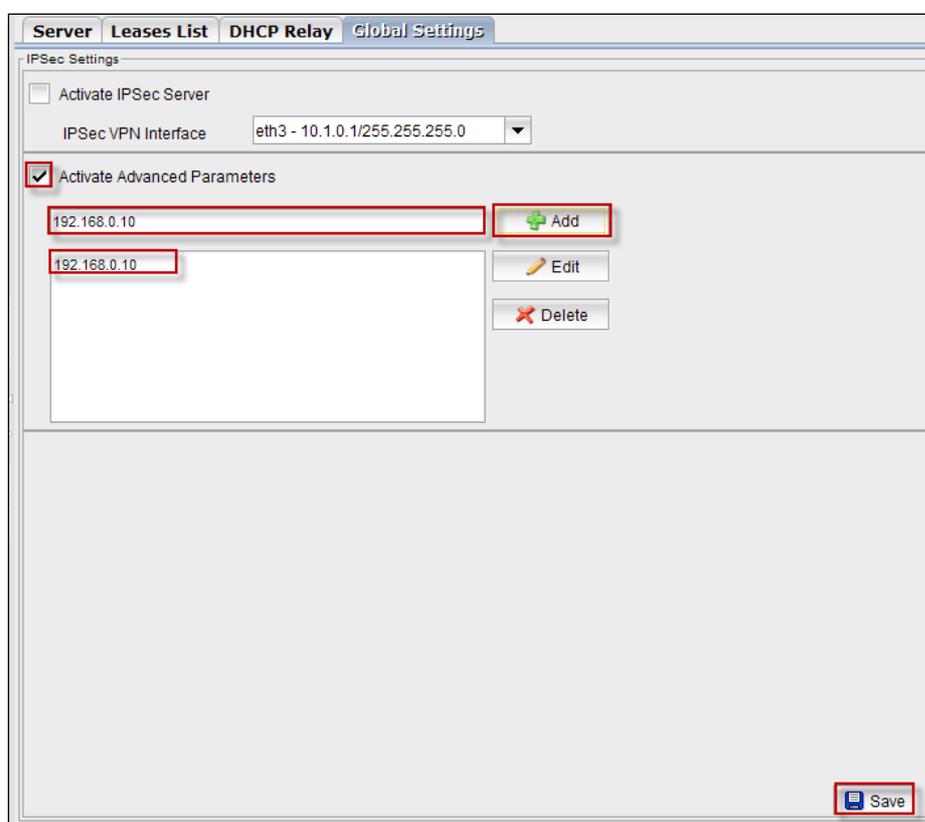
Global Settings options

When we click on **Global Settings**, below screen appears.

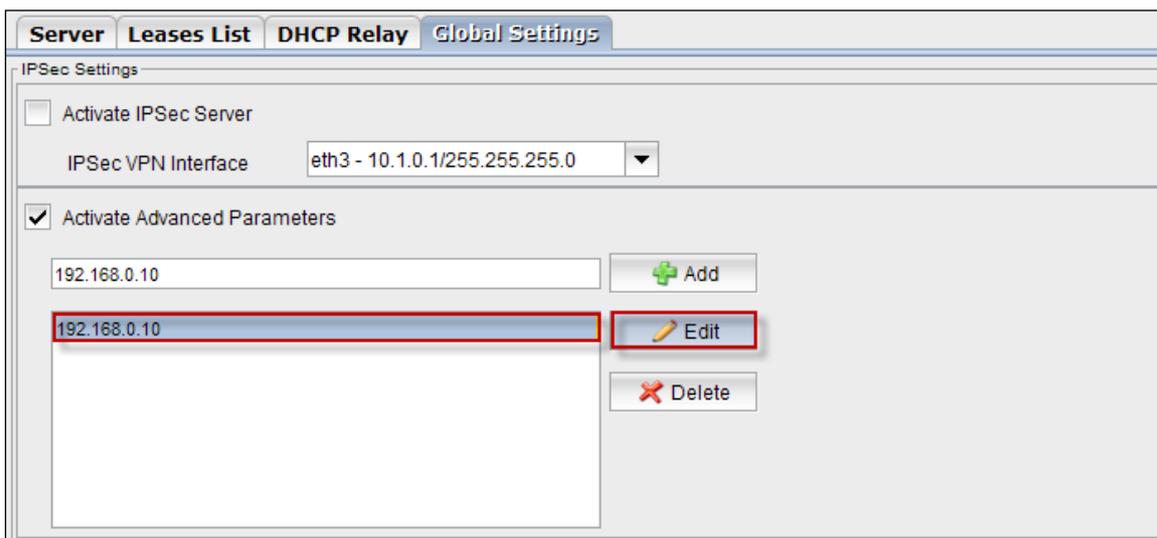
From the **IPSec VPN Interface** drop down list select the Ethernet adapter.



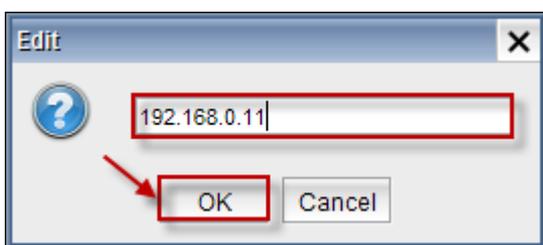
Enable **Activate Advanced Parameters**, give the **IP Address** and click on **Add** and then **Save**.



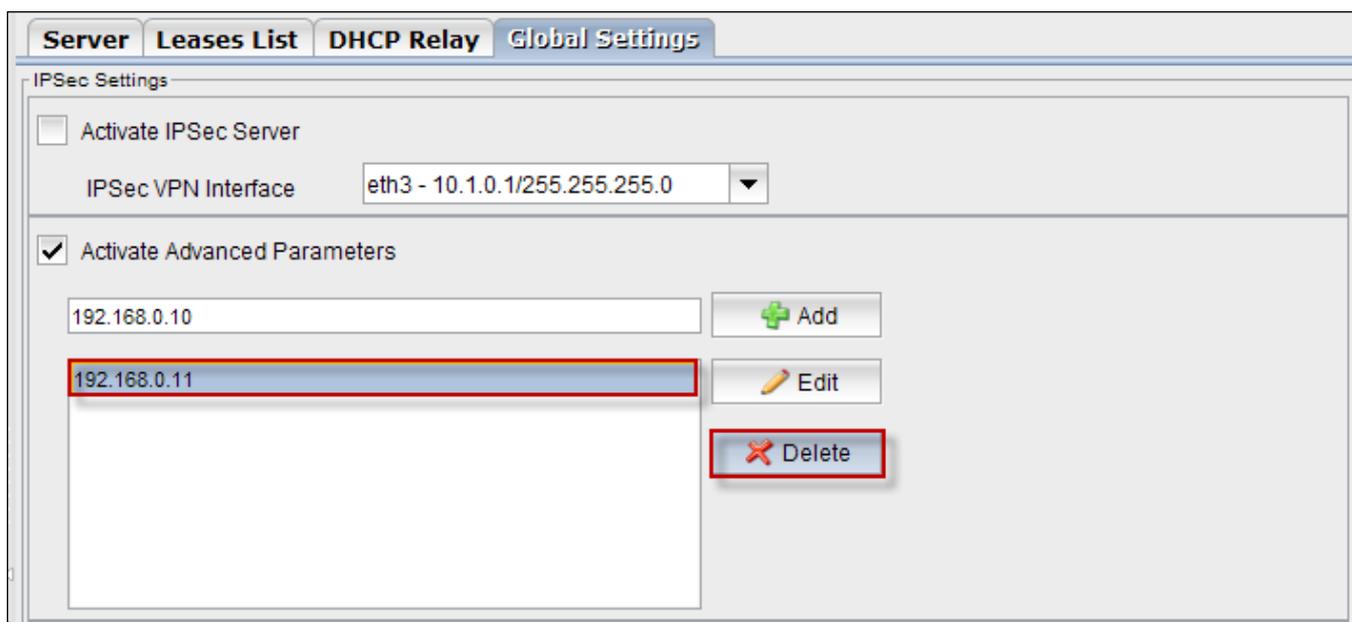
Select the **IP Address** and click on **Edit tab** to edit **IP Address**.



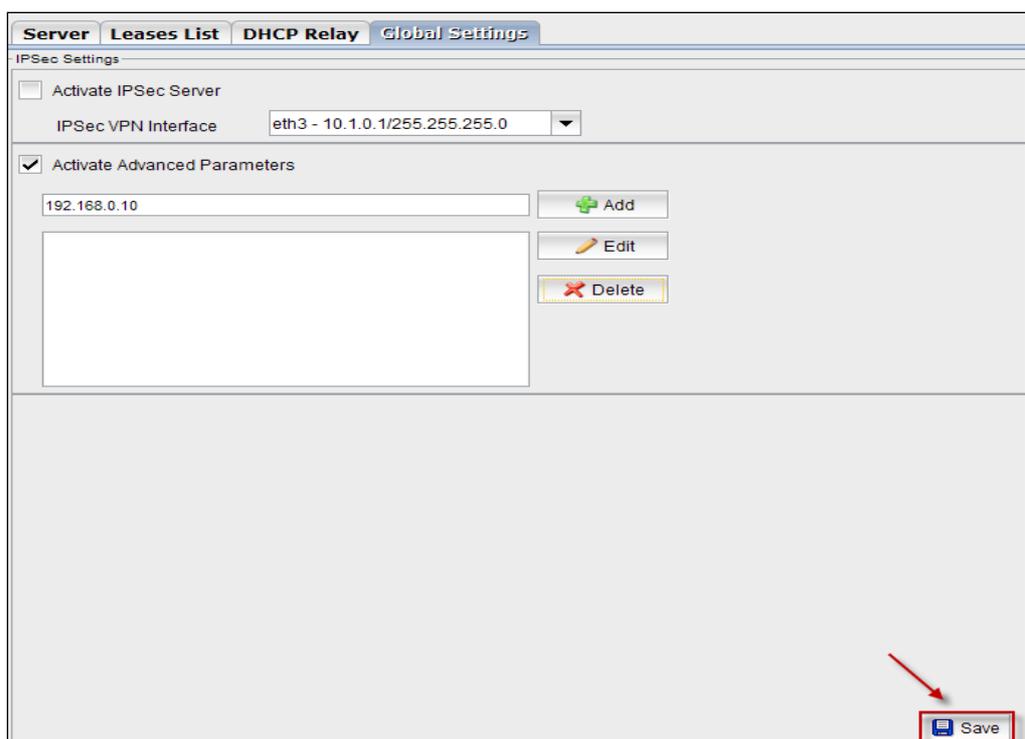
Edit the **IP Address** and click **OK**.



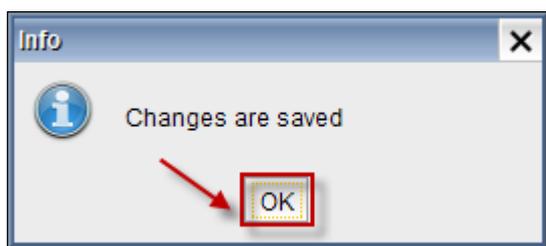
Select the **IP Address** and click on **Delete** button to delete the IP Address.



We can notice that IP Address is deleted, click on **Save Tab** to save the changes.



Below screen appears stating that **Changes are Saved**. Click **OK** to close the current tab.



28. DNS

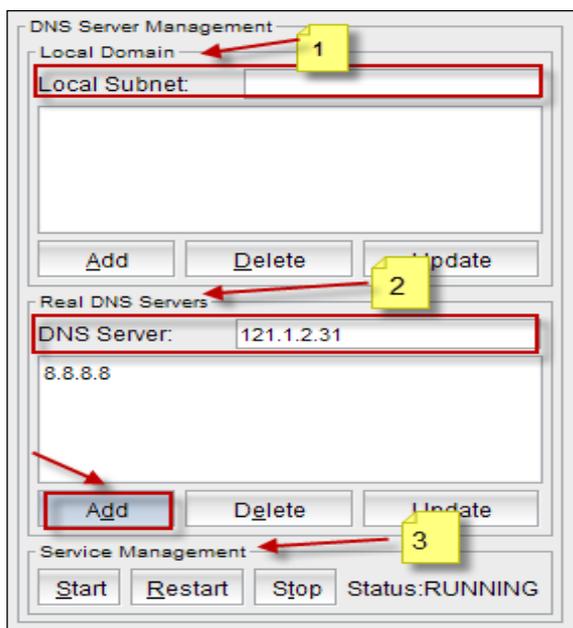
Domain Name System (DNS) is the name resolution protocol for TCP/IP networks, such as the Internet. DNS translates Internet domain and host names to IP addresses. DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites.

DNS is that it serves as the "phone book" for the Internet by translating human-friendly computer hostnames into IP addresses.

In **System Module**, right pane click on **Services tab** and select **Cached DNS Server** to manage **DNS Server**.



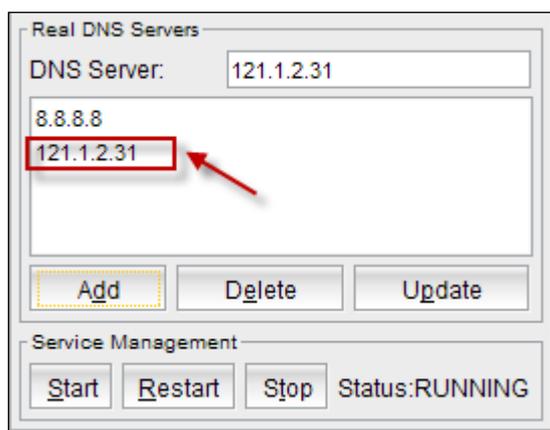
In the **DNS Server Management** tab we find different options like Local Subnet, Real DNS Servers. In the Real DNS Servers give the **IP Address** of the **DNS server** and click on **Add**.



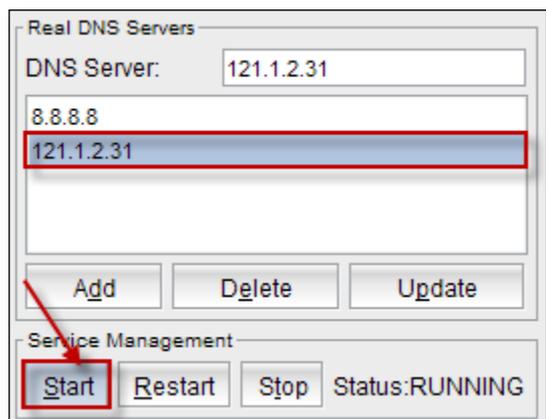
Viewing fields in DNS

1	DNS Server Management	In this we can Add, Delete, Update Local Domain
2	Real DNS Server	In this we can Add, Delete, Update DNS server
3	Service Management	In this we can Start, Restart, Stop DNS Server and it also displays status of the DNS Server

In the below screen we can notice **DNS Server** is added.



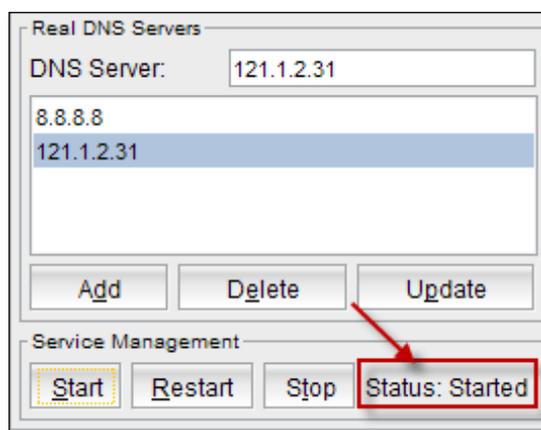
Select the server and click on **Start tab** to start the services of **DNS Server**.



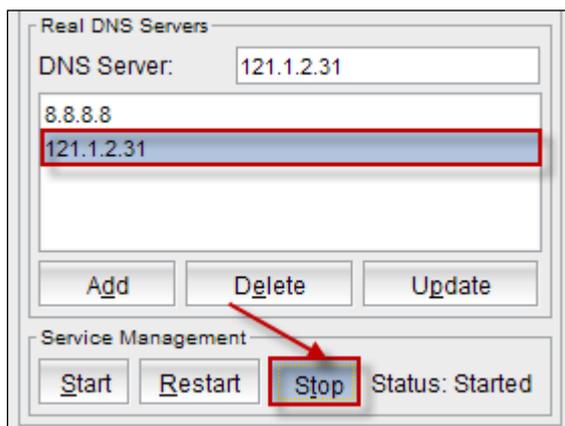
Below screen appears stating that **DNS Service Started**, click **Ok** to close the current tab.



In the below screen we can notice the **Status** of the **DNS Server** is shown as **Started**.



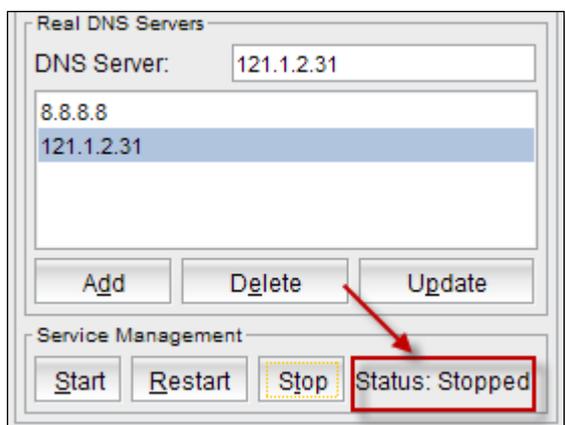
Select the Server and click on **Stop** button to stop the services of **DNS Server**.



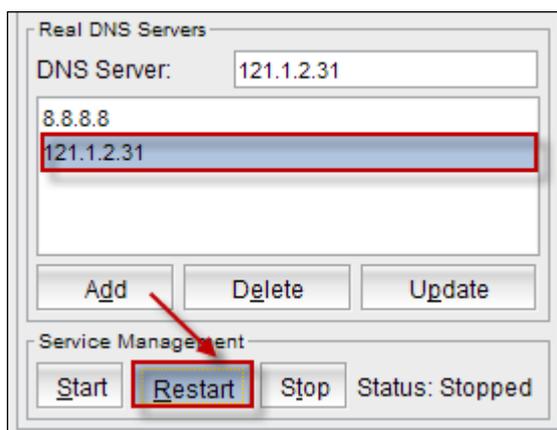
Below screen appears stating that **DNS Service Stopped**, click **OK** to close the current tab.



In the below screen we can notice the status of the **DNS Server** is shown as **Stopped**.



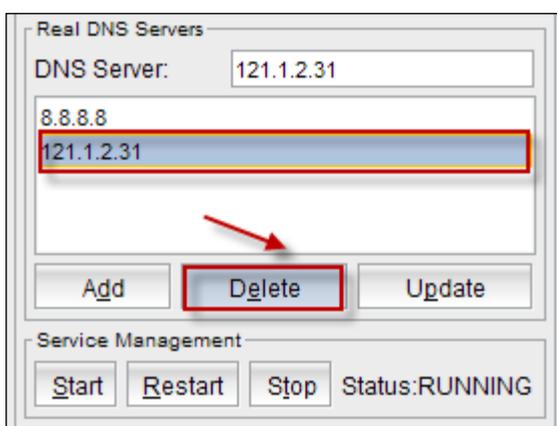
Select the Server and click on **Restart** button to Restart the Services of **DNS Server**.



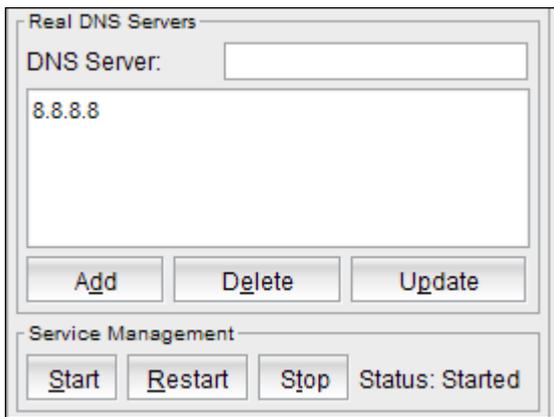
Below screen appears stating that **DNS Service Restarted**, click **OK** to close the current tab.



Select the Server and click on **Delete** button to delete a **DNS Server**.



In the below screen we can notice newly added **DNS Sever** got deleted.

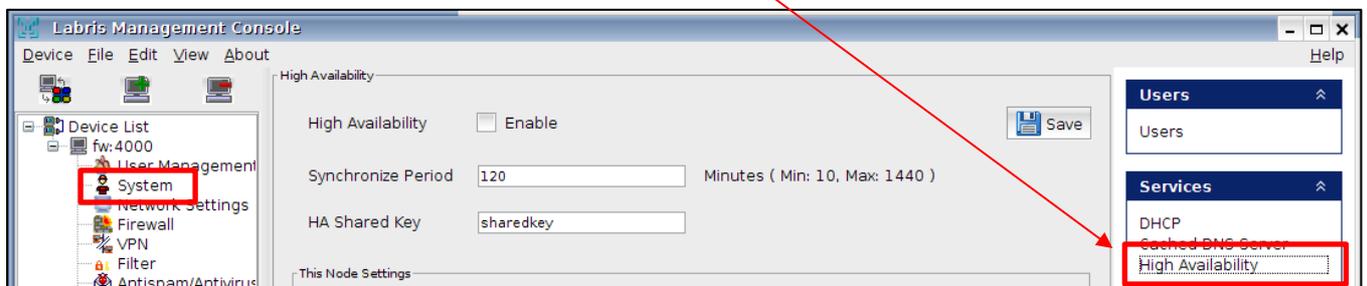


29. HA - High Availability Appliance Deployment Architecture

High Availability service is designed for Labris UTM devices to run in a redundant (active-passive) mode. With this service, you can configure two Labris UTM devices in a redundant way and ensure non stop service.

Note

• You can also change your preferred language even after you login to the appliance as shown in following image



Steps;

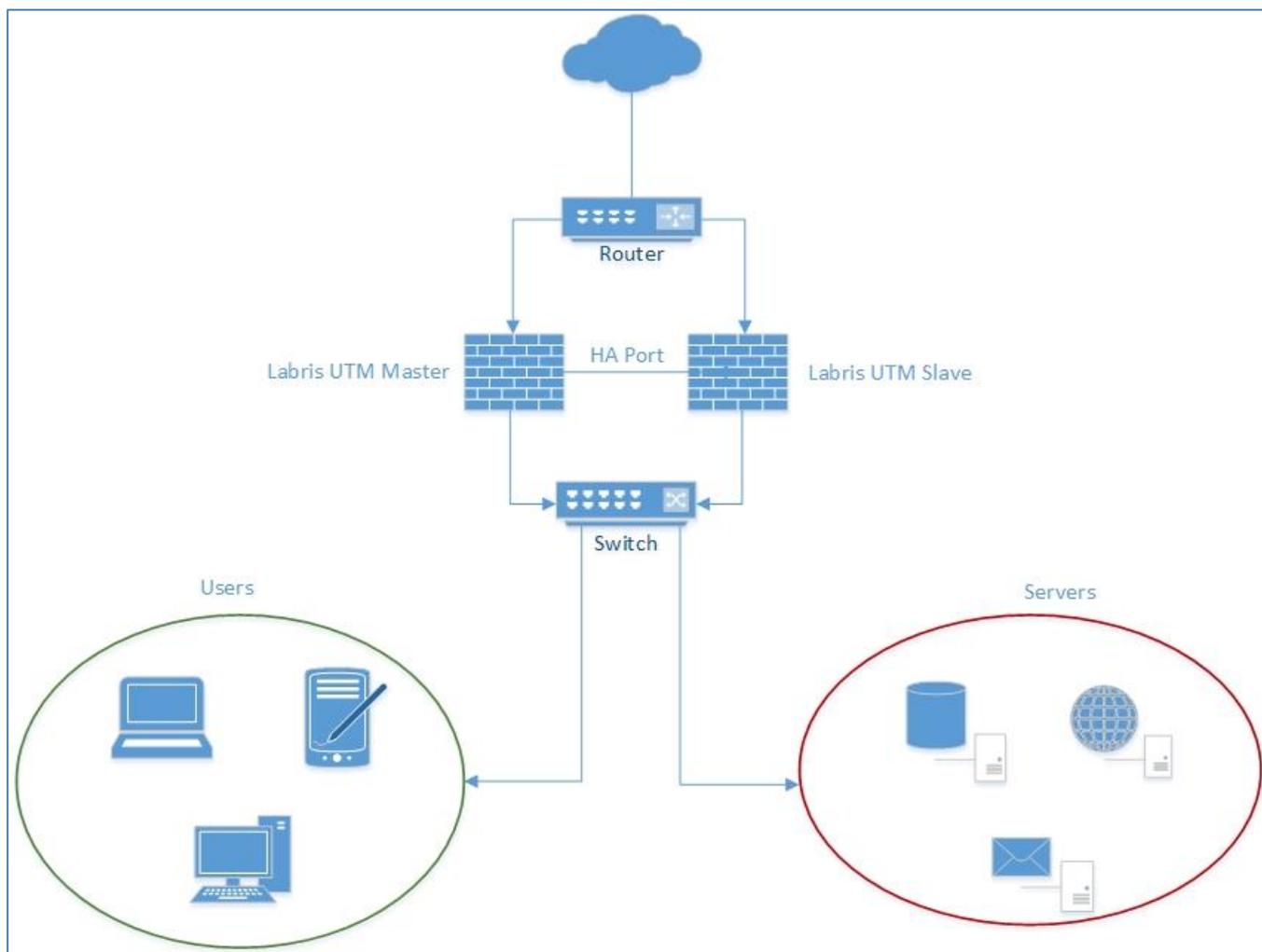
By following the steps below and with the information in the document, Labris High Availability system can be setup.

<u>Active Device (Master)</u>	<u>Passive Device (Slave)</u>
	1 - Device hostname is configured
	2 - IP configuration is done. Here, High Availability port and dummy IP settings are configured. (Alias IP address configuration is done on the active device on first configuration)
	3 - Console access settings are configured.
4 - Device hostname is configured.	
5 - IP configuration is done. High Availability port, dummy IP and alias IP settings are configured.	
6 - Console access settings are configured.	
7 - High Availability service is configured.	
8- All the other configurations are done. Firewall, webfilter etc.	
High Availability system is tested.	

Topology

For the redundant setup of Labris UTM devices, the following topology can be used as a reference.

The basic logic while setting the topology is to connect both of the Labris devices via ethernet cable to the other devices that they are connected and connect the two Labris UTM devices to each other, for health checking.



For the High Availability system, first of all hostname, IP settings (except alias IP addresses) and console access settings are configured on the second device.

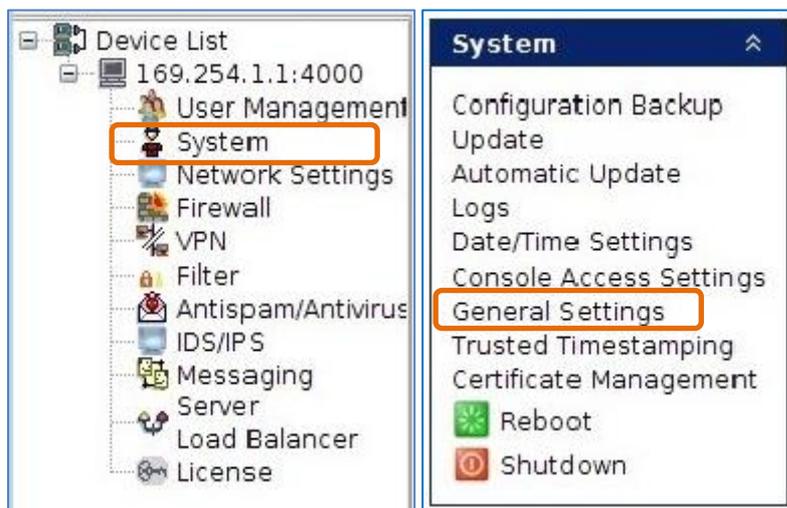
All other configurations are done on the first device. When high availability is started all the configurations will be synchronized between the two devices.

After setting the above topology, you can continue following the configuration steps.

Hostname Settings

Devices used in High Availability should have different hostnames. High Availability service checks access control between each other using this hostname.

To configure the hostname, enter the system module from LMC. After clicking *General Settings* you can edit the hostname.

The image shows a configuration form for setting the hostname. It has a label 'Hostname' and a text input field containing the value 'labris1'. Below the input field is a 'Save' button.

1	Hostname	Labris UTM Device Name
2	Save	Configuration Save

The same setting is also configured on the second Labris UTM device. On the second device another hostname should be given.

IP Configuration

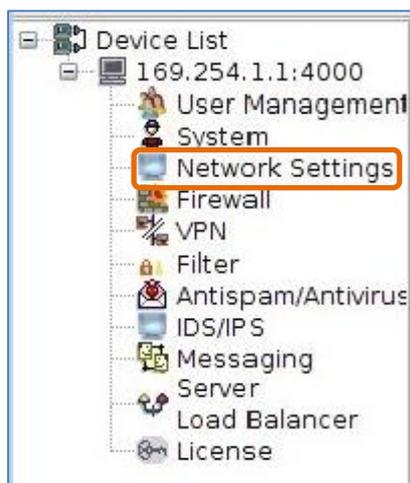
When setting up the High Availability system an unused IP address from the internal network is given from the *Network Settings* module.

Active and passive devices are configured to have different IP addresses.

The IP addresses that will actually be used should be defined as an alias IP on the related ethernet. (Only defined on the active device on first configuration.)

For IP configuration, enter the *network settings* module from LMC.

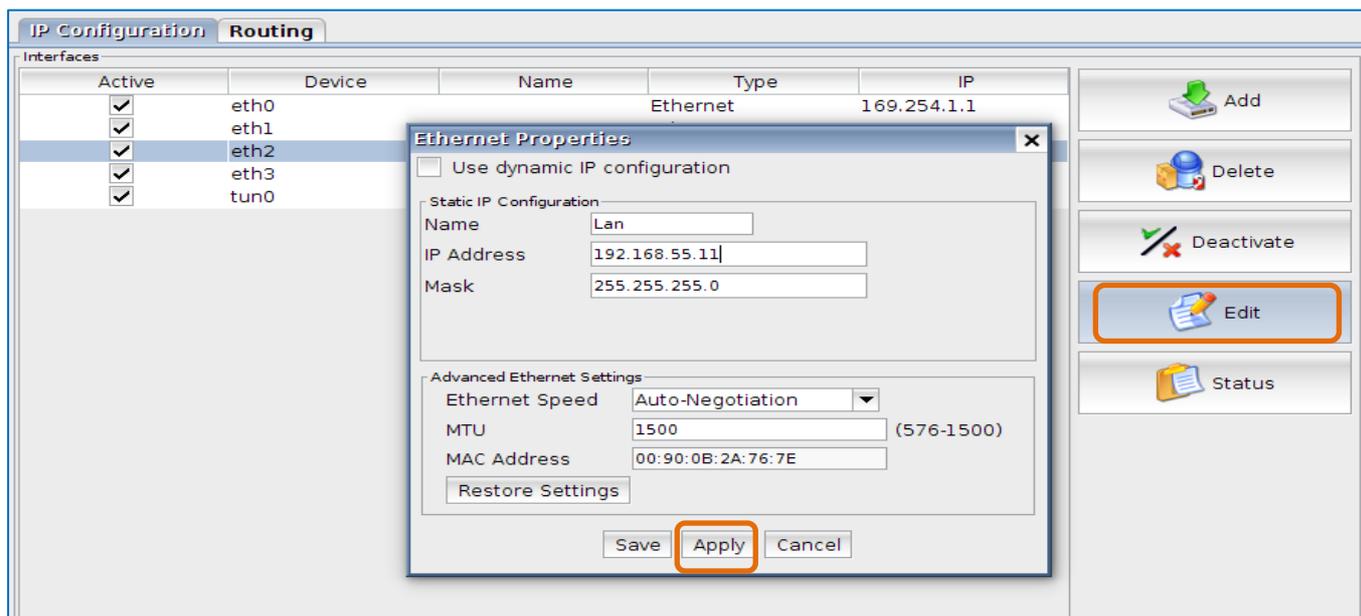
IP settings are configured according to your network topology.



Dummy IP Address

For ethernet interfaces to be active, an unused IP address which will not normally be used should be set on an ethernet. The IP addresses which will be actually used will be defined as an alias IP on the ethernets. The alias IP addresses are automatically run on the current active device by High Availability service.

Dummy IP addresses, which are not used in the network, are given to the related ethernets via the IP Configuration menu. For this, after selecting the related ethernet, right click and press edit. After the configurations press apply button.

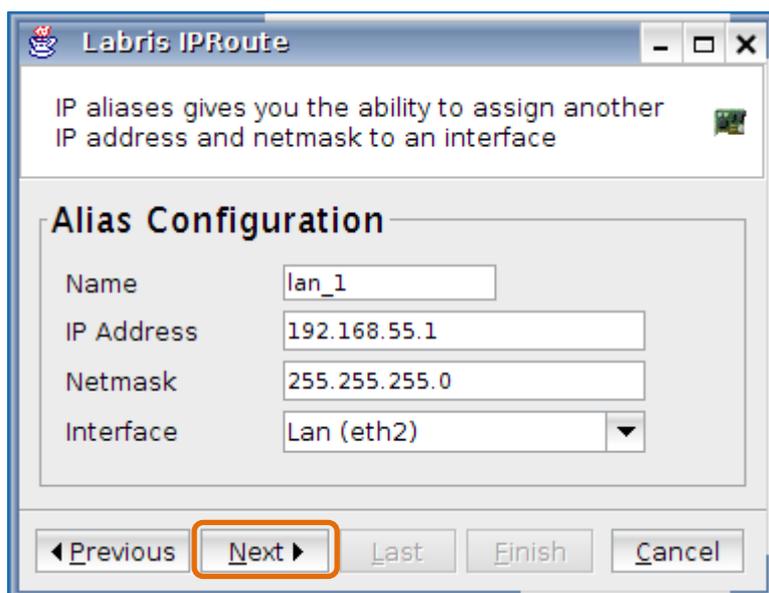
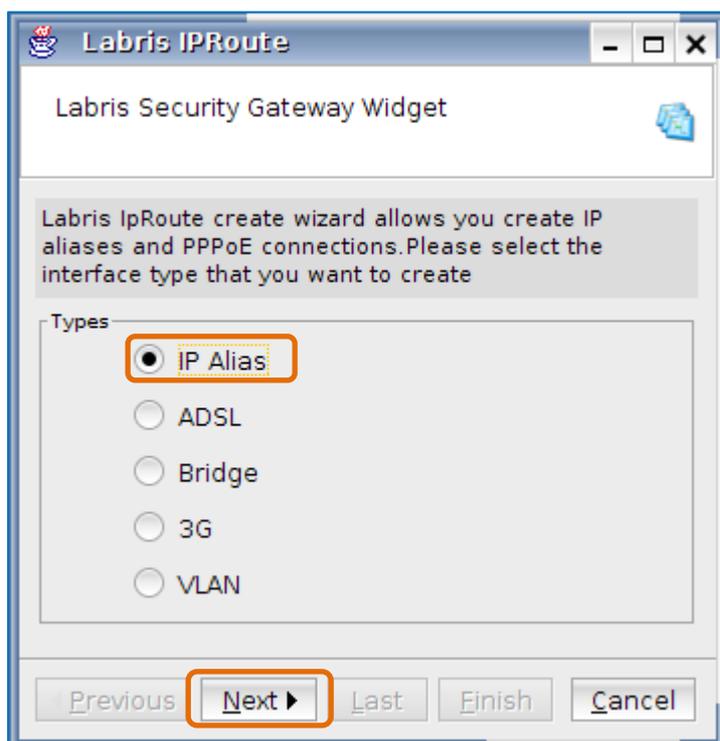


1	Name	A name defining the ethernet interface
2	IP Address	The IP address used for the selected interface. In this scenario, an unused IP address should be given. Also on the second device an unused IP address should be given.
3	Mask	Mask of the network address.
4	Apply	Applies the configurations.
5	Other Parameters	For other parameters, please refer to the Ethernet Settings section in the admin guide.

This procedure is done for all the used ethernets.

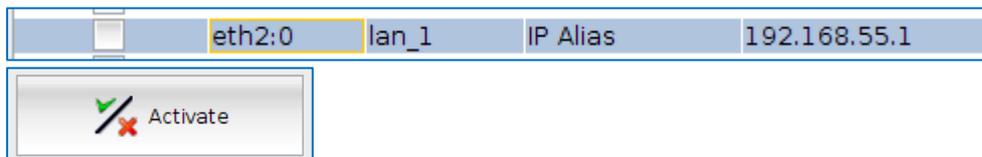
Alias IP

More than one IP address can be defined on a physical ethernet interface. For this, alias IP addresses are added to the system. When using Labris High Availability service, IP settings are done using alias IPs. Press on the *Add* button in *IP Configuration* menu and select *Alias IP*. Define the IP addresses which will actually be used.



1	Name	A name defining the alias ethernet interface.
2	IP Address	The IP address used for the selected interface. In this scenario, an unused IP address should be given. Also on the second device an unused IP address should be given.
3	Mask	Mask of the network address
4	Interface	The ethernet interface which the alias IP will be configured on
5	Next	After the settings are configured click on the <i>Next</i> button and the alias interface will be defined.

This way, all IP addresses which will actually be used are added as an alias ethernet interface. After the definitions are made, the alias ethernet interfaces which have been defined are selected and activated.



This procedure is done for all alias ethernet.

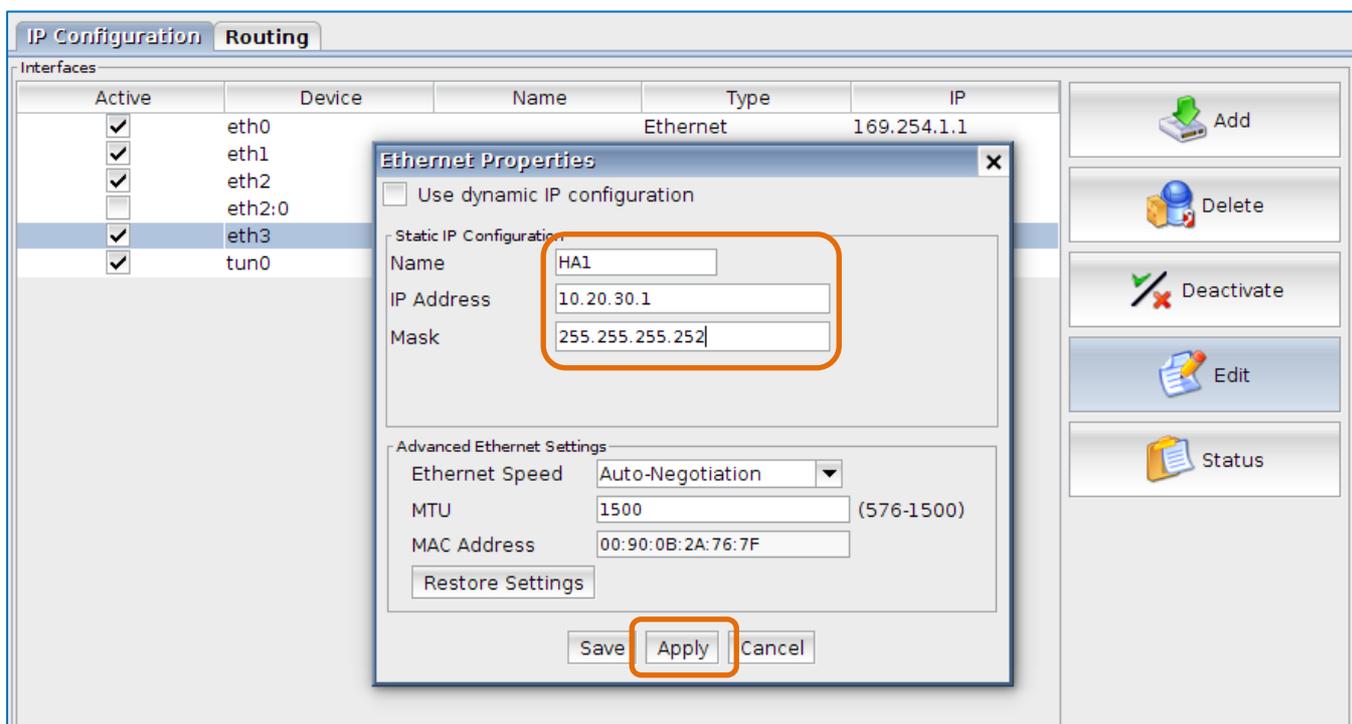
Alias IP addresses are only configured on the active device. There is no need to do this configuration for the passive device.

HA Port

It is the ethernet interface which will be used to communicate between Labris UTM devices. HA ethernet interface is defined on both the active and passive devices. The two devices are connected via an ethernet cable using these ports configured for HA.

The ethernet interfaces used for HA should be the same on both devices. In other words, if the active device is using eth3 for HA, the passive device should also use eth3.

An IP address is given to the ethernet interface configured as HA port. Any unused IP address having a minimum mask of /30(255.255.255.252) in the local network can be given. The IP addresses given to the HA ports of the active and passive device should be in the same subnet.



1	Name	A name defining the ethernet interface.
2	IP Address	The IP address used for the selected interface. The IP address given to the HA port for the access of two Labris devices.
3	Mask	Mask of the network address.
4	Apply	Applies the changes.

5	Other Parameters	For other parameters, please refer to the Ethernet Settings section in the admin guide.
---	-------------------------	---

The same configuration is done for the second device.

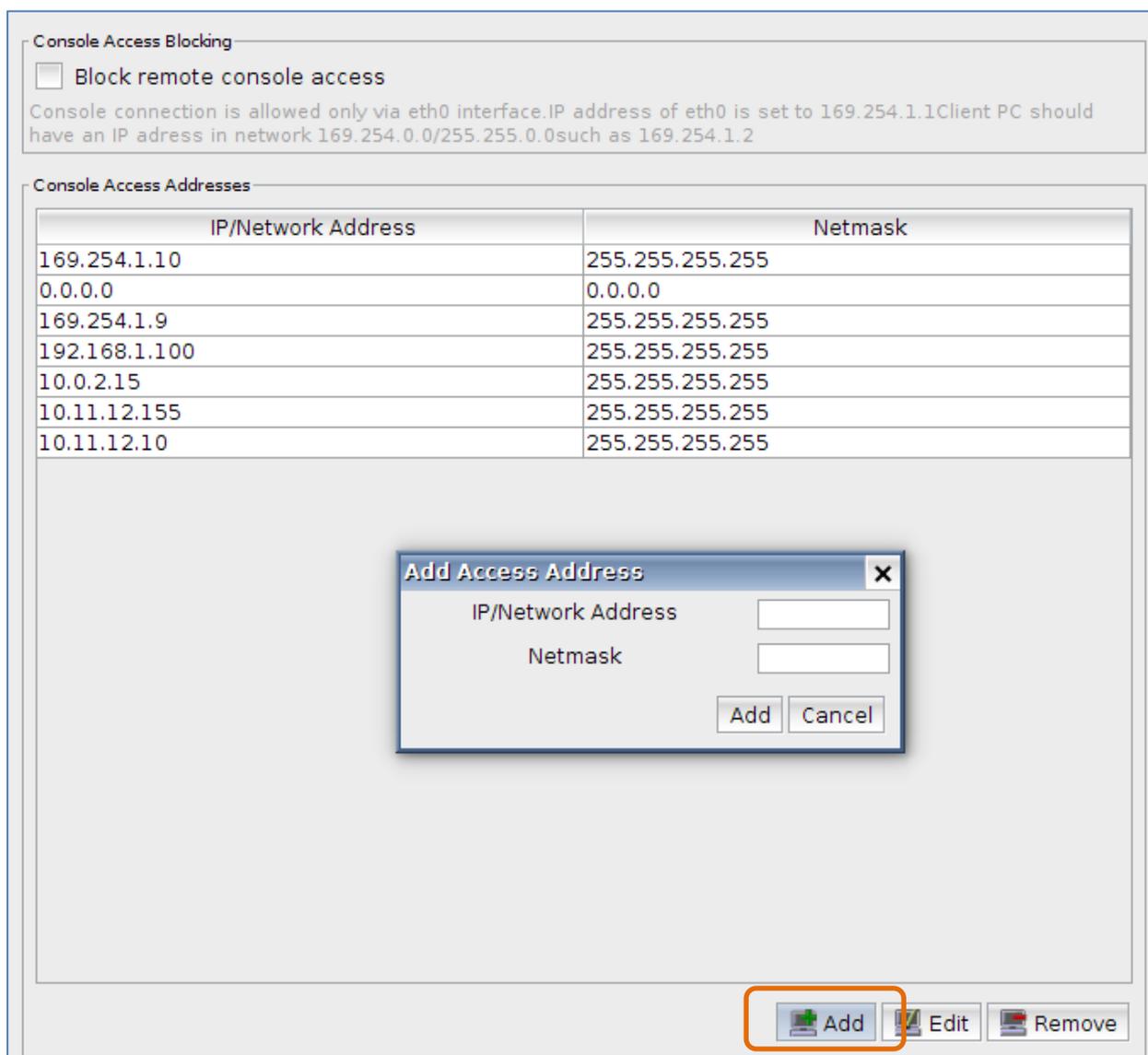
Console Access (Access Between Devices)

For allowing connection between active and passive devices, the IP addresses given to the HA ports should be written to the console access configuration of the active and passive devices.

Just for the first time this setting should be done on both devices. After HA starts running, it is enough to configure the console access on active device.

Under the system module in LMC you will see the *console access settings*. The IP addresses defined for the HA ports of both devices should be added here.





1	IP/Network	The IP or network address which will be allowed for accessing the device. In this scenario, the IP/network address defined for the HA ports are written.
2	Netmask	The netmask of the IP/network address which is allowed to access is written.
3	Add	After clicking this button, it will also be applied. There is no need to click the save button additionally.

High Availability Service Settings

HA service settings are located under the *services menu* in *system module* of LMC.

It is sufficient to make the configurations from the active device. The configuration of the passive device is done by the active device automatically.

High Availability Enable  Save

Synchronize Period Minutes (Min: 10, Max: 1440)

HA Shared Key

1	High Availability	Enable. Activation of the service
2	Synchronize Period	The time period of the synchronization between Active and Passive devices.
3	HA Shared Key	The shared key of the HA service between the two device.
4	Save	The button to save and apply the configurations.

This Node Settings

Node

Interface

1	Node	This is used to determine if the device being configured is the first (master) device or the second (slave) device. Master device is the active device whereas the slave device is the device on stand by mode.
2	Interface	The HA ethernet port configured for this device.

Peer Node Settings

IP Address

1	IP Address	The IP address given to the HA port of the other device.
---	-------------------	--

Reliable Host Settings

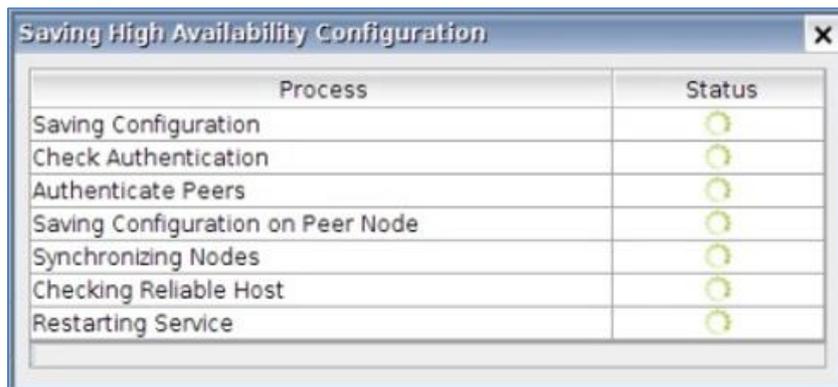
Interface

Reliable Ping IP

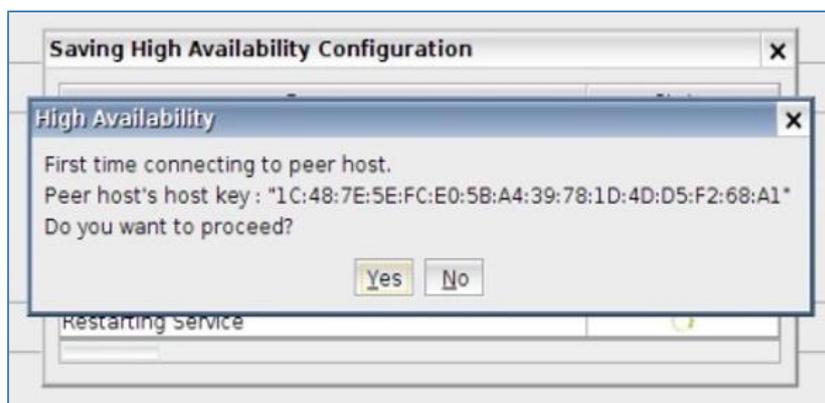
1	Interface	This is used to determine the ethernet which has the address which is used to control the life status of the devices by sending ping packets. It is advised to select the ethernet which is on the LAN.
2	Reliable Ping IP	The IP address of a device which is behind the selected IP address, which will be always up and sent ping packets to.

Saving and Applying Configurations

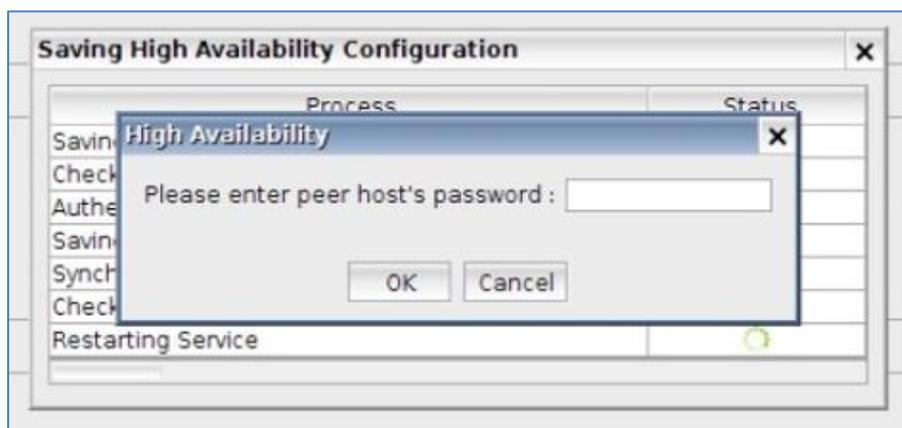
After pressing the save button the configurations are saved.



Access to the second device is started over SSH protocol. The key of the second device is seen. Click yes if the key is correct.

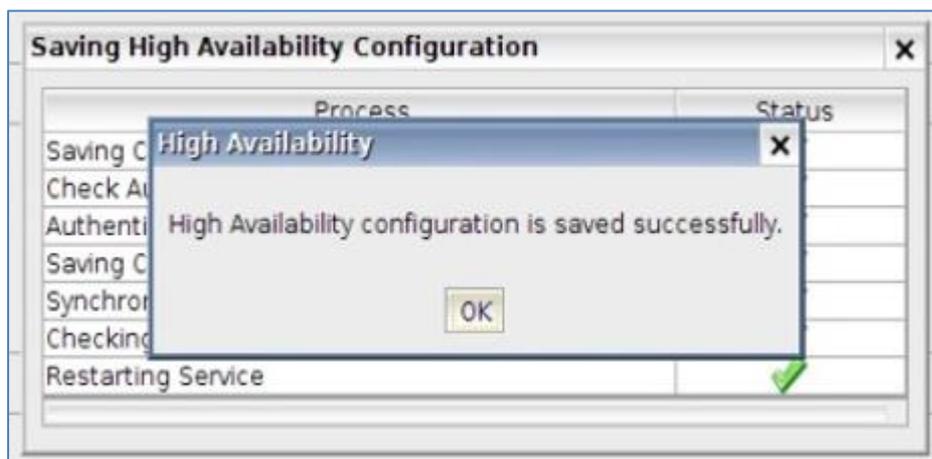


Enter the root password of the other device. This procedure is done only once. It will not appear on consecutive configurations.



After establishing the connection, the configuration of the other device is saved and the synchronization between devices start.

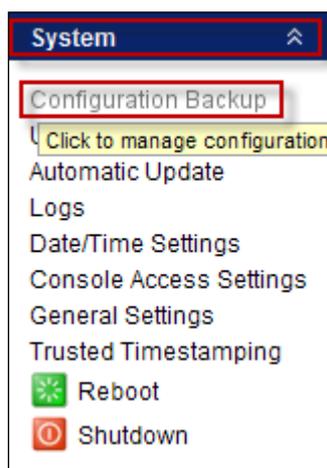
After the procedure completes successfully High Availability system will be established.



The status of the High Availability service can be seen below the page.

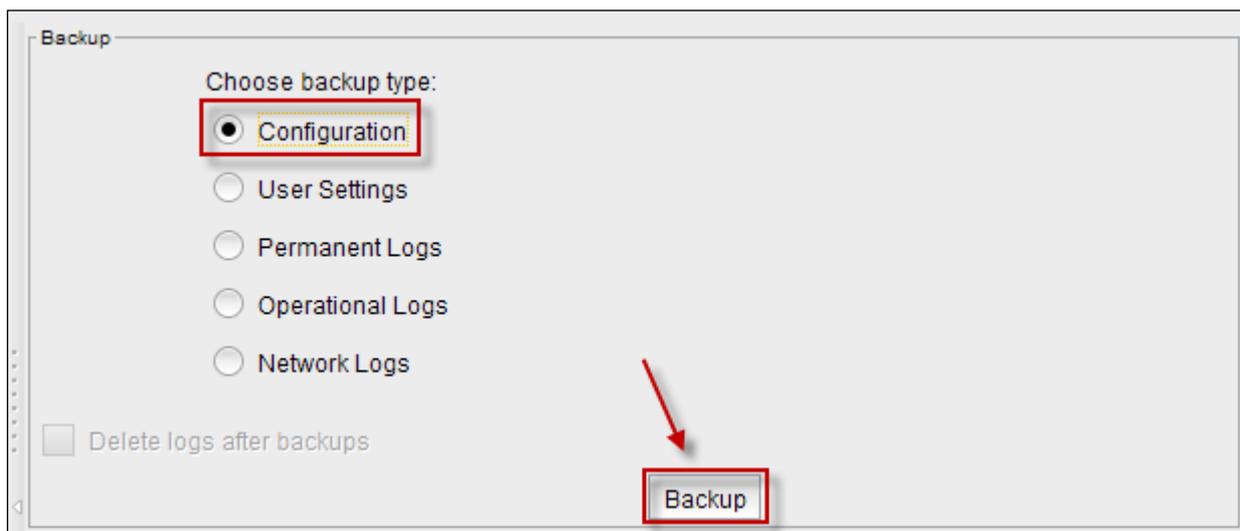
30. Configuration Backup / Restore

In **System module**, right pane select **Configuration Backup**

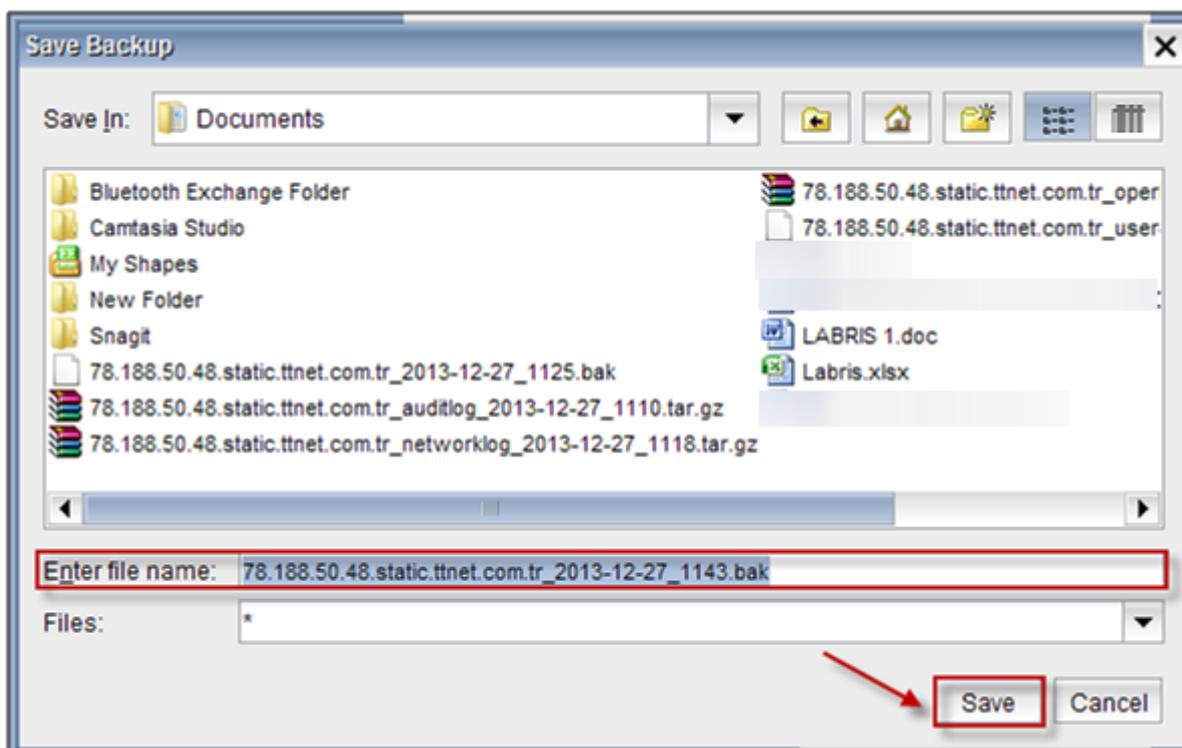


According to user requirement choose any one of the radio button in the below screen and click on **Backup Tab** to start the Backup process.

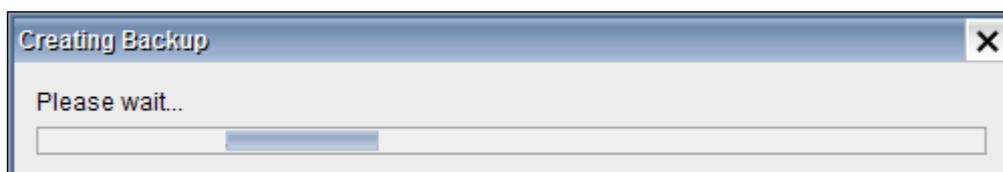
Choose **Configuration** radio button and click on **Backup** button.



Click on **Save tab** to save the file with **file name.bak** extension in your local machine as in the below screenshot.



Creating **Backup** process for **Configuration** is in progress.



Below screen appears stating that **Backup** saved at the chosen location in your hard drive, click **OK** to close the current tab.

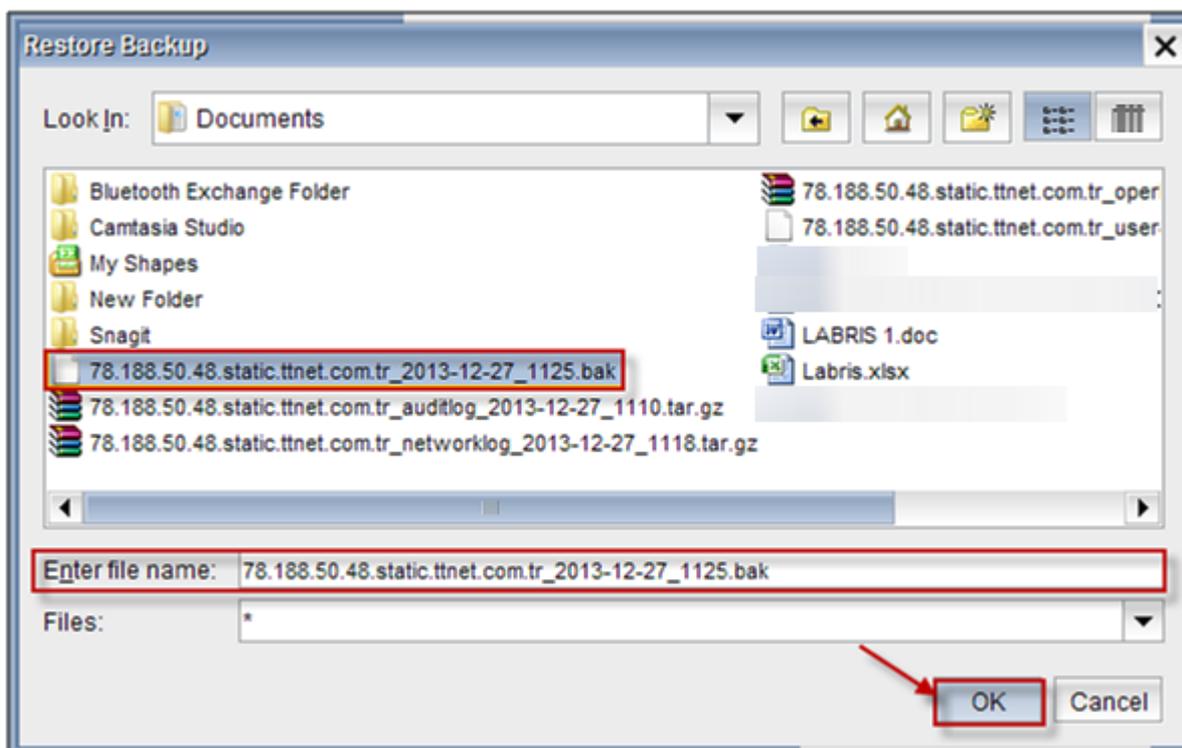


According to user requirement choose any one of the radio button in the below screen and click on **Restore** to start restore process

Choose **Configuration** and click on **Restore** button.



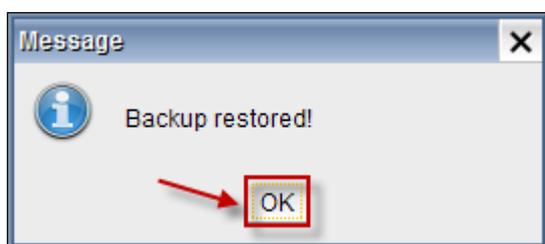
Choose the backup file from the local machine and click **OK** to **Restore Backup**



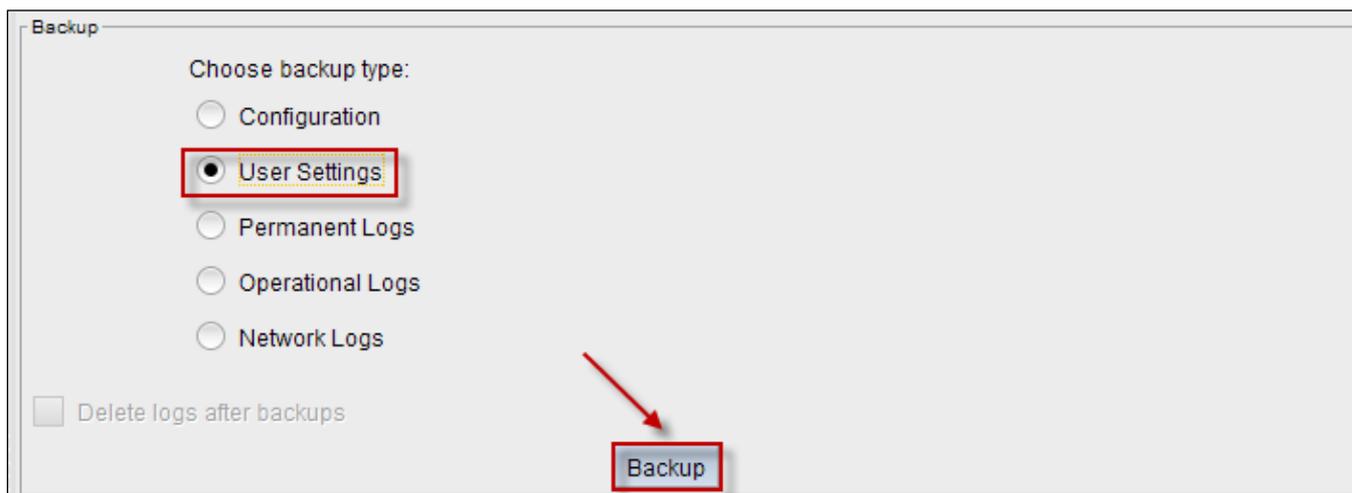
Restoring Backup process for **Configuration** is in progress.



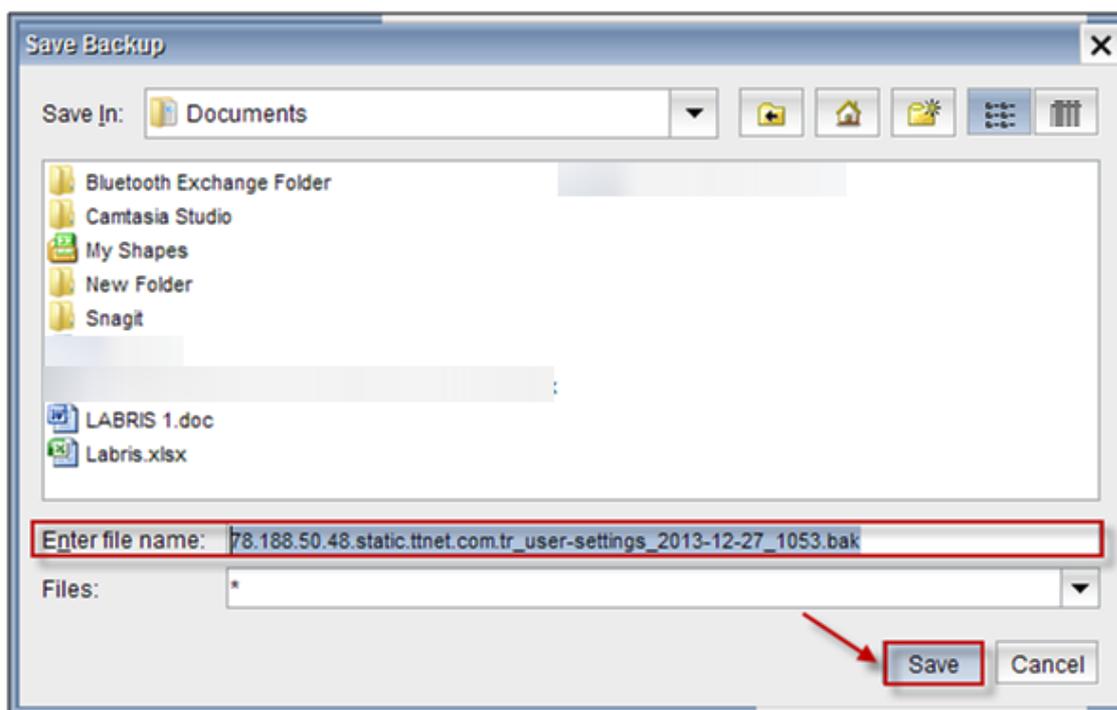
Below screen appears stating that **Backup restored**, click **OK** to close the current tab.



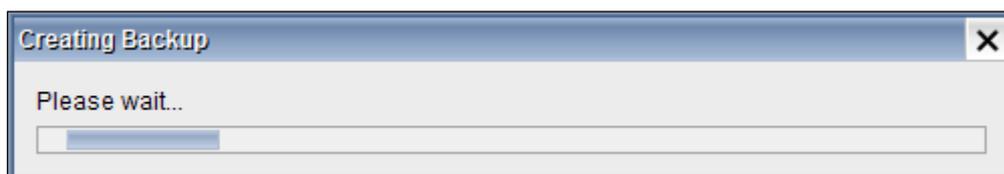
Choose **User Settings** and click on **Backup Tab**



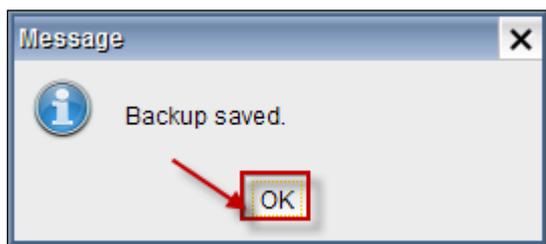
Click on **Save** tab to save the file with **file name.bak** extension in your local machine as shown in the below screen.



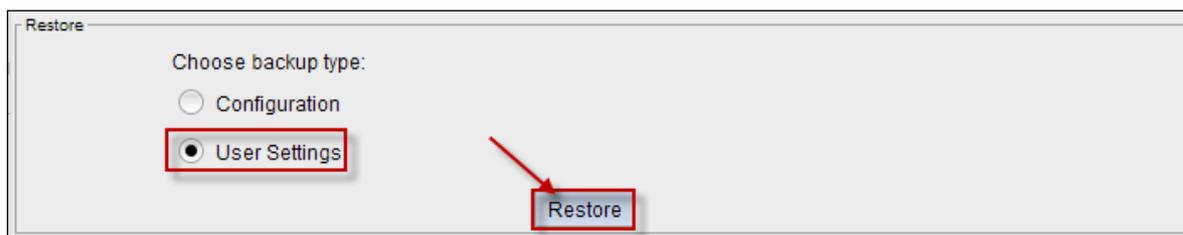
Creating **Backup** process for **User Settings** is in progress.



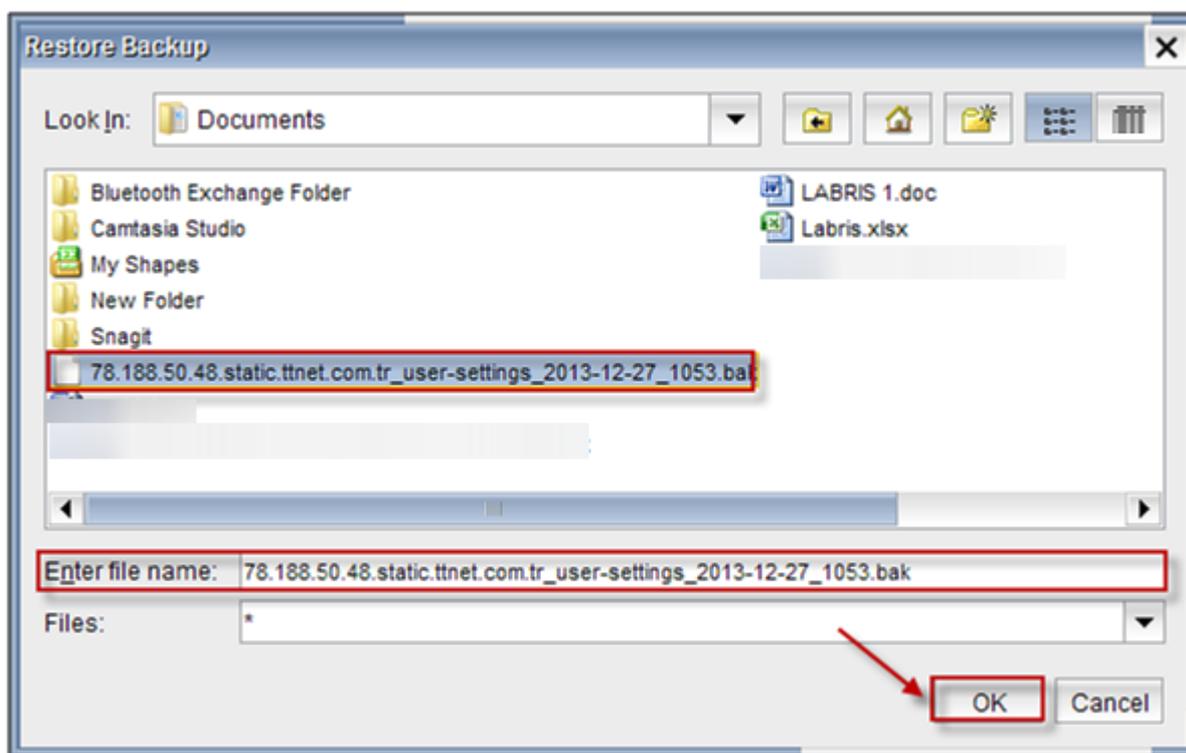
Below screen appears stating that **Backup Saved**, click **OK** to close the current tab.



Choose **User Settings** and click on **Restore** button.



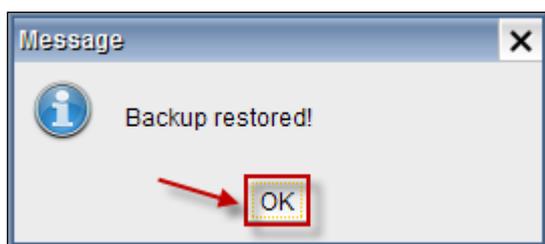
Choose the backup file from the local machine and click **Ok** to **Restore Backup**



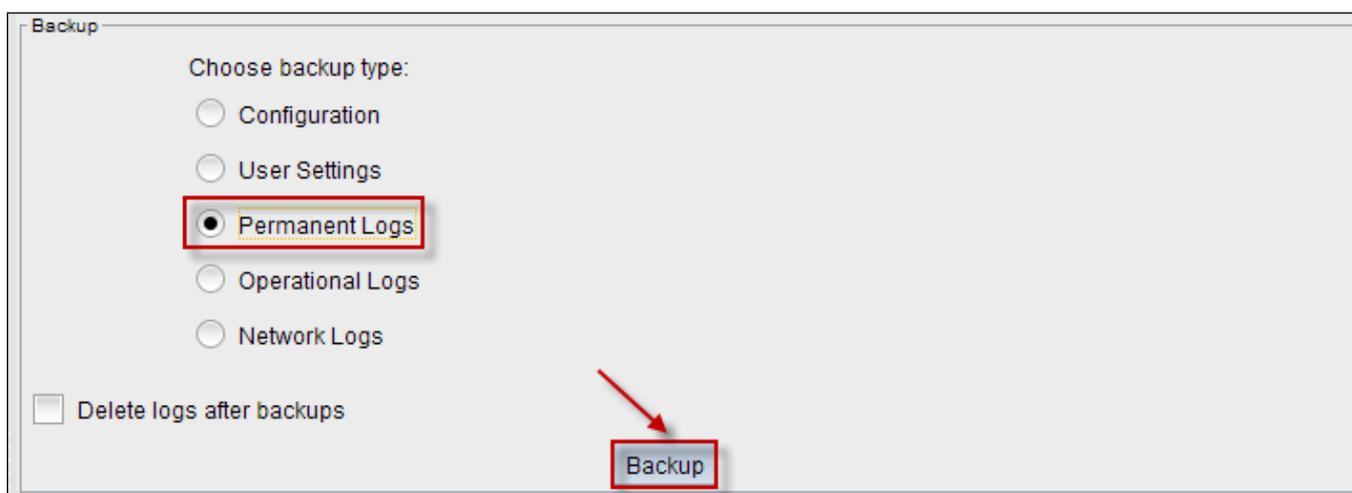
Restoring Backup process for **User Settings** is in progress.



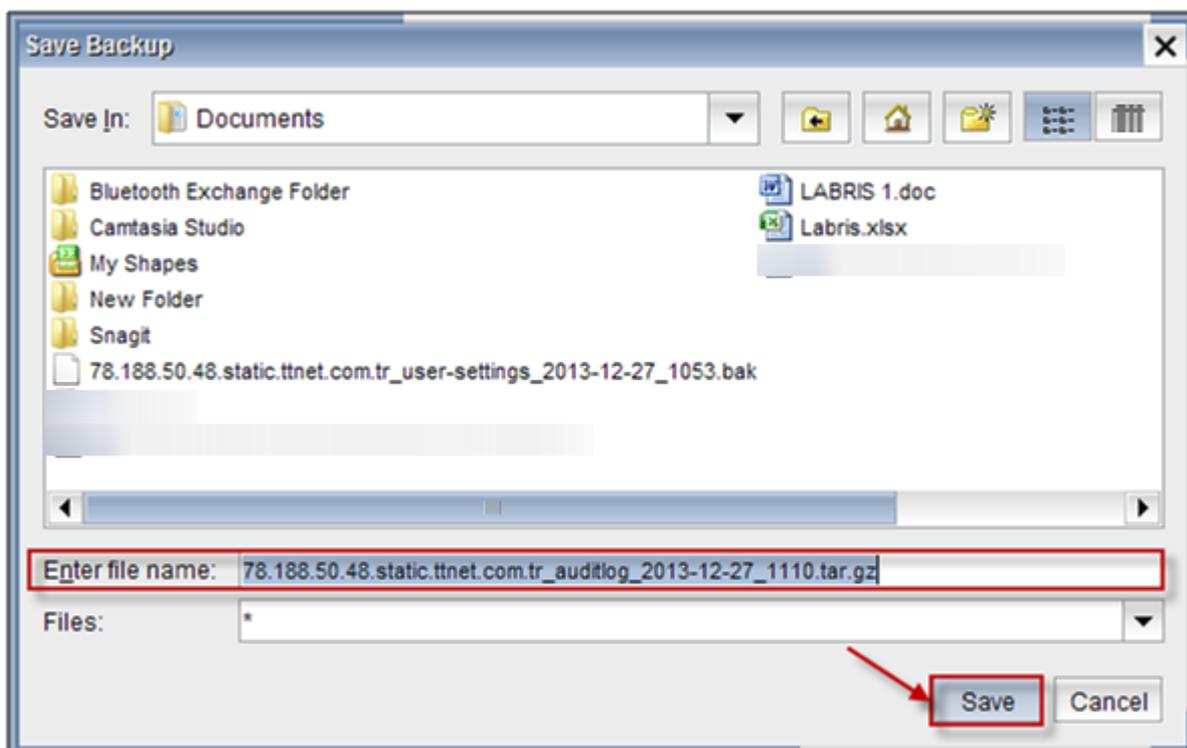
Below screen appears stating that **Backup restored**, click **OK** to close the current tab.



Choose **Permanent Logs** and click on **Backup** button.



Click on **Save tab** to save the file with **file name. tar.gz** extension in your local machine at your chosen location as shown below.



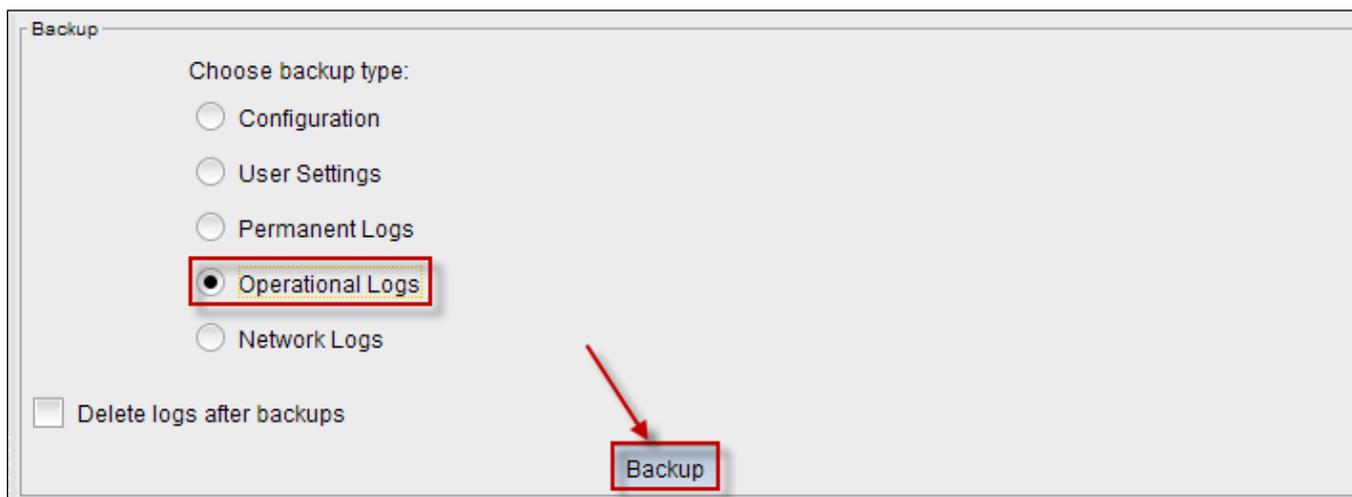
Creating **Backup** process for **Permanent logs** is in progress.



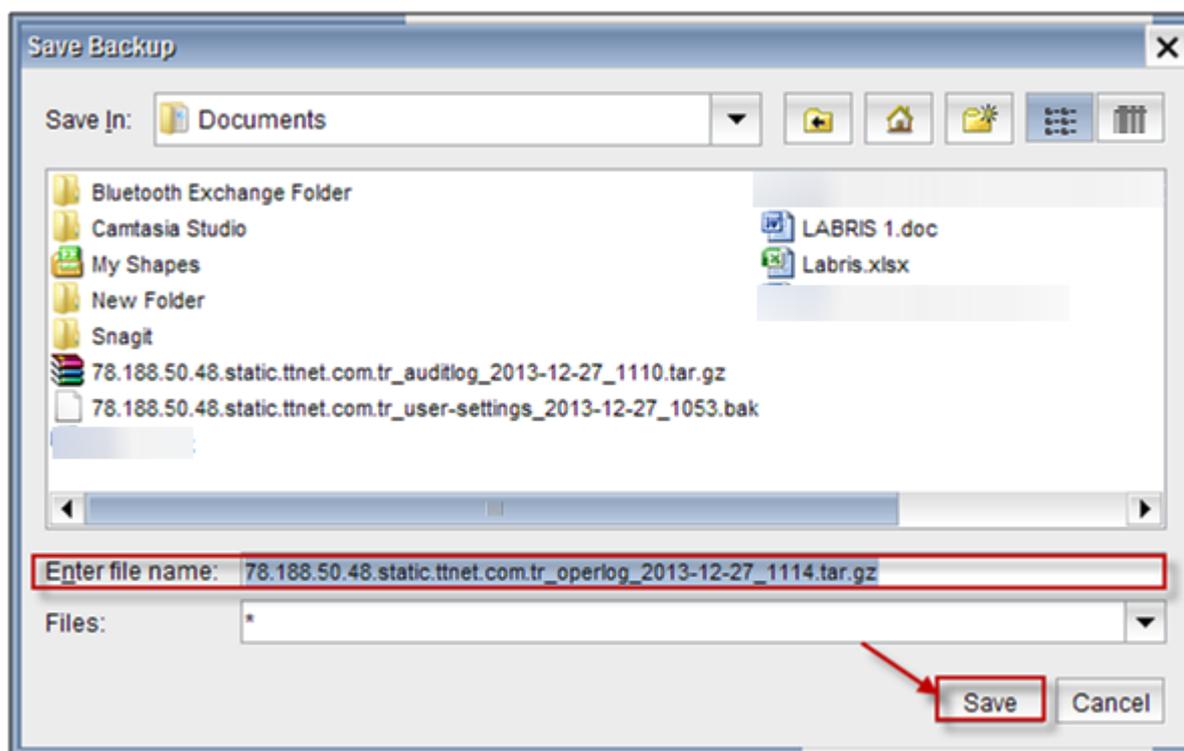
Below screen appears stating that **Backup Saved**, click **OK** to close the current tab.



Choose **Operational Logs** and click on **Backup Tab**



Click on **Save tab** to save the file with **file name .tar.gz** extension in your local machine to save the operational logs as shown below.



Creating **Backup** process for **Operational logs** is in progress.



Below screen appears stating that **Backup Saved**, click **OK** to close the current tab.

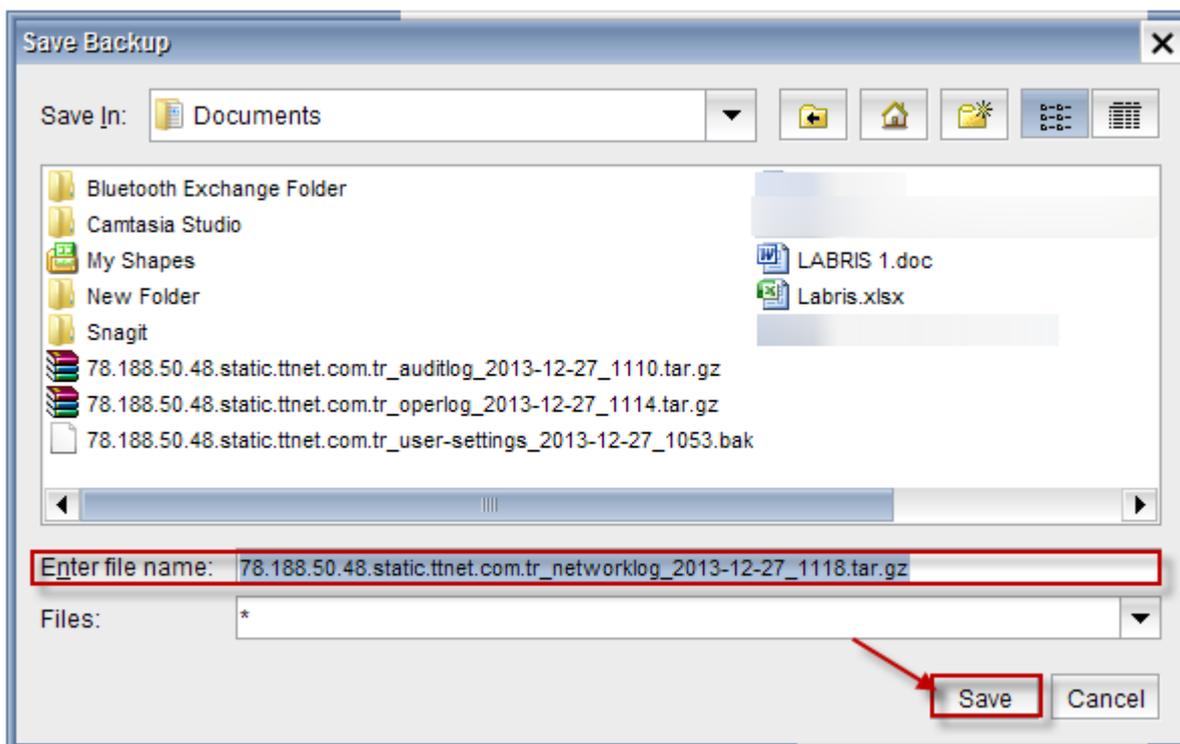


Choose **Network Logs** and click on **Backup Tab**.

If we want to delete logs after completion of Backups process for each log, Check the **Delete logs after backups** check box.



Click on **Save tab** to save the file with **file name .tar. gz** extension in your local machine as shown below.



Creating **Backup** process for **Network logs** is in progress.



Below screen appears stating that **Backup Saved**, click **OK** to close the current tab.



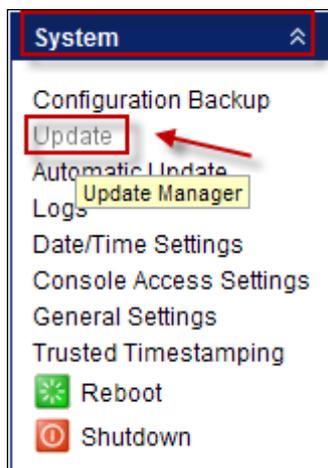
Factory settings

Click on **Factory** to roll back Labris UTM the default settings.



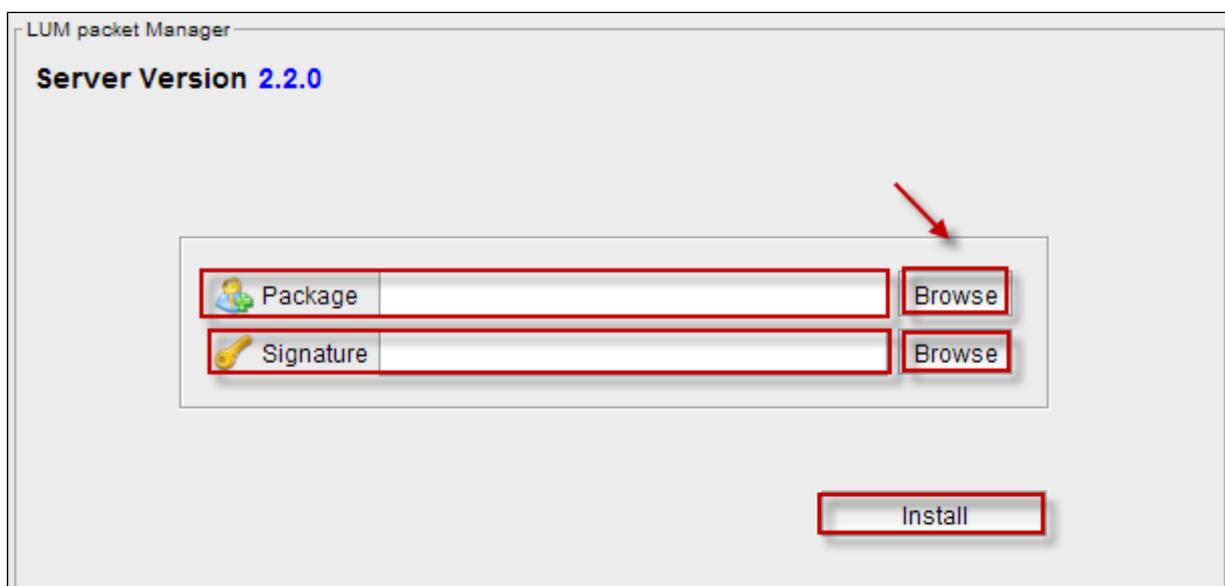
31. Update

In System module, Right Pane under system tab click on **update** tab



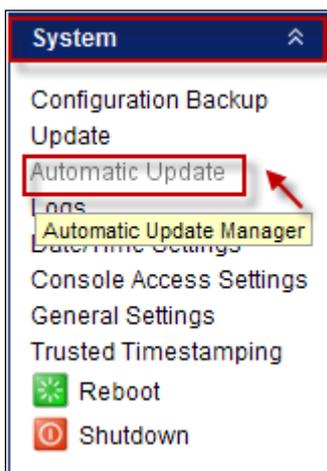
Note – In the below screen if any package is pending for upgrade, please request from the service provider using the mail id or call.

When we click on **Update Tab**, below screen appears, **Package** of the Server version and **Signature** has to be browsed from local machine and click **Install**



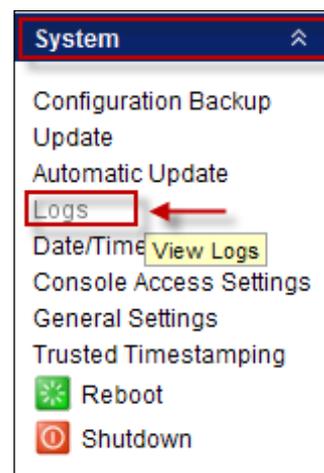
32. Automatic Update

In **System Module**, right pane under **System Tab** click on **Automatic Update Tab** to get Updated automatically



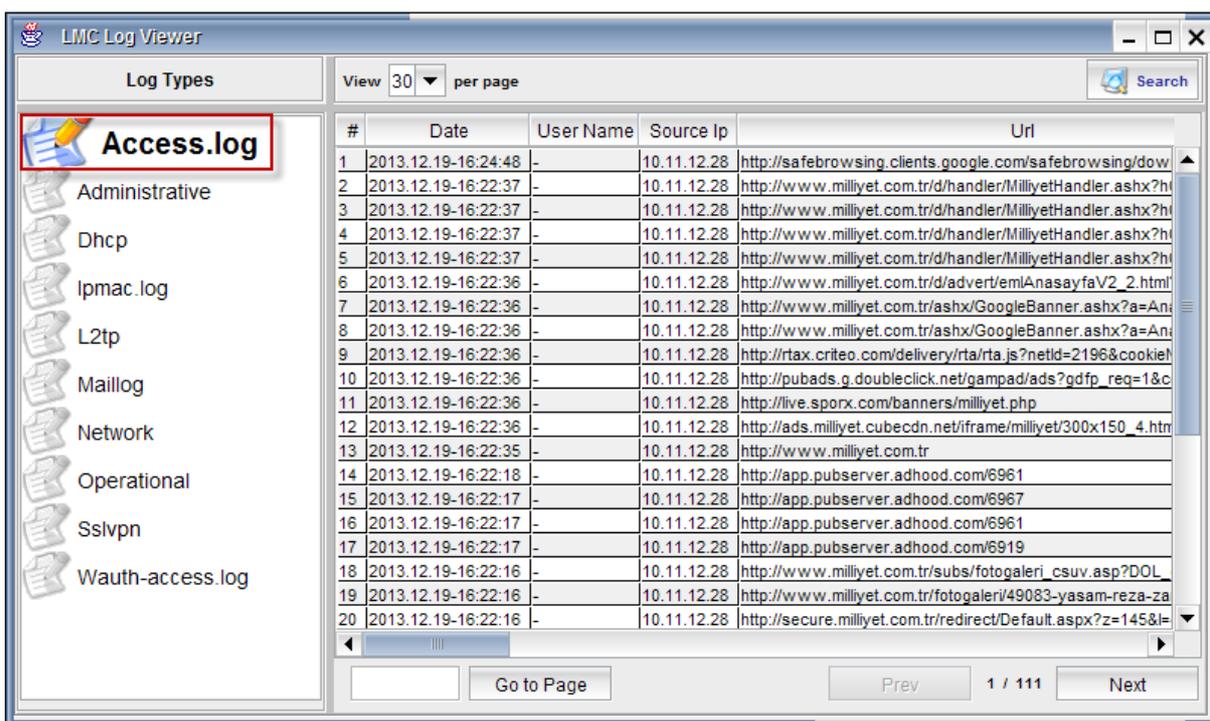
33. Record

In **System Module**, right pane under **System Tab** click on **Logs** to view Logs of LMC



Below screen appears displaying all the **Log Types** in LMC.

Select any required log from the **Log Types** then the related information is displayed in the right pane.

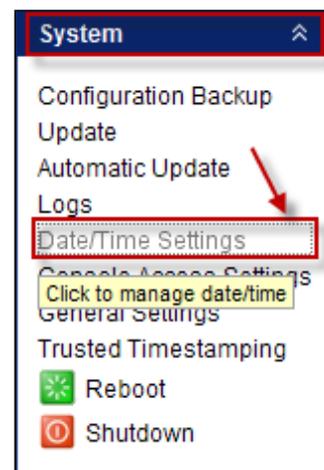


Different types of Logs in LMC.

1	Access.log	Log messages related to Access can be viewed
2	Administrative	Log messages related to Administrative can be viewed
3	Dhcp	Log messages related to Dhcp can be viewed
4	Lpmac.log	Log messages related to Lpmac can be viewed
5	L2tp	Log messages related to L2tp can be viewed
6	Maillog	Log messages related to Maillog can be viewed
7	Network log	Log messages related to Network log can be viewed
8	Operational	Log messages related to Operational can be viewed
9	Ssslvpn	Log messages related to Ssslvpn can be viewed
10	Wauth-access.log	Log messages related to Wauth-access can be viewed

34. Date / Time Settings

In **System Module**, right pane under **System Tab** click on **Date/Time Settings**.

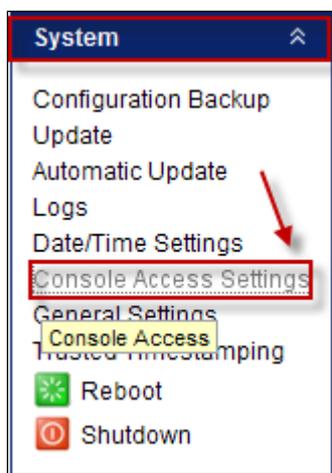


Below screen appears, set the date and time and click **Save** to save the **Current Date/Time**.



35. Console Access Settings

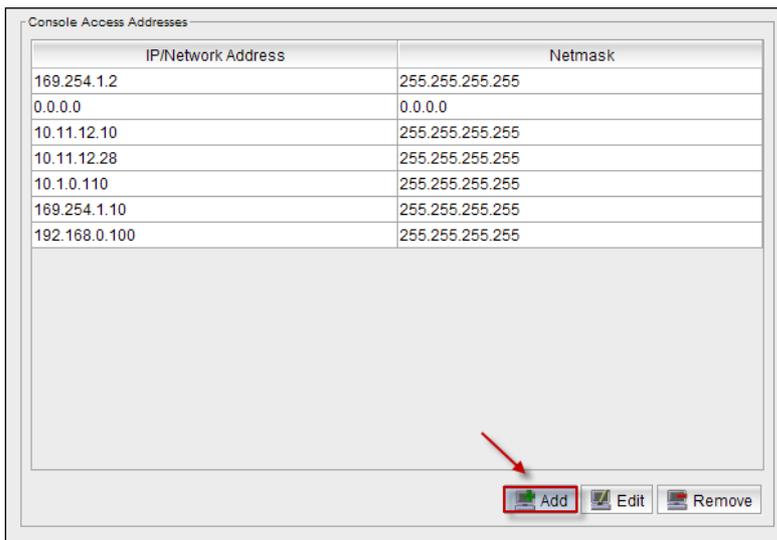
In **System Module**, right pane under **System Tab** click on **Console Access Settings**.



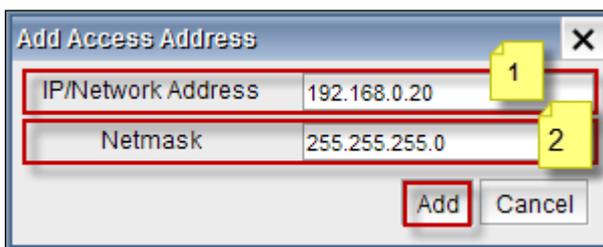
Enable **Block remote console access** check box to block remote access for other users or desktops.



Click on **Add Tab** to add an **IP/Network Address** to **Console Access Address**.

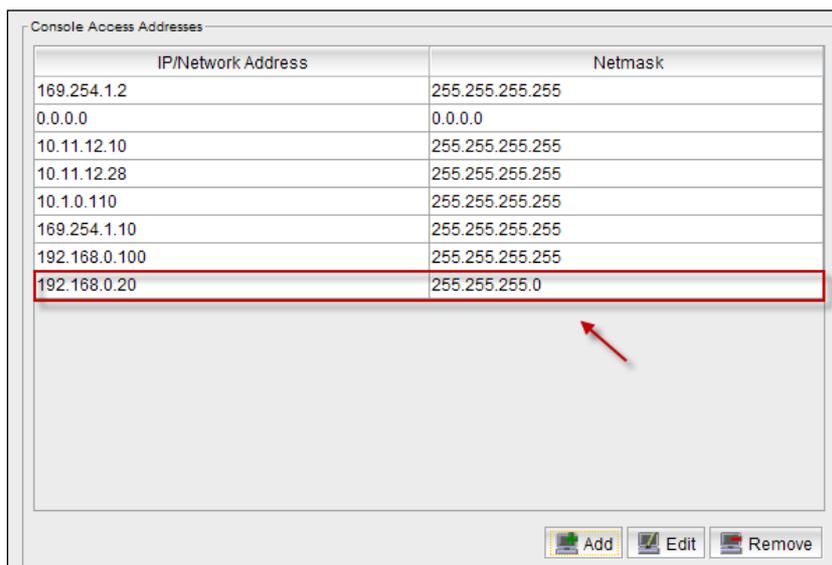


Below screen appears

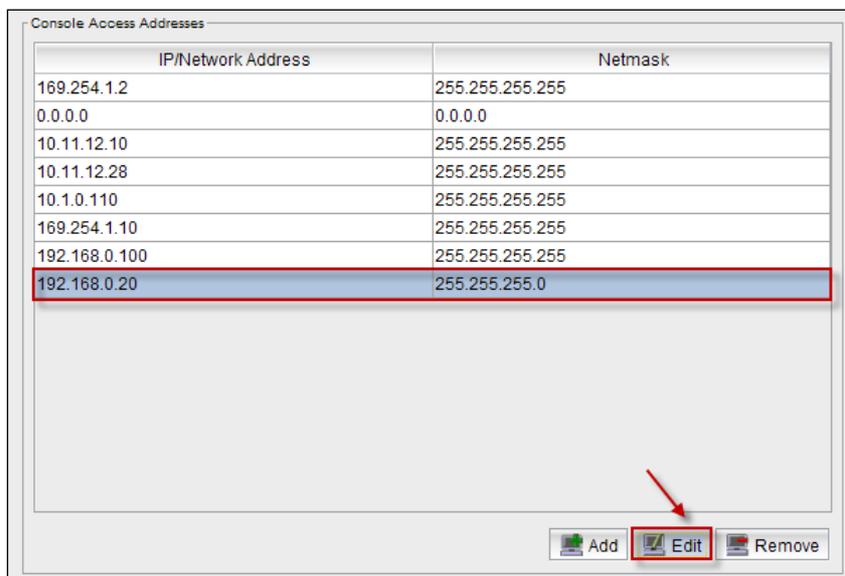


1	IP/Network Address	Type IP/Network Address
2	Netmask	Type Sub Netmask

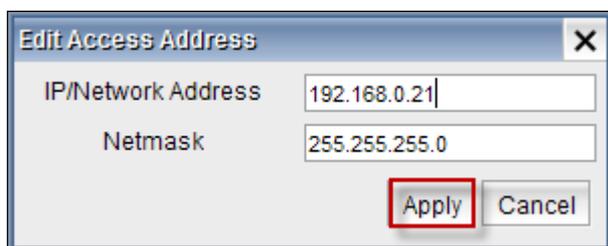
We can notice the **IP/Network** address in the **Console Access Address**



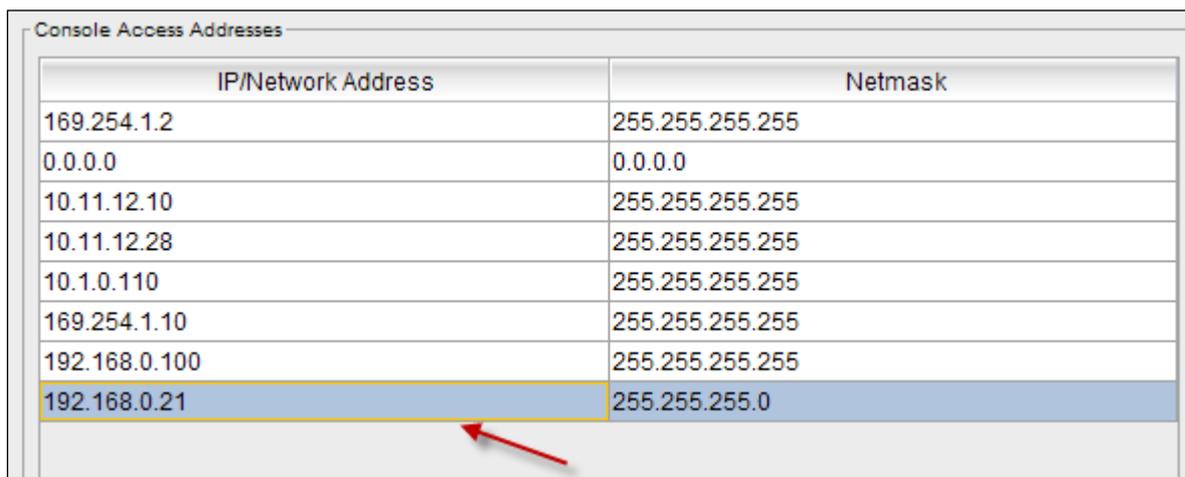
Select the **IP/Network Address** and click on **Edit** button.



We can **Edit** the **IP/Network Address** and click **Apply**.

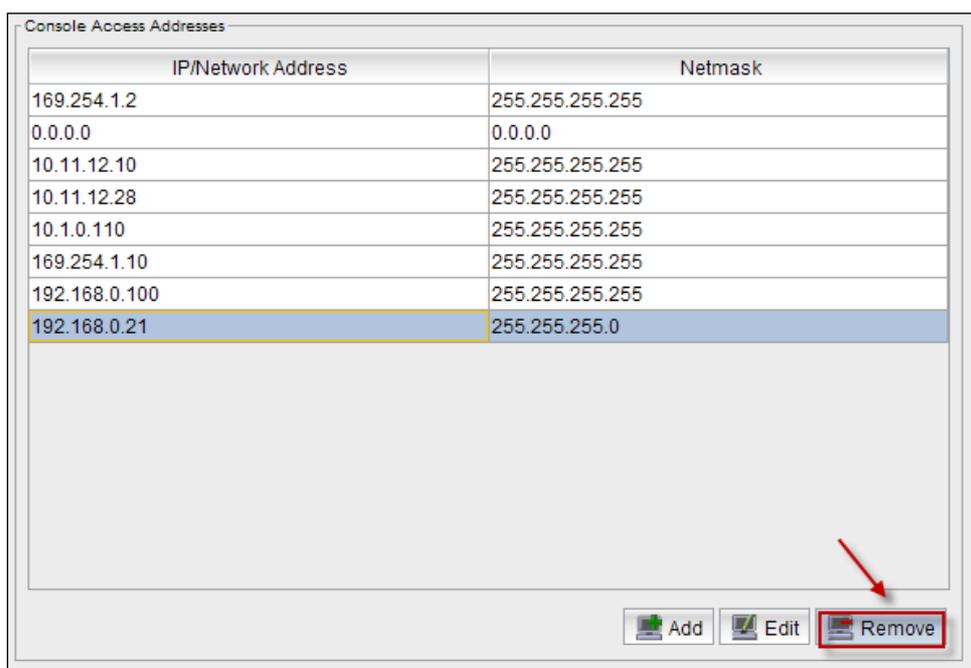


We can notice the applied changes



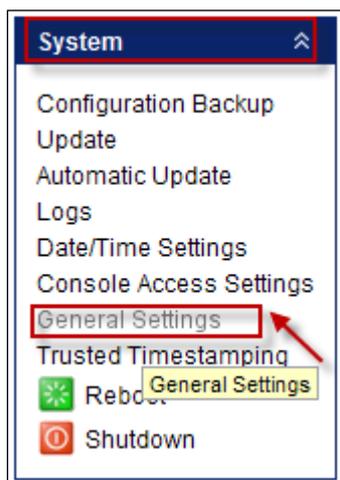
IP/Network Address	Netmask
169.254.1.2	255.255.255.255
0.0.0.0	0.0.0.0
10.11.12.10	255.255.255.255
10.11.12.28	255.255.255.255
10.1.0.110	255.255.255.255
169.254.1.10	255.255.255.255
192.168.0.100	255.255.255.255
192.168.0.21	255.255.255.0

Select the **IP/Network Address** and click on **Remove** button, then it will be removed from the **Console Access Address**.



36. General Settings

In **System Module**, right pane under **System Tab** click on **General Settings**.

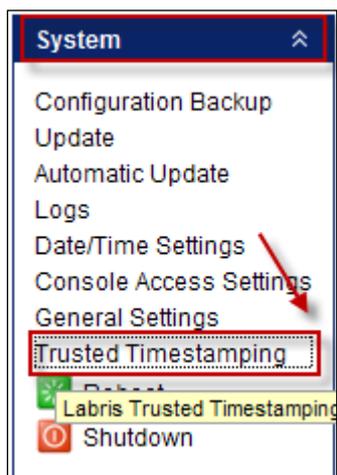


Below screen will appear displaying **Hostname**, **Internal network hostname/IP address**, and **Notification mail address**.

A screenshot of a configuration page with three sections. The first section is "Hostname" with a text input field containing "slave" and a "Save" button. The second section is "Web Access Address" with a text input field containing "localhost.localdomain" and a "Save" button. The third section is "System Monitor Settings" with a text input field containing "noreply@labristeknoloji.com" and a "Save" button. Each input field is highlighted with a red rectangular box.

37. Trusted Time Stamp

In **System Module**, rightpane under **System tab** select **Trusted Time stamping**



Below screen appears displaying **settings** and **Previous Time Stamped Log Packages**, select **log/date/hash row** click on **Save Tab**.

Turkey is valid within the boundaries of the "Law No. 5651" requirement;

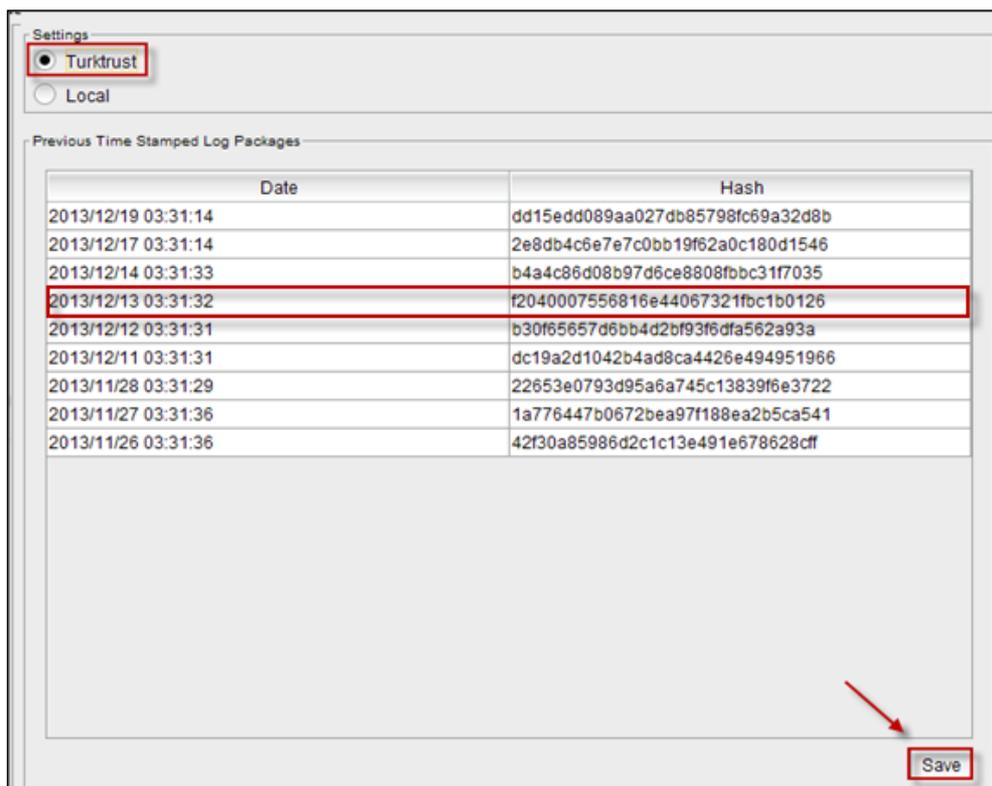
content provider, provider, access provider and public liability and responsibilities of providers of certain crimes committed on the internet with the content relating to the fight over the location and access providers and procedures.

The item is provided on behalf of the meet.

Must be held according to law, and the mandatory or hits just set **cvvars labris** UTM equipment that meets the requirement of the law in any way.

In the case of certain specified property on every day or **istenillmesiperiyorlarda** for the protection of the State against the log file, which consists of modified authorized the signing of the "TURK TRUST" side of the premises.

Select the Log file and click on **Save**

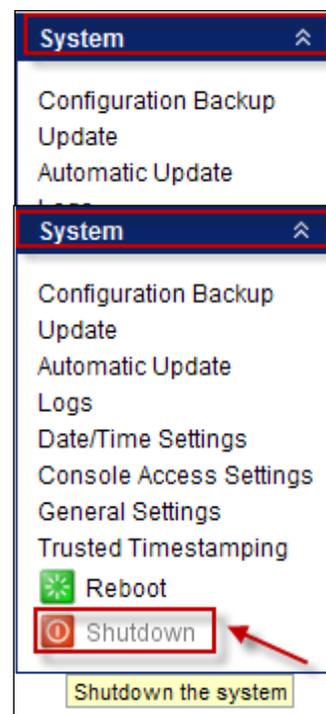


38. Restart

In System Module, under **System Tab** click on **Reboot** to Reboot the System.

39. Shutdown

In System Module, under **System Tab** click on **Shutdown** to shutdown the System.



Network Settings

In Network settings IP Configuration and Routing can be done for Labris UTM appliance.

In this section we can **Add, Delete, Edit** and **View** the Status of the Interface.

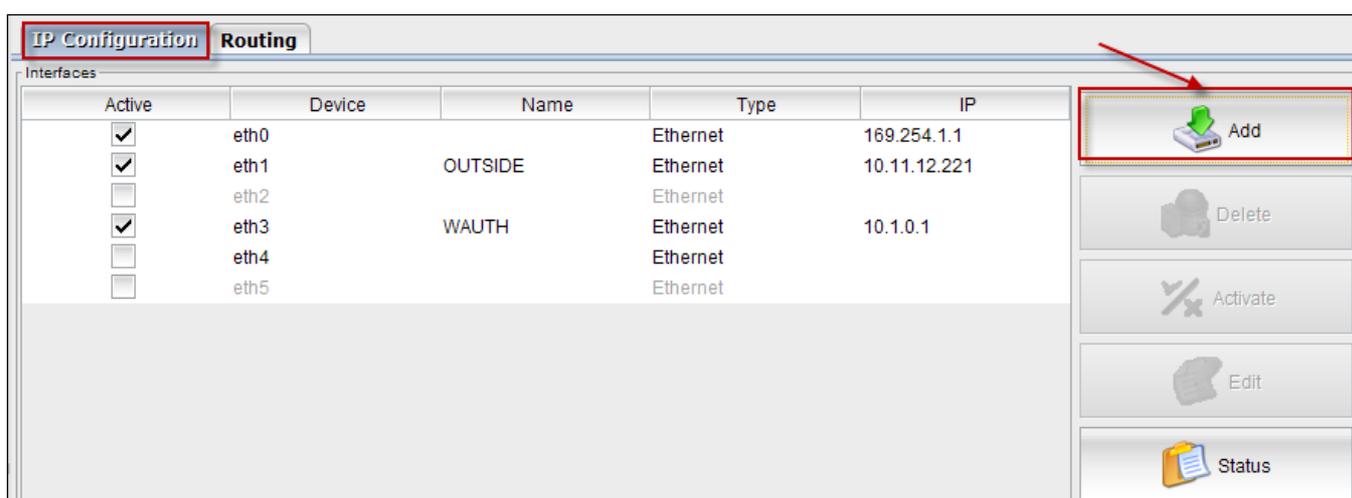
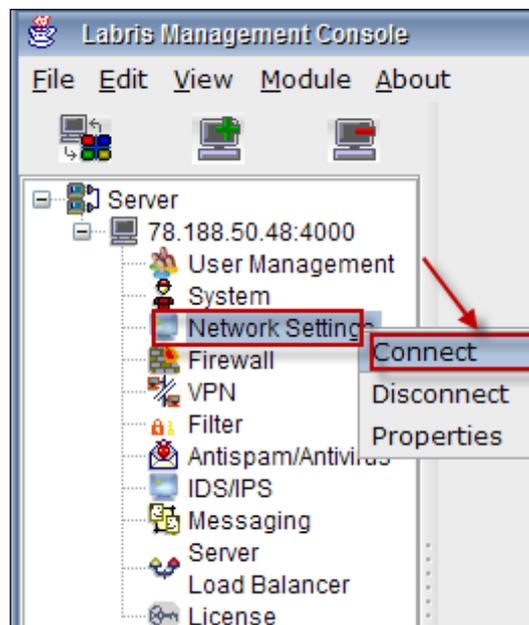
40. IP Configuration

Labris Secure Gateway is a capable router, and it has many Ethernet interfaces both used for security and also routing, load balancing and many other network tasks. IP Routing is used to Configure Ethernet interfaces and routing configuration of Labris Security Gateway.

Right click on **Network Settings** and select **Connect**.

IP Alias (Add, Edit, Delete, Status, Enable/disable)

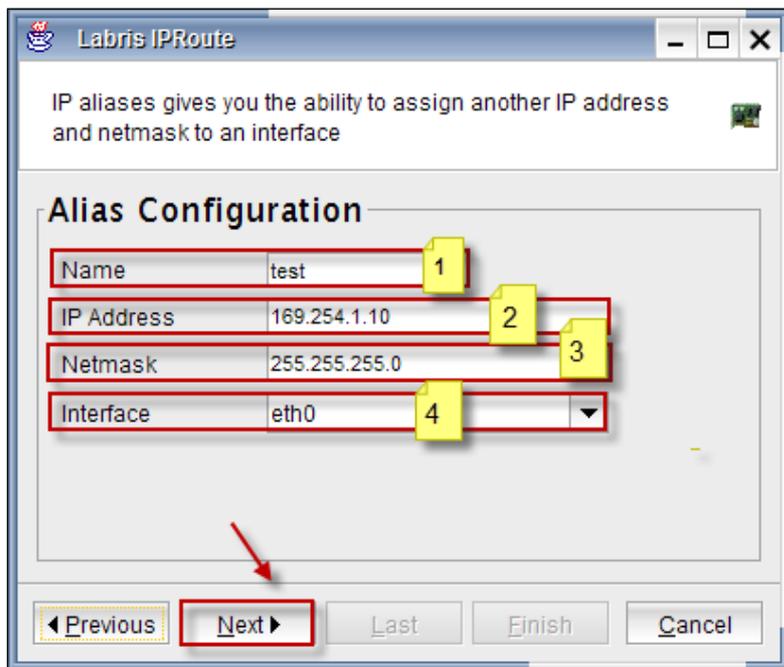
Below screen appears select **IP Configuration**, click on **Add** button.



Choose **IP Alias** radio button from the types of **Interfaces**, Click on **Next** button to continue the process.



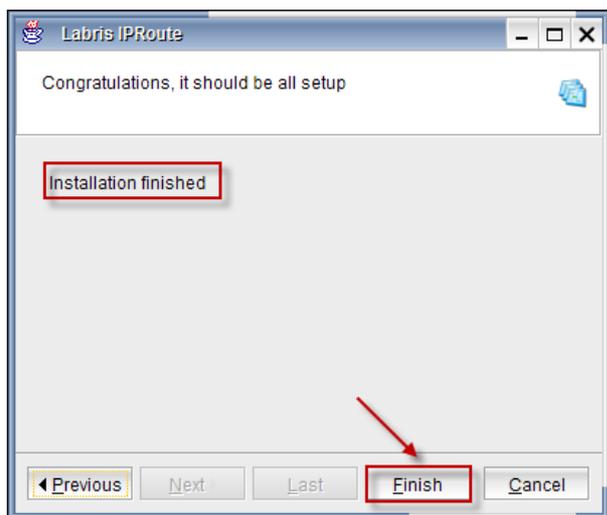
Configuration of the **Alias connection**.



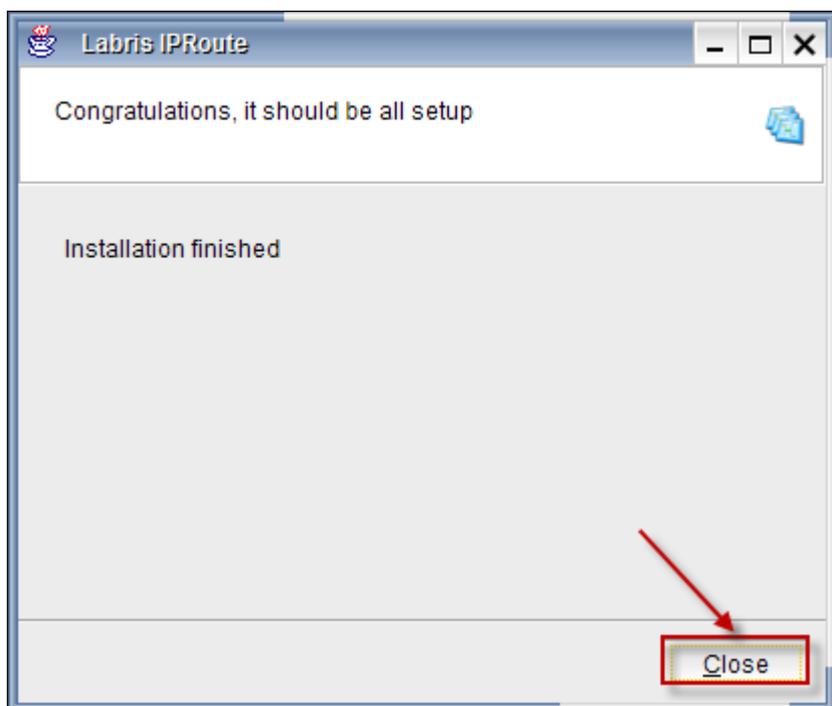
These are the inputs for the Configuration of Interface.

1	Name	Type the Name
2	IP Address	Give the IP Address
3	Netmask	Type the Netmask
4	Interface	Select Interface from the drop down Menu

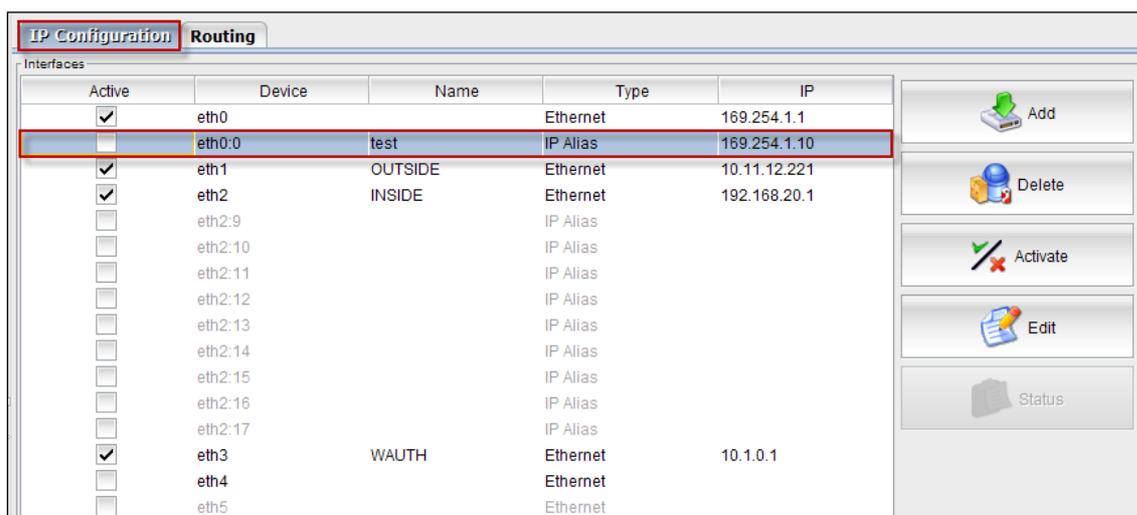
Installation is finished, Click on **Finish** button.



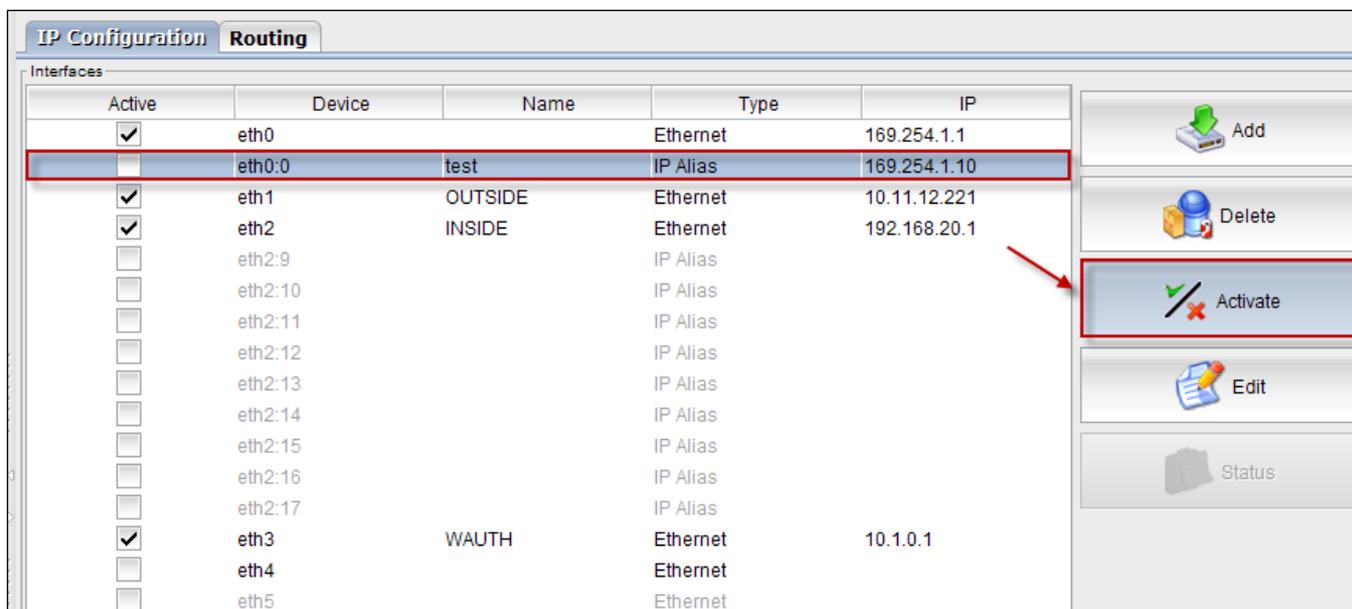
Below screen appears, click on **close** button.



We can notice the New interface added to the Interfaces list with **IP Alias connection**.



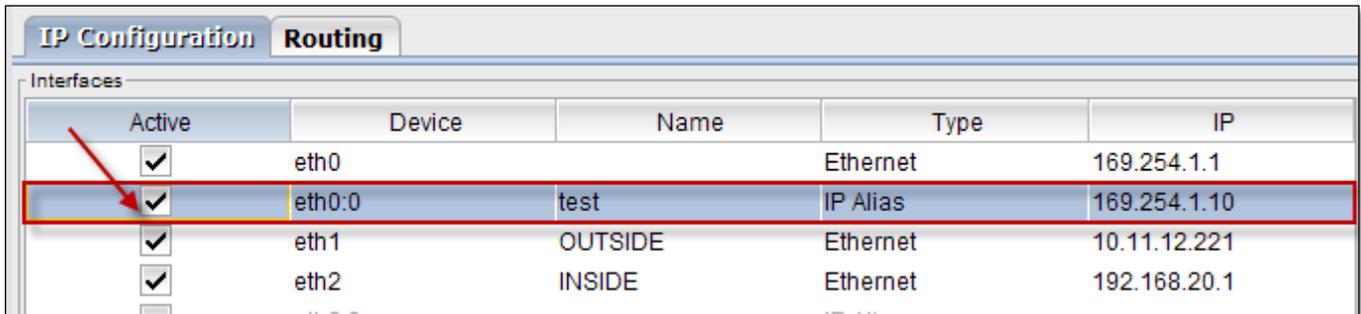
Select the Interface and click on **Activate** button.



Activation process is in progress.



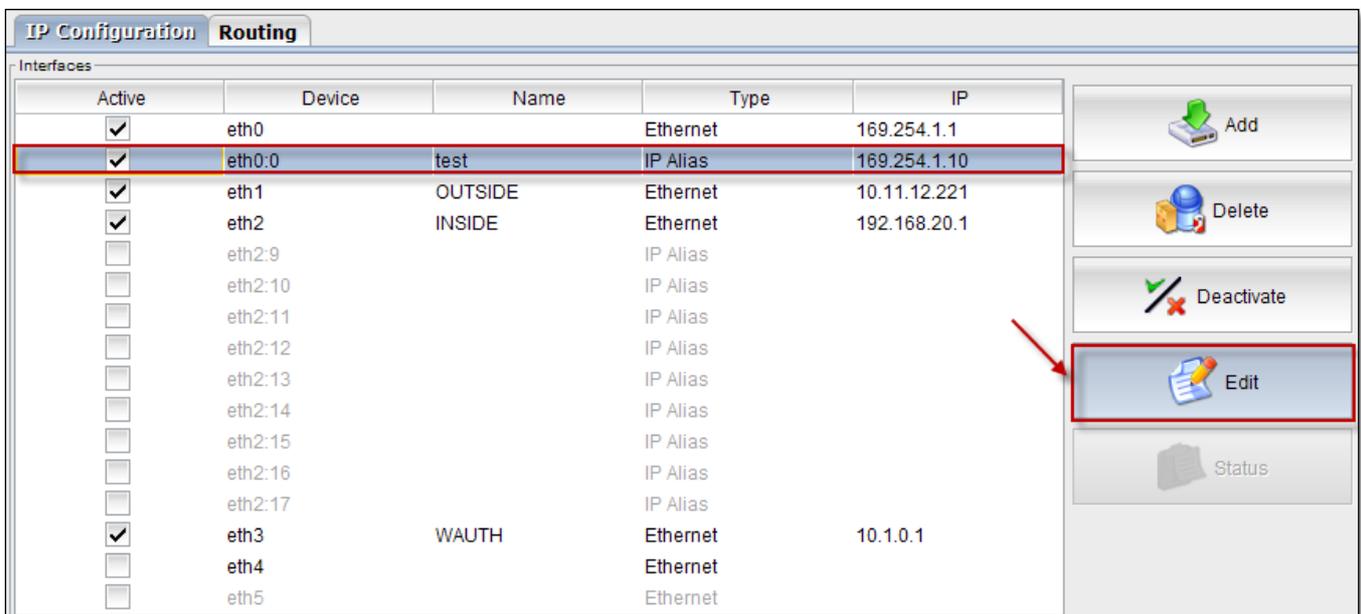
Now we can notice that the newly added Interface is **Active**.



Active	Device	Name	Type	IP
<input checked="" type="checkbox"/>	eth0		Ethernet	169.254.1.1
<input checked="" type="checkbox"/>	eth0:0	test	IP Alias	169.254.1.10
<input checked="" type="checkbox"/>	eth1	OUTSIDE	Ethernet	10.11.12.221
<input checked="" type="checkbox"/>	eth2	INSIDE	Ethernet	192.168.20.1

Editing IP Alias

Select the Interface and click on **Edit** button to Edit the Interface.

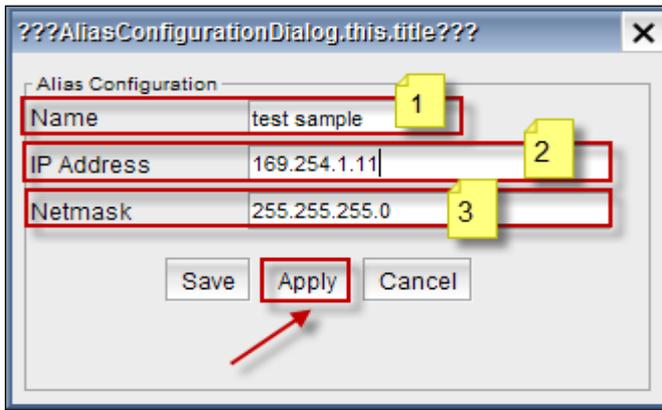


Editing the **Alias configuration**, give the inputs and click on **Apply** tab to apply the changes.

Note

- Click on **Save tab** to save the changes in Configuration

Note: Click on **Save tab** to save the changes in configuration.



These are the inputs for **Editing** the Interface

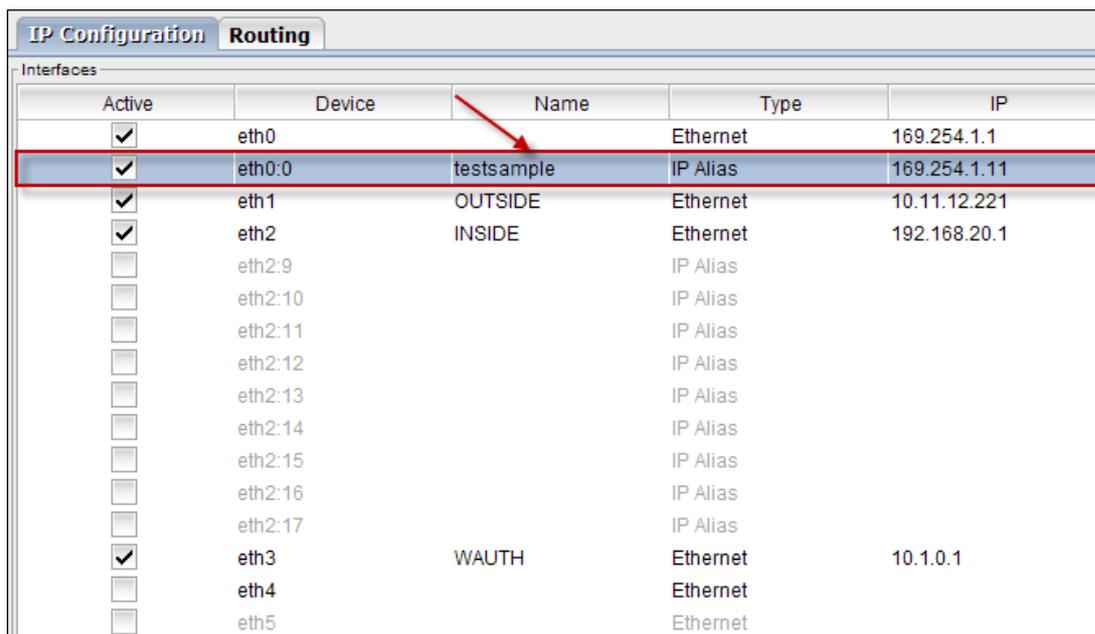
1	Name	We can Edit the existing Name
2	IP Address	We can Edit the existing IP Address
3	Netmask	Give the Netmask for the given IP Address

After applying the changes, Interface will restart.

Restart process is in progress.



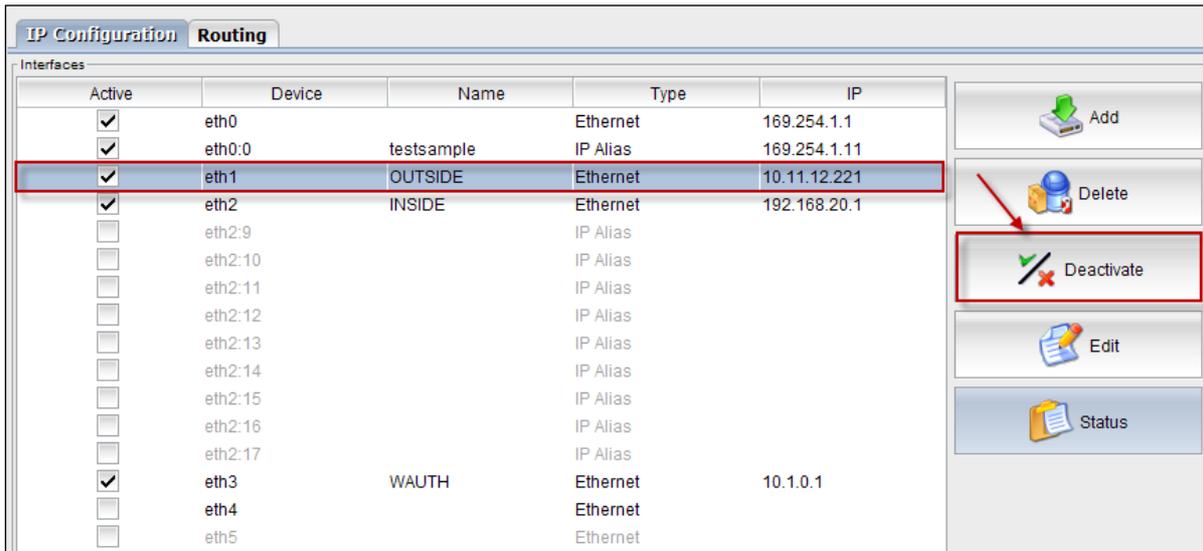
We can notice the changes in the Interface in the **Interfaces** list.



Active	Device	Name	Type	IP
<input checked="" type="checkbox"/>	eth0		Ethernet	169.254.1.1
<input checked="" type="checkbox"/>	eth0:0	testsample	IP Alias	169.254.1.11
<input checked="" type="checkbox"/>	eth1	OUTSIDE	Ethernet	10.11.12.221
<input checked="" type="checkbox"/>	eth2	INSIDE	Ethernet	192.168.20.1
<input type="checkbox"/>	eth2:9		IP Alias	
<input type="checkbox"/>	eth2:10		IP Alias	
<input type="checkbox"/>	eth2:11		IP Alias	
<input type="checkbox"/>	eth2:12		IP Alias	
<input type="checkbox"/>	eth2:13		IP Alias	
<input type="checkbox"/>	eth2:14		IP Alias	
<input type="checkbox"/>	eth2:15		IP Alias	
<input type="checkbox"/>	eth2:16		IP Alias	
<input type="checkbox"/>	eth2:17		IP Alias	
<input checked="" type="checkbox"/>	eth3	WAUTH	Ethernet	10.1.0.1
<input type="checkbox"/>	eth4		Ethernet	
<input type="checkbox"/>	eth5		Ethernet	

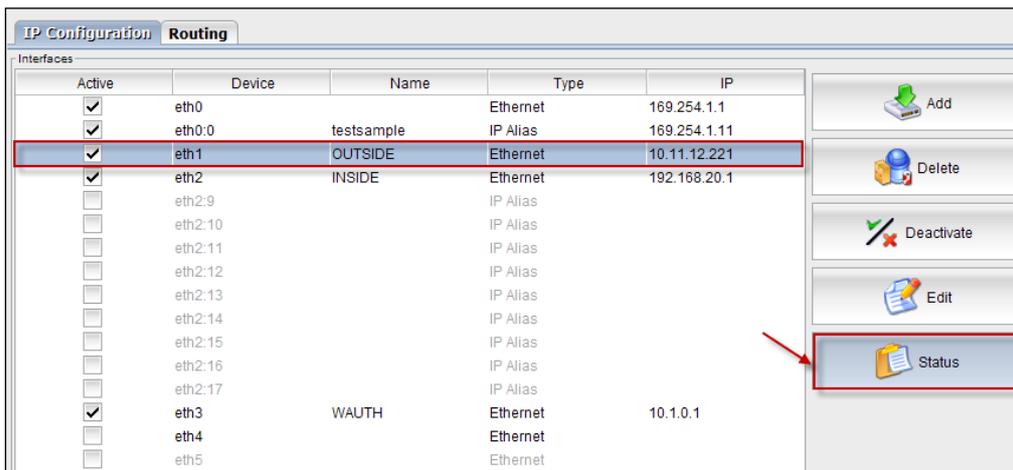
Enable / Disable

Select the **Interface** and click on **Deactivate** button to deactivate the Interface.

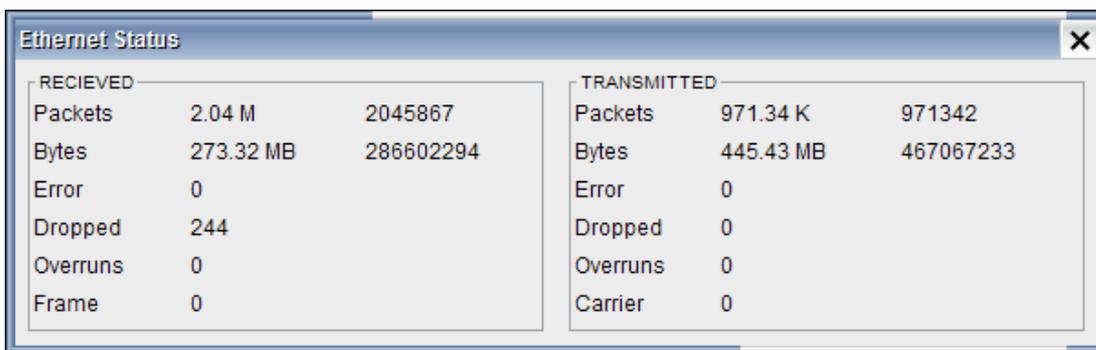


Status

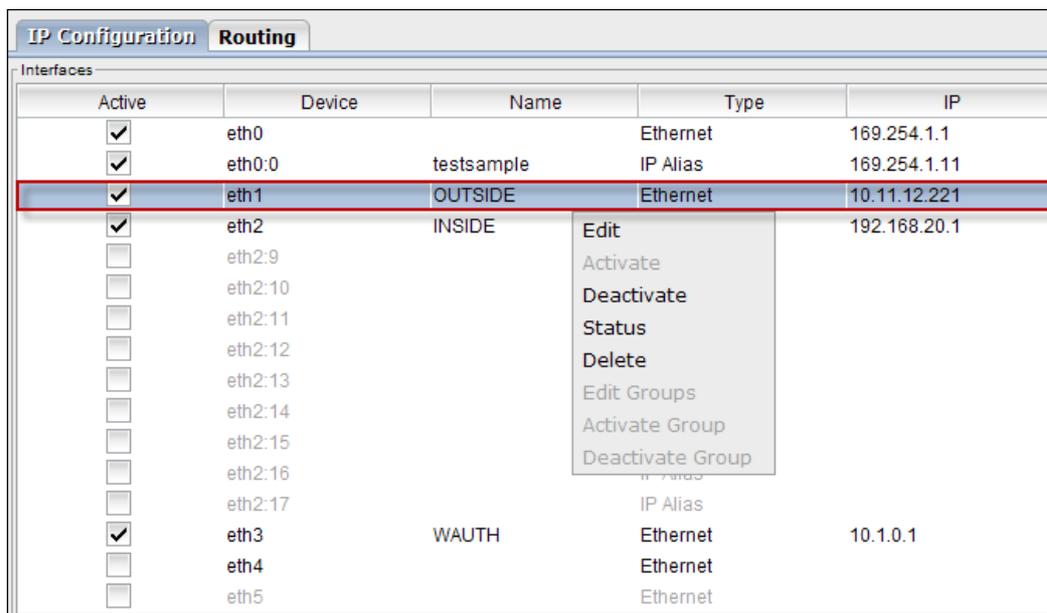
Select the **Interface** and Click on **Status** button to check the status of the Interface



Below screen gives the status of the Interface

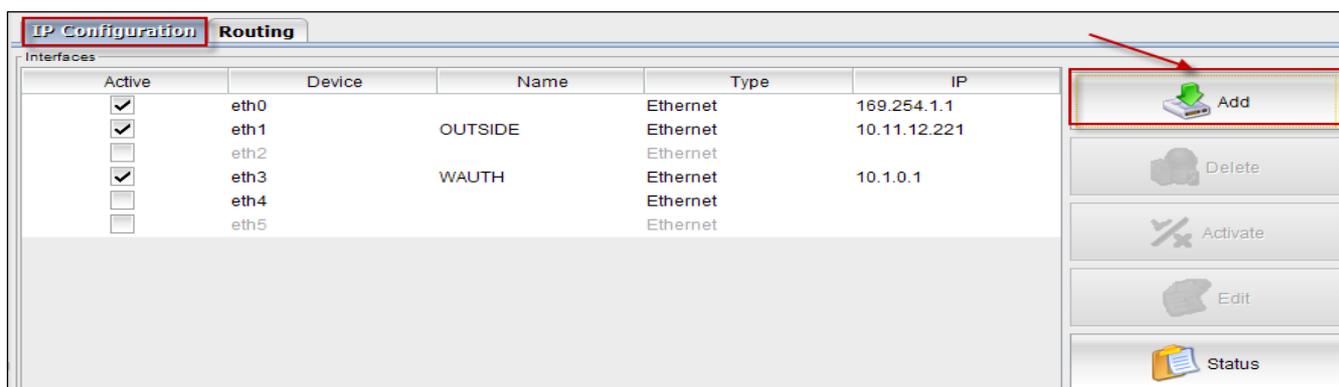


Right click on the Interface, to perform **Edit, Activate, Deactivate, status, Delete, Edit groups, Activate groups, Deactivate groups** actions.



ADSL (Add, Edit, Delete, Status, Enable/Disable)

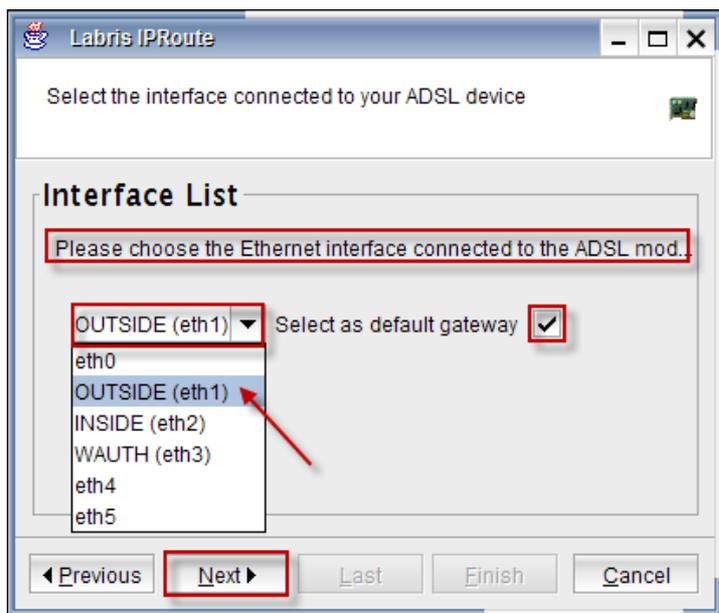
Select **IP Configuration** and click on **Add** button



Choose **ADSL** from the types of Interfaces and click on **Next** button to continue.



Choose the Ethernet Interface to the ADSL from the drop down list, check mark the default Gateway and click on **Next** button.



User Information should be provided

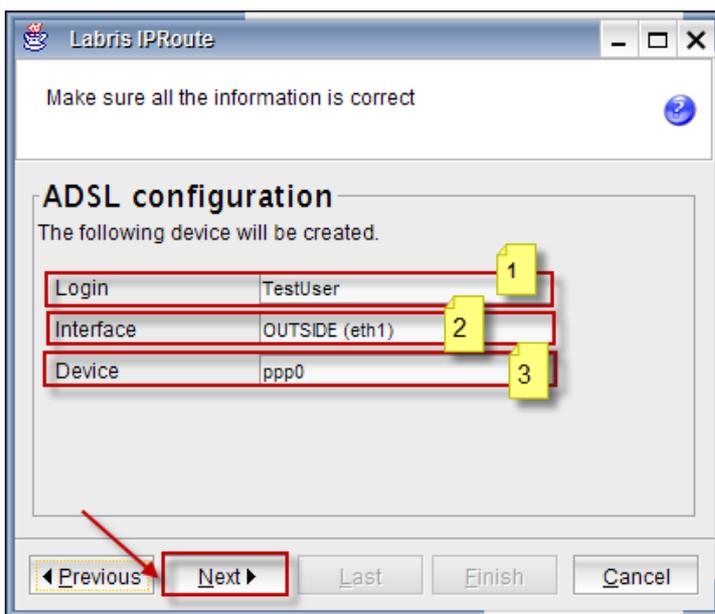


These are the inputs for the User

1	Login	Type Login name of the User
2	Password	Type the Password of the User
3	Password (again)	Type the Password of the User again for confirmation

ADSL

Configuration of ADSL connection.

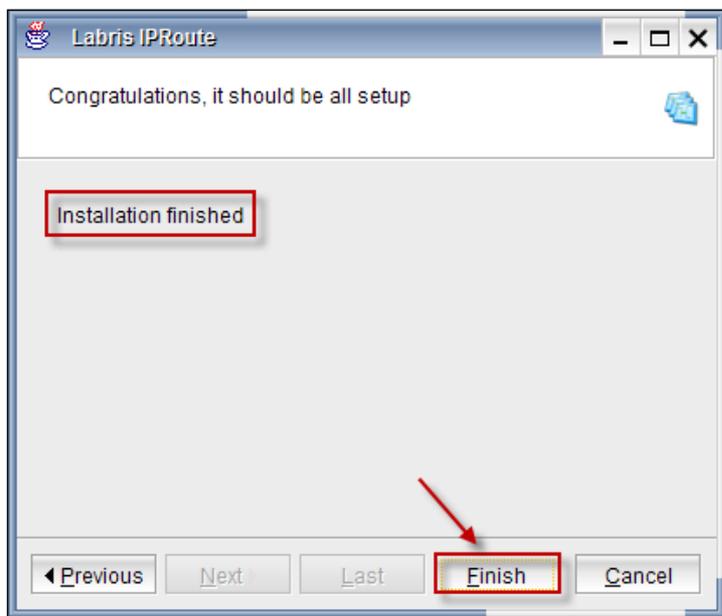


1	Login	It displays Login name of the User
2	Interface	It displays the Interface type

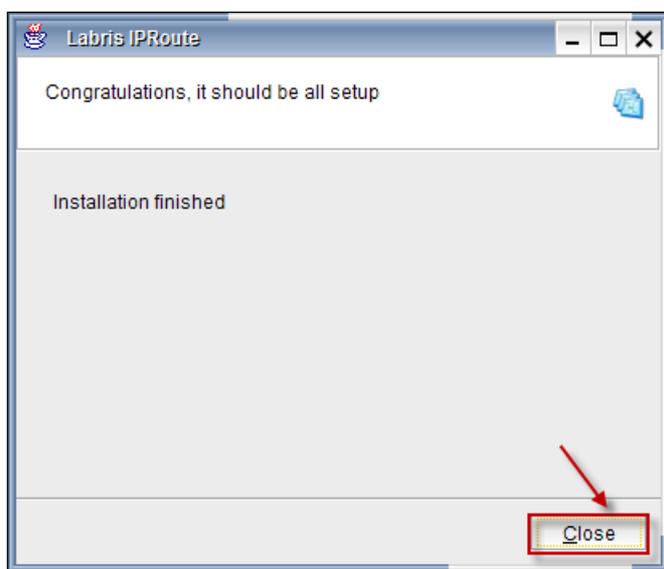
3	Device	It displays device name
---	---------------	-------------------------

Click on **Next** button to continue.

Once the installation is finished, Click on **Finish** button.



Below screen appears, click on **close** button.



We can notice Interface added in the Interfaces list with ADSL type of connection

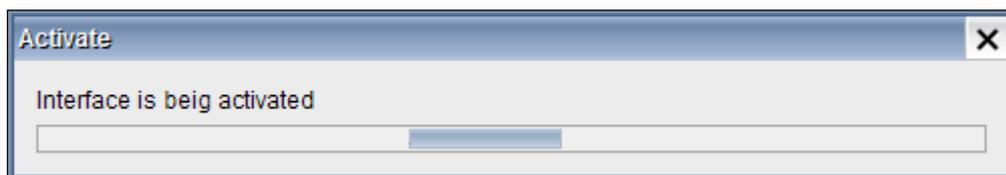
Active	Device	Name	Type	IP
<input checked="" type="checkbox"/>	eth0		Ethernet	169.254.1.1
<input checked="" type="checkbox"/>	eth0:0	testsample	IP Alias	169.254.1.11
<input checked="" type="checkbox"/>	eth1	OUTSIDE	Ethernet	10.11.12.221
<input type="checkbox"/>	ppp0		ADSL	
<input checked="" type="checkbox"/>	eth2	INSIDE	Ethernet	192.168.20.1
<input type="checkbox"/>	eth2:9		IP Alias	
<input type="checkbox"/>	eth2:10		IP Alias	
<input type="checkbox"/>	eth2:11		IP Alias	
<input type="checkbox"/>	eth2:12		IP Alias	
<input type="checkbox"/>	eth2:13		IP Alias	
<input type="checkbox"/>	eth2:14		IP Alias	
<input type="checkbox"/>	eth2:15		IP Alias	
<input type="checkbox"/>	eth2:16		IP Alias	
<input type="checkbox"/>	eth2:17		IP Alias	
<input checked="" type="checkbox"/>	eth3	WAUTH	Ethernet	10.1.0.1
<input type="checkbox"/>	eth4		Ethernet	
<input type="checkbox"/>	eth5		Ethernet	

Active	Device	Name	Type	IP
<input checked="" type="checkbox"/>	eth0		Ethernet	169.254.1.1
<input checked="" type="checkbox"/>	eth0:0	testsample	IP Alias	169.254.1.11
<input checked="" type="checkbox"/>	eth1	OUTSIDE	Ethernet	10.11.12.221
<input type="checkbox"/>	ppp0		ADSL	
<input checked="" type="checkbox"/>	eth2	INSIDE	Ethernet	192.168.20.1
<input type="checkbox"/>	eth2:9		IP Alias	
<input type="checkbox"/>	eth2:10		IP Alias	
<input type="checkbox"/>	eth2:11		IP Alias	
<input type="checkbox"/>	eth2:12		IP Alias	
<input type="checkbox"/>	eth2:13		IP Alias	
<input type="checkbox"/>	eth2:14		IP Alias	
<input type="checkbox"/>	eth2:15		IP Alias	
<input type="checkbox"/>	eth2:16		IP Alias	
<input type="checkbox"/>	eth2:17		IP Alias	
<input checked="" type="checkbox"/>	eth3	WAUTH	Ethernet	10.1.0.1
<input type="checkbox"/>	eth4		Ethernet	
<input type="checkbox"/>	eth5		Ethernet	

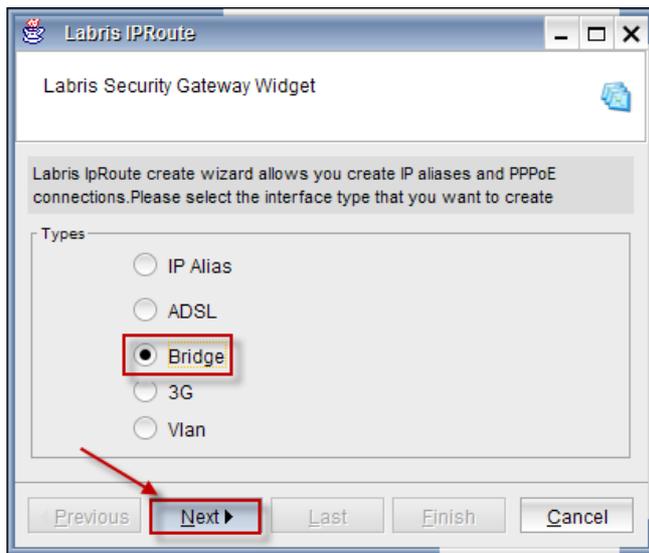
Buttons: Add, Delete, **Activate**, Edit, Status

Select the Interface and click on **Activate** button to activate the **Interface**.

Activation process is in progress

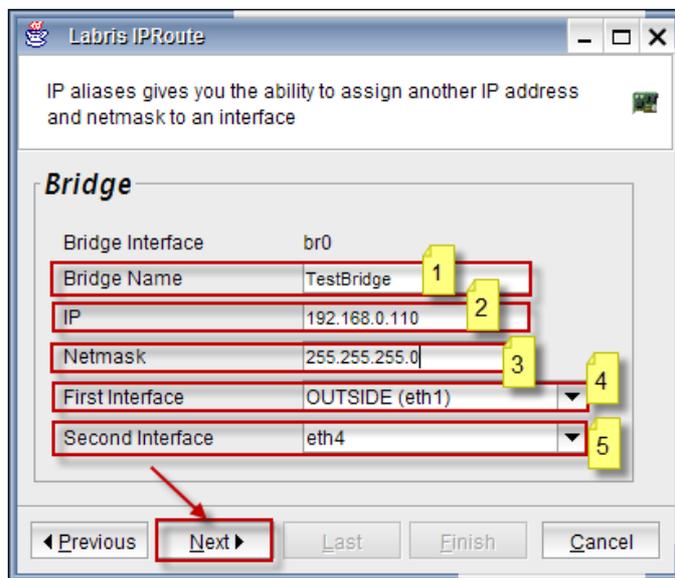


Bridge(Add ,Edit, Delete, Status , Enable/disable)



To configure Bridge connection for the Interface select **Bridge radio button** from the types of connection.

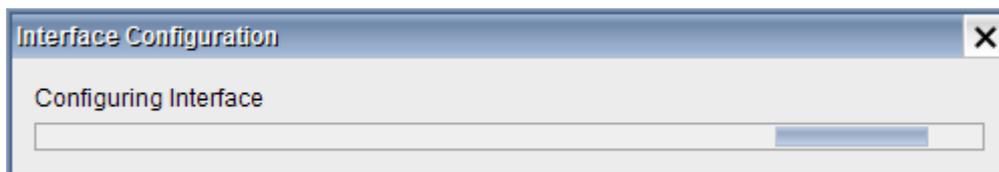
Configuration of Bridge Connection screen.



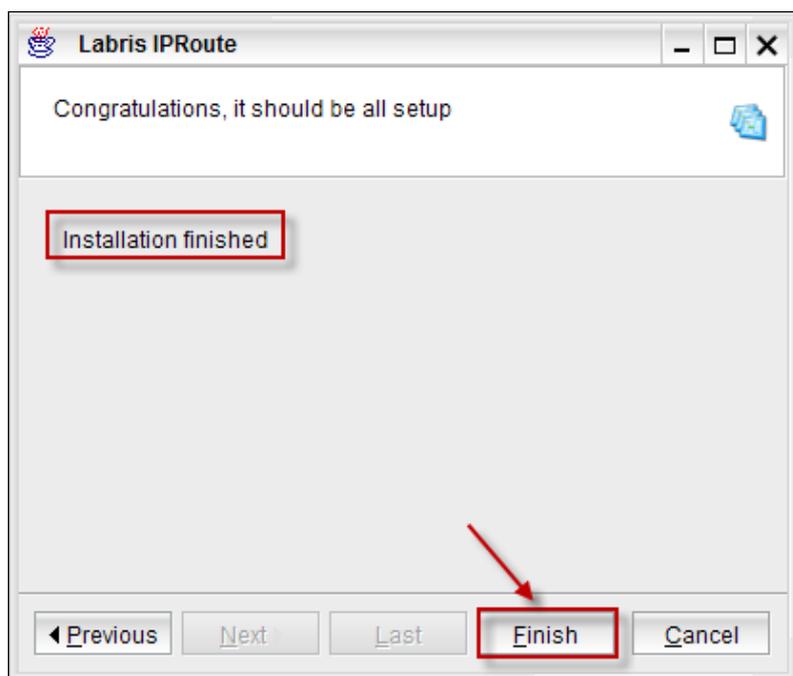
These are the inputs for Bridge connection

1	Bridge Name	Type the Bridge connection
2	IP	Type the IP Address
3	Netmask	Type the Netmask
4	First Interface	Select the First Interface from the drop down list
5	Second Interface	Select the Second Interface from the drop down list

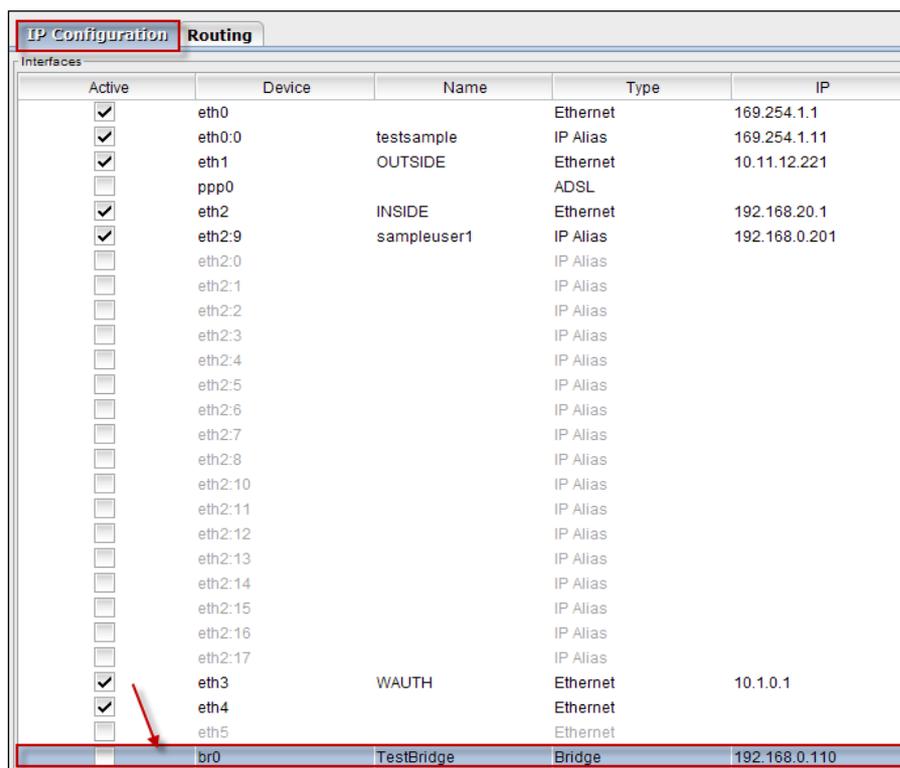
Interface Configuration process is in progress



Once the installation finished click on **Finish** button.



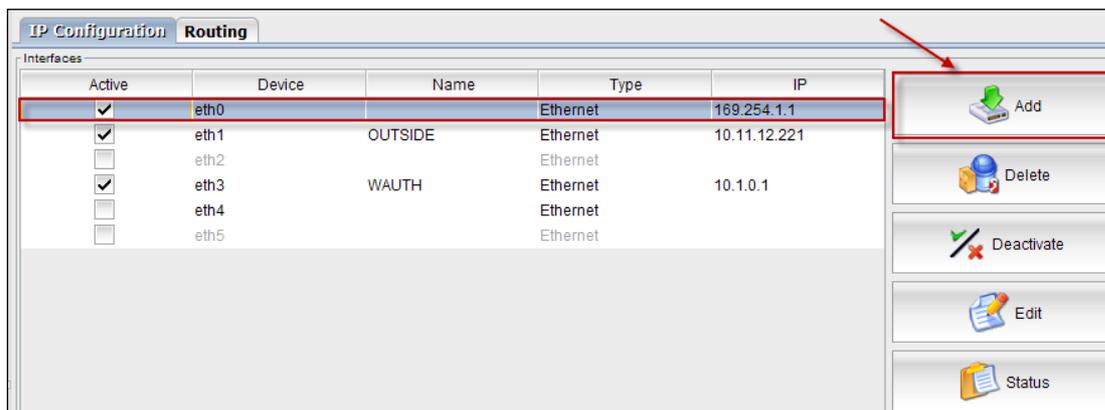
We can notice that the Interface is added in the Interfaces list with **Bridge** type of connection.



Activation process is in progress.



Click on **Add** button to add an interface.



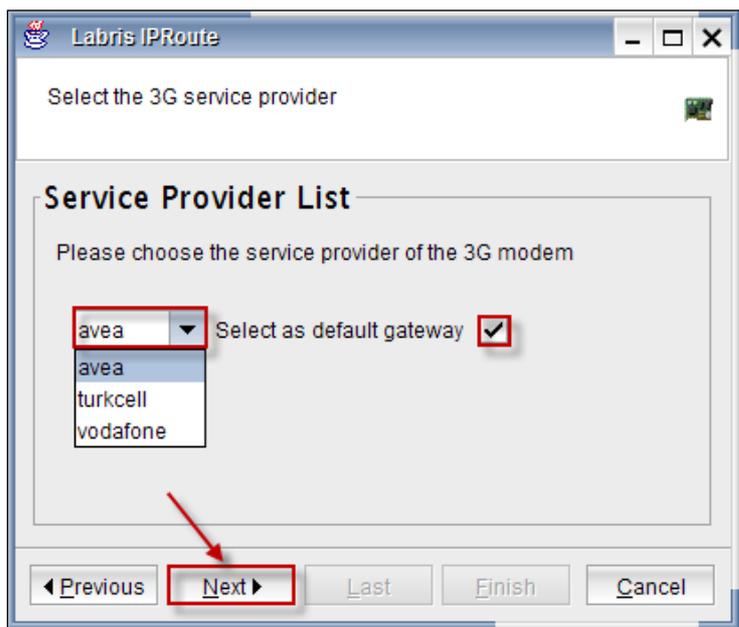
3G (Add, Edit, Delete, Status, Enable/disable)

To configure 3G connection for the Interface

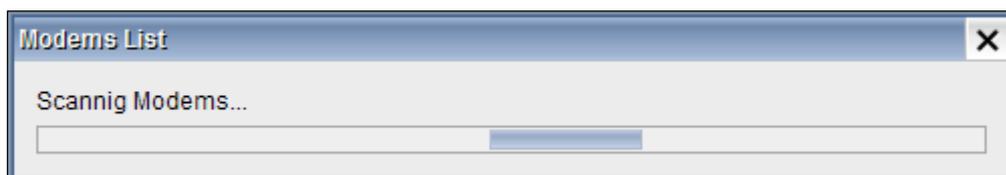
Select **3G** button from the types of connection.



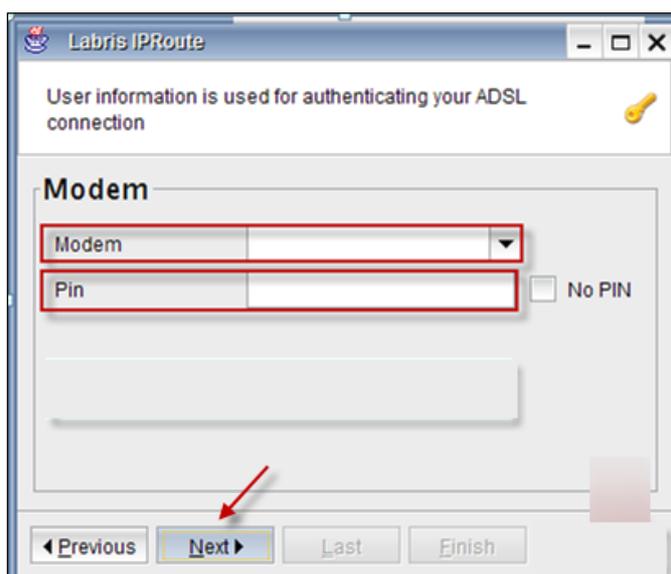
Choose the service provider of the 3G modem from the drop down list, check the default gateway.



Scanning of 3G Modems process is in progress.



Then the below screen appears stating that, User information is used for authentication. Choose the **“Modem”** from the drop down list and enter the **“pin”** of the modem and click on **“Next”** to proceed further.



Note – Since we don't have connection to the 3G modem, in the below screen message is displayed as "There is no plugged modem on the Labris device Please check your modem". Click on Cancel tab.



3G Release Note;

1 Configuration of old generation 3G Modem

- Plug the modem into the USB port on the device.
- Labris Management Console is opened and accessed to the system with an authorized user name and password.
- By clicking on the add button on the right in the IP Configuration tab from the Network Settings Module the Labris Interface Wizard opens.
- The forward button is clicked by selecting the 3G on the opened screen.
- The service provider is selected on the next screen, and in case the added 3G shall be used as the default gateway the related box is selected and clicked on next button.
- In the next screen are the 3G modems listed on the modem line. The appropriate modem is selected and , if available, the pin entered, if no pin available then the" no pin" box is selected and clicked on the next button.
- On the next screen are the features of the configured modem listed, the PPP interface is created

by clicking on the next button.

- By clicking on end button on the next screen the interface wizard is closed.
- The created PPP interface is listed under interfaces.
- The related PPP interface is selected and enabled with the help of the "Activate" button on the right or right-clicking on the interface. Activation may last up to 1-2 minutes..
- The type, IP address, connection status, referrals status, signal status will be shown on the enabled interface.
- In case the added modem shall not be used as the default gateway and will be used as additional line it has to be saved as an additional line. For this, it can be added as a line by clicking on the advanced button on the Network Settings> Routing screen.
- The permission rule of the created interface is added to the firewall general policy.
- According to the usage status of the created interface in the firewall NAT policy the NAT rule is added and the modem is made available to use.

2. Configuration of new generation 3G modem

- The modem is plugged into the USB port on the device.
- The Labris Management Console is opened and accessed to the system with an authorized user name and password.
- Network settings module is opened. The new generation of devices plugged on the device is seen as ether interface. The latest added interface on the interface list is the interface of the modem.
- The IP address of the modem is usually example:192.168.1.1 or 192.168.2.1. We can give the IP address of the modem interface on the device in the same subnet with the modem interface by clicking on create on the right side, for example:192.168.1.2 or 192.168.2.2
- If the modem is selected as the default gateway the IP address of the modem is entered by selecting the related interface in the pre-defined network gateway from the Network Settings> Routing section and saved with the button in the bottom right.
- In case the added modem shall not be used as the default gateway and will be used as additional line it has to be saved as an additional line. For this, it can be added as a line by clicking on the advanced button on the Network Settings> Routing screen.
- The permission rule of the created interface is added to the firewall general policy.
- According to the usage status of the created interface in the firewall NAT policy the NAT rule is added and the modem is made available to use.

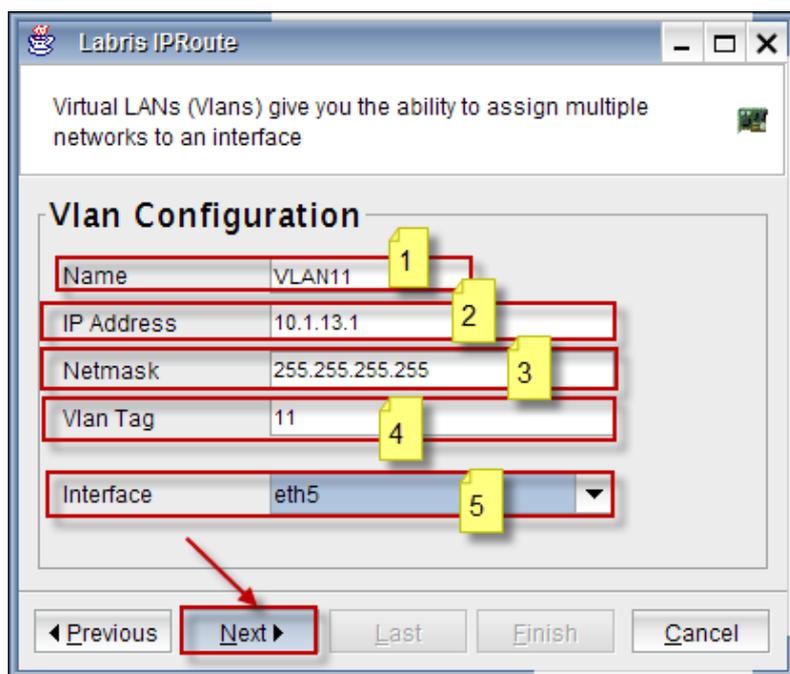
Vlan (Add , Edit, Delete, Status , Enable/disable)

To configure VLAN for the Interface.

Select **VLAN button** from the types of connection.



Configuration of VLAN



These are inputs for configuration of **VLAN**

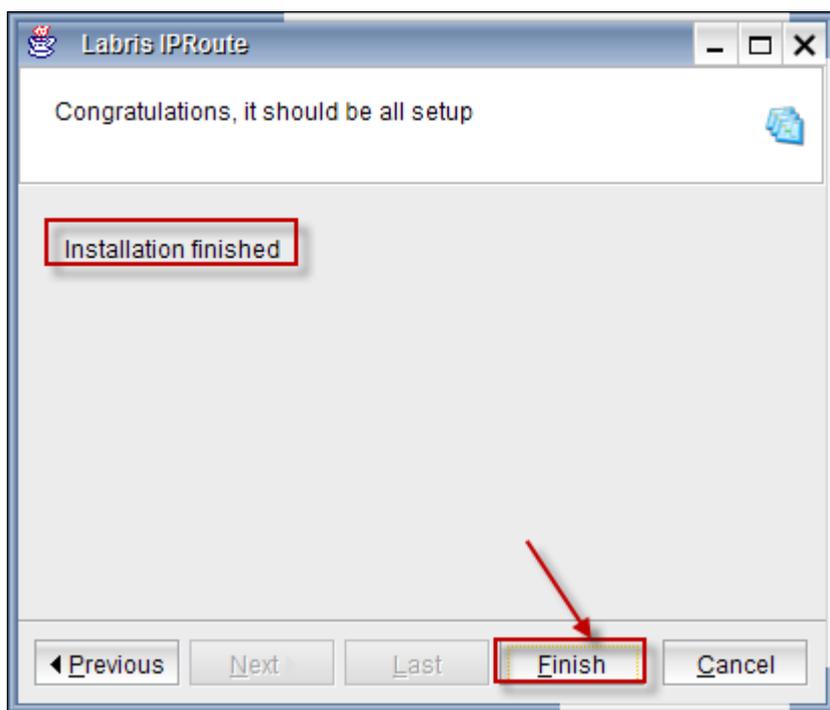
1	Name	Type the Name
2	IP Address	Give the IP Address
3	Netmask	Give the Netmask of the IP Address
4	Vlan Tag	Give the Tag of the Vlan
5	Interface	Choose the Interface from the drop down list

Click on **Next** tab to continue

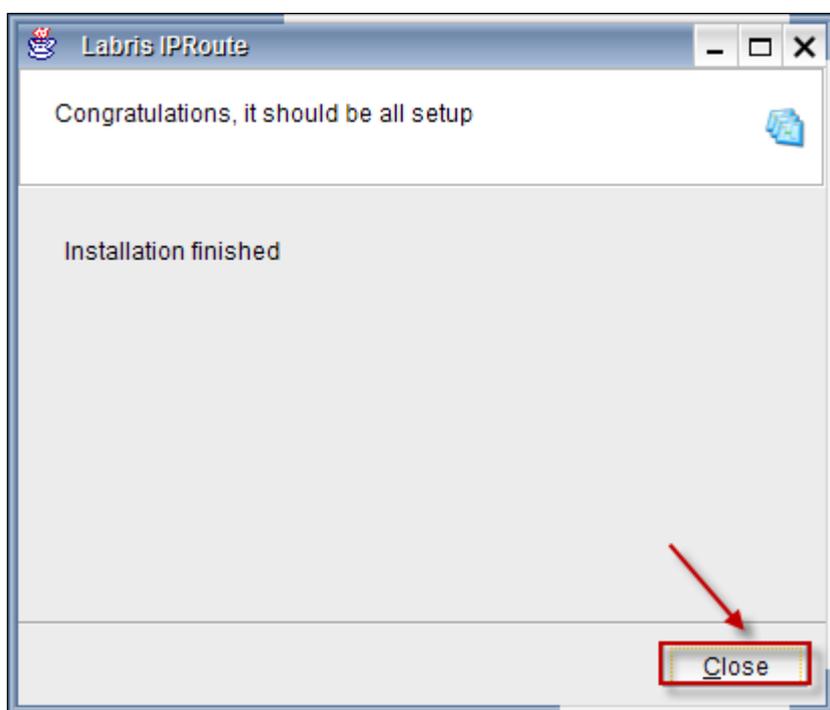
Interface Configuration process is in progress



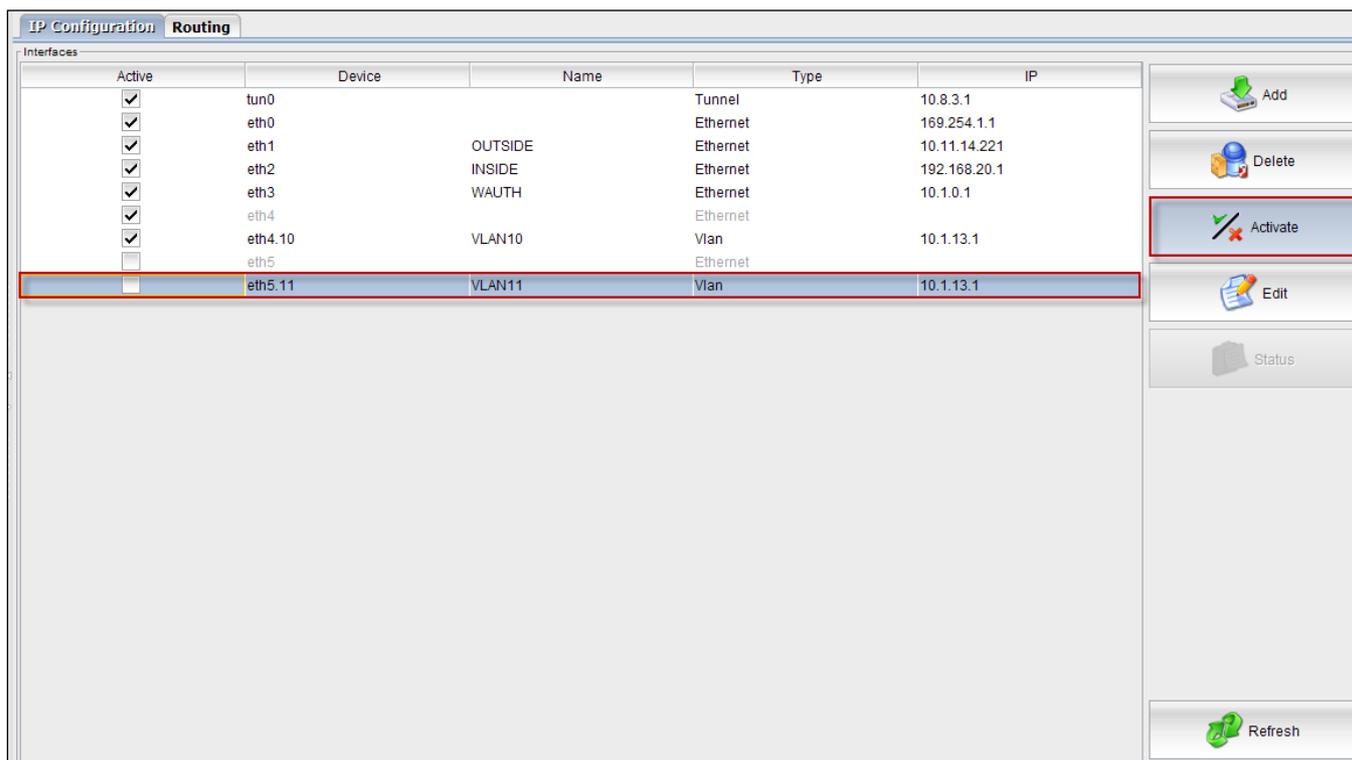
Installation finished click on **Finish** button.



Below screen appears, click on **close** button.



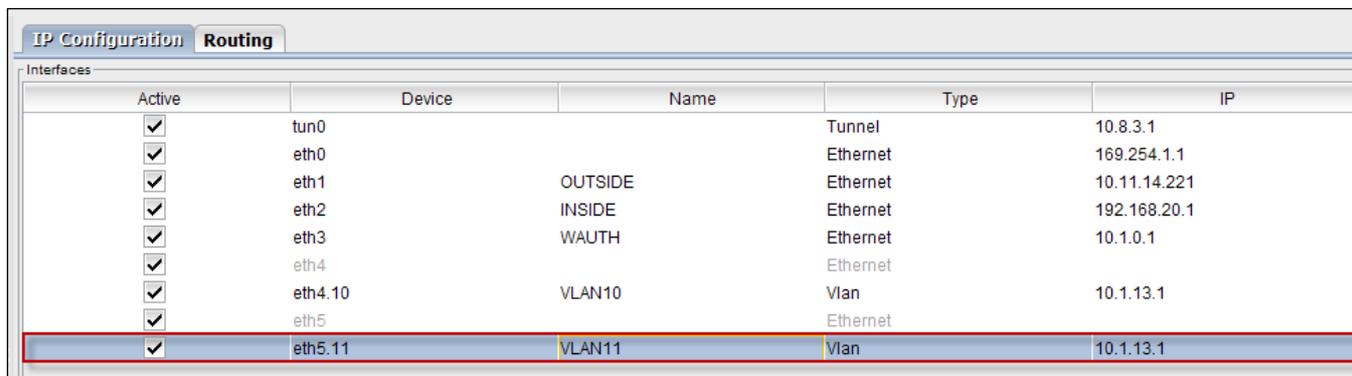
In the below screen we can notice Interface, click on Activate tab to activate the Interface.



Activation process is in progress.



We can notice Interface is Activated in the below screen.



41. Routes

In **Routing tab** the routing table of Labris Secure Gateway is displayed. In this table you can see the

Destination, Mask, Default Gateway, Interface and Metric properties of each route. Destination is the destination IP or network; mask defines the destination host or network's Netmask, default gateway is next way point of the package. Interface is the interface which will be used for routing operation.

Destination	Mask	Default Gateway	Interface	Metric
10.1.0.0	255.255.255.0	0.0.0.0	WAUTH (eth3)	0
10.8.3.0	255.255.255.0	0.0.0.0		0
10.11.12.0	255.255.255.0	0.0.0.0	OUTSIDE (eth1)	0
169.254.0.0	255.255.0.0	0.0.0.0	eth0	0

Advanced Add Delete

Default Gateway
Gateway: 10.11.12.1
Interface: OUTSIDE (eth1)

Load Balancing Disabled Enable

Save Refresh

Default Gateway

The Default gateway is the default next hop for every packet, when there is no explicitly specified gateway for destination of that packet. In order to change the default gateway firstly enter an IP address of the default gateway and choose an interface from which Packets are sent to the gateway.

Default Gateway
Gateway: 10.11.12.1
Interface: OUTSIDE (eth1)
eth0
OUTSIDE (eth1)
WAUTH (eth3)

Load Balancing Disabled Enable

Static Route

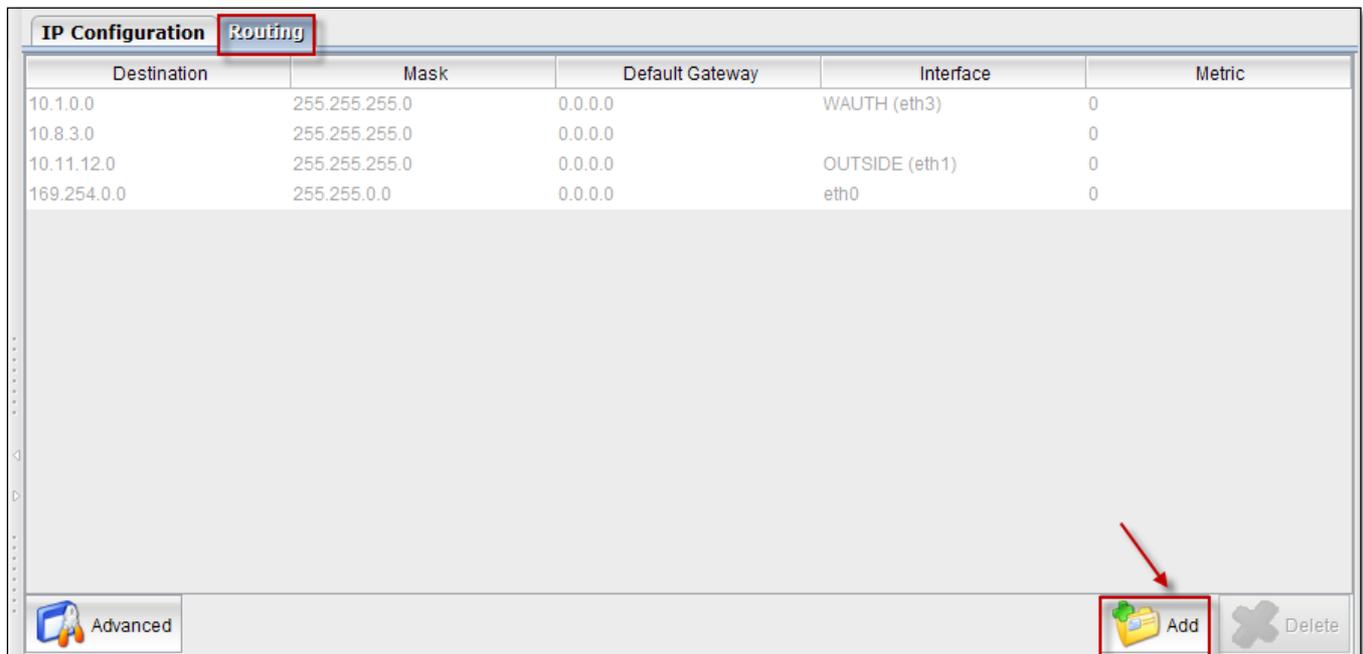
A static route is a manually configured mapping of an IP address to a next-hop destination.

A static route causes packets to be forwarded to a different next hop other than the configured default gateway. By specifying through which interface/gateway the packet will leave and to which device the packet should be routed, static routes control the traffic exiting Labris UTM.

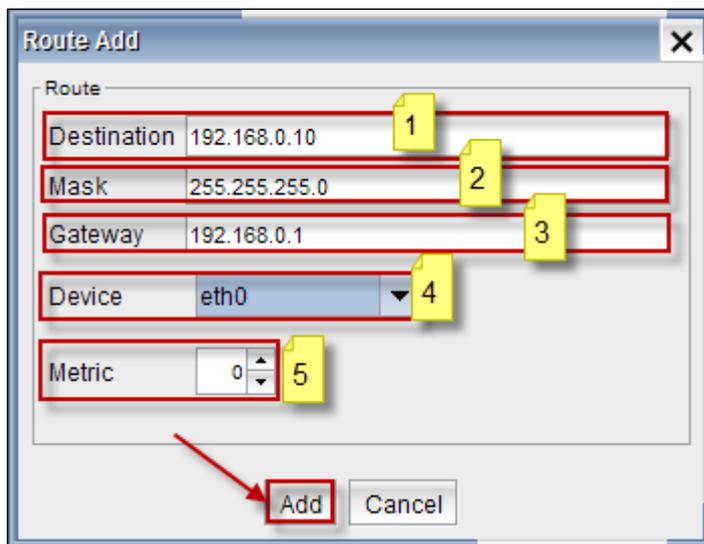
Add (Static Route)

Add static routes when you want to route traffic destined for specific network/host via a different next hope instead of a default route.

Click on **Add** button to add static route.



Below screen appears.



These are the inputs to **Add** route

1	Destination	Give the Destination IP Address
2	Mask	Give the Netmask of the Destination IP Address
3	Gateway	Give the Gateway IP Address
4	Device	Choose Device from drop down list
5	Metric	Choose Metric value

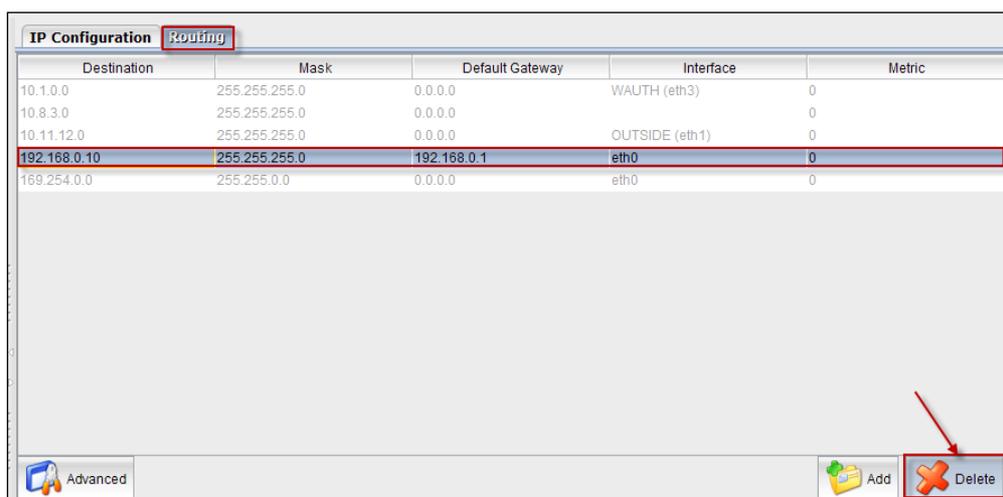
Click on **Add** button.

We can notice **Static route** in the Routing list.

Destination	Mask	Default Gateway	Interface	Metric
10.1.0.0	255.255.255.0	0.0.0.0	WAUTH (eth3)	0
10.8.3.0	255.255.255.0	0.0.0.0		0
10.11.12.0	255.255.255.0	0.0.0.0	OUTSIDE (eth1)	0
192.168.0.10	255.255.255.0	192.168.0.1	eth0	0
169.254.0.0	255.255.0.0	0.0.0.0	eth0	0

Delete (Static Route)

Select the Static Route from the list and click on **Delete** button, to delete Static route.



Load Balance (OLD)

Load Balance (NEW)

42. Load Balance

-----BEGIN NEW STUFF-----

Load balance module allows administrators to create Policy Based Rules using links and/or link groups. PBR allows administrators to write advanced route rules. User, group, ip based rules can be written to specific destinations over chosen links or link groups. Also for network stability administrators can add backup links and link groups. To load balance traffic between links administrators can create link groups.

MAIN SCREEN

The screenshot displays the Labris Management Console interface. The main window title is "Labris Management Console" and it includes a menu bar with "Device", "File", "Edit", "View", and "About". The "Link/Load Balance/PBR" tab is selected, showing the following configuration:

Links and Link Groups

Buttons: Add Link (3), Add Link Group (4), Edit (5), Delete (6)

Name (4)	Gateway (6)	Interface	Reachable	Router (7)
GROUPS				
labris_group				
eth3	10.101.0.201	eth3	✓	✓
eth1	10.100.0.201	eth1	✓	✓
LINKS				
eth3	10.101.0.201	eth3	✓	✓
eth1	10.100.0.201	eth1	✓	✓

Policy Based Routing

Buttons: Add (9), Edit (10), Delete (11)

Id (9)	Source (11)	Destination	Link	Backup
1	allier@u20	0.0.0.0/0	eth3 (link)	
2	0.0.0.0/0	0.0.0.0/0	labris_group (link_group)	
3	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	eth3 (link)	

Service Status: Running (13) | Start (14) | Stop (15) | Restart (16) | Save (17) | Refresh (18)

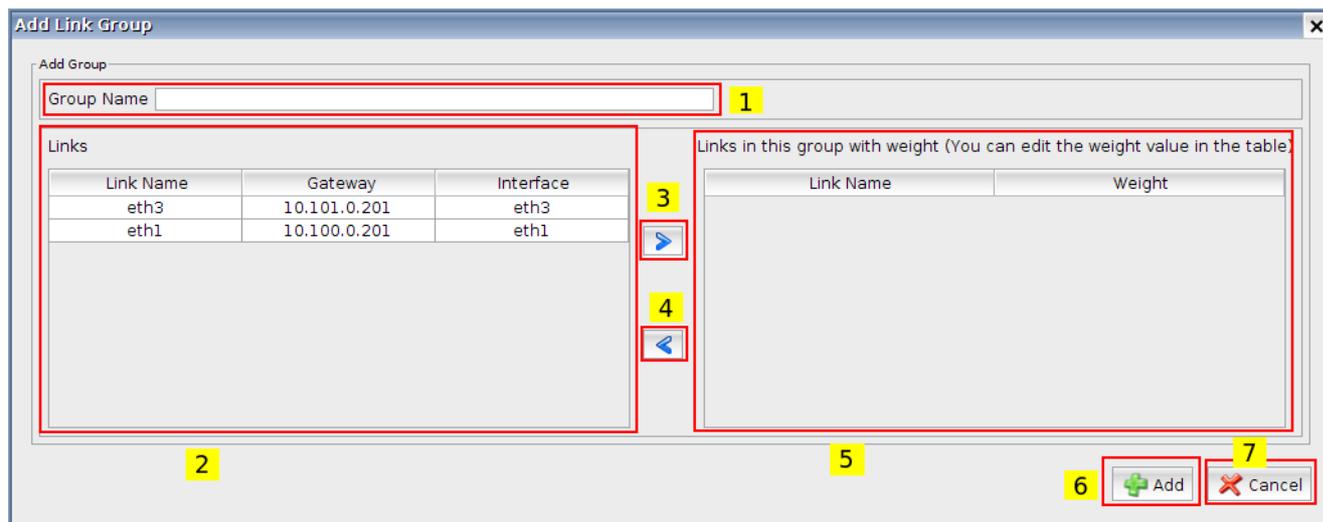
Bottom status bar: Lmc server address you are connected to is: 192.168.0.58

No	Name	Description
1	Link and Link Groups	Manage all links and link groups
2	Policy Based Routing	Manage all policy based routing rules (PBR)
3	Add Link	Create a new link to use in a link group or in a PBR.
4	Add Link Group	Create a new link group to use in a PBR.
5	Edit Link/Link Group	Edit an existing link or link group.
6	Delete Link/Link Group	Delete an existing link or link group.
7	Link Groups	Link groups section.
8	Links	Links section.
9	Add PBR	Create a new policy based routing rule.
10	Edit PBR	Edit an existing policy based routing rule.
11	Delete PBR	Delete an existing policy based routing rule.
12	Default Route	Default gateway written in Route tab is automatically written as last rule of PBR.
13	Load Balance Service Status	Service status. PBR rules only work when service status is "Running".
14	Start Service	Start service.
15	Stop Service	Stop service.
16	Restart Service	Restart service.
17	Save Changes	Save changes.
18	Refresh Screen	Refresh everything in the screen.

Add Link Screen

No	Name	Description
1	Link Name	Name of the new link.
2	Gateway	Gateway IP address of new link.
3	Interface	Interface of new link.
4	Ping Address Input	Use this field to add a new ping ip address.
5	Add Ping Address	Add the value in Ping Address Input.
6	Edit Ping Address	Edit selected ping address.
7	Delete Ping Address	Delete selected ping address
8	Ping Addresses	Show all ping addresses. To edit/delete, select one.
9	Add Link	Save new link
10	Cancel	Cancel.

Add Link Group Screen



No	Name	Description
1	Group Name	Name of the new link group.
2	All Links	Available links for adding to this link group.
3	Add link to group	Add selected link to link group (left -> right)
4	Remove link from group	Remove selected link from group. (left <- right)
5	Links in this group	Selected links in this link group.
6	Create Link Group	Create this link group.
7	Cancel	Cancel.

Network traffic going through link group is load balanced between links in the link group according to links' weights. Also links in a link group are failovered, network traffic is not redirected to down links.

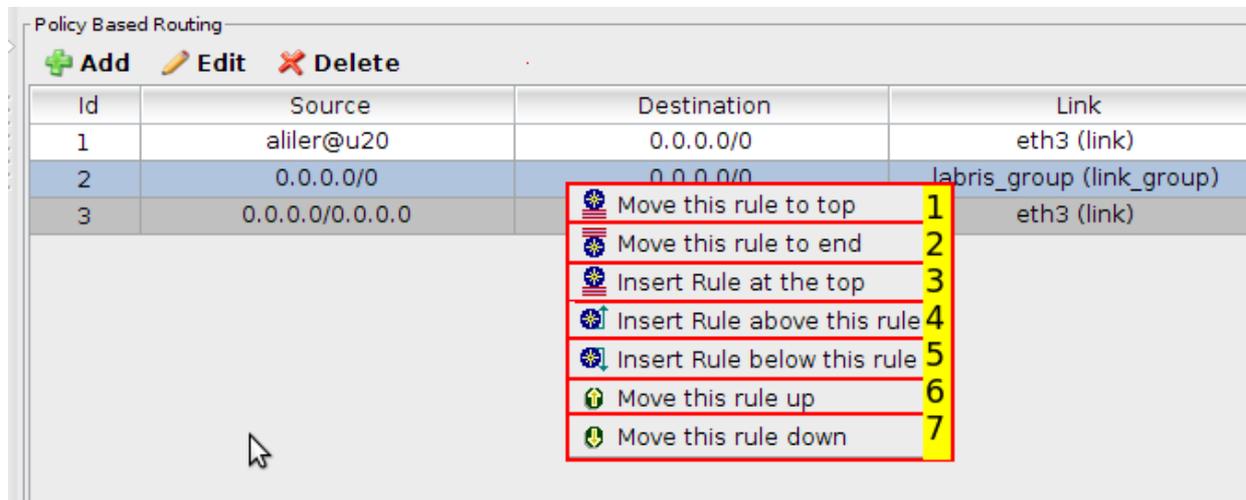
Add Policy Based Route Screen

The screenshot shows a dialog box titled "Add Policy Based Route" with a close button (X) in the top right corner. The dialog is divided into three main sections: Sources, Destinations, and Link and Link Backup. The Sources section contains a table with columns "Source" and "Type", and buttons for "Add IP or Network", "Add Users or Groups", and "Delete". The Destinations section contains a table with columns "Destination" and "Type", and buttons for "Add IP or Network", "Add Users or Groups", and "Delete". The Link and Link Backup section contains two dropdown menus: "Link / Link Group" and "Link / Link Group Backup". At the bottom of the dialog are "Add" and "Cancel" buttons.

No	Name	Description
1	Sources	Sources for this policy based routing rule.(PBR)
2	Destinations	Destinations for this policy based routing rule.
3	Link and Link Backup	Link and link backup choice for this PBR.
4	Add IP or Network	Add a new IP or network to this PBR. Examples: 192.168.0.5, 192.168.0.0/24, 10.0.20.0/255.0.255.0
5	Add Users or Groups	Add User or Group
6	Delete	Delete selected IP/Network/User/Group.
7	Link/Link Group	Configure link choice for this PBR.
8	Backup Link / Backup Link Group	Enable/Disable backup link choice for this PBR.
9	Add Policy Based Route	Save changes.
10	Cancel	Cancel.

Backup links/link groups are activated if main link is down or if all links in the main link group are down. Backup links/link groups are active until main link is up or one of links in main link group's is up again.

Policy Based Route Right Click



No	Name	Description
1	Move to top	Move selected rule to the top.
2	Move to end	Move selected rule to the end.
3	Insert at top	Insert a rule at top.
4	Insert above	Insert a rule above the selected rule.
5	Insert below	
6	Move up	
7	Move down	

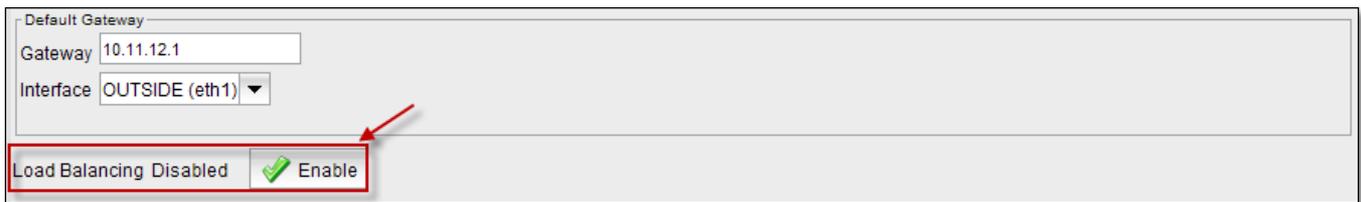
-----END NEW STUFF-----

-----BEGIN OLD STUFF-----

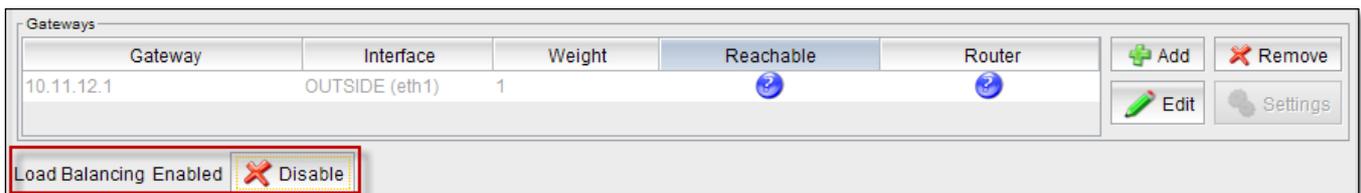
Load balance can be configured based on following types

- Configuring a virtual web server with three real web servers
- Adding a server load balance port forwarding virtual IP
- Weighted load balancing configuration
- HTTP and HTTPS persistence configuration
- Packet load balance or destination load balance

By default **Load Balance** is in disable mode, click on **Enable** button.

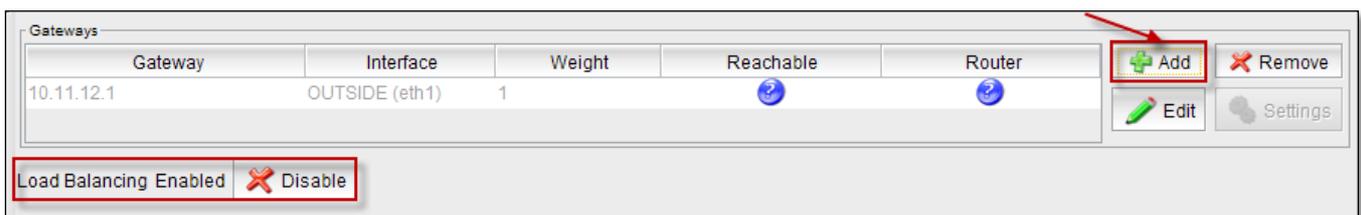


When Load Balance is enabled Gateways section with the fields **Gateway, Interface, Weight, Reachable, Router** are seen

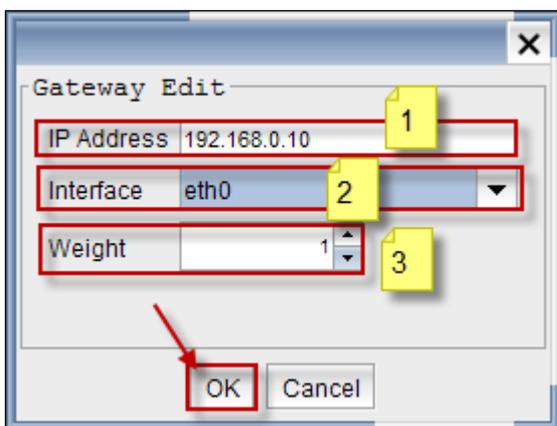


Add (Load Balance Route)

Click on **Add** tab to add Gateway



Below screen appears

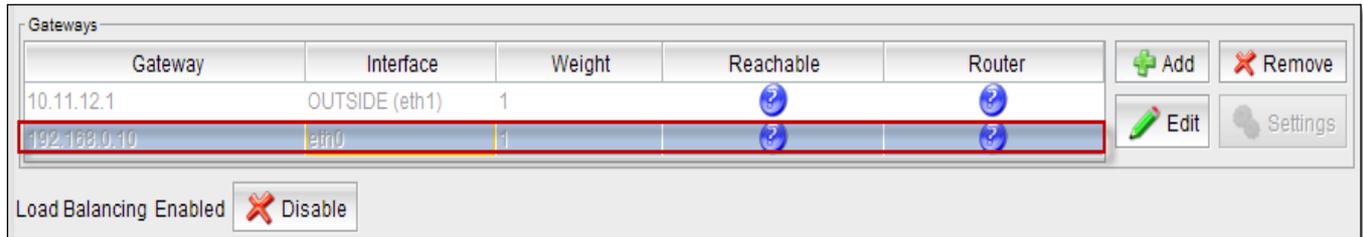


These are the inputs to add Gateway.

1	IP Address	Type IP Address
2	Interface	Choose the Interface from the drop down list
3	Weight	Choose Weight value

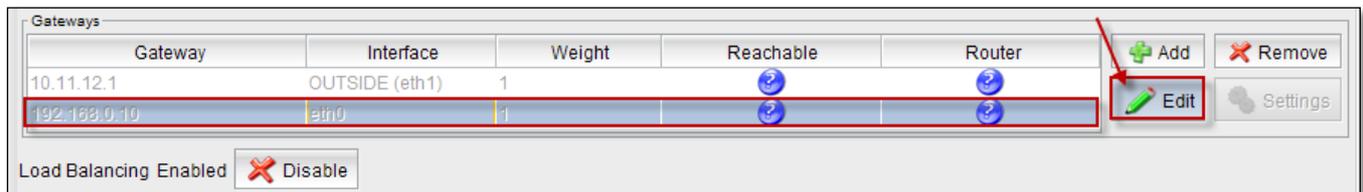
Click **Ok** to add Gateway

We can notice Gateway added in the below screen

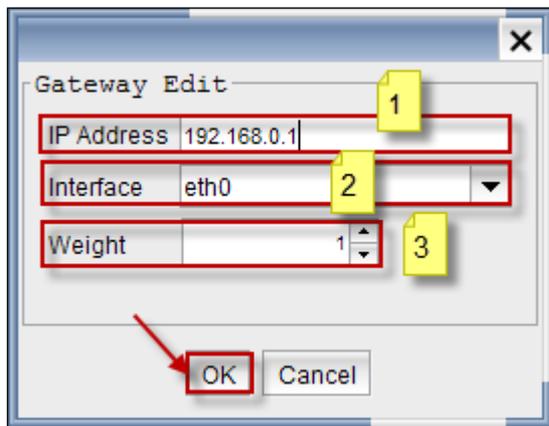


Edit (Load Balance Route)

Select the Gateway and click on **Edit** tab to Edit the Gateway



Below screen appears



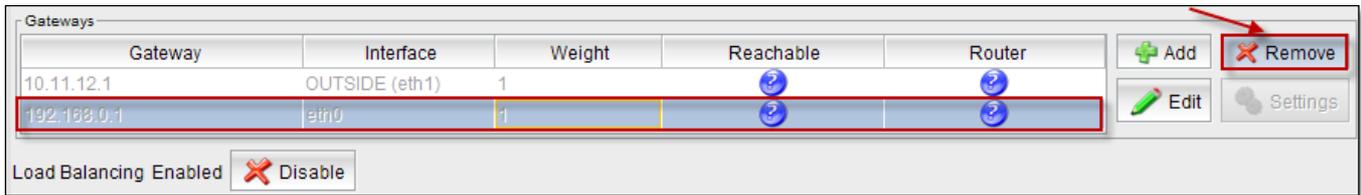
These are the inputs to edit gateway

1	IP Address	We can Edit the existing IP Address
2	Interface	We can Edit Interface (Optional)
3	Weight	We can Edit Weight value (Optional)

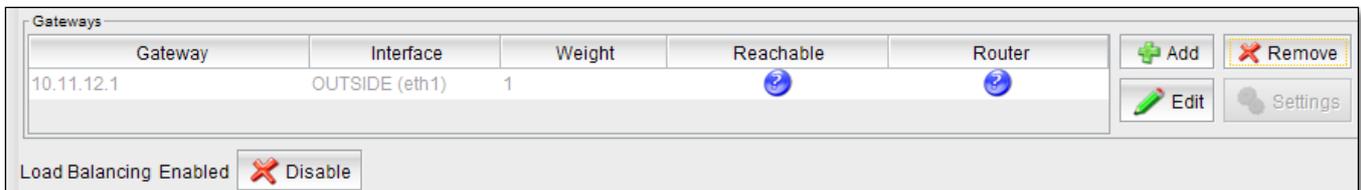
Click **Ok** to apply changes

Delete (Load Balance Route)

Select the **Gateway** and click on **Remove tab** to remove gateway

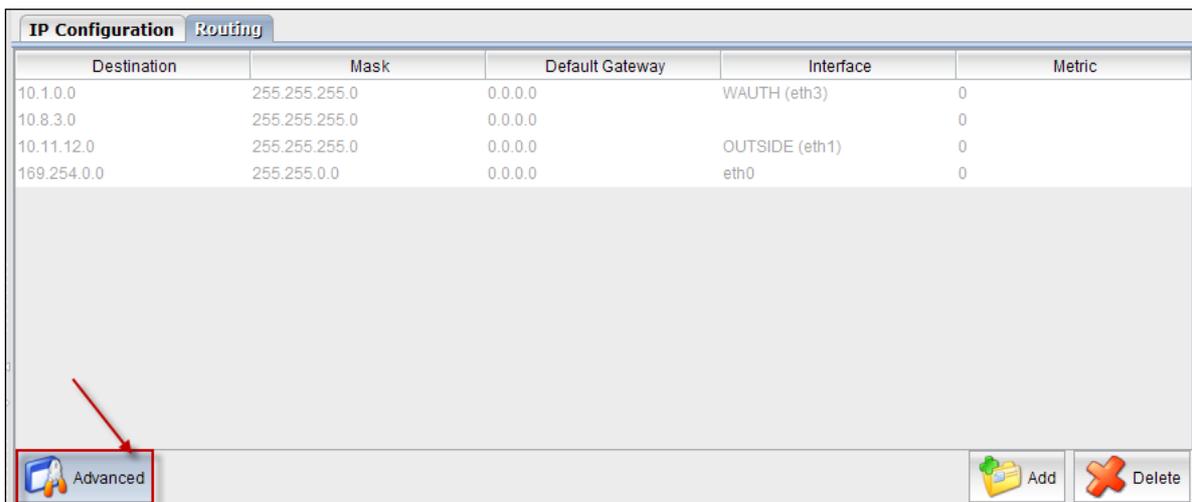


We can notice **Gateway** removed from the list in the below screen

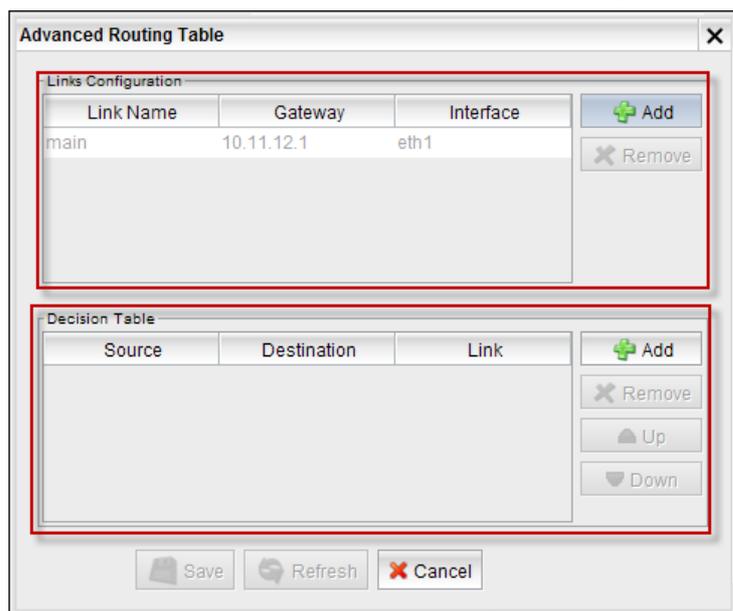


43. Advanced/ Policy Based Routing

Click on **Advanced Tab**



There are two sections in the Advanced Routing table:

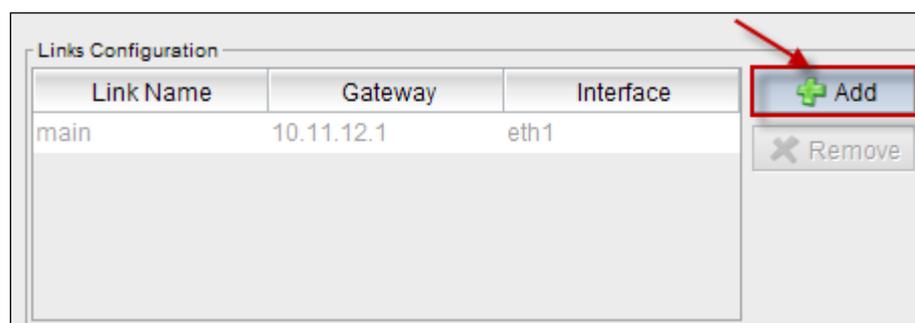


Upper section is for link configuration and the other one is for decision configuration. A Link is a virtual “link” for packets to a specific interface and a gateway. By defining decisions, one can redirect a package to a link based on the package's source and destination IP or network addresses.

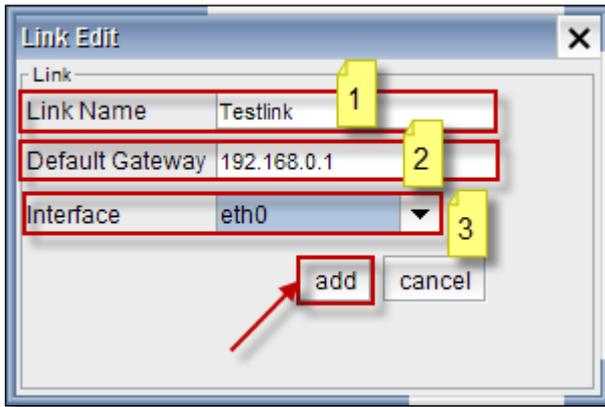
Link Configuration

A Link is represented by a name, a default gateway and an interface.

To create an Interface, click on **Add** button in the Link Configuration table.



Below screen appears to create a **New Gateway**

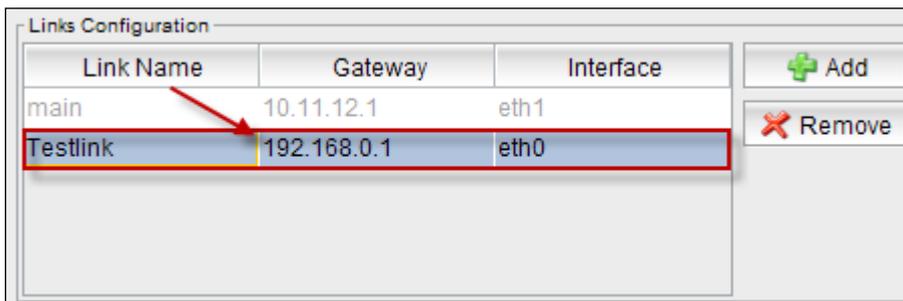


These are the inputs to add Link

1	Link Name	Type the Name of the Link
2	Default Gateway	Give the Default Gateway
3	Interface	Choose the Interface from the drop down list

Click on **Add** tab

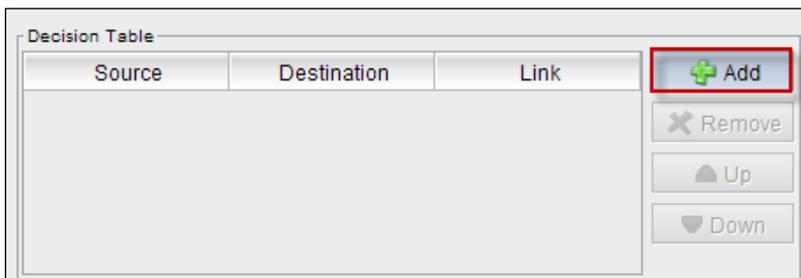
We can notice New **Link** added in the Link Configuration in the below screen



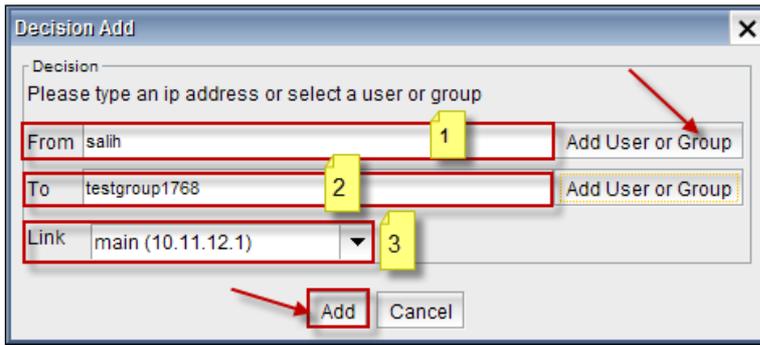
Decision Table

A Decision is represented by source IP/network, destination IP/network and the link name to which the packages are redirected.

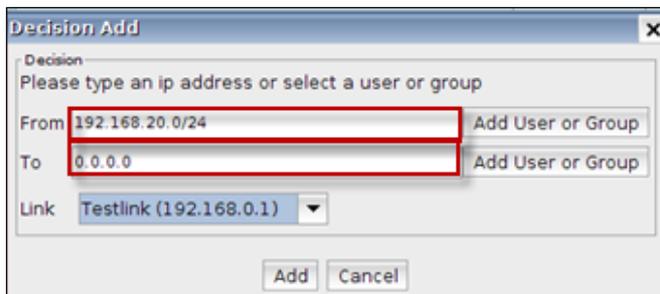
To add new decision, click on **Add** tab



Below screen appears



(OR)



These are the inputs to add **Decision**

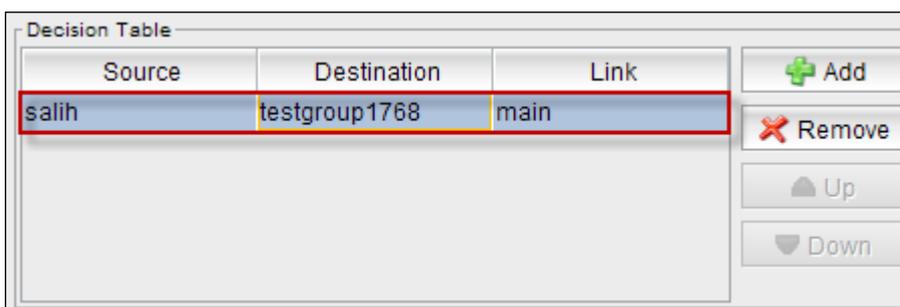
1	From	Click on Add User or Group and browse User or Group as Source or we can give the IP address
2	To	Click on Add User or Group and browse User or Group as Destination or provide the IP address
3	Link	Choose Link from the drop down list

Click on **Add** tab

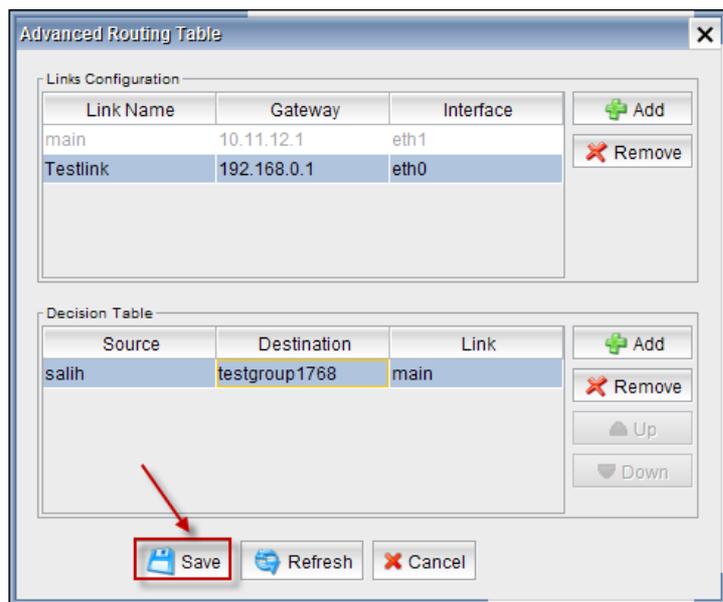
Note

- Source IP can also be mentioned in the **From tab** instead of browsing User or Group.
- Destination IP can also be mentioned in the **To tab** instead of browsing User or Group

We can notice **Decision** added in the **Decision table** in the below screen

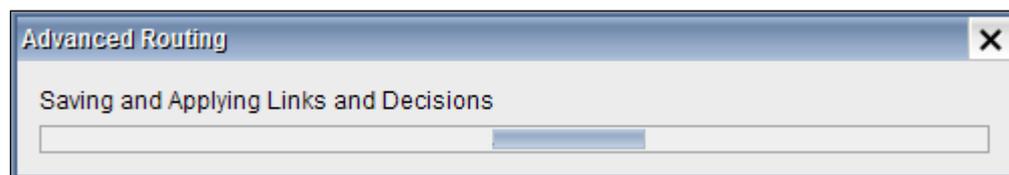


Click on **Save** button to save newly added **Link** and **Decision** to the **Advanced Routing Table**.

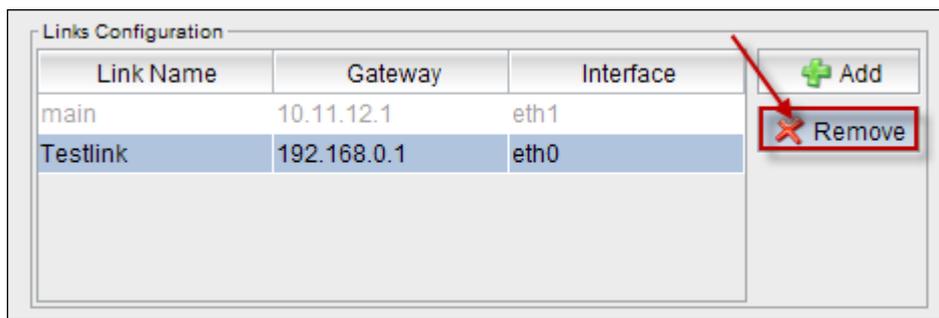


1	Save	It enables us to Save changes made to the Advanced Routing Table
2	Refresh	It enables us to Refresh Advanced Routing Table
3	Cancel	It enables us to Cancel and close the tab

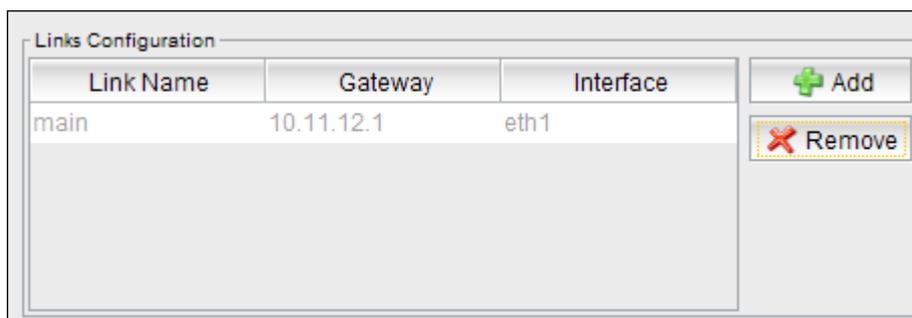
Saving and Applying Links and Decisions is in progress.



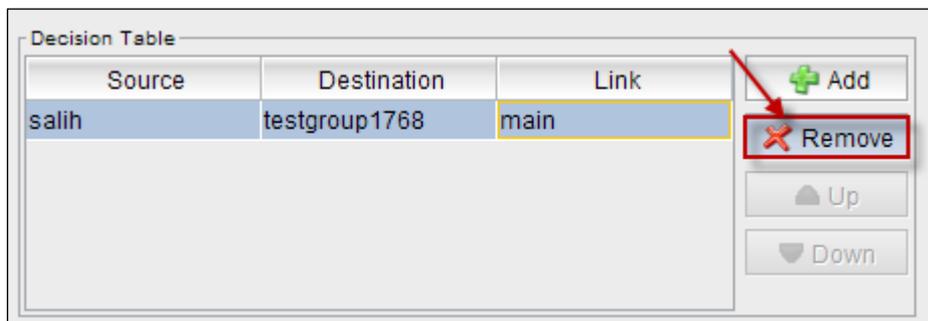
Select the **Link** and click on **Remove** tab to remove **Link** from **Link Configuration**.



We can notice **Link** is removed from the **Link Configuration**.



Select the Decision and click on **Remove** tab to remove Decision from the Decision table.



Click on **Save** tab to save the changes made to the **Routing**.

Click on **Refresh** tab to refresh **Routing**.

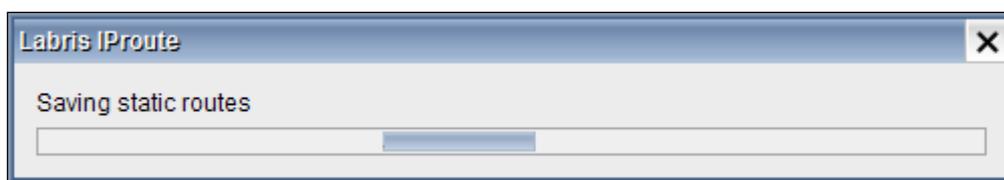
Destination	Mask	Default Gateway	Interface	Metric
10.1.0.0	255.255.255.0	0.0.0.0	WAUTH (eth3)	0
10.8.3.0	255.255.255.0	0.0.0.0		0
10.11.12.0	255.255.255.0	0.0.0.0	OUTSIDE (eth1)	0
169.254.0.0	255.255.0.0	0.0.0.0	eth0	0

Gateway	Interface	Weight	Reachable	Router
10.11.12.1	OUTSIDE (eth1)	1		

Load Balancing Enabled Disable

Save Refresh

Saving process is in progress



WAN failover (WAN Backup)

By default load balance is disabled, Click on **enable tab**, to make Load balance Enable.

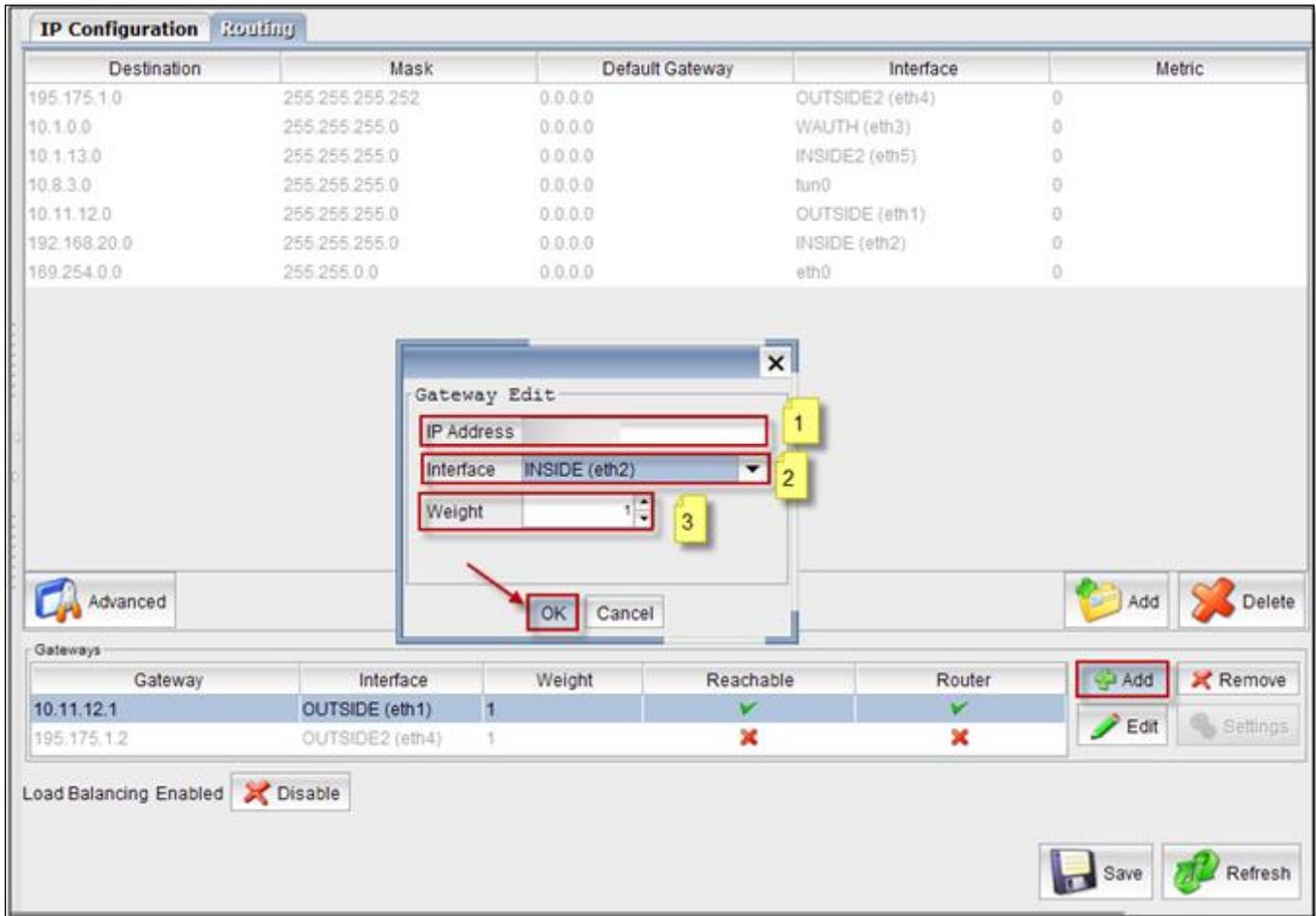
In the below screen we can notice **Load Balance Enabled**

Gateway	Interface	Weight	Reachable	Router
10.11.12.1	OUTSIDE (eth1)	1		
195.175.1.2	OUTSIDE2 (eth4)	1		

Load Balancing Enabled Disable

Save Refresh

Click on **Add** tab

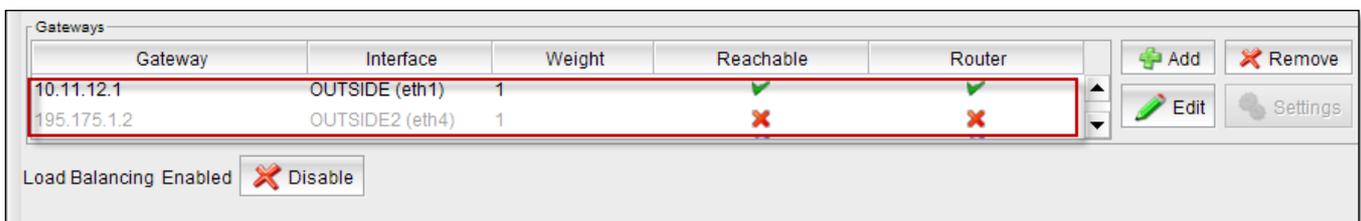


These are the inputs for the Gateway Edit.

1	IP Address	Type IP Address
2	Interface	Choose Interface from the drop down list
3	Weight	Select Weight. Weight of the distribution ratio between each of the two represents default gateway.

Click on **Ok** tab.

We can notice one interface in active mode.



WAN Failover using CLI

When more than one internet line is used for active-passive in-line redundancy then in that case truncation of the preferred line is the second line, in the second line of the first line again when auto and auto disable.

This process is carried out via the CLI.

These are the following command lines.

Information

WAN1 IP Address:10.10.10.2/30

WAN1 Gateway: 10.10.10.1

WAN2 IP Address:20.20.20.2/30

WAN2 Getaway: 20.20.20.1

LAN IP Address: 192.168.168.0/24

DMZ IP Address: 10.0.0.0/24

WAN Failover Configuration

Step 1:

The configuration file patch

NOTE: Open CLI and Open conf file for editing using the below command

```
vim /opt/labris/etc/sysconfig/labris-trigger.conf
```

The following is the configuration file, you can use your own network ip addresses contained in the update according to the requirement.

#It's starting

```
#NOTE : Default GW for WAN1 (Active)  
route1 = "10.10.10.1"
```

#NOTE : WAN1 up Interface

```
route1.iface = "eth1"
```

#NOTE : WAN1 live checkup the line will make the control of the external environment, ip addresses.

```
route1.ping = "144.122.166.1 195.175.39.40"
```

#NOTE : WAN1 in the absence of the line to the following line in this line.

```
route1.action.NOT_ROUTER = "\  
echo ---METRO ETHERNET1DOWN--- | logger \  
route del default gw10.10.10.1 \  
\
```

#NOTE : Add a new route for backup link WAN2

```
route add default gw20.20.20.1 \  
\
```

#NOTE: Users are added to the Internet through a NAT policy to WAN2. The IP address of the LAN. If more than one of the same row is copied only ip addresses are changed.

```
iptables -t nat -I POSTROUTING -o eth2 -s 192.168.168.0/24 -j SNAT --to-source 20.20.20.2 \  
iptables -t nat -I POSTROUTING -o eth2 -s 10.0.0.0/24 -j SNAT --to-source 20.20.20.2 \  
\
```

#NOTE : updates the settings for the web filter

```
/etc/init.d/labris-webfilter reload \  
\
```

```
echo "---SNAT changed to METROETHERNET1" | logger"
```

#NOTE: Check the status of the line would last WAN1 3 second

```
route1.action.ROUTER = " \  
echo ---METRO ETHERNET 1 UP--- | logger \  
\
```

#NOTE :If the WAN1 WAN2 to stand up for the route will be deleted.

```
route del default gw20.20.20.1 \  
\
```

#NOTE :WAN1 to route again.

```
routeadd default gw10.10.10.1 \  
\
```

//NOTE: Delete old rule for WAN2

```
iptables -t nat -D POSTROUTING -o eth2 -s 192.168.168.0/24 -j SNAT --to-source 20.20.20.2\  
iptables -t nat -D POSTROUTING -o eth2 -s 10.0.0.0/24 -j SNAT --to-source 20.20.20.2\  
\
```

//NOTE: updates the settings for the web filter

```
/etc/init.d/labris-webfilter reload \  
\
```

```
echo "---SNAT changed to METRO ETHERNET1" | logger"

route2 = "20.20.20.1"

route2.iface = "eth2"

route2.ping = "144.122.166.1 195.175.39.40"

route2.action.UNREACHABLE = "echo ---METRO ETHERNET 2DOWN--- | logger"
route2.action.REACHABLE = "echo ---ADSLMODEMUP--- | logger"
route2.action.ROUTER = "echo ---ADSL-LINE-UP--- | logger"
route2.action.NOT_ROUTER = "echo ---ADSL-LINE-DOWN--- | logger"

/etc/init.d/labris-trigger restart

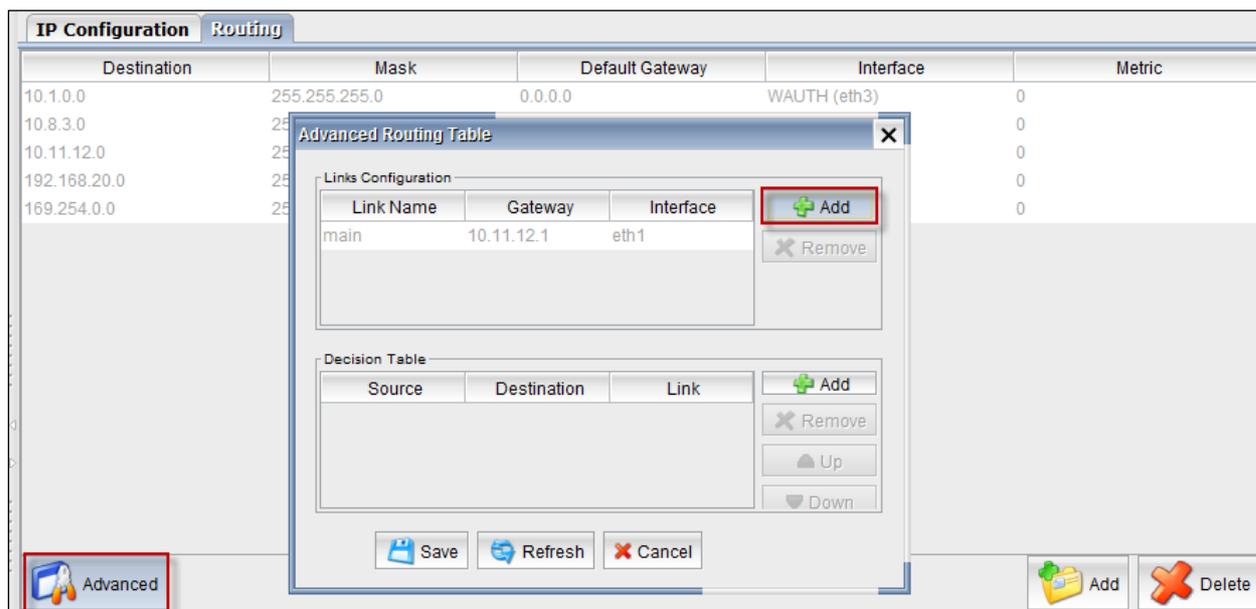
#It's finished
```

Step 2:

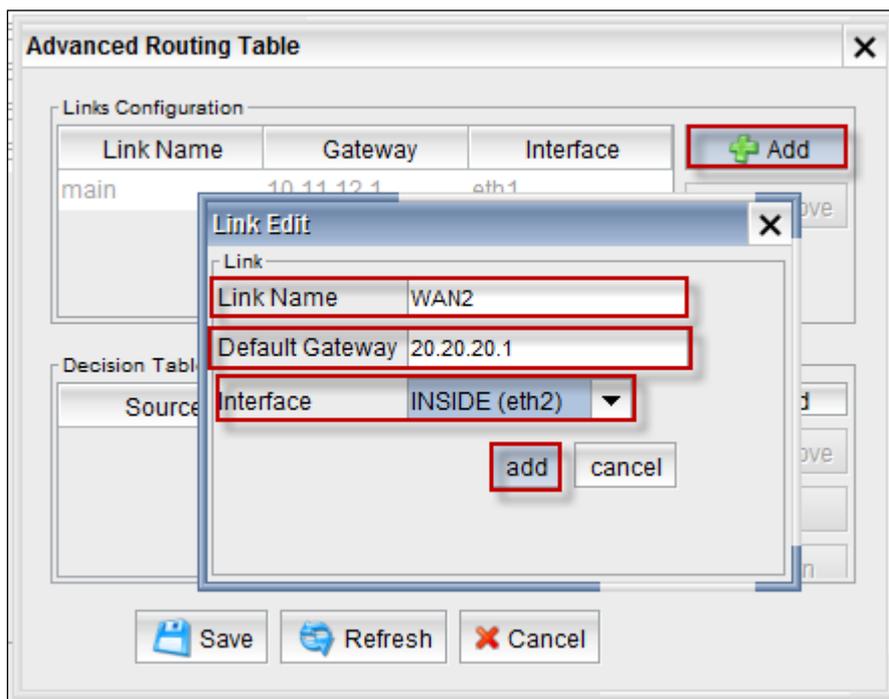
Add Advance routing on the new gateway for wan2.

Click on **Advanced** option under **Routing** in **Network Settings** tab.

Click on **Add** tab to add a link.

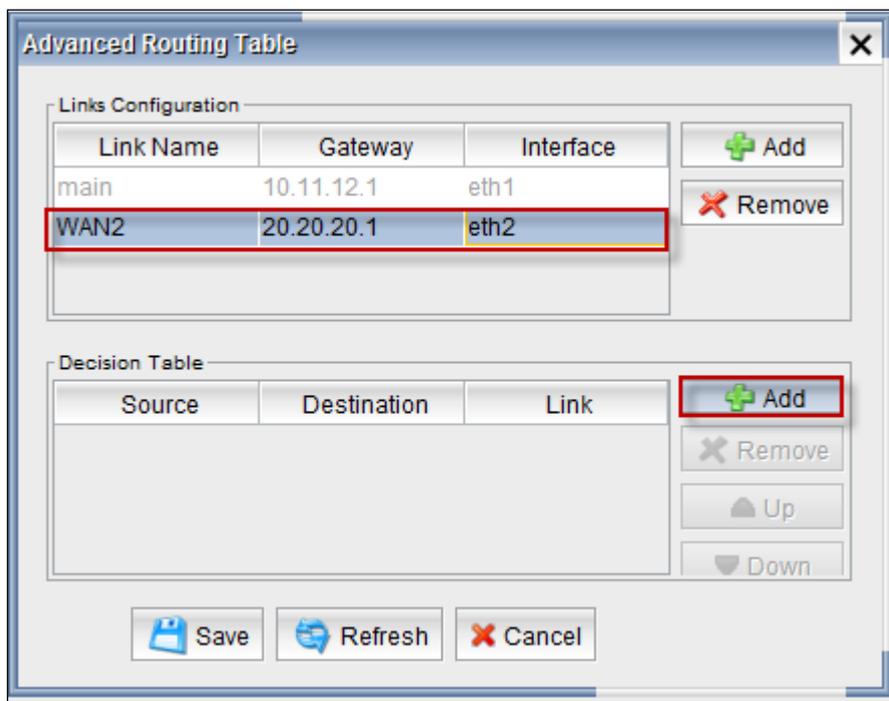


Give the **Link Name**, mention **Default Gateway** and choose **interface** from the drop down list and click on **Add** tab.



We can notice new Link added to the Link Configuration table.

Under Decision Table click on **Add** tab.

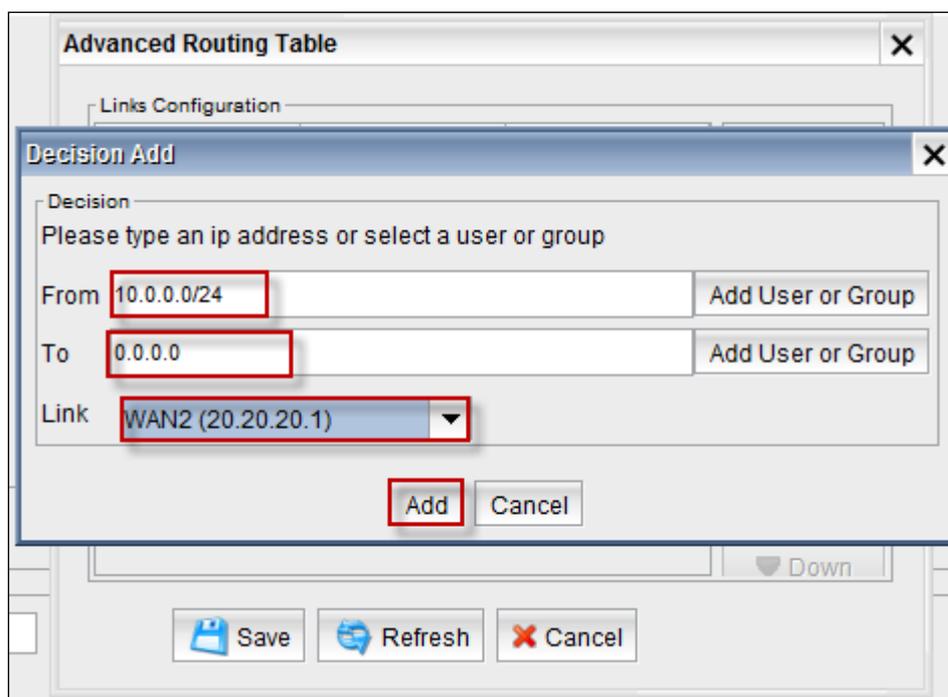


Step 3:

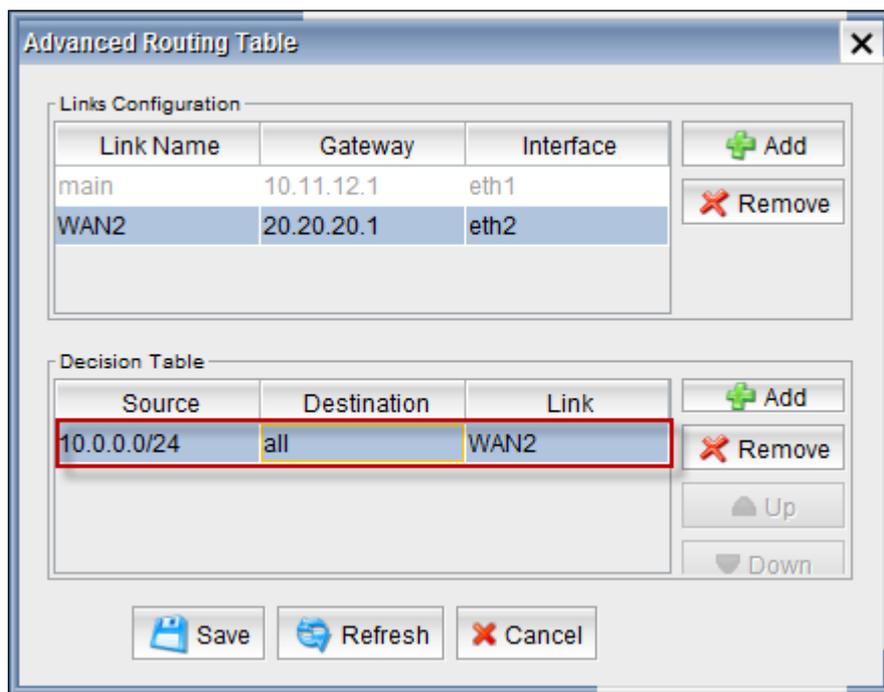
Add a source/policy base route on the decision table for DMZ and LAN network.

Mention **Source** and **Destination** IP address and choose Link from the drop down list.

Click on **Add** tab.



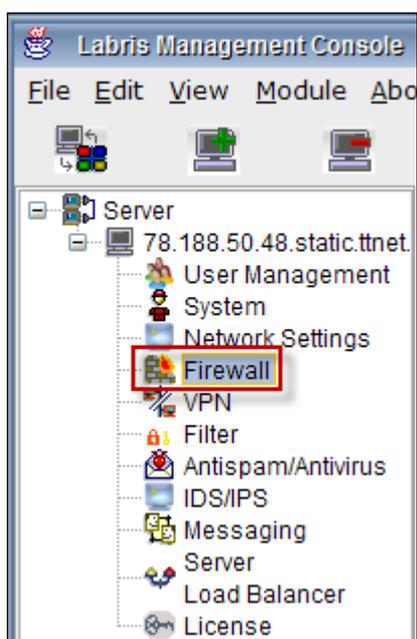
In the below screen, we can notice Decision added in the Decision table.



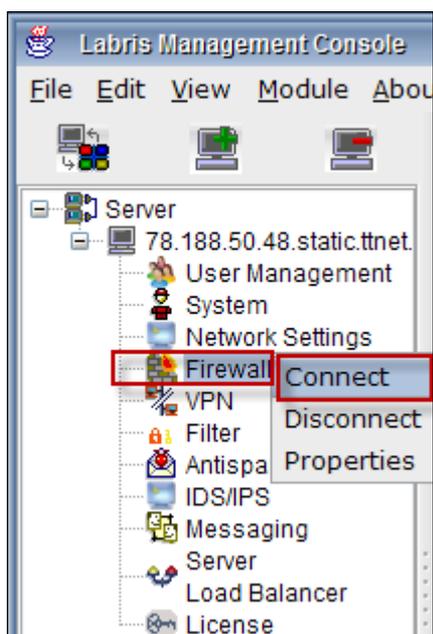
Firewall

Firewall is software which controls the traffic of incoming and outgoing by analyzing the data packets which is allowable or not in a network. It serves as a gate keeper between servers and outside of the world.

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet.



Right click on **Firewall** and select **Connect**.



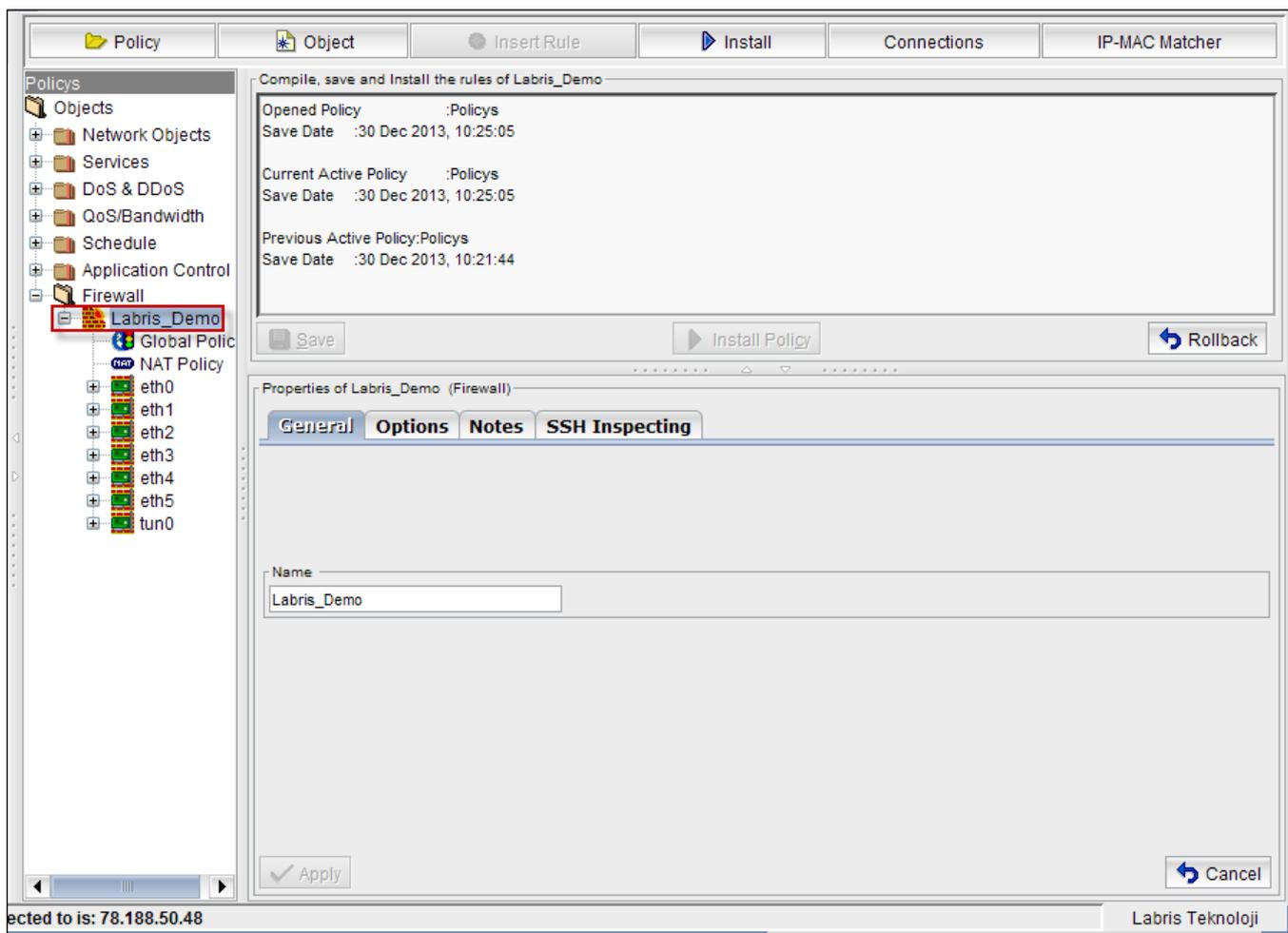
44. Make a new firewall object

A firewall is a rule that describes us what all the incoming connections that are accepted by which instances. Each firewall contains one rule, which specifies a permitted incoming connection request, defined by source, destination, ports, and protocol.

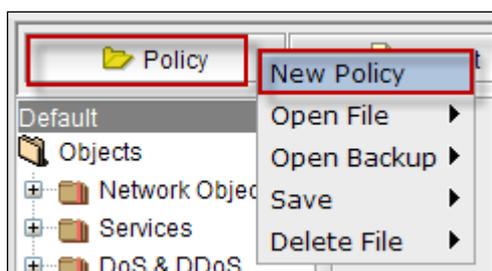
By default, all incoming traffic from outside a network is blocked and without an appropriate firewall rule, no packet is allowed into an instance. You need to set up firewalls to allow incoming network traffic to permit these connections. Each firewall represents a single rule that determines what traffic is permitted into the network. It is possible to have many firewall rules and to be as general or specific as we would like.

When we get connected to Firewall, below screen appears.

By default Labris Demo is displayed.



Right click on Policy, Select **New Policy**

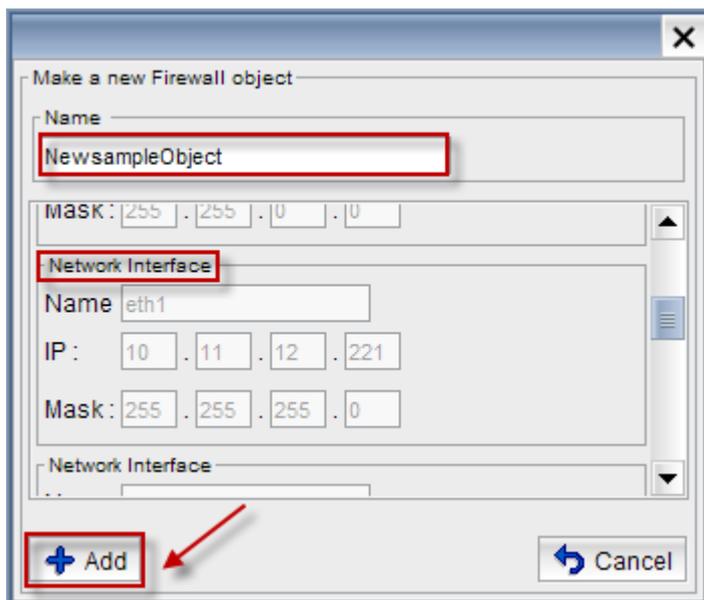


It consists of two fields, Name and Network Interfaces.

In the **Name tab**, name of the new firewall object should be mentioned.

Network Interfaces with **Name, IP , Mask** are selected by default.

Click on **Add** tab.



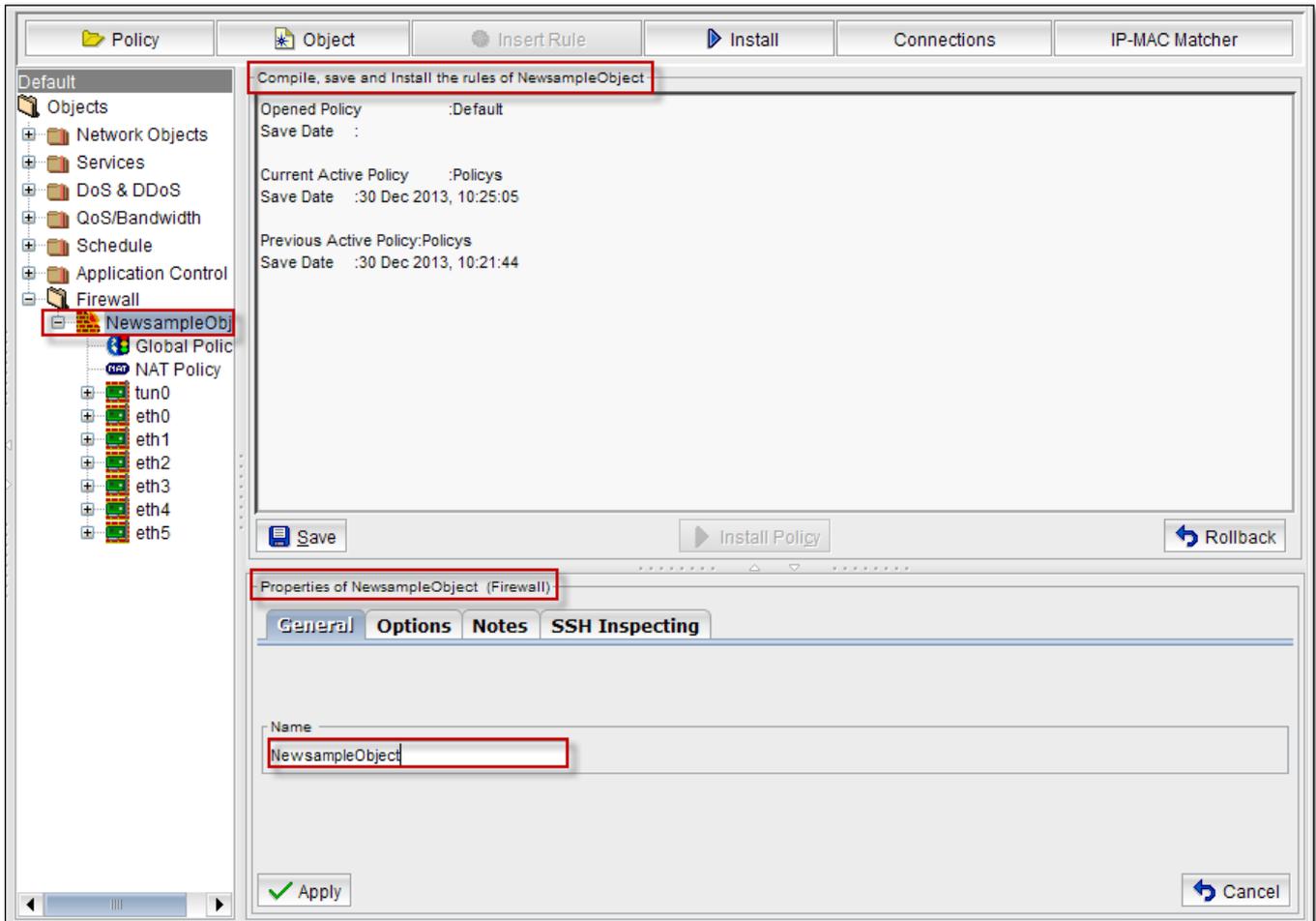
We can notice new firewall object under firewall.

It consists of two fields.

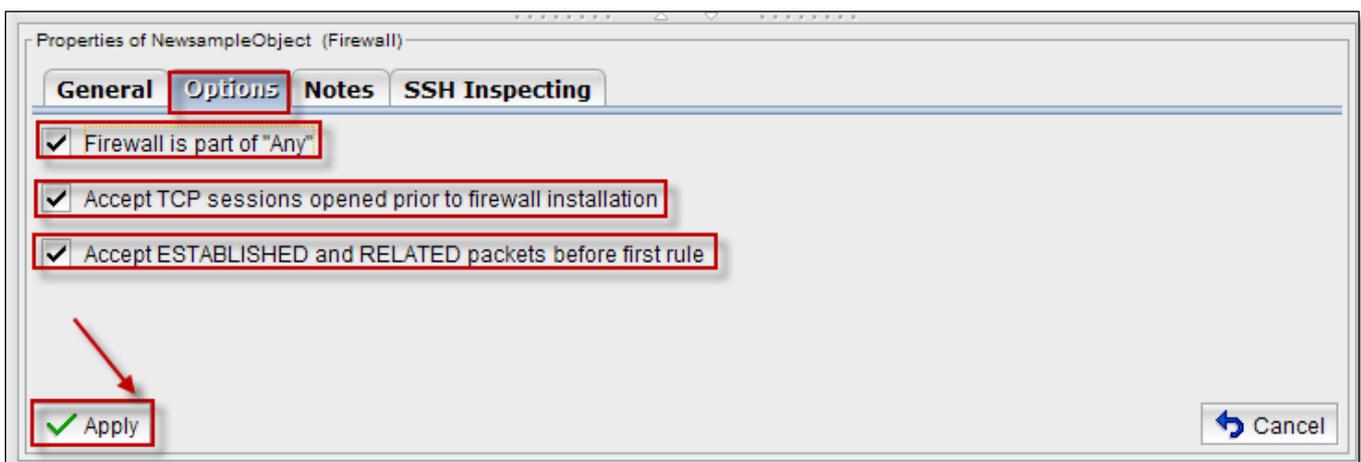
Compile, Save and Install the rules of new firewall object field displays information regarding newly added object to the firewall.

Properties of new firewall object displaying **General, Options, Notes, SSH Inspecting.**

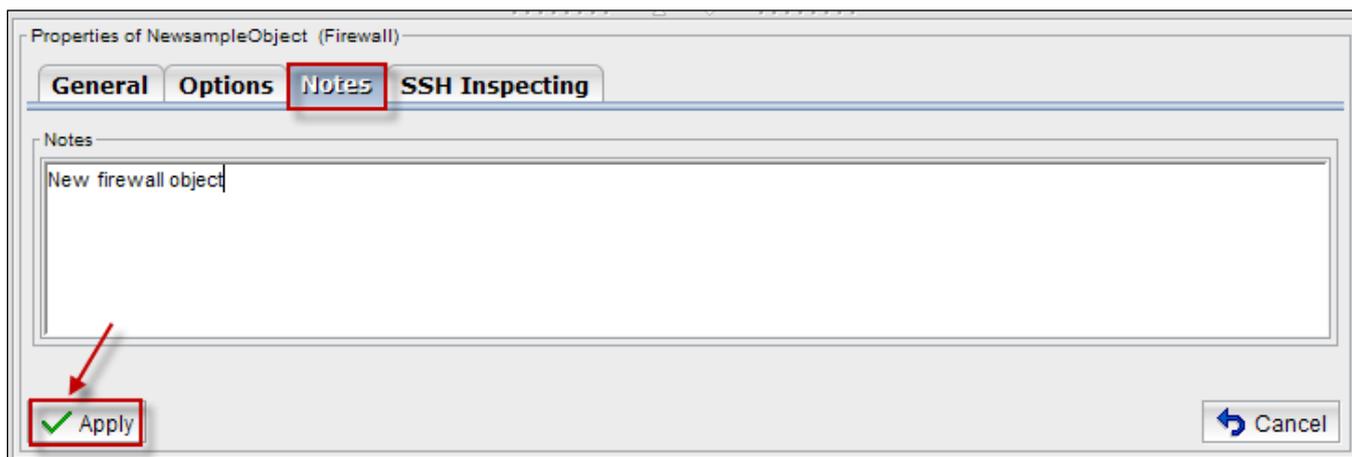
Under General tab, the name of the new firewall object is displayed



Under **Options tab**, we can checkmark options like **Firewall is part of "ANY"**, **Accept TCP sessions opened prior to firewall installation**, **Accept ESTABLISHED and RELATED packets before** and click on **Apply tab** to apply these rules to the firewall object.



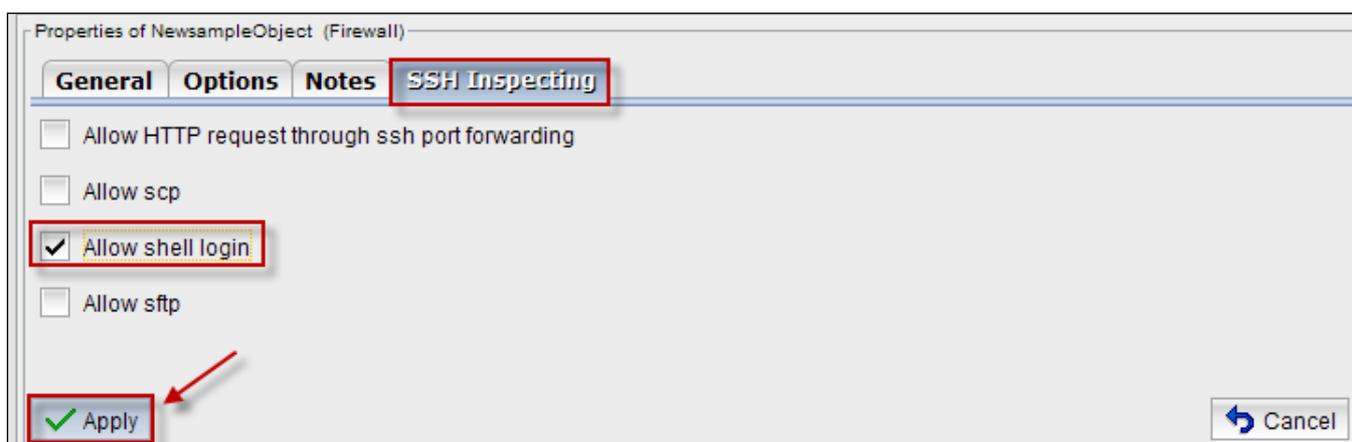
Under **Notes tab**, we can describe any points regarding new firewall Object and click on **Apply tab**.



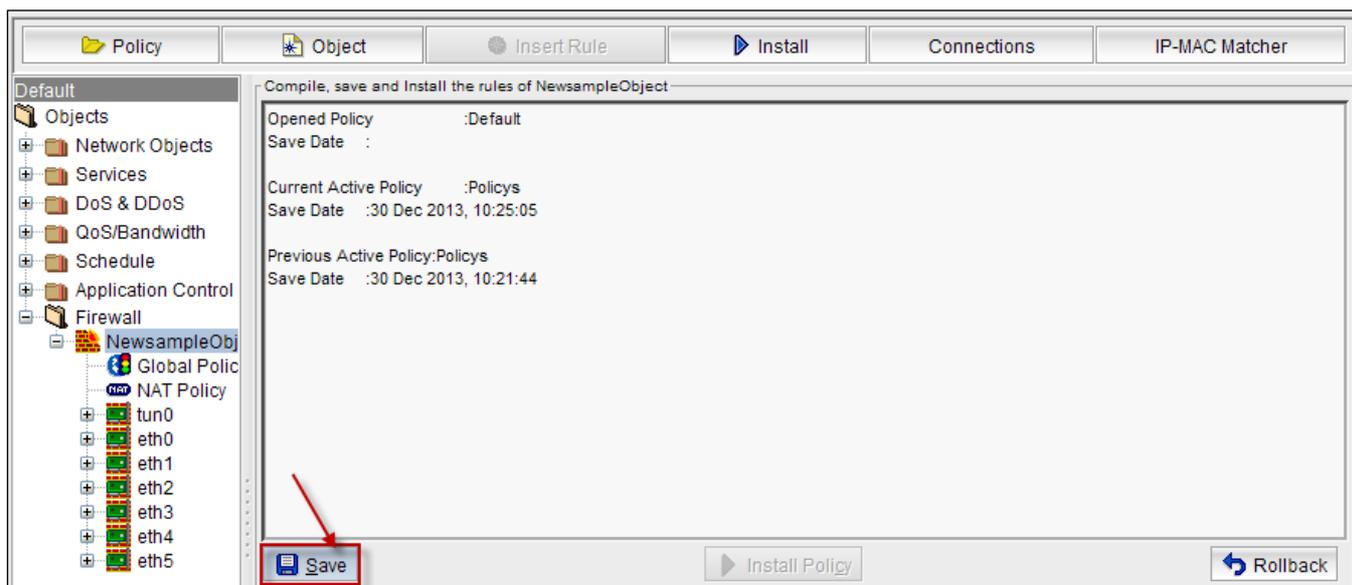
SSH inspecting

SSH inspecting is a unique security solution which enables both real-time inspection, and full replay of SSH, SFTP, Telnet, and RDP traffic and sessions to meet compliance, governance, auditing, and forensics requirements in enterprises and government entities.

In **SSH Inspecting tab**, we can check mark options like **Allow HTTP request through ssh port forwarding**, **Allow scp**, **Allow shell login**, **Allow sftp** and click on **Apply tab** to apply them to the firewall object.



Click on **Save** tab to save changes.



Input tab appears, Give the name of the **New file** (new firewall object name) and click on **Ok** to close the current tab.



Below screen appears stating that “**New sample Object have been saved successfully**” click **Ok** to close the current tab



45. Objects

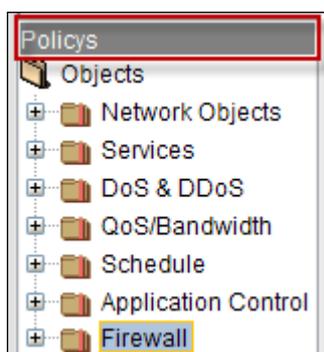
Firewall rules can be created in an object-oriented design. A firewall object is a named collection that represents specific networks, services, or connections. Using firewall objects gives you the following advantages:

- Each object has a unique name that is more easily referenced than an IP address or a network range.

- Maintenance of the firewall rules is simplified. When you update a firewall object, the change is automatically updated in every rule that uses the object.

The Firewall objects are a prime example of those building blocks. They are something that can be configured once and then used over and over again to build what you need. They can assist in making the administration of the LABRIS UTM unit easier and more intuitive as well as easier to change. By configuring these objects with their future use in mind as well as building in accurate descriptions the firewall will become almost self-documenting. That way, months later when a situation changes, you can take a look at a policy that needs to change and use a different firewall object to adapt to the new situation rather than build everything new from the ground up to accommodate the change.

Objects folder consists of **Network Objects, Services, Dos &DDoS, QoS/Bandwidth, Schedule, Application Control, Firewall.**

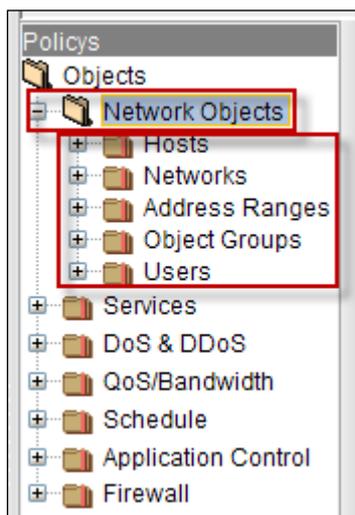


Network Objects

Network objects are used to categorize IP addresses into different types of network entities. These network entities are then used to represent sources and destinations in the access rules, publishing rules, cache rules, traffic chaining rules, and HTTP compression settings that make up your firewall policy.

Expand Network Objects.

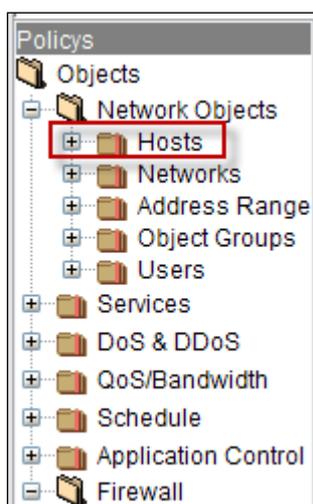
It consists of **Hosts, Networks, Address Ranges, Object Groups, Users.**



Brief Summary about each of the parameters in Network Objects:

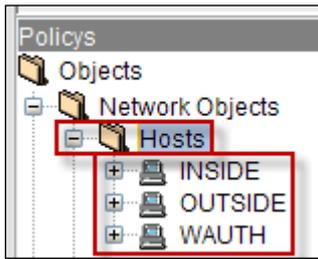
1	Hosts	It enables us to Add new Host
2	Networks	It enables us to Add new Networks
3	Address Ranges	It enables us to Create new Address Range
4	Objects Groups	It enables us to Add new Object Groups
5	Users	It enables us to Add new User Groups

Hosts

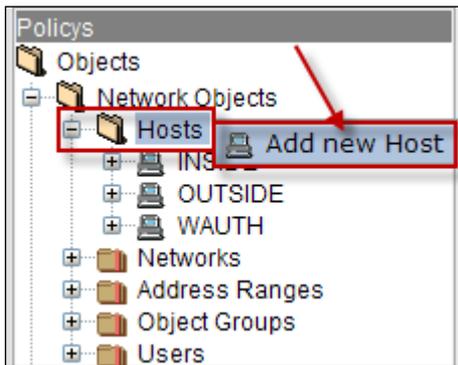


Expand Hosts, by default it consists of three Hosts.

They are **INSIDE, OUTSIDE, WAUTH**



Right click on **Hosts** to **Add new Host**.



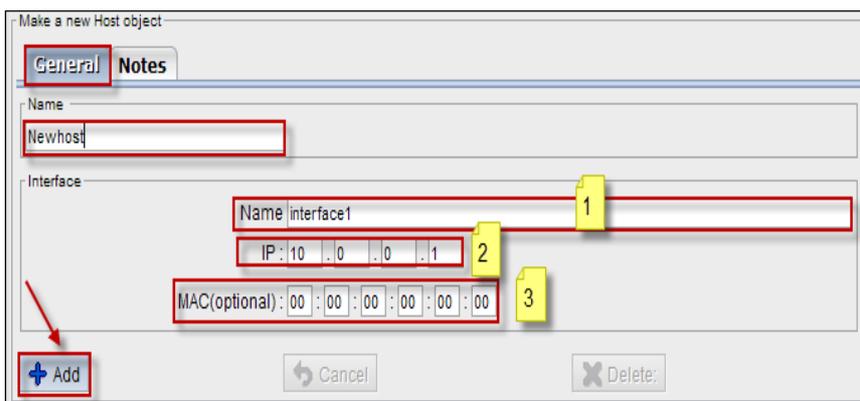
Below screen appears, Select **General tab**.

It consists of two fields, **Name** and **Interfaces**.

In the **Name tab**, name of the new Host Object should be mentioned.

These are the inputs for the Interfaces:

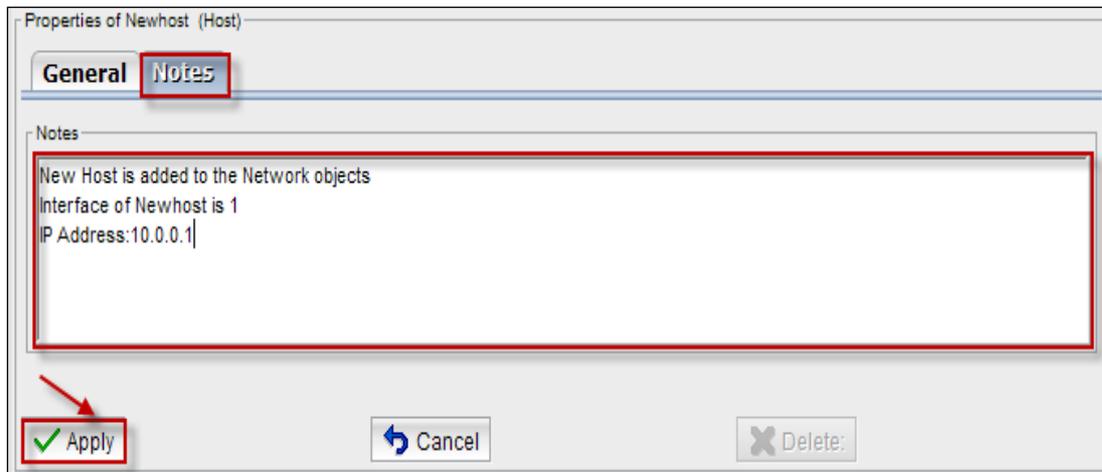
1	Name	Type the name of the Interface
2	IP	Give the IP Address of the Interface
3	MAC(Optional)	Give the MAC Address (Optional)



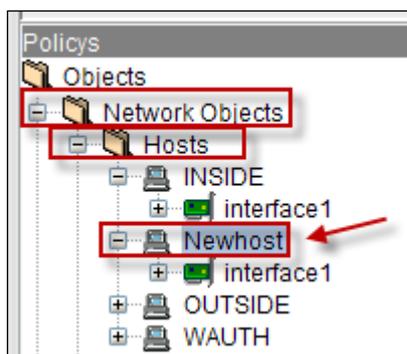
Click on **Add** tab to Add new Host.

Select **Notes** tab to provide information about the newly added Host and click on **Apply** tab.

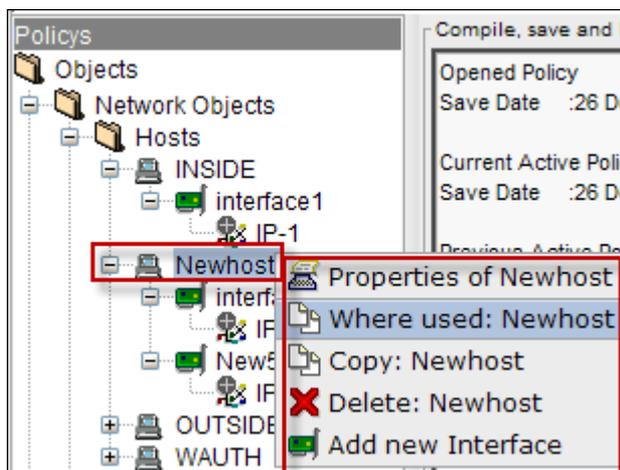
Cancel tab helps to cancel the Notes.



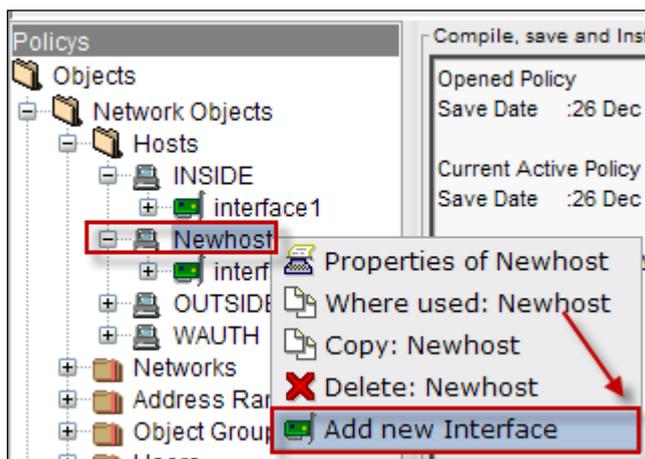
We can notice newly added Host under the Hosts list with selected type of the Interface.



Right click on added Host, to perform actions like viewing **Properties** of the Host, to find out where it is used, **copying** Host, **Deleting** Host and **Adding new Interface** to the Host.



To Add new Interface to the Host, Right click on the Host select **Add new Interface** tab.



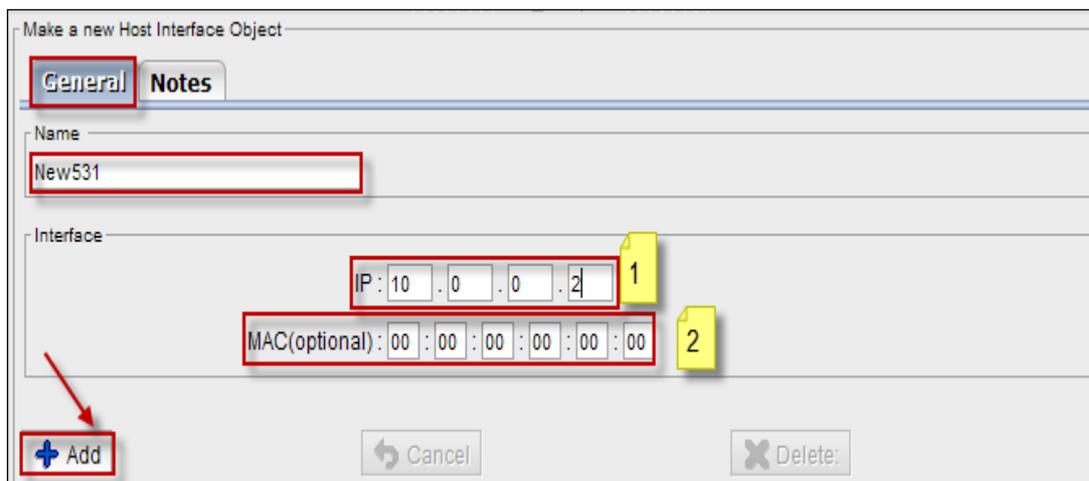
Below screen appears, Select **General** tab.

It consists of two fields, **Name** and **Interfaces**.

In the **Name** tab, name of the new Interface should be mentioned.

These are the inputs for the Interfaces:

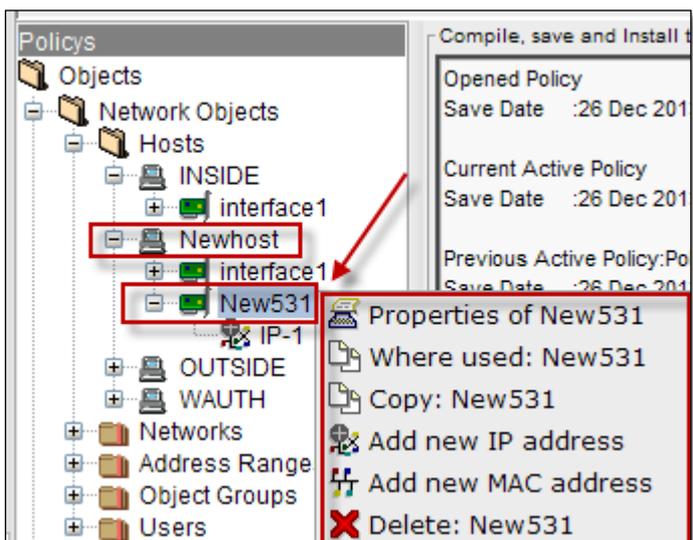
1	IP	Give the IP Address of the Interface
2	MAC(Optional)	Give the MAC Address (Optional)



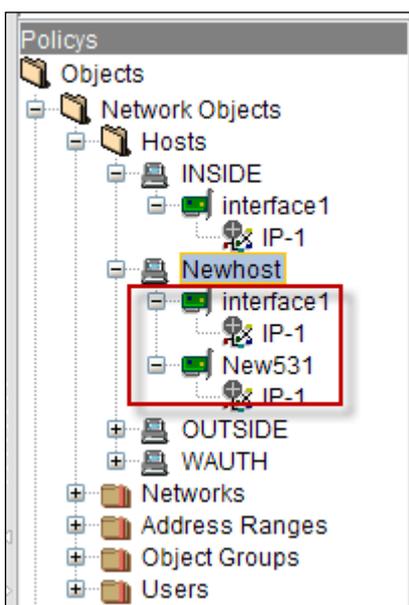
Click on **Add** tab.

We can notice the newly added Interface under the New Host.

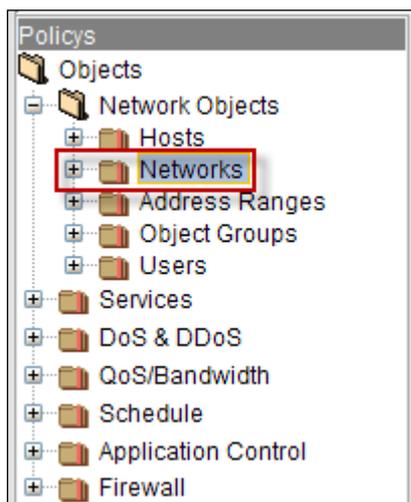
Right click on the Interface to perform actions like viewing **Properties** of the Interface, to find out where it is used, **copying** Interface, **Adding new IP address** to the Interface, **Adding new MAC address** to the Interface and **Deleting** Interface.



We can notice Interfaces for the newly added Host in the below screen.

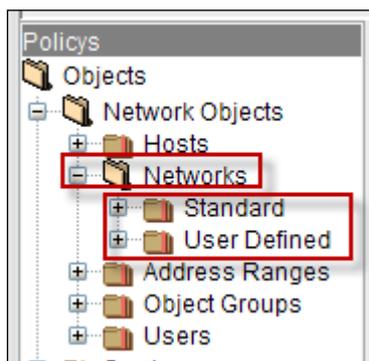


Networks

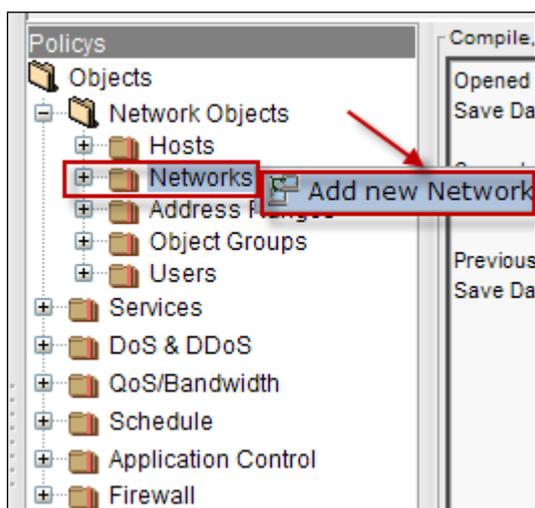


Expand Networks, by default it consists of two Network

They are **Standard** and **User Defined** networks



Right click on Networks, to **Add new Network**



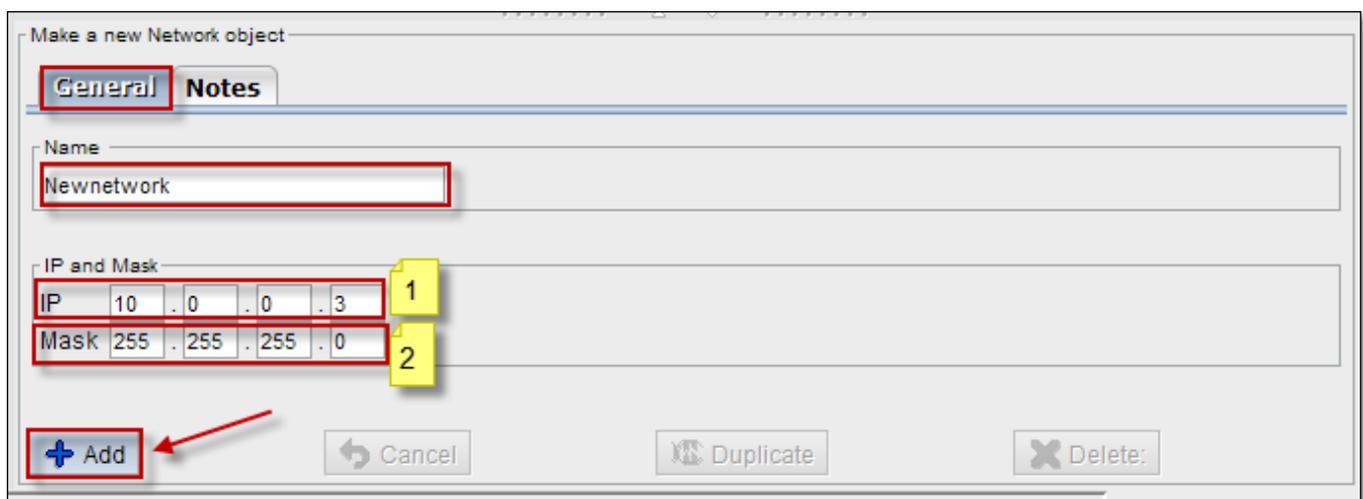
Below screen appears, Select **General tab**.

It consists of two fields, **Name** and **Interfaces**.

In the **Name tab**, name of the new Network object should be mentioned.

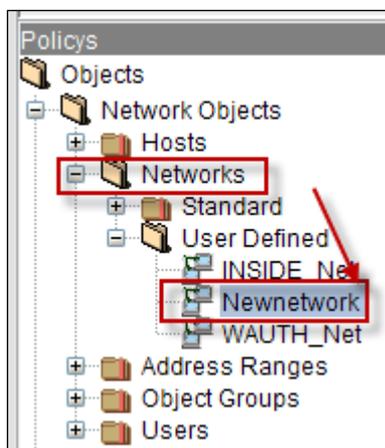
These are the inputs for the Interfaces:

1	IP	Give the IP Address of the Interface
2	MAC(Optional)	Give the MAC Address (Optional)

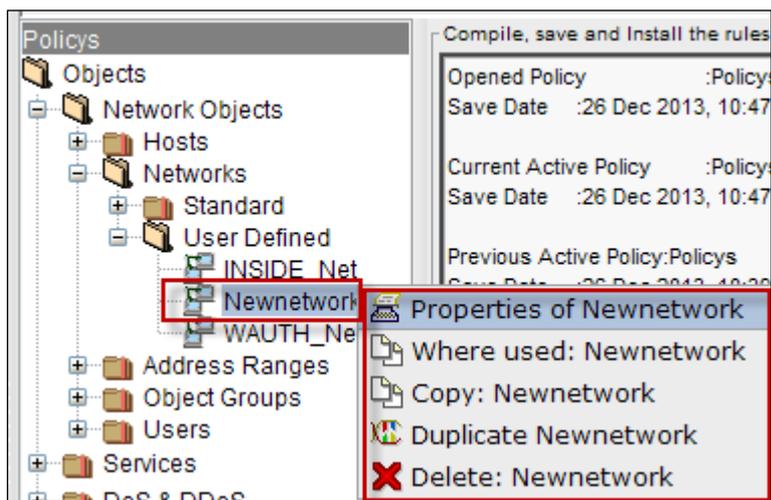


Click on **Add** tab.

We can notice Newly added Network under the **User Defined Network** with selected type of the Interface.



Right click on added Network, to perform actions like viewing **Properties** of the Network, to find out where it is used, **copying** Network, **Duplicating** Network and **Deleting** Network.



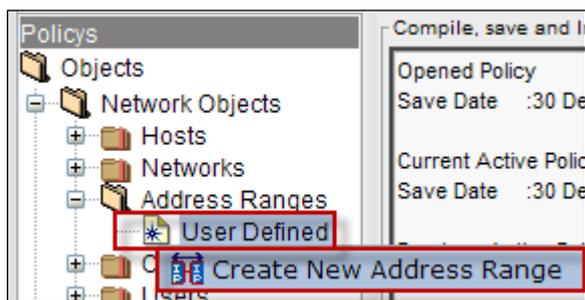
Address Ranges



Expand Address Ranges, User Defined is displayed



Right click on User Defined, to **Create New Address Range**



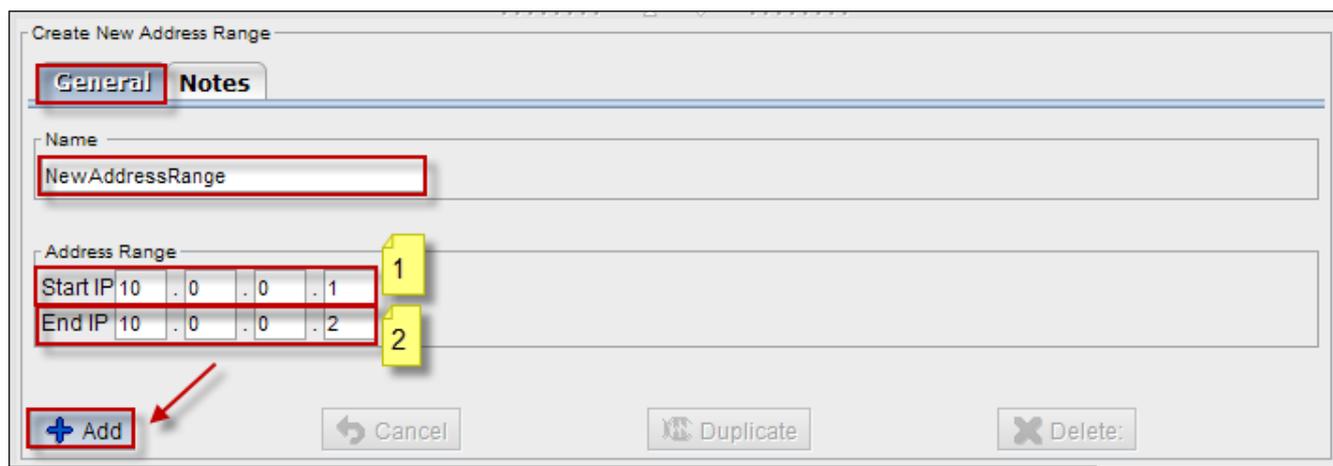
Below screen appears, Select **General tab**.

It consists of two fields, **Name** and **Address Range**.

In the **Name tab**, name of the new Address Range should be mentioned.

These are the inputs for the Address Range:

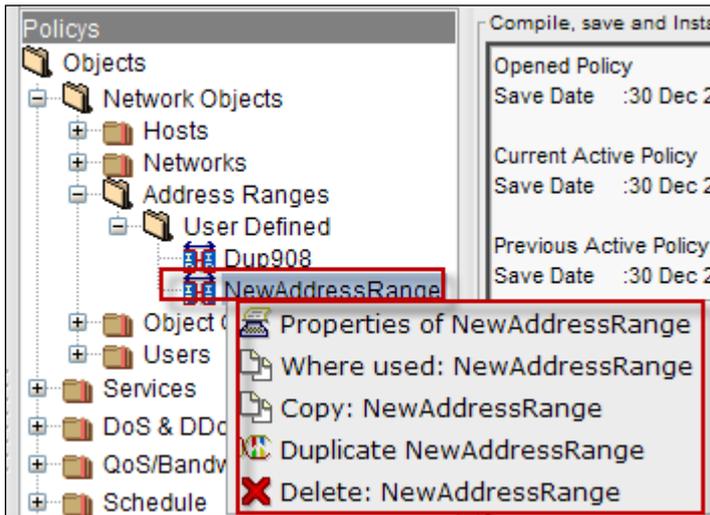
1	Start IP	Give the IP Address of the Interface
2	End IP	Give the MAC Address (Optional)



Click on **Add** tab.

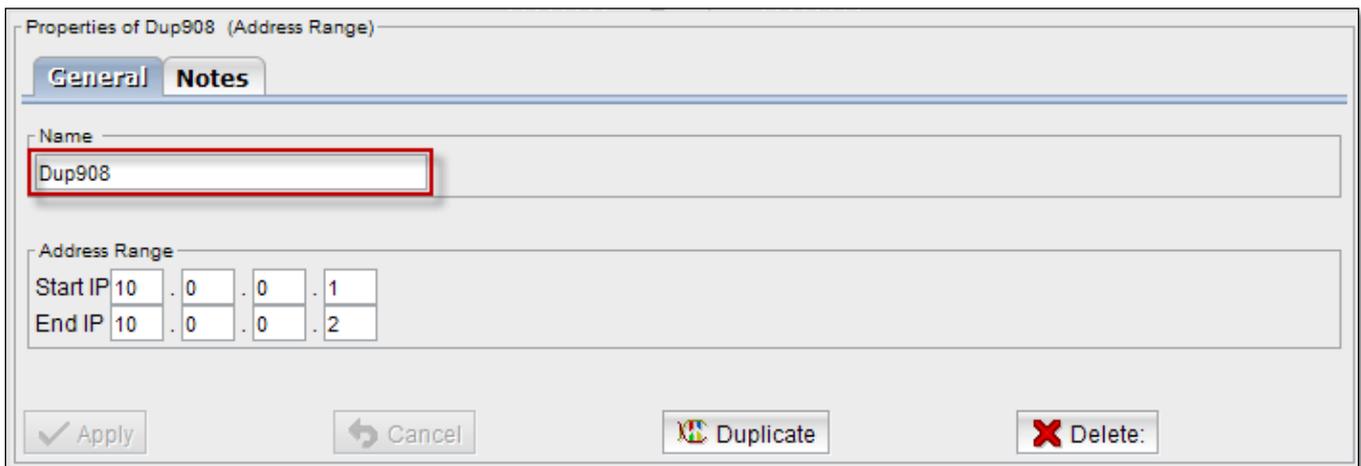
We can notice the new Address Range in the below screen.

Right click on added Address Range, to perform actions like viewing **Properties** of the New Address Range, to find out where it is used, **copying** New Address Range, **Duplicating** New Address Range and **Deleting** New Address Range.

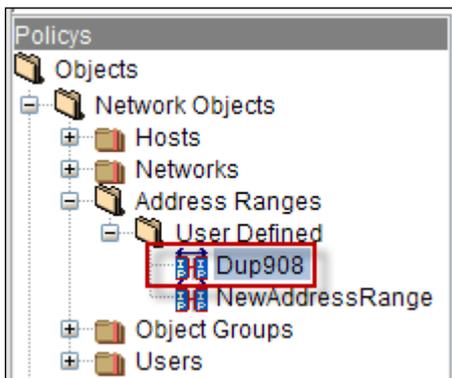


When we click on Duplicate **New Address Range**, below screen appears.

In which it displays **Name** of the Duplicate Address Range and **Address Range**.



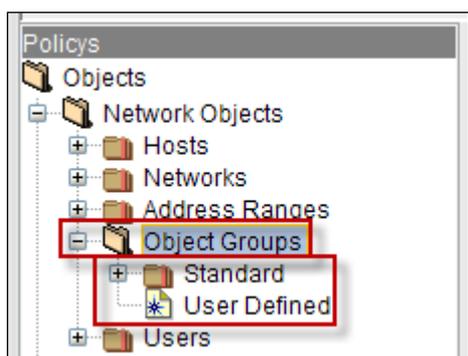
We can notice **Duplicate Address Range** under User Defined list.



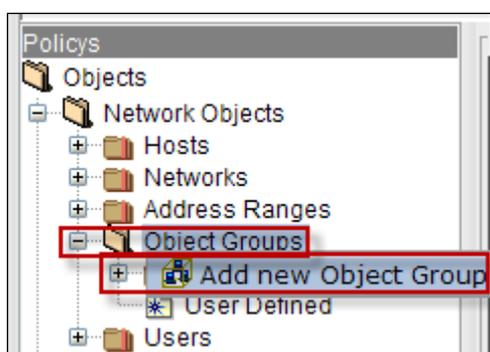
Object Groups



Expand **Object Groups**, by default **Standard** and **User Defined Object Groups** are displayed.



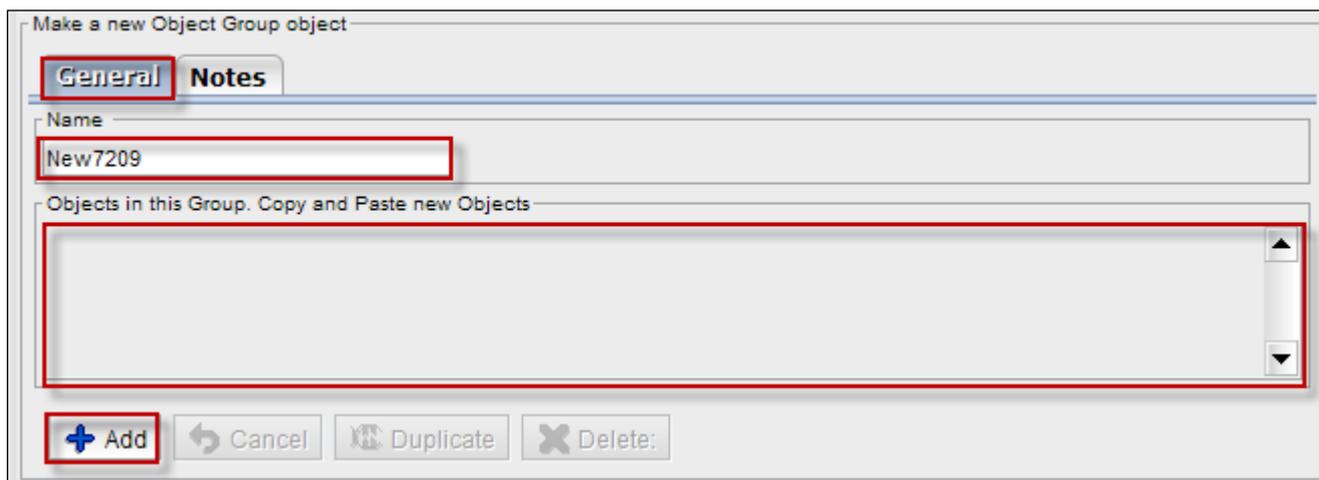
Right click on Object Groups, to add new object Group.



Below screen appears.

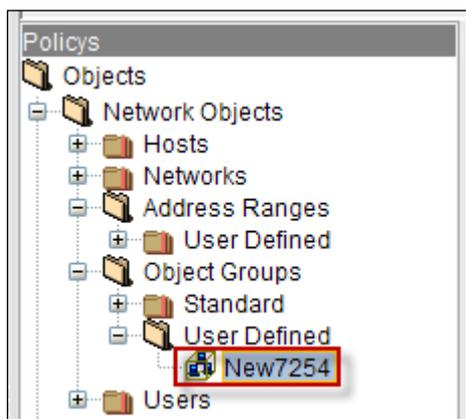
Select **General tab**, give the name of the new Object Group.

We can copy and paste new Objects in this Object Group.

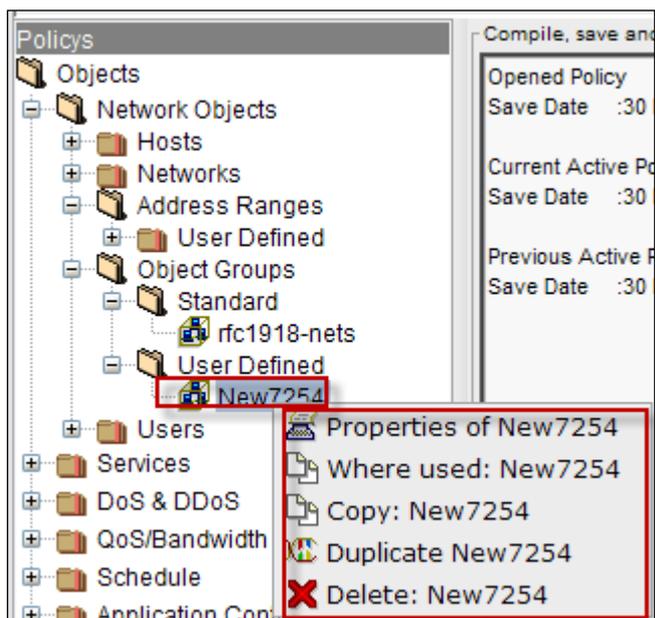


Click on **Add** tab.

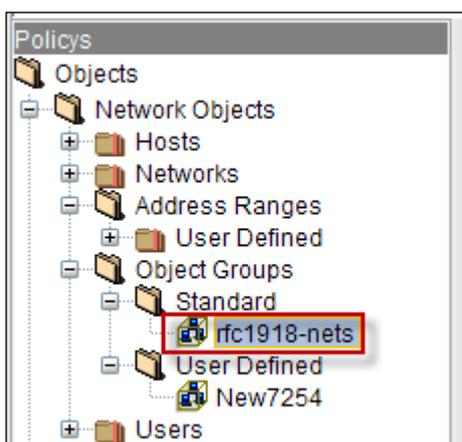
We can notice new **Object Group** in the **User Defined**.



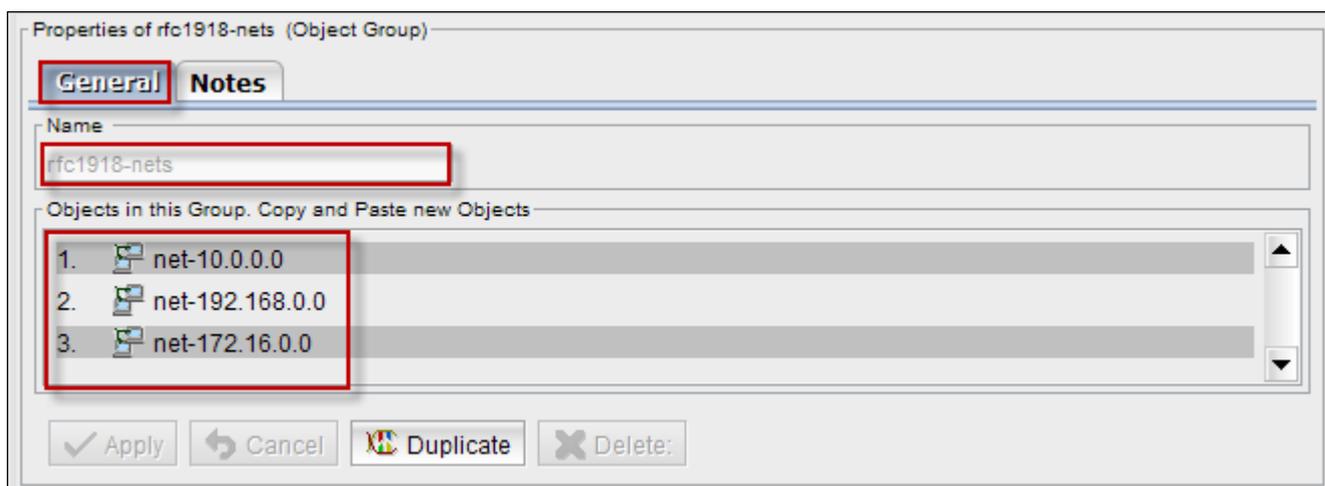
Right click on the **Object Group**, to perform actions like viewing **Properties** of the Object Group, to find out where it is used, **copying** Object Group, **Duplicating** Object Group and **Deleting** Object Group.



Right click on the **object Group** and select **Properties**.



We can notice name of the **Object Group** and list of objects in the Group.

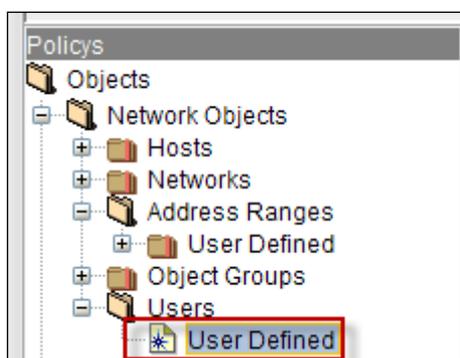


Users

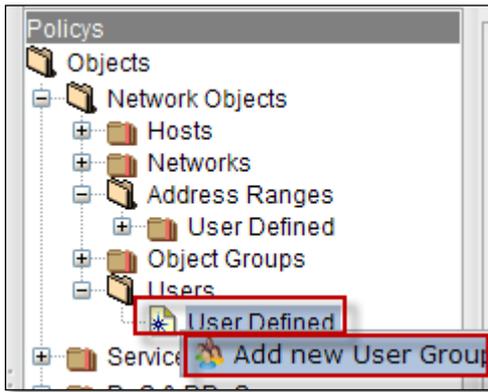
Expand **Users**.



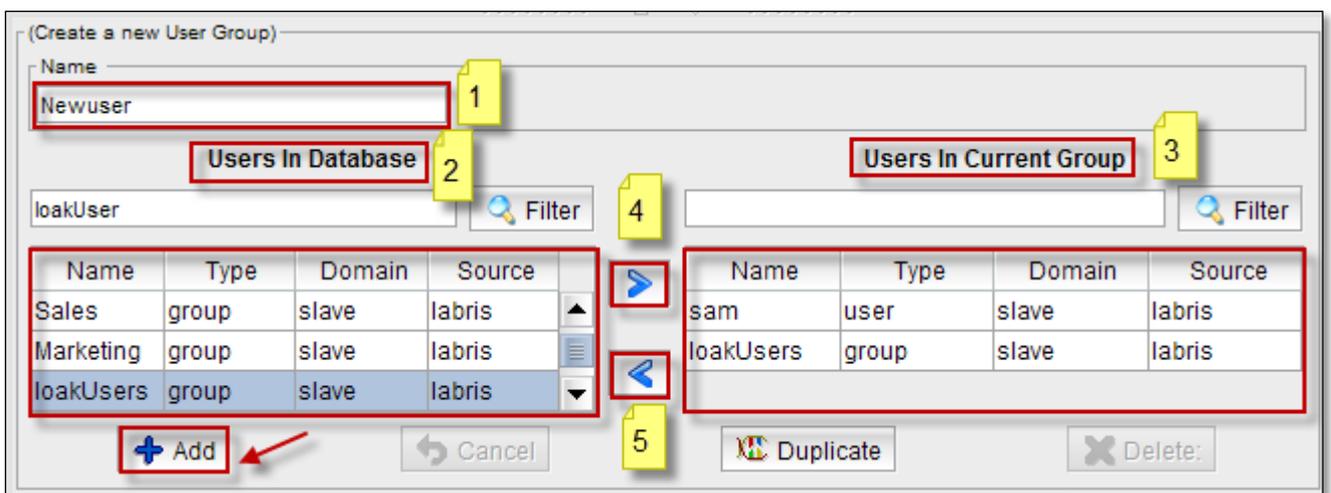
By default **User Defined** is displayed.



Right click on the **User Defined** to Add new **User Group**.



Below screen appears.

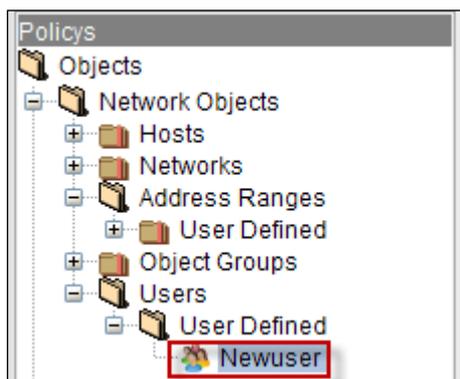


These are the inputs two add new **User Group**:

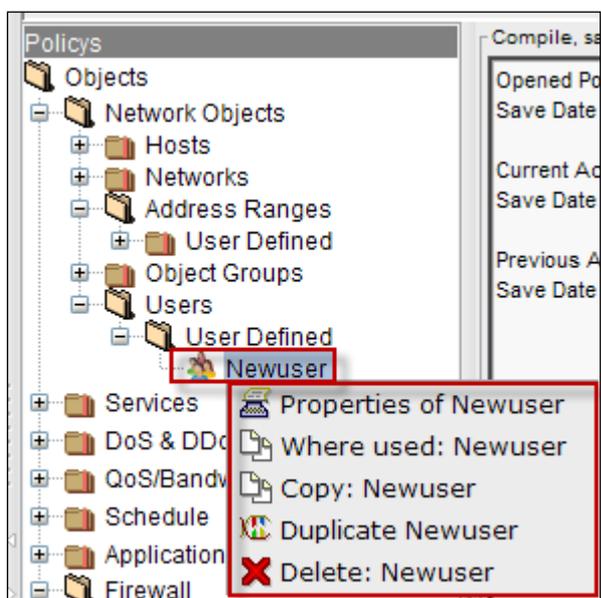
1	Name	Type Name of the new User Group
2	Users in Data base	Displays Users in Data base
3	Users in Current Group	Displays Users in Current Group
4		It enables to add Users from Database to Current Group
5		It enables to remove Users from Current Group

Click on **Add** tab.

We can notice new **User Group** under the **User Defined** list.



Right click on the User Group, to perform actions like viewing **Properties** of the User Group, to find out where it is used, **copying** User Group, **Duplicating** User Group and **Deleting** User Group.

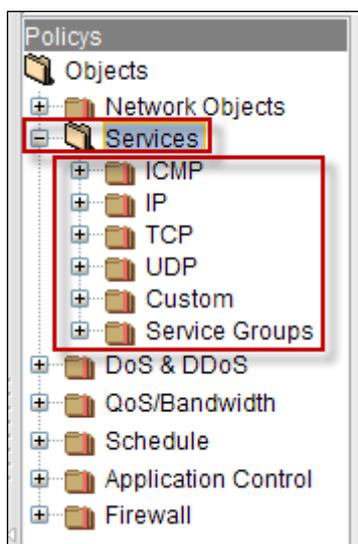


46. Services

In Firewall Builder, service objects are represented by IP, ICMP, TCP, and UDP services such as "host unreachable" in ICMP, HTTP in TCP, GRE in IP, and DNS in UDP. Firewall Builder plays a crucial role in providing necessary service objects for hundreds of well-known and frequently-used services in ICMP (IP protocol number 1), TCP (IP protocol number 6), and UDP (IP protocol number 17).

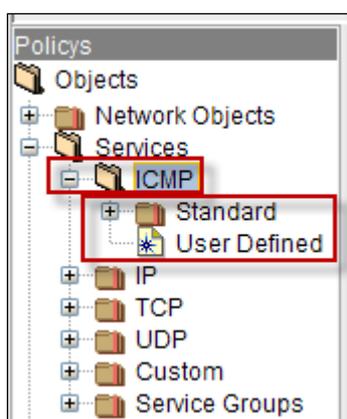


Expand **Services**, service Objects **ICMP, IP, TCP, UDP, Custom, Service Groups** are displayed

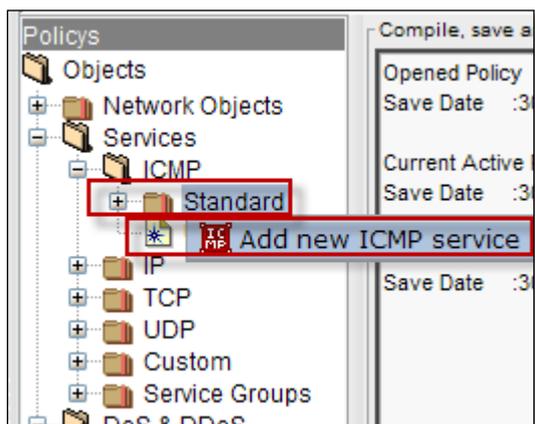


ICMP

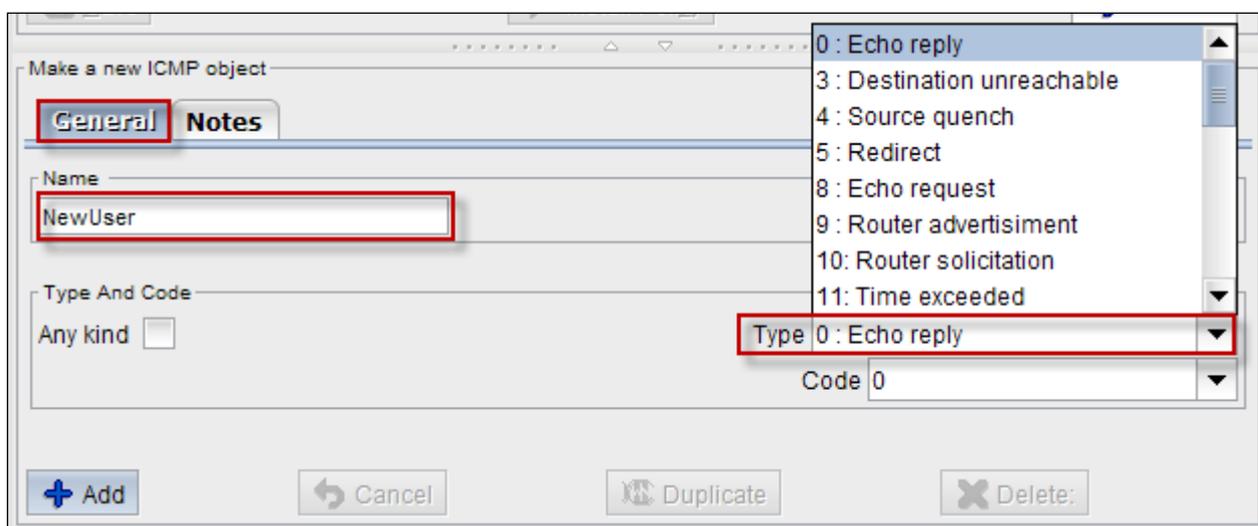
Expand **ICMP**, by default **Standard** and **User Defined**.



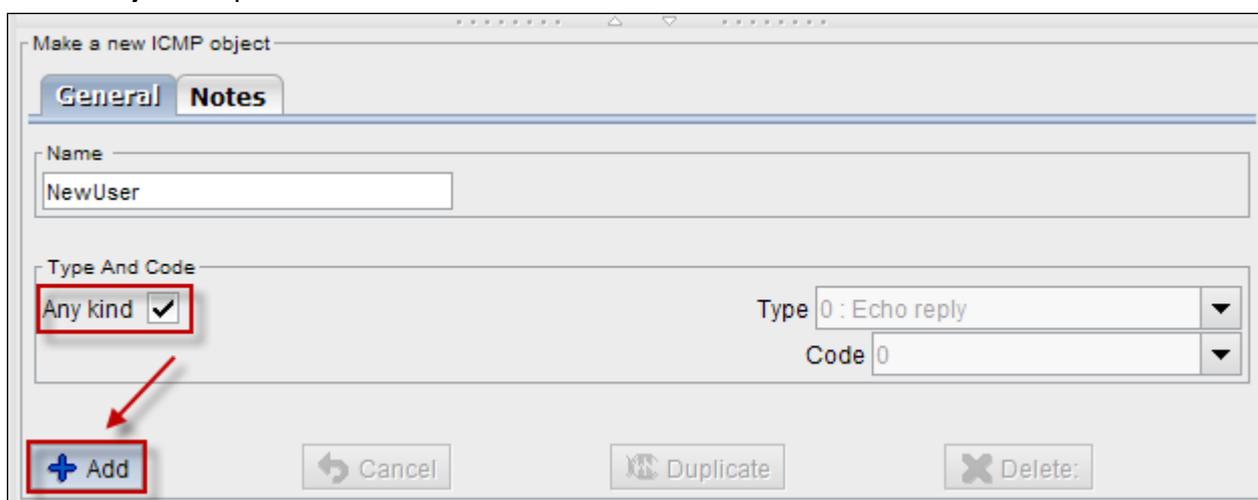
Right click on **Standard**, to add new **ICMP** service



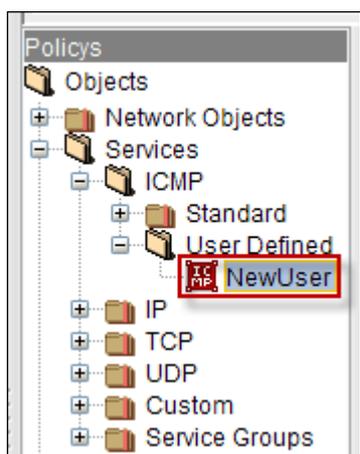
Select **General** tab, to give the name of the **ICMP** object and choose the type of object from the drop down list in the **Type** tab



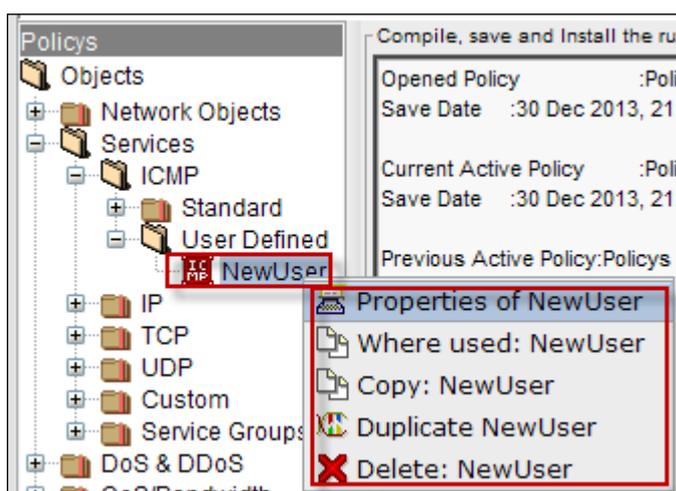
Enable **Any kind** option and click on **Add** tab



We can notice new Object under **User Defined**.

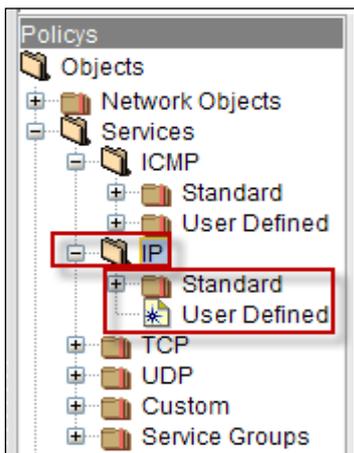


Right click on the new ICMP Service object, to perform actions like viewing **Properties** of the ICMP Service object, to find out where it is used, **copying** ICMP Service object, **Duplicating** and **Deleting** ICMP Service object.

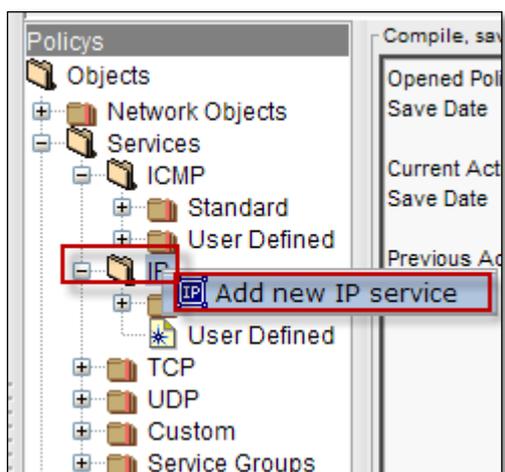


IP

Expand **IP**, by default **Standard** and **User Defined**.

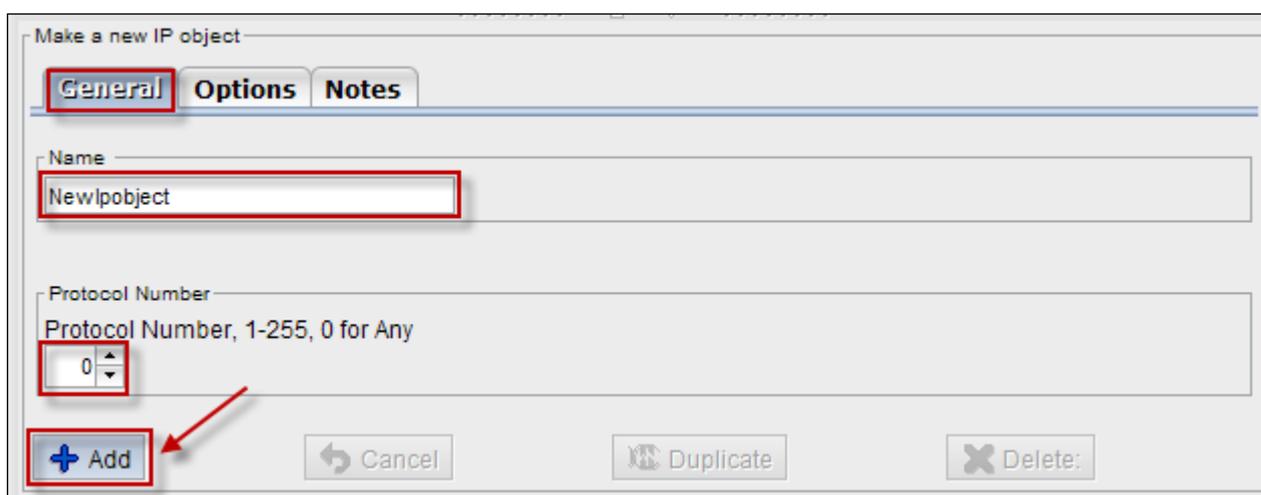


Right click on **IP**, to add new **IP** service

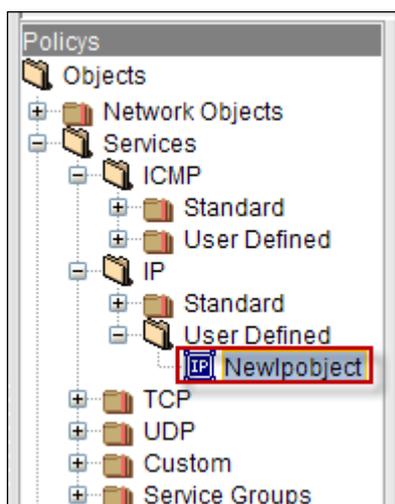


Select **General** tab, give the name of the **IP** object and choose Protocol Number.

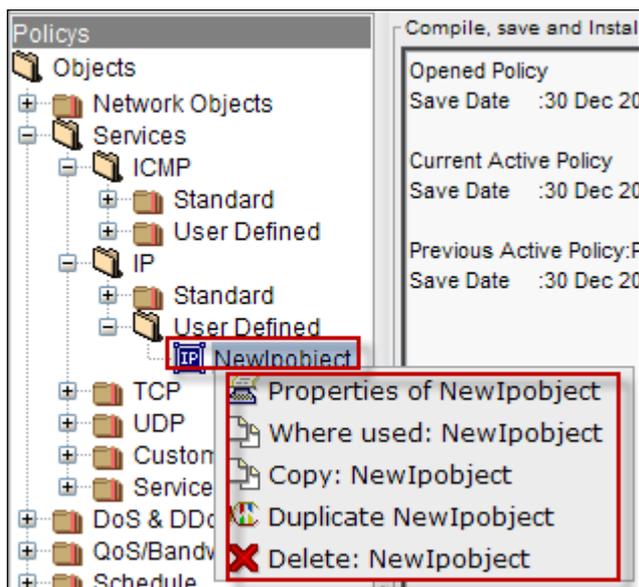
Click on **Add** tab.



We can notice new IP object under **User Defined**.

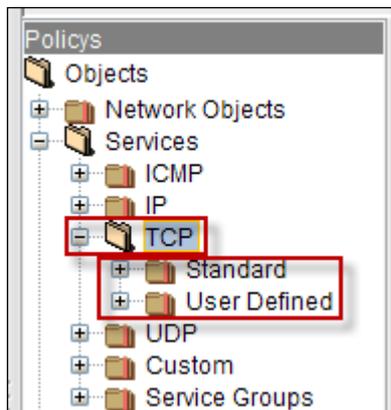


Right click on the new IP Service object, to perform actions like viewing **Properties** of the IP Service object, to find out where it is used, **copying** IP Service object, **Duplicating** and **Deleting** IP Service object.

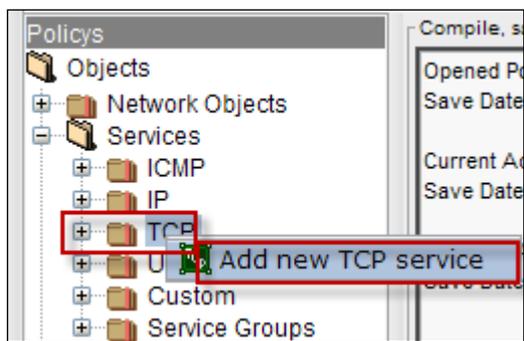


TCP

Expand **TCP** ,by default **Standard** and **User Defined** are displayed.



Right click on **TCP**, to add new **TCP** service.



Select **General tab**, give the **Name** of the TCP object and choose **Source port range**, **Destination port range**.

Click on **Add tab**.

Make a new TCP object

General Flags Notes

Name
NewTcobject

Source port range
Start: 0
End: 4

Destination port range
Start: 0
End: 4

+ Add Cancel Duplicate Delete

Select **Flags tab**, to enable Flags which need to be examined by the firewall.

Click on **Apply tab**.

Properties of NewTcobject (TCP)

General **Flags** Notes

TCP Flags

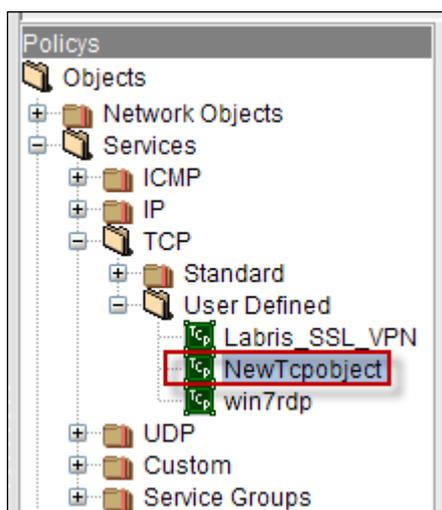
Match when the TCP flags are as specified.

Flags that firewall should examine:
 URG ACK PSH RST SYN FIN

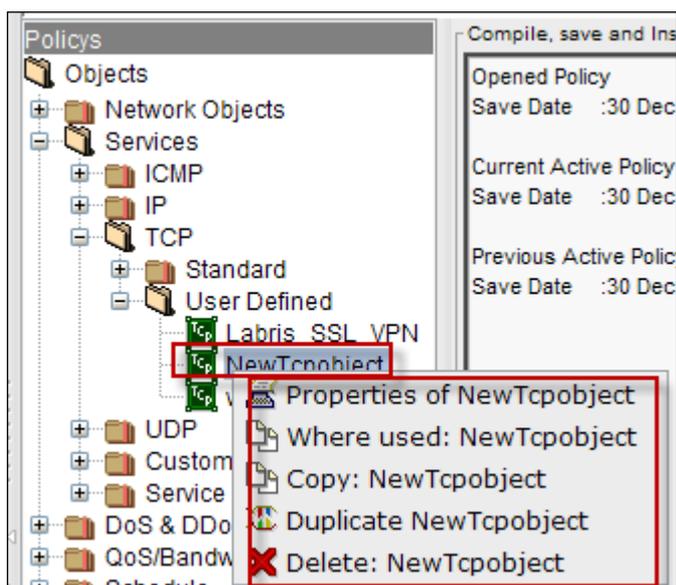
Flags that must be set:
 URG ACK PSH RST SYN FIN

✓ Apply Cancel Duplicate Delete

We can notice new **TCP** object in the **User Defined** option.

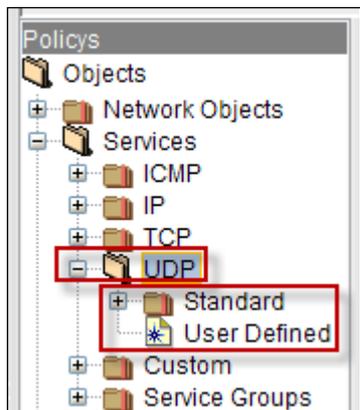


Right click on the new TCP Service object, to perform actions like viewing **Properties** of the TCP Service object, to find out where it is used, **copying** TCP Service object, **Duplicating** and **Deleting** TCP Service object.

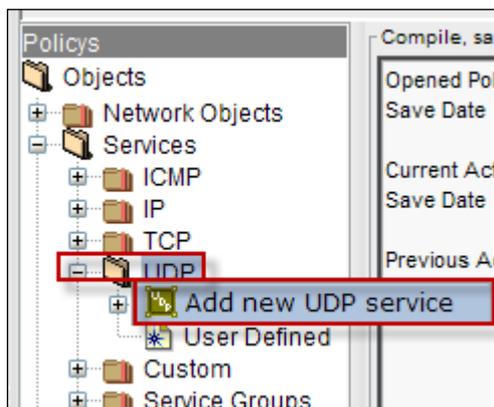


UDP

Expand **UDP** ,by default **Standard** and **User Defined** are displayed.

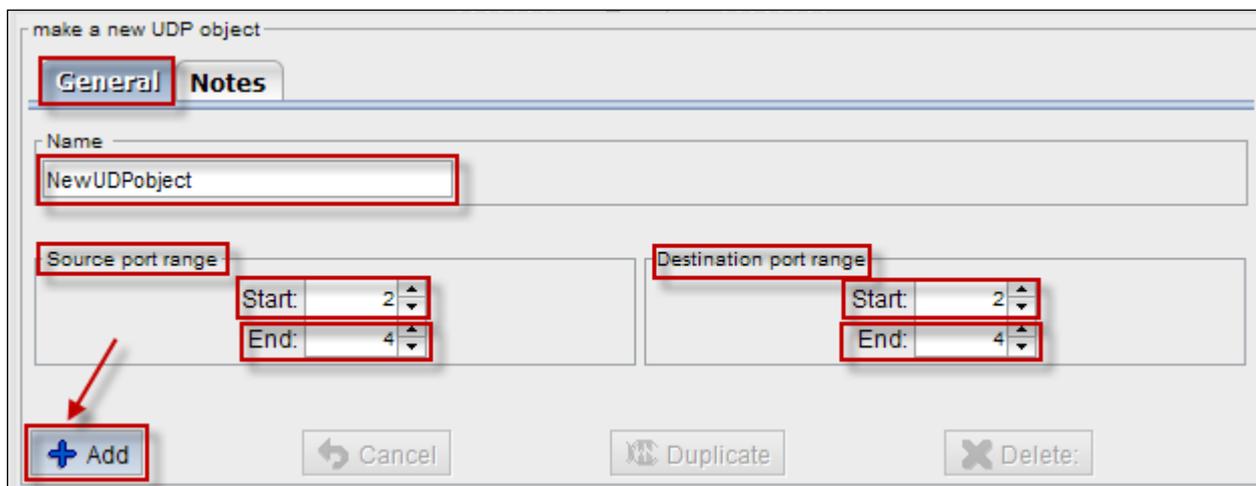


Right click on **UDP** ,to add new **UDP** service.

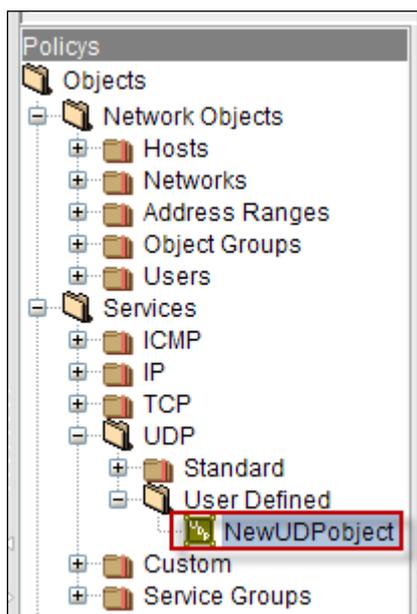


Select **General tab**, give the **Name** of the UDP object and choose **Source port range**, **Destination port range**.

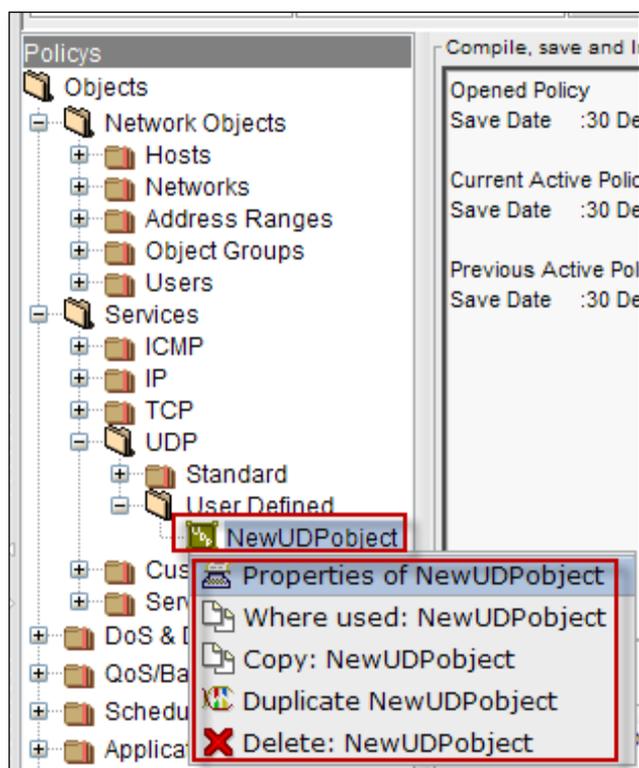
Click on **Add tab**.



We can notice new **UDP** object under **User Defined**.

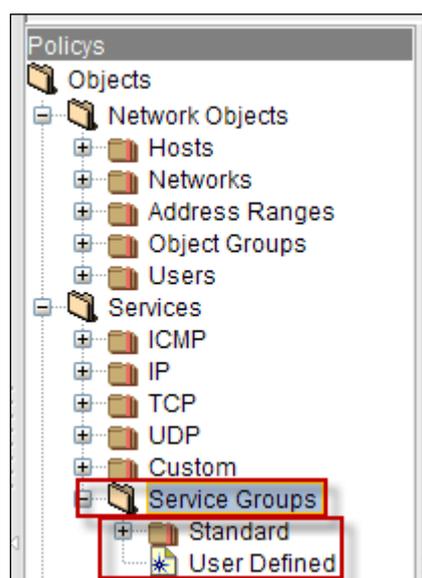


Right click on the new UDP Service object, to perform actions like viewing **Properties** of the UDP Service object, to find out where it is used, **copying** UDP Service object, **Duplicating** and **Deleting** UDP Service object.

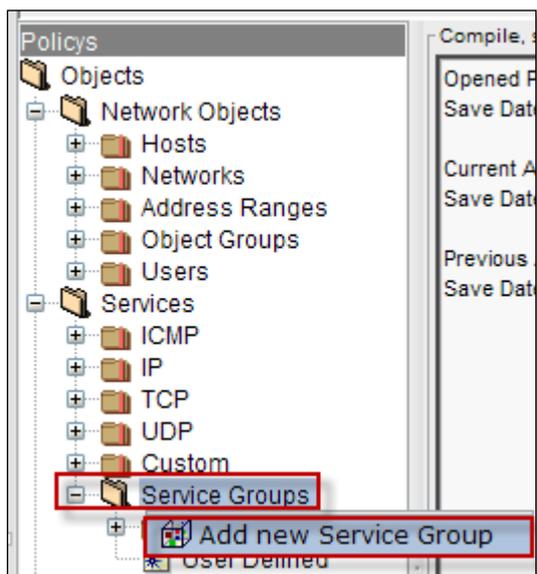


Service Groups

Expand **Service Groups**, by default **Standard** and **User Defined** are displayed.



Right click on **Service Groups**, to add new **Service Group**.

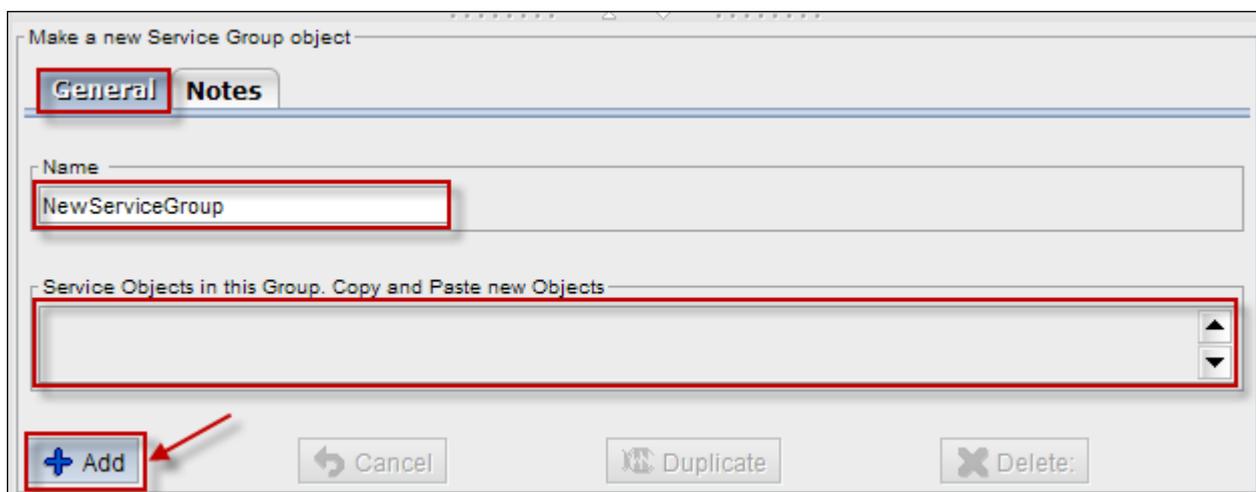


Below screen appears.

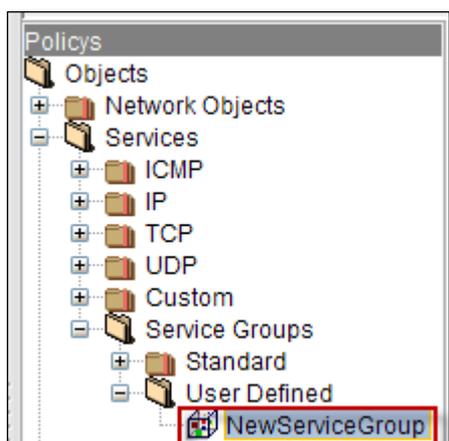
Select **General tab**, give the name of the new Service object Group.

We can copy and paste new Objects in this Service Object Group.

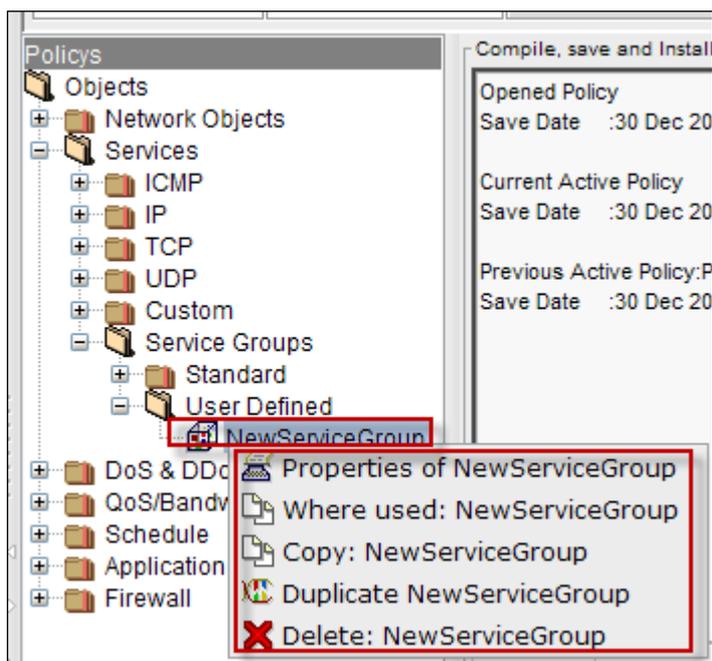
Click on **Add tab**.



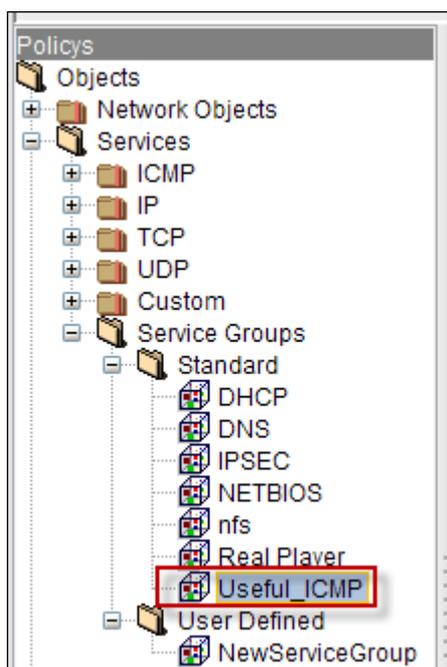
We can notice new **Service Group** under **User Defined**.



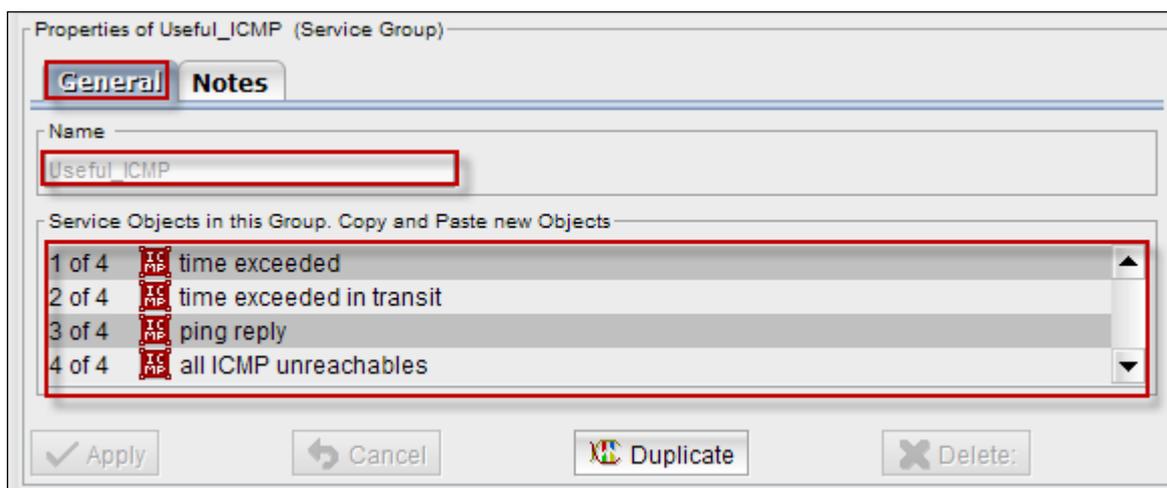
Right click on the new Service Group, to perform actions like viewing **Properties** of the New Service Group, to find out where it is used, **copying** New Service Group, **Duplicating** and **Deleting** New Service Group.



Right click on the **Service Group** and select Properties.



Below screen appears, name of the **Service Group** and list of Objects in this **Service Group** is displayed.



47. DoS/DDoS

A Denial of Service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.

The most common type of Denial of Service attack involves flooding the target resource with external communication requests. This overloaded prevents the resources from responding to legitimate traffic, or slows its responses so significantly that it is rendered effectively unavailable.

A Distributed Denial-of-Service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

In a typical DDoS attack, the assailant begins by exploiting a vulnerability in one computer system and making it the DDoS master. The attack master, also known as the boot master, identifies and identifies and infects other vulnerable systems with malware. Eventually, the assailant instructs the controlled machines to launch an attack against a specified target.

*Source - www.searchsecurity.com



Expand DoS & DDoS, by default **User Defined** is displayed.



Right click on **Dos &DDoS**, to add new DoS

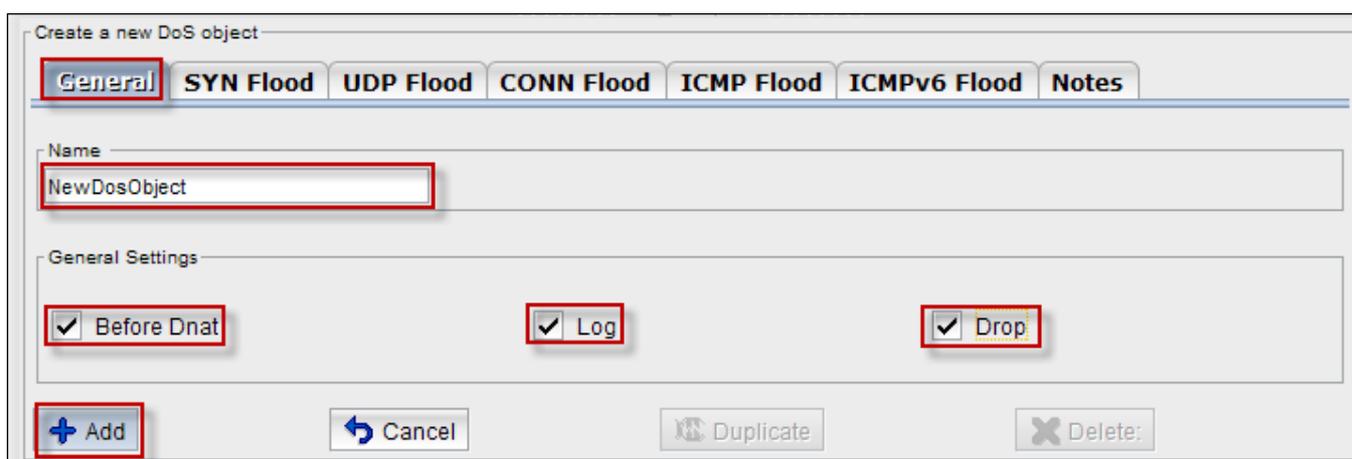


General

Below screen appears. Select **General tab** it consists of two fields, Name & General Settings.

In the Name field, name of the Dos object should be mentioned.

In General Setting's field, we can enable or disable **Before Dnat, Log, Drop**.



SYN Flood

SYN Flood helps us to view and change the SYN Flood Settings.

We can enable or disable SYN Flood, Per Source, Per Destination, and Total.

Give the appropriate Count and Burst values.

The screenshot shows the 'Create a new DoS object' window with the 'SYN Flood' tab selected. The 'SYN Flood Settings' section contains a list of checkboxes on the left and input fields for 'Count' and 'Burst (1-10000)' on the right. The checkboxes are: SYN Flood, Per Source, Per Destination, and Total. The input fields are: Count 1, Burst (1-10000) 400; Count 40, Burst (1-10000) 55; and Count 999, Burst (1-10000) 800. At the bottom, there are buttons for '+ Add', 'Cancel', 'Duplicate', and 'Delete'.

UDP Flood

UDP Flood helps us to view and change the UDP Flood Settings.

We can enable or disable UDP Flood, Per Source, Per Destination, and Total.

Give the appropriate Count and Burst values.

The screenshot shows the 'Create a new DoS object' window with the 'UDP Flood' tab selected. The 'UDP Flood Settings' section contains a list of checkboxes on the left and input fields for 'Count' and 'Burst (1-10000)' on the right. The checkboxes are: UDP Flood, Per Source, Per Destination, and Total. The input fields are: Count 30, Burst (1-10000) 60; Count 60, Burst (1-10000) 900; and Count 800, Burst (1-10000) 1000. At the bottom, there are buttons for '+ Add', 'Cancel', 'Duplicate', and 'Delete'.

CONN Flood

CONN Flood helps us to view and change the UDP Flood Settings.

We can enable or disable CONN Flood, Per Source, Per Destination, Total.

Give the appropriate Count and Burst values.

Create a new DoS object

General SYN Flood UDP Flood **CONN Flood** ICMP Flood ICMPv6 Flood Notes

CONN Flood Settings

<input checked="" type="checkbox"/> CONN Flood	Count	50	Burst (1-10000)	599
<input checked="" type="checkbox"/> Per Source	Count	300	Burst (1-10000)	3000
<input checked="" type="checkbox"/> Per Destination	Count	500	Burst (1-10000)	878
<input checked="" type="checkbox"/> Total	Count		Burst (1-10000)	

+ Add ↶ Cancel Duplicate X Delete

ICMP Flood

ICMP Flood helps us to view and change the UDP Flood Settings.

We can enable or disable ICMP Flood, Per Source, Per Destination, Total.

Give the appropriate Count and Burst values.

Create a new DoS object

General SYN Flood UDP Flood CONN Flood **ICMP Flood** ICMPv6 Flood Notes

ICMP Flood Settings

<input checked="" type="checkbox"/> ICMP Flood	Count	70	Burst (1-10000)	299
<input checked="" type="checkbox"/> Per Source	Count	67	Burst (1-10000)	887
<input checked="" type="checkbox"/> Per Destination	Count	200	Burst (1-10000)	300
<input checked="" type="checkbox"/> Total	Count		Burst (1-10000)	

+ Add ↶ Cancel Duplicate X Delete

ICMPv6 Flood

ICMPv6 Flood helps us to view and change the UDP Flood Settings.

We can enable or disable ICMPv6 Flood, Per Source, Per Destination, and Total.

Give the appropriate Count and Burst values.

The screenshot shows the 'Create a new DoS object' dialog box with the 'ICMPv6 Flood' tab selected. The 'ICMPv6 Flood Settings' section contains a list of checkboxes: 'ICMPv6 Flood', 'Per Source', 'Per Destination', and 'Total', all of which are checked. To the right, there are three rows of input fields for 'Count' and 'Burst (1-10000)'. The values are: Count 220, Burst 330; Count 880, Burst 4500; and Count 1, Burst 5. The 'ICMPv6 Flood' tab is highlighted with a red box.

Notes

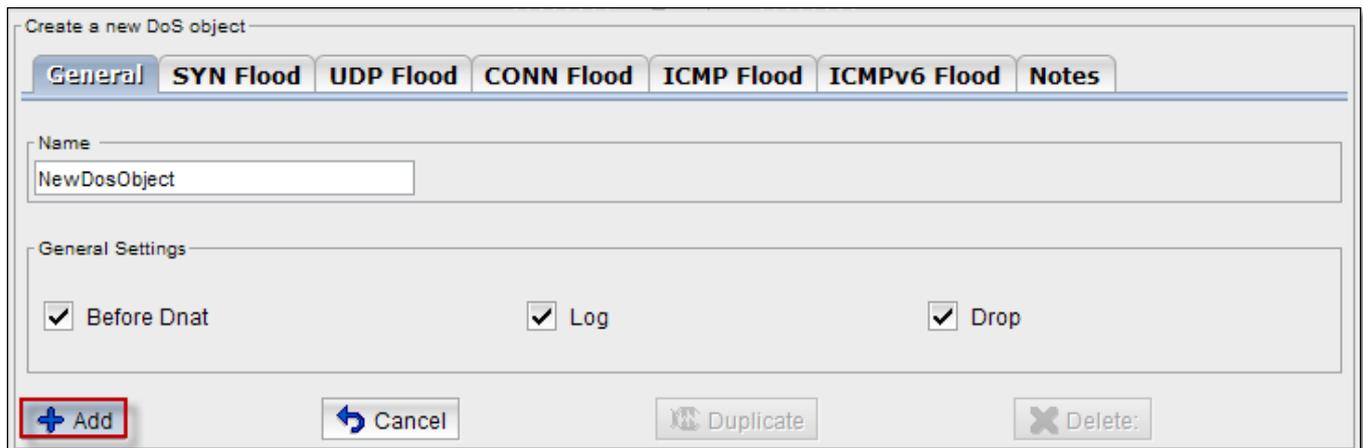
In Notes column, we can write information regarding new DOS Object.

The screenshot shows the 'Create a new DoS object' dialog box with the 'Notes' tab selected. The 'Notes' section contains a text area with the text 'NewDosObject' entered. The 'Notes' tab is highlighted with a red box. At the bottom, there are buttons for '+ Add', 'Cancel', 'Duplicate', and 'Delete:'.

After providing all the inputs to the New Dos Object, click on **Apply** tab.

The screenshot shows the 'Properties of NewDosObject (DoS)' dialog box with the 'General' tab selected. The 'Name' field contains 'NewDosObject'. The 'General Settings' section contains three checkboxes: 'Before Dnat', 'Log', and 'Drop', all of which are checked. The 'Apply' button is highlighted with a red box. At the bottom, there are buttons for 'Apply', 'Cancel', 'Duplicate', and 'Delete:'.

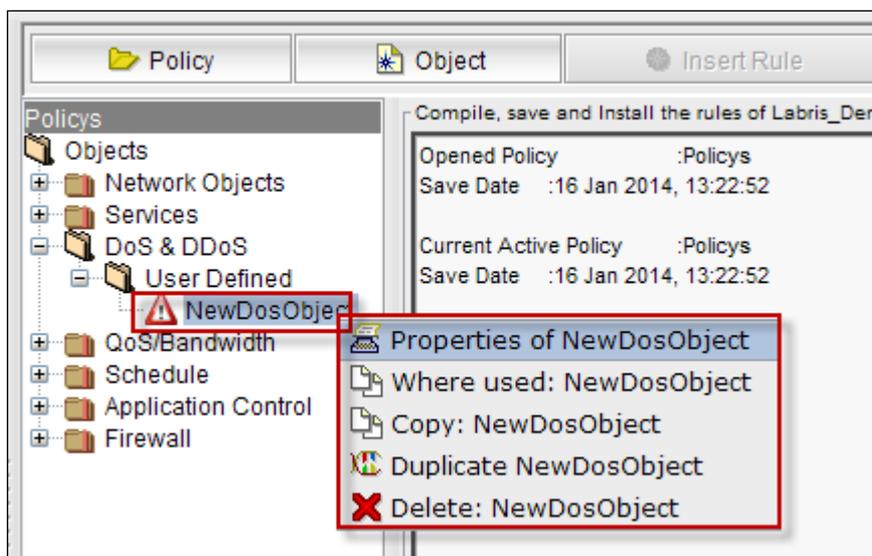
Click on **Add** tab.



In the below screen, we can notice New Dos Object under User Defined.



Right click on the New Dos object, to perform actions like viewing **Properties** of the Dos object, to find out where it is used, **copying** object, **Duplicating** and **Deleting** Dos object.

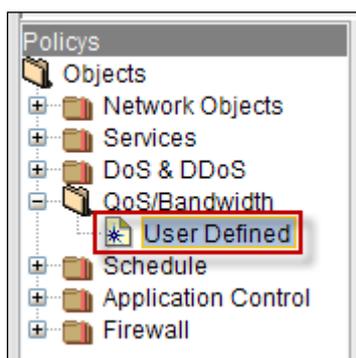


48. QoS/Bandwidth

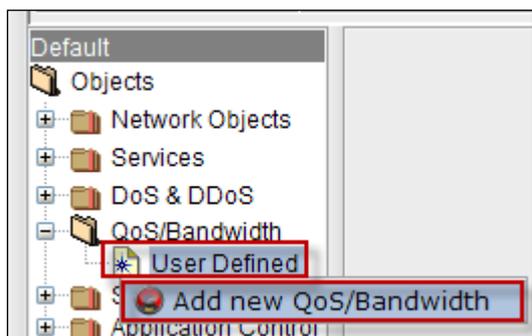
QoS (Quality of Service) plays a crucial role in ensuring high-quality performance to latency and bandwidth sensitive applications. Differential treatment of traffic based on rules are accepted and prioritized. Necessary protocols and performance of the network is effectively improved by QoS.



Expand QoS/Bandwidth, by default **User Defined** is displayed.



Right click on User Defined under QoS/Bandwidth, to add new QoS/Bandwidth.



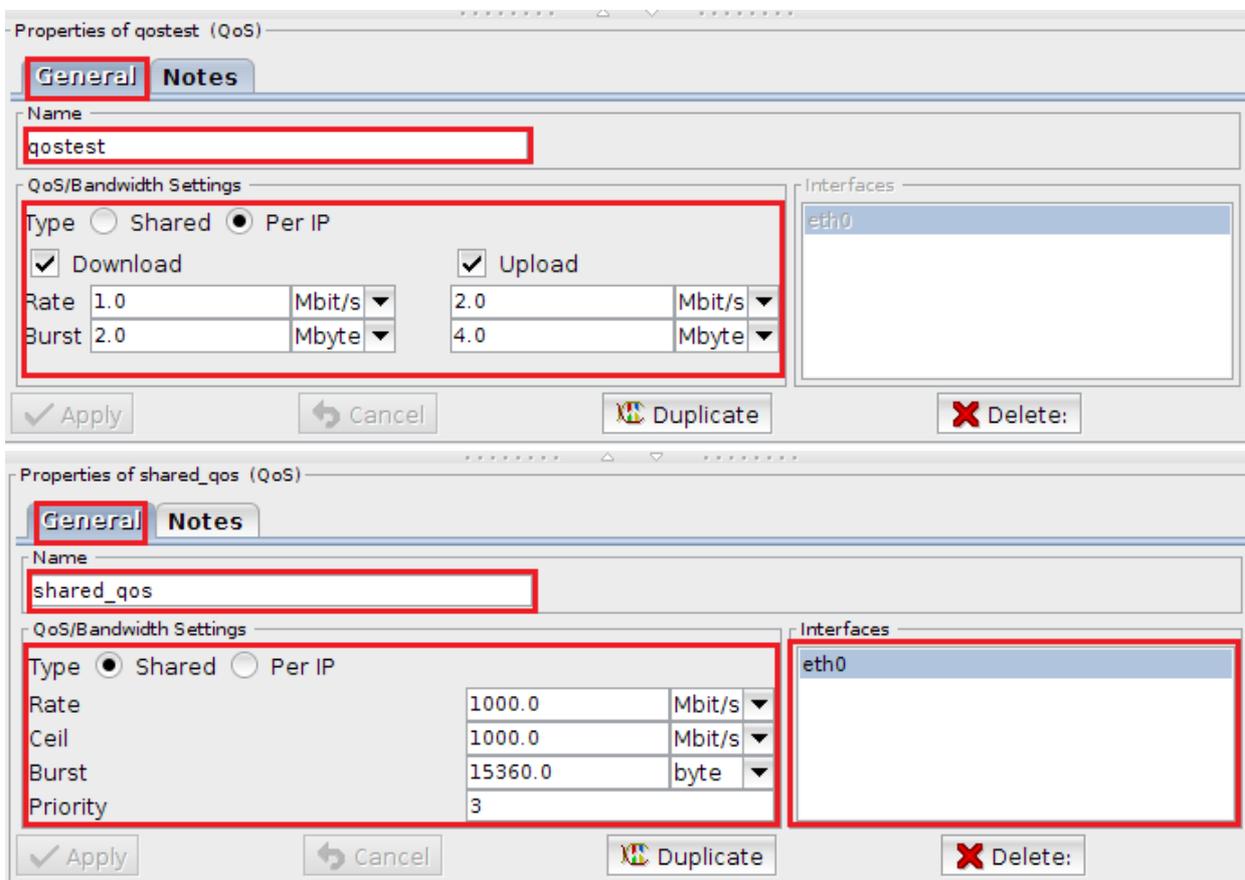
General

To make a new QoS/Bandwidth, select **General tab**.

Give the name of the QoS/Bandwidth object.

Give appropriate values for Rate (Mbit/s), Ceil (Mbit/s), Burst (Byte) and Priority in **QoS/Bandwidth Settings**.

Choose Interface for the New QoS/Bandwidth object from the list of **Interfaces**.



Choose between per ip or shared, for your rule's purpose. Then press apply to save changes.

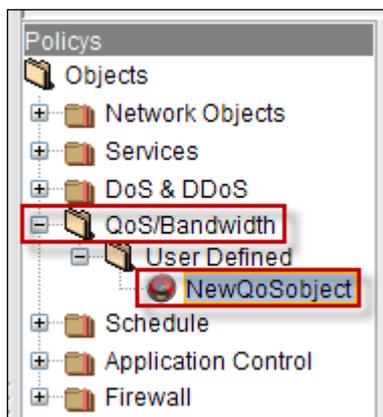
Notes

Select **Notes tab** to write notes regarding new object creation.

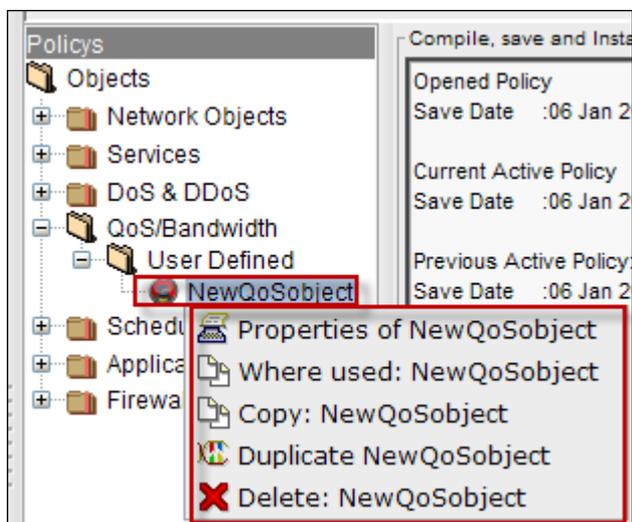


Click on **Apply** tab.

In the below screen we can notice **QoS/Bandwidth** object.



Right click on the new QoS/Bandwidth object, to perform actions like viewing **Properties** of the QoS/Bandwidth object, to find out where it is used, **copying** object, **Duplicating** and **Deleting** QoS/Bandwidth object.

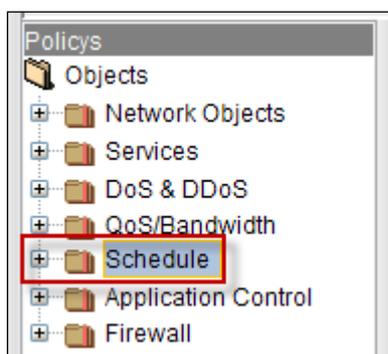


49. Schedule

Firewall rules are scheduled in such a way that they must be Active only at certain times of the day or particular days or particular hours and minutes.

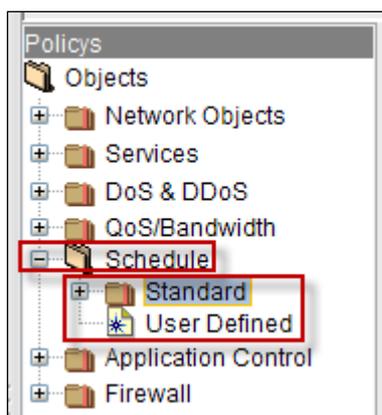
Firstly schedule should be created under Firewall and then apply a schedule to the rule or while creating a rule pick up appropriate defined schedule to the rule.

We can create one time schedule or recurring time schedule. One time schedule is applied only once for the specified period in the schedule, recurring time schedule are applied repeatedly at specified times.

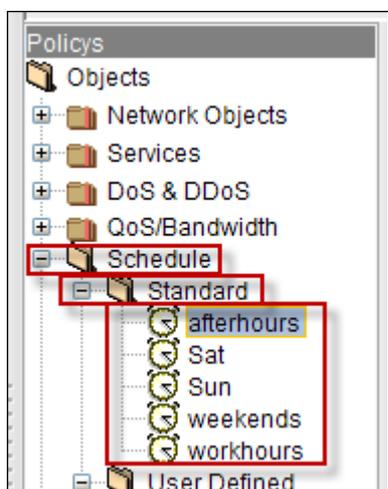


Standard

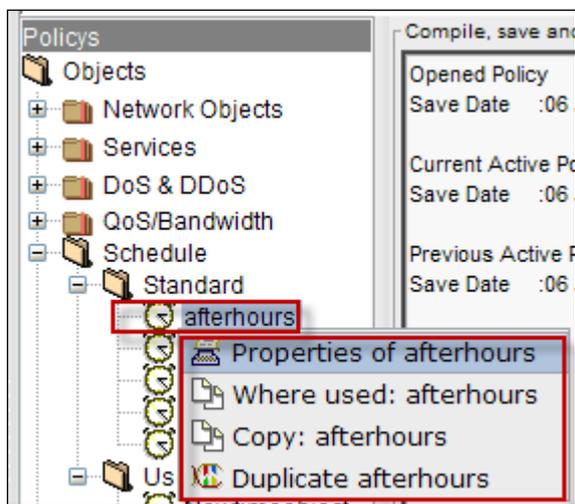
Expand schedule, **Standard** and **User Defined** is displayed.



Expand **standard**, by default some schedule objects are displayed under **Standard Schedule**.

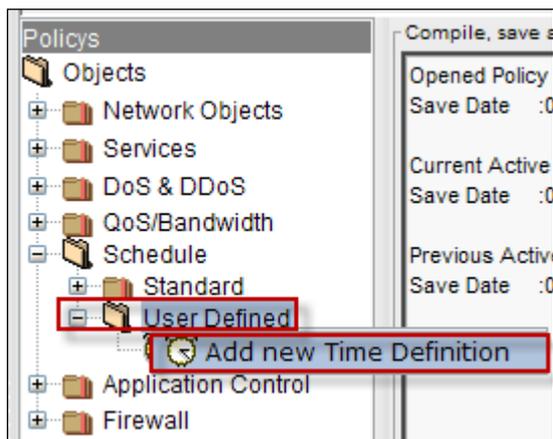


Right click on the schedule object, to perform actions like viewing **Properties** of the Schedule object, to find out where it is used, **copying** object, **Duplicating** and **Deleting** Schedule object.



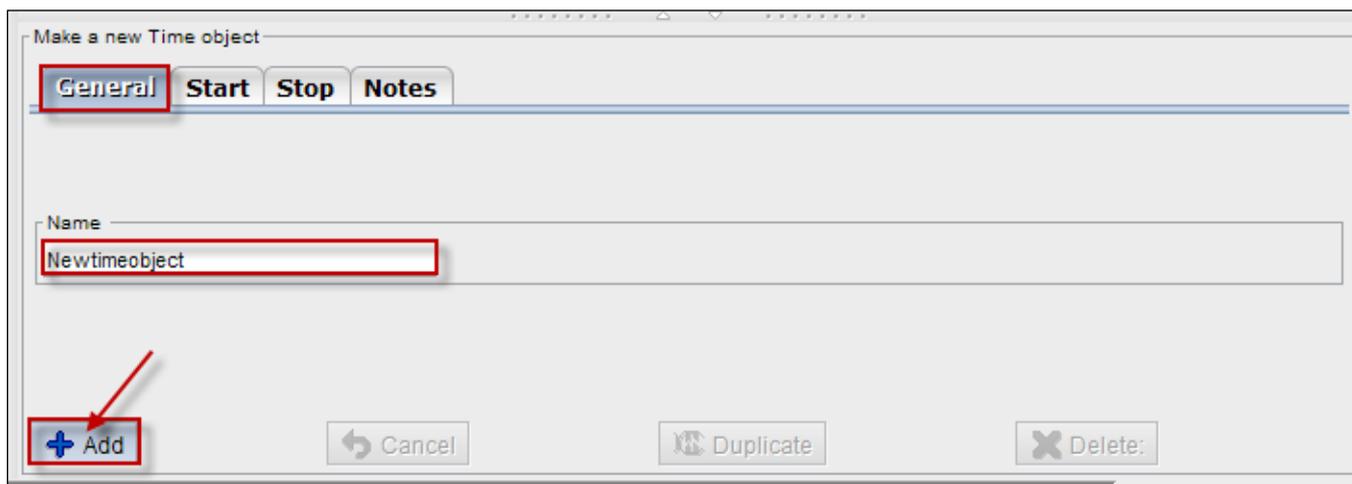
50. User Defined

Right click on **User Defined** to Add new Time Definition.



General

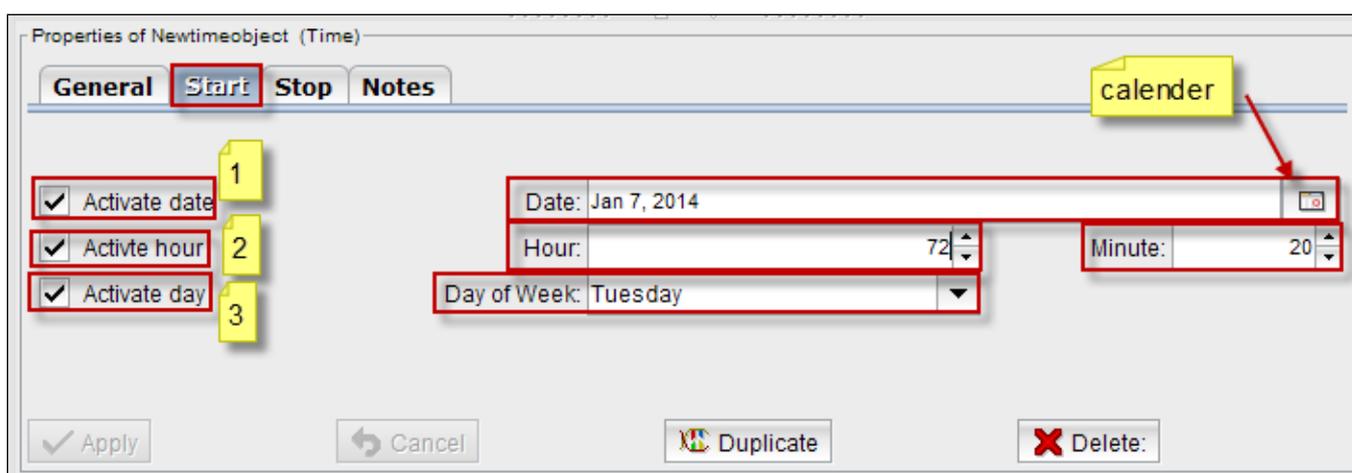
Select General tab, Give the name of new time Object in the Name field.



Click on **Add tab**.

Start

Schedule object start time should be mentioned in this section, select **Start** tab.



These are the inputs for Start

1	Active date	Enable Active date to choose start date from the calendar
2	Active hour	Enable Active hour to choose starting hours and minutes
3	Active day	Enable Active day to choose starting day from drop down list

After choosing appropriate date, hour and day disable Active mode of date, hour, day and click on **Apply tab**

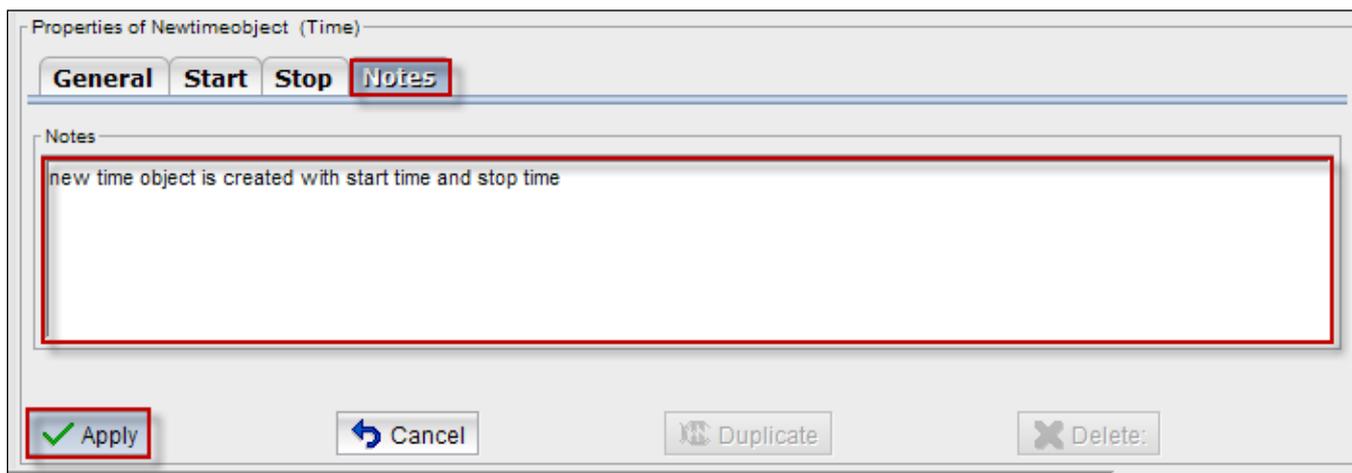
Stop

Schedule object stop time should be mentioned in this section, select **Stop** tab.

1	Active date	Enable Active date to choose stop date from calendar
2	Active hour	Disable Active hour for not mentioning stop hour and minutes
3	Active day	Enable Active day to choose week day

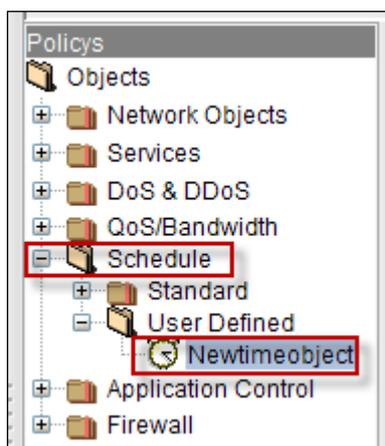
Notes

Select **Notes** tab, to write necessary information regarding time Object.

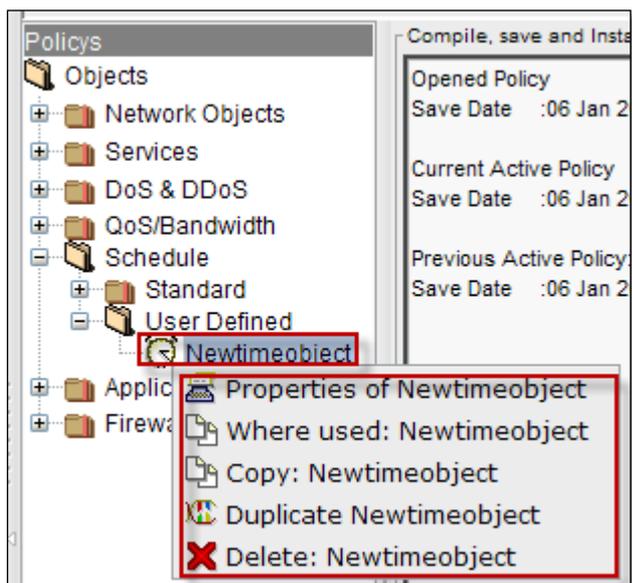


Click on **Apply** tab.

We can notice new time Object in the below screen.



Right click on the schedule object, to perform actions like viewing **Properties** of the Schedule object, to find out where it is used, **copying** object, **Duplicating** and **Deleting** Schedule object.



51. Application Control

Using Application Control in firewall enables us to block applications based on Users or User Groups. So, that you can control risky port and protocol hopping applications before they get in. You can also reduce your attacks surface by enforcing mobile applications and social media application policies. You can even control bandwidth

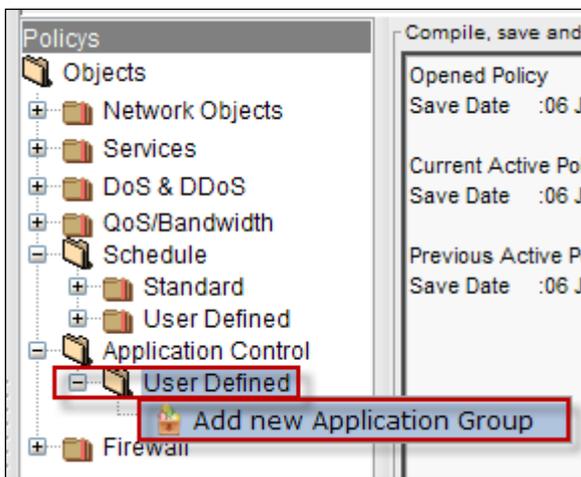


User Defined

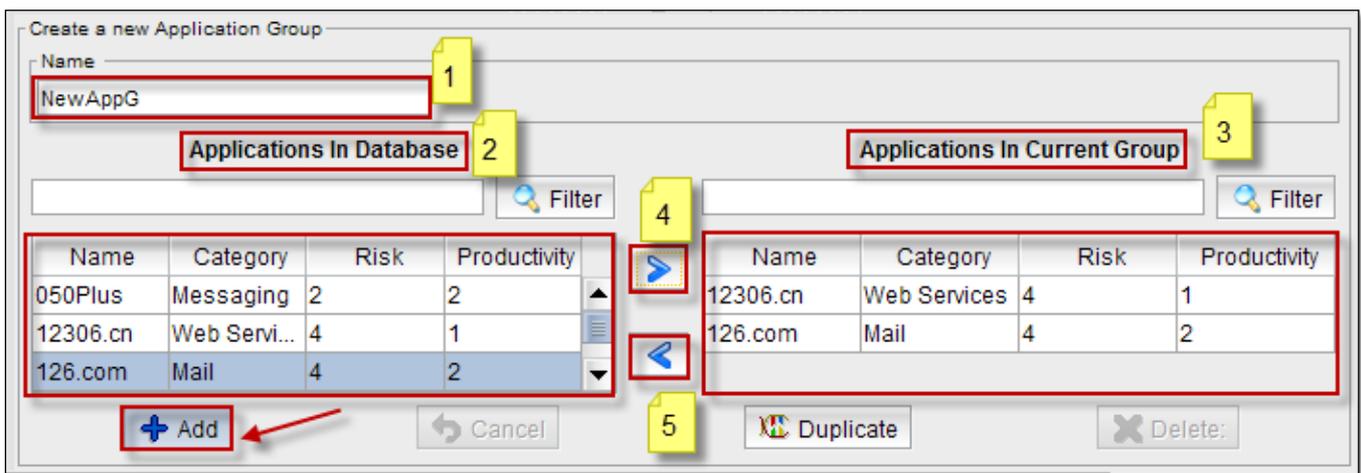
Expand Application Control, by default User Defined is displayed.



Right click on **User Defined** to add new Application Group.



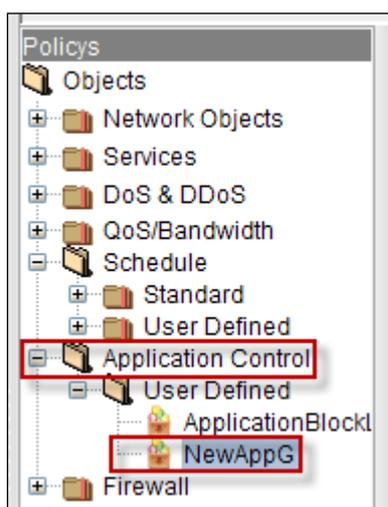
Creating new application group



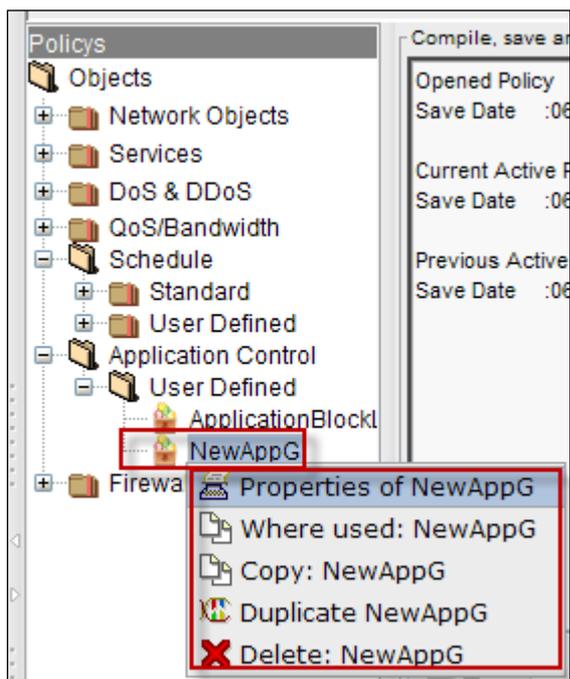
These are the inputs for new Application Group.

1	Name	Type the name of the Application Group
2	Application in Database	It displays list of Application in Database
3	Application in Current Group	It displays list of Applications in Current Group
4		This symbol enables to add Applications in to Current Group from Database
5		This symbol enables to remove Applications from Current Group to Database

In the below screen we can notice new Application Group.



Right click on the Application Group, to perform actions like viewing **Properties** of the Application Group, to find out where it is used, **copying** Application Group, **Duplicating** and **Deleting** Application Group.



52. Firewall

Firewall is a concept which blocks unwanted traffic and passes desirable traffic to and from both sides of the network.

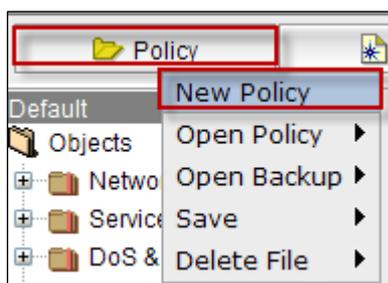
A firewall is a system (either software or hardware or both) that enforces an access control policy between two networks.

Example:

- Allows: http, mails etc
- Keeps out : Intruders ,Denial of services attacks, spam etc.

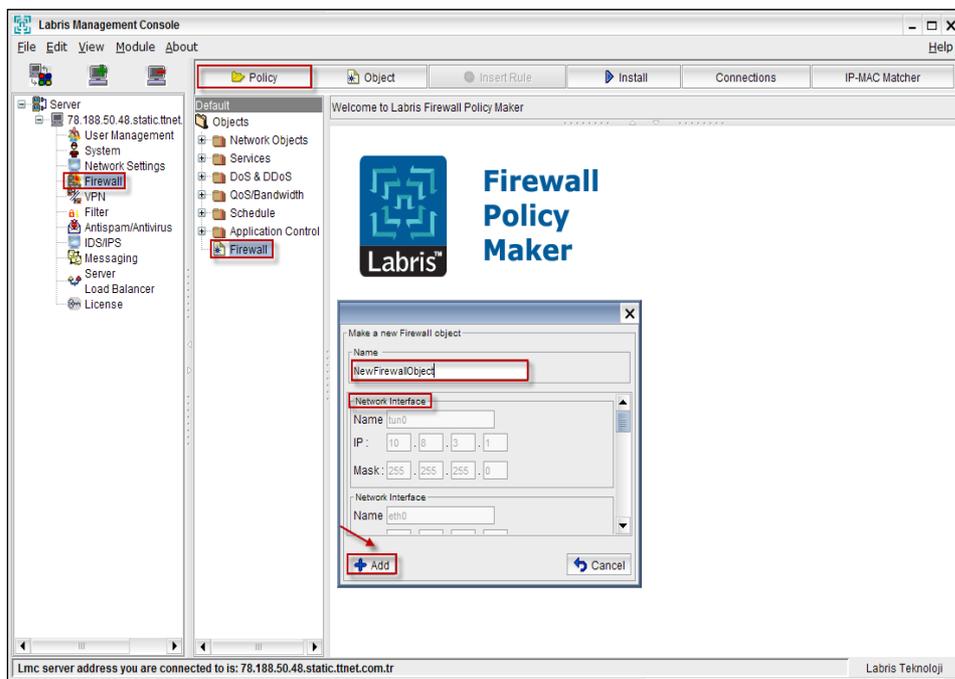
53. Labris Firewall Management

Install, Save (create a new policy object for first setup), Install Policy

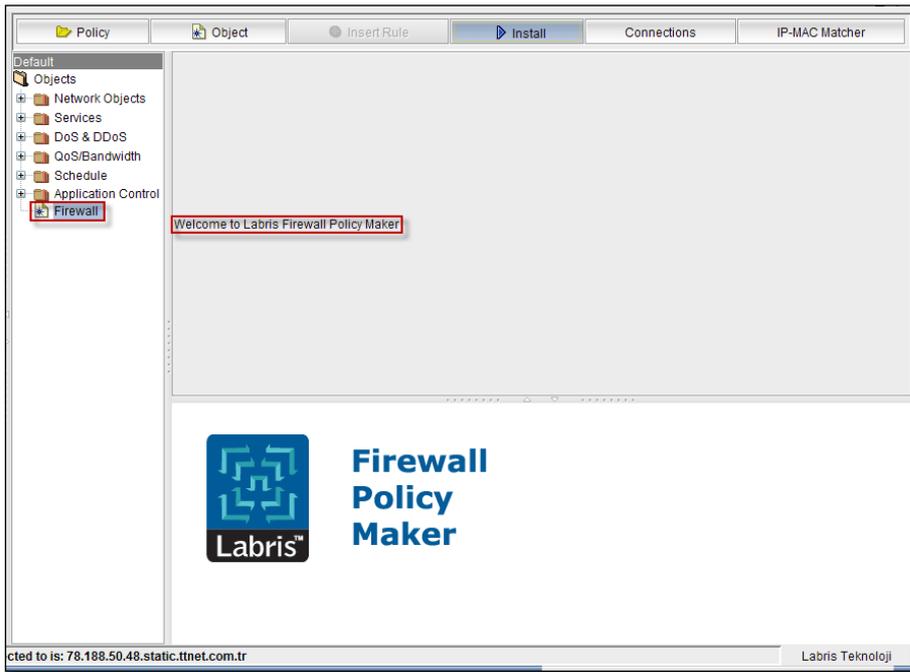


Creating new policy firewall object

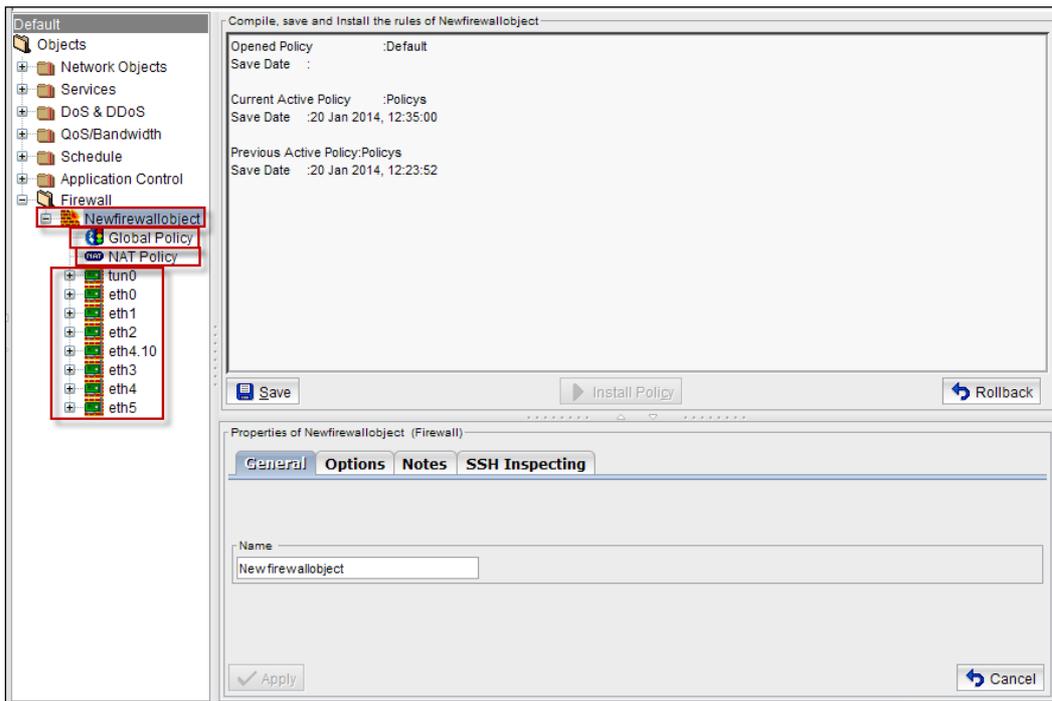
Give the **Name** of the Object in the Name tab, by default Network Interfaces have been selected for the new firewall object and click on **Add** tab.



Below screen appears stating **Welcome to Labris Firewall Policy Maker.**



Now we have created a new firewall object and we will configure it now.



Add Next Generation Firewall

First step:

Create Global policies

Global policy

Global policies in one logical system are in a separate context than other security policies. According to the source from the target set on the way to the Objects or forbids. In addition, these rules can be imported from the previously created Network Objects(Hosts, Networks, Addresses, Address Ranges, Object Groups and Users), Services (ICMP,IP,TCP,UDP, Custom, Service Group), DoS/DDoS Objects, QoS(Bandwidth Management) Objects can be added to the schedule Objects for controlling application profiles.

Second step:

Create NAT Policies

NAT Policy

NAT: It is a service of routing provides network address translation from private to public

When we have 2 networks public & private in order to protect private network from public network (intruders) we need NAT.

NAT enables one way communication. i.e. private network can communicate with public network but not vice versa.

NAT policies

It allows you to control Network Address Translation based on matching combinations of Source IP address, Destination IP address, and Destination Services.

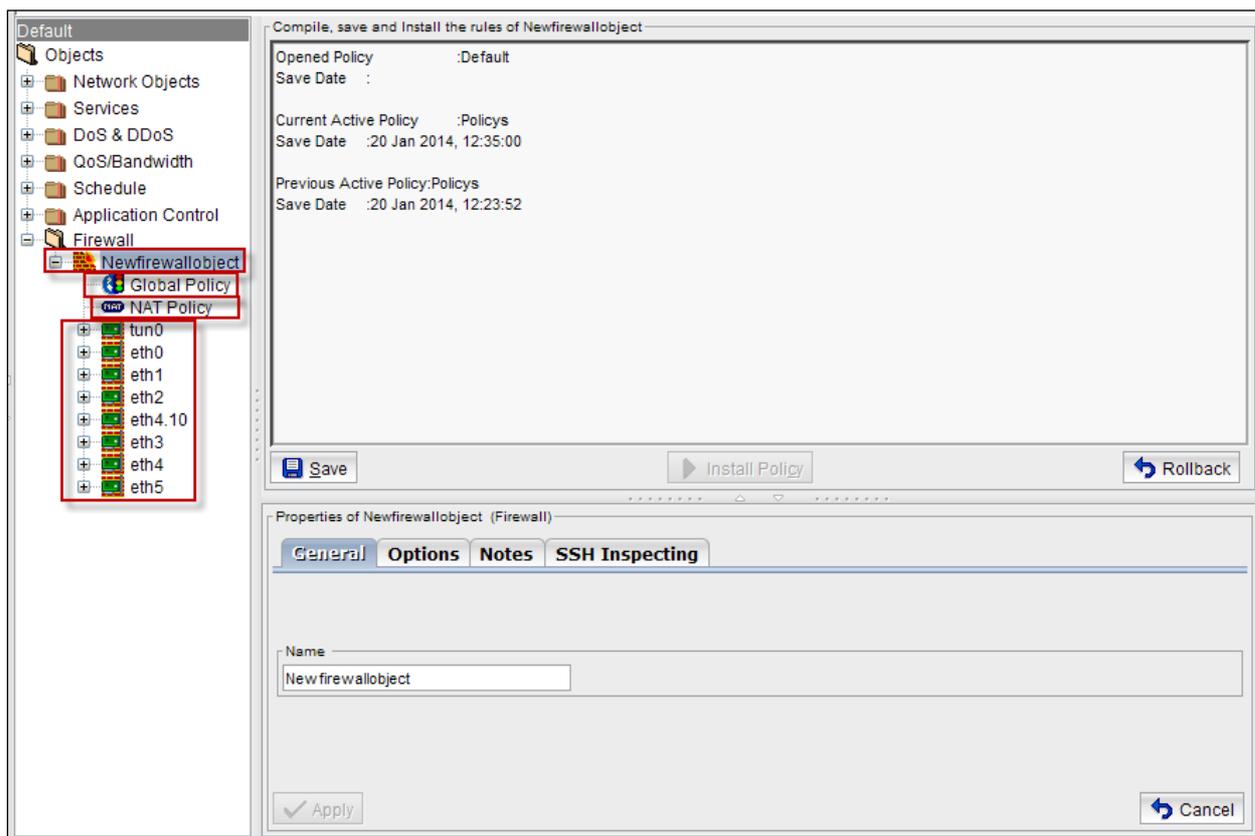
For example, a lot of the IP subnet address from internal network will route to outside network with single IP address.

Third step:

Physical interfaces

The physical interface that are supported by the device and subsequently added to the interface listed in the area.

This field contains the interfaces for the WAUTH interface, Dynamic source address translation interface, and the external network interface definitions.



Firewall Properties

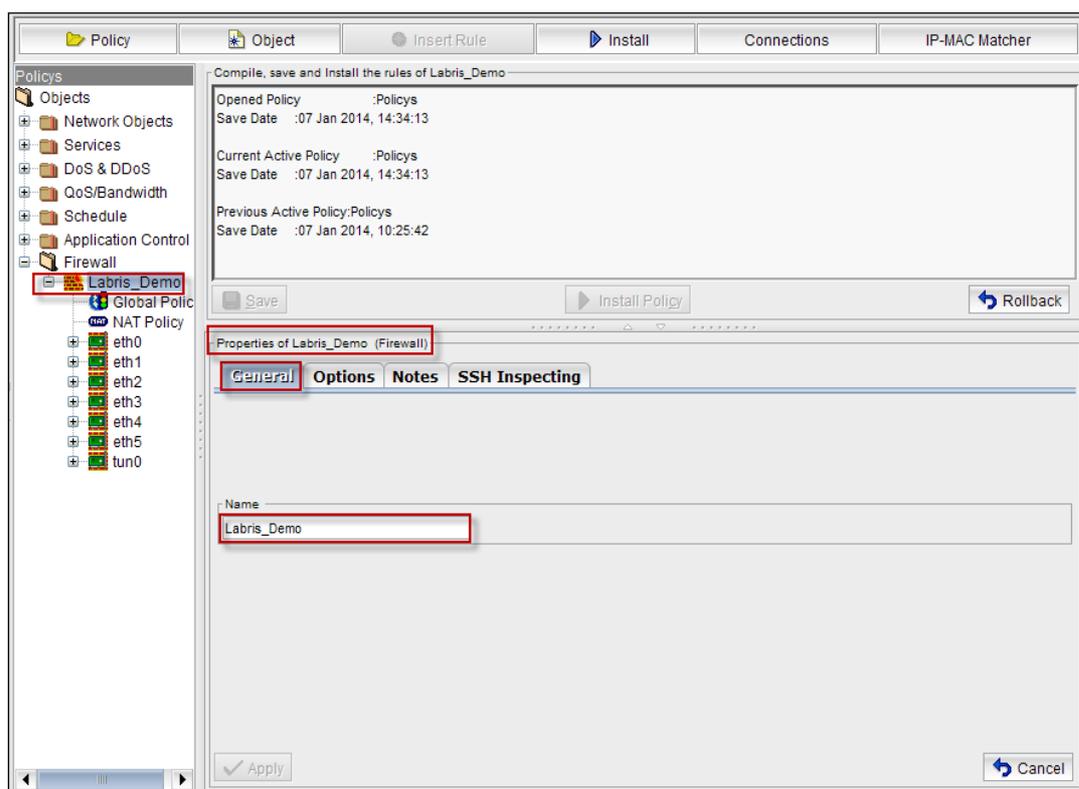
- **Interface** - Use this property to match which network port or data link packet is traversing such as "eth0" for Ethernet built-in.
- **Source MAC Address** - Use this property to specify an Ethernet Hardware Address that matches the source MAC (Media Access Control) address in the link layer frame header.
- **Destination MAC Address** - Use this property to specify an Ethernet **Hardware Address that matches the destination MAC (Media Access Control)** address in the link layer frame header.
- **Source Net** - Use this property to specify a single IP address or network range that matches the source IP address of a packets IP header.
- **Destination Net** - use this property to specify a single IP address or network range that matches the destination IP address of a packets IP header Network ranges can be specified as address1-address2.
- **Protocol** - Use this property to specify the protocol number that appears in a packets IP header.
- **IP Options** - Use this property to specify the IP option numbers that appear in a packets IP header.
- **ICMP Type** - Use this property to specify the ICMP type that appears in a packets ICMP header.
- **ICMP Code** - Use this property to specify the ICMP code that appears in a packets ICMP header.

- **TCP Header Flags** - Use this property to specify the TCP header flags that appear in a packets of TCP header.
- **TCP Options** - Use this property to specify the TCP option numbers that appear in a packetsof TCP header.
- **Destination Port** - Use this property to specify a single protocol port or range of protocol ports that matches the destination port of a packets TCP or UDP header. Port ranges can be specified as port1-port2.
- **URL Keyword** - Use this property to search for keywords that appear within a HTTP (web site) URL.
- **Parent Match Count** - Use this property to notify you if the parent rule has been matched a specified number of times.
- **Parent Byte Count** - Use this property to notify you if the parent rule has been matched by network traffic containing a specified number of bytes.

Right click on Firewall object to view Properties of firewall object.

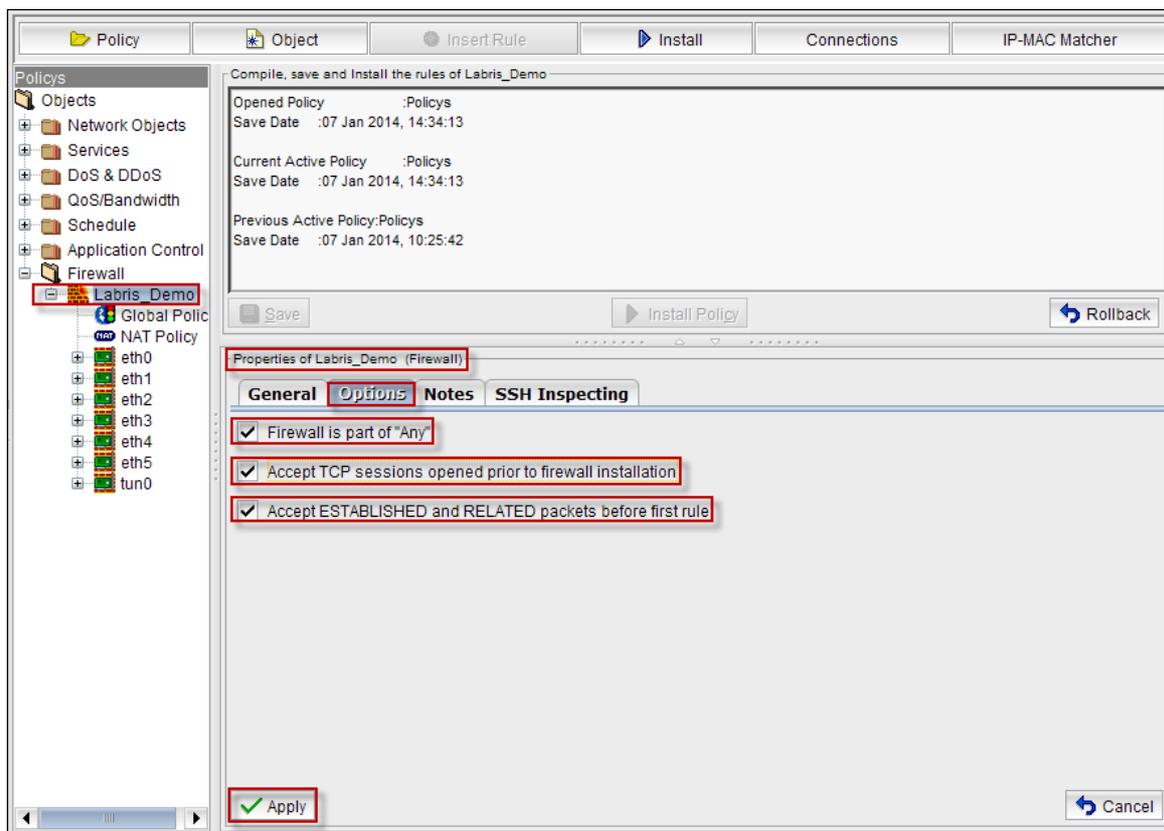
Select **General tab** to view details about Name of the Firewall object.

We can change name and click on Apply tab to change the name.



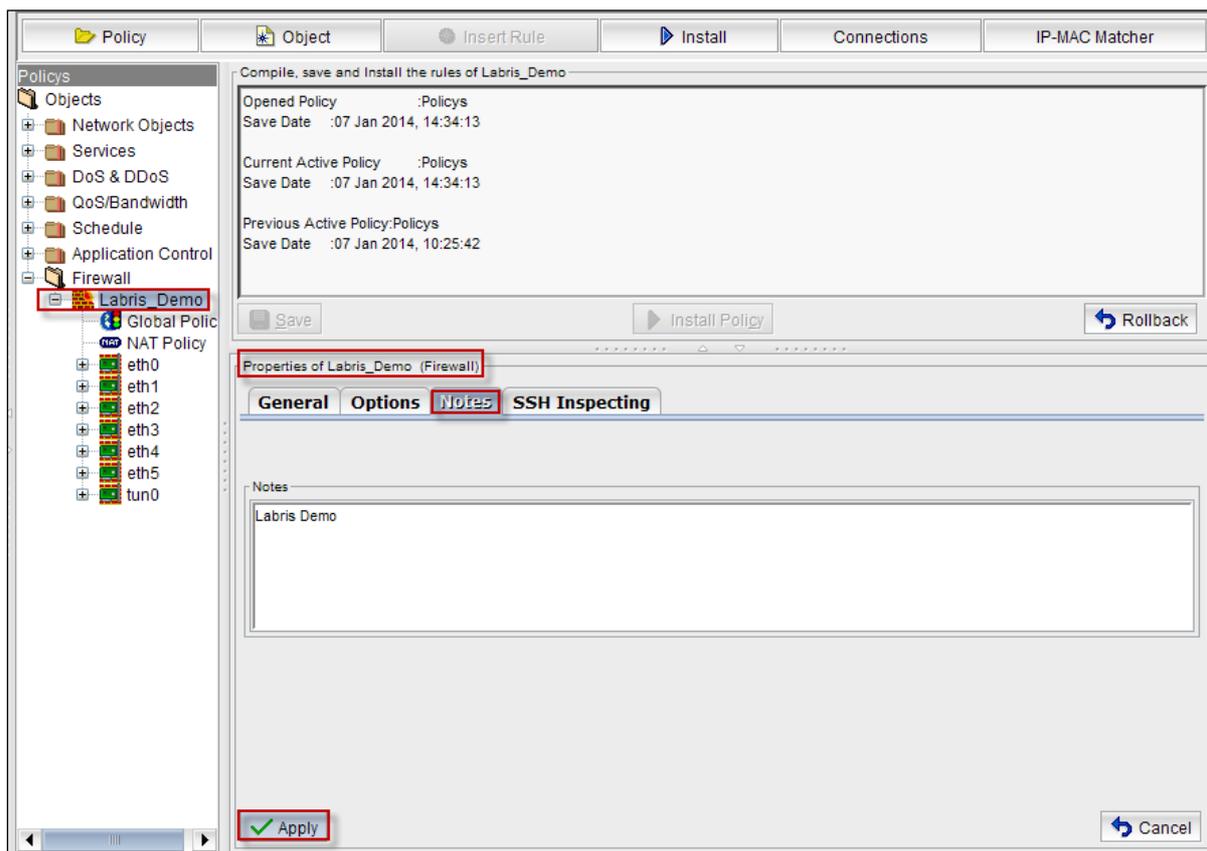
Select **Options tab**.

We can Enable or Disable Options **Firewall is part of “ANY”**, **Accept TCP sessions opened prior to firewall installation**, **Accept ESTABLISHED and RELATED packets before first rule**.



Click on **Apply** tab to apply changes to the firewall object.

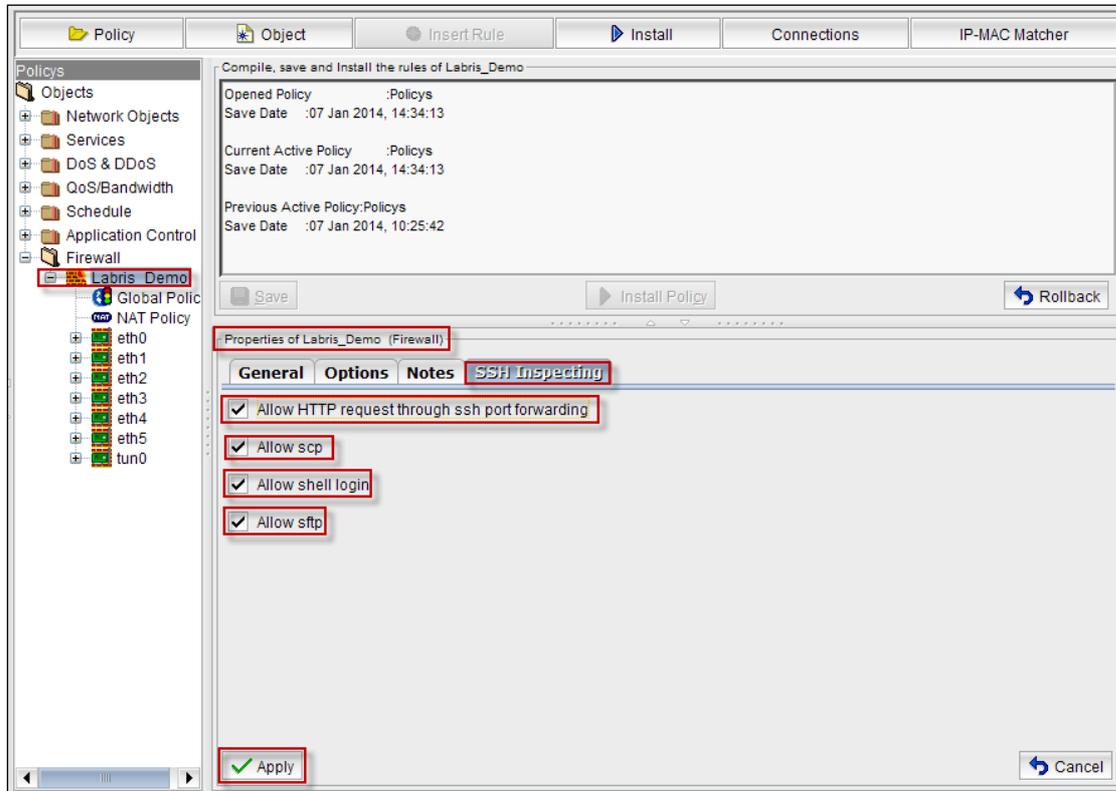
Select **Notes** tab to write information regarding firewall object (Optional).



Click on **Apply** tab to apply changes.

Select SSH Inspecting tab

We can Enable or Disable **Allow HTTP request through SSH port forwarding, Allow SCP, Allow shell login, Allow sftp.**



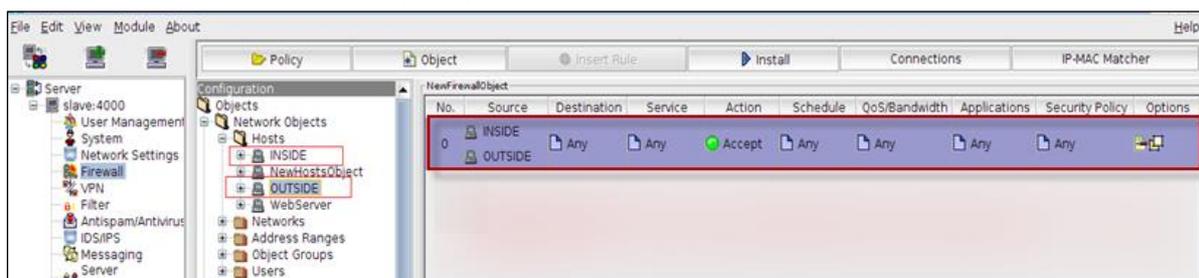
Click on **Apply** tab to apply changes

Global Policy table

Global policy table is displayed with the fields **Source, Destination, Service, Action, Schedule, QoS/Bandwidth, Application, Security policy, Options.**

How to add new Global policy? And what can be done?

Example1: My host objects for policy

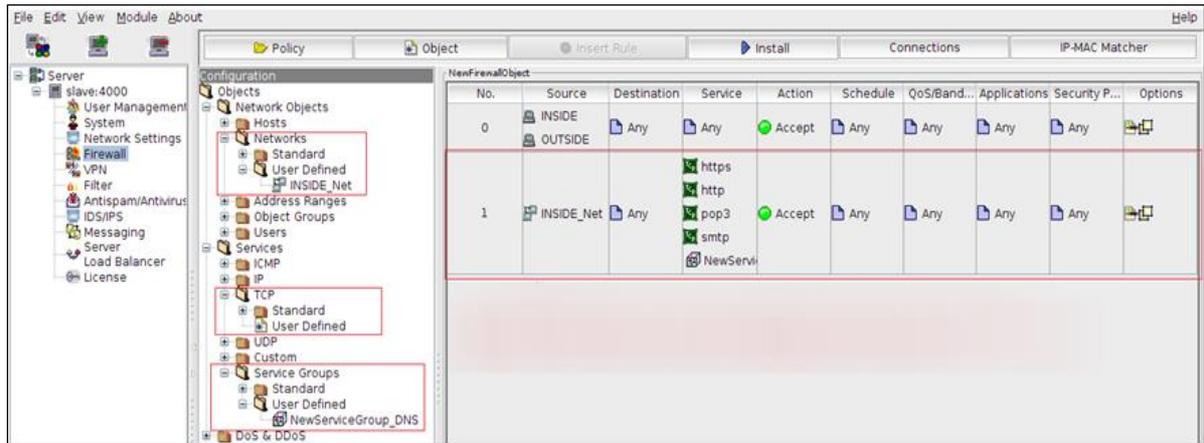


My global policy

In the above screen we can notice columns such as Source, Destination, Service, Action, Schedule, QoS/Bandwidth, Application, Security Policy, Options.

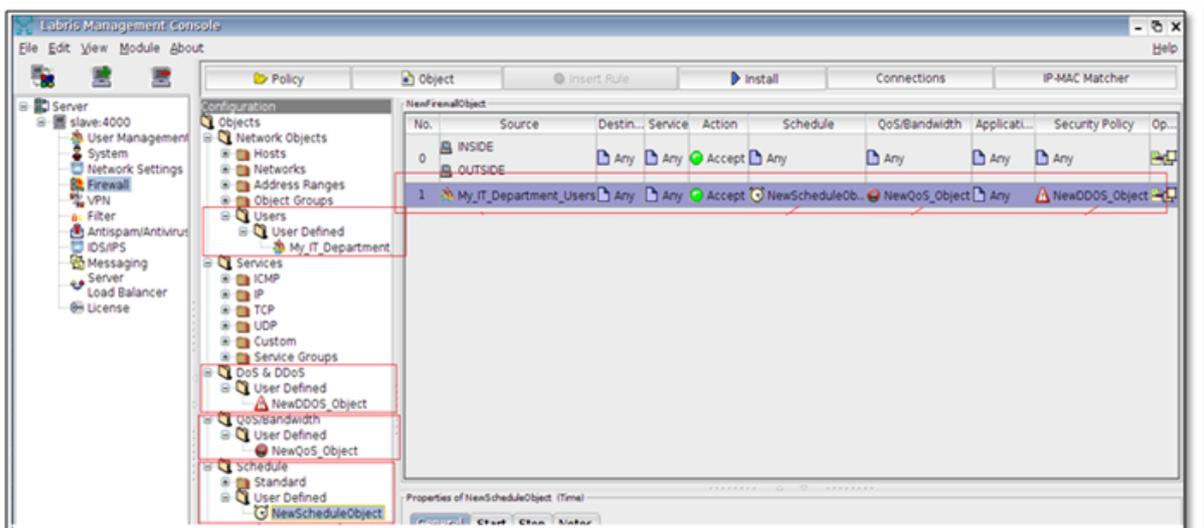
Application is allowed if the created Source with interfaces INSIDE & OUTSIDE is accessed, and when the Destination, Service, Schedule, QoS/Bandwidth, Application, Security Policy options are Selected as ANY. We can even drag-and-drop the desired objects created earlier, or copy and paste can be added with it.

Example 2: My network objects for policy.



All of the destinations on the IP addresses of the source of the rule INSIDE_Net with access to only the specified services. This rule also holds at their outer radio marker internal IP addresses on the policy.

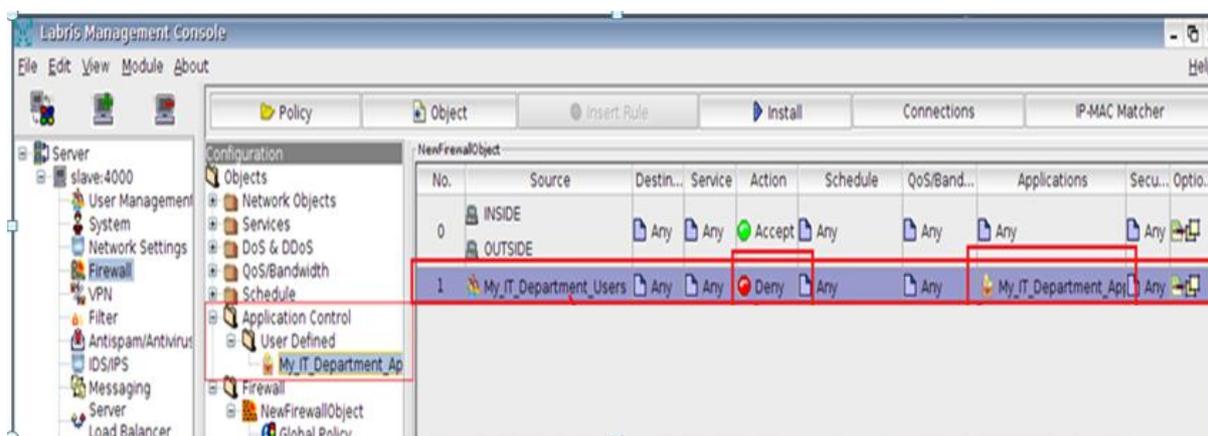
Example 3: How do we add a rule for users and My.applicaition.info.stacktrace users with QoS, control, DDOS and schedule how do we apply.



The rule previously created users ((For creating users please refer to **users section in User Management**) in the same way as the example demonstrates how to use the drop-down with

the yerede rule, let's link the current field) and user network appeal (For adding users in Network objects please refer to **users field in Network Objects Section**)owed as the source, and again before our Schedule-appeal (Please refer to **Schedule section in Network Objects** and the link in the same was the example demonstrates how to use the drop-down with the yerede rule, let's link the current field),QoS-appeal (Please refer to **Qos/Bandwidth section in Network Objects** here's the link and the link in the same way as the example demonstrates how to use the rule drop down yerede with the current field link), and DoS/DDoS previously created object located at the source by placing the user in the appropriate fields in the rule or the rope according to the specified criteria.

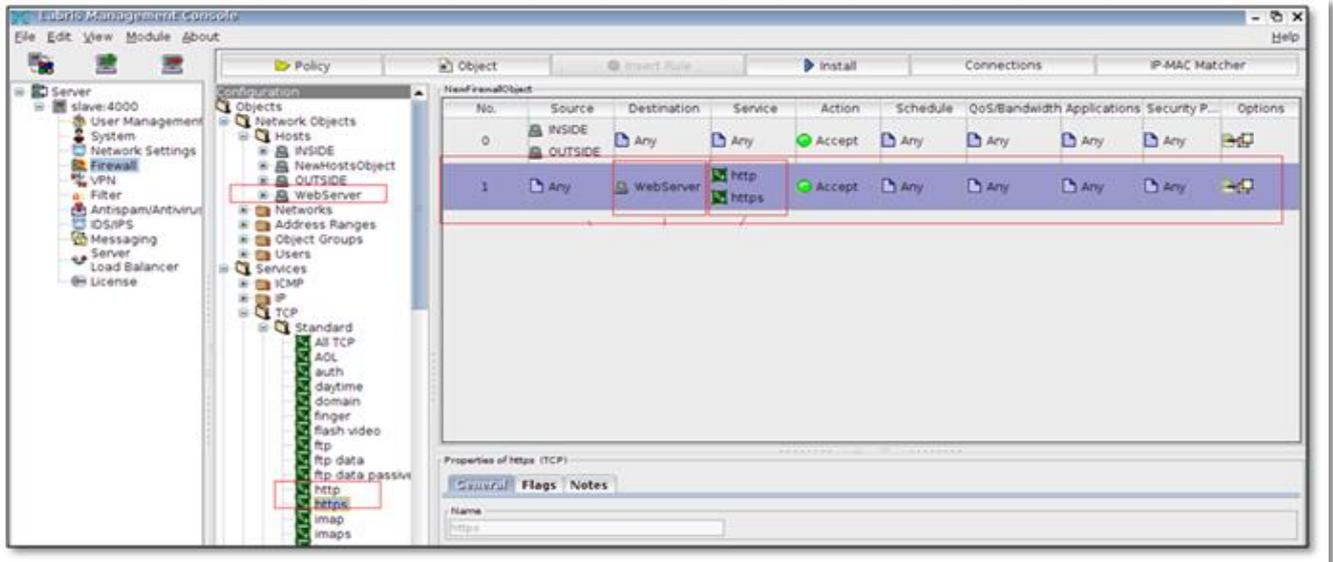
How to add an application control rule for users?



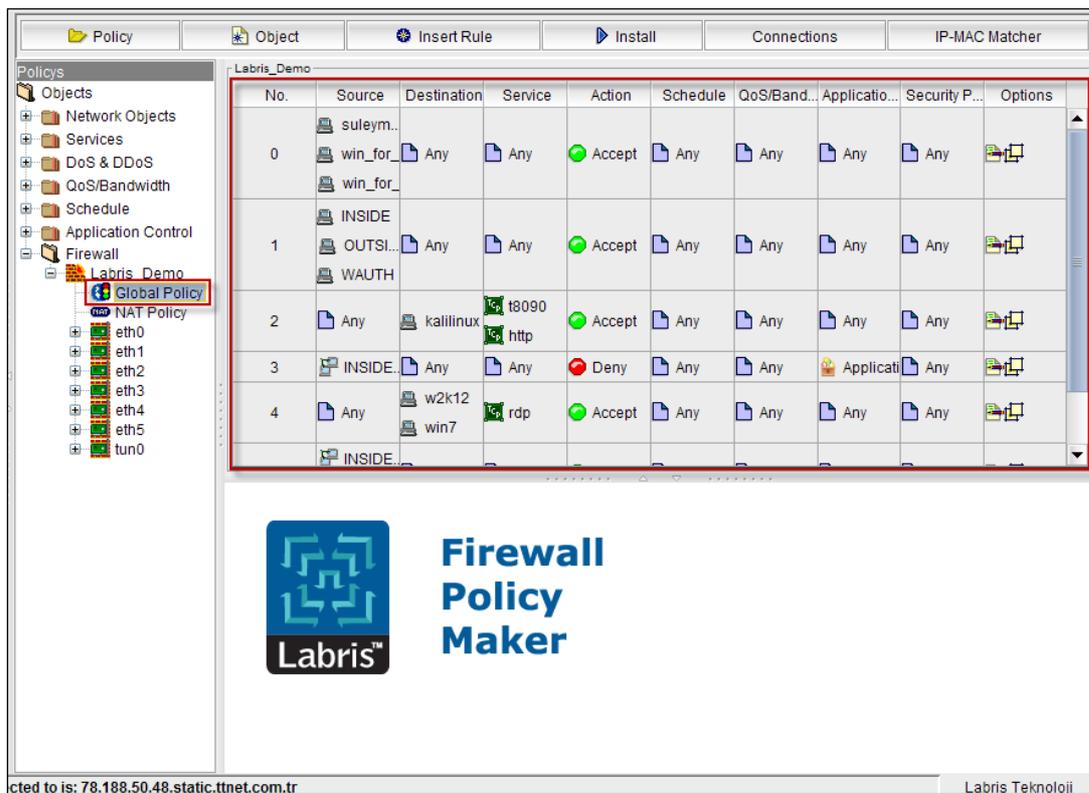
The rule previously created users ((For creating users please refer to **users section in User Management**) and here is the link in the same way as the example demonstrates how to use the drop-down with the yerede rule, let's link the current field) and Application control profile (Please refer to **Application control section in Network Objects** and here is the link in the same way as the example demonstrates how to use the drop-down with the yerede rule, let's link the current field).

Read all the rules in the table. Buy why you must be careful when writing the canonical ordering Application control. If the source specified in the rule is a rule used in the queues and objects in higher action has been ruling on the accept or deny rule.

Example 4: The outside should be accessed with specific protocols for access to the web or other services to the rule writing. And create a new NAT policy (NAT policy Please refer Example2)



For example, one in which each web server and outside a place gave over to access http and https protocols. The source column of the address will be "any", which is the target column because the target to a specific server to be accepted through the "host object" (for creating **hosts object** Please refer to **Hosts field** in **Network object** section here is the link to give the host object will be created in the same manner as the host and the creation stage of the policy section and use the example currently in the link).

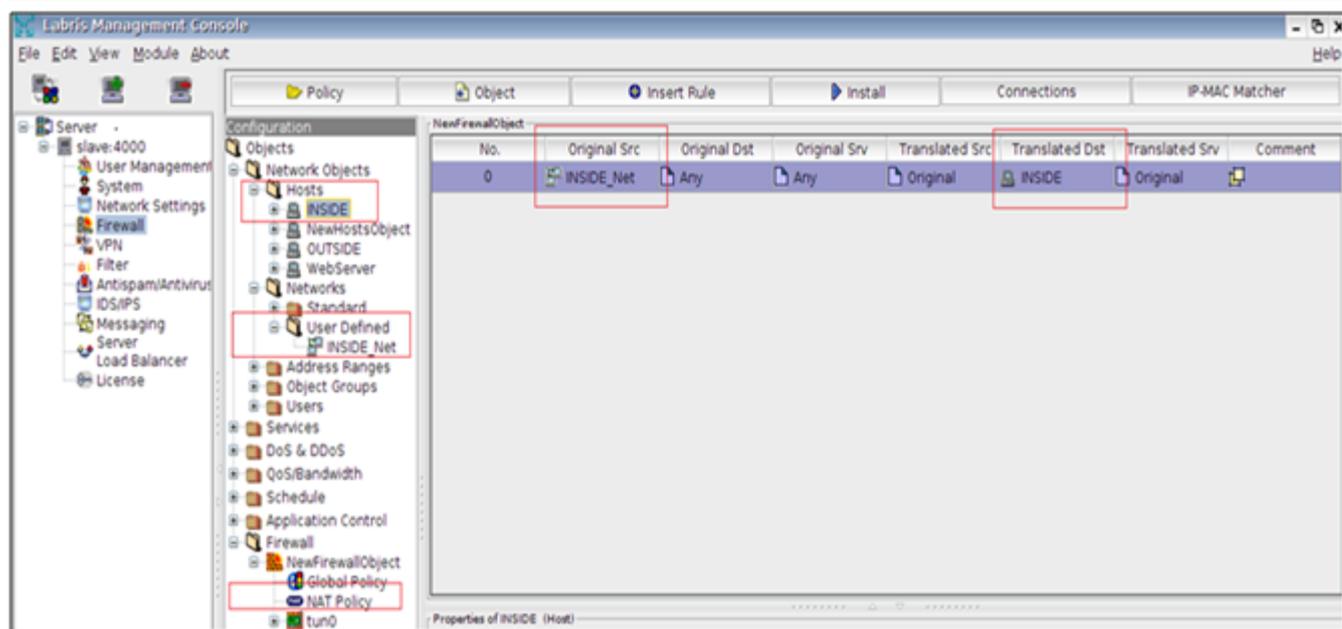


NAT (Network Address Translate) Policy table

NAT Policy table is displayed with the fields **Original Src, Original Dst, Original Srv, Translated Src, Translated Dst, Translated Srv, Comment.**

In this section, in accordance with the global policy also created the device permissions, changing the status of the source, destination, and services will write the rules.

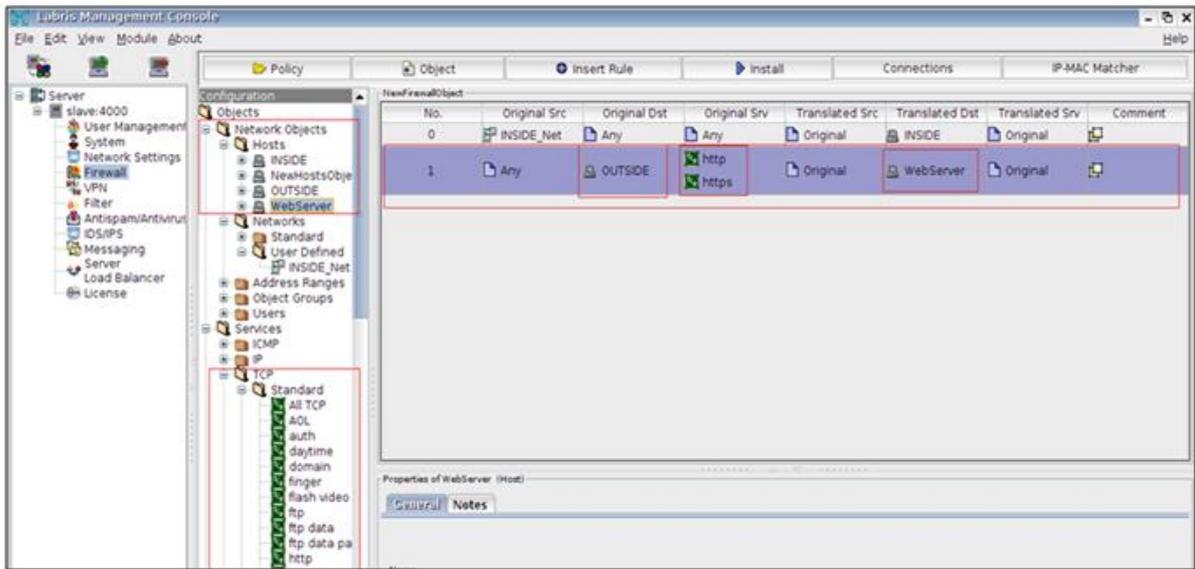
Example1: Internet NAT policy



For example, a lot of the IP subnet address my device contains and leave all our internet users out of their IP addresses through a single IP address we need over. So we have to translate the network address.

IP subnet is 255.255.255.0 and your default gateway is 192.168.168.1 and 192.168.168.0 considering the need to build rule my IP Address; a of range IP address and target the source 192.168.168.0 255.255.255.0 on the Internet as a place to which "any" and all the services in the same way that any change in the subverted will be converted to the destination address in the above policy, such as changing to run assuming the IP address. In our example, changing IP address is 192.168.168.1

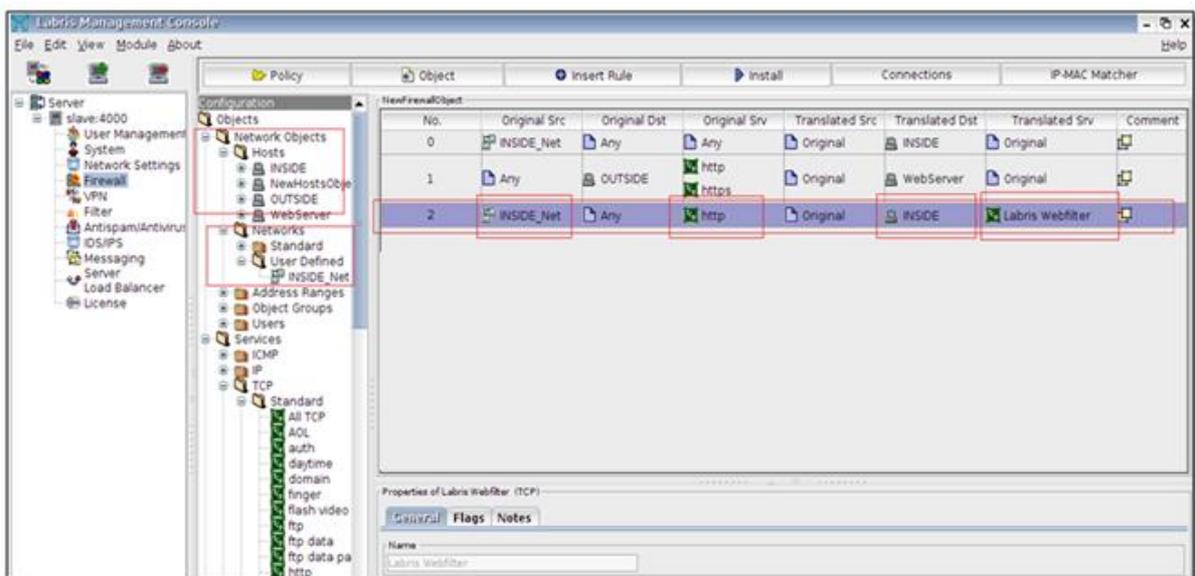
Example2: Web server access from Wide Area Network.



Any source outside web server "any" http and https access to the supplier global policy is written as (For **global policy** please refer to **ADD Next generation firewall** section) and later to the server on specific ports from outside should identify which requests inside.

Example 3: Web Filter service enables.

Internet web filter service requests that returning web filtering. The following rule is written to the NAT policy.



The resources specified in the rule, the user/user group, IP addresses/IP range, in the case of http service running on the device to web subnet, IP filter rule is required to be sent to the service. This rule should be written to all devices with web filtering. (For web filter please refer

to **Filters section** here is the link to the web filter also web filter configuration screens to give the link).

The screenshot displays the Labris Firewall Policy Maker interface. On the left, a tree view shows the configuration hierarchy: Policies > Firewall > Labris_Demo > Global Policy > NAT Policy. The main area shows a table of NAT rules for the 'Labris_Demo' policy. The table has columns for No., Original Src, Original Dst, Original Srv, Translated Src, Translated Dst, Translated Srv, and Comment. Rules 0, 1, and 5 are highlighted in yellow and marked with a red 'X' in the 'No.' column, indicating they are disabled. Rule 5 is a web filter rule for 'http' traffic from 'INSIDE_Net' to 'Any', translated to 'INSIDE' and 'Labris We...'. The interface also features a 'Policy' menu, 'Object', 'Insert Rule', 'Install', 'Connections', and 'IP-MAC Matcher' buttons at the top. The Labris logo and 'Firewall Policy Maker' text are visible at the bottom, along with the IP address 'ected to is: 78.188.50.48.static.ttnet.com.tr' and 'Labris Teknoloji'.

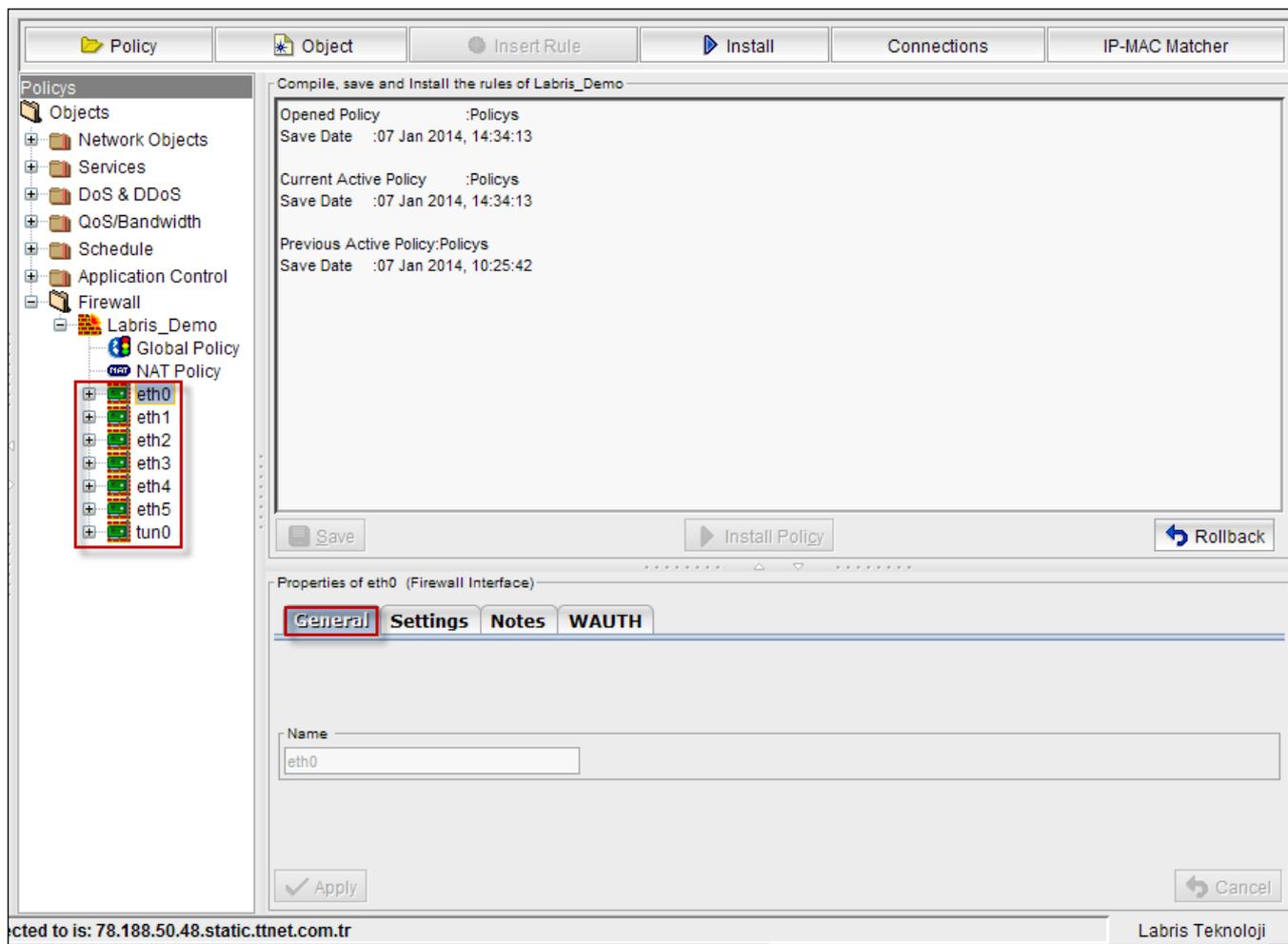
No.	Original Src	Original Dst	Original Srv	Translated Src	Translated Dst	Translated Srv	Comment
X 0	INSIDE_Net	routenet	Any	Original	Original	Original	
X 1	routenet	INSIDE_Net	Any	Original	Original	Original	
2	Any	OUTSIDE	http t8090	Original	kalilinux	Original	
3	Any	OUTSIDE	rdp	Original	w2k12	Original	
4	Any	OUTSIDE	win7rdp	Original	win7	rdp	
X 5	INSIDE_Net	Any	http	Original	INSIDE	Labris We...	
6	INSIDE_Net	Any	Any	OUTSIDE	Original	Original	

Interfaces

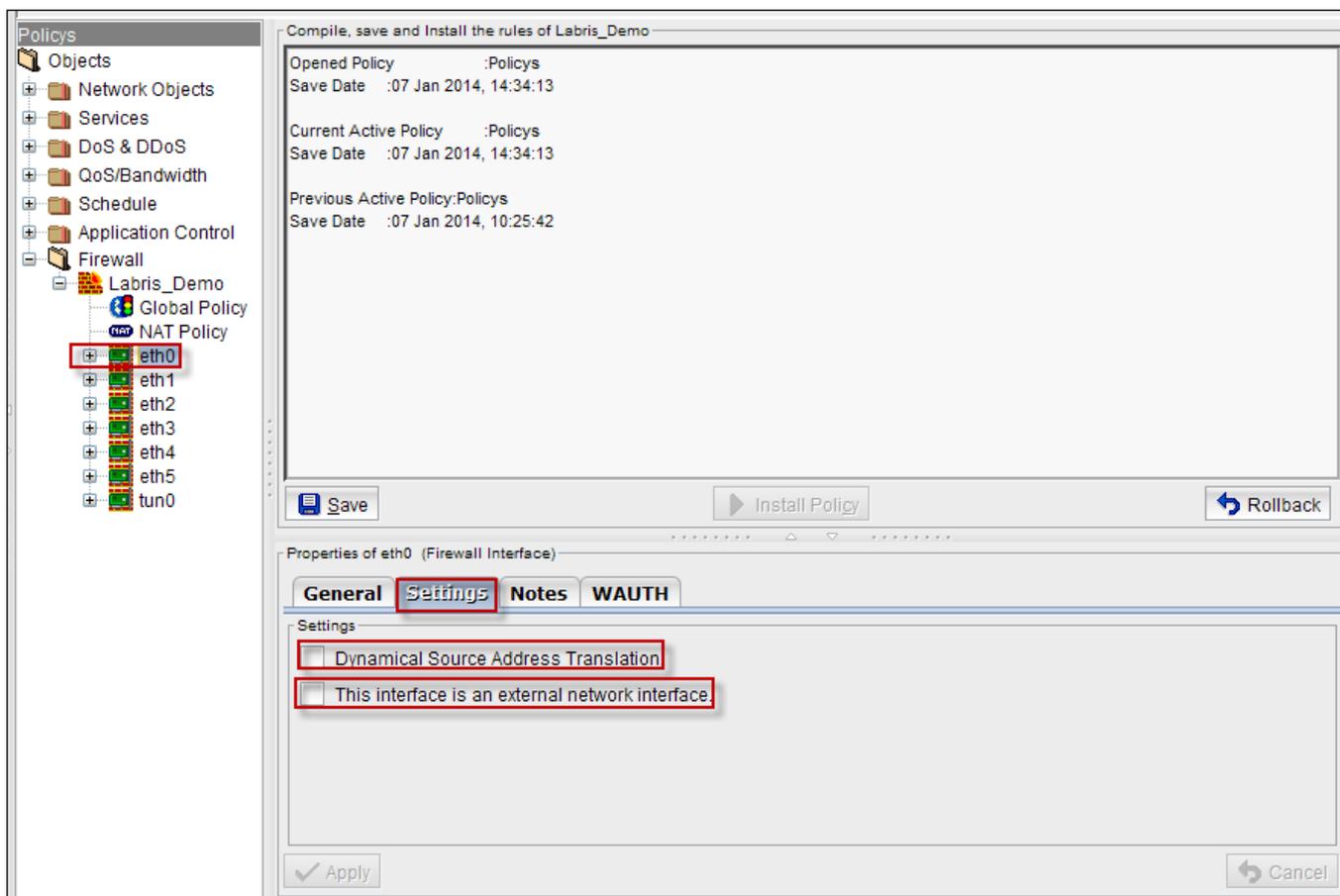
By default seven Interfaces are present in the firewall object.

They are **eth0, eth1, eth2, eth 3, eth4, eth5, tun0**.

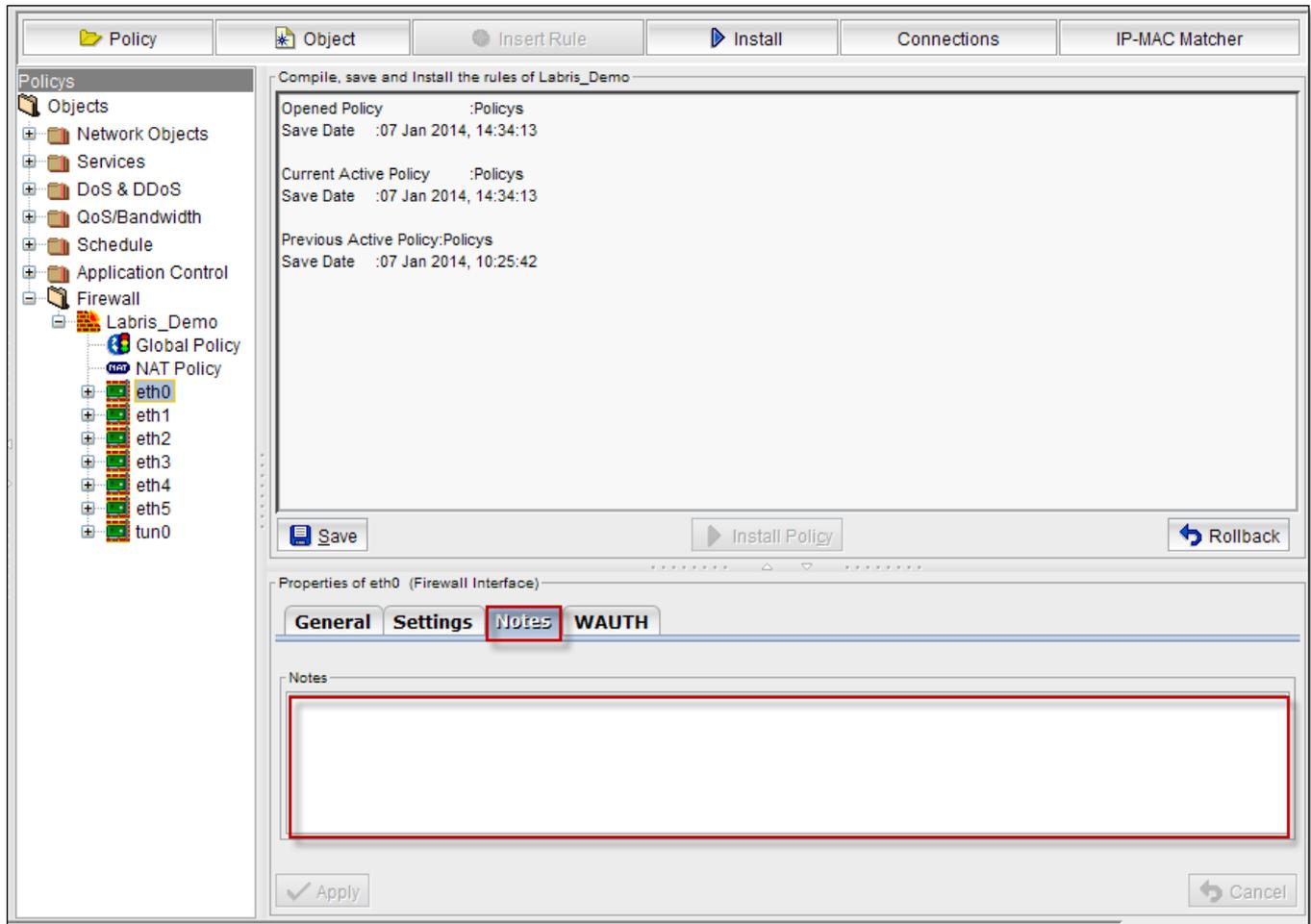
Select **General tab**, Name of the interface is displayed.



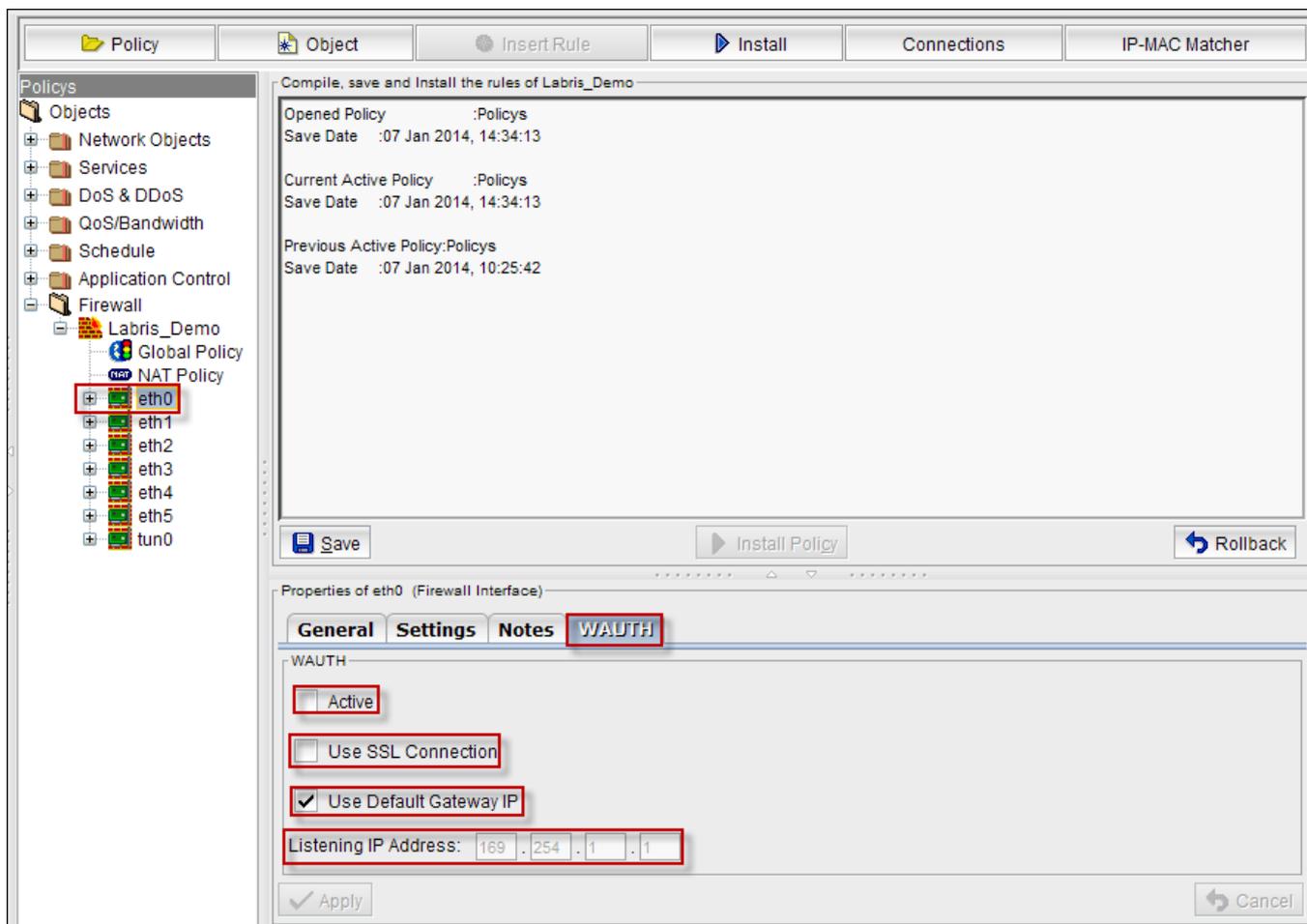
Select **Settings tab**, we can Enable or Disable **Dynamical source Address Translation**, This interface is an external network interface.



Select **Notes** tab, to write information regarding Interface (Optional).



Select WAUTH tab, we can enable or disable options like **Active**, **Use SSL Connection**, **Use Default Gateway IP**



Firewall Application

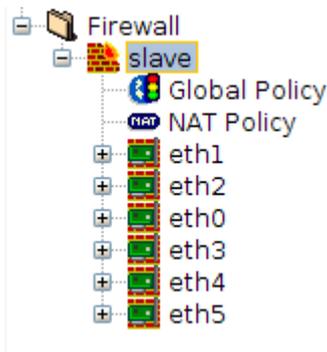
- The Web Application Firewall (WAF) protects applications from current and future security threats by combining multiple security engines into a cohesive Web defense.
- Not like a “normal” firewall- Applies rules to HTTP conversations
- Allow or deny based on expected input – Unexpected input is a common method of exploiting an application.
- SQL injection – Add your own commands to an application’s SQL query.
- A major focus of payment card industry, Data Security Standard (PCI DSS).

SSH Inspection

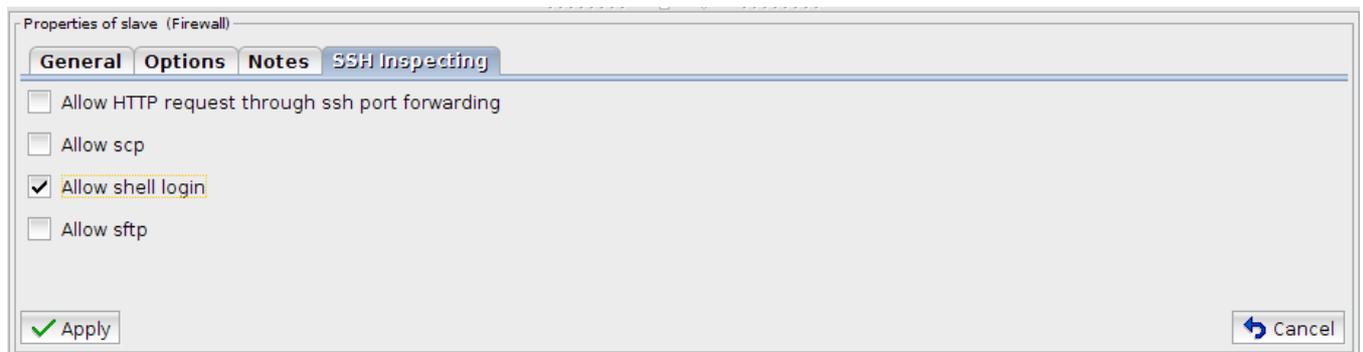
Labris SSH Inspector provides an easy and effective way to limit actions allowed over ssh. Its engine detects the internals of ssh traffic and allows administrators to manage and log ssh traffic in depth. Administrators can allow/block/log shell login, sftp, scp or HTTP request through ssh port forwarding.

Enabling SSH Inspection

SSH Inspection configuration is done in firewall object settings under **Firewall** module.



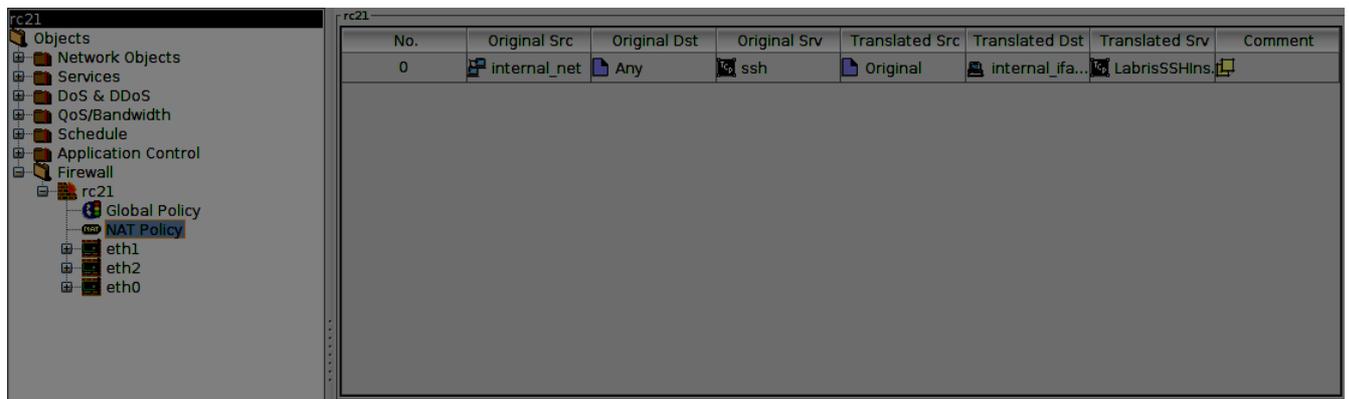
In firewall object properties administrators can choose which actions will be enabled in ssh traffic.



Restricting SSH Activities

In **Firewall** module under **NAT Policy** administrators decide which users will be redirected to SSH Inspector.

Administrators add users/hosts/networks to be restricted to Original Src of NAT rule, port number of SSH service to **Original Srv**, internal interface IP of restricted network to **Translated Dst** and port number of SSH Inspector to **Translated Srv**.



After installing NAT rule SSH traffic of users will be inspected by Labris SSH Inspector and unauthorized actions will be blocked.

Monitoring SSH Activities

SSH activities of users are logged under **/var/log/labris/sshinspection** and can be monitored by accessing Labris UTM over ssh.

```
root@rc21:~# tail -f /var/log/labris/sshinspection
Jul 17 11:48:44 2014 labris-ssh-inspector[28454]: source 10.0.0.2 53804 target 192.168.0.1 5632 action: 'shell login'
Jul 17 11:53:14 2014 labris-ssh-inspector[32745]: source 10.0.0.2 51128 target 192.168.0.198 5632 action: 'shell login'
Jul 17 11:53:31 2014 labris-ssh-inspector[32760]: source 10.0.0.2 51129 target 192.168.0.198 5632 action: 'shell login'
Jul 17 11:53:46 2014 labris-ssh-inspector[3131]: source 10.0.0.2 51130 target 192.168.0.198 5632 action: 'shell login'
Jul 17 11:54:22 2014 labris-ssh-inspector[1073]: source 10.0.0.2 51131 target 192.168.0.198 5632 action: 'scp login has blocked'
Jul 17 11:55:21 2014 labris-ssh-inspector[1503]: source 10.0.0.2 51132 target 192.168.0.198 5632 action: 'shell login'
Jul 17 11:55:34 2014 labris-ssh-inspector[1503]: source 10.0.0.2 51132 target 192.168.0.198 5632 action: 'http tunnelling has blocked'
Jul 17 12:35:34 2014 labris-ssh-inspector[27856]: source 10.0.0.2 51134 target 192.168.0.198 5632 action: 'sftp login has blocked'
```

Usage Notes About Labris SSH Inspector

- When using Labris SSH Inspector clients should accept Labris SSH Inspector's SSH key as their remote SSH server key.
- When using Labris SSH Inspector remote SSH key changes are not visible to clients behind Labris SSH Inspector.

Network Address Translate (NAT)

Network Address Translation is used to communicate the internal network to internet. It will be configured in the Router.

What is the NAT?

Network Address Translation is nothing but converting a group of computers IP Address to communicate or to send the packets to the outside of the world through the internet. Whenever the host computer in a Network need to send packets to the other internet user it will be possible through the Router. In the router it must be configured for the communication between outside of the internet user and host computer in a company LAN Network. The router only will take care the changes in IP address whenever sending and receiving the packets to and from outside of the network and internal LAN. It will be configured in Router in a table.

Why it is made?

In the whole world there are billions of computers. For communication between them they need unique IP Address like our street numbers and door numbers .NAT is a network protocol used in IPv4 networks that allows multiple devices to connect to a public network using the same public IPv4 address. NAT was originally designed in an attempt to help conserve IPv4 addresses. NAT has become a common, indispensable feature in routers for home and small-office Internet connections.

NAT Types

There are three types of NAT

SNAT

Static NAT: In this type, host computer will have particular IP Address to communicate with outside network. It is used for one device to communicate with outside network.

DNAT

Dynamic NAT: In this type, Router will assign the IP Address to communicate with outside network. It is used for communication of group of computers with outside network.

PAT

PAT (Port Address Translation): This is the type of dynamic, but it will map multiple unregistered IP Addresses to registered single IP Address using port numbers called Port Address Translation.

Port Forwarding/Port Mapping

Port Forwarding is also known as Port Mapping is the process that a router uses to sort the right kind of network data to the right port. Computers and routers use ports as a way to organize network data. Different types of data, like web sites, file downloads, and online games, each are assigned a port number. The router or firewall uses forwarding to send the correct data to the correct place.

A firewall protects a computer by blocking unauthorized information, but if a firewall blocked all the incoming and outgoing data, the computer would be unable to access the Internet. When a computer user wants some data to go through the firewall and to send it to a specific location, he can set up port forwarding. This gives the firewall instructions about which types of data are allowed and how they should be directed.

Information on the Internet is associated with a port. Web pages, for example, are typically assigned port 80. File transfer protocol (FTP), often used for downloading and uploading files, typically uses port 21. Online games may use a number of different port numbers, but often choose numbers in the thousands.

Port forwarding also serves as another way to protect computers. People outside the network will only have access to the router or firewall, which will, in turn, control which types of data reach the computers. Any data that does not come to the router with the correct port will not be passed through to the computers inside the network.

Reverse Proxy engine

Reverse proxy engine is the feature for proxying web sites hosted on different real server with different internal IPs through a single public IP address. Engine welcomes any incoming web connection to your web sites. Then, fetch the web site data from the real server in your LAN or DMZ and gives to the client.

For example, any incoming web connection to your public IP (for example 85.10.10.10) will be welcomed by the engine. There may be several web sites be hosted on this IP address. These web sites may be hosted in different real/virtual machines inside your network. The engine will bring web sites from where they are located and give to the client.

The engine is configured through a configuration file on current version. (/etc/sysconfig/Labris-reverseproxy.conf). Configuration options and remarks are explained in the following table.

<pre>[options] listen_port=2480 listen_port_ssl=2443</pre>	<p>"listen_port" and "listen_port_ssl" attributes are used for configuring listen ports for http ad https, respectively. Default value should be used, if there are not any special conditions.</p>
<pre>default_certificate_file=/etc/httpd/certs/server1.crt default_certificate_key_file=/etc/httpd/certs/privkey.pem</pre>	<p>These attributes used for setting SSL certificates which are used for terminating SSL connections.</p>
<pre>[revproxy1] original_website_name=www.labrisnetworks.com incoming_conn_type=nonssl realserver_conn_type=nonssl realserver_conn_url=http://www.labrisnetworks.com/</pre>	<p>A block of variables are defined for each web site served through this reverse proxy engine. Each block has a name which is enclosed between "[]" and should include 4 attributes.</p> <p>"original_website_name" attribute is the web site name that the end user uses in his/her web browser to request your web site.</p> <p>"incoming_conn_type" attribute defines incoming connection type. Options are "ssl" and "nonssl".</p> <p>"realserver_conn_type" attribute defines protocol with the real server hosting the web site. Options are "ssl" and "nonssl".</p> <p>"incoming_conn_type" and "realserver_conn_type" attributes are also used for terminating a SSL connection and fetching data from a nonssl web server.</p> <p>"realserver_conn_url" attribute defines the address for the real web server inside your networks. Each definition should end with a "/". Internal IP addresses for the real servers are defined in hosts file (etc/hosts) or in first DNS forwarder server.</p>

After configuring the engine itself, traffic should be redirected to the engine.

1. First of all traffic should be allowed. Traffic coming into YourPublicIP:2480 and YourPublicIP:2443 should be allowed.

Example Global Policy;

No.	Source	Destination	Service	Action	Schedule	QoS/Bandw...	Applications	Security Po...	Options
0	Any	OUTSIDE	Tcp P_2443 Tcp P_2480	Accept	Any	Any	Any	Any	

2. HTTP/HTTPS traffic should be redirected into the engine. Traffic coming into YourPublicIP:80 (or other http port) should be redirected to UTM_IP:2480 (or configured listen_port). Traffic coming into YourPublicIP:443 (or other https port) should be redirected to UTM_IP:2443 (or configured listen_port_ssl).

Example NAT Policy;

No.	Original Src	Original Dst	Original Srv	Translated Src	Translated Dst	Translated Srv	Comment
0	Any	OUTSIDE	http	Original	WebServer1	P_2480	
1	Any	OUTSIDE	https	Original	WebServer2	P_2443	

54. Sample configuration:

/etc/sysconfig/labris-reverseproxy.conf:

```

;options must be set
[options]
listen_port=2480
listen_port_ssl=2443
; default certificate will be using on a ssl connection if any
; certificate for VirtualServer defined
; default_certificate_file=/opt/labris/etc/labris-lmc/certs/server.crt
; default_certificate_key_file=/opt/labris/etc/labris-lmc/certs/server.key
default_certificate_file=/etc/httpd/certs/server1.crt
default_certificate_key_file=/etc/httpd/certs/privkey.pem

; Configuration parameters for VirtualServer setup
; numbers at the end of section names (revproxy*)
; must be increased sequentially
; (but writing order can be random)
; following configuration examples demonstrate connection types
; (incoming_conn_type - realserver_conn_type)
; non-ssl - non-ssl
; ssl - non-ssl
; non-ssl - ssl
; ssl - ssl

[revproxy1]
original_website_name=www.labrisnetworks.com

```

```
incoming_conn_type=nonssl  
realserver_conn_type=nonssl  
realserver_conn_url=http://www.labrisnetworks.com/
```

```
[revproxy2]  
original_website_name=www.labrisnetworks.com  
incoming_conn_type=ssl  
realserver_conn_type=nonssl  
realserver_conn_url=http://www.labrisnetworks.com/
```

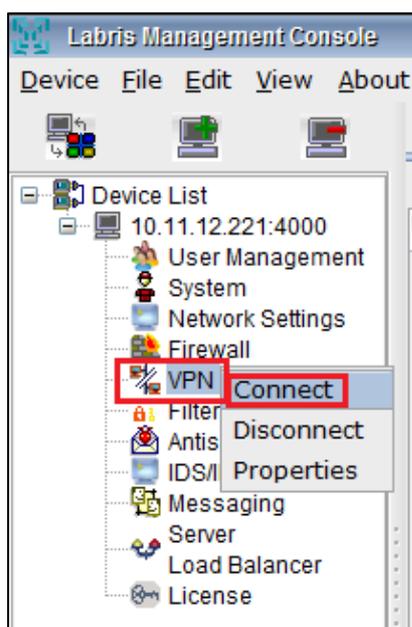
VPN

VPN stands for Virtual Private Network. It is a Private Network which allows us to connect to public network remotely in a secured way.

Personal VPN's allow you to encrypt your data from being sent from your computer to a VPN Server. This prevents hackers from stealing your information when you access the Internet from a public Wi-Fi. VPN's can be used for several other things, than just getting passed blocked sites, use Windows Firewall to block non-VPN traffic for selected applications, e.g. your torrent client, a browser, download manager, etc. When using a VPN to secure a public Wi-Fi spot.

From using your ISP connection, permit it to connect the the Internet using only the VPN connection. Unfortunately, this will not work with the built-in firewall in Windows XP or Vista.

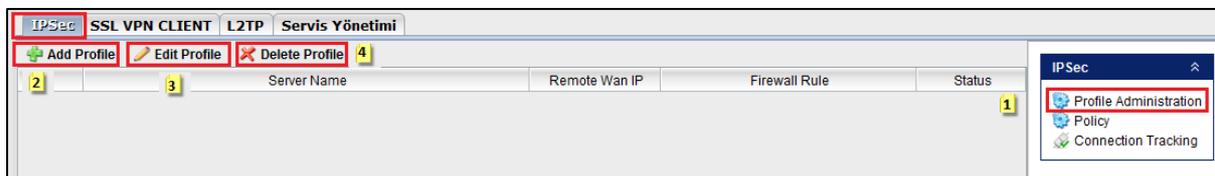
Right click on the **VPN tab** and select Connect.



IPSEC VPN Configuration

55. Profile Administration;

It is the section where IPSEC Profile definitions are made.

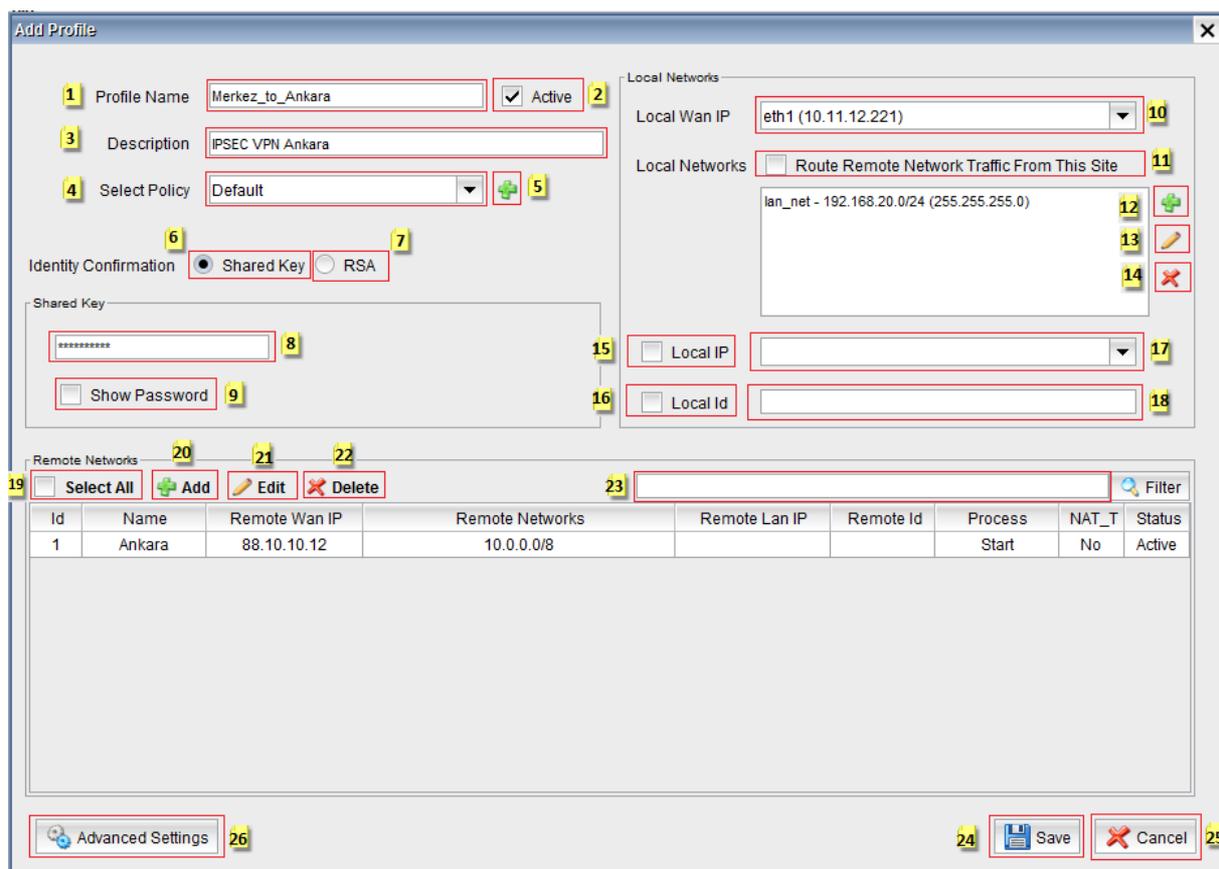


1	Profile Administration	Manage IPSEC Profile
2	Add Profile	Create a New IPSEC Profile
3	Edit Profile	Edit Selection IPSEC Profile
4	Delete Profile	Delete Selection IPSEC Profile

Step 1:

56. Add Profile

It is used to create a new IPSEC Profile.



1	Profile Name	IPSEC Profile Name
2	Active	Status Active / Passive
3	Description	Description for IPSEC Profile
4	Select Policy	Select Policy for FAZ1 and FAZ2

5	Add Policy	Add New Policy Profile. Click for Details or Example
6	Identity Confirmation	Shared Key
7	Identity Confirmation	RSA. Click for Details or Example
8	Shared Key	Shared Key Input
9	Show Password	Show Shared Key
10	Local WAN IP	Select Local WAN Interface
11	Local Networks (Automatic)	All Local Networks Route Remote Network
12	Add Local Networks (Manuel)	Add Local Networks or IP Address Manuel
13	Edit Local Networks (Manuel)	Edit Local Networks or IP Address Manuel
14	Delete Local Networks (Manuel)	Delete Local Networks or IP Address Manuel
15	Local IP	Local IP Active / Passive
16	Local ID	Lacal ID Active / Passive
17	Local IP	Select Local IP from List
18	Local ID	Local ID Input
19	Select All	Remote Networks Select All
20	Add Remote Networks	Create a Remote Networks Button Click for Details or Example
21	Edit Remote Networks	Edit Remote Networks
22	Delete Remote Networks	Delete Remote Networks
23	Filter	Filter Remote Networks Input
24	Save	Save IPSEC Profile
25	Cancel	Cancel IPSEC Profile
26	Advanced Settings	Advanced Settings Button

57. Identity Confirmation RSA;

RSA (Rivest Shamir Adleman)

It is the section where common security key, used in the stage of establishing connection with the remote network with which IPSEC VPN will be made, is defined.

RSA is an internet encryption and authentication system.



1	RSA	Identity Confirmation for RSA
2	Create RSA Key	RSA Key Execute Button
3	Local	Local RSA Key Input
4	Remote	Remote RSA Key Input

58. Add Local Networks (Manuel);

It is the section where local network or IP addresses which can communicate with the remote network with which IPSEC VPN will be made, are defined.

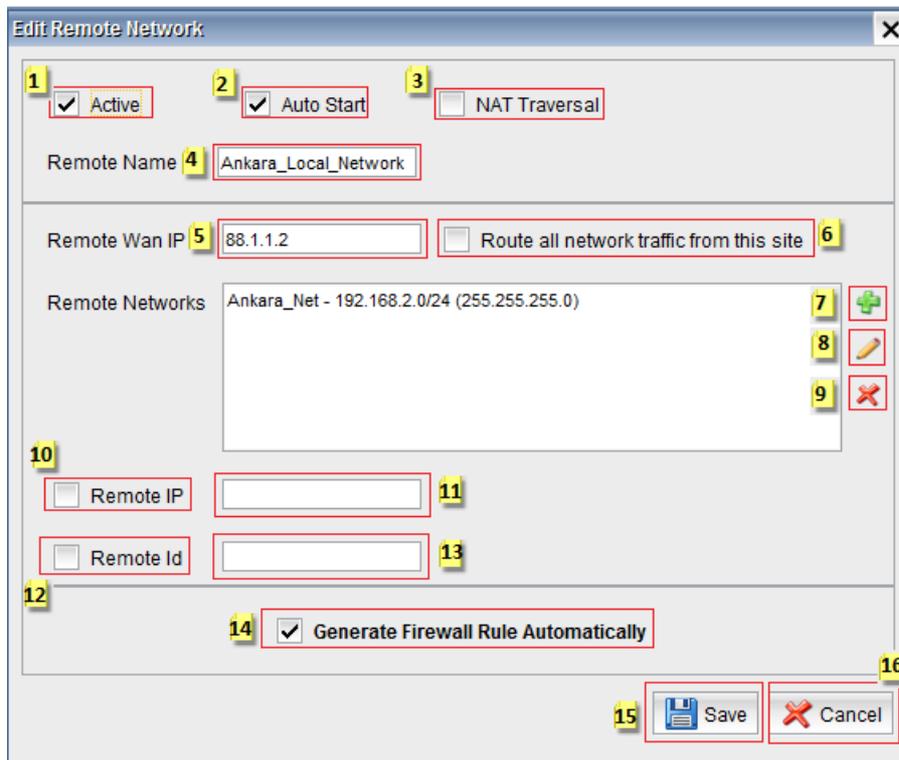
The screenshot shows a dialog box titled "Add Network" with a close button (X) in the top right corner. The dialog contains the following elements:

- 1. A radio button labeled "Select".
- 2. A radio button labeled "New".
- 3. A radio button labeled "IP".
- 4. A radio button labeled "Network".
- 5. A text input field labeled "Name".
- 6. A text input field labeled "Network Address".
- 7. A dropdown menu labeled "Netmask" with the value "/24 (255.255.255.0)".
- 8. A "Save" button.
- 9. A "Cancel" button.

1	Select	Select Network or IP Address from Database
2	New	Create a New Network or IP Address
3	IP	Create a New IP Address
4	Network	Create a New Network
5	Name	Network Name
6	Network or IP Address	Network or IP Address Input
7	Netmask	Netmask for Network
8	Save	Save Configuration
9	Cancel	Cancel Configuration

59. Add Remote Networks;

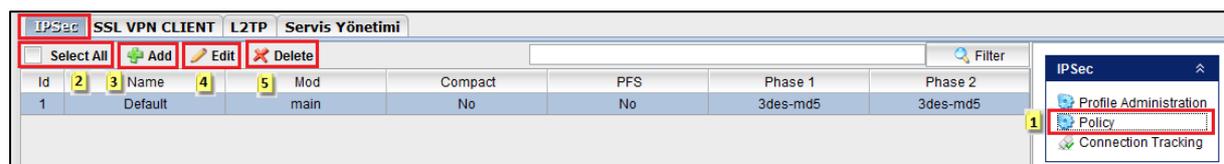
It is the section where local network or IP addresses in the remote network with which IPSEC VPN will be made, are defined.



1	Active	Remote Network Projile Active/Passive
2	Auto Start	Connection Auro Start When Disabled
3	NAT Traversal	NAT Traversal Active/Passive
4	Remote Name	Name for Remote Network
5	Remote WAN IP	Remote Static WAN IP Address
6	Local Networks (Automatic)	All Local Networks Route Remote Network
7	Add Local Networks (Manuel)	Add Local Networks or IP Address Manuel
8	Edit Local Networks (Manuel)	Edit Local Networks or IP Address Manuel
9	Delete Local Networks (Manuel)	Delete Local Networks or IP Address Manuel
10	Remote IP	Remote IP Active / Passive
11	Remote IP Input	Remote IP Input
12	Remote ID	Remote ID Active / Passive
13	Remote ID Input	Remote ID Input
14	Genarate Firewall Rule Autmatically	Add Firewall Rule Automatically for Remote Network Access

60. Policy;

It is the section where IPSEC PHASE1 and PHASE2 definitions are assigned to created profile.



1	Policy	Manage IPSEC Profile
2	Select All	Select All Policy
3	Add	Create a New Policy

4	Edit	Edit Selection Policy
5	Delete	Delete Selection Policy

Step 2:

61. Add Policy

It is the section where connection method and policy general definitions before IPSEC PHASE1 and PHASE2 are made.

1	Policy Name	Policy Name Input
2	Description	Description for Policy
3	Main Mod	Connection Mod is Main
4	Aggressive Mod	Connection Mod is Aggressive
5	Ikev2 Mod	Connection Mod is Ikev2
6	Compact Data Transfer	Compact Data Transfer Active / Passive
7	Fragmented Packet Handling	Fragmented Packet Handling Active / Passive
8	Re-keying Enable	Re-keying Enable / Disable
9	Key Tries	Key Tries Value Input

62. Add PHASE-1;

It is the section where settings such as Encryption, Authentication, Connection times, The method to follow in case of disconnection, are defined. It is required that the configuration made here is mutually equal with the settings in the second place with which IPSEC VPN connection will be made.

1	Encryption	Encryption Method
2	Authentication	Authentication Method
3	Encryption-More	Encryption Method
4	Authentication-More	Authentication Method
5	Encryption-More	Encryption Method
6	Authentication-More	Authentication Method
7	Key Life Time	Key Life Time / Sec
8	Rekey Margin	Rekey Margin / Sec
9	Randomize Re-keying Margin	Randomize Re-keying Margin / %
10	Diffie Hellman Groups-1	Dh Groups -1 / 768 bit
11	Diffie Hellman Groups-2	Dh Groups -2 / 1024 bit
12	Diffie Hellman Groups-14	Dh Groups -14 / 2048 bit
13	Diffie Hellman Groups-15	Dh Groups -15 / 3072 bit
14	Diffie Hellman Groups-5	Dh Groups -5 / 1536 bit
15	Diffie Hellman Groups-16	Dh Groups -16 / 4096 bit
16	Dead Peer Detection	Dead Peer Detection Active / Passive
17	Action	Action : Restart / Clear / Hold
18	Delay	Delay Time / Sec
19	Timeout	Connection Timeout / Sec
20	Save	Save Configuration
21	Cancel	Cancel Configuration

63. Add PHASE-2;

It is the section where the second PHASE settings such as Encryption, Authentication, Connection times, are defined. It is required that the configuration made here is mutually equal with the settings in the second place with which IPSEC VPN connection will be made.

The screenshot shows the 'PHASE 2' configuration window. It contains the following elements:

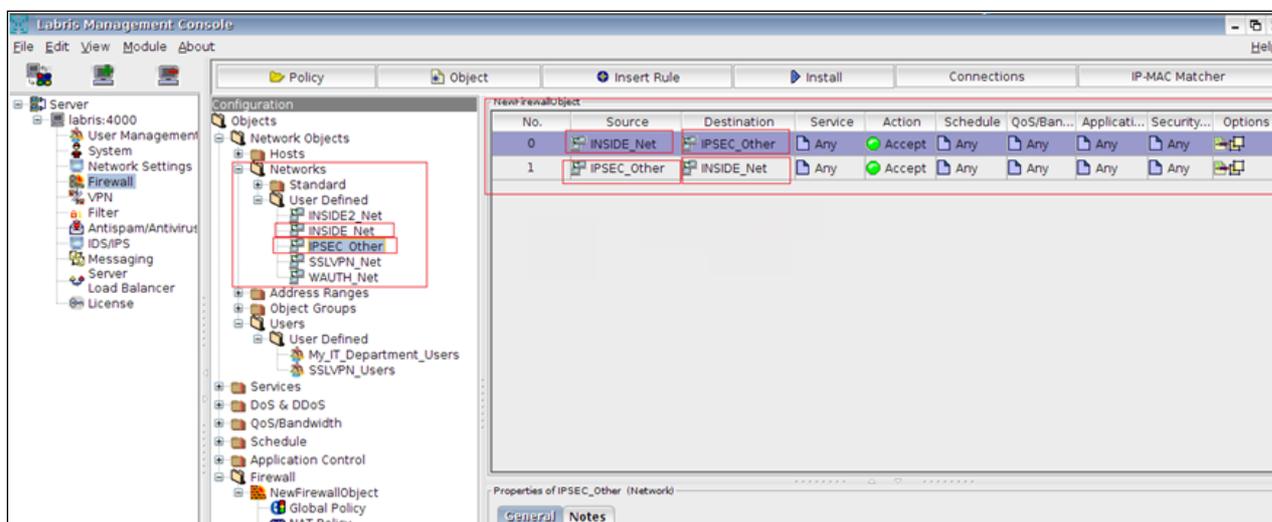
- Phase 1:** Encryption set to '3des' (1), Authentication set to 'md5' (2).
- Phase 2:** Encryption set to 'none' (3), Authentication set to 'none' (4).
- Phase 3:** Encryption set to 'none' (5), Authentication set to 'none' (6).
- Key Life Time:** Set to 3600 seconds (7).
- PFS Groups (DH):** Checked (8). Groups include: 1 (DH-768) (9), 2 (DH-1024) (10) - checked, 5 (DH-1536) (11), 14 (DH-2048) (12), 15 (DH-3072) (13), and 16 (DH-4096) (14).
- Buttons:** 'Save' (15) and 'Cancel' (16) buttons at the bottom right.

1	Encryption	Encryption Method
2	Authentication	Authentication Method
3	Encryption-More	Encryption Method
4	Authentication-More	Authentication Method
5	Encryption-More	Encryption Method
6	Authentication-More	Authentication Method
7	Key Life Time	Key Life Time / Sec
8	PFS Groups (DH)	PFS Groups Active / Passive
9	Diffie Hellman Groups-1	Dh Groups -1 / 768 bit
10	Diffie Hellman Groups-2	Dh Groups -2 / 1024 bit
11	Diffie Hellman Groups-14	Dh Groups -14 / 2048 bit
12	Diffie Hellman Groups-15	Dh Groups -15 / 3072 bit
13	Diffie Hellman Groups-5	Dh Groups -5 / 1536 bit
14	Diffie Hellman Groups-16	Dh Groups -16 / 4096 bit
15	Save	Save Configuration
16	Cancel	Cancel Configuration

Step 3:

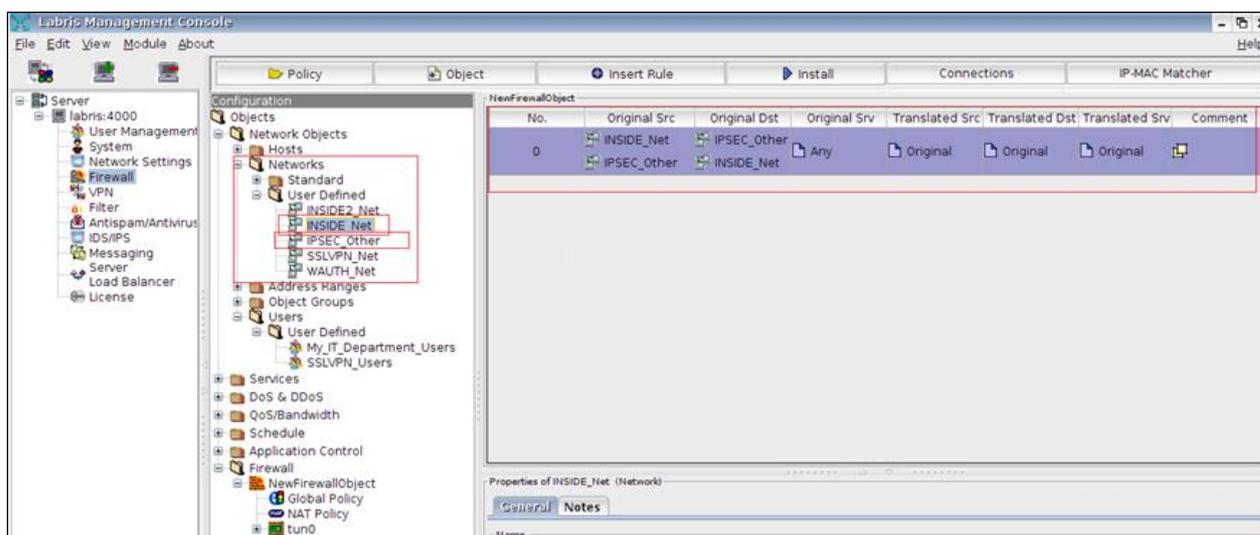
64. Add Global Policy

For Remote Network access permissions in cases where Generate Firewall Rule Automatically option is not selected, Step 3 and Step 4 must be applied.



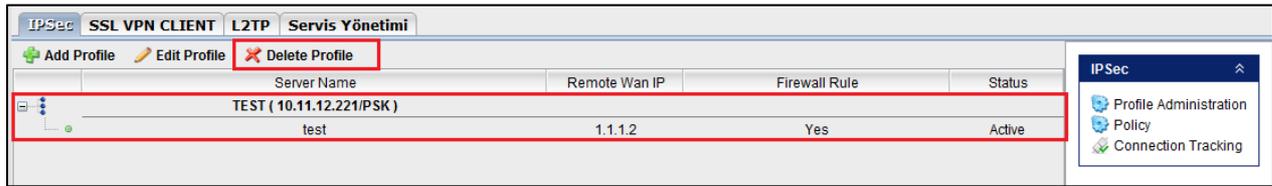
Step 4:

65. Add NAT policy

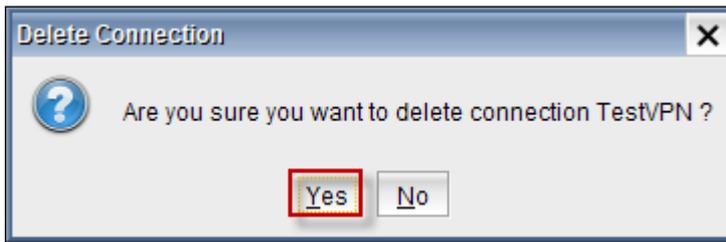


66. Delete Profile

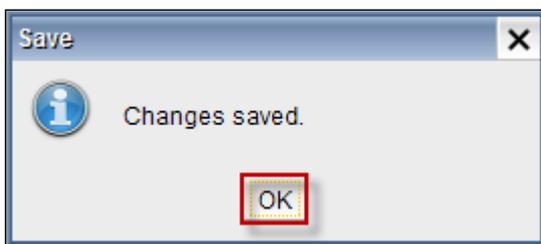
Select **Delete profile** to delete Connection.



Then a screen appears prompting **Are you sure you want to delete connection Test VPN**, click on **Yes** tab to delete connection.

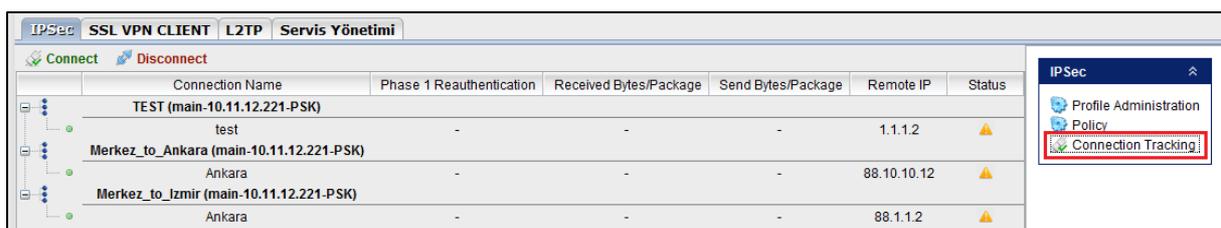


Below screen appears stating **Changes saved**, click on **Ok**.



67. Connection Tracking;

IPSEC Connection Monitoring / Status, Send and Recive Bytes/Package, Phase-1/Phase-2 ReAuthentication Status.



SSL VPN Configuration using CLI.

Open CLI using root user

Step 1:

For SSL VPN, sample Configuration file is copied to relevant folder. labris-ssl-vpn.conf file is edited taking the following sample as base.

```
# cd /etc/openvpn/  
# ls
```

samples

```
# cp -a samples/labris-ssl-vpn/* .
```

```
# ls -ltr
```

```
labris-ssl-vpn labris-ssl-vpn.conf up-down.sh samples
```

```
# vim labris-ssl-vpn.conf
```

And edit labris-ssl-vpn.conf;

```
#SSL VPN client using ip address (SSLVPN Network)
```

```
server 172.16.0.0 255.255.255.0
```

```
# Change Maximum online client count
```

```
max-clients 100
```

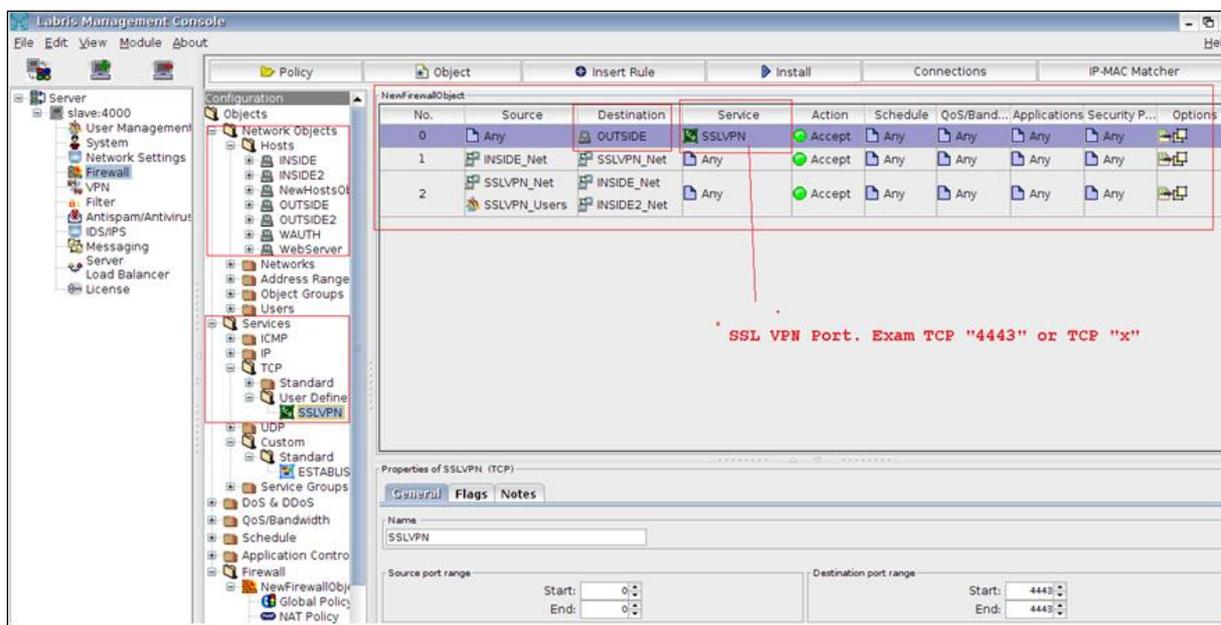
```
# access to Local Area Network address (INSIDE Network)
```

```
push "route 192.168.2.0 255.255.255.0"
```

Step 2:

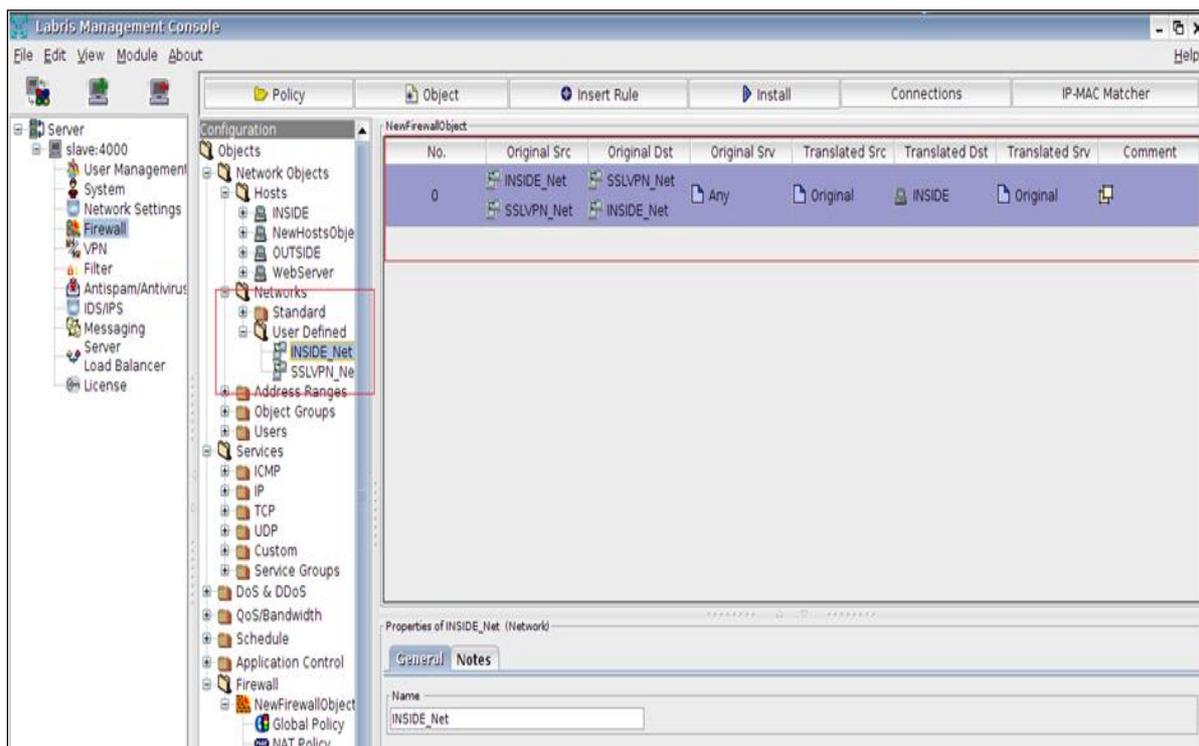
68. Create a new global policy

INSIDE Network access to SSLVPN Network and SSLVPN Network access to INSIDE Network.



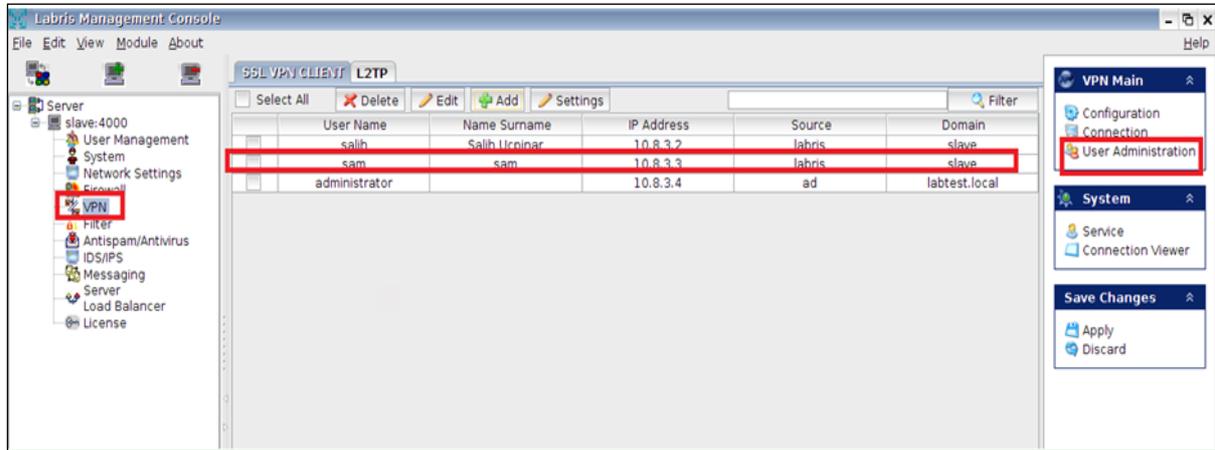
Step3:

69. Create a new NAT Policy



Step4:

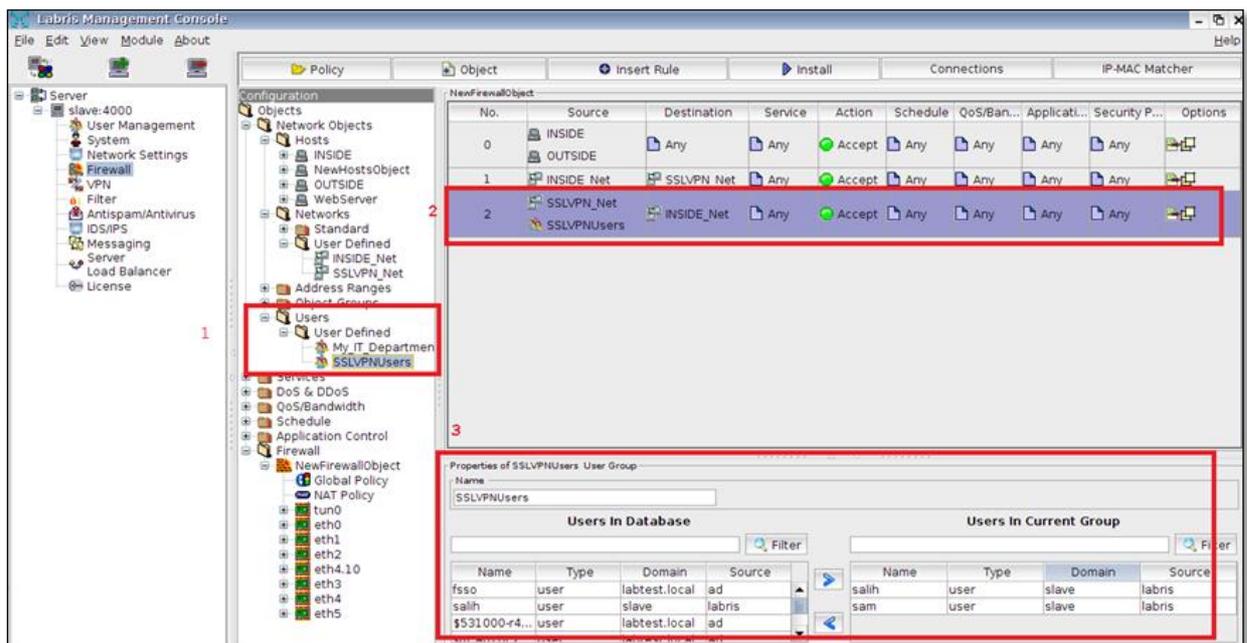
Select a SSL VPN User (Please refer User Management section to **add user**) and add/Select VPN user (Please refer SSI VPN Client section for VPN → User Administration → Add)



Step5:

70. Add a user on policy.

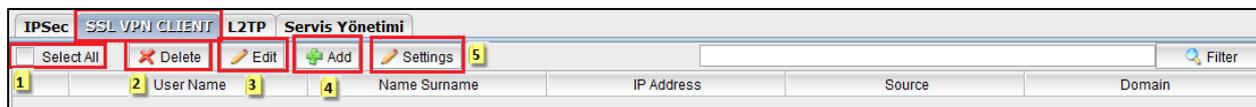
(Please refer to Users in Object Group section for Create Network Object → Users)



71. SSL VPN CLIENT - User Administration

The management part deals with adding user names and passwords to electronic directories along with the assignment of rights to data and network resources such as files, databases, printers, Internet. Maintenance includes updating the directories when employees change their job classifications or departments or leave the company.

In the right pane under **VPN Main**, select **SSL VPN CLIENT - User Administration**.

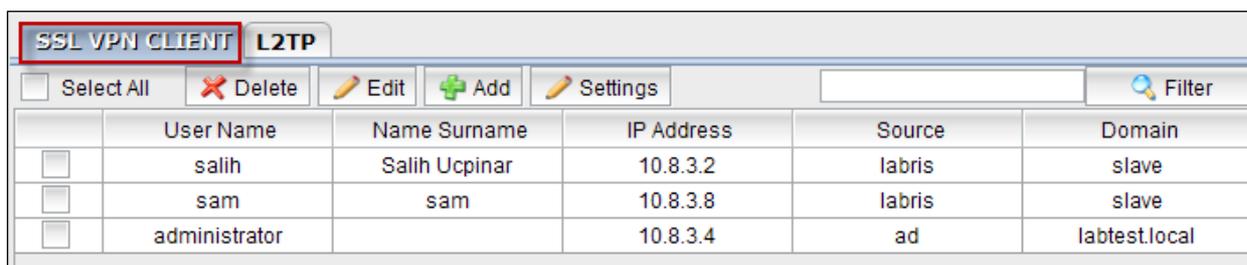


1	Select All	Select All Users
2	Delete	Delete Selection User/Users
3	Edit	Edit Selection User
4	Add	Add User
5	Settings	Setting SSL VPN CLIENT

SSLVPN Client

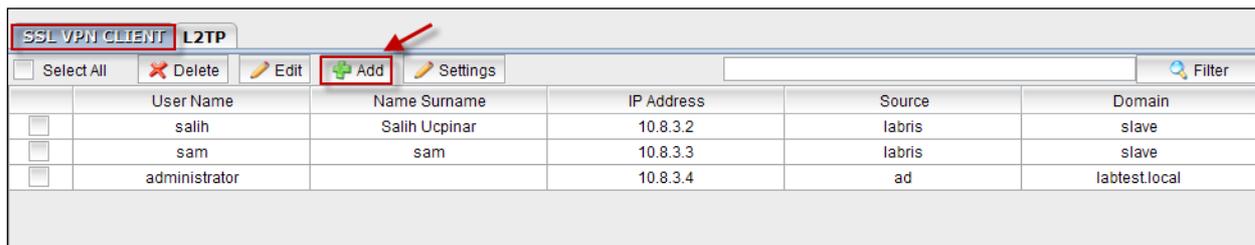
SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. In contrast to the traditional Internet Protocol Security (IPsec) VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer. It is used to give remote users with access to Web applications, client or server applications and internal network connections.

An SSL VPN consists of one or more VPN devices to which the user connects by using his Web browser. The traffic between the Web browser and the SSL VPN device is encrypted with the SSL protocol or its successor, the Transport Layer Security (TLS) protocol. An SSL VPN offers versatility, ease of use and granular control for a range of users on a variety of computers, accessing resources from many locations

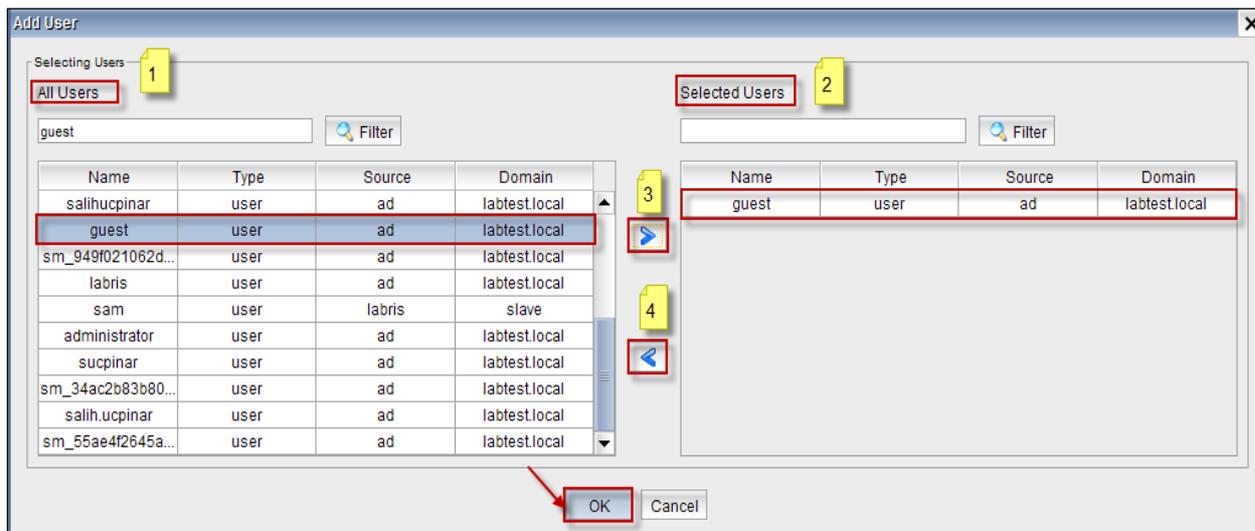


Add

Click on **Add** tab



Below screen appears.



These are the inputs adding User to SSLVPN Client

1	All Users	All the Users are displayed in this field
2	Selected Users	Selected Users are only displayed in this field
3		This symbol helps us to add Users to Selected Users from All Users
4		This symbol helps us to remove User from Selected Users list

Click on **Ok** to add User.

Adding User is in Progress



In the below screen we can notice Selected User added to the SSLVPN Client.

	User Name	Name Surname	IP Address	Source	Domain
<input checked="" type="checkbox"/>	guest		10.8.3.3	ad	labtest.local
<input type="checkbox"/>	salih	Salih Ucpinar	10.8.3.2	labris	slave
<input type="checkbox"/>	sam	sam	10.8.3.8	labris	slave
<input type="checkbox"/>	administrator		10.8.3.4	ad	labtest.local

Edit

Select User and click on **Edit tab**

	User Name	Name Surname	IP Address	Source	Domain
<input type="checkbox"/>	salih	Salih Ucpinar	10.8.3.2	labris	slave
<input checked="" type="checkbox"/>	sam	sam	10.8.3.3	labris	slave

Edit User tab appears, we can only edit IP Address and click on **Ok** tab.

Edit User

User Name:

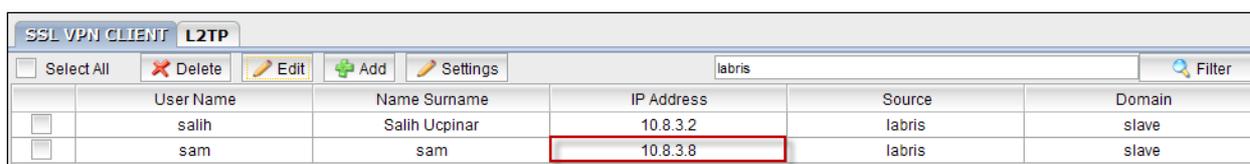
Domain:

IP Address: Automatic

Editing User is in Progress.



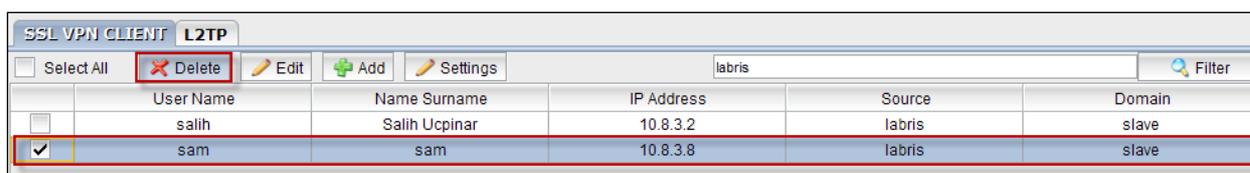
In the below screen, we can notice IP Address has been changed.



	User Name	Name Surname	IP Address	Source	Domain
<input type="checkbox"/>	salih	Salih Ucpinar	10.8.3.2	labris	slave
<input type="checkbox"/>	sam	sam	10.8.3.8	labris	slave

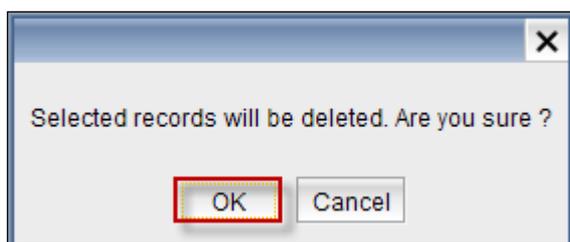
Delete

Select User and click on **Delete** tab.

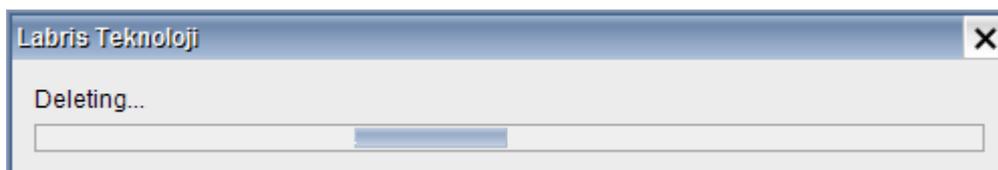


	User Name	Name Surname	IP Address	Source	Domain
<input type="checkbox"/>	salih	Salih Ucpinar	10.8.3.2	labris	slave
<input checked="" type="checkbox"/>	sam	sam	10.8.3.8	labris	slave

Then below screen appears, Click **Ok** to delete.



Deleting Process is in progress.

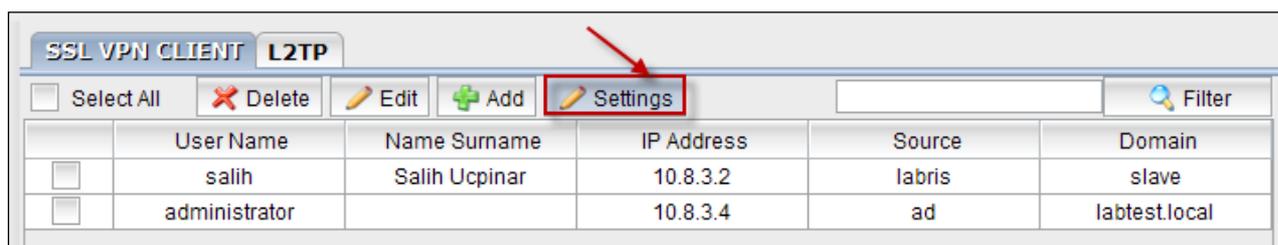


Below screen appears displaying information, Selected records have been deleted. Click on **Ok** to close the current tab.

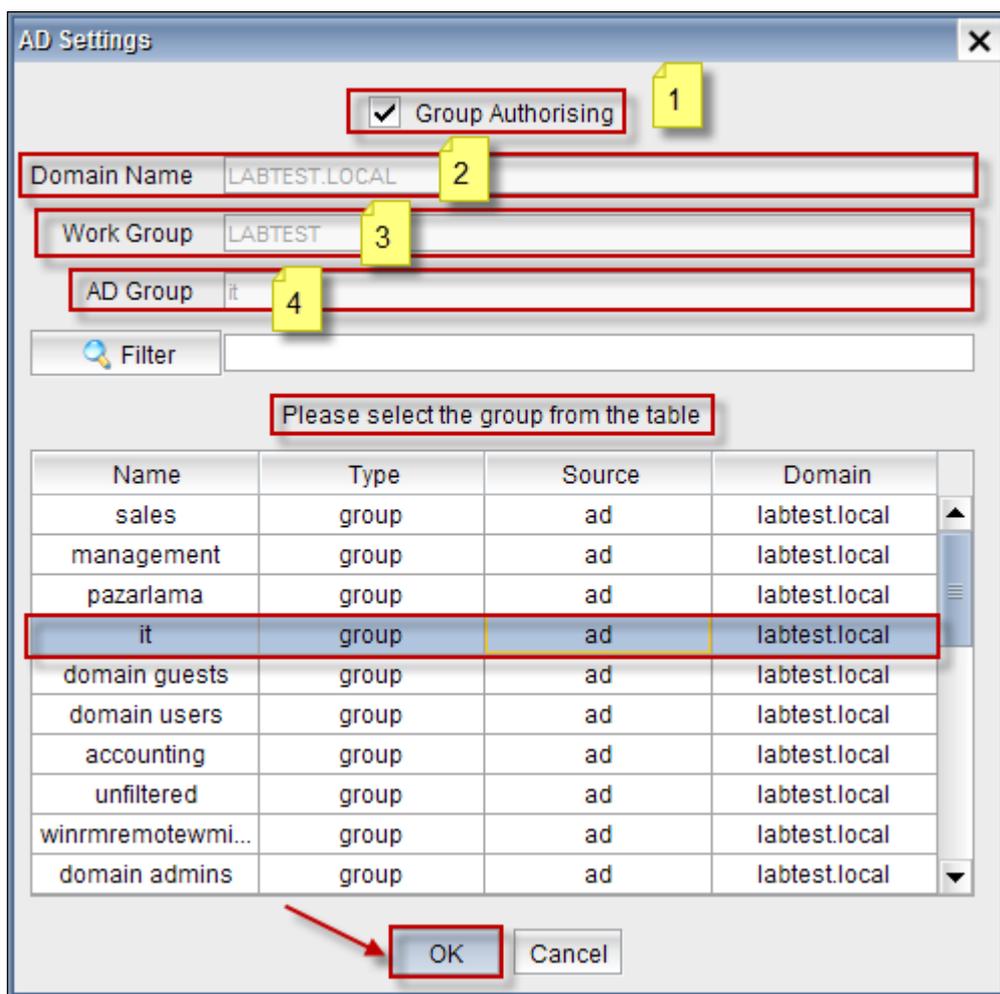


Settings

Click on **Settings tab** to view and change the Settings of SSL VPN Client.



AD Settings tab appears.



1	Group Authorizing	We can enable or disable this option
2	Domain Name	Domain Name is selected by default
3	Work Group	Work Group is selected by default
4	AD Group	Select AD Group from the group table.

Click on **Ok**.

L2TP

L2TP uses packet-switched network connections to make it possible for the endpoints to be located on different machines. Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet.

The two main components that make up L2TP are the L2TP Access Concentrator (LAC), which is the device that physically terminates a call and the L2TP Network Server (LNS), which is the device that terminates and possibly authenticates the PPP stream.

SSL VPN CLIENT **L2TP**

Enable L2TP connection

Settings

Server IP:

Pre-shared Key:

IP Range:

Local IP:

Router:

Other:

Users

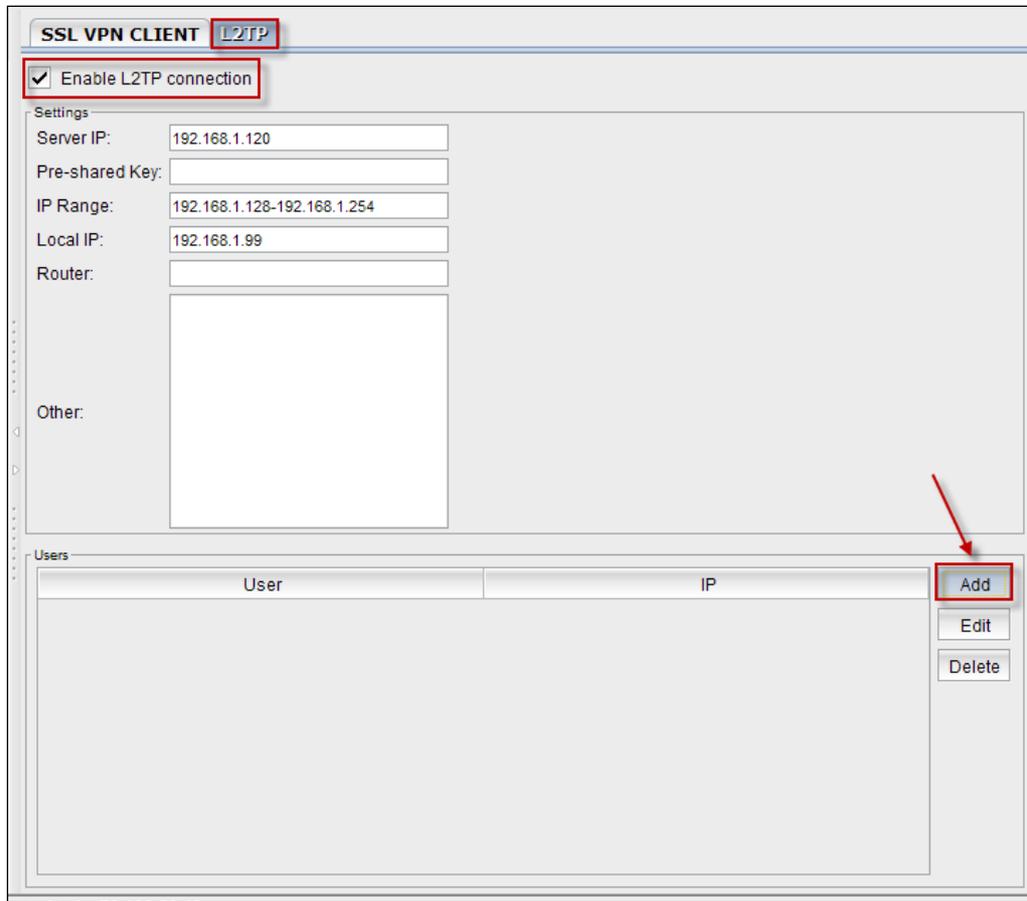
User	IP
------	----

Add
Edit
Delete

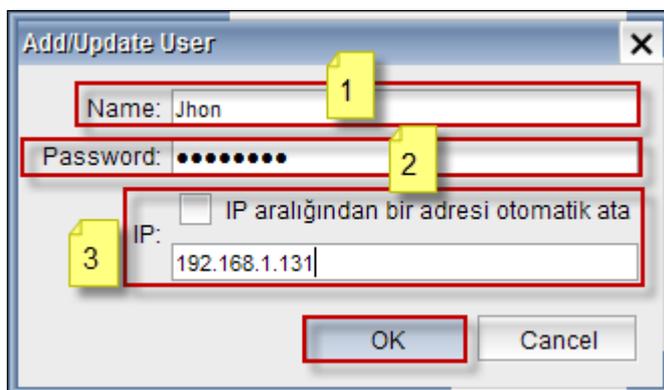
Add

Enable L2TP connection to view and change settings of L2TP and to Add, Edit, Delete Users to L2TP.

Click on **Add tab**



Add User tab is appeared.



These are the inputs to add an User.

1	Name	Type the name of the User
2	Password	Type the Password for the User
3	IP	We can enable default IP or give an IP within the IP range

Click on **Ok** to add User.

In the below screen, we can notice new **User** added to the Users list of **L2TP** within the IP Range.

SSL VPN CLIENT L2TP

Enable L2TP connection

Settings

Server IP: 192.168.1.120

Pre-shared Key:

IP Range: 192.168.1.128-192.168.1.254

Local IP: 192.168.1.99

Router:

Other:

Users

User	IP	
Jhon	192.168.1.131	Edit

Add
Delete

Edit

Select the User and click on **Edit tab**.

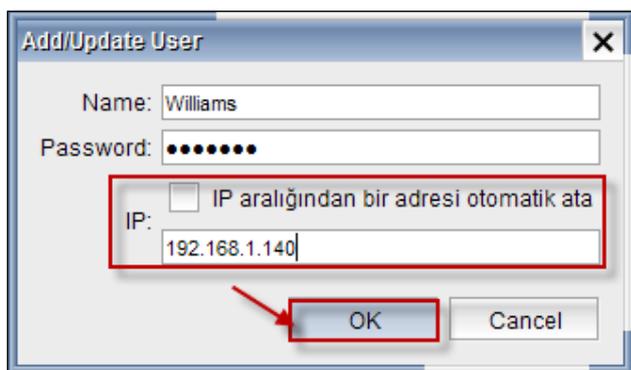
Users

User	IP	
Williams	*	Edit
Jhon	192.168.1.131	

Add
Delete

Below screen appears.

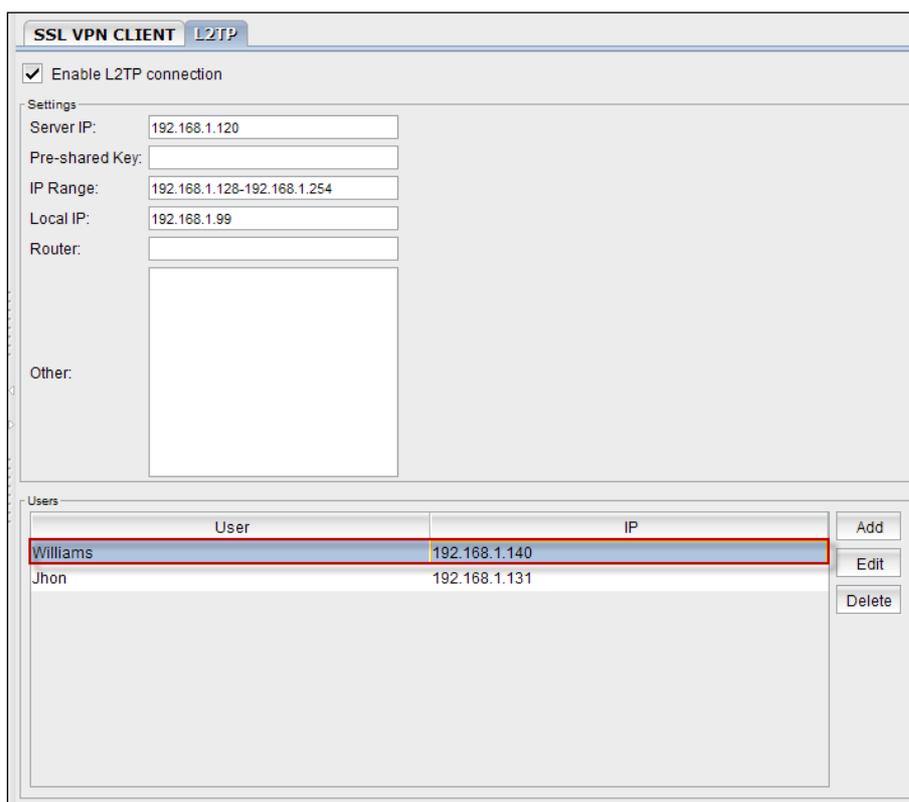
We can edit **Name**, **Password** and the **IP** of the User.



The screenshot shows a dialog box titled "Add/Update User". It has a close button (X) in the top right corner. The "Name" field contains the text "Williams". The "Password" field is filled with ten dots. Below the password field, there is a checkbox labeled "IP aralığında bir adresi otomatik ata" which is unchecked. Below the checkbox is the "IP" field containing the text "192.168.1.140". At the bottom of the dialog, there are two buttons: "OK" and "Cancel". A red box highlights the "IP" field and the "OK" button, and a red arrow points to the "OK" button.

Click on **Ok**.

We can notice the changes made to the **User** in the below screen.



The screenshot shows the "SSL VPN CLIENT" configuration window with the "L2TP" tab selected. The "Enable L2TP connection" checkbox is checked. The "Settings" section includes the following fields:

- Server IP: 192.168.1.120
- Pre-shared Key: (empty)
- IP Range: 192.168.1.128-192.168.1.254
- Local IP: 192.168.1.99
- Router: (empty)

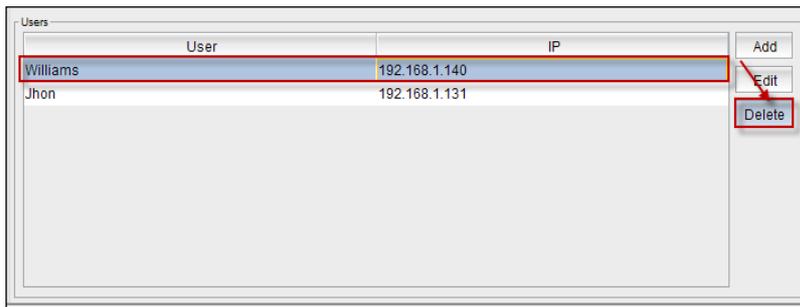
The "Users" section shows a table with two users:

User	IP
Williams	192.168.1.140
Jhon	192.168.1.131

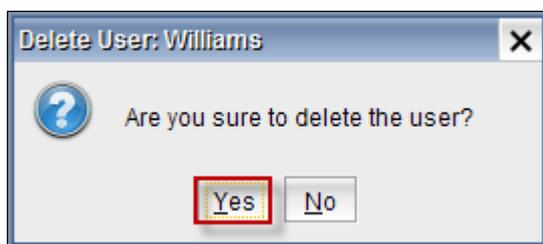
The "Williams" row is highlighted with a red border. To the right of the table are buttons for "Add", "Edit", and "Delete".

Delete

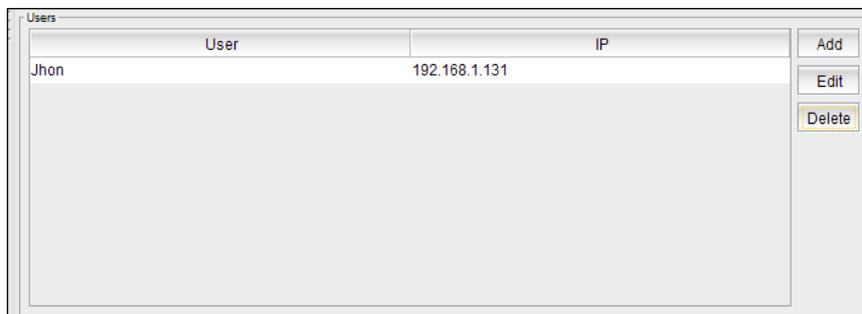
Select the User and click on **Delete tab**.



Delete User tab appears with User name, click on **Yes tab** to delete the User.



We can notice the selected User deleted.



72. Service Management

In the right pane under **VPN tab**, select **Service Management**.

VPN Bağlantı Türü	DURUM	İşlem		
1 IPsec VPN	2			
L2TP VPN				
PPTP VPN				
SSL VPN				

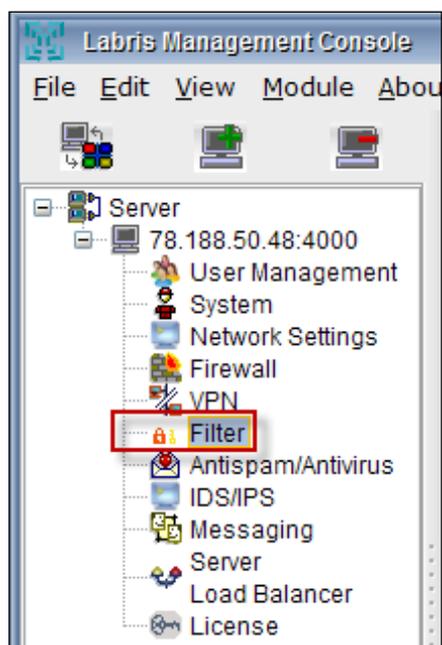
1	VPN Connection Type	VPN Connection Type List
---	---------------------	--------------------------

2	Status	Connection Status
3	Action	Connection Start / Stop / Restart

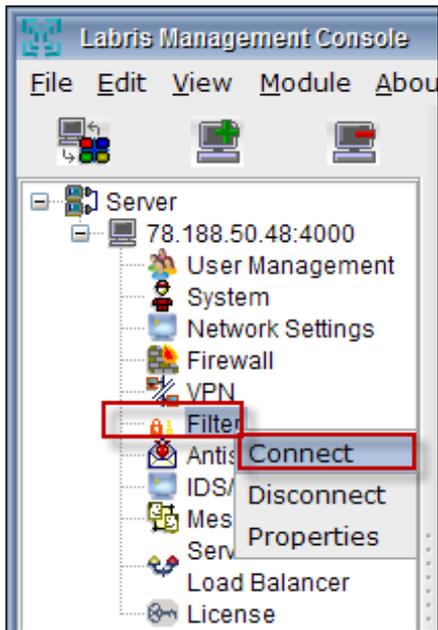
FILTER

Filters are rule sets that control the flow of traffic into and out of a device. It consists of a series of from-then statements.

You cannot apply more than one firewall filter per port, VLAN or router interface per direction input and output. For example, for a given port you can apply at most one filter in the input direction and one filter in the output direction. You should try to be conservative in the number of terms that you include in each filter, because a large number of terms require longer processing time during a commit operation and can make testing and troubleshooting more difficult.

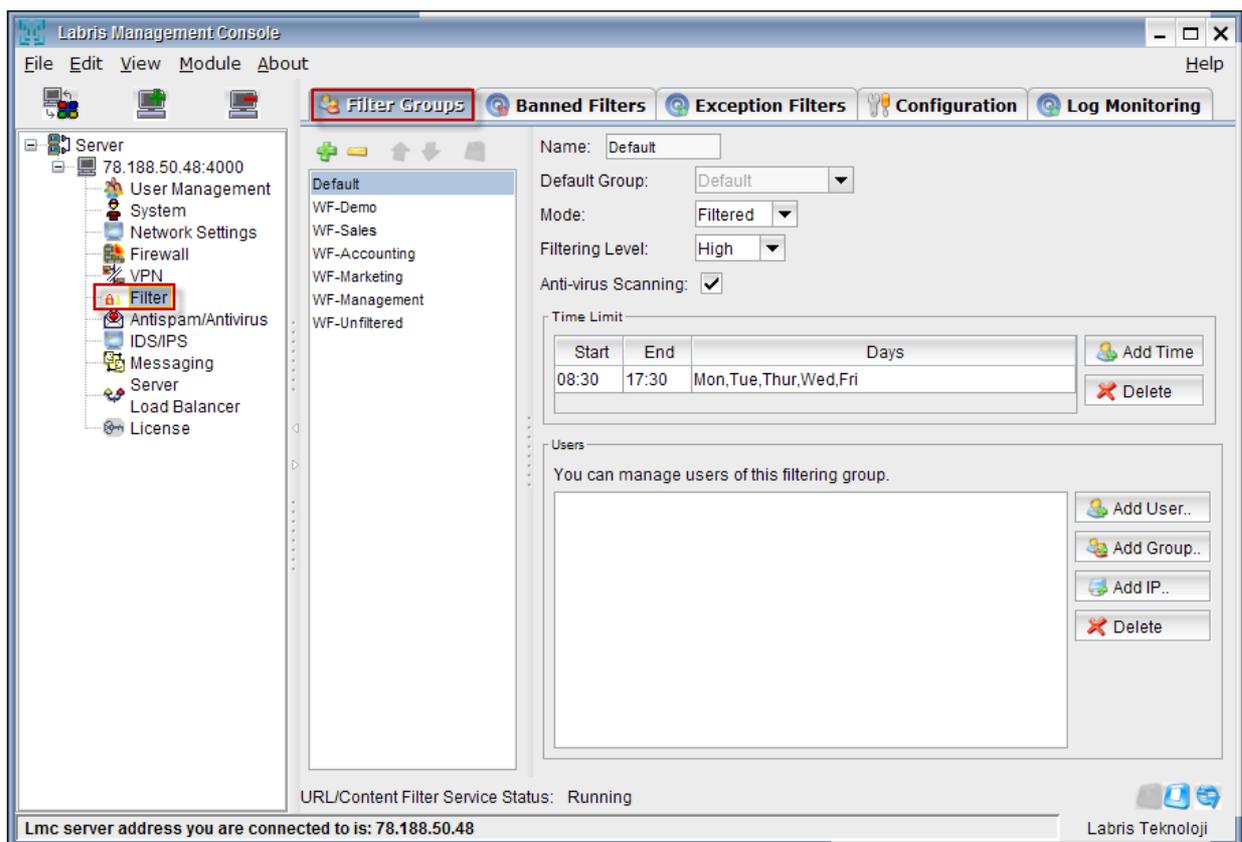


The purpose of the filter is system can drop packets based on header information, rate-limit traffic, classify packets into forwarding classes, log and count packets or prevent denial of service attacks.



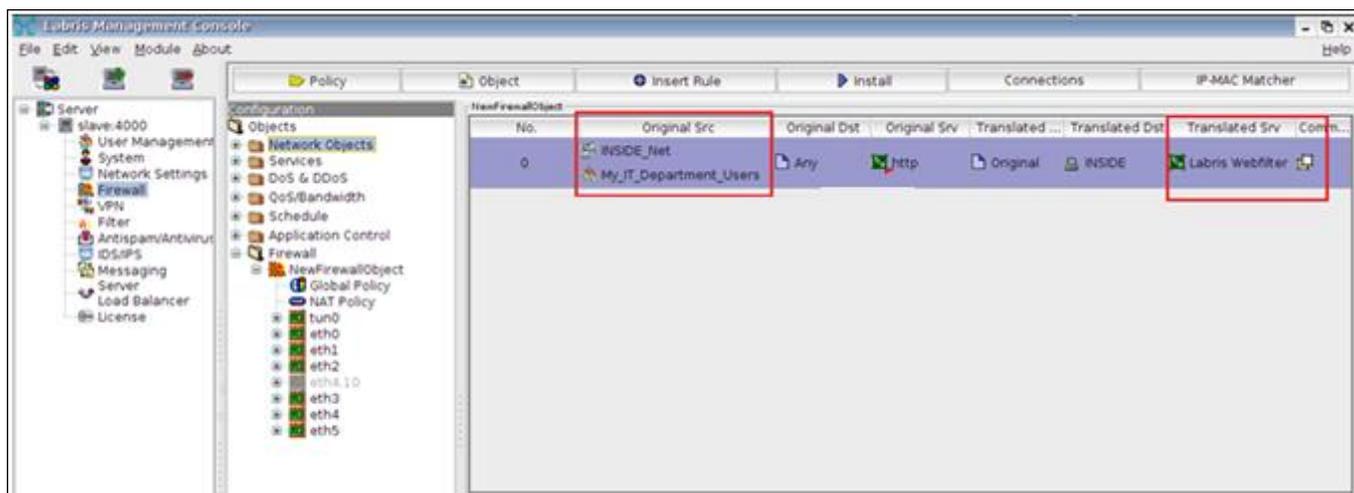
Right click on **Filter** and select **Connect**.

73. Filter Groups



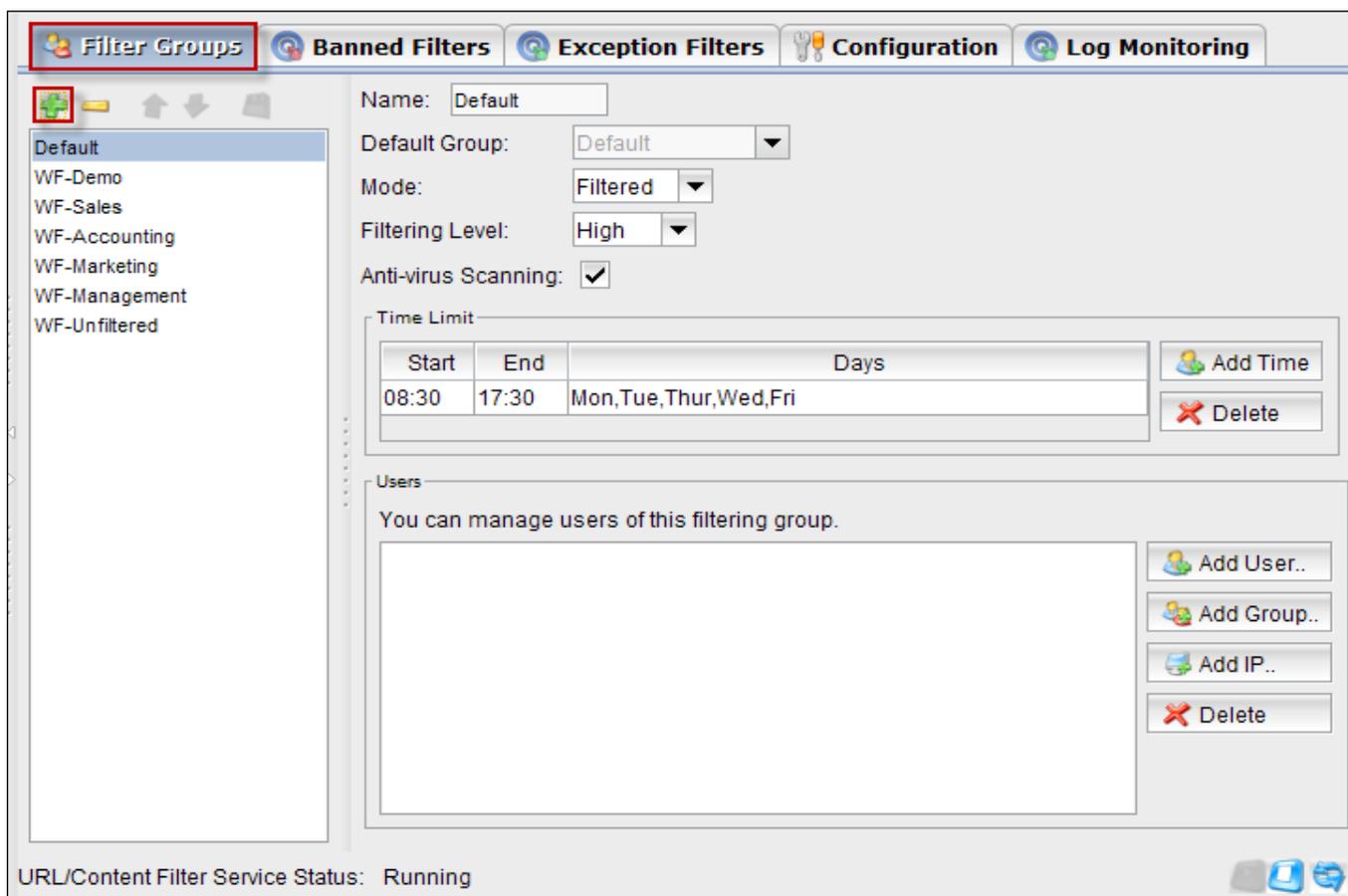
Add New Filter Policy

These options will be exposed to the web filter.



Add/Edit Filter Group

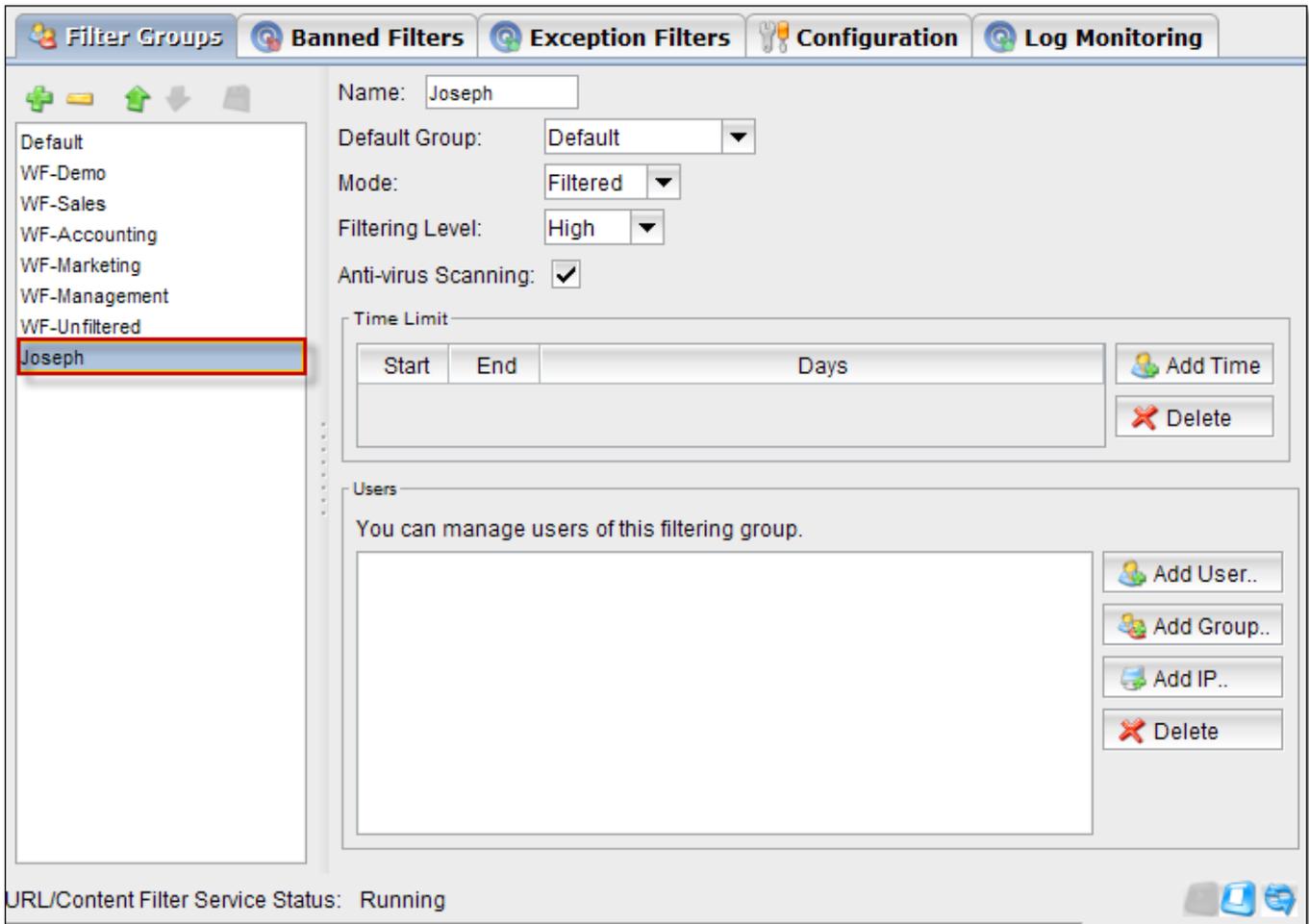
Click on **Add** icon to add a filter group.



Add Group tab appears, Give the Name of the Group and click on **Ok**.



In the below screen we can notice new Filter Group added in the list.



Editing Filter Group

The screenshot shows the 'Filter Groups' configuration interface. On the left, a list of filter groups includes 'Default', 'WF-Demo', 'WF-Sales', 'WF-Accounting', 'WF-Marketing', 'WF-Management', 'WF-Unfiltered', and 'Joseph' (highlighted). The main configuration area for the 'Joseph' group includes:

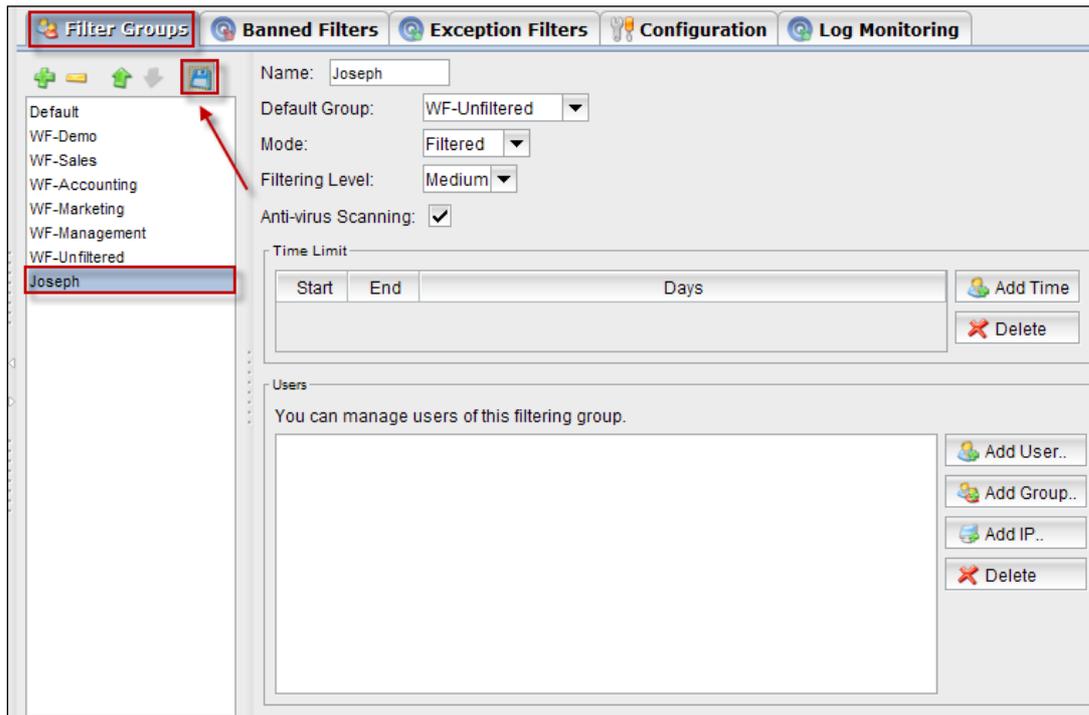
- Name:** Joseph (highlighted with callout 1)
- Default Group:** WF-Unfiltered (highlighted with callout 2)
- Mode:** Filtered (highlighted with callout 3)
- Filtering Level:** Medium (highlighted with callout 4)
- Anti-virus Scanning:** (highlighted with callout 5)

Below these fields are sections for 'Time Limit' (with Start, End, Days fields and Add Time/Delete buttons) and 'Users' (with a text area and Add User.., Add Group.., Add IP.., and Delete buttons).

These are the inputs for Filter Groups

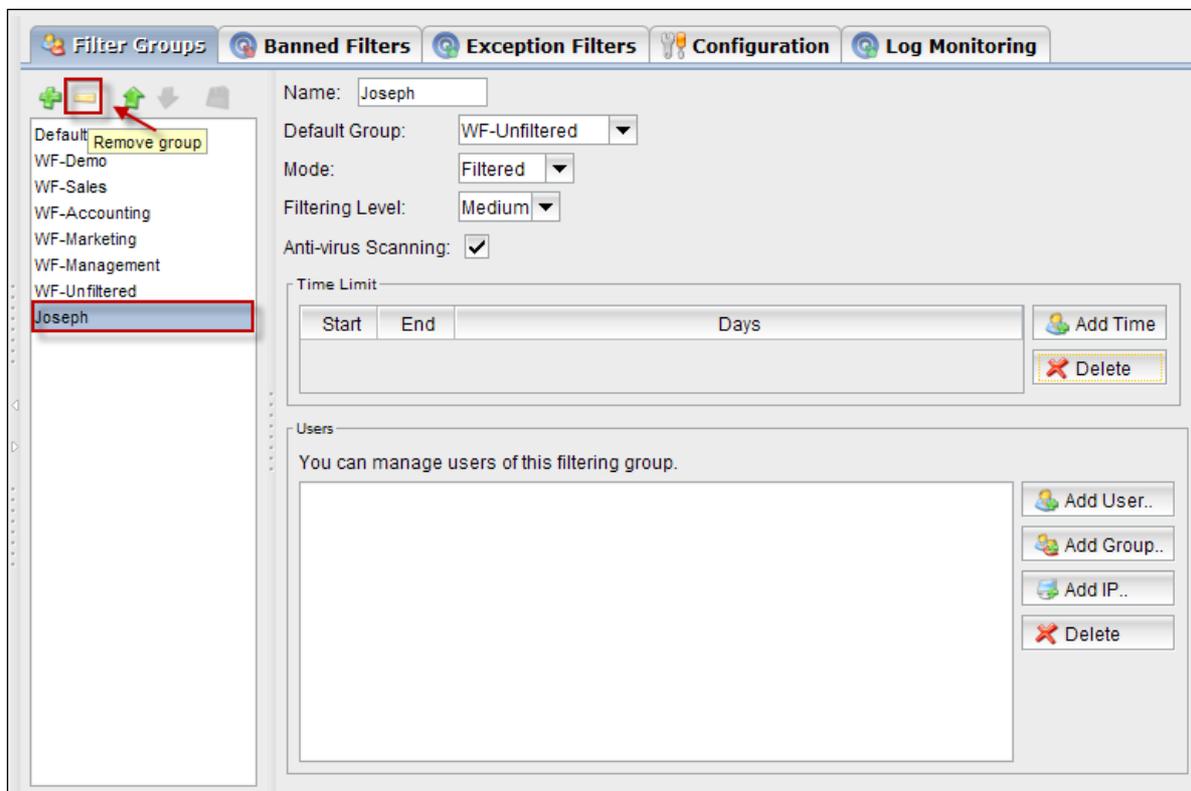
1	Name	We can edit name of the filter group
2	Default Group	Choose Default Group from the drop down list
3	Mode	Choose Mode type from the drop down list
4	Filtering Level	Choose Filtering level form the drop down list
5	Anti-virus Scanning	We can Enable/Disable this option

Click on **Save** icon to save the Group configuration

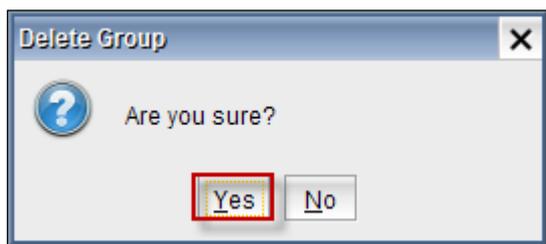


Delete Filter Group

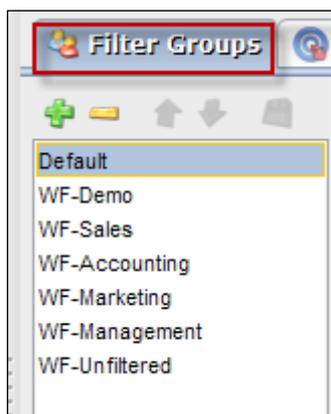
Click on the Remove icon to Delete Group.



Delete Group tab appears, click on **Yes** to Delete Group.

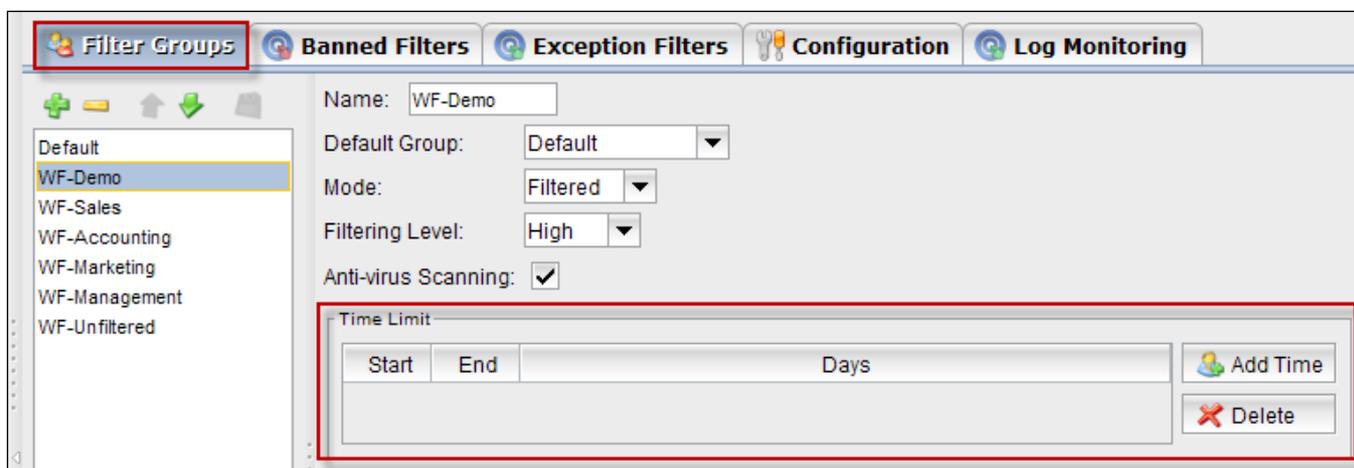


In the below screen we can notice Filter Group deleted.



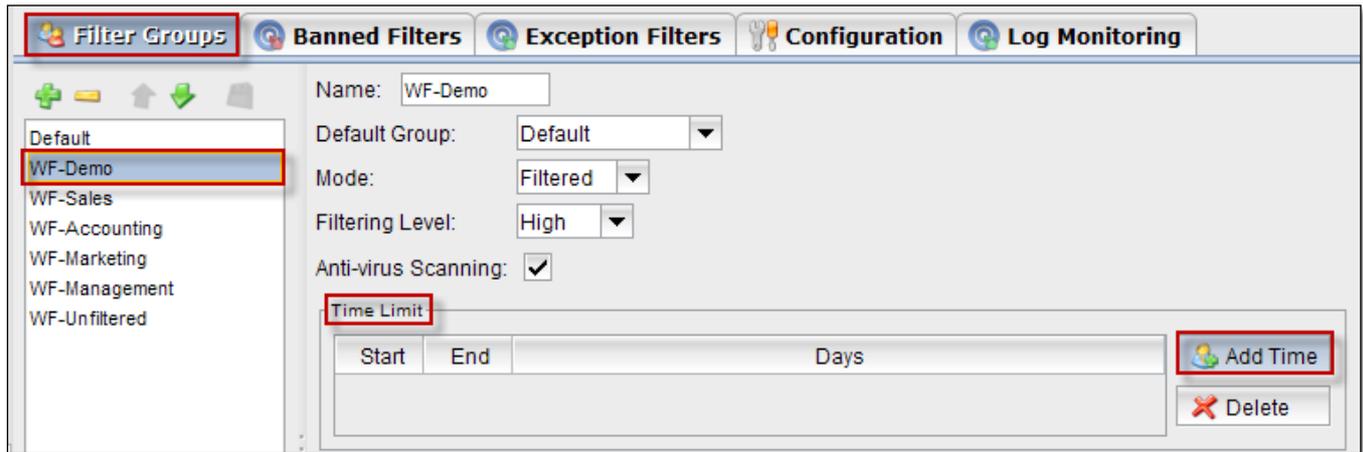
Time limit

Time limit enables us to set up Starting time and ending time of the **Filter Groups**.

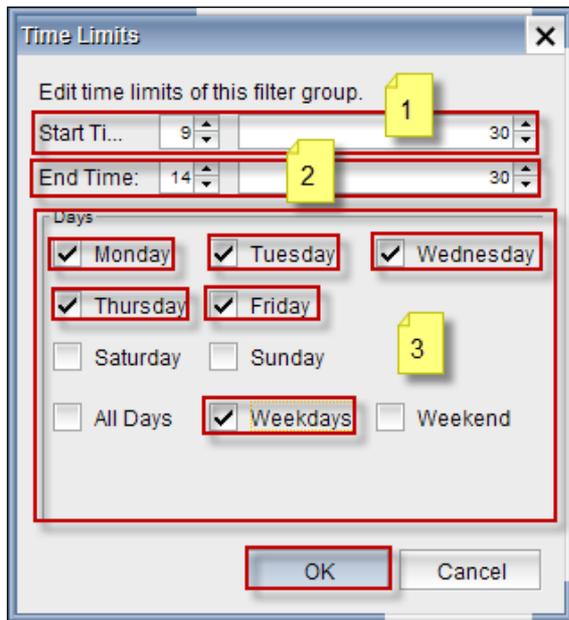


Add Time

Click on **Add time** tab



Time Limits tab appears.

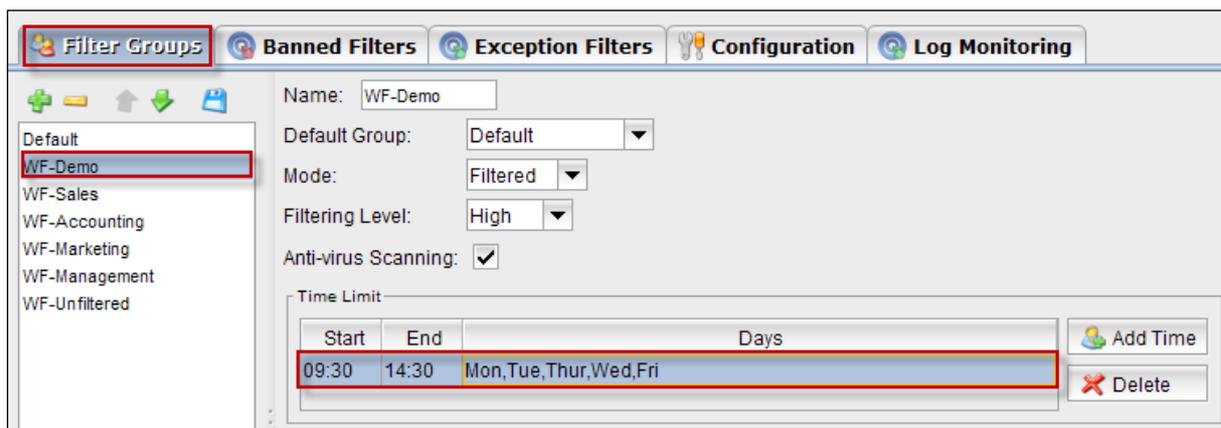


These are the inputs for adding Time Limit.

1	Start Time	Choose the starting time
2	End Time	Choose the ending time
3	Days	We can enable specific days

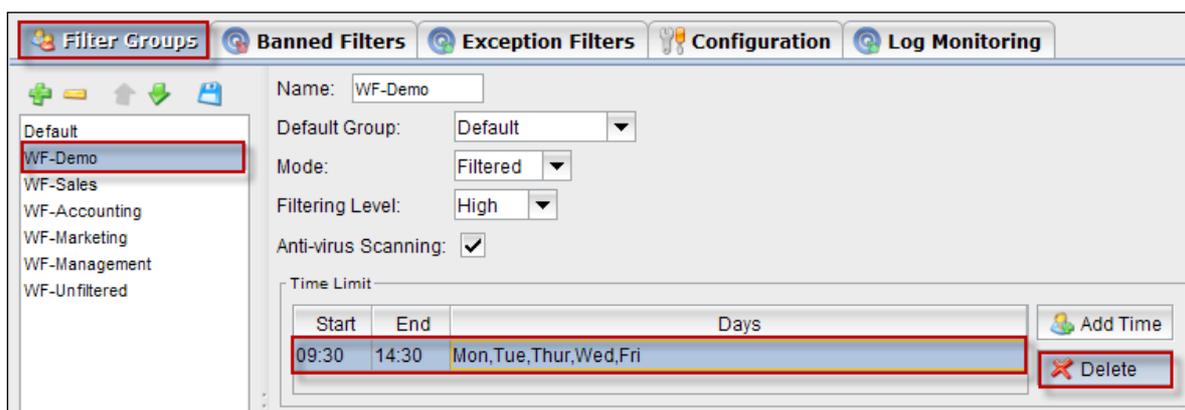
Click on **Ok**.

In the below screen, we can notice Time Limit

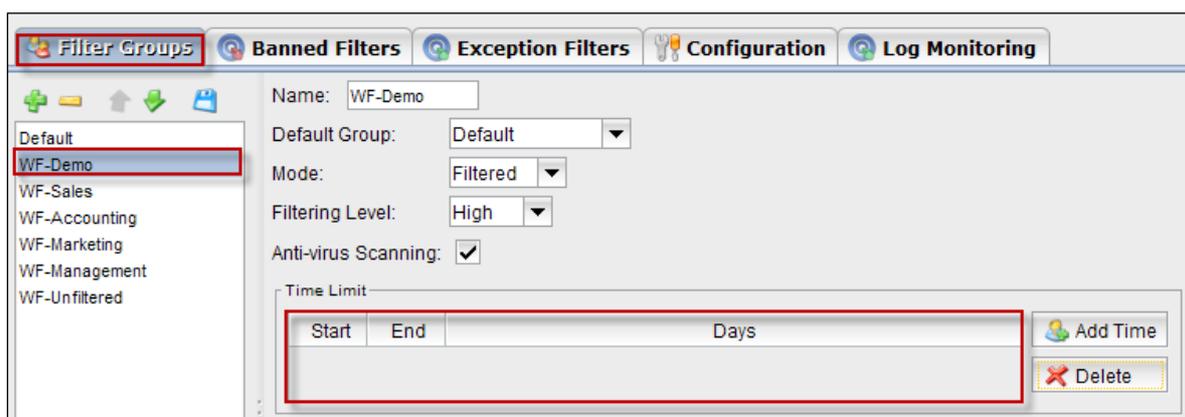


Delete Time

Select the Time Limit and click on **Delete** tab.

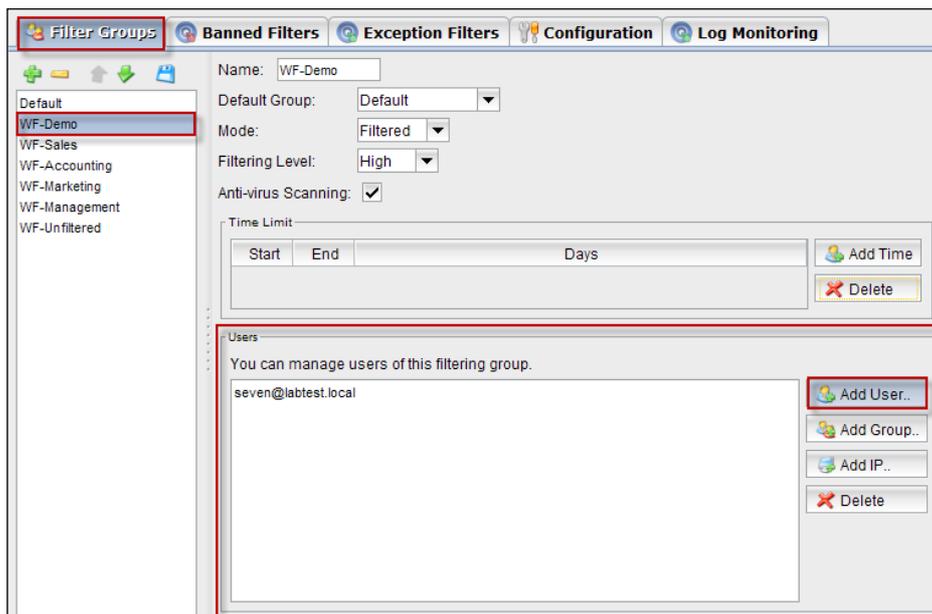


In the below screen we can notice Time Limit deleted.

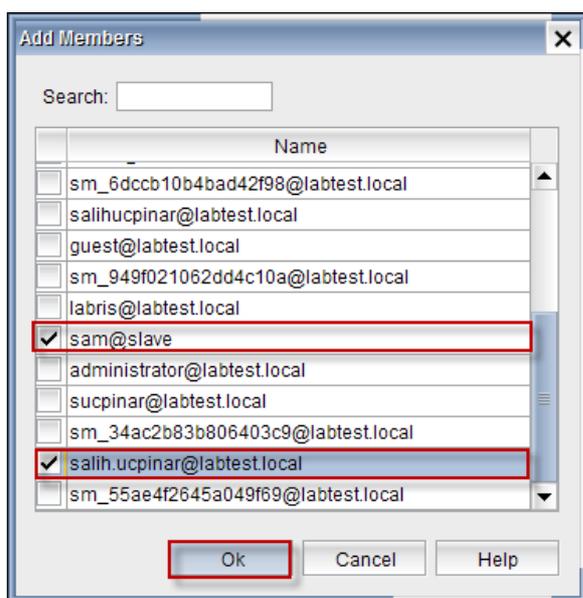


Add Users

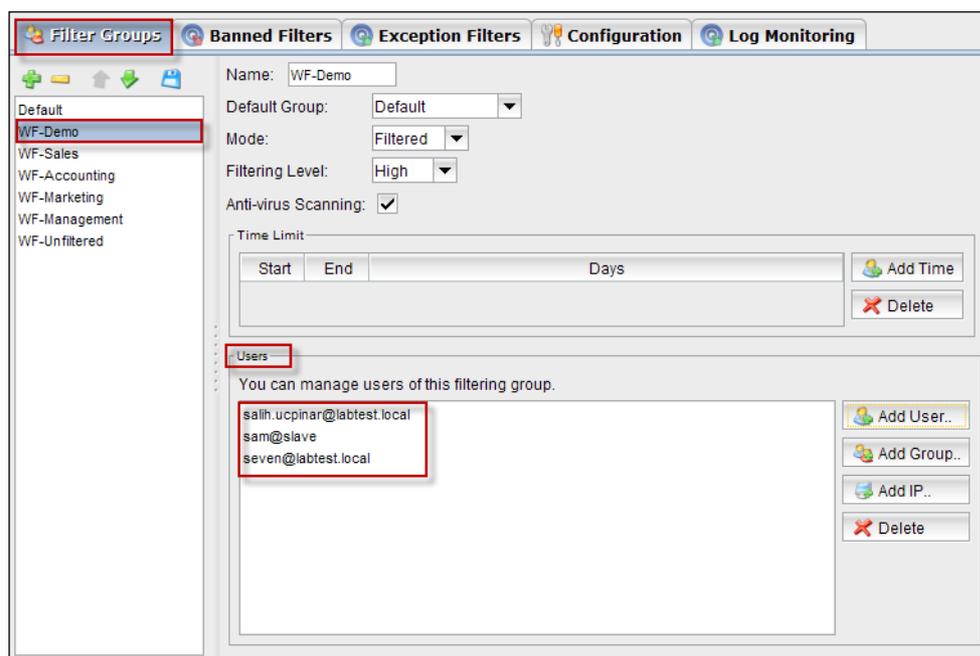
Click on **Add Users** tab



Add Members tab appears, in which we can choose Members and click on **Ok**.

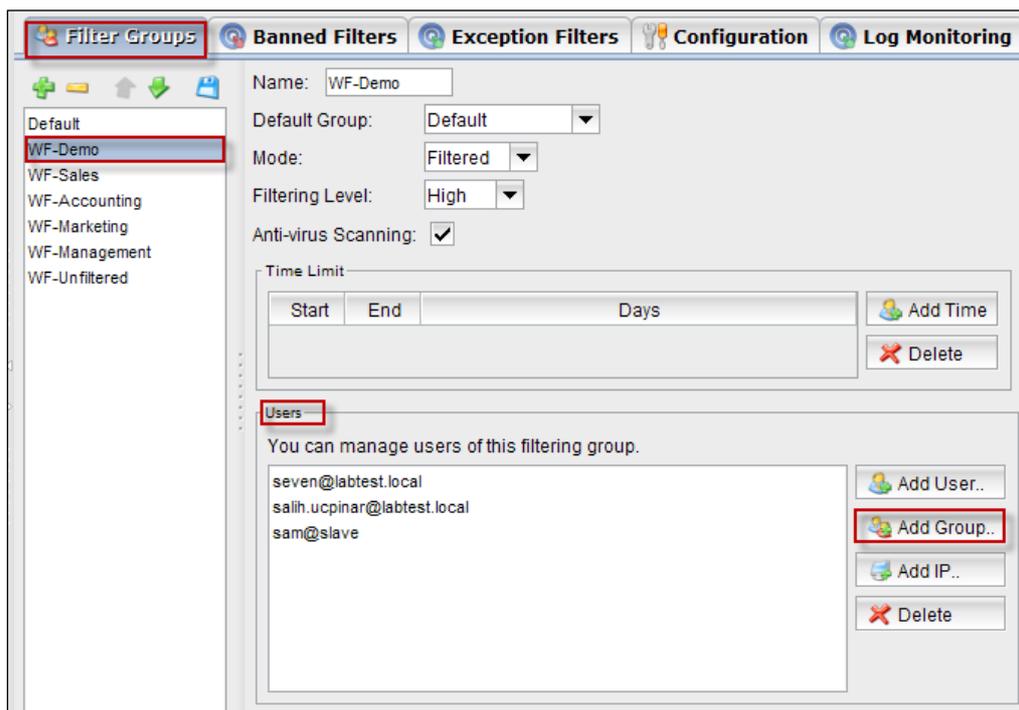


In the below screen, we can notice selected Members added to the Filter Group.

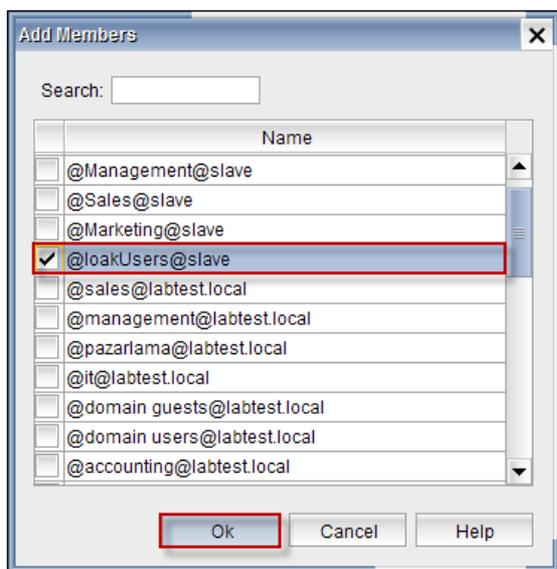


Add Groups

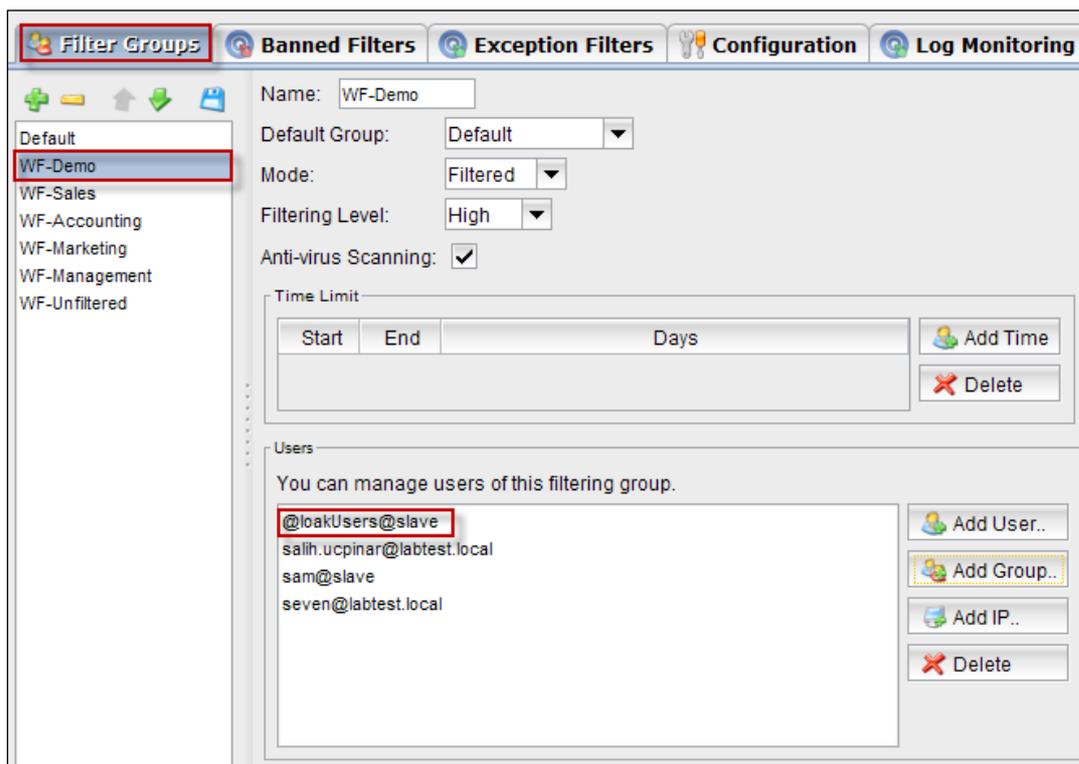
Click on **Add Groups** tab.



Add Members tab appears, select the Groups and click on **Ok**.

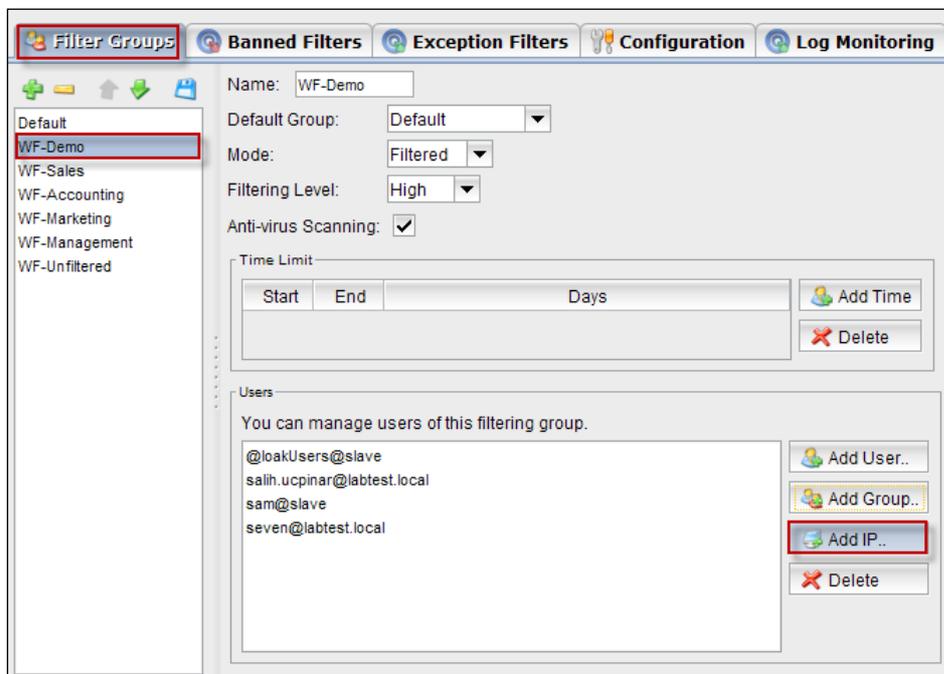


In the below screen, we can notice **Group** added in the Users list.

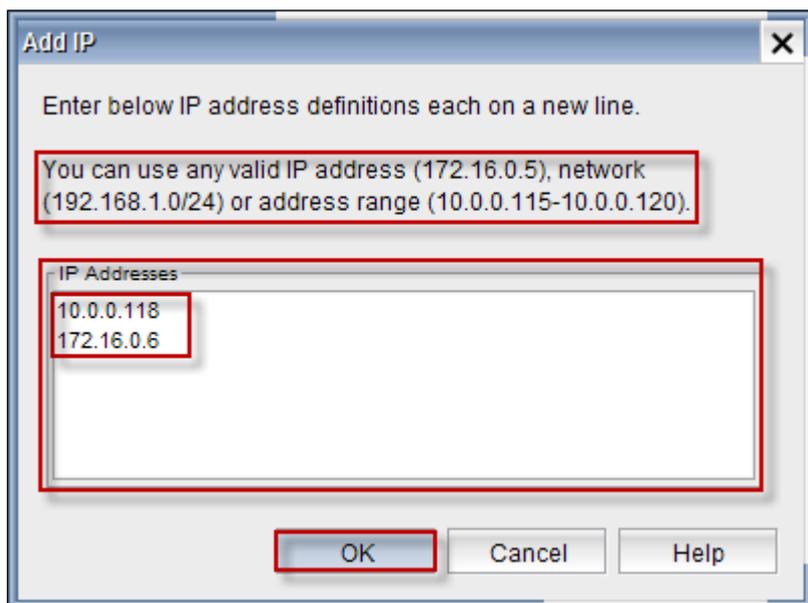


Add IP/ IP Range

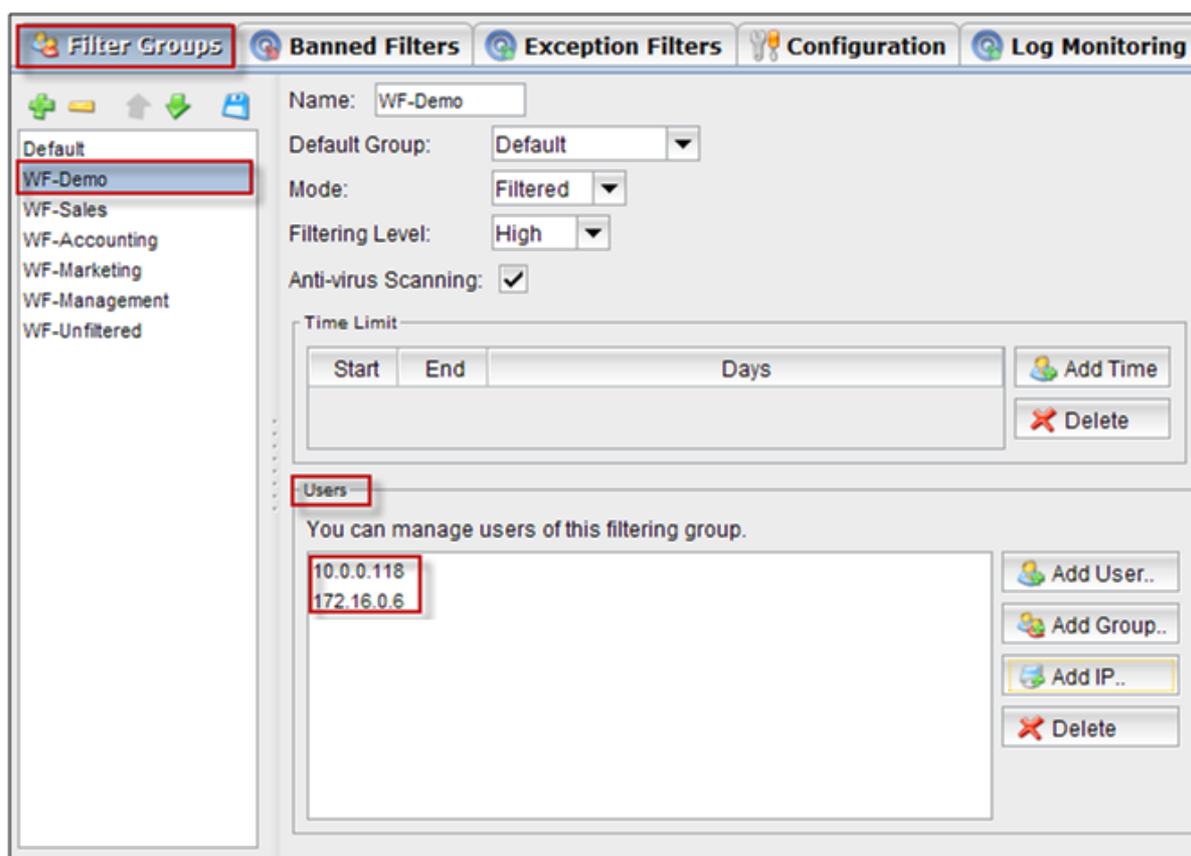
Click on **Add IP** tab.



Add IP tab appears, type valid IP Address within the range mentioned in the below tab and click on **Ok**.

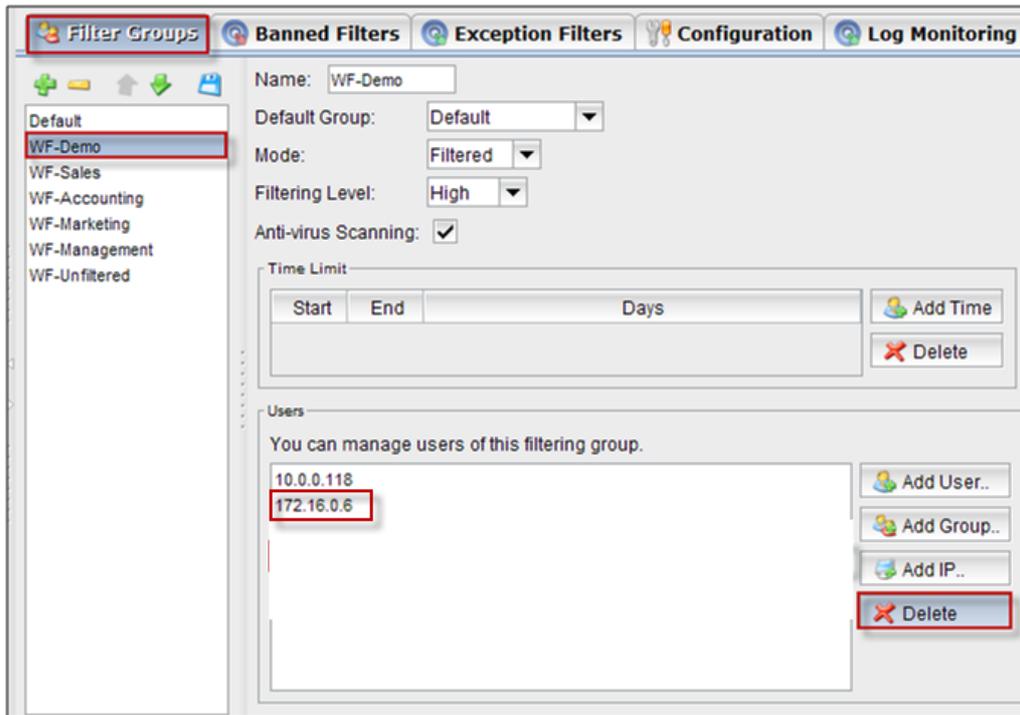


In the below screen, we can notice IP Address in the Users tab.

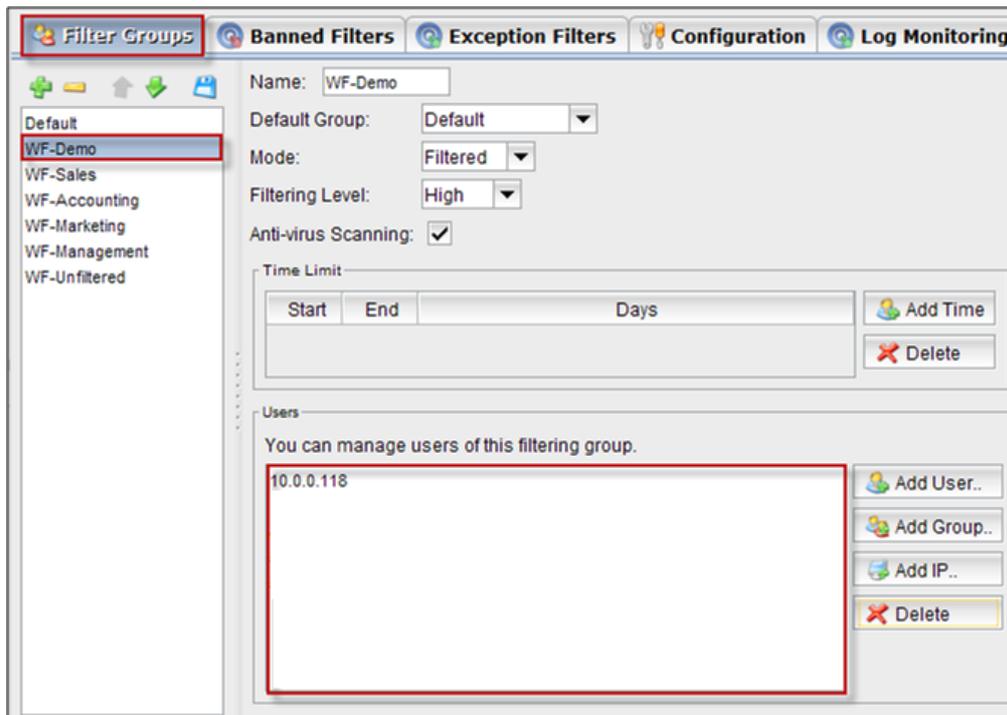


Delete

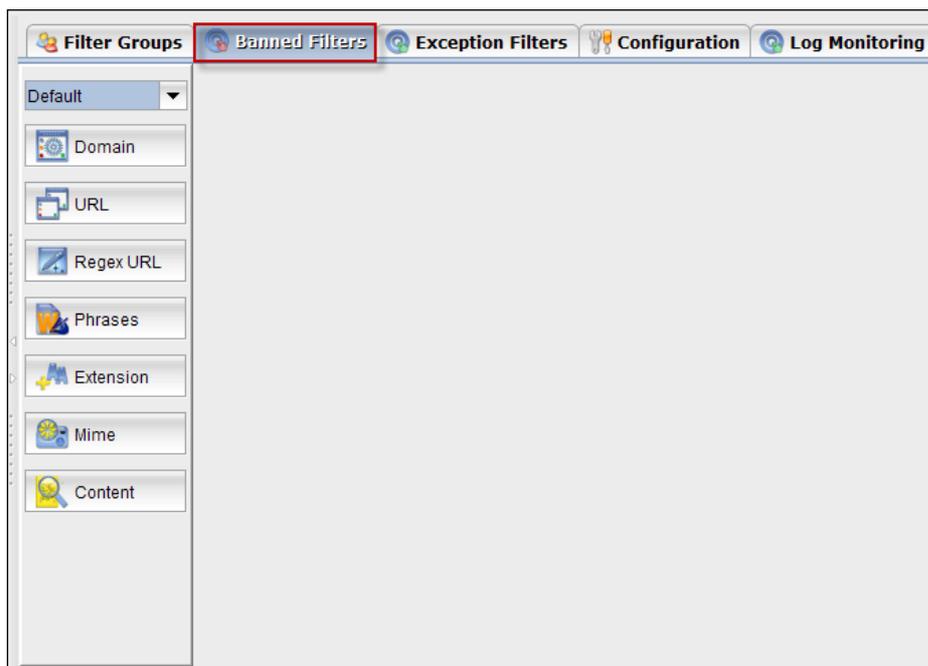
Select the IP Address or User or Group and click on **Delete** tab.



In the below screen, we can notice selected Group deleted.

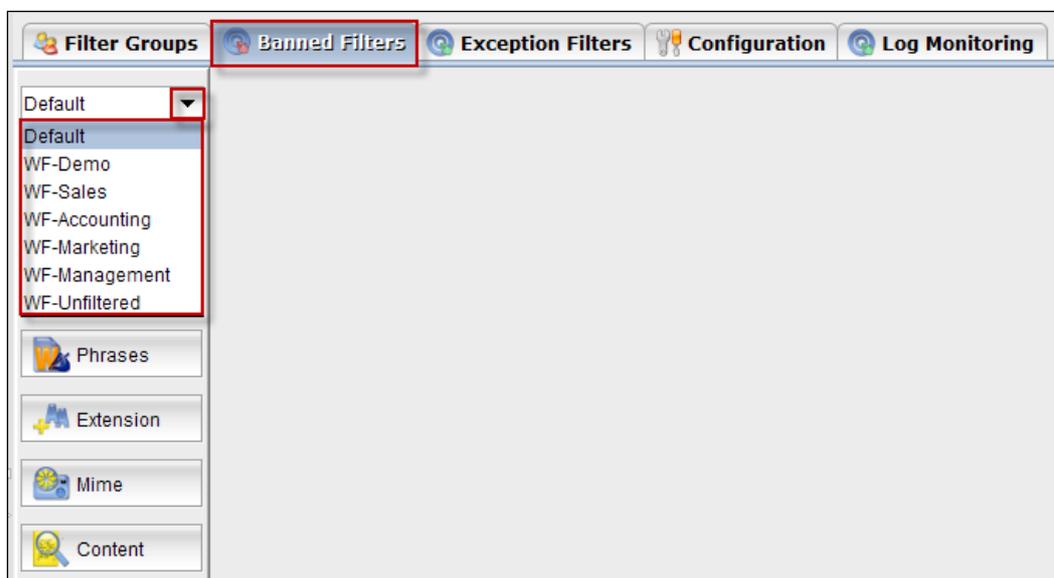


74. Banned Filters



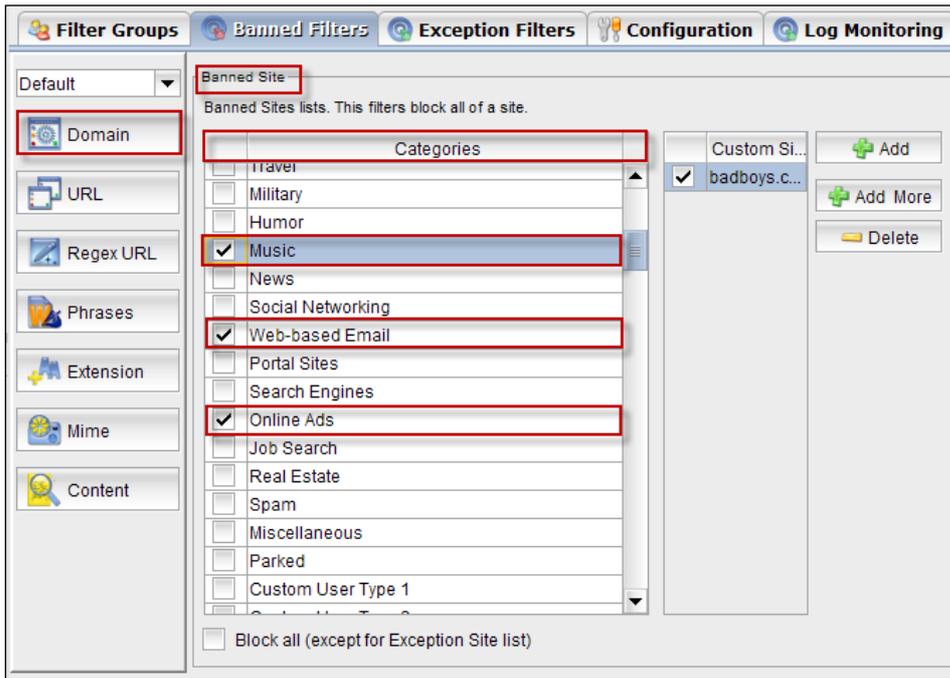
Select the profile from the drop-down menu and below shown settings (Domain, URL, Regex URL, Phrases, Extensions, Mime, and Content) can be done separately for each profile.

In the below screen we have selected default profile.



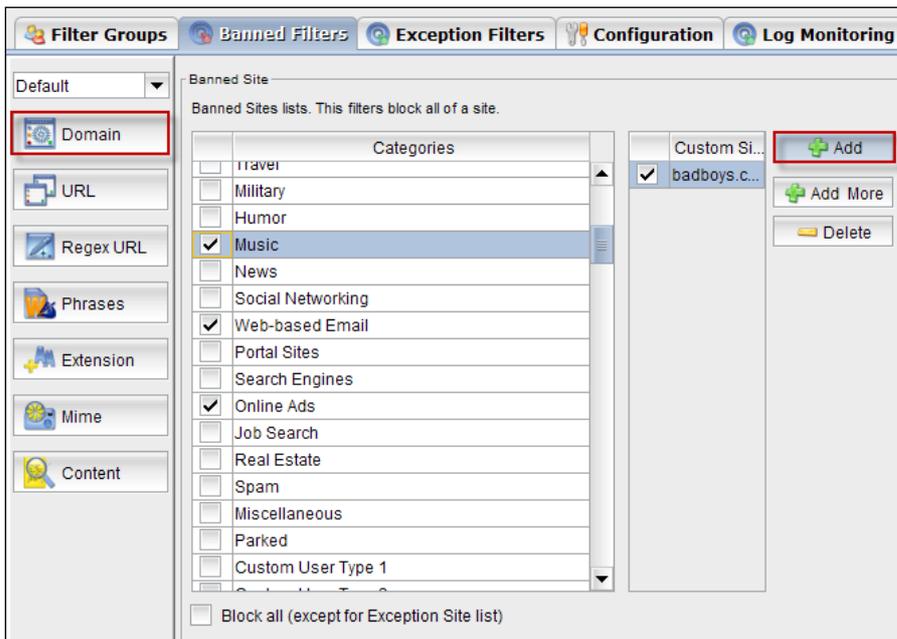
75. Domain/ Category Filtering

Domain filter is the firewall function to help you block the specified domain. When we click on Domain tab, all the categories in the Domain are displayed. Exceptional sites from banning are being selected in the Categories list.

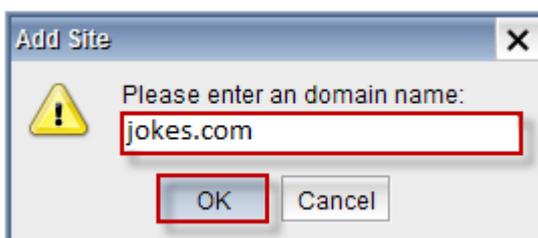


Add

Click on **Add** tab.



Add site tab appears, type domain name to be banned and click **Ok**.

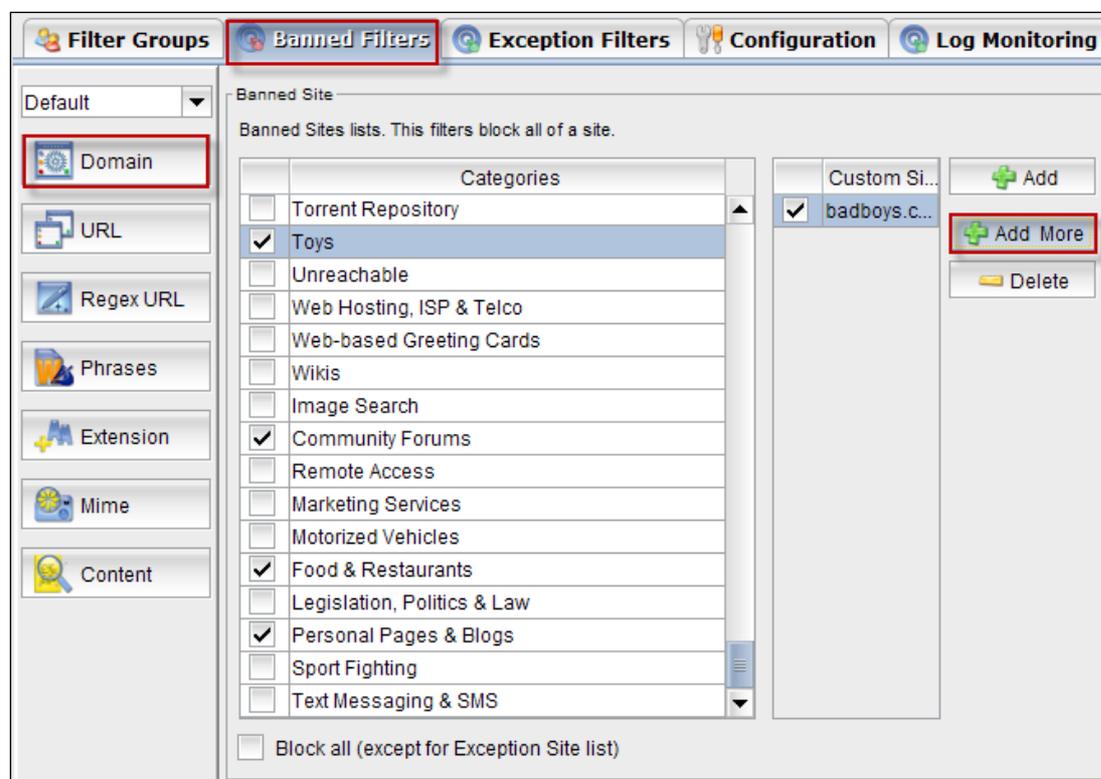


Message tab appears stating that **This site is already in banned list**, Click **Ok**.



Add More

Click on **Add More** tab.



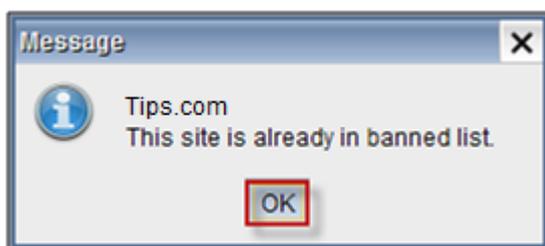
Add Bulk Site tab appears type name of the domain as one in each line and click **Ok**.



Message tab appears stating that **This site is already in banned list**, Click **Ok**.



Message tab appears stating that **This site is already in banned list**, Click **Ok**.

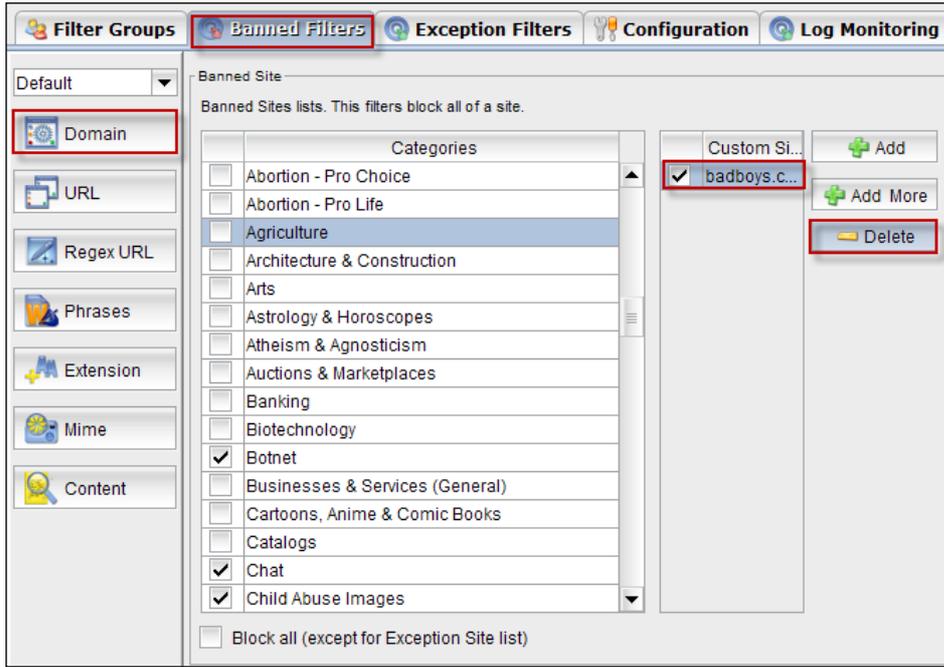


Message tab appears stating that **This site is already in banned list**, Click **Ok**.



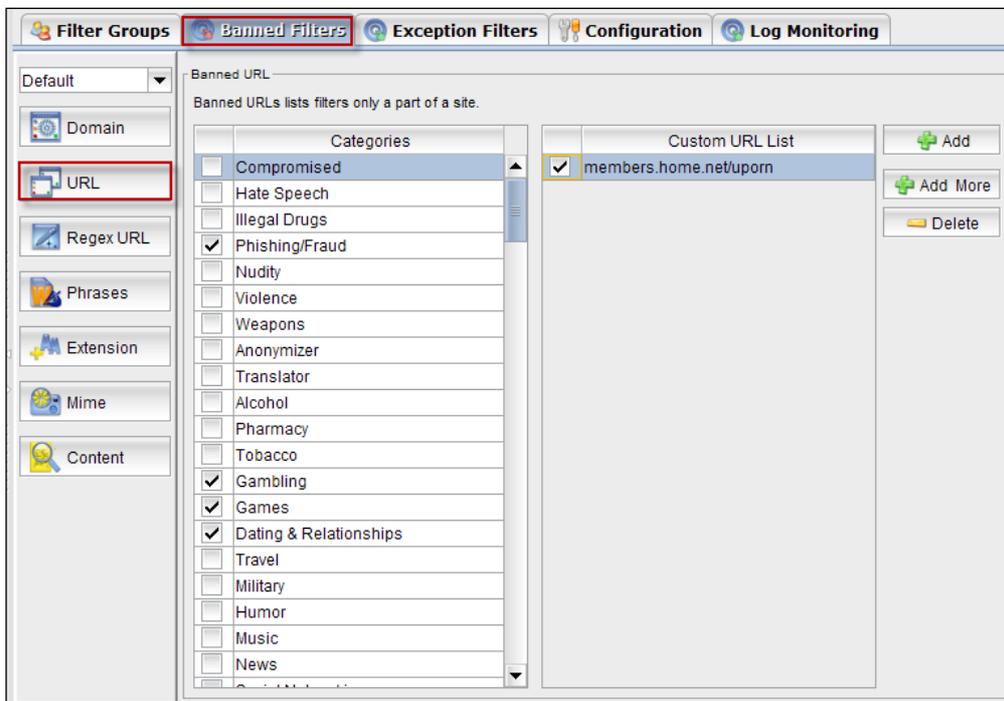
Delete

Select the site and click on **Delete** tab.



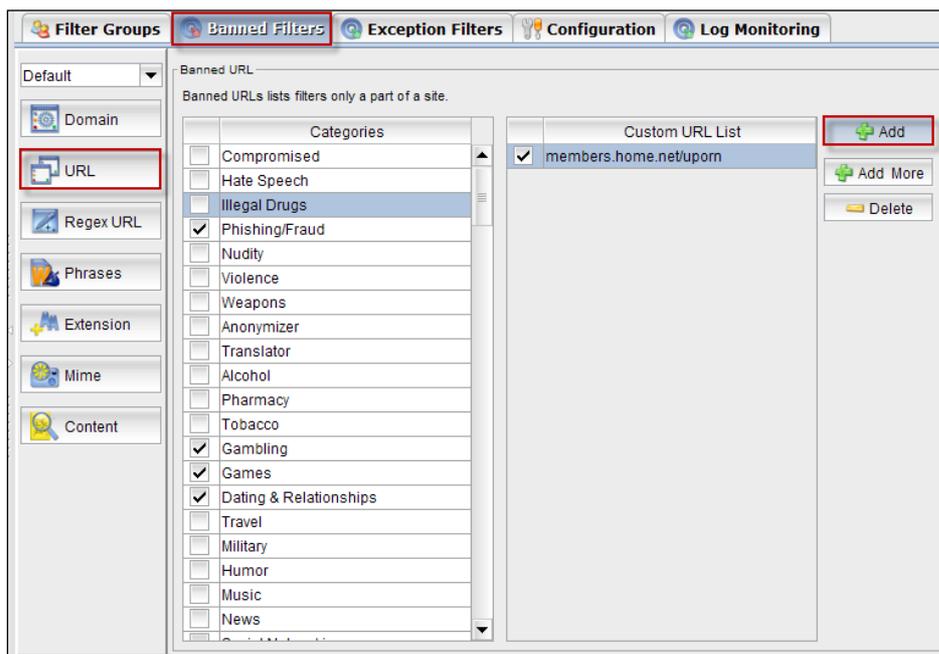
76. URL/Category Filtering

URL categories help us ensure real-time protection against today's targeted and advanced threats.



Add

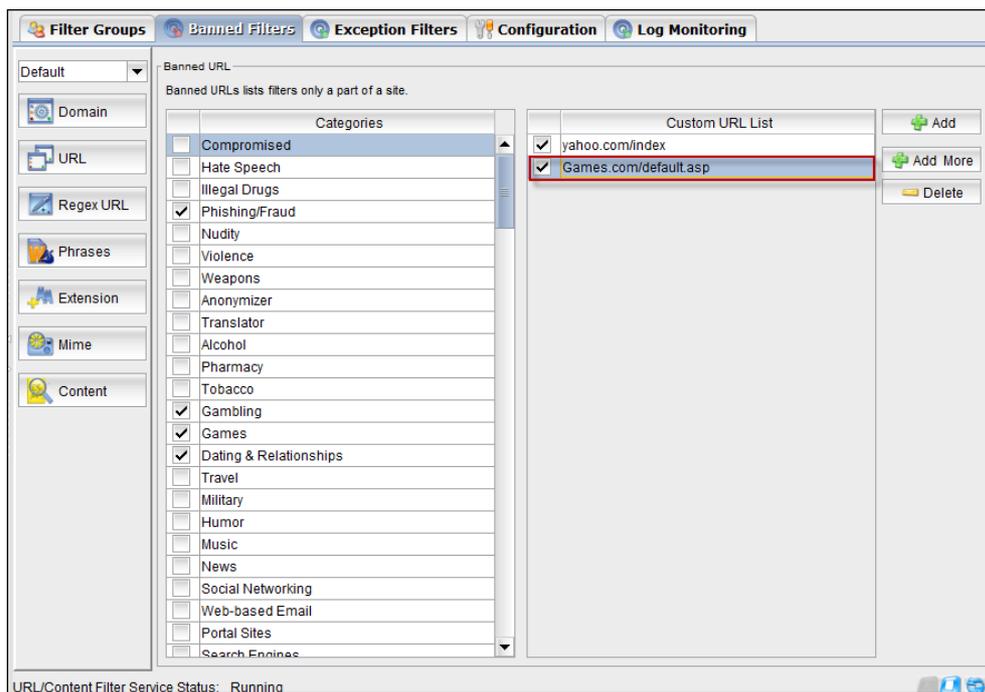
Click on **Add** tab



Add Site tab appears type domain name to be banned and click **Ok**.

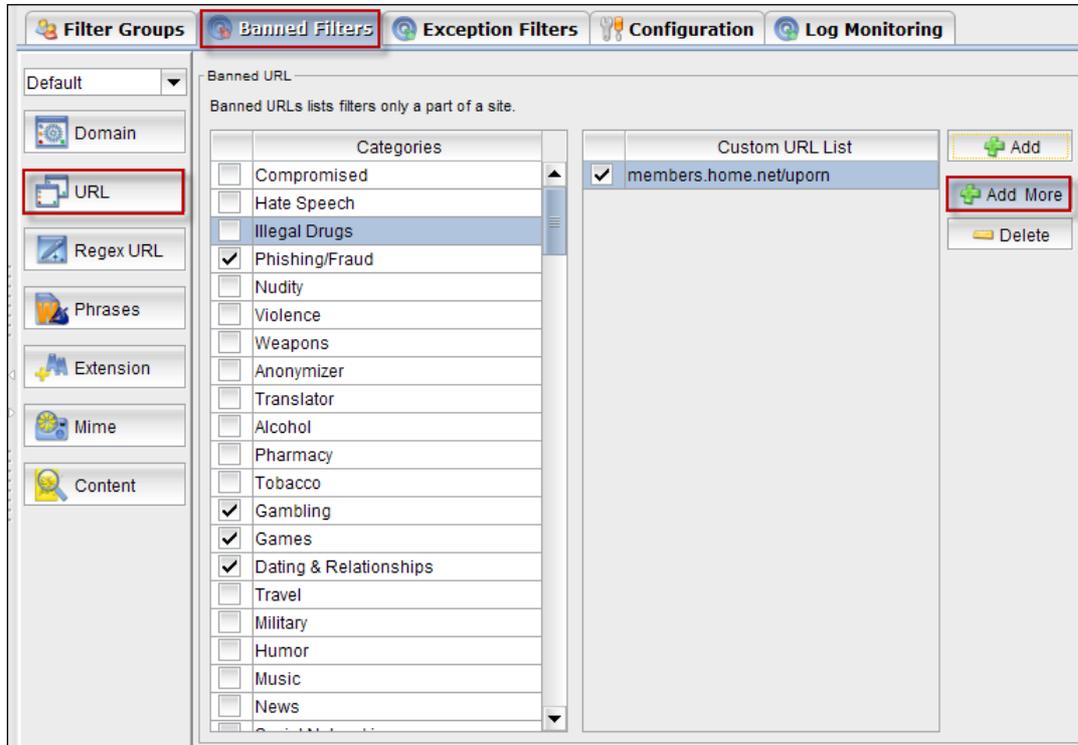


In the below screen, we can notice domain name added in the Banned list.

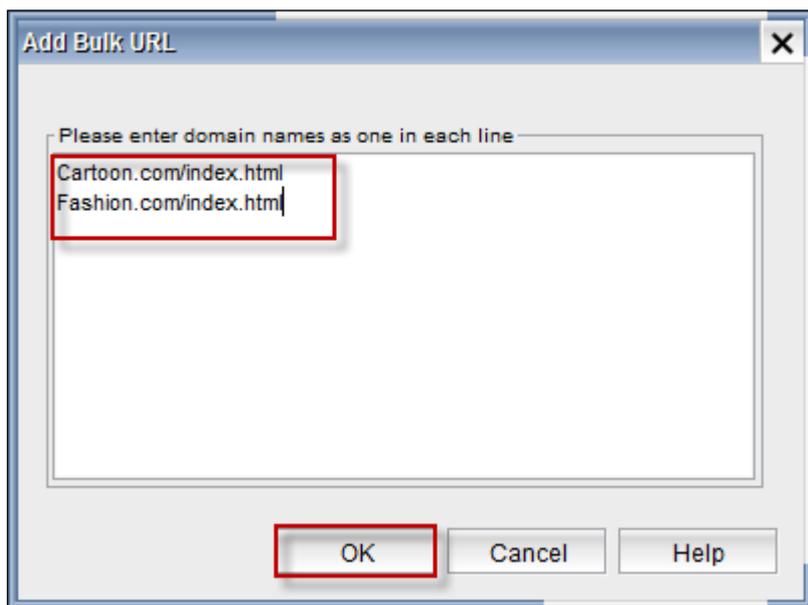


Add More

Click on **Add More** tab.

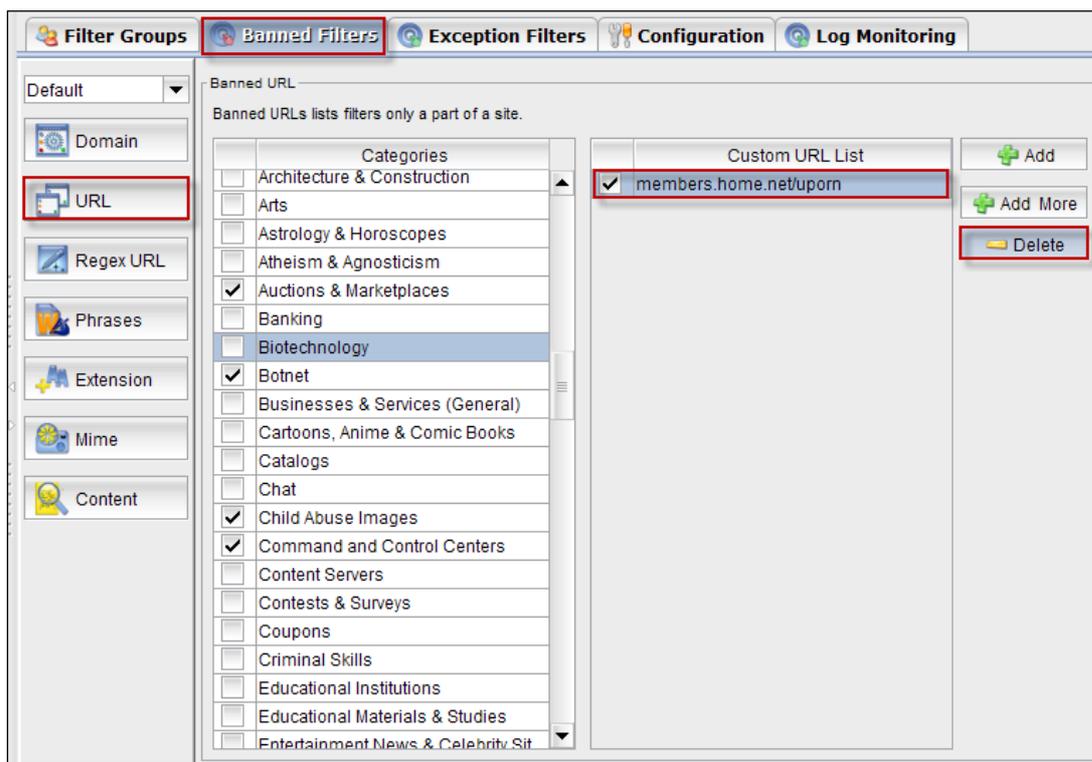


Add Bulk URL tab appears, type name of the domain as one in each line and click **Ok**.



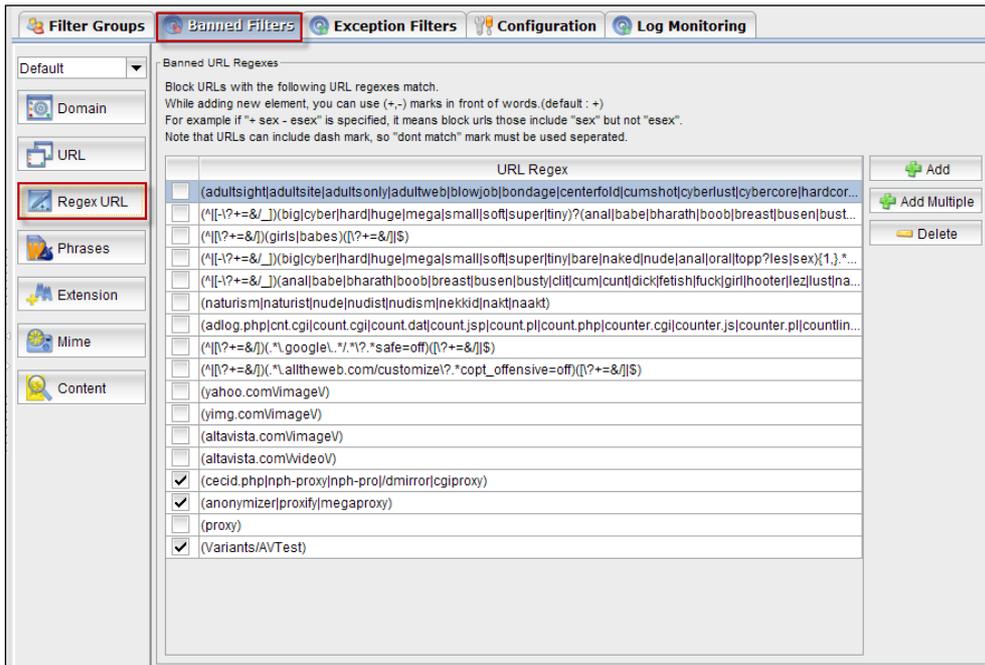
Delete

Select the URL and click on **Delete** tab.



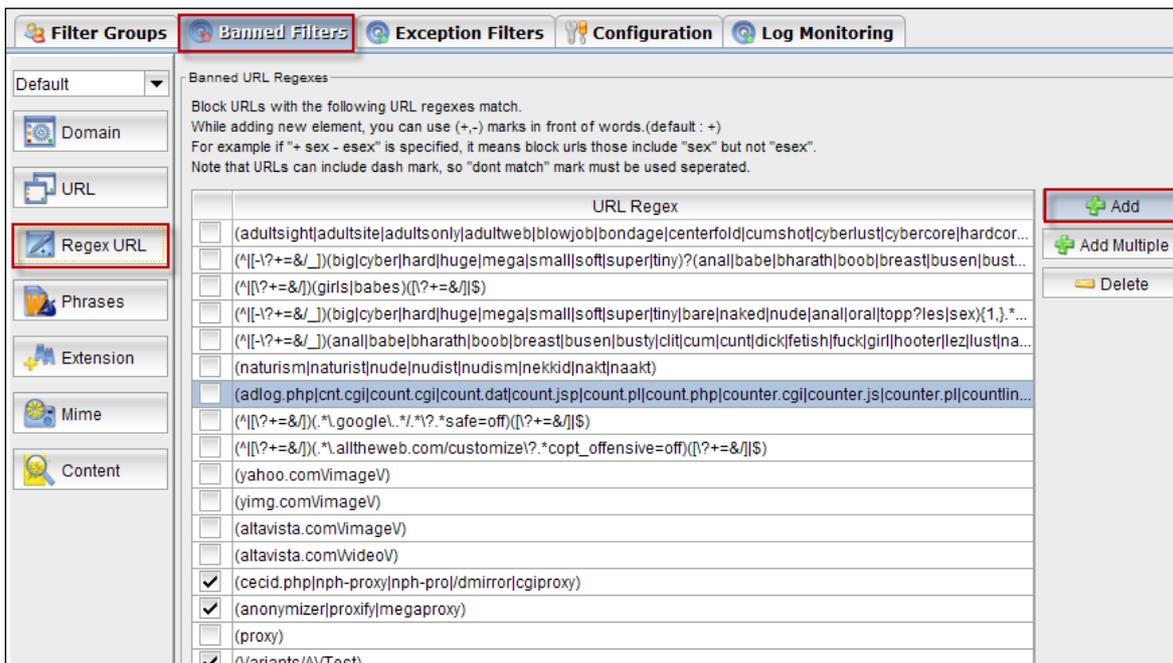
77. Regex URL Filtering

This is completed when parts of the HTTP request are matched with the use of a list of regex patterns. You can either block specific URL's or block all URL's except for a select few particular URL's.



Add

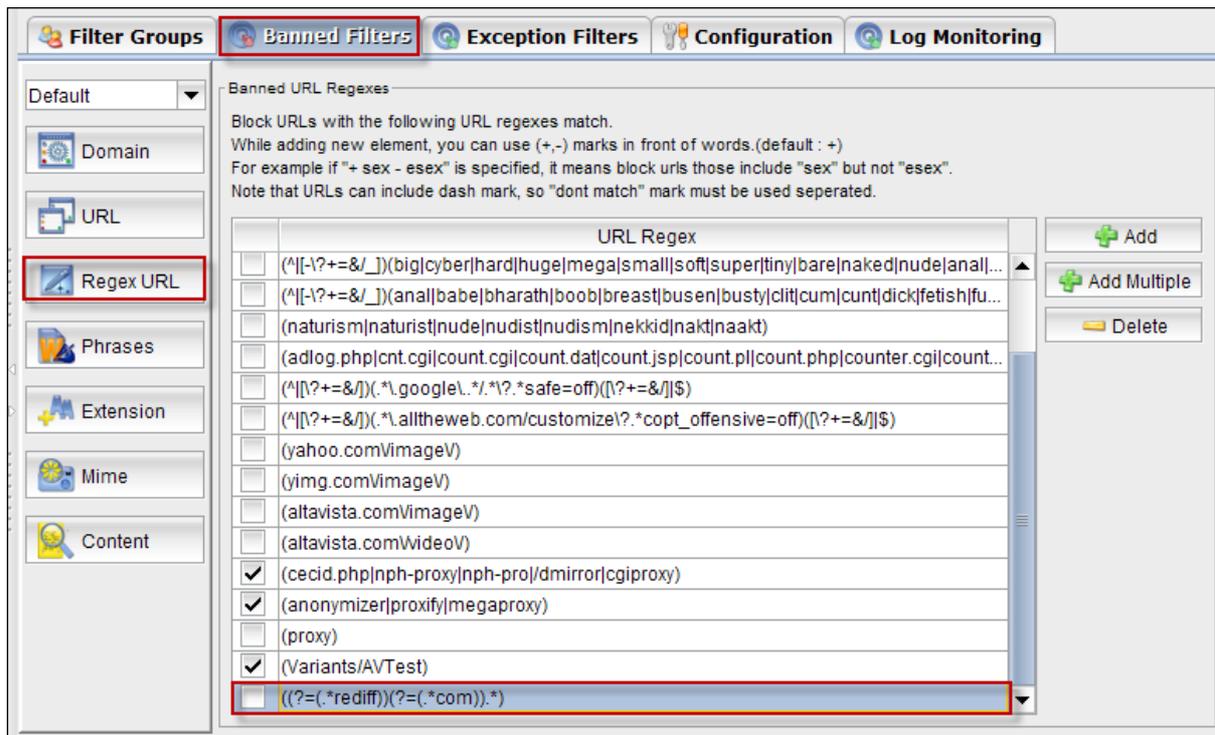
Click on **Add** tab



Add URL Regex tab appears, type regex to be banned and click **Ok**.

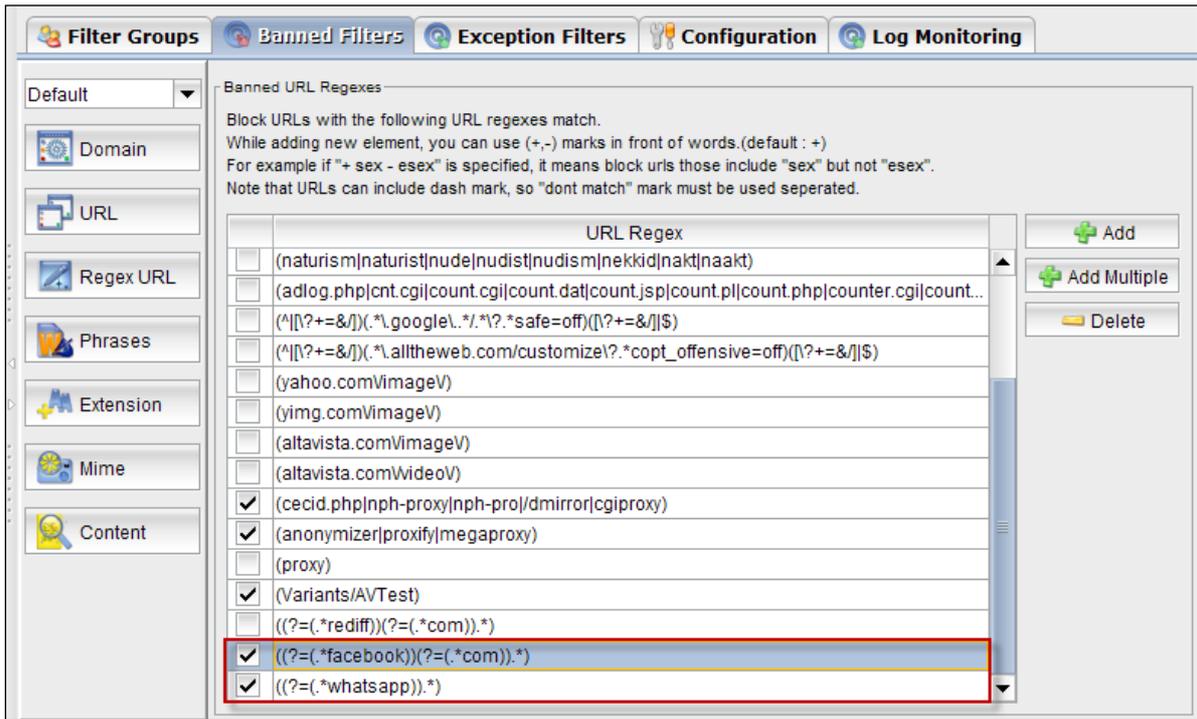


In the below screen, we can notice Regex URL added to list



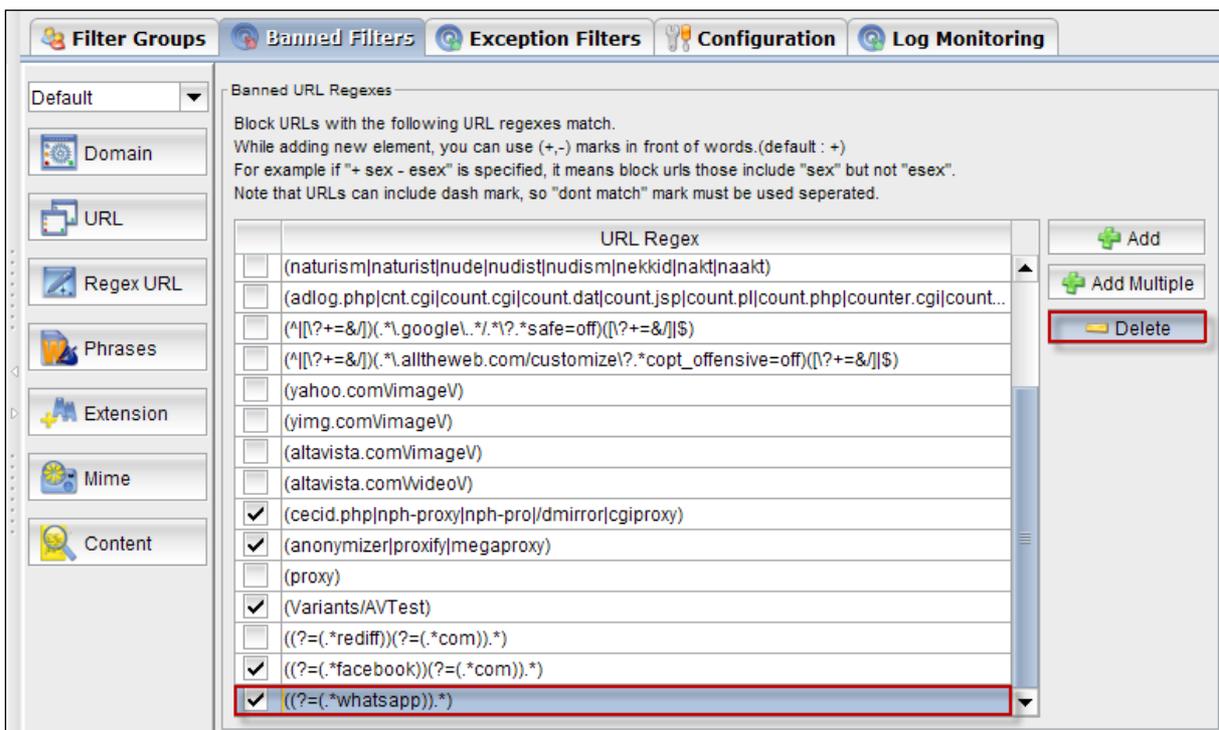
Add More

Click on **Add Multiple** tab.



Delete

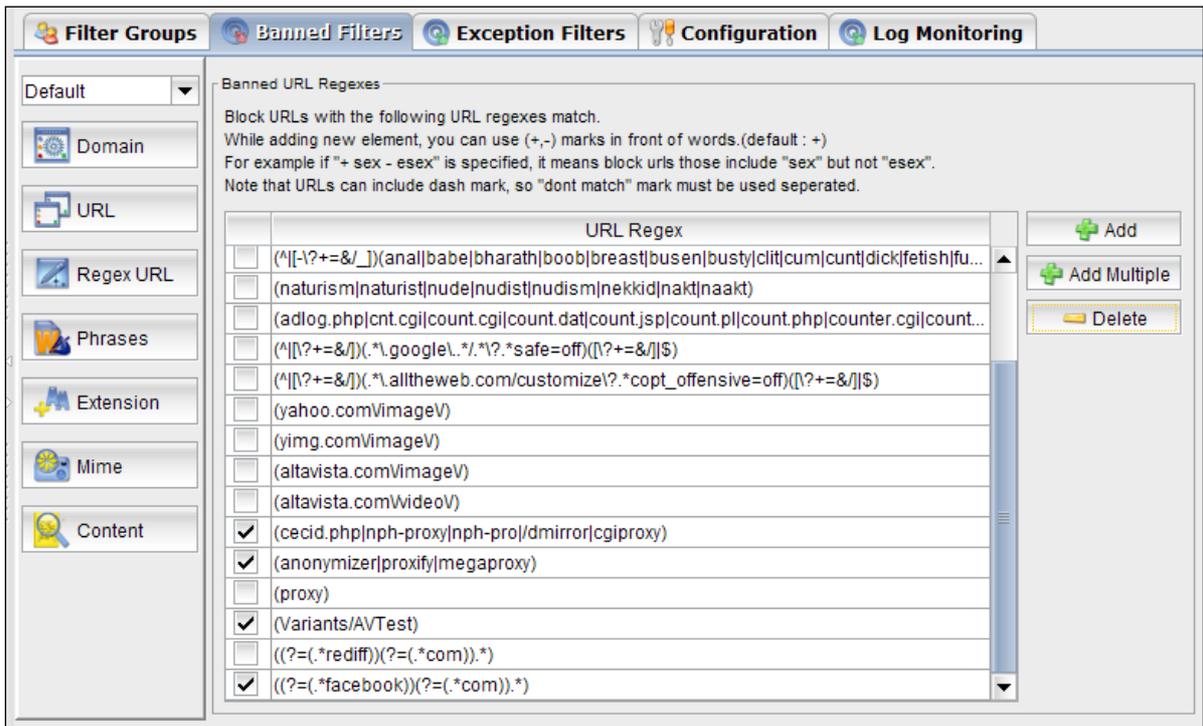
Select Regex URL and click on **Delete** tab.



Delete URL Regex tab appears, click on **Yes**.



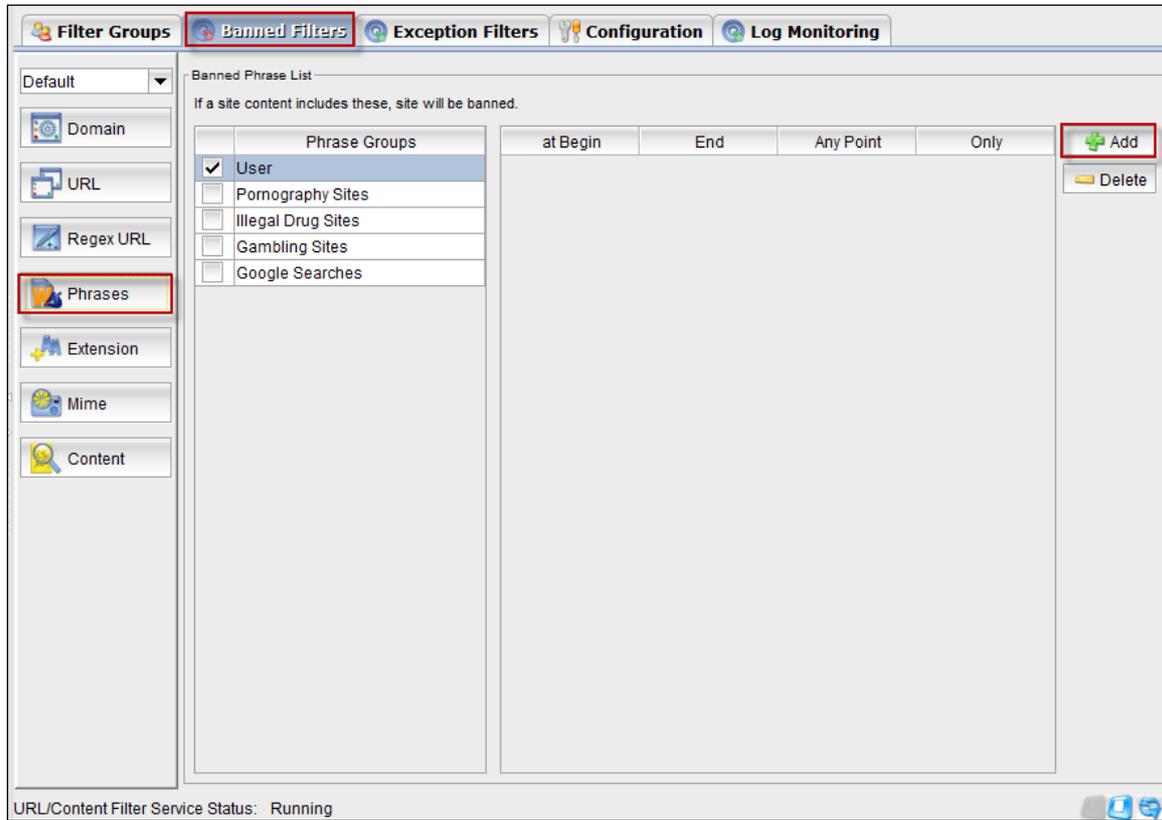
In the below screen, we can notice Regex URL deleted.



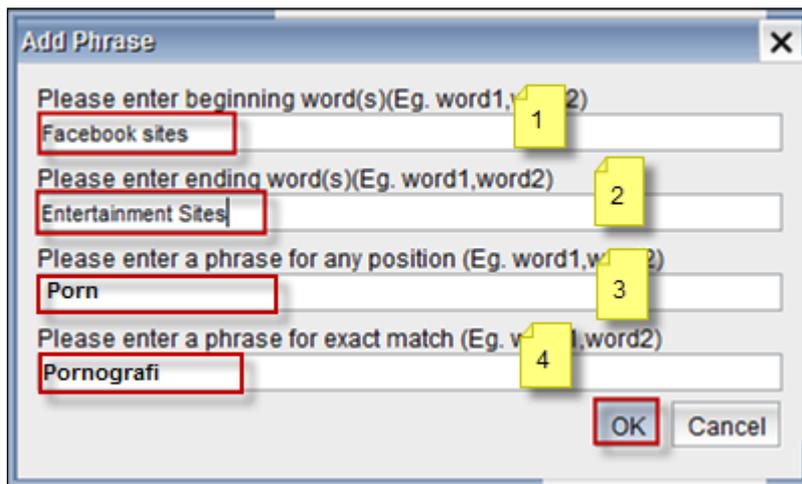
78. Phrases

Add

In Banned filters, Select Phrases and Click on **Add tab**



Add phrase tab appears.



These are the inputs to **Add Phrase**.

1	Beginning Words	Enter the Beginning words of the phrase
2	Ending Words	Enter the Ending words of the phrase
3	Phrase for any position	Enter a phrase
4	Phrase for exact match	Enter a phrase for exact match

Click on **OK**.

In the below we can notice that **Phrase** is added to the list.

The screenshot shows the 'Banned Filters' configuration page. The 'Banned Phrase List' section contains a table with the following data:

Phrase Groups	at Begin	End	Any Point	Only
<input checked="" type="checkbox"/> User	Facebook Sites	Entertainment Sites	porn	pornografi
<input type="checkbox"/> Pornography Sites				
<input type="checkbox"/> Illegal Drug Sites				
<input type="checkbox"/> Gambling Sites				
<input type="checkbox"/> Google Searches				

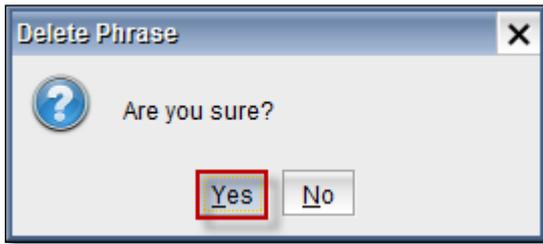
The 'Add' button is visible on the right side of the table.

Delete

Select the Phrase from the list and click on **delete** tab.

The screenshot shows the 'Banned Filters' configuration page, identical to the previous one, but with the 'Delete' button highlighted in red. The 'User' phrase group is selected in the list.

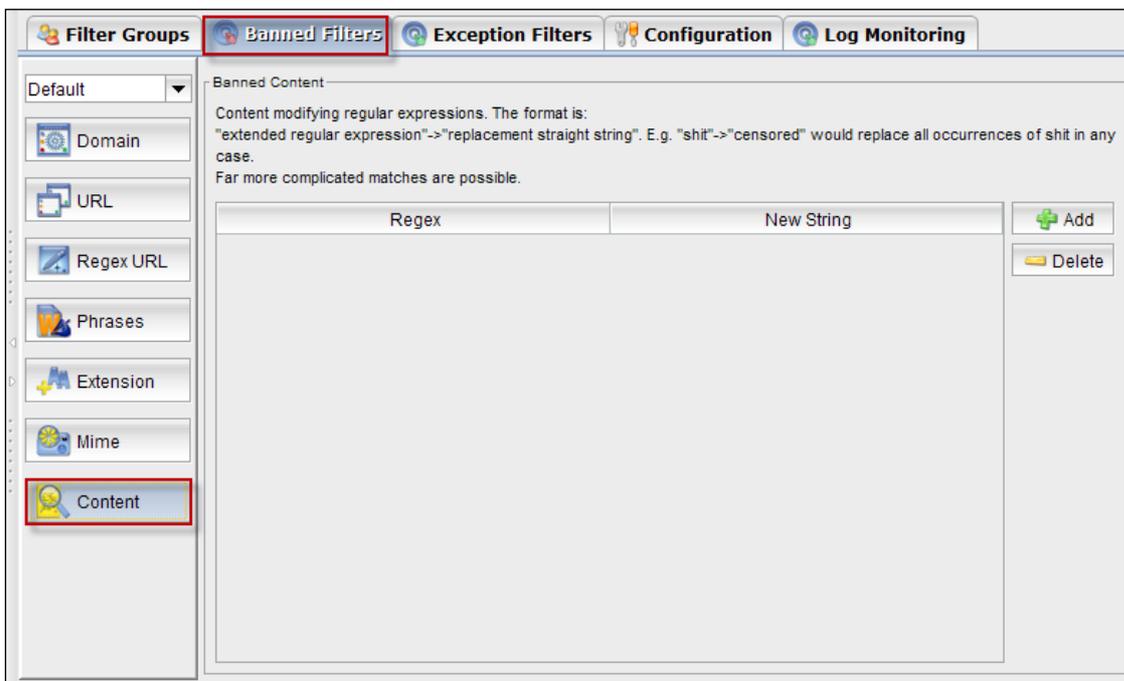
Delete Phrase tab appears stating Are you sure? Click on **Yes**.



79. Content Change

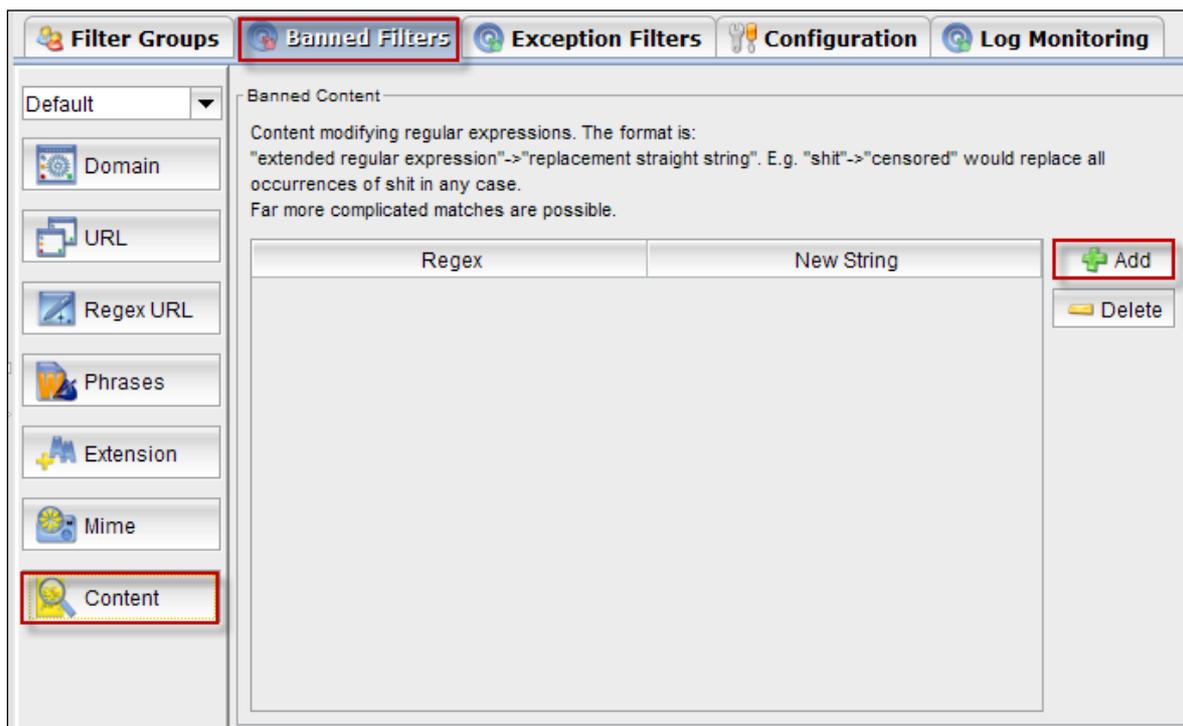
In this section, as seen in the places specified words or addresses to the new string to be replaced with the value entered into the field provided.

Content Filtering generally refers to the filtering of inappropriate content or messages, such as content containing objectionable materials, personal or sensitive information, in terms of information security. Content Filtering has different applications like for example, in internet the browsing, receiving mails accessing database, etc.



Add

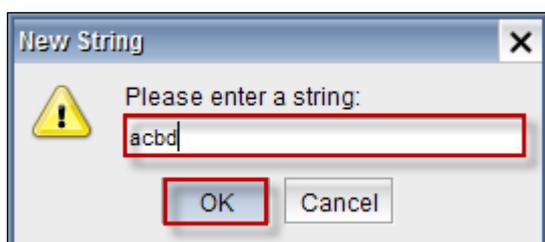
Click on **Add** tab



Add New Regular Expression tab appears, type regex and click **Ok**.



New string tab appears, type string and click **Ok**.



In the below screen, we can notice Regex with new string.

The screenshot shows the 'Banned Filters' configuration page. On the left is a sidebar with filter categories: Default, Domain, URL, Regex URL, Phrases, Extension, Mime, and Content. The main area is titled 'Banned Content' and contains instructions: 'Content modifying regular expressions. The format is: "extended regular expression"->"replacement straight string". E.g. "shit"->"censored" would replace all occurrences of shit in any case. Far more complicated matches are possible.' Below this is a table with two columns: 'Regex' and 'New String'. A single row is present with 'facebook.com' in the 'Regex' column and 'acbd' in the 'New String' column. To the right of the table are 'Add' and 'Delete' buttons.

Regex	New String
facebook.com	acbd

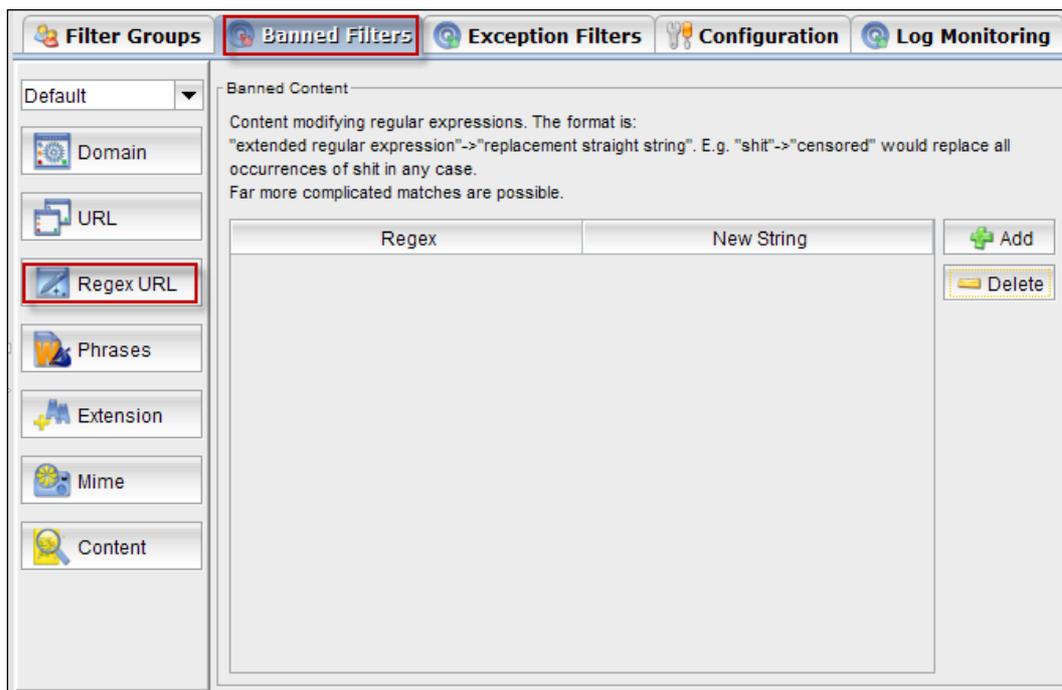
Delete

This screenshot is identical to the one above, showing the 'Banned Filters' configuration page with the 'facebook.com' entry. In this version, the 'Delete' button on the right side of the table is highlighted with a red border, indicating the action to be performed.

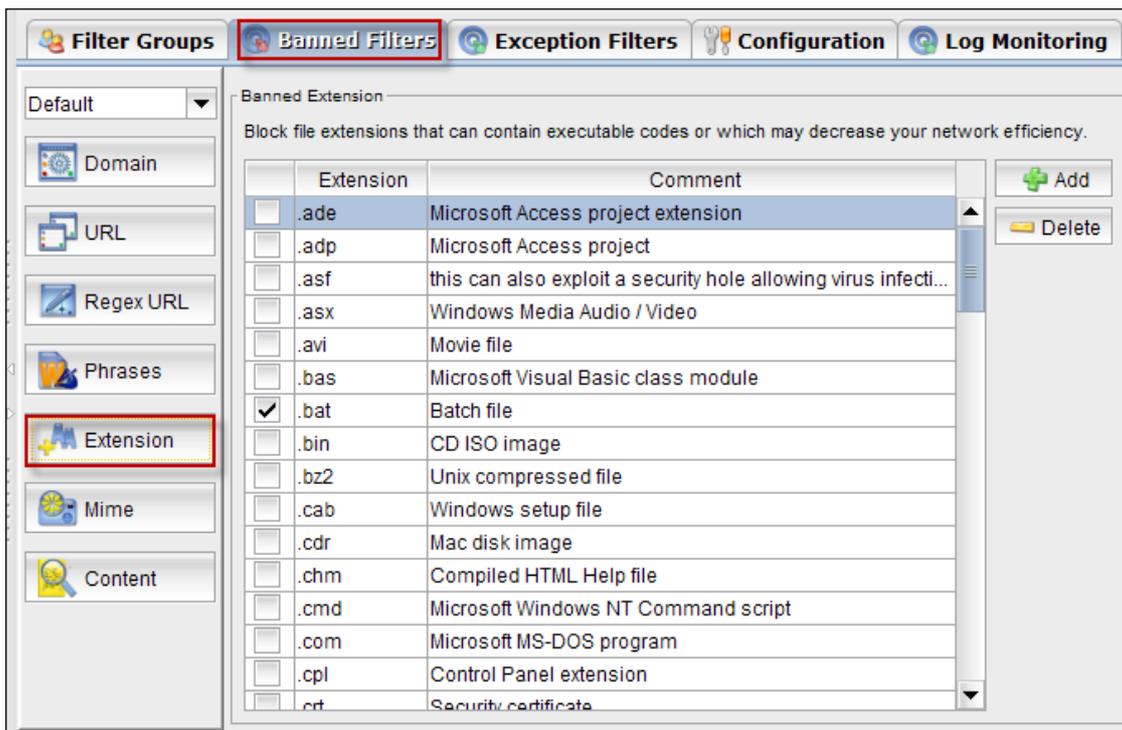
Delete Content tab appear, click on **Yes**.



In the below screen, we can notice content is deleted.

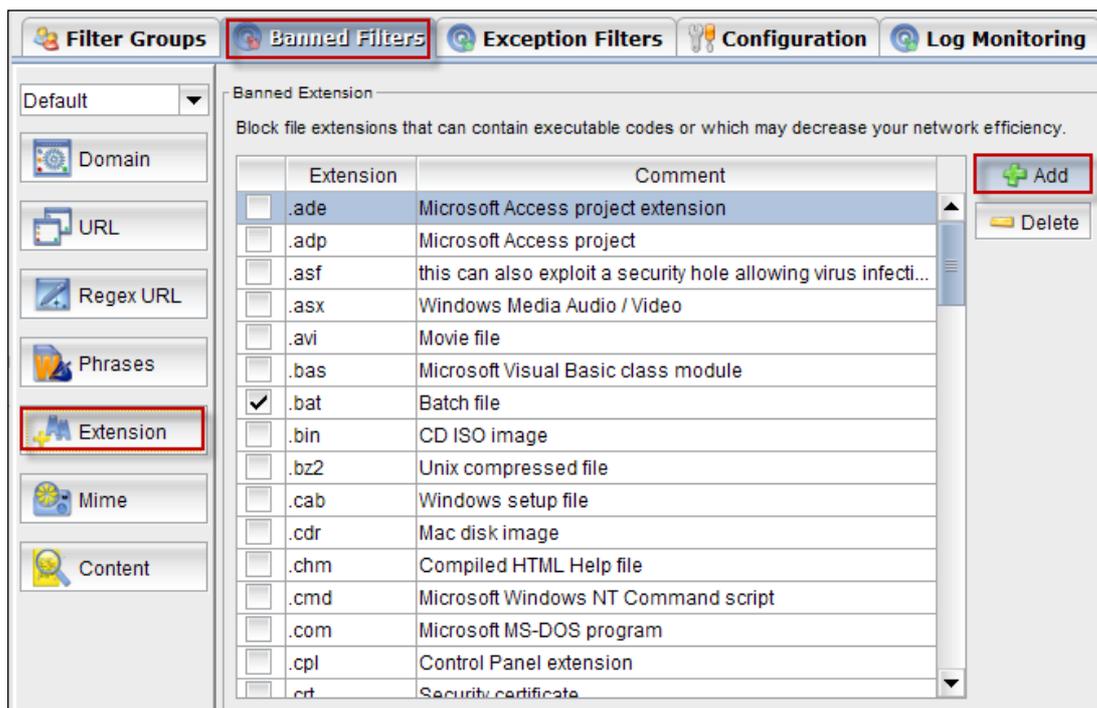


80. Extension Filter

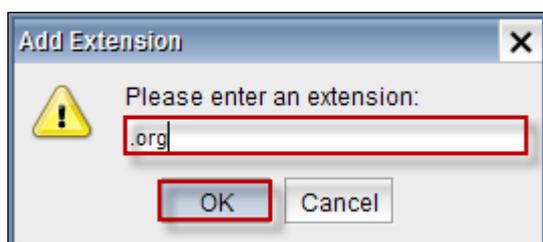


Add

Click on **Add** tab.



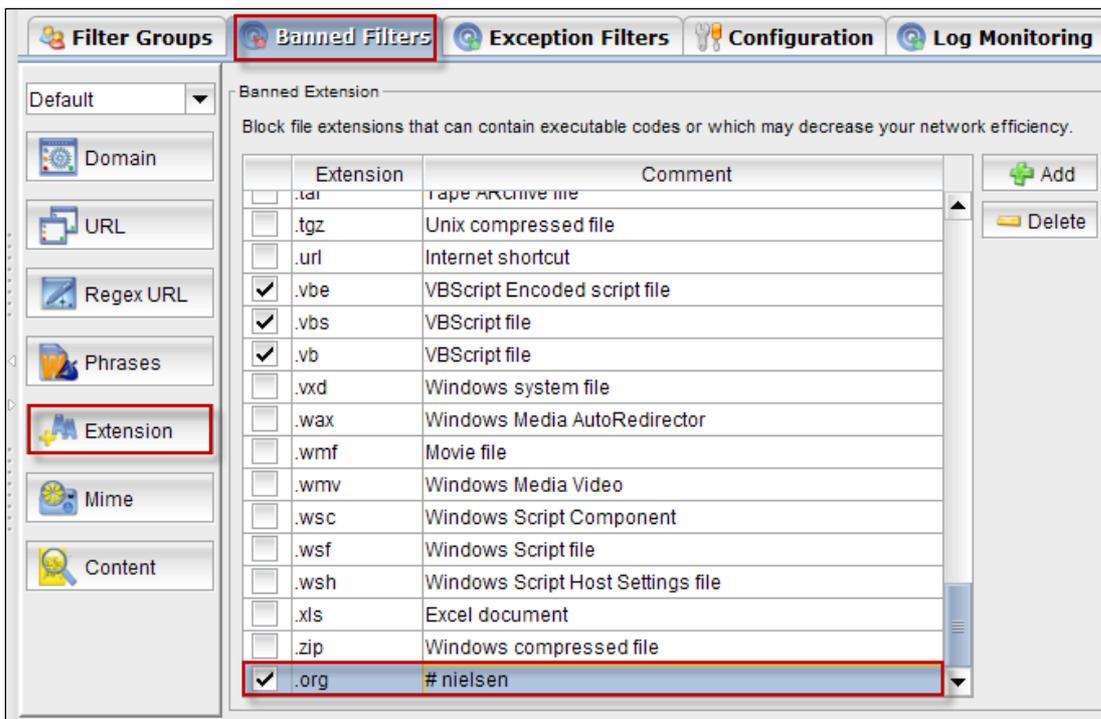
Add Extension tab, type extension and click **Ok**.



Add Comment tab appears, type comment for the extension and click **Ok**.

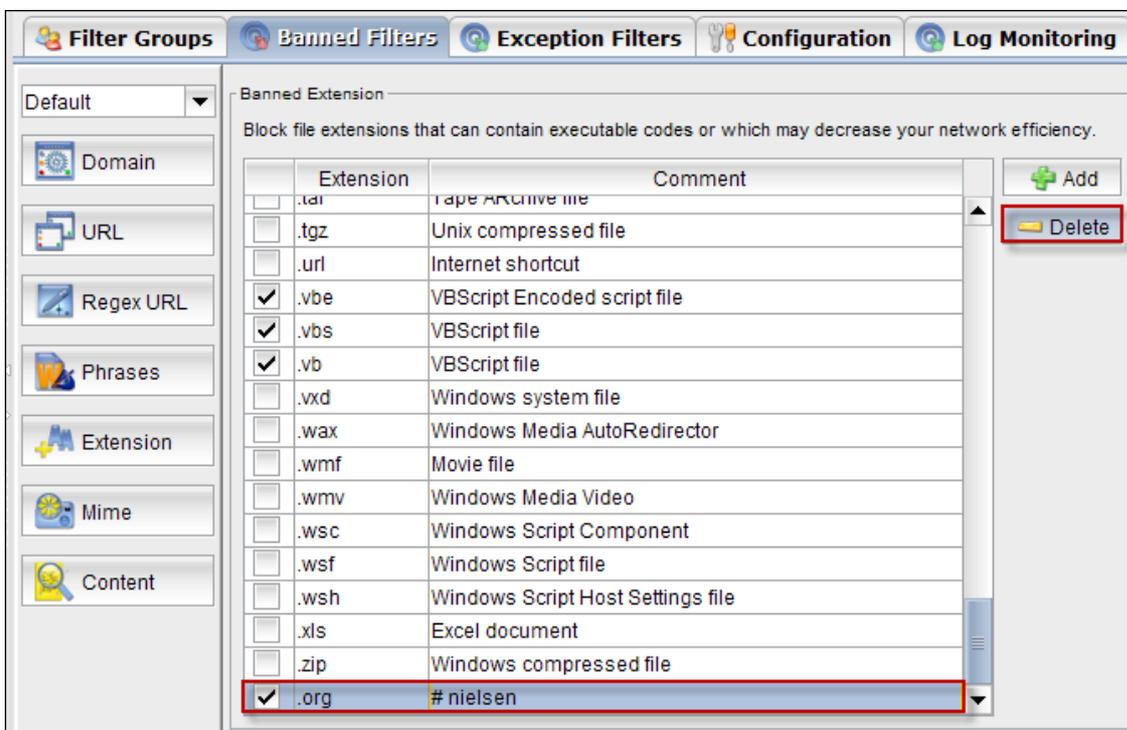


In the below screen, we can notice extension added to list.

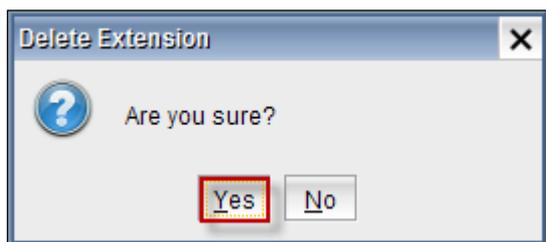


Delete

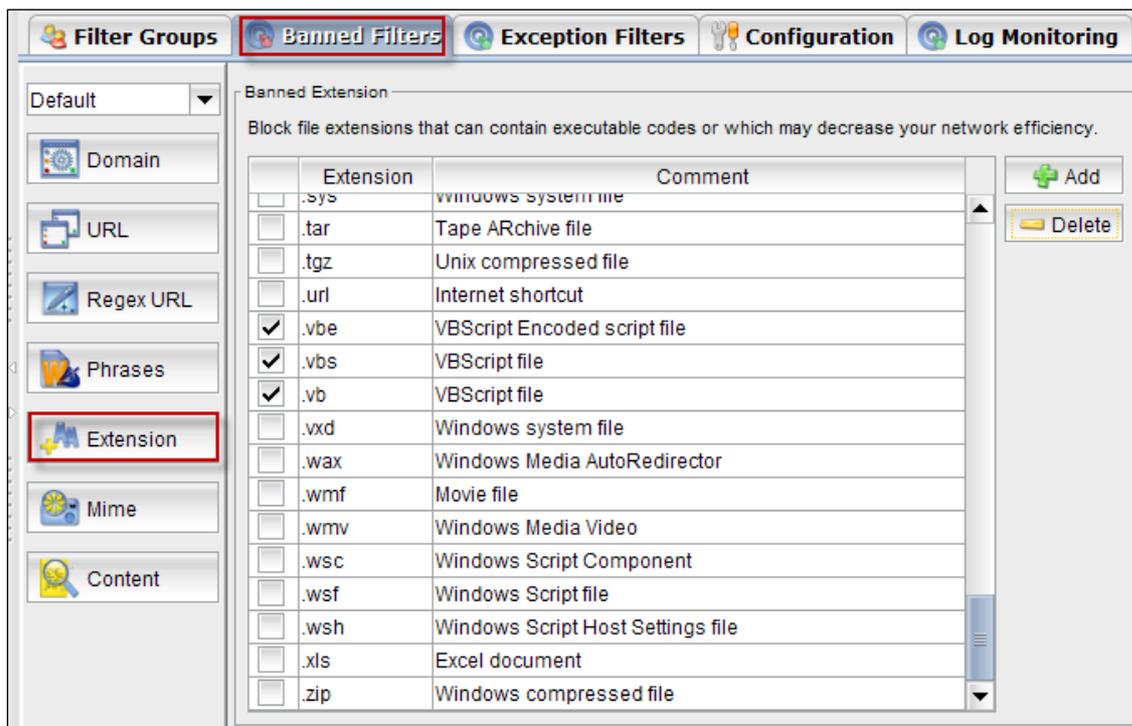
Select the extension and click on **Delete** tab.



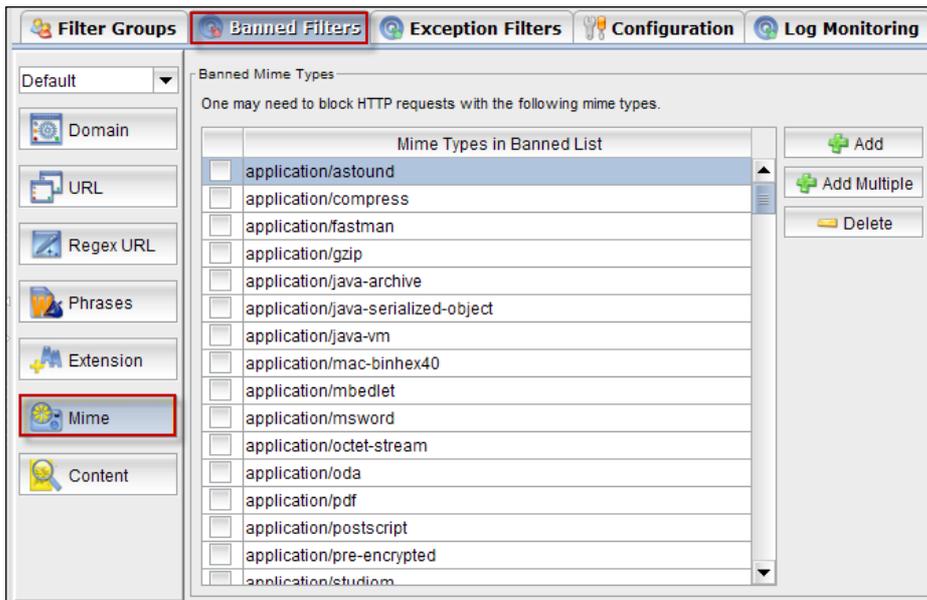
Delete Extension tab appears, click on **Yes**.



In the below screen, we can notice extension deleted.

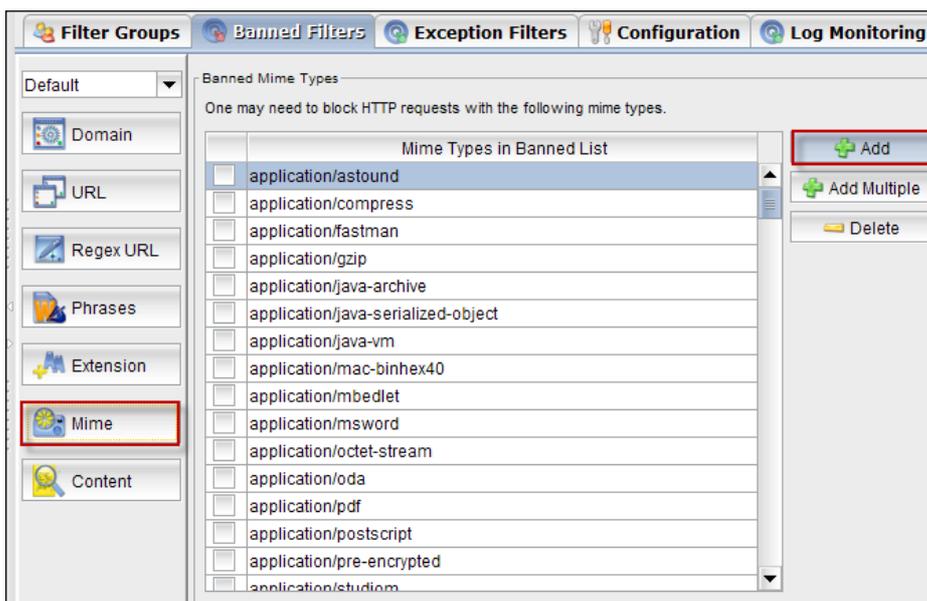


81. Application Types Filter (MIME)



Add

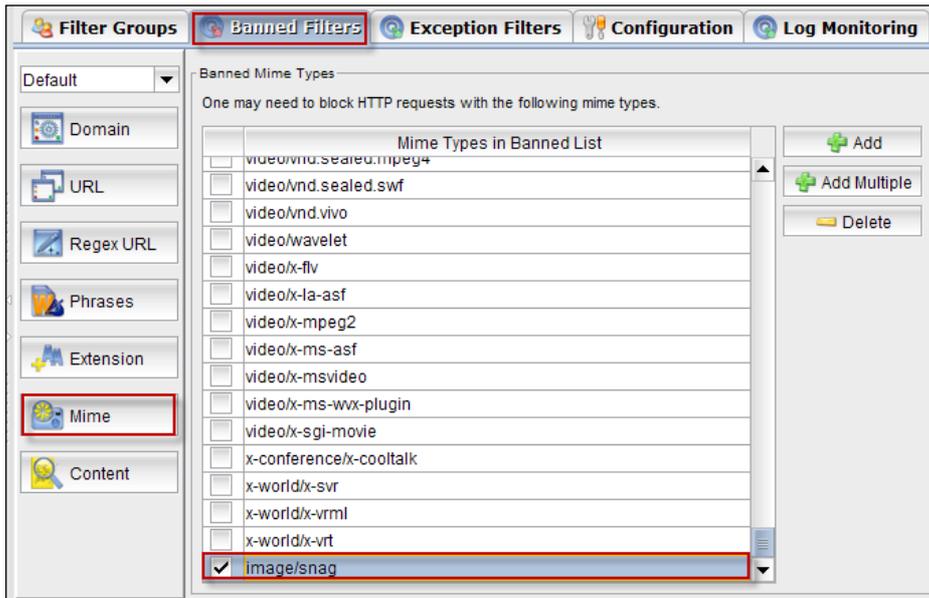
Click on **Add** tab.



Add Mime tab appears, give Mime type and click **Ok**.

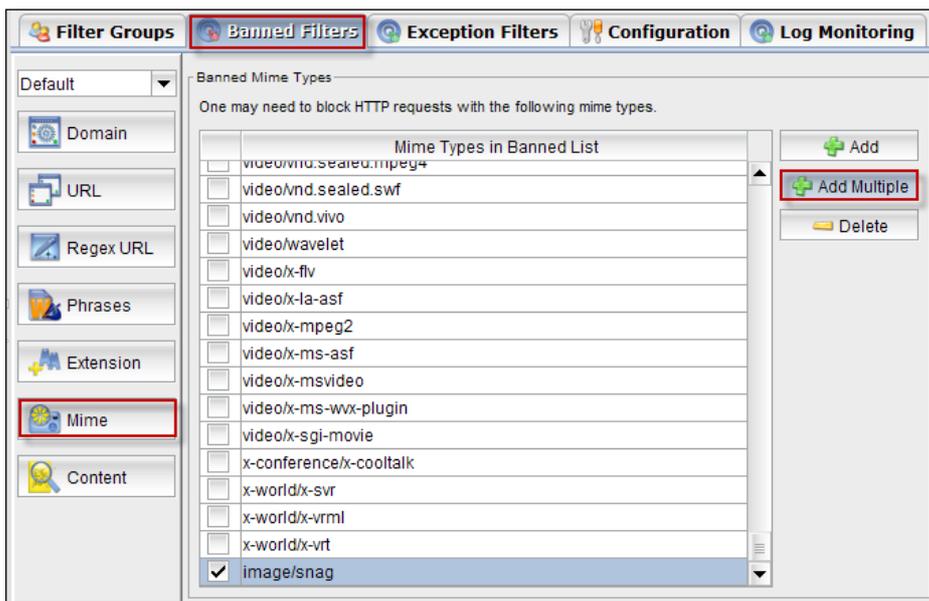


In the below screen, we can notice Mime type added in the list.

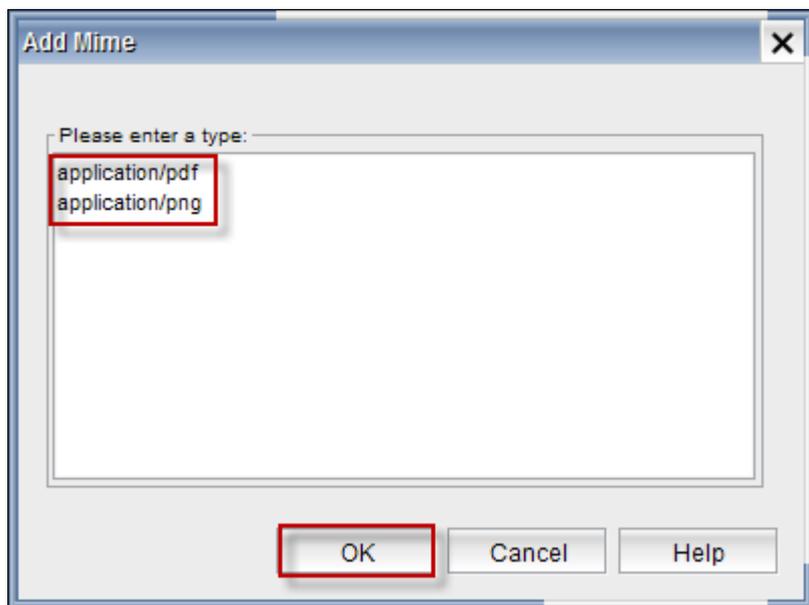


Add More

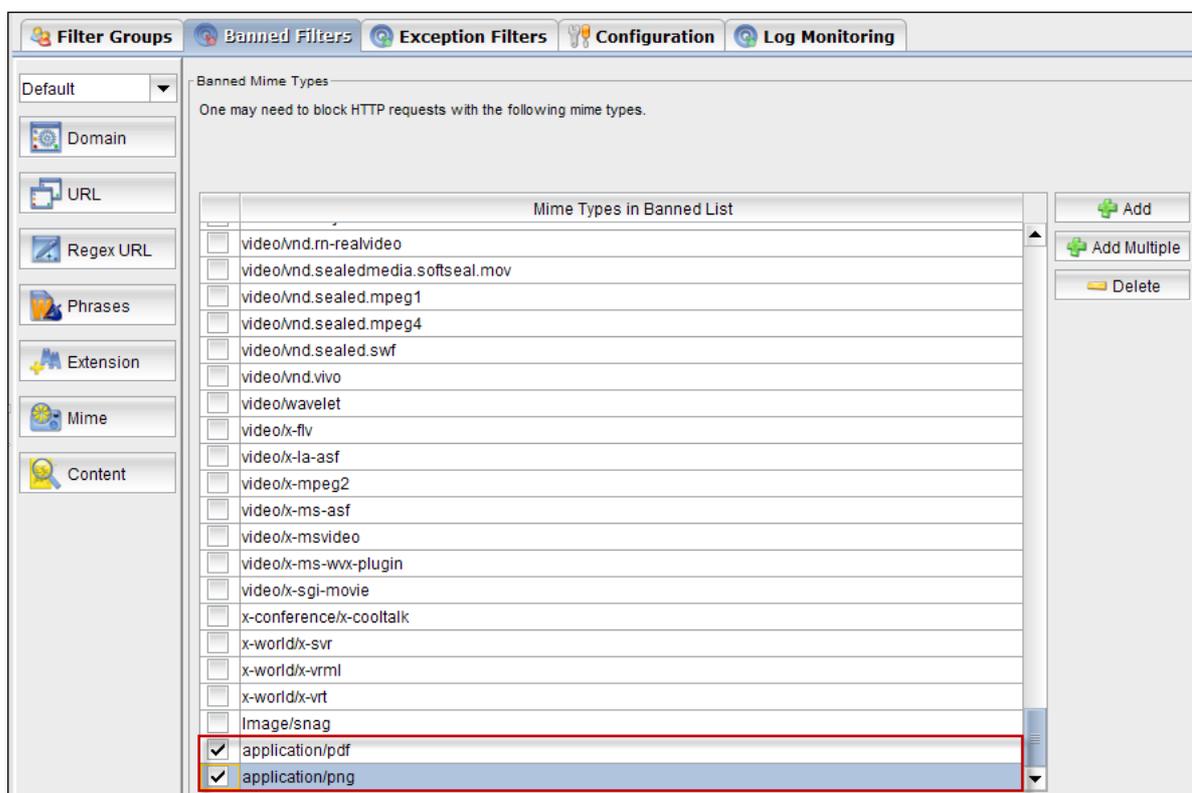
Click on **Add Multiple** tab.



When the below screen appears enter the Mime extensions of the applications which you want to ban and click on **Ok**.

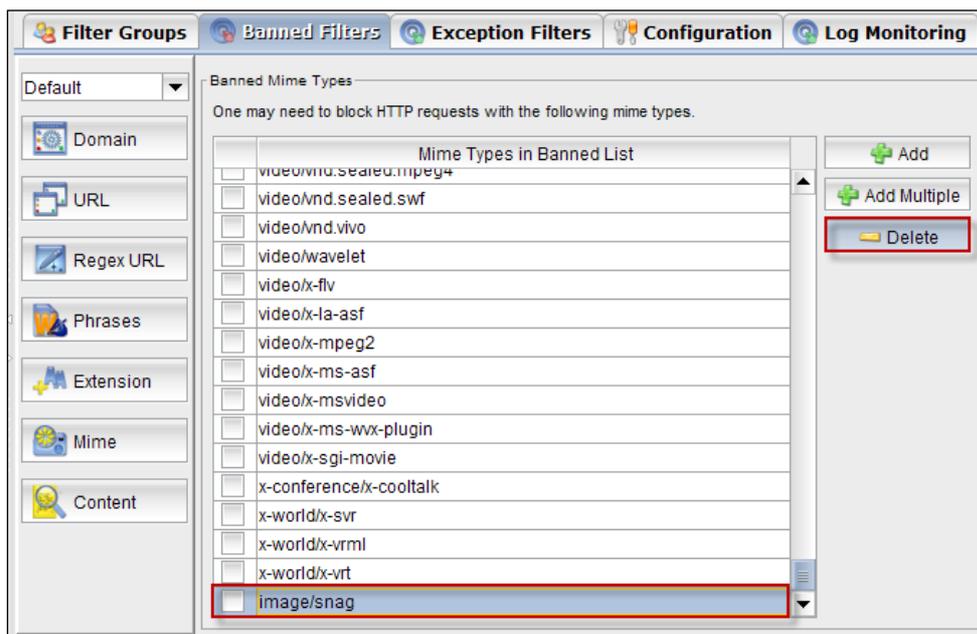


In the below screen, we can notice Mime types added in the list.

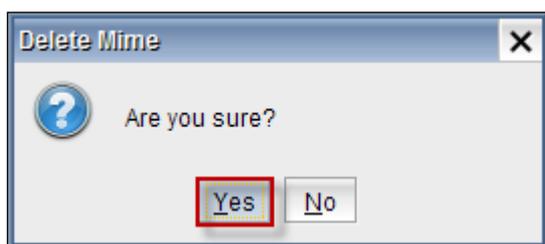


Delete

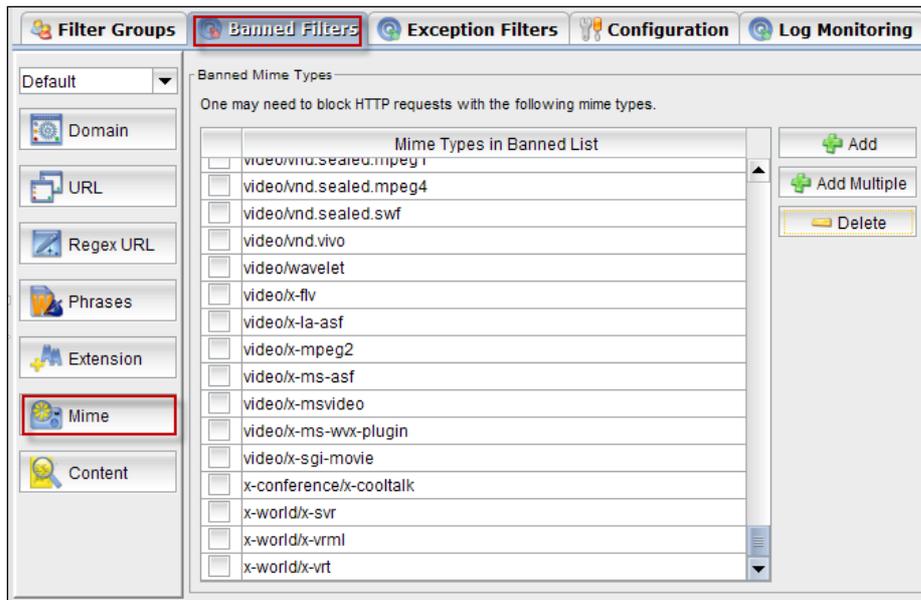
Select the Mime type and click on **Delete** tab.



Delete Mime tab appears, Click on **Yes**.



In the below screen, we can notice Mime type deleted.

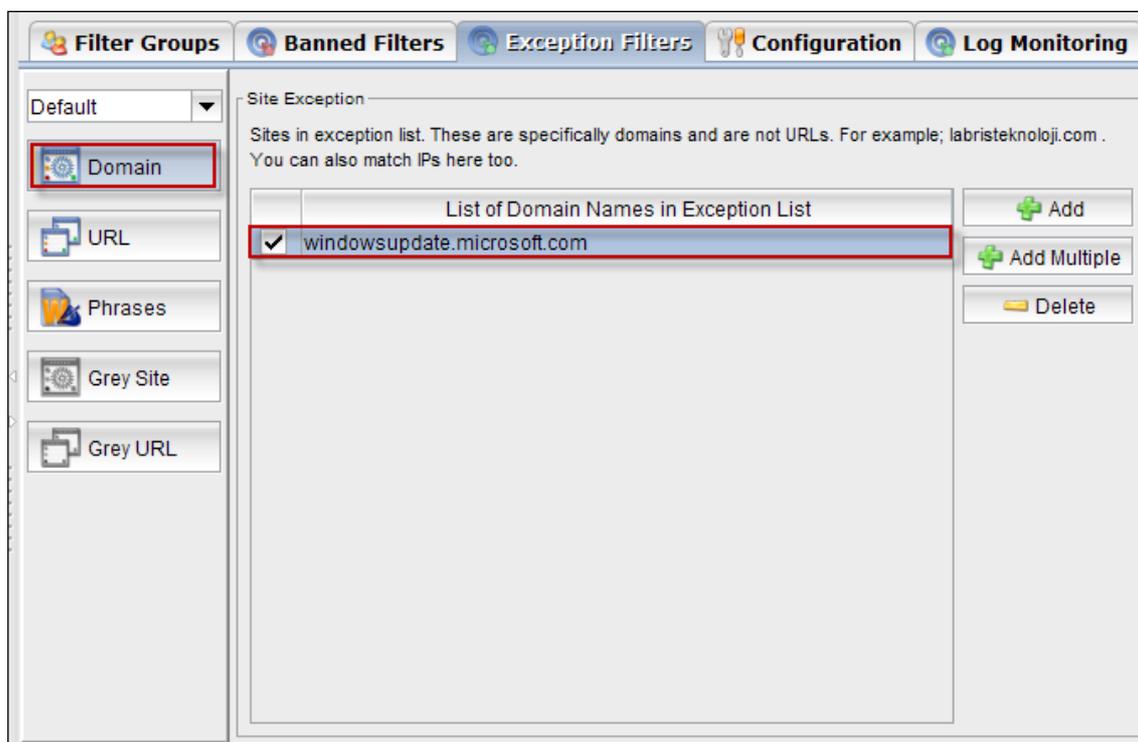


82. Exception Filters



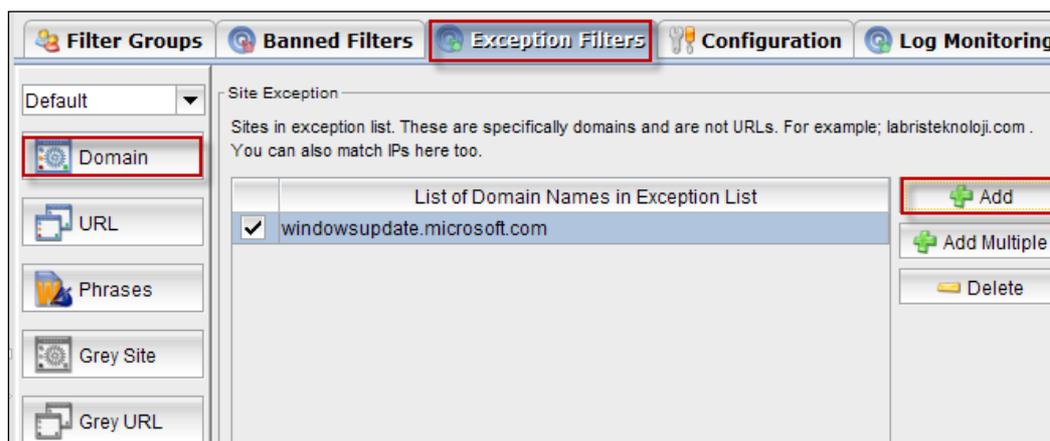
83. Domain

Click on **Domain** tab

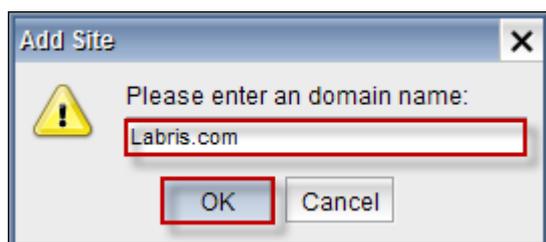


Add

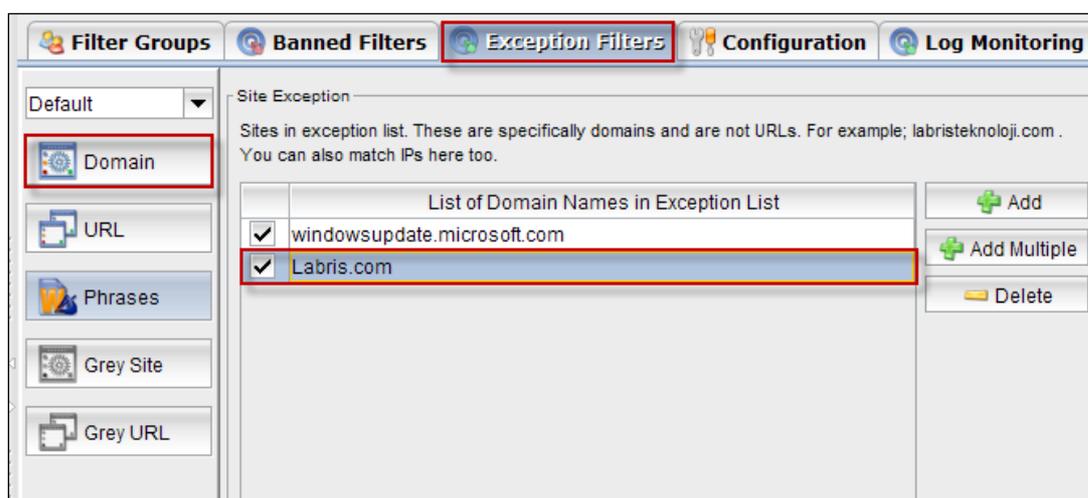
Click on **Add** tab.



Add site tab appears type domain name and click **Ok**.

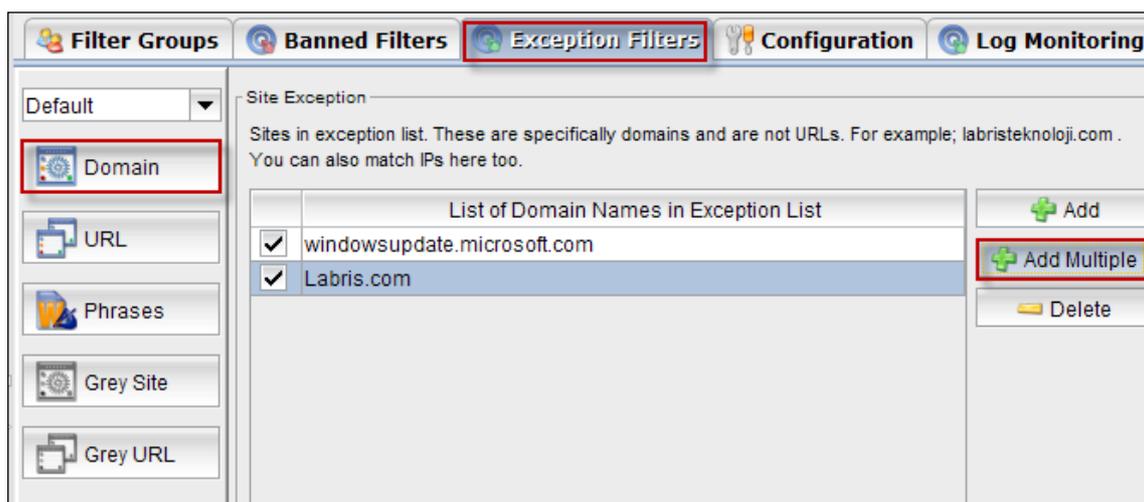


In the below screen, we can notice domain name added.

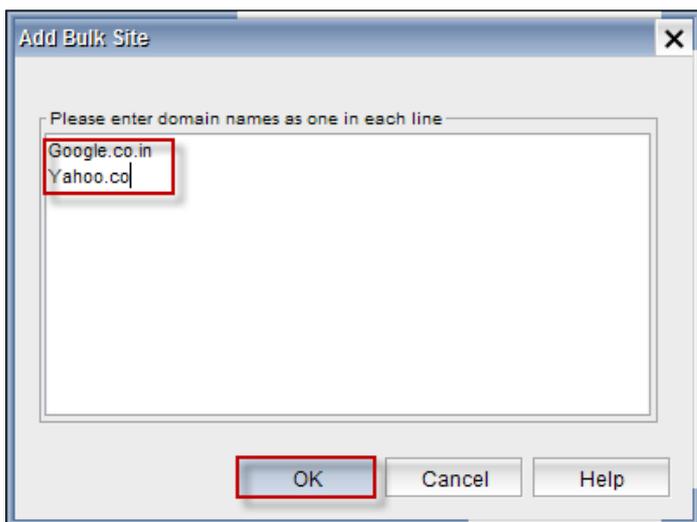


Add Multiple

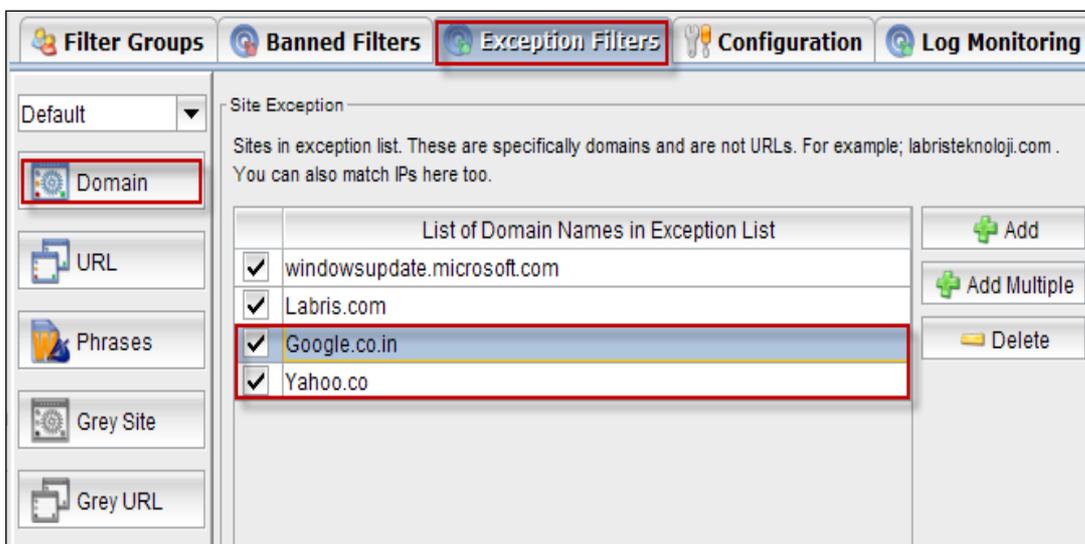
Click on **Add Multiple** tab.



Add Bulk site tab appears, type domain name one in each line. Click **Ok**.

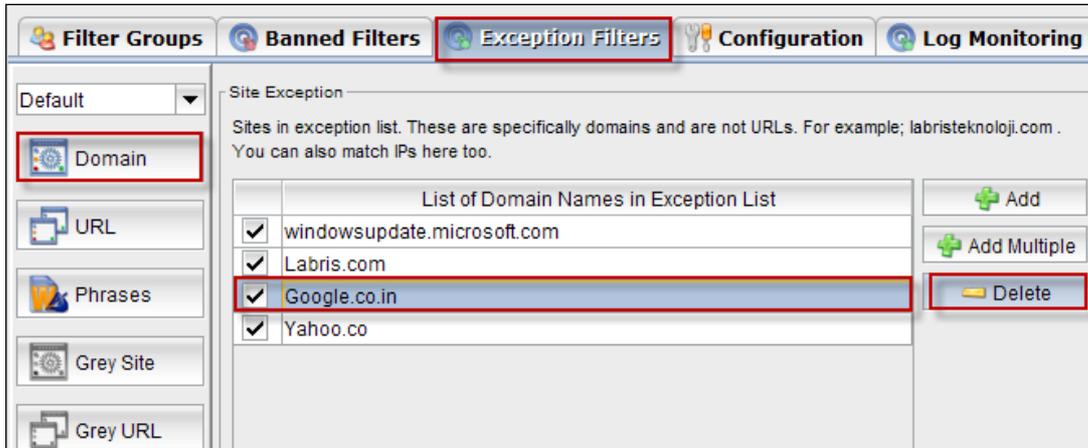


In the below screen, we can notice Multiple domains added.

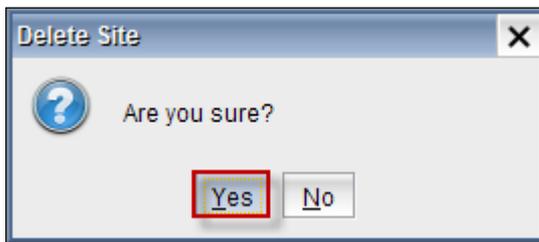


Delete

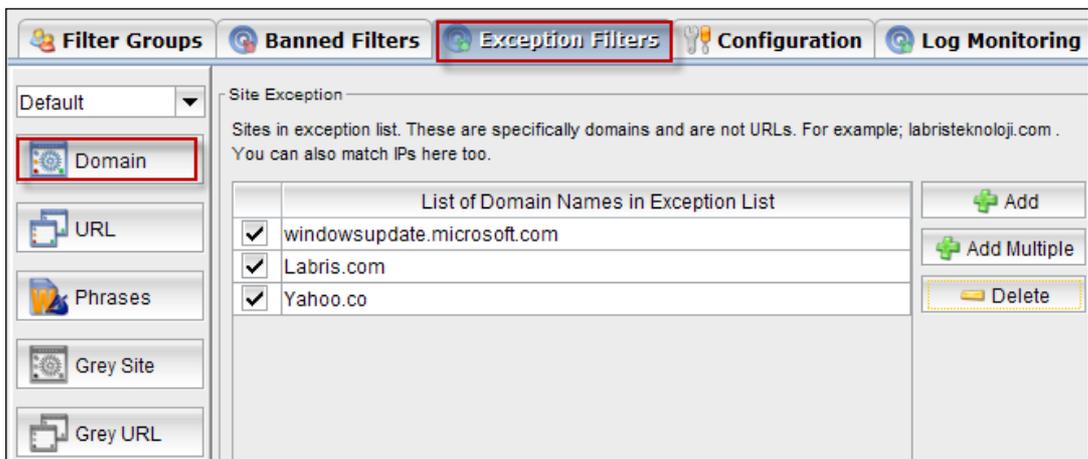
Select Domain and click on **Delete** tab.



Delete Site tab appears, click on **Yes**.

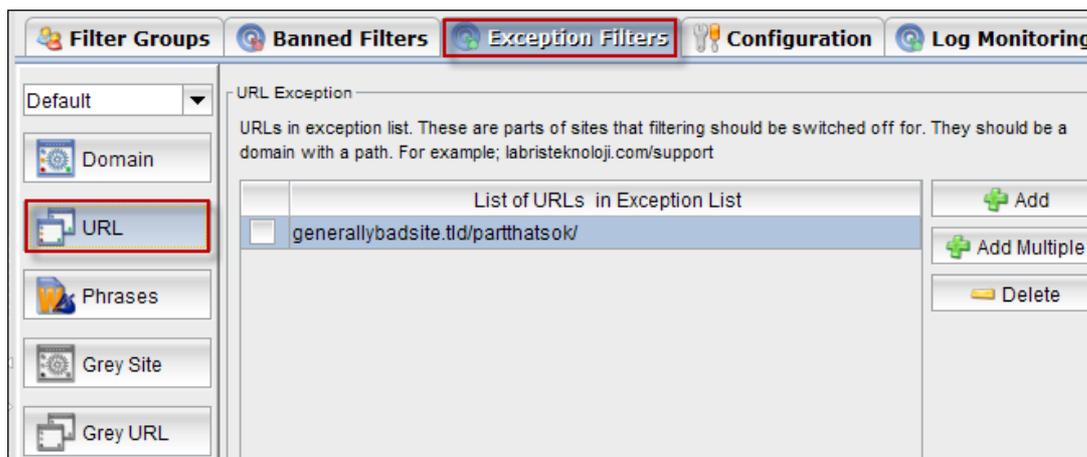


In the below screen, we can notice selected domain deleted.



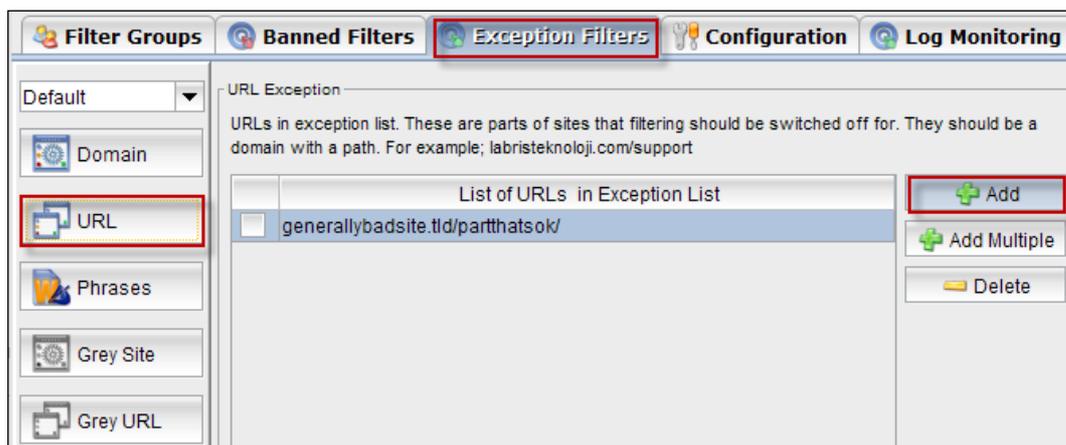
84. URL

Click on **URL** tab

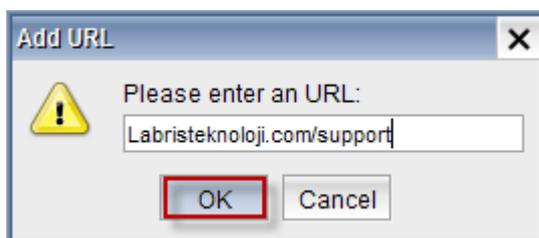


Add

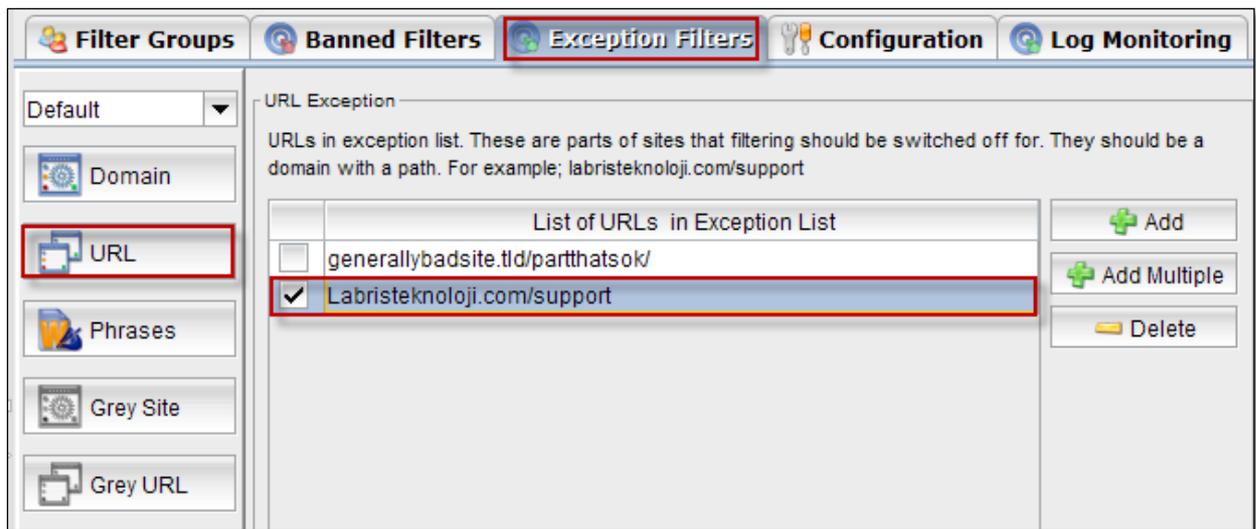
Click on **Add** tab.



Add URL tab appears, type URL and click **Ok**.

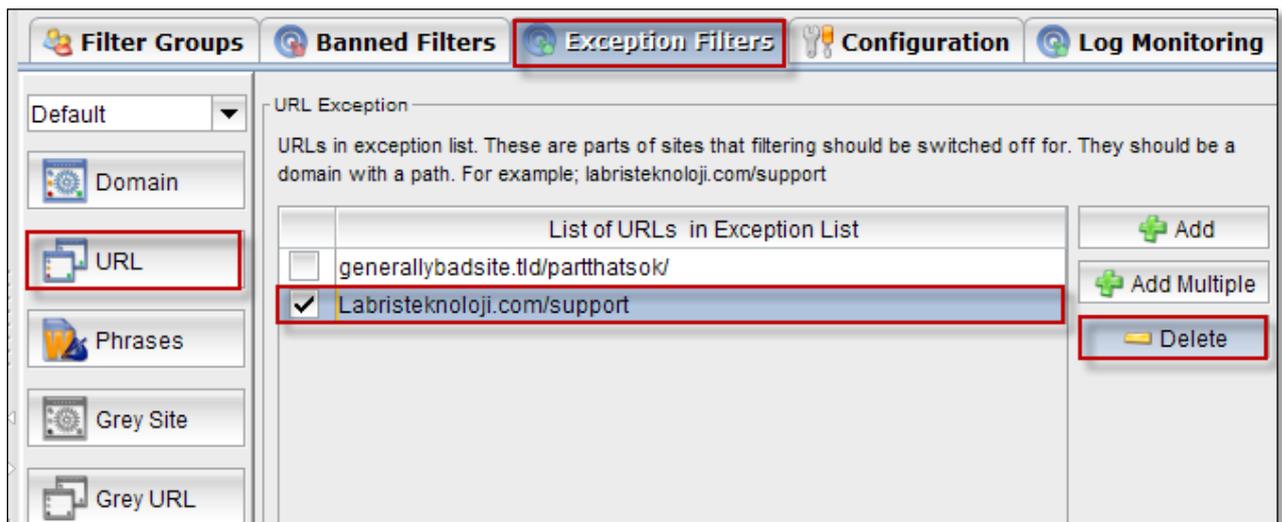


In the below screen, we can notice URL added.



Delete

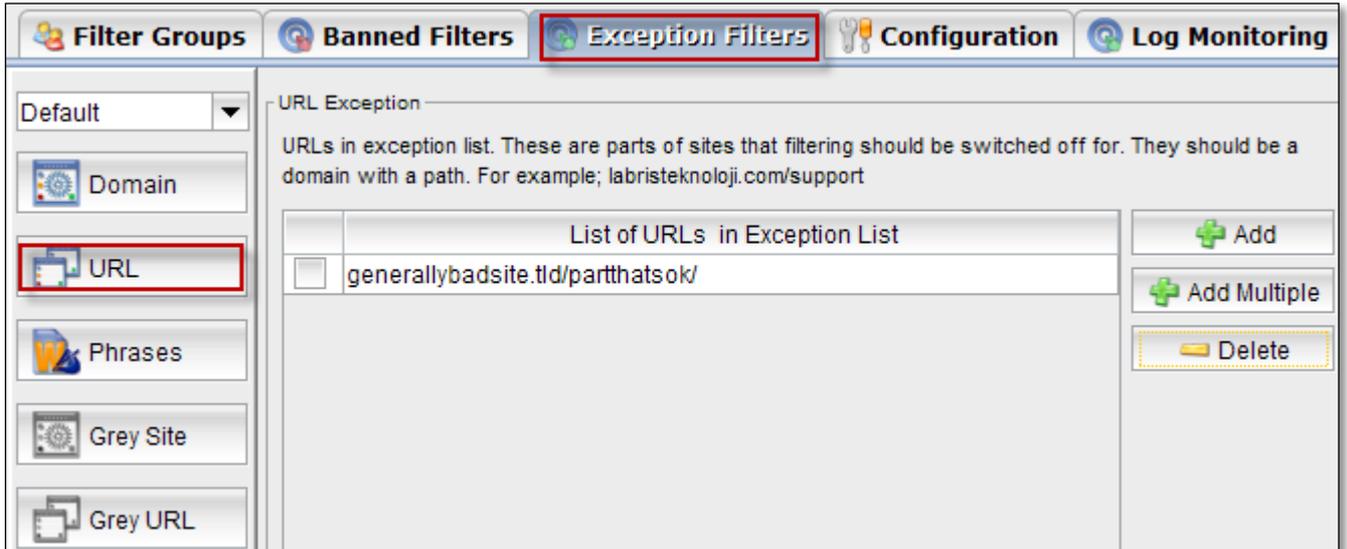
Select URL and click on **Delete** tab.



Delete URL tab appears, click on Yes.

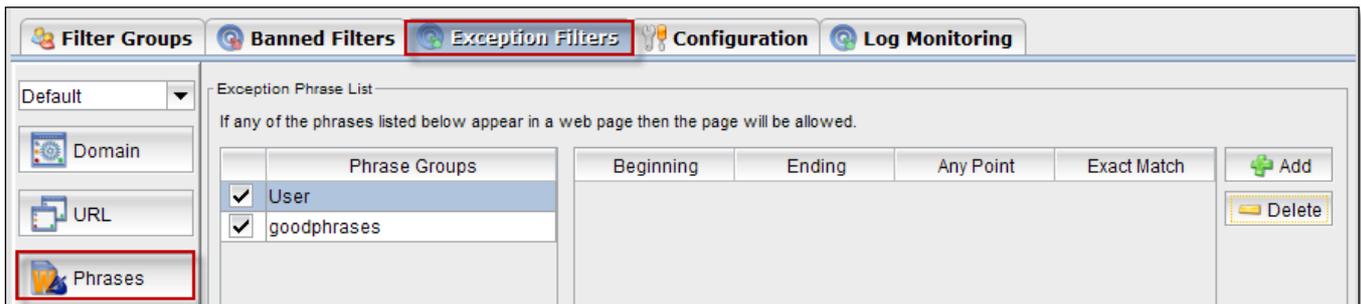


In the below we can notice URL deleted.



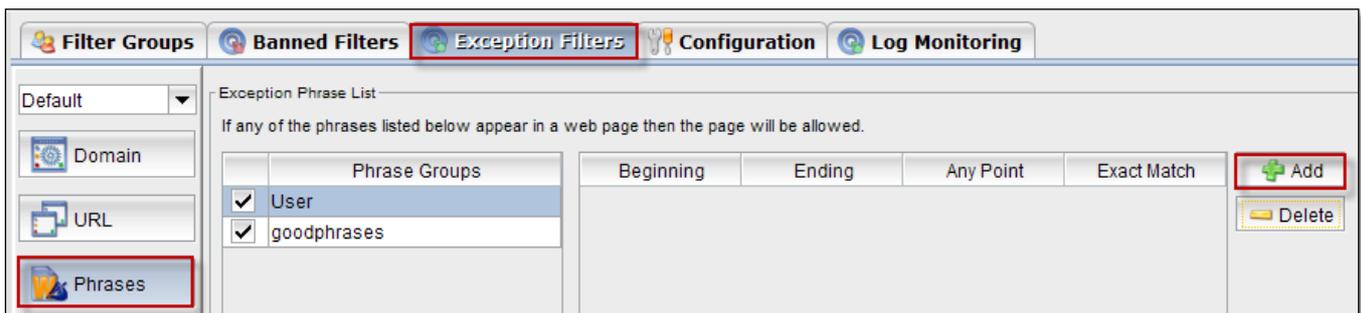
85. Phrases

In the exceptions Filters, Select **Phrases** tab

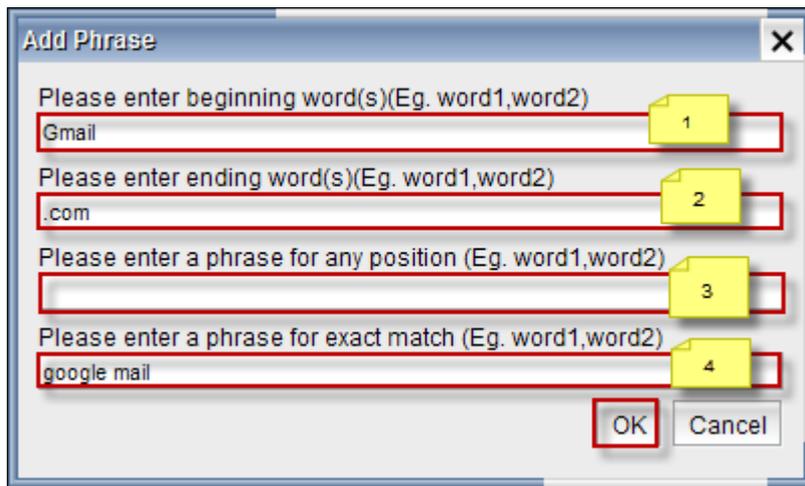


Add

Click on **Add** to add the **Phrases** to the exception phrase list



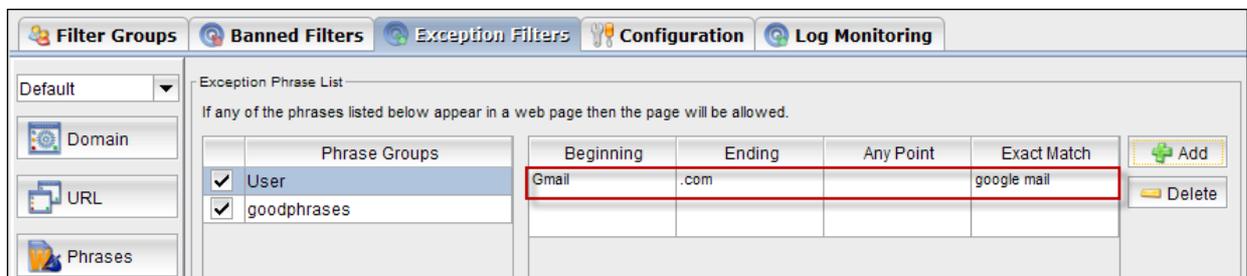
When the **Add phrase** screen appears , give the necessary inputs in the boxes



Options in Add phrase screen are

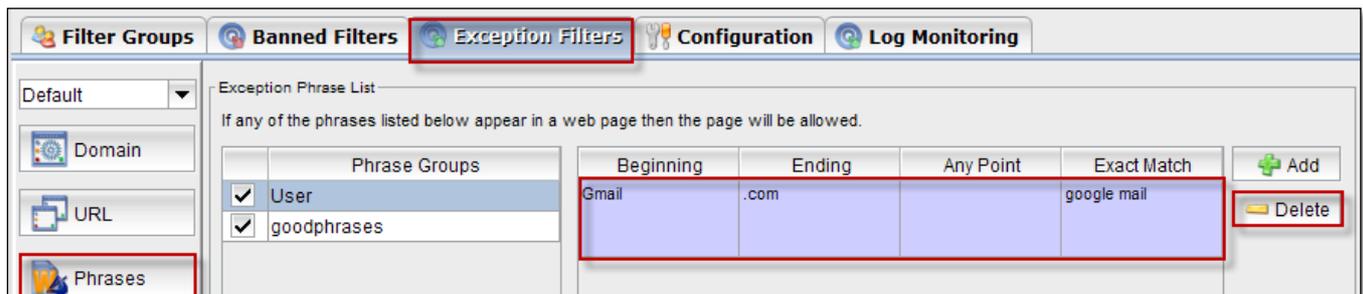
1	Beginning word	In the beginning word box , enter the benning word of the phrase
2	Ending word	In the Ending word box , enter the ending word of the phrase
3	Phrase for any position	In the Phrase for any position box , enter a Phrase for any position
4	Phrase for exact match	In the Phrase for exact match box , enter a Phrase whicg matches exactly

You can notice that a phrase is added to the list

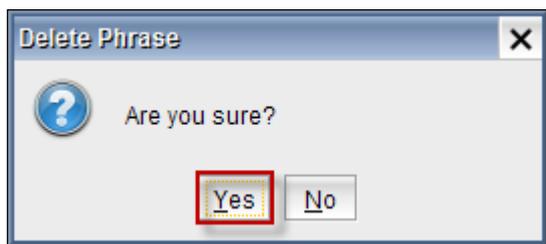


Delete

Select the phrase and click on **Delete** tab to delete the phrase from the list



Below screen appears stating that Are you sure, click on **Yes**



86. Grey Site

Select Grey Site tab.

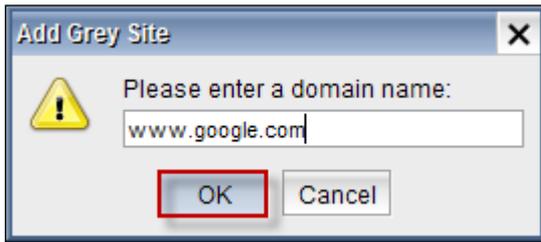


Add

Click on **Add** tab.



Add Grey Site tab appears, type domain name and click **Ok**.



In the below screen we can notice domain added.

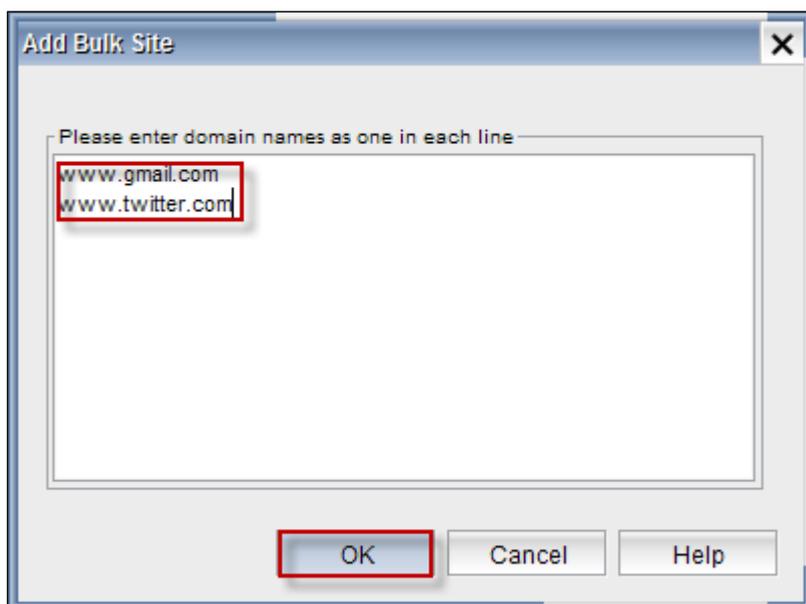


Add Multiple

Click on **Add Multiple** tab.



Add Bulk Site tab appears, type domain name as one in each line and click **Ok**.



In the below screen we can notice multiple domains added.

Filter Groups | Banned Filters | **Exception Filters** | Configuration | Log Monitoring

Default

Domain

URL

Phrases

Grey Site

Grey URL

Grey Site

Domains in grey list. Don't bother with the www. or the http://.

The 'grey' lists override the 'banned' lists. The 'exception' lists override the 'banned' lists also. The difference is that the 'exception' lists completely switch off *all* other filtering for the match. 'grey' lists only stop the URL filtering and allow the normal filtering to work.

An example of grey list use is when in Blanket Block (whitelist) mode and you want to allow some sites but still filter as normal on their content.

Another example of grey list use is when you ban a site but want to allow part of it.

The greyurlist is for partly unblocking PART of a site. The greysitelist is for partly unblocking ALL of a site.

	Domain	
<input checked="" type="checkbox"/>	www.bbc.co.uk	
<input checked="" type="checkbox"/>	www.gmail.com	
<input checked="" type="checkbox"/>	www.google.com	
<input checked="" type="checkbox"/>	www.twitter.com	

Delete

Select the domain and click on **delete** tab.

Filter Groups | Banned Filters | **Exception Filters** | Configuration | Log Monitoring

Default

Domain

URL

Phrases

Grey Site

Grey URL

Grey Site

Domains in grey list. Don't bother with the www. or the http://.

The 'grey' lists override the 'banned' lists. The 'exception' lists override the 'banned' lists also. The difference is that the 'exception' lists completely switch off *all* other filtering for the match. 'grey' lists only stop the URL filtering and allow the normal filtering to work.

An example of grey list use is when in Blanket Block (whitelist) mode and you want to allow some sites but still filter as normal on their content.

Another example of grey list use is when you ban a site but want to allow part of it.

The greyurlist is for partly unblocking PART of a site. The greysitelist is for partly unblocking ALL of a site.

	Domain	
<input checked="" type="checkbox"/>	www.bbc.co.uk	
<input checked="" type="checkbox"/>	www.google.com	

Delete Grey Site tab appears, Click on **Yes**.

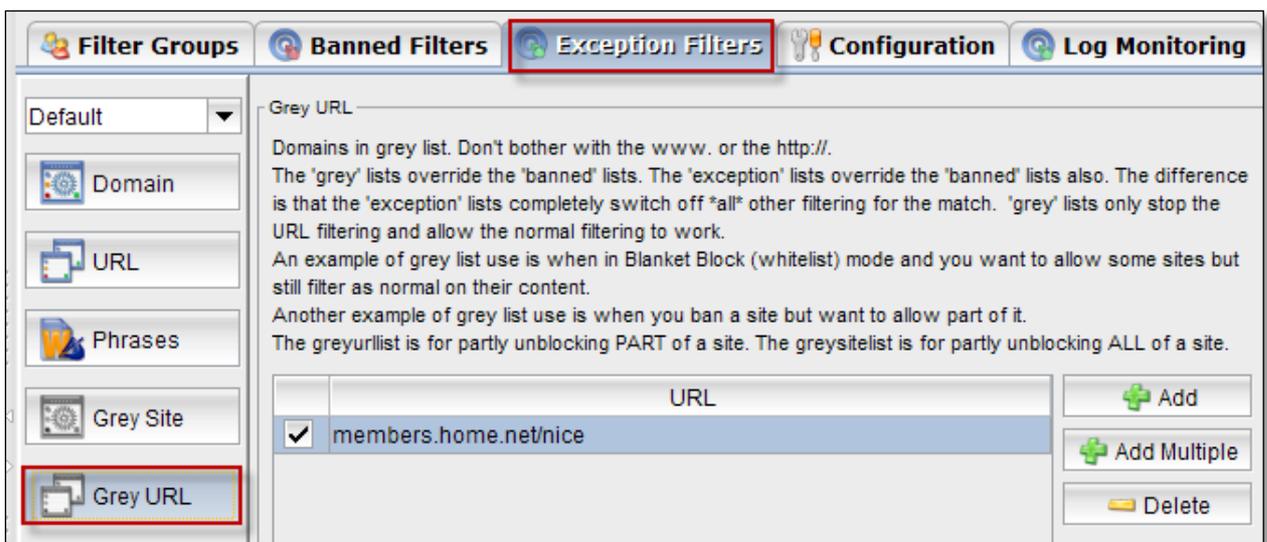


In the below screen we can notice Domain deleted.



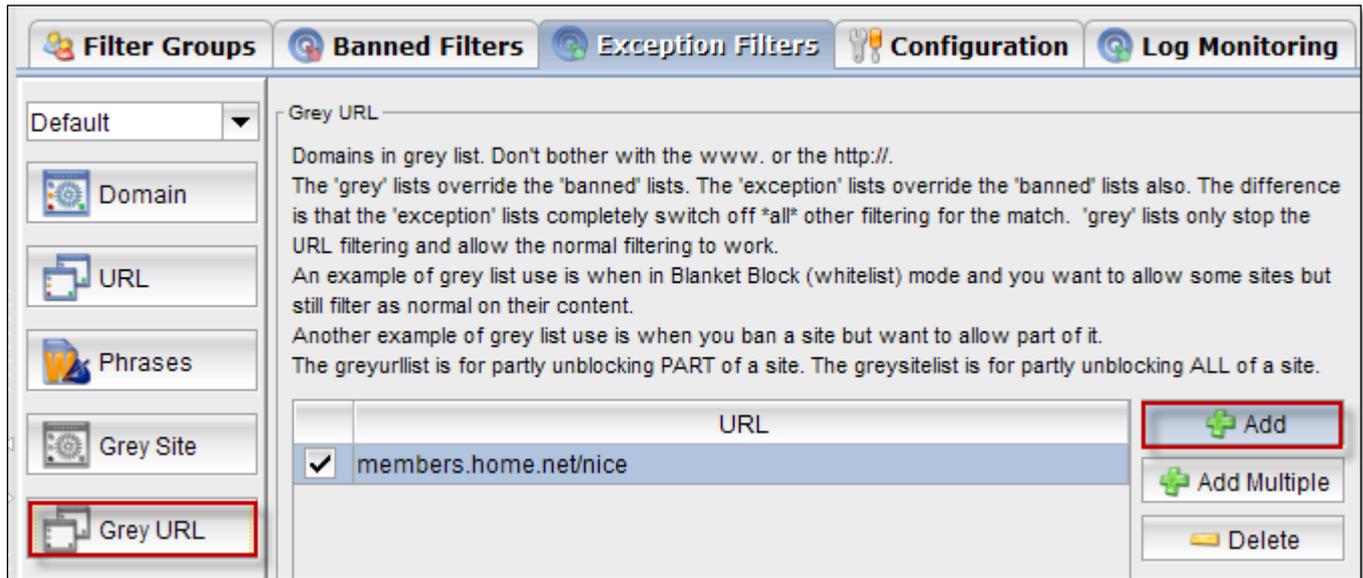
87. Grey URL

Select Grey URL tab.

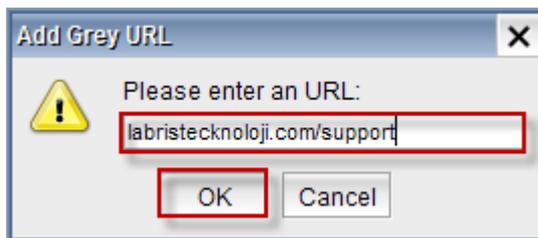


Add

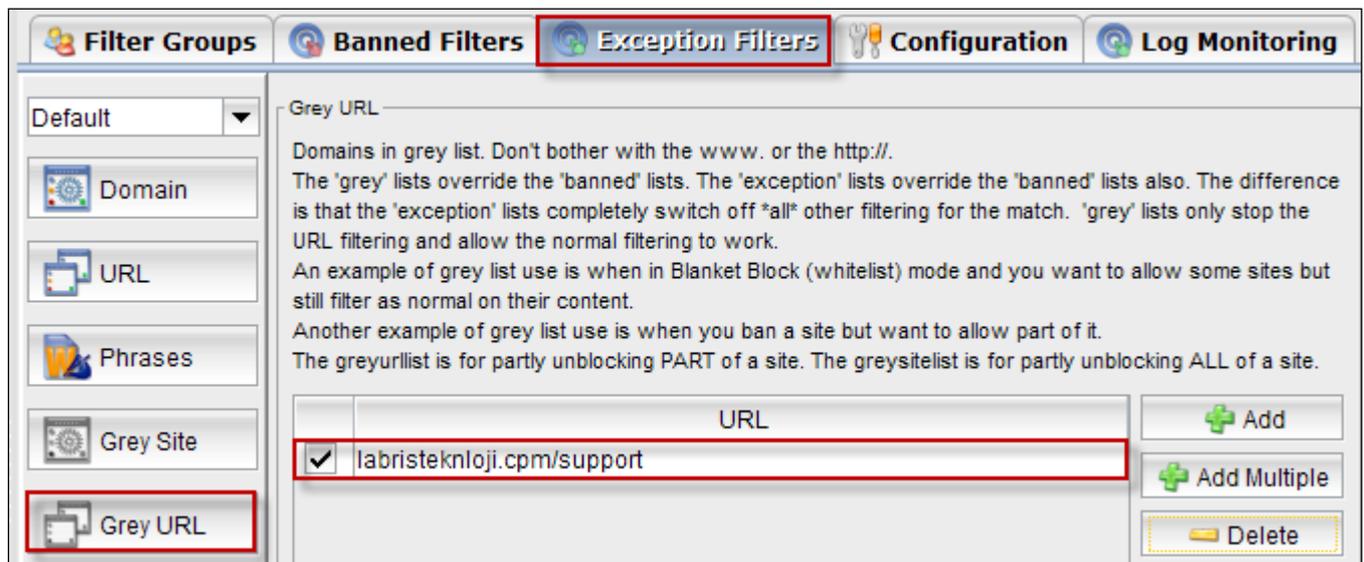
Click on **Add** tab.



Add Grey URL tab appears, type URL and click **Ok**.

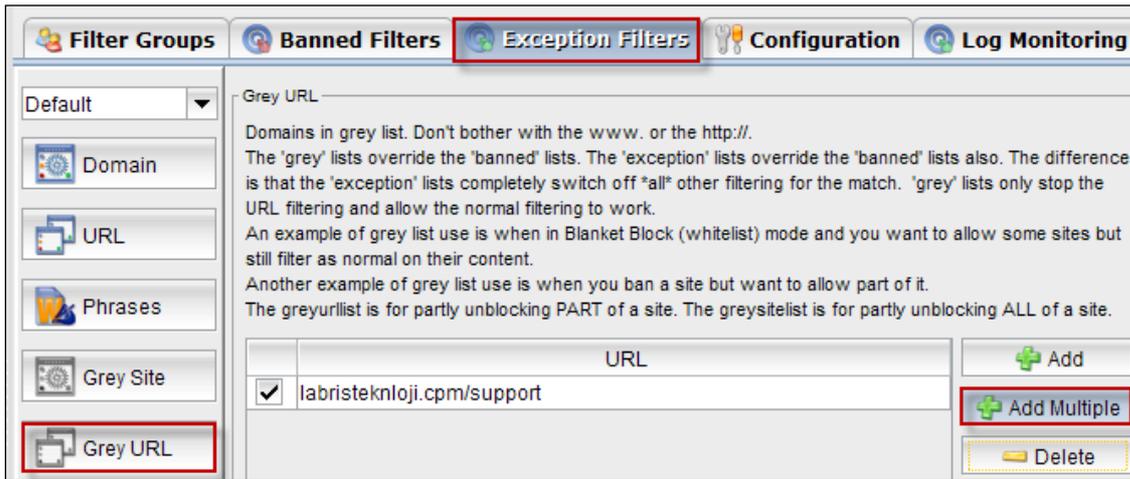


In the below screen we can notice URL added.

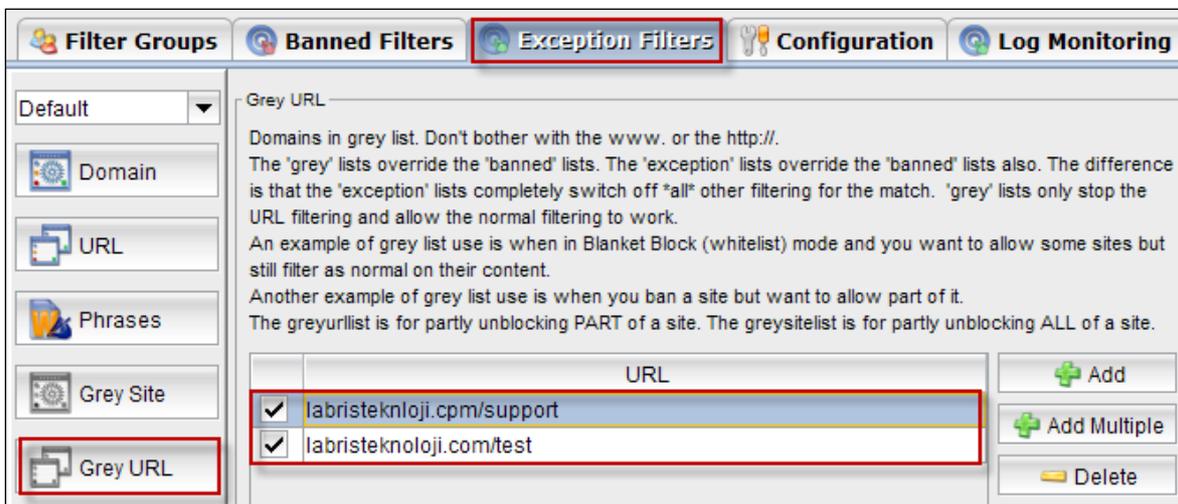


Add More

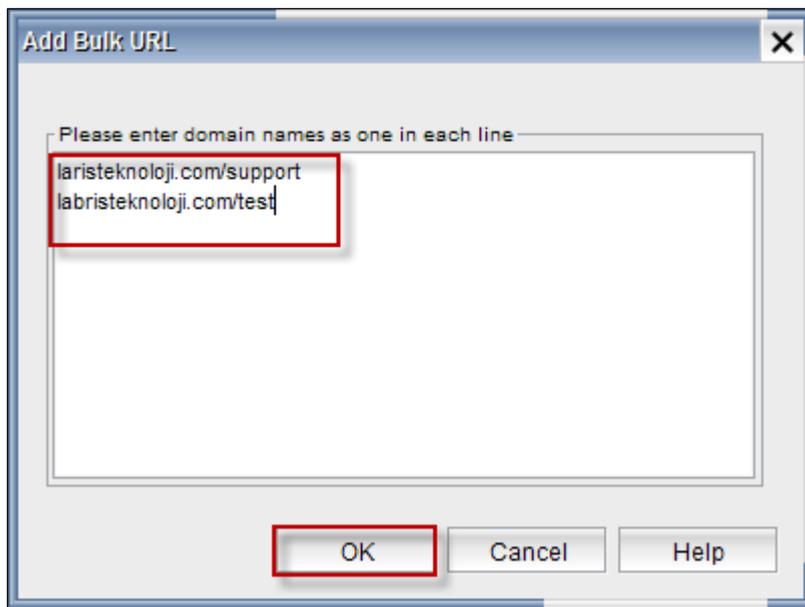
Click on **Add Multiple** tab.



In the below screen we can notice multiple URL added.

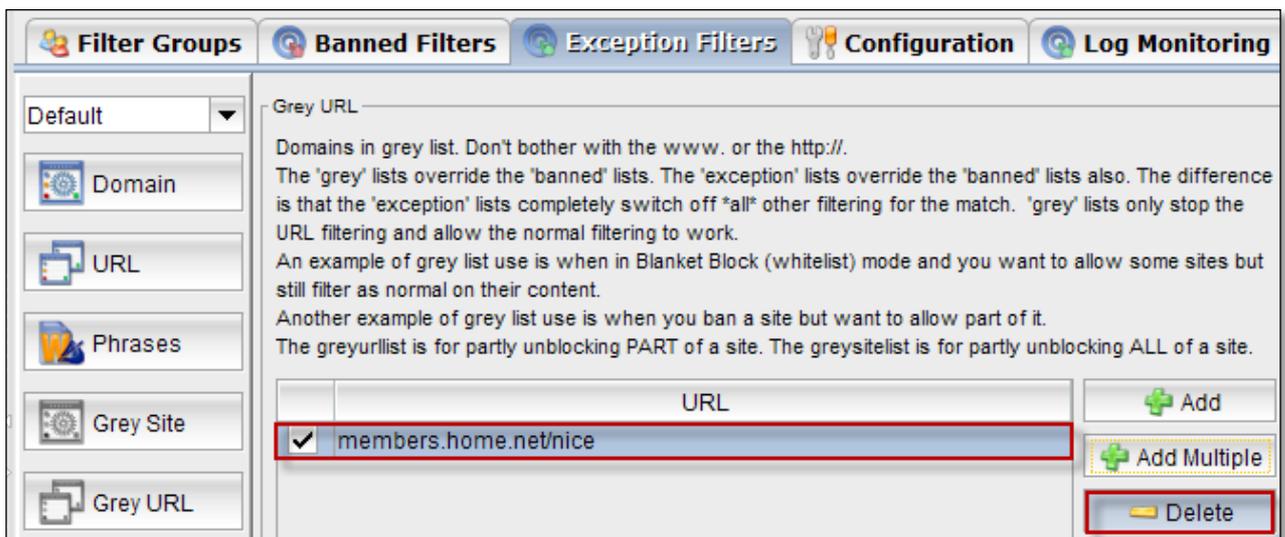


Add Bulk URL tab appears, type domain name one in each line and click **Ok**.



Delete

Select the URL and click on **Delete** tab.



Delete Grey URL tab appears, Click on **Yes**.



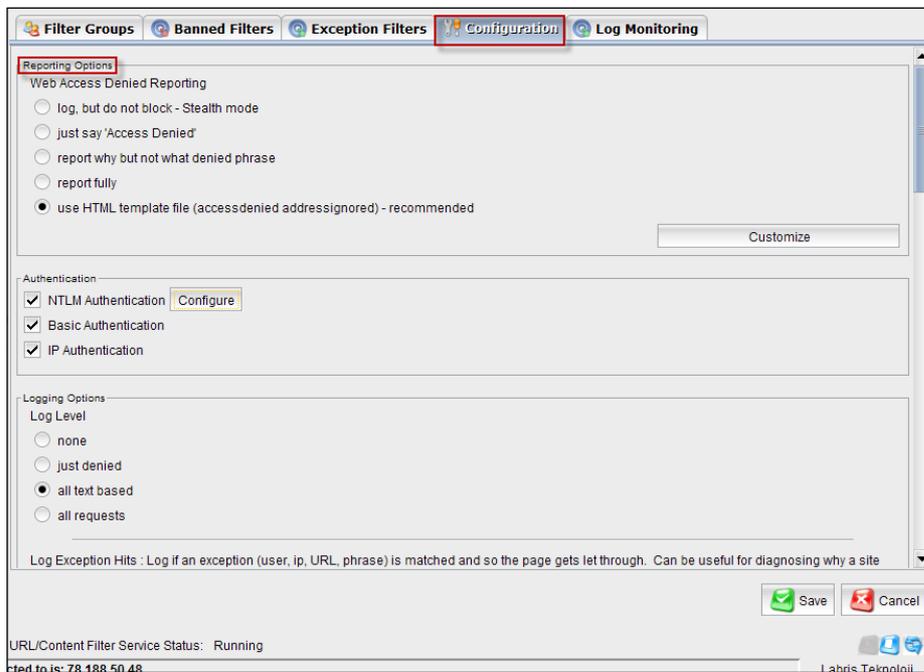
In the below screen we can notice Grey URL deleted.



88. Settings

Reporting Options

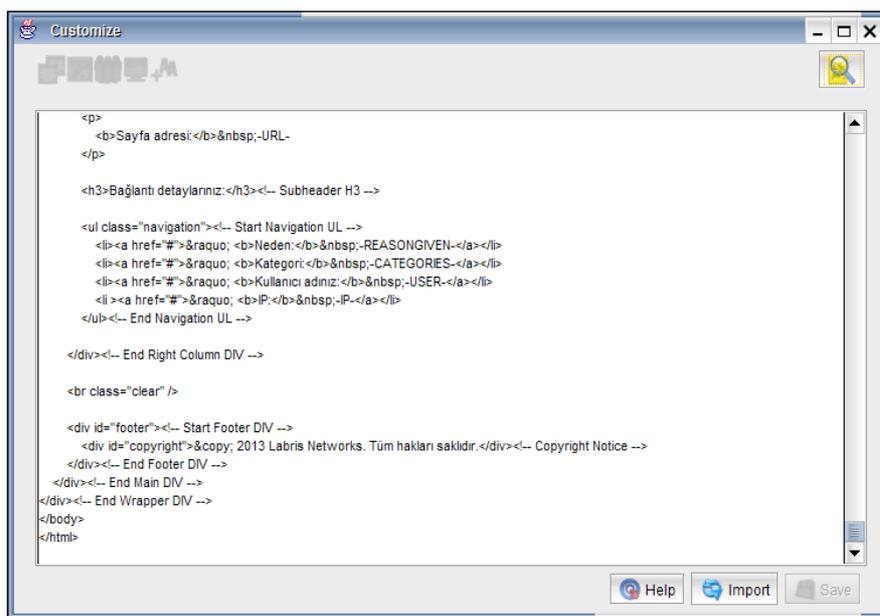
Choose use HTML template file radio button for Web Access Denied Reporting.



In Reporting options click on **Customize** tab.



Customize tab appears displaying HTML coding. Here we can modify the code if required

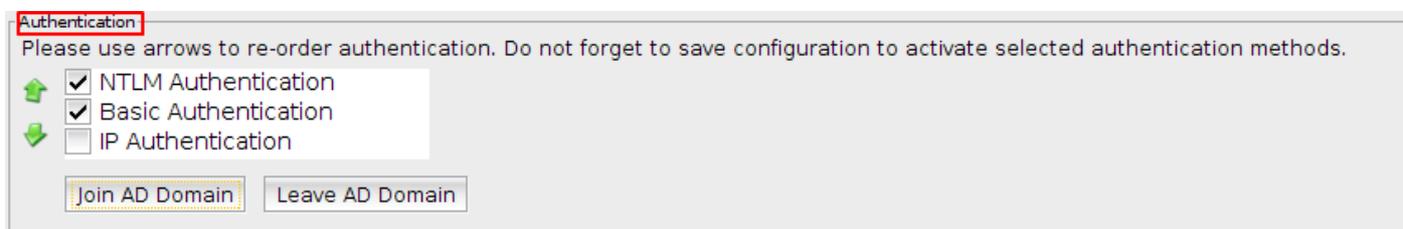


Authentication

Three types of Authentication are available.

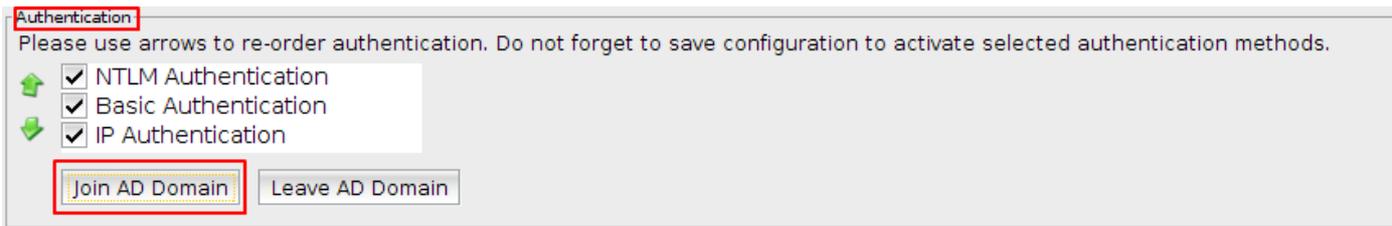
They are NTLM Authentication, Basic Authentication, IP Authentication.

We can enable or disable above mentioned three Authentication types.

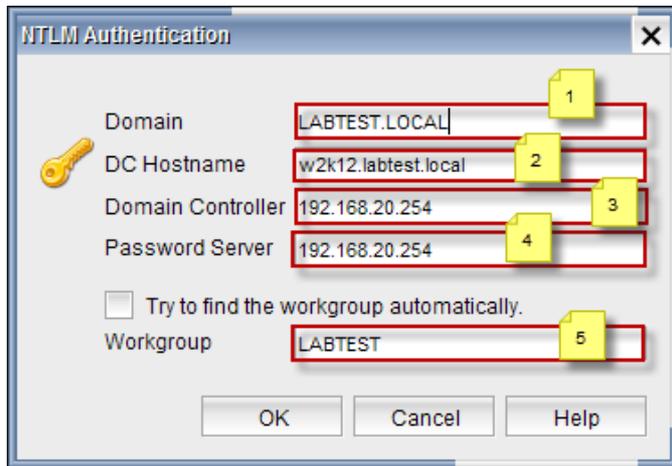


Join Active Directory Domain

Enable NTLM Authentication and click on **Join AD Domain** button.



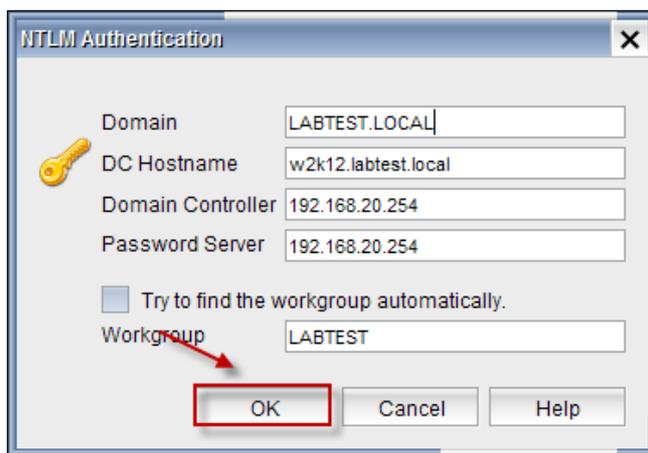
NTLM Authentication tab appears.



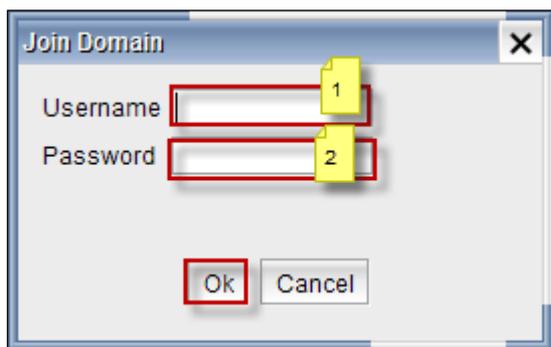
These are the inputs for NTLM Authentication.

1	Domain	Type domain name
2	DC Hostname	Type DC Hostname
3	Domain Controller	Give the Domain Controller IP
4	Password Server	Give the Server Password
5	Workgroup	Type Workgroup or enable Try to find work group automatically

Click **Ok**.



Join Domain tab appears.

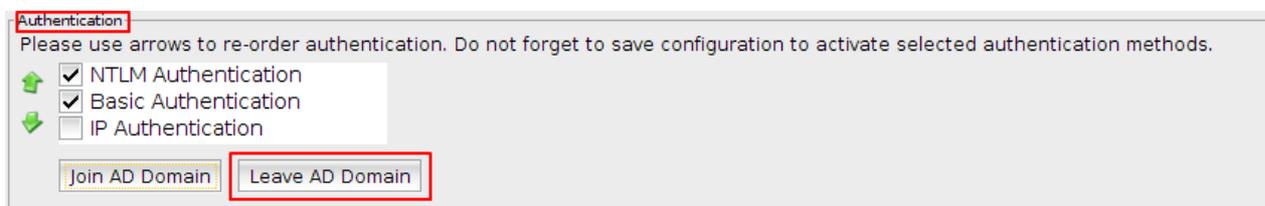


These are the inputs to join domain.

1	Username	Type Username to join Domain
2	Password	Type Password

Leave Active Directory Domain

Click **Leave AD Domain** button.



89. HTTPS Filtering

Introduction and Preliminary Information

What is SSL/TLS and HTTPS?

"SSL" means "Secure Sockets Layer". This was coined by the inventors of the first versions of the protocol, Netscape

"TLS" means "Transport Layer Security". The name was changed to avoid any legal issues with Netscape so that the protocol could be "open and free" (and published as a RFC). It also hints at the idea that the protocol works over any bidirectional stream of bytes, not just Internet-based sockets.

TLS is the new name for SSL. Namely, SSL protocol got to version 3.0; TLS 1.0 is "SSL 3.1". TLS versions currently defined include TLS 1.1 and 1.2. So it's generally called SSL/TLS.

HTTPS is a protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data.

Note: Explanation and definitions are borrowed from StackExchange and Wikipedia.

Certificate Authorities (CA), Chain of Trust and Certificate Chain

A certificate authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made by the private key that corresponds to the certified public key. In this model of trust relationships, a CA is a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate.

Digital certificates are verified using a chain of trust. The trust anchor for the digital certificate is the root certificate authority.

A certificate chain is a list of certificates (usually starting with an end-entity certificate) followed by one or more CA certificates (usually the last one being a self-signed certificate), with the following properties:

- 1 - The Issuer of each certificate (except the last one) matches the Subject of the next certificate in the list.
- 2 - Each certificate (except the last one) is supposed to be signed by the secret key corresponding to the next certificate in the chain (i.e. the signature of one certificate can be verified using the public key contained in the following certificate).
- 3 - The last certificate in the list is a trust anchor: a certificate that you trust because it was delivered to you by some trustworthy procedure.

Note: Explanations and definitions are borrowed from relevant Wikipedia pages.

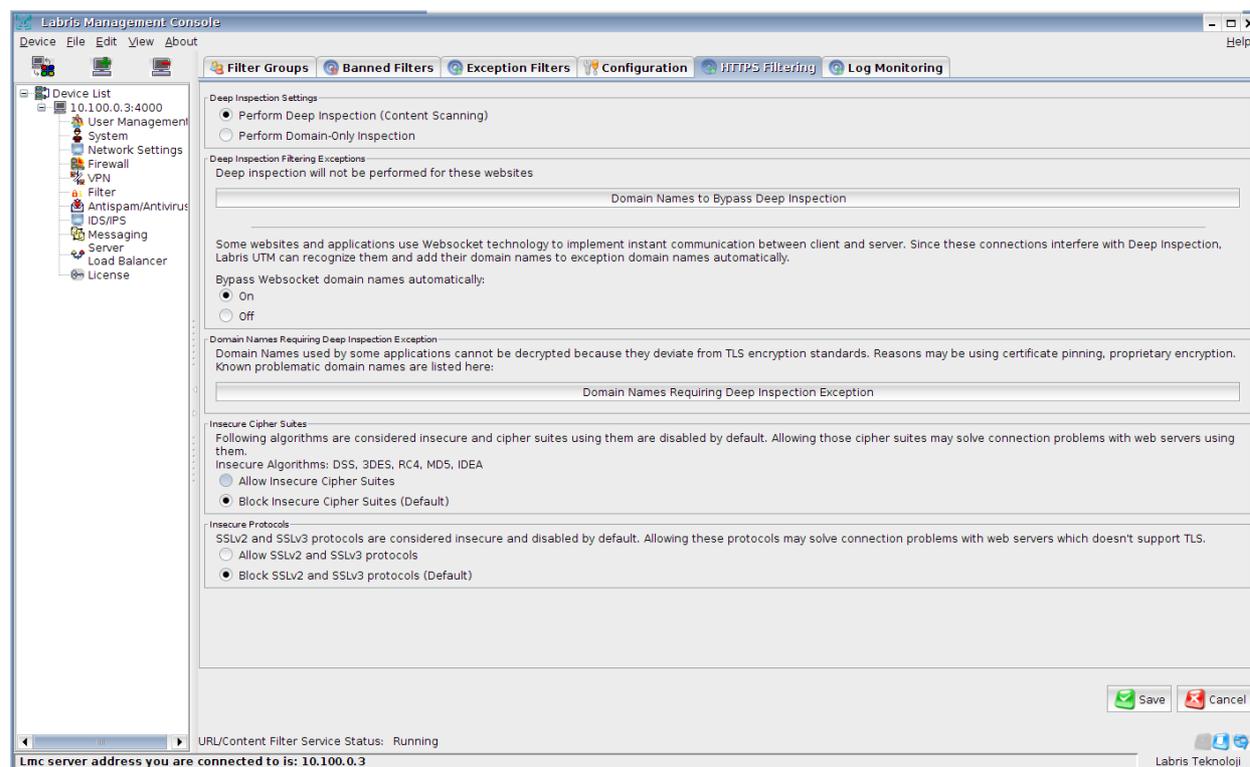
Creation of Labris UTM CA

Since HTTPS connection and chain of trust is unbreakable by definition, explicit permission needs to be granted by clients in order to inspect the content of HTTPS connections. This happens in the form of Root CA import in client machines.

Importing the Root CA of Labris UTM means that client trusts the UTM and promises to trust certificates issued by Labris UTM. When a client tries to establish a new HTTPS connection with a web server, Labris UTM intercepts the connection and redirects it to labris-webcache daemon. Labris-webcache analyses the connection request, extracts the destination domain and decides if this connection should be inspected or not. If the connection requires inspection, labris-webcache establishes a new HTTPS connection with the webserver, verifies its certificate chain and issues a new certificate for domain signed by Labris UTM CA. This whole process allows labris-webcache to maintain two HTTPS connections, first one between client and UTM, second one between UTM and webserver. This allows decryption and re-encryption of HTTPS connection on-the-fly and inspection of its content. This is also called Man-in-the-Middle (MitM) and makes labris-webcache man in the middle. Doing this on a public network (like ISP provided) and without explicit permission from clients may be illegal.

Configuration

This tab allows tuning the configuration options of HTTPS Filtering.



HTTPS Filtering Settings

Deep Inspection (Default)

Perform man-in-the-middle inspection for HTTPS connection. Requires Labris UTM Root CA import in client machines.

Domain-only Inspection

Try to extract destination domains and apply domain-based rules if it's possible. This option doesn't require certificate import. On the other hand, labris-webcache can't perform deep analysis of packets and in some situations where domain name is not present during HTTPS connection, domain-based rules may not work.

HTTPS Filtering Exceptions

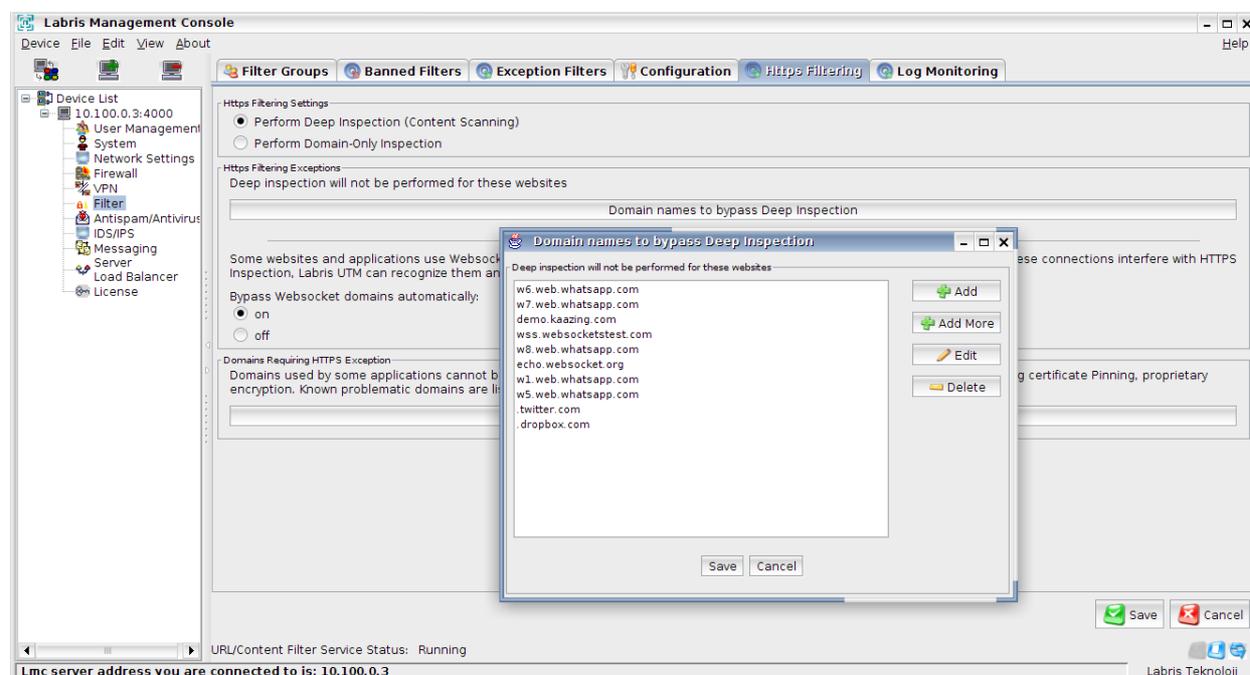
Domain Names to Bypass Deep Inspection

Some applications and domains used by them can't be inspected for various reasons including but not limited to:

- Key pinning
- Deviation from SSL/TLS protocol
- Proprietary algorithms or cipher suites
- Using TCP port 443 for Non-HTTPS protocols.

Some of the problems above may be solved by adding relevant domains to exception. If adding an exception doesn't solve the problem, not redirecting connections to labris-webcache for known destination IP addresses should solve the problem.

Certain domains (or all subdomains of a domain) can be added to this list if it causes problem or it's not appropriate to decrypt and inspect its content on-the-fly.



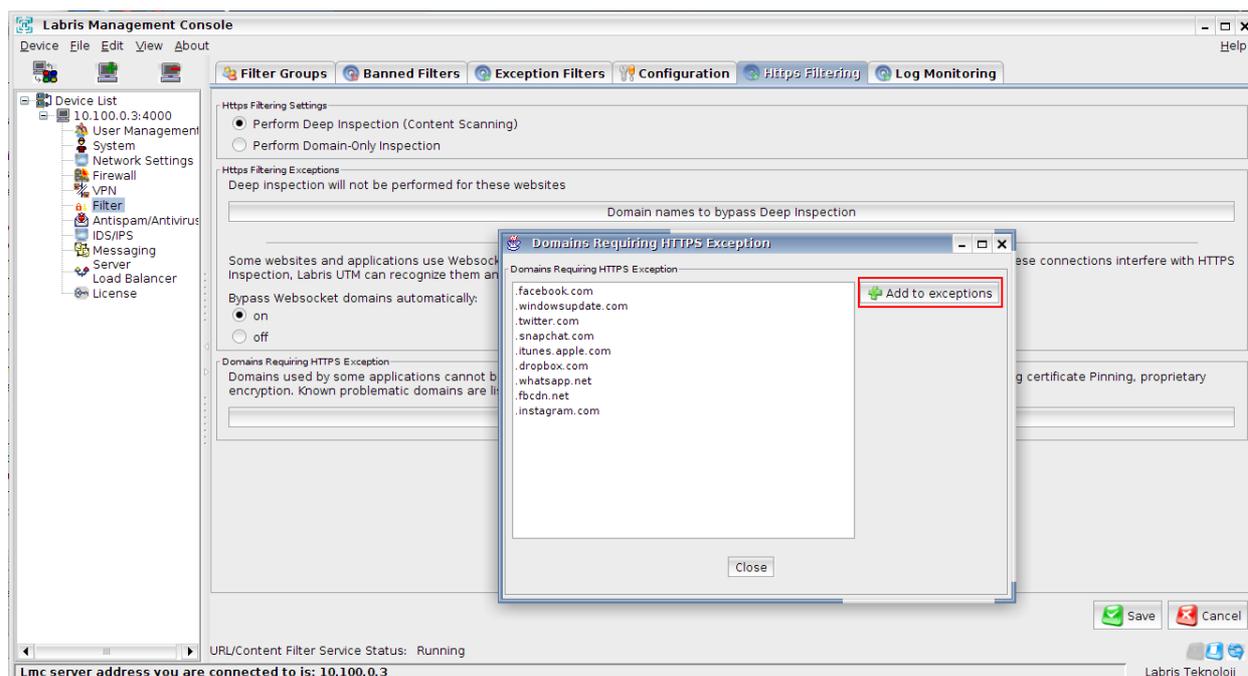
Bypass Websocket Domain Names Automatically

Some websites and applications use Websocket connection over HTTPS connections. Websocket connections start with HTTP handshake and uses 101 Upgrade response to upgrade the connection to Websocket protocol. Since they are not actually HTTP over TLS they cannot be effectively inspected and passed. So domains using Websocket needs exception to not break them. Labris UTM may inspection HTTP headers and recognize Websocket headers on-the-fly. This allows auto-adding Websocket domains to exception list. User may manage and examine these domains later in the "Domain Names to Bypass Deep Inspection" list.

Warning: Allowing Websocket domains may allow bypassing filter rules. Make it 'off' if you think your clients may act maliciously.

Domain Names Requiring Deep Inspection Exception

Labris provides a list of known domains which require exception in order to make related applications to work. You can examine the list and add them directly to "Domain Names to Bypass Deep Inspection" list.



Insecure Cipher Suites

Some algorithms are considered insecure and cipher suites using them are disabled by default. Allowing them solve connection problems with web servers using these cipher suites.

Insecure algorithms: DSS, 3DES, RC4, MD5, IDEA

Cipher suites using them:

TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_DSS_WITH_SEED_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_ECDSA_WITH_RC4_128_SHA
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_IDEA_CBC_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

Insecure Protocols

SSL version 2 and version 3 are considered insecure and disabled by default. Allowing them may solve connection problems with web servers which doesn't support TLS.

Certificate Import (Desktop)

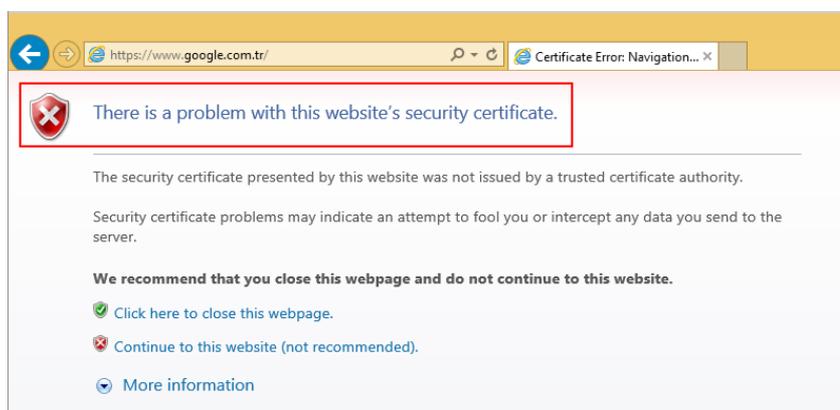
Windows

System-wide Import (Internet Explorer, Chrome)

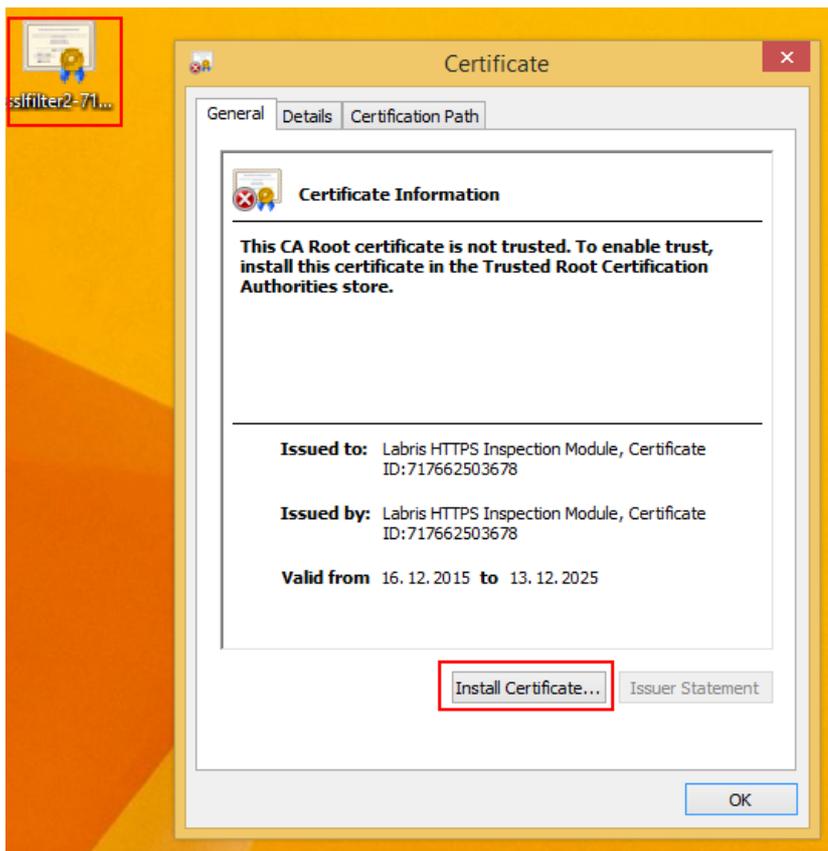
Importing certificate to system certificate store of windows allows Internet Explorer, Chrome and other applications trusting system store to work without certificate warning.

If root certificate is not imported to the system, browser shows a warning about certificate security.

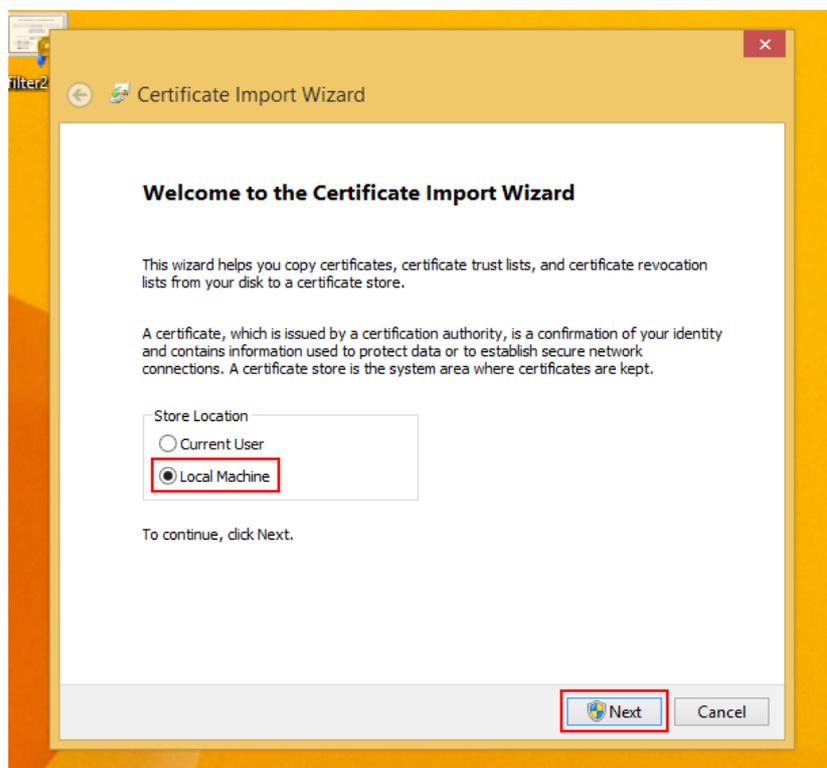
Internet Explorer shows certificate warning before import



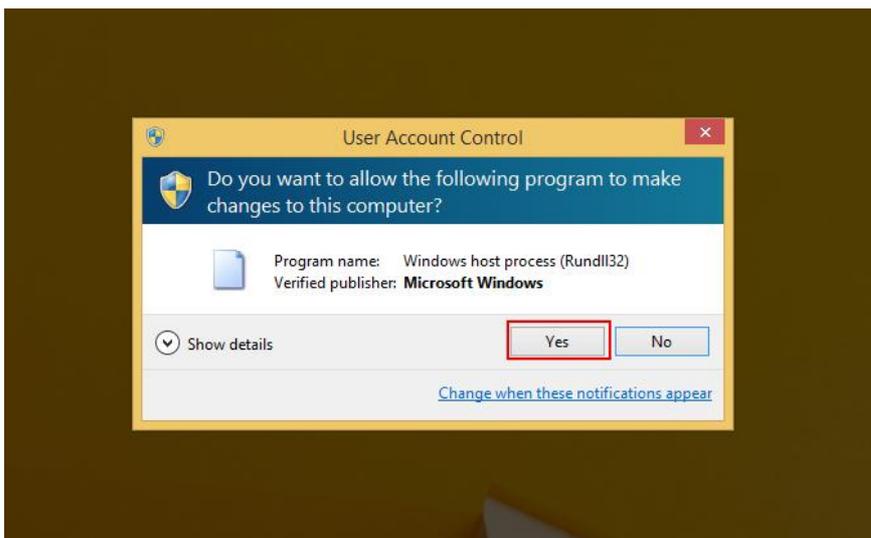
Double-clicking on the root certificate opens certificate details windows. Clicking on Install Certificate option opens a new dialog.



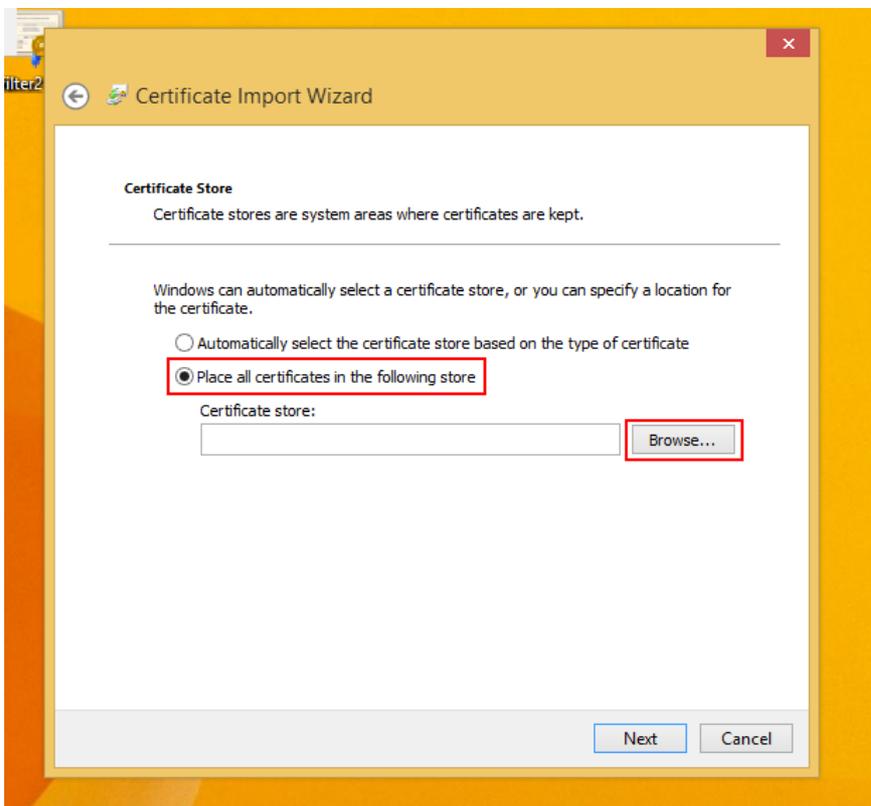
Please choose Local Machine and click Next.



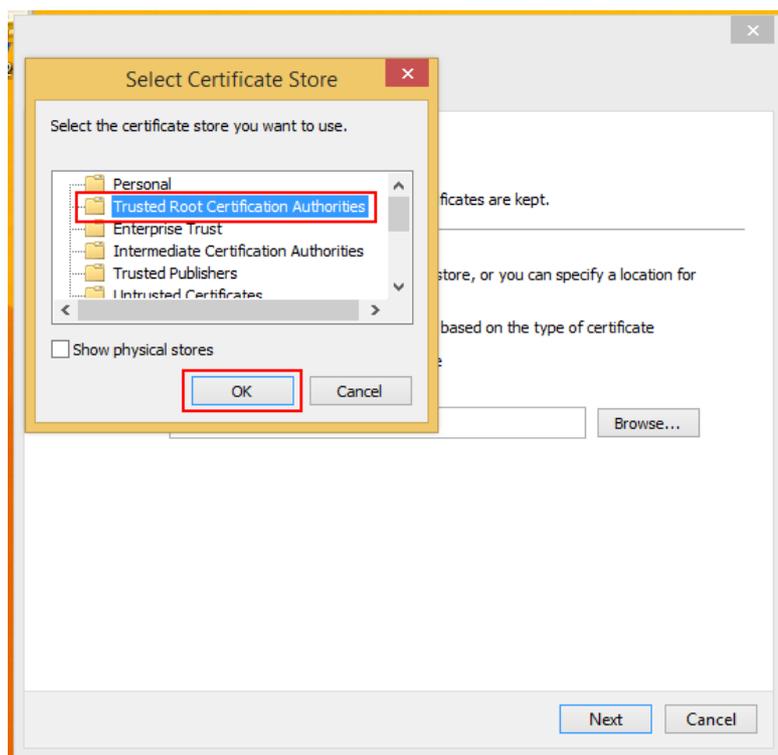
Click Yes.



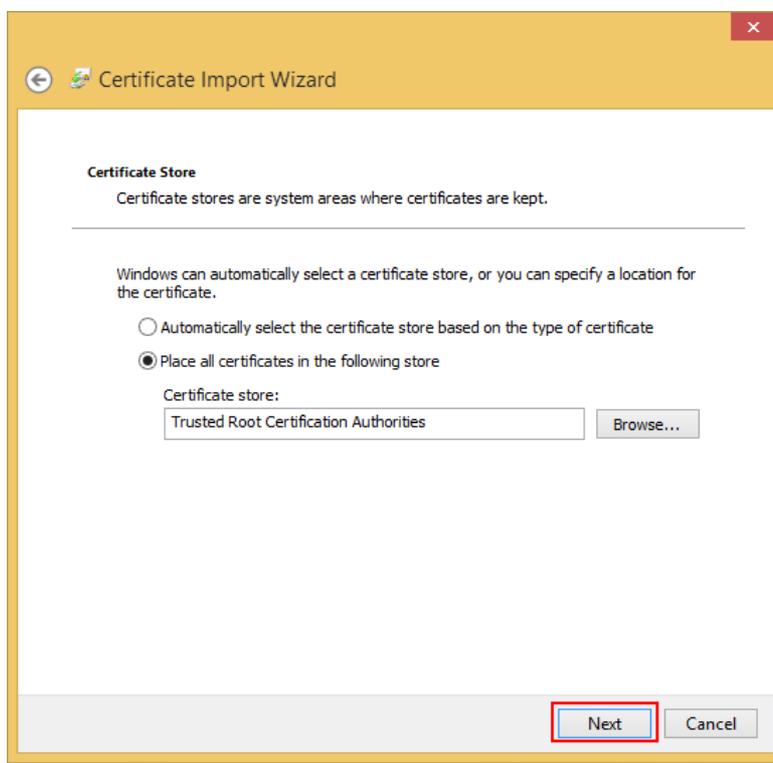
Choose "Place all certificates in the following store" and click Browse.



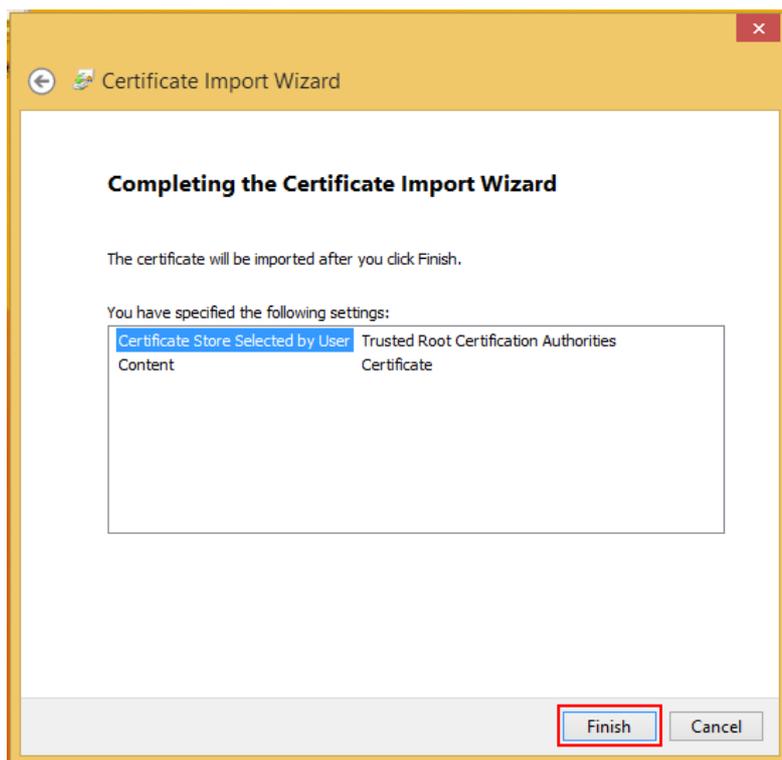
Choose Trusted Root Certification Authorities as store.



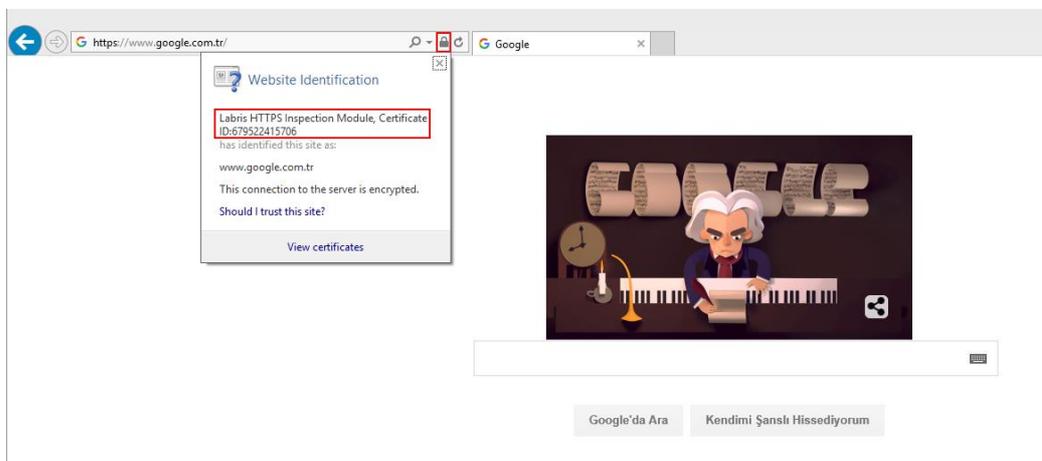
Click Next.



Click Finish.

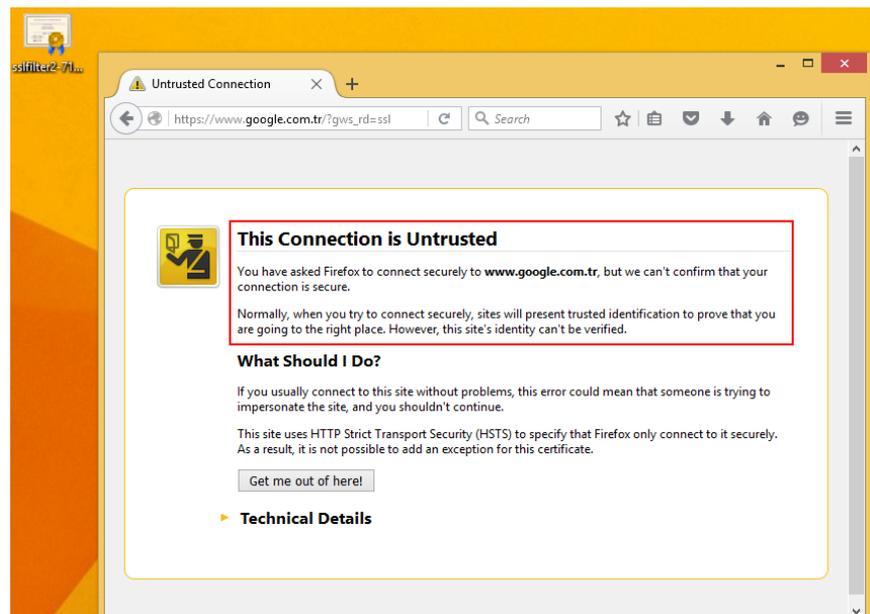


Internet Explorer shows no warning after certificate import.

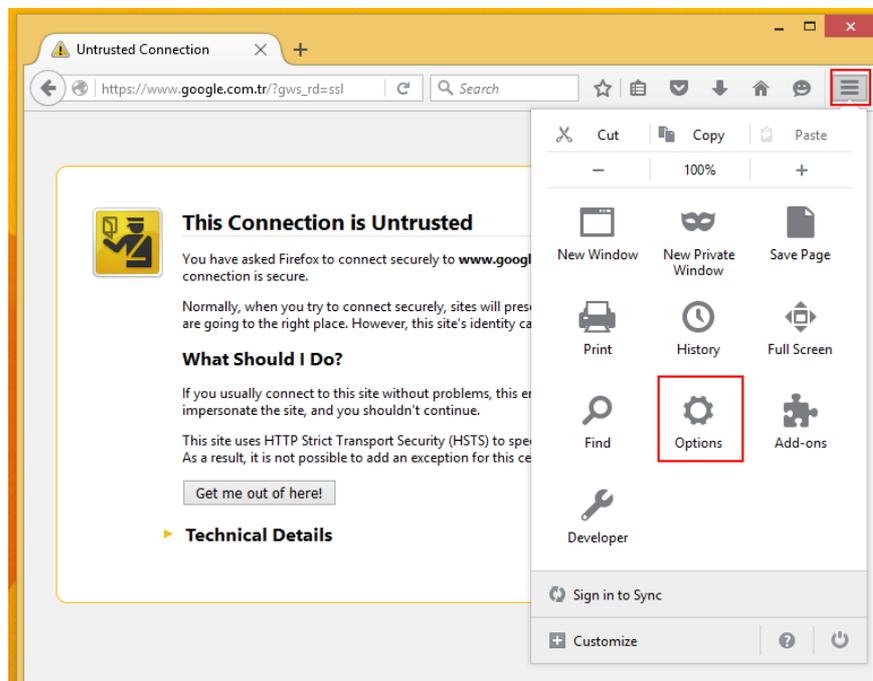


Firefox

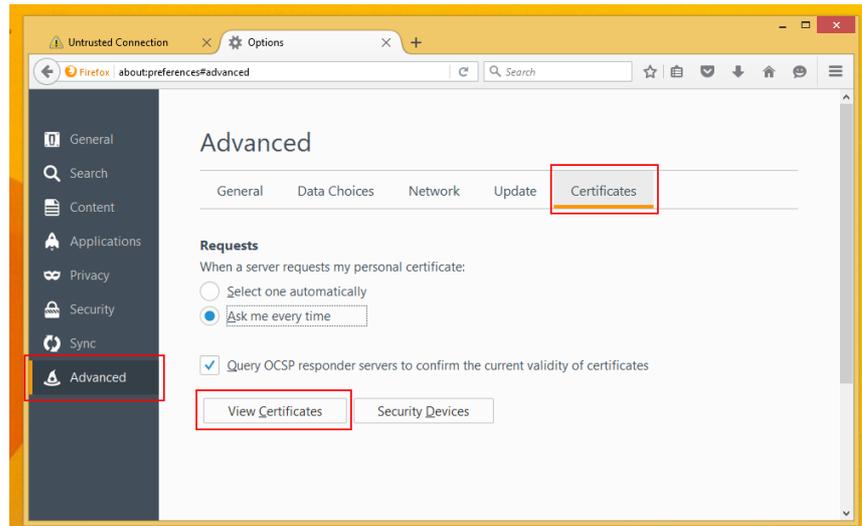
Firefox doesn't use system store instead uses its own certificate store. Shows a warning before certificate import.



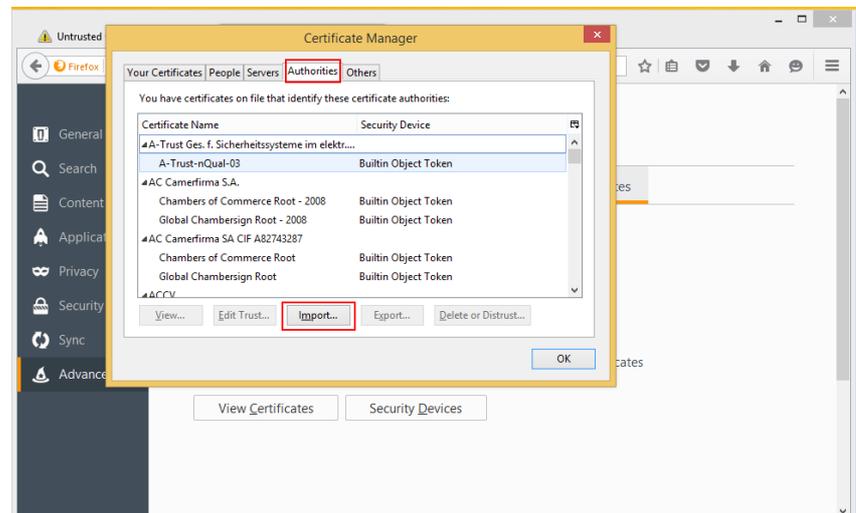
On the right click options.



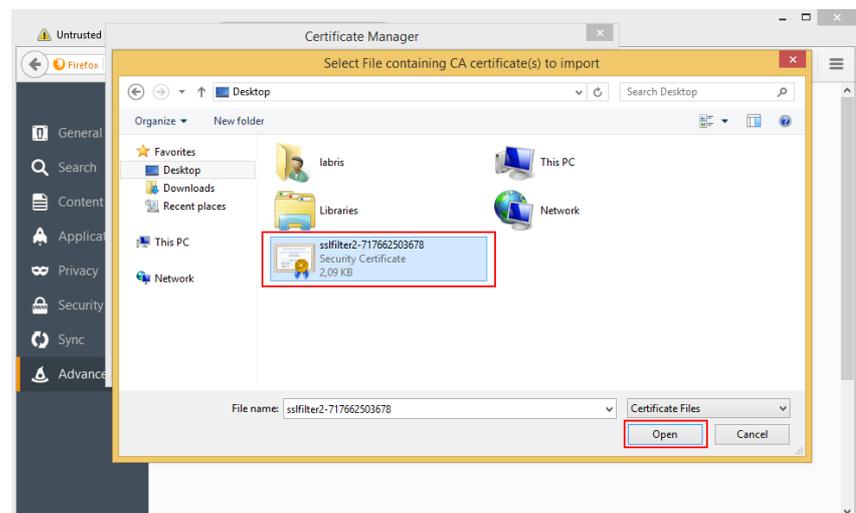
In Advanced menu, choose Certificates tab and click View Certificates.



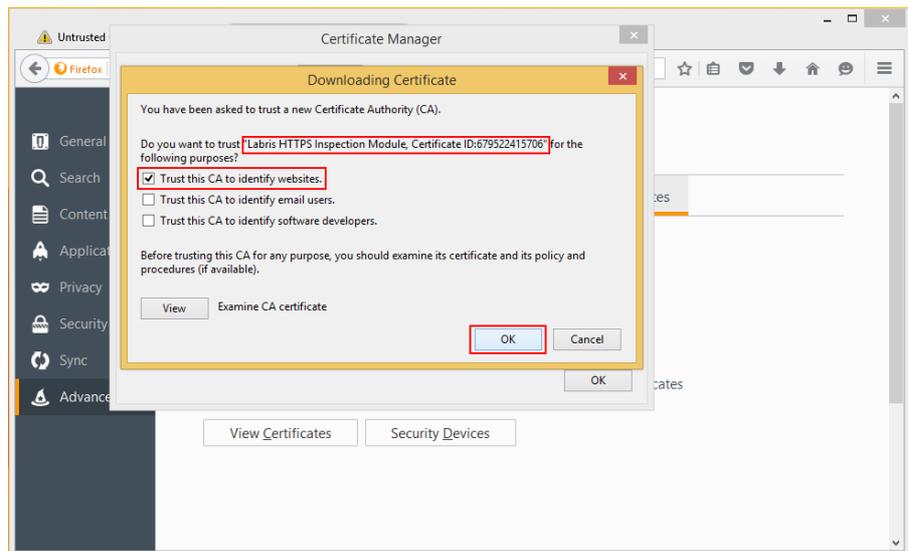
On Authorities tab, click Import.



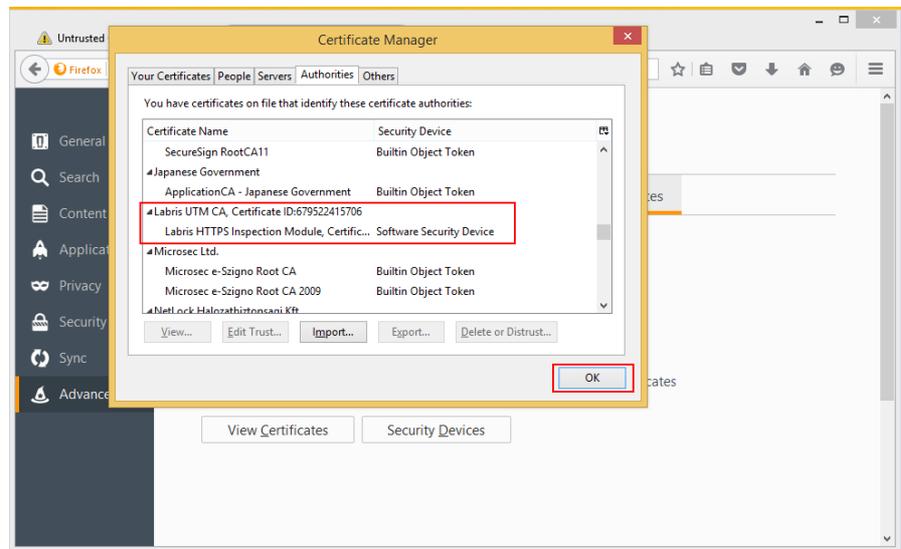
Choose Root UTM CA.



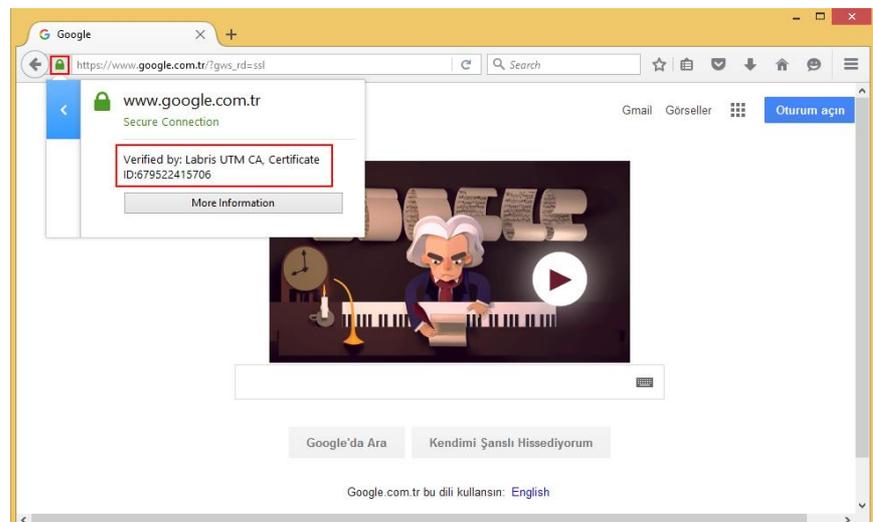
Click “Trust this CA to identify websites.”



You can see Labris UTM CA is present in Certificate Store.



Firefox shows no warning after certificate import.



OS X

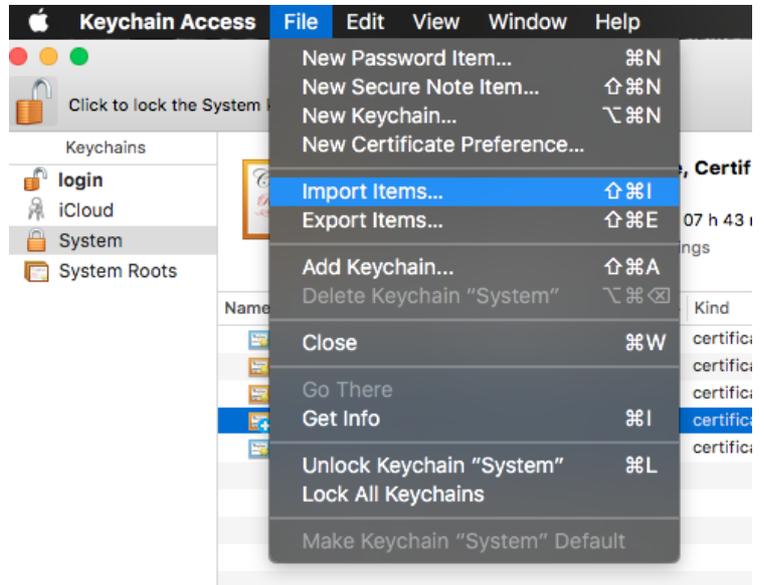
System-wide Import (Safari, Chrome)

Importing to system allows Safari and Chrome certificate problems.

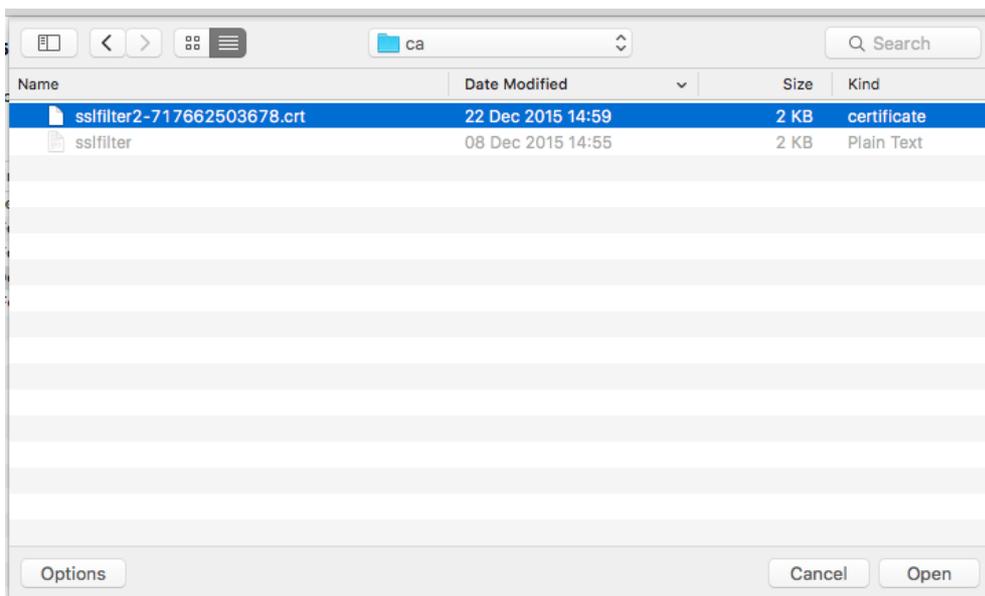
Open Keychain Access.

On the left sidebar ensure System keychain and Certificates are selected.

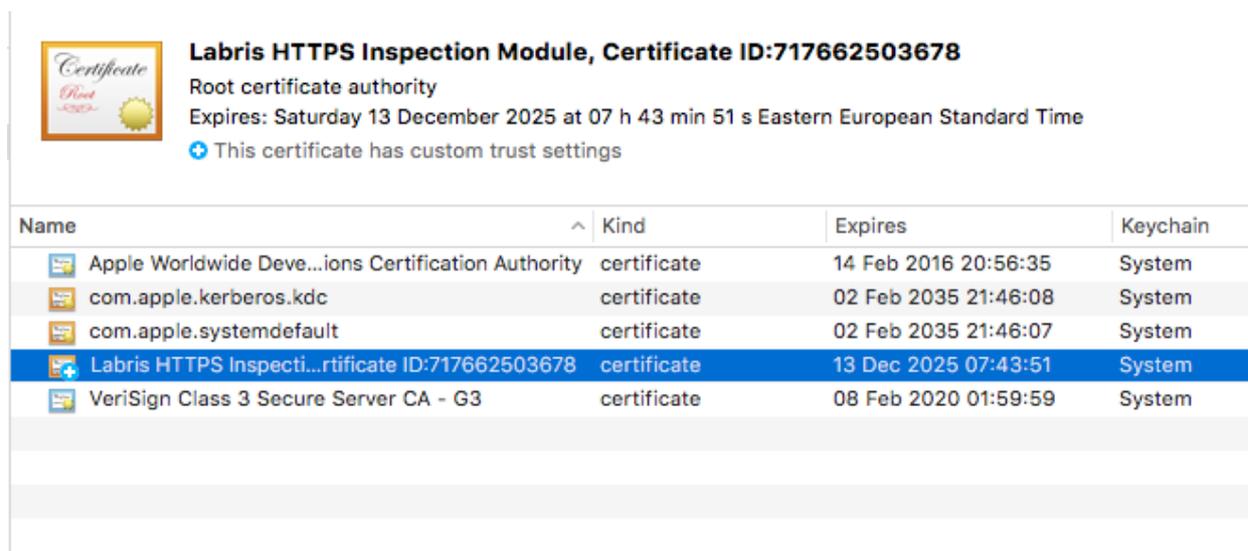
Click File -> Import Items



Choose UTM Root CA certificate file click Open.



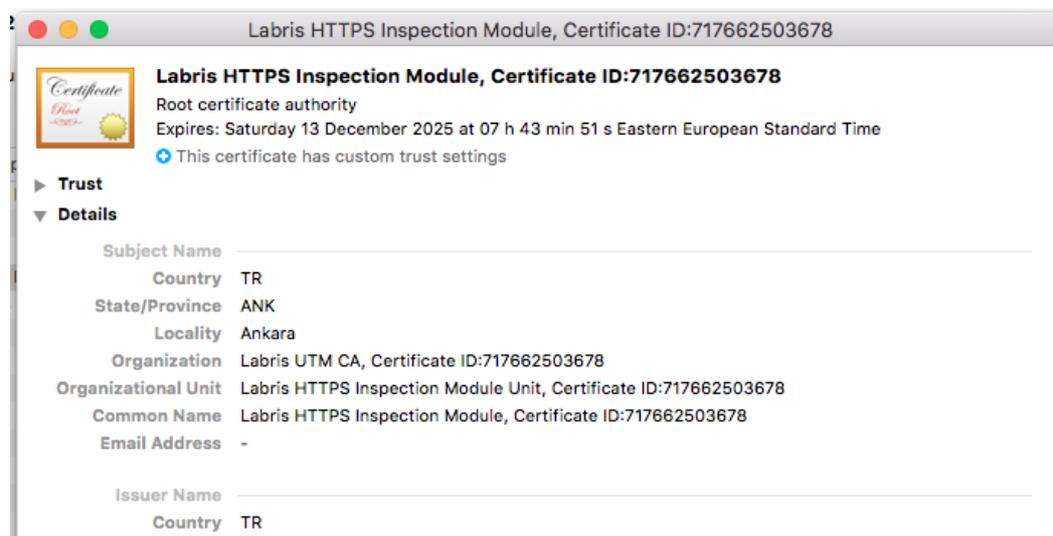
Double click on the imported certificate. This will open certificate details.



Labris HTTPS Inspection Module, Certificate ID:717662503678
Root certificate authority
Expires: Saturday 13 December 2025 at 07 h 43 min 51 s Eastern European Standard Time
+ This certificate has custom trust settings

Name	Kind	Expires	Keychain
Apple Worldwide Deve...ions Certification Authority	certificate	14 Feb 2016 20:56:35	System
com.apple.kerberos.kdc	certificate	02 Feb 2035 21:46:08	System
com.apple.systemdefault	certificate	02 Feb 2035 21:46:07	System
Labris HTTPS Inspecti...rtificate ID:717662503678	certificate	13 Dec 2025 07:43:51	System
VeriSign Class 3 Secure Server CA - G3	certificate	08 Feb 2020 01:59:59	System

Expand the section Trust.



Labris HTTPS Inspection Module, Certificate ID:717662503678
Root certificate authority
Expires: Saturday 13 December 2025 at 07 h 43 min 51 s Eastern European Standard Time
+ This certificate has custom trust settings

► Trust

▼ Details

Subject Name _____

Country TR

State/Province ANK

Locality Ankara

Organization Labris UTM CA, Certificate ID:717662503678

Organizational Unit Labris HTTPS Inspection Module Unit, Certificate ID:717662503678

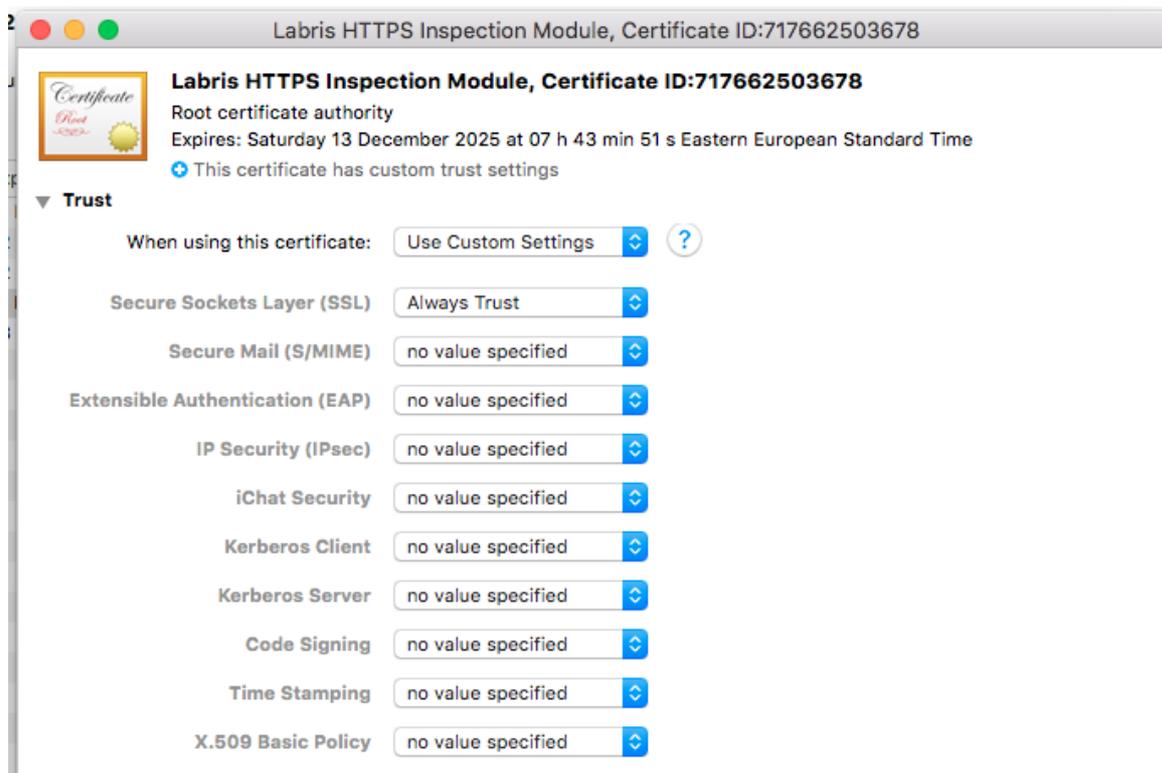
Common Name Labris HTTPS Inspection Module, Certificate ID:717662503678

Email Address -

Issuer Name _____

Country TR

Choose Always Trust for Secure Sockets Layer.



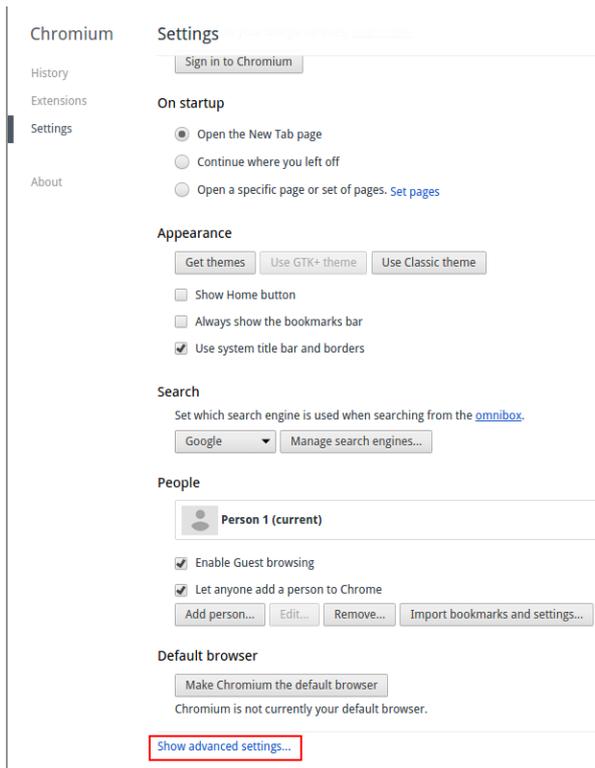
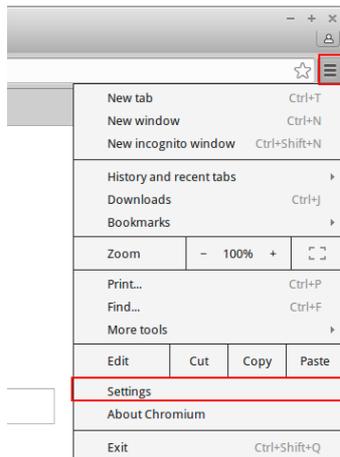
Linux

Firefox

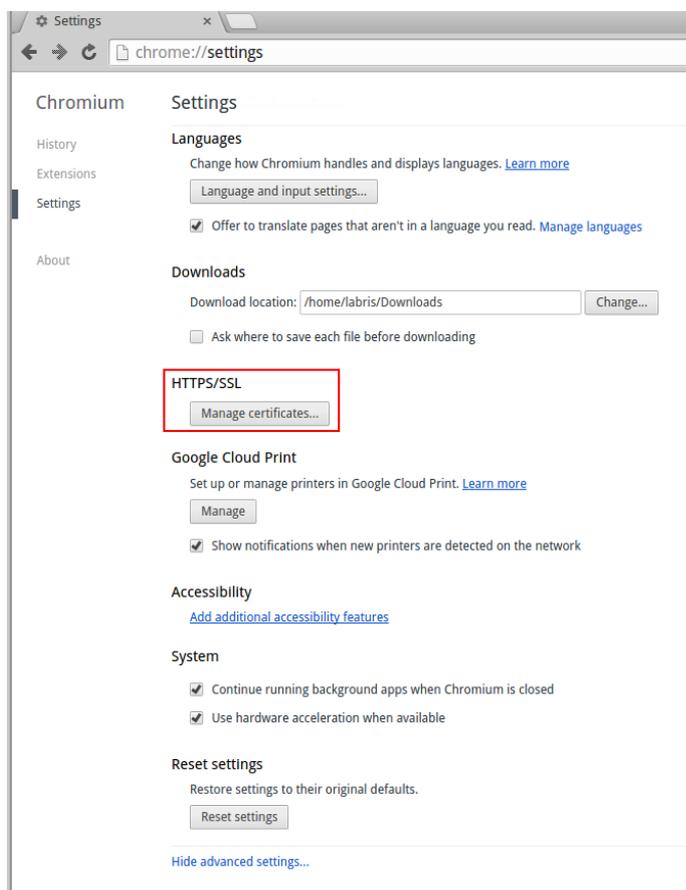
Steps are the same as Firefox on Windows.

Chromium

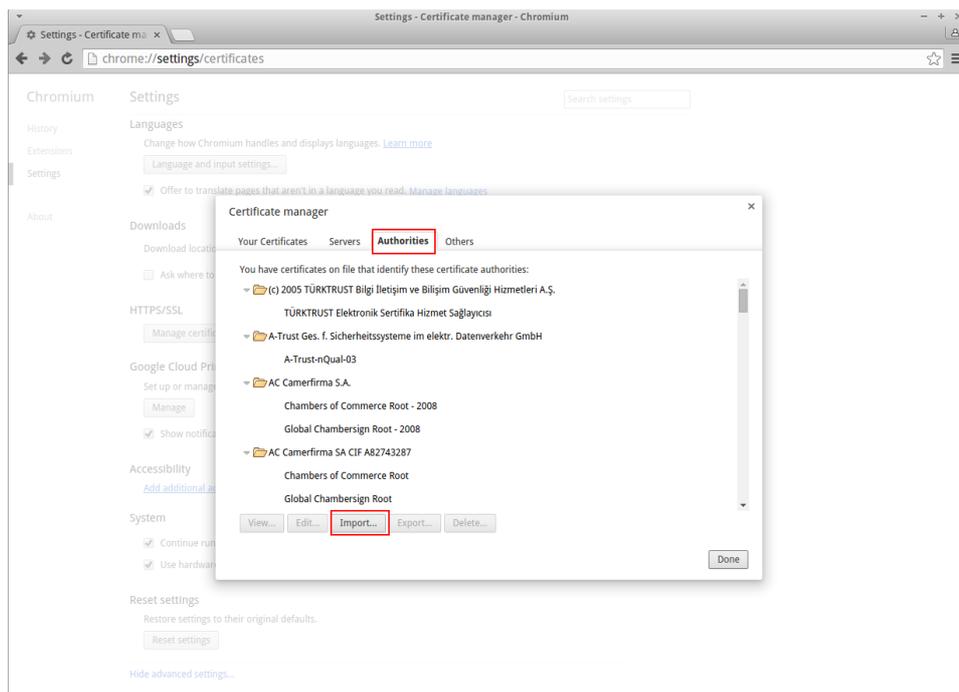
Click Settings on right and click Show advanced settings.



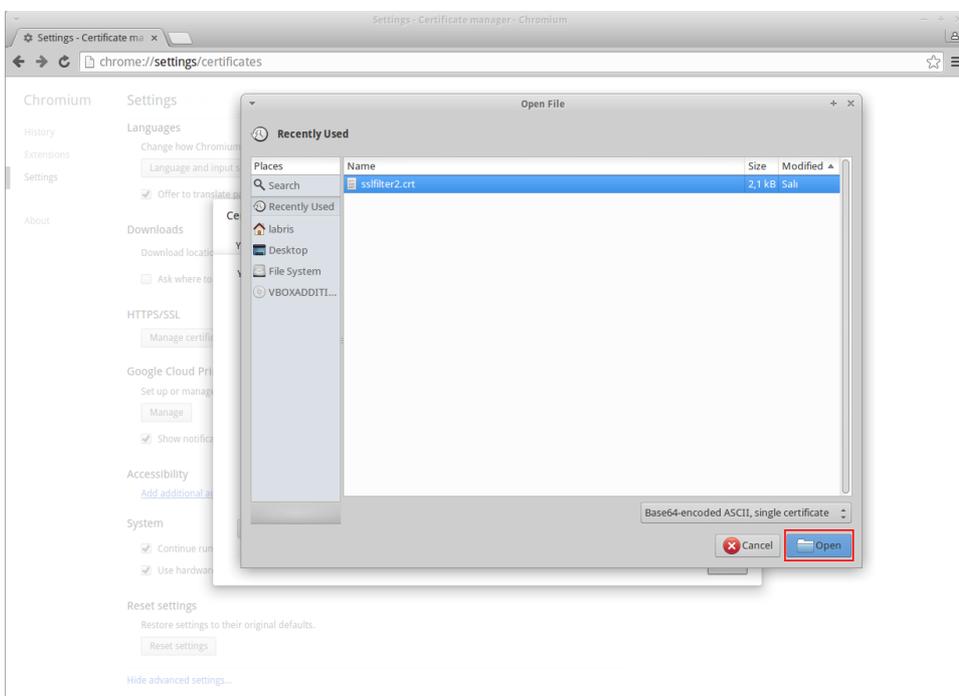
Click Manage certificates.



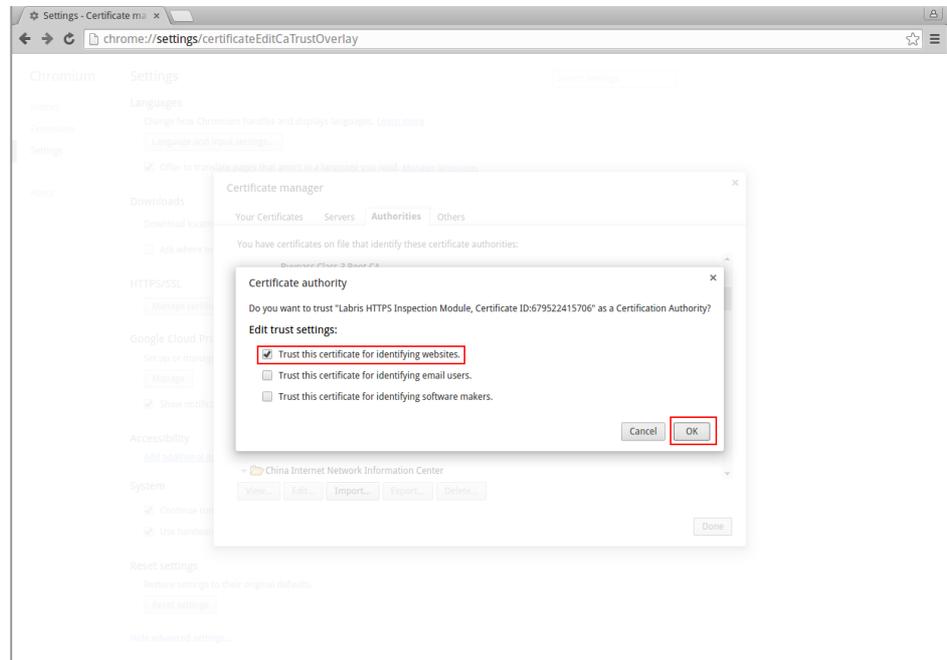
Open Authorities tab
and click Import.



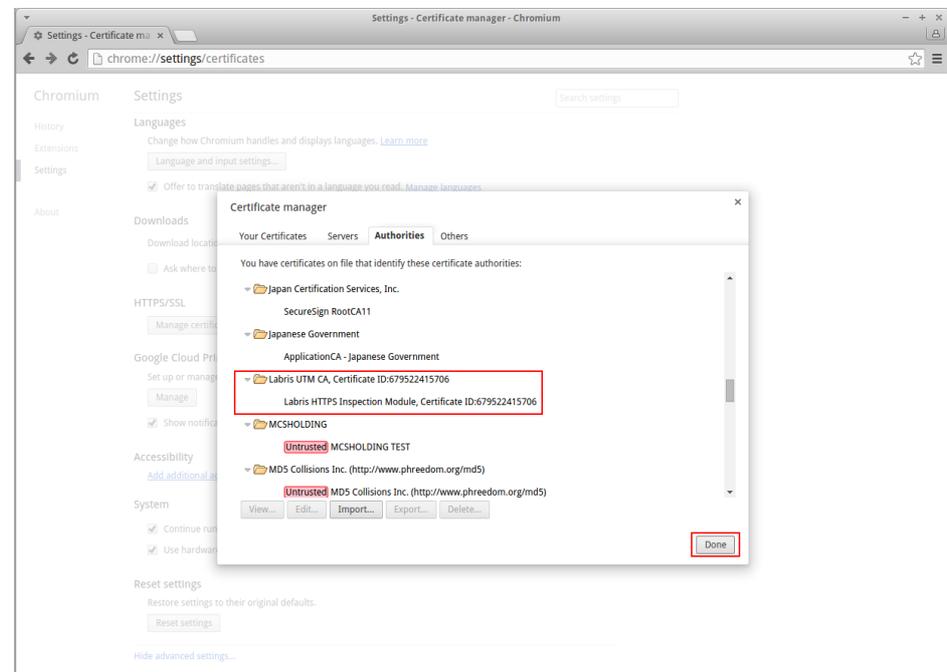
Choose Root UTM
CA.



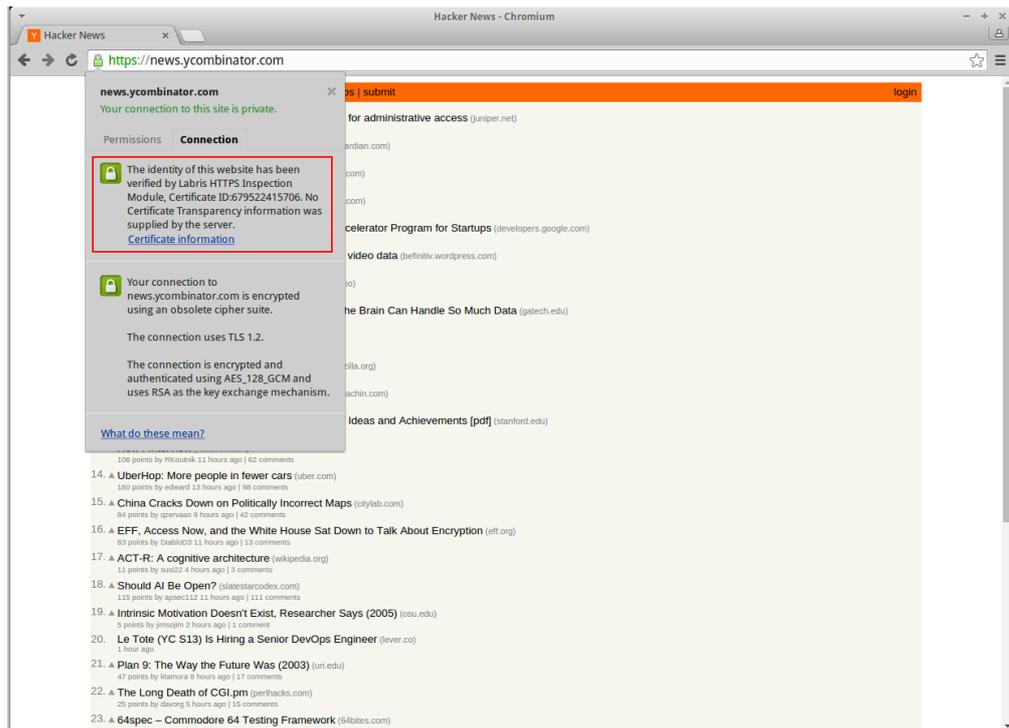
Click “Trust this certificate to identify websites”.



Certificate is listed here.



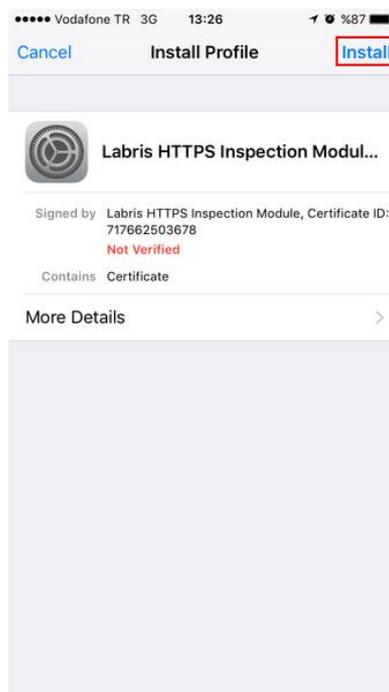
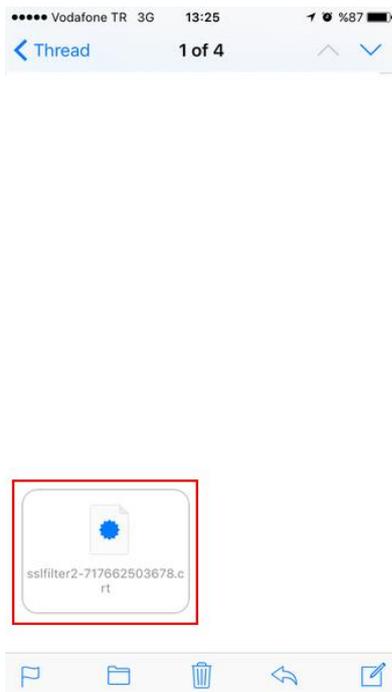
Chromium shows no warning and certificate is signed by Labris UTM CA.

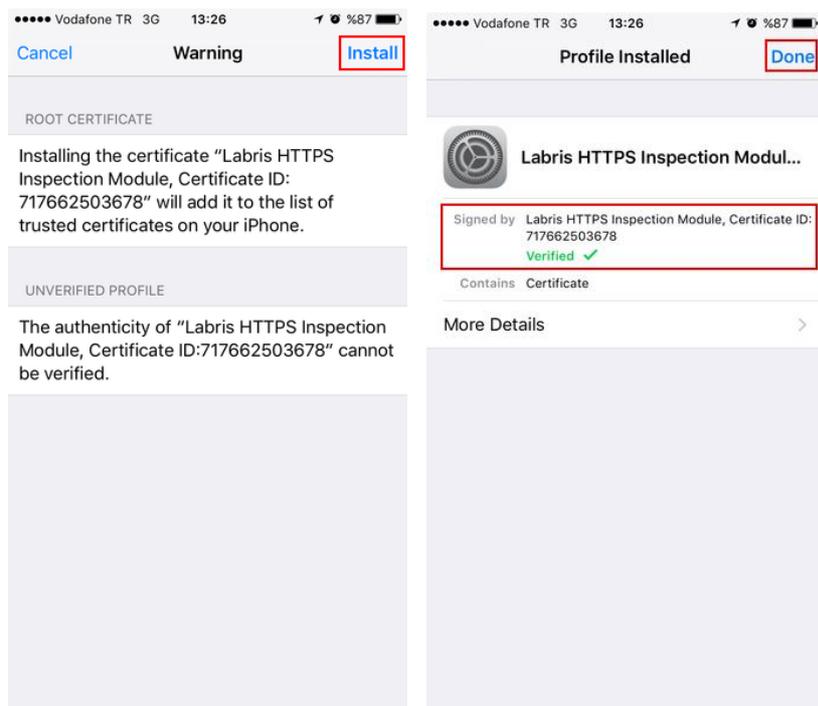


Certificate Import (Mobile)

iOS

Certificate can be transported to device via e-mail. Importing is simple. Use the steps below.





Android

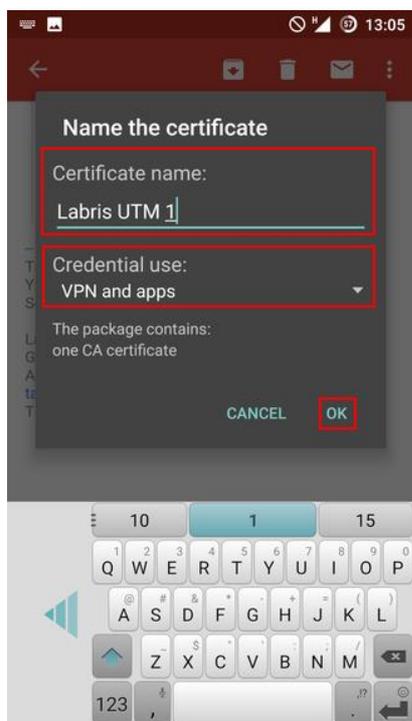
System-wide Import

Certificate should be imported to Android Trusted Credentials. Sending the certificate via mail is the recommended way. Other possible options would be placing the certificate on a HTTP server or on a FTP server.

Download attachment from mail

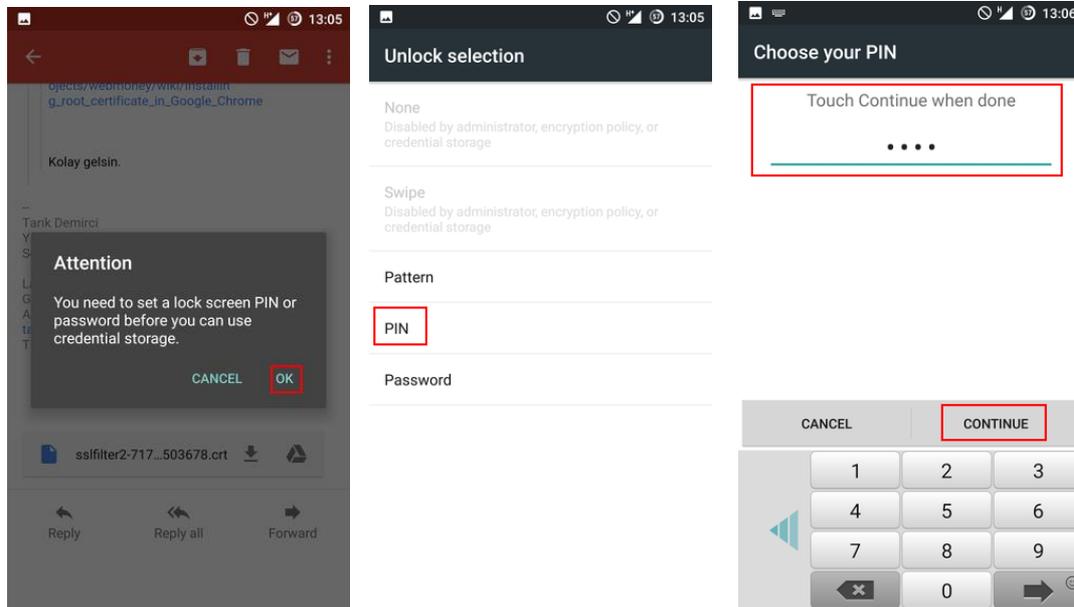


Give a name to certificate

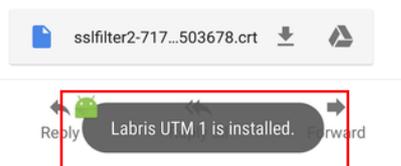


Set-up screen lock

If device doesn't have a screen lock set up already, Android may require this prior to certificate import. Different vendors and different Android versions have implemented different policies about this issue. Some of them may enforce PIN lock while some others seems to accept also Pattern screen lock.

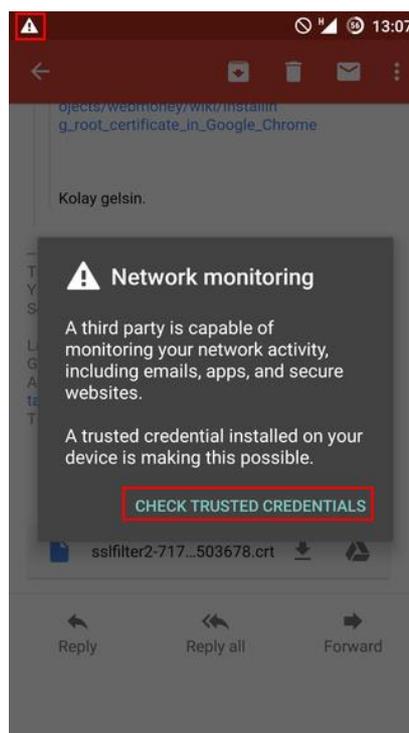


Certificate import completed



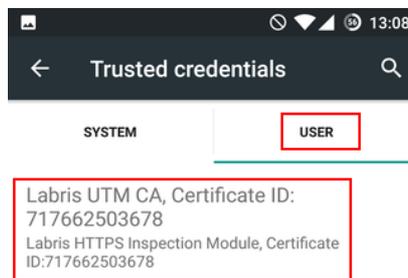
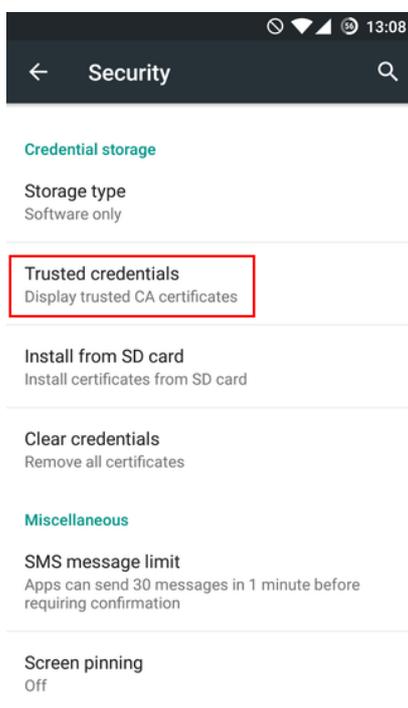
Network Monitoring Warning

After importing the certificate, Android System shows a warning with the title of 'Network Monitoring' even if cellular connection is used instead of Wi-Fi. Some vendors and some Android versions allow dismissing this warning while others don't. If system doesn't allow dismissing, there is no way to disable this warning.



Checking trusted CAs

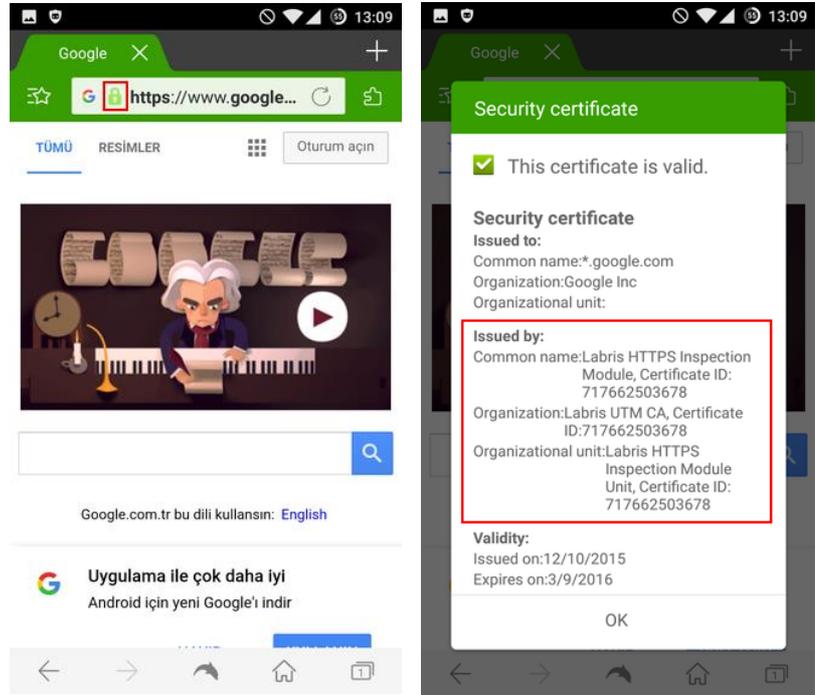
Imported certificate can be examined under the Trusted Credentials menu.



Testing certificate import

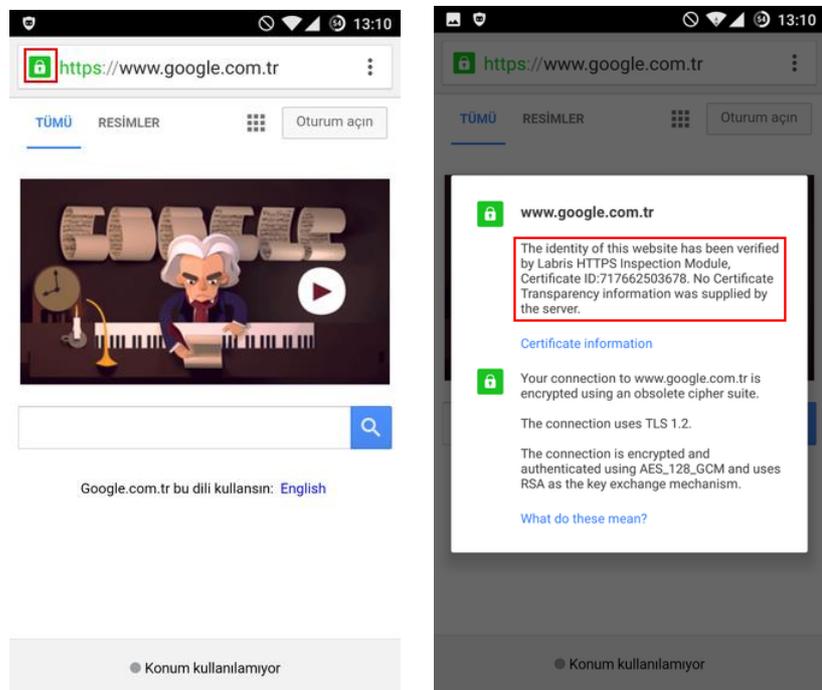
Dolphin Browser

Dolphin respects CAs trusted by system. HTTPS Filtering works with no issues after certificate is imported. Inspection of connection details shows that Labris UTM analyses the connection.



Chrome

Chrome respects CAs trusted by system. HTTPS Filtering works with no issues after certificate is imported. Inspection of connection details shows that Labris UTM analyses the connection.



Opera

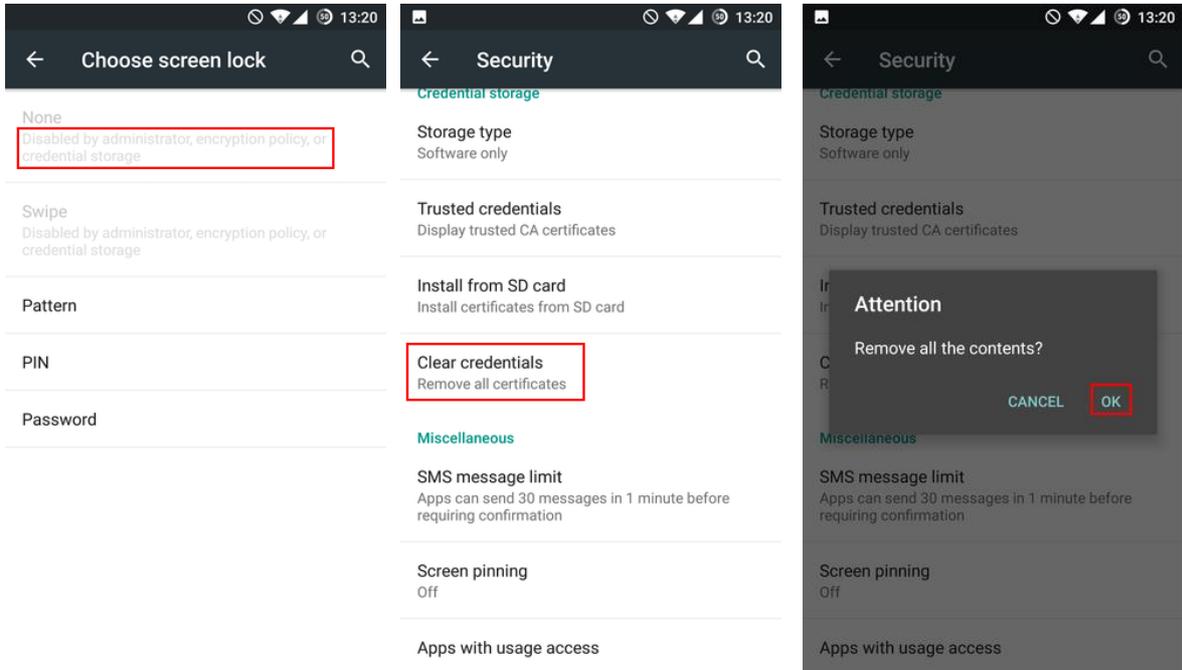
No issues after importing certificate.



Clearing Trusted Credentials and Disabling Screen Lock

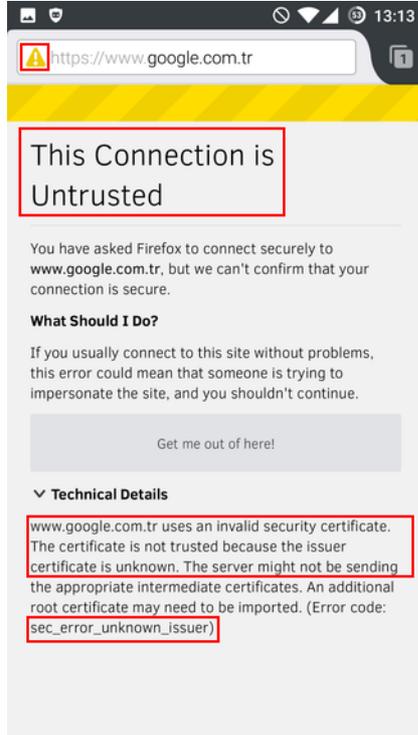
Android doesn't allow disabling screen lock when a third-party CA is imported. To clear the credentials store and disable screen lock, follow the steps below.

Warning: Clearing credentials will prevent establishing HTTPS connections. Do this only if the device will not be subject to HTTPS filtering anymore.



Firefox (Not Supported)

Firefox for Android doesn't use System CA Store for validation and doesn't provide a way to import third-party CAs. So it can't be used with HTTPS filtering.



Windows Phone

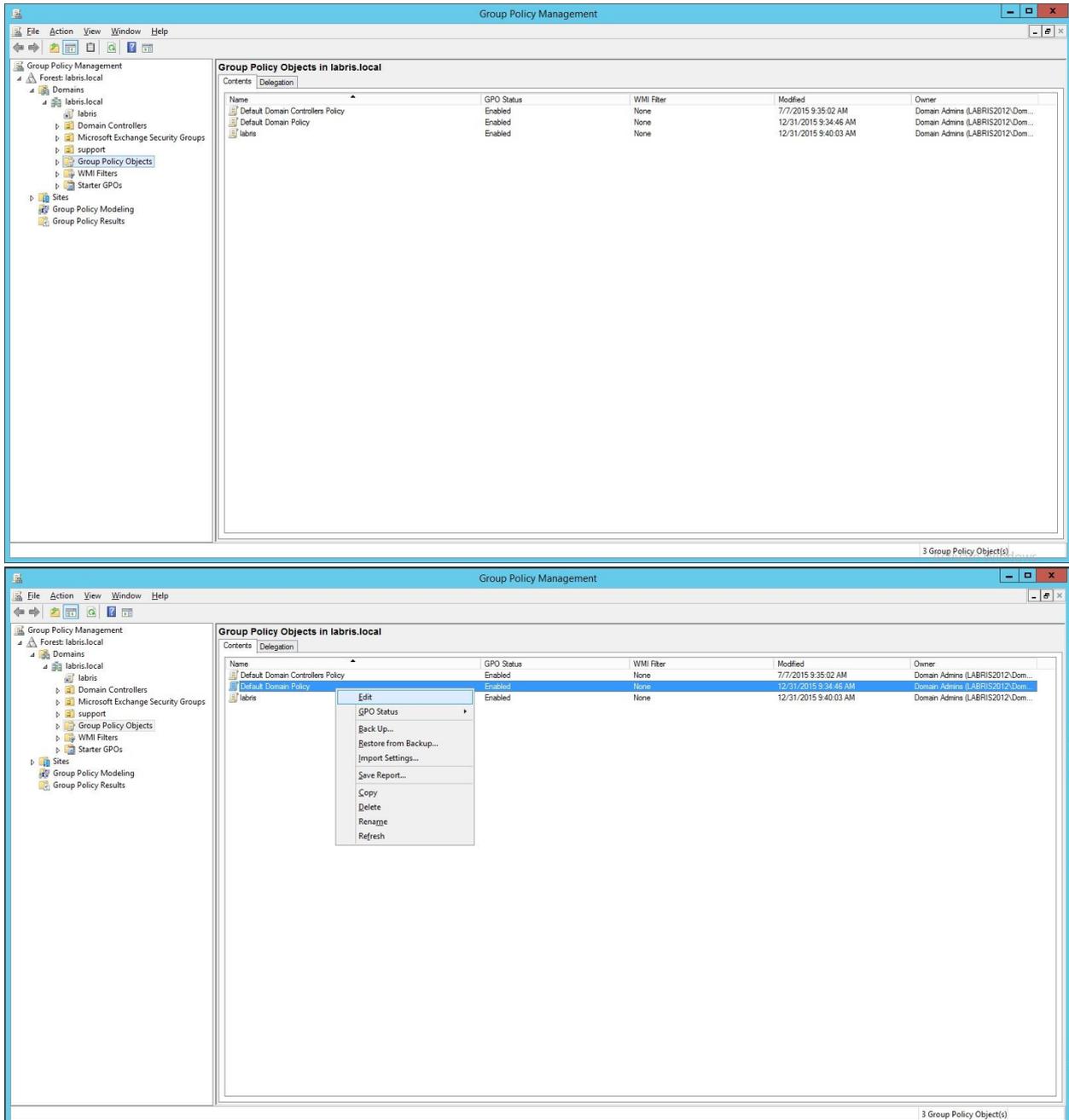
Windows phone doesn't recognize PEM encoded "*.crt" certificates. Certificate needs to be converted to DER format and its extension must be ".cer". This can be accomplished in a Linux system with the following command:

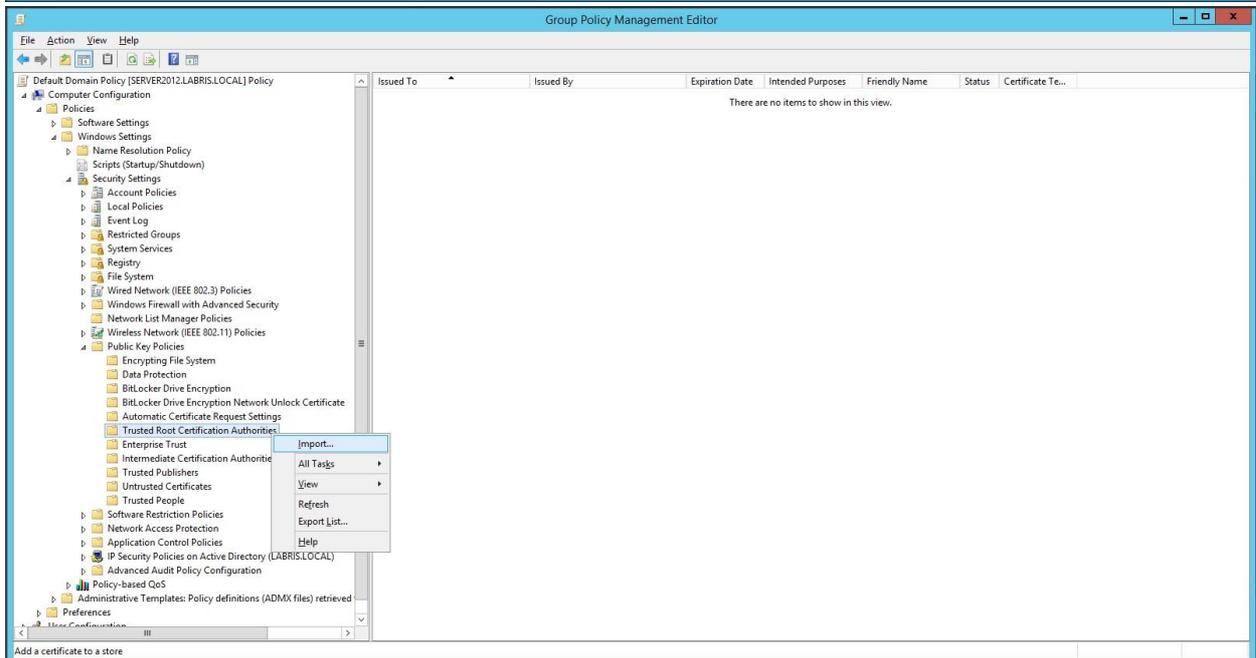
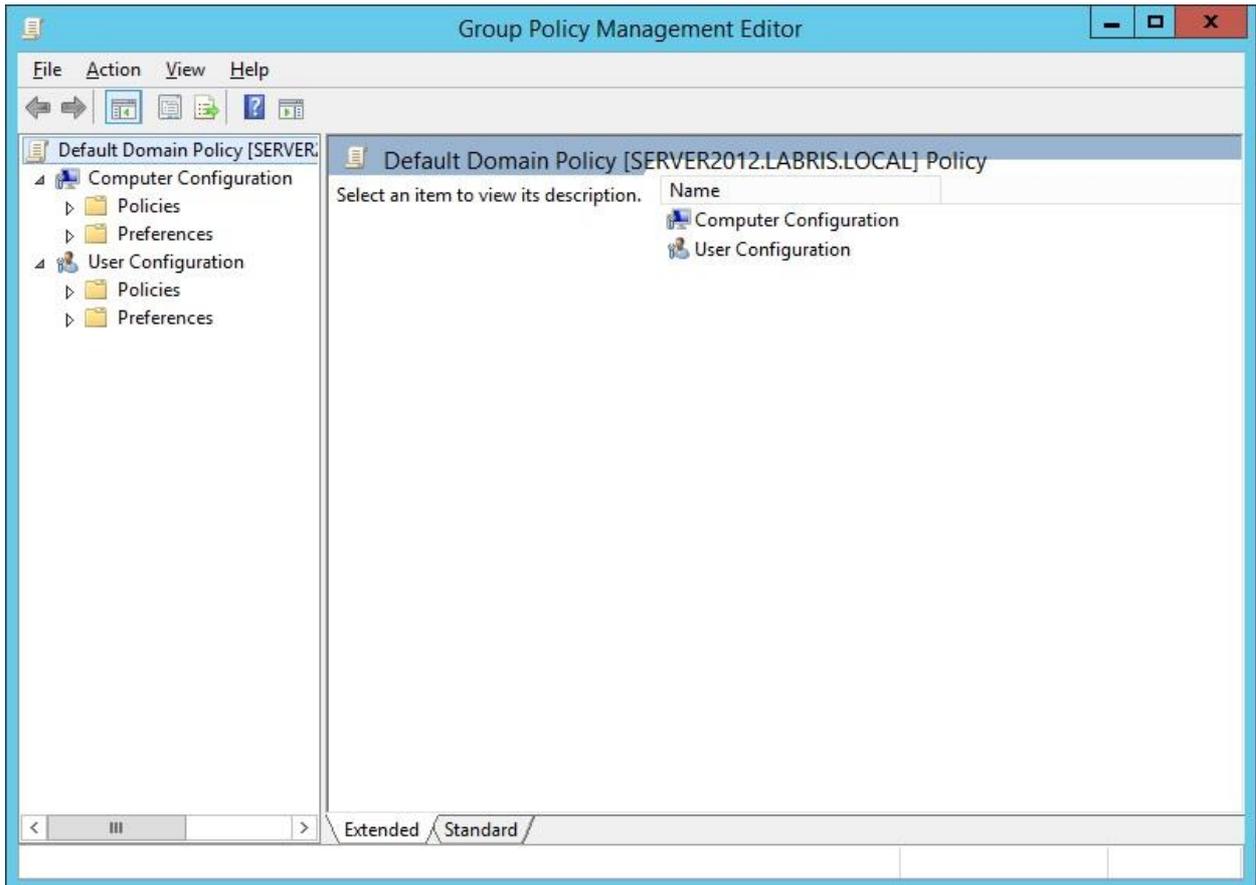
```
openssl x509 -in sslfilter2.crt -outform der -out sslfilter2.cer
```



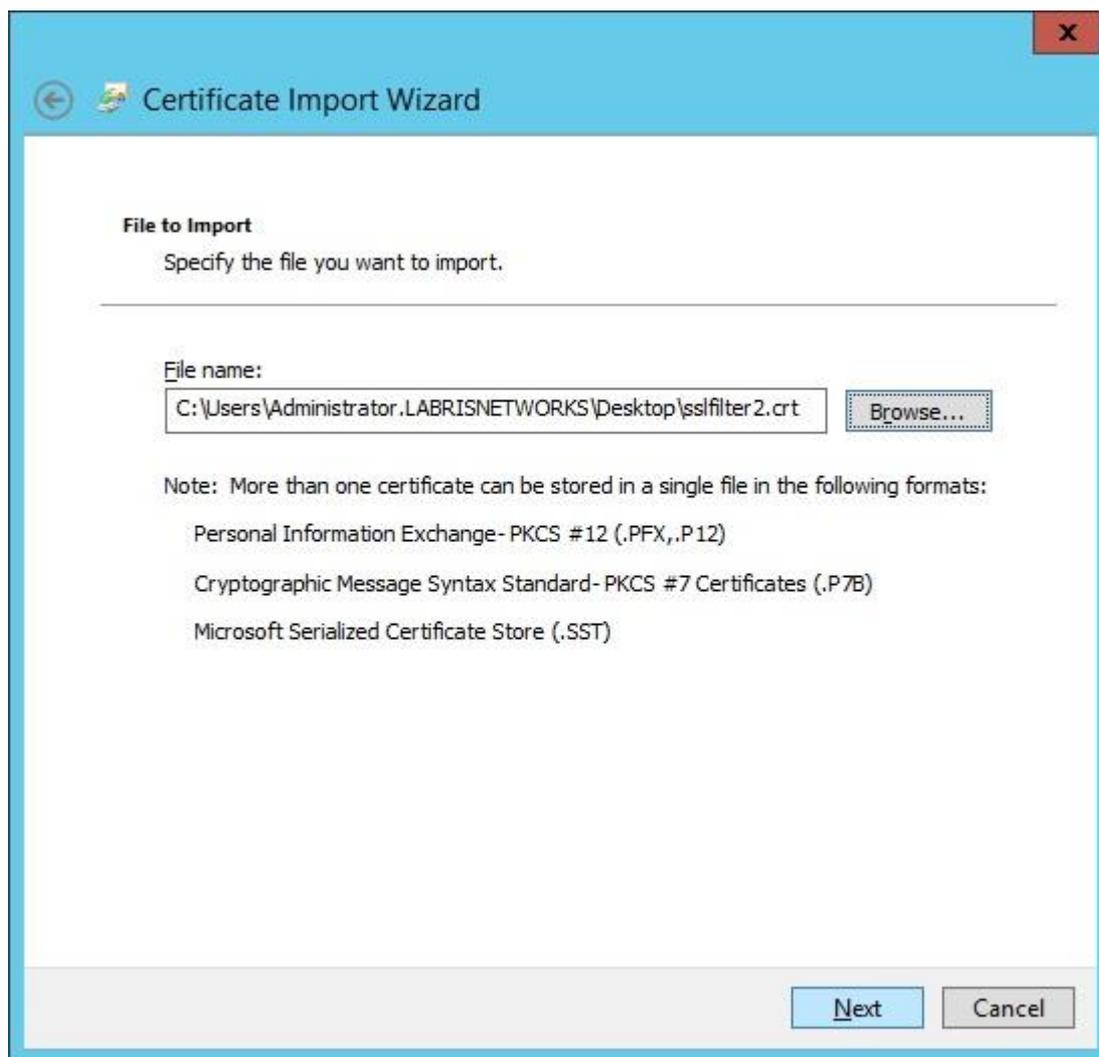
Certificate Distribution via Active Directory

You can use the steps below to distribute Labris UTM Root CA via Active Directory.

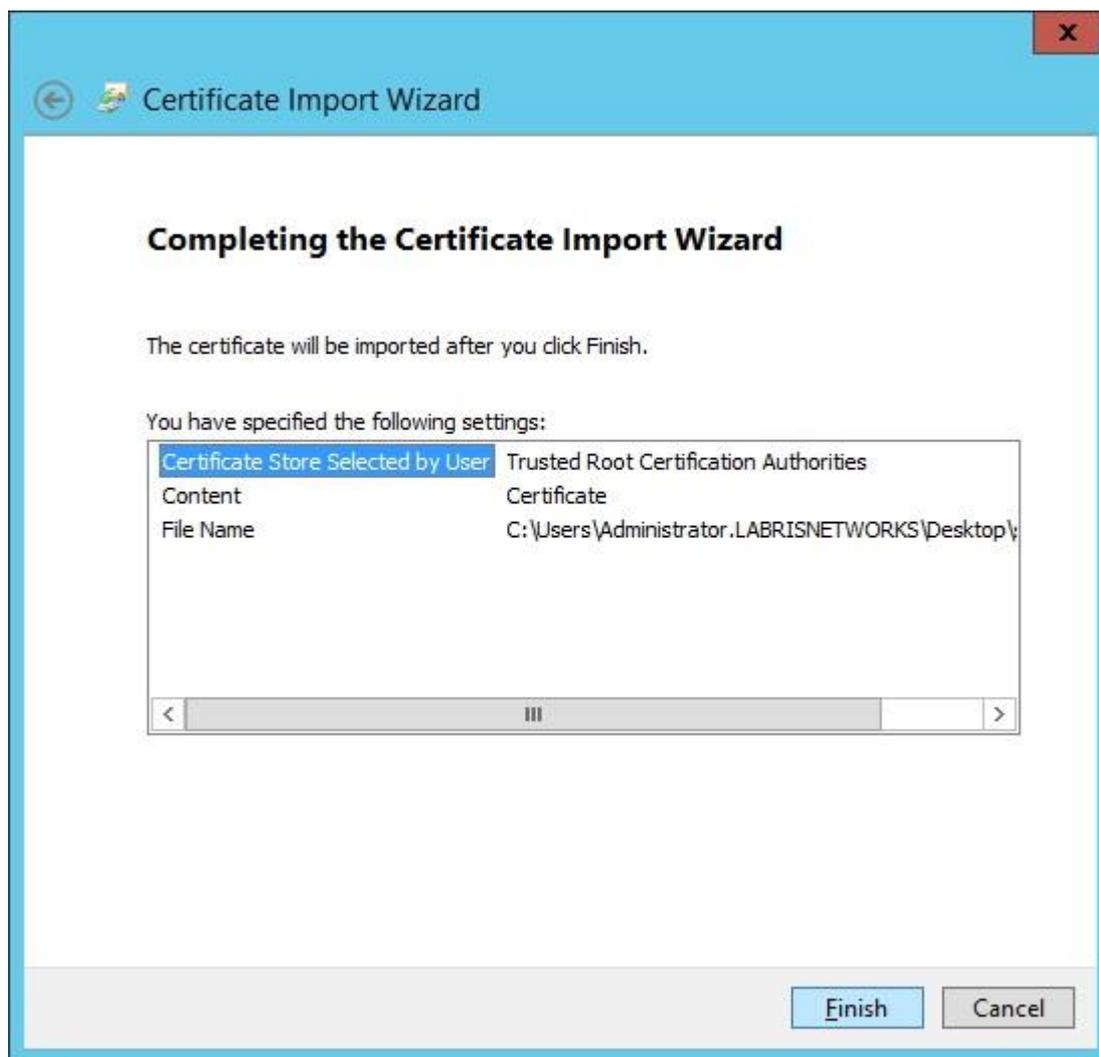


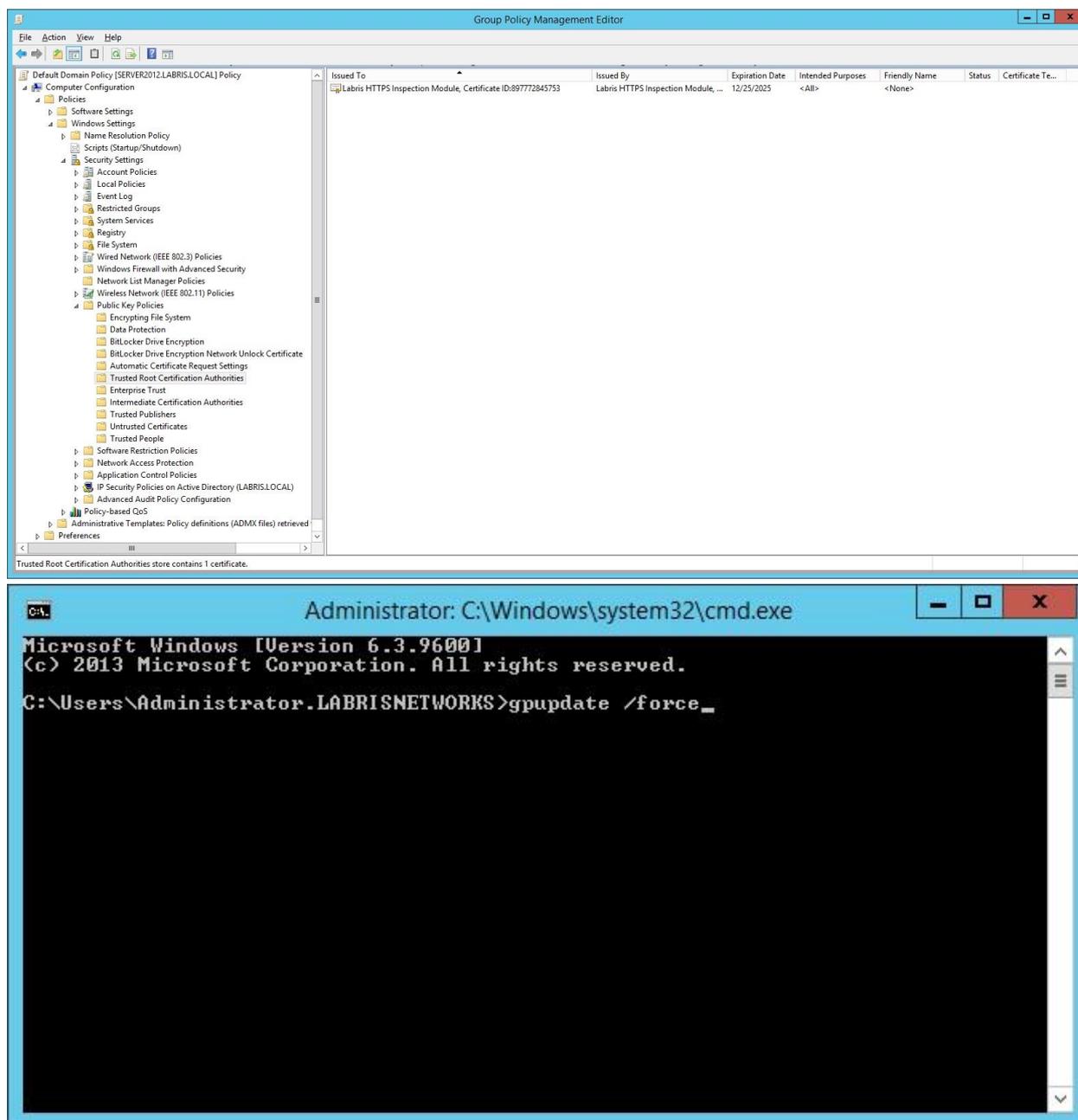












Customizing Root CA Details

You can use the below command to regenerate the certificate with custom details:

```
openssl req -new -key /opt/labris/etc/labris-webcache/certs/sslfilter2.key -x509 -days 3650 -out /opt/labris/etc/labris-webcache/certs/sslfilter2.crt
```

Openssl will ask for details. Fields and **default values of Labris UTM CA** are shown below:

Country Name (2 letter code) [GB]: **TR**

State or Province Name (full name) [Berkshire]: **ANK**

Locality Name (eg, city) [Newbury]: **Ankara**

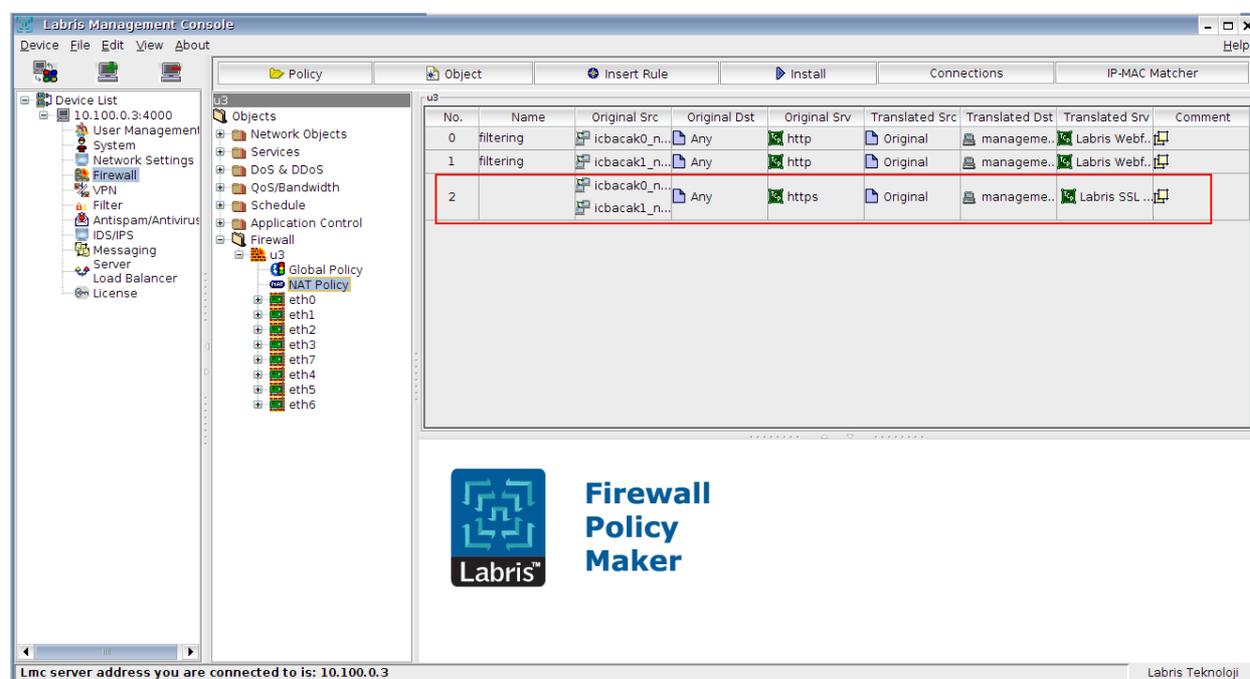
Organization Name (eg, company) [My Company Ltd]: **Labris UTM CA, Certificate ID: <ID>**

Organizational Unit Name (eg, section) []: **Labris HTTPS Inspection Module Unit, Certificate ID: <ID>**

Common Name (eg, your name or your server's hostname) []: **Labris HTTPS Inspection Module,**
Certificate ID:<ID>
Email Address []: -

Firewall Configuration

Connections to TCP Port 443 must be intercepted in order to make HTTPS Filtering work.



NTLM Authentication AD Configuration

90.General View

Active Directory users can be used in areas such as Firewall, Webfilter, VPN, Wauth by integrating Labris products with Active Directory. Authorization can be made with the user name or rules can be written.

Logon script must be set for all users with Group Policy on Active Directory for using simple authentication system. Logon script shares user information periodically with Labris. With this method, the correct settings can be made by making the necessary settings on structures which have more than one location and using the same active directory.

91.Prerequisite

Active Directory Structure must be set and all computers must be included in Active Directory. Active Directory integration must be made with Labris.

92. Scenario

Logon script settings will be made by using Group Policy on active directory integrated with Labris. How to make settings on structures which have more than one location and using the same active directory will be explained

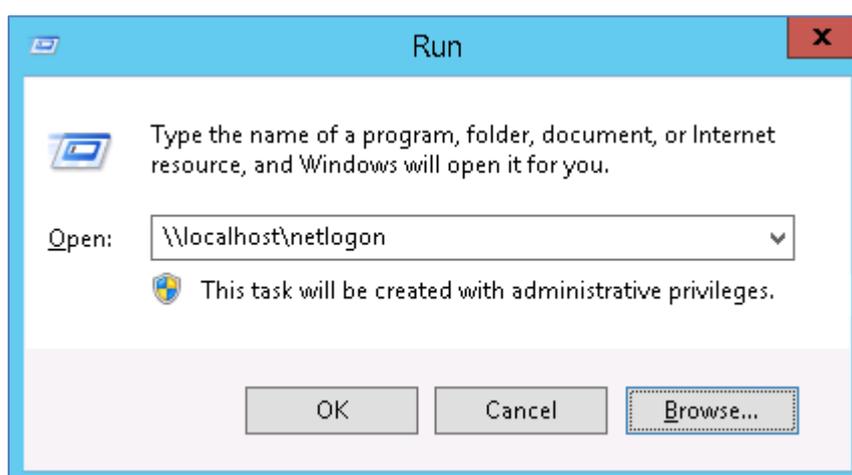
This expression was performed on Windows Server 2012.

Although general method is same for Windows Server 2003/2008, the location of the menu on server can be different.

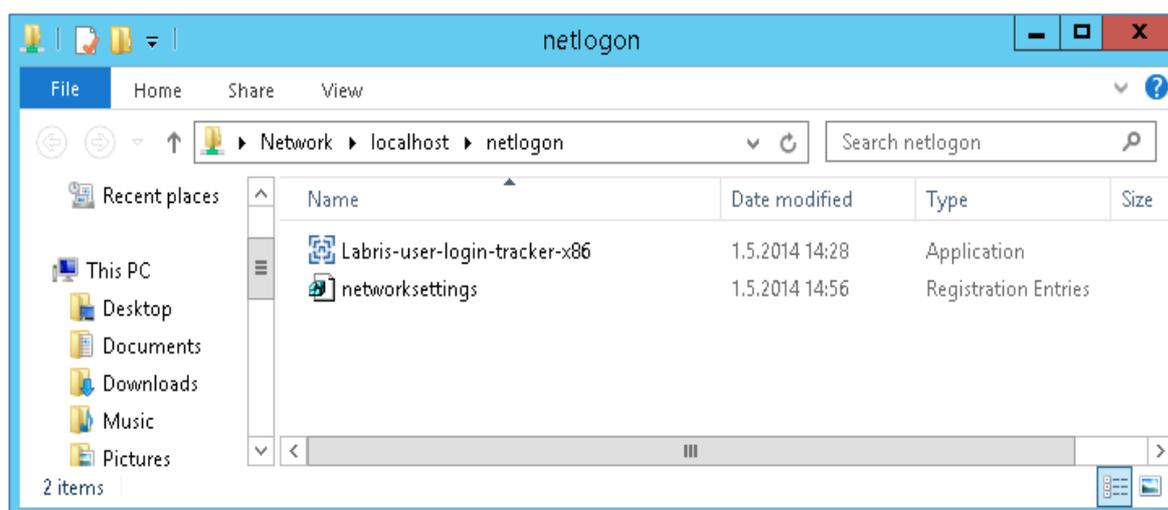
93. Configuration

Step 1: The attached files are downloaded and are copied to netlogon directory of Active Directory server.

- a. **Run** opens by using "**Windows + R**" keys combination and netlogon directory is called as in the picture.

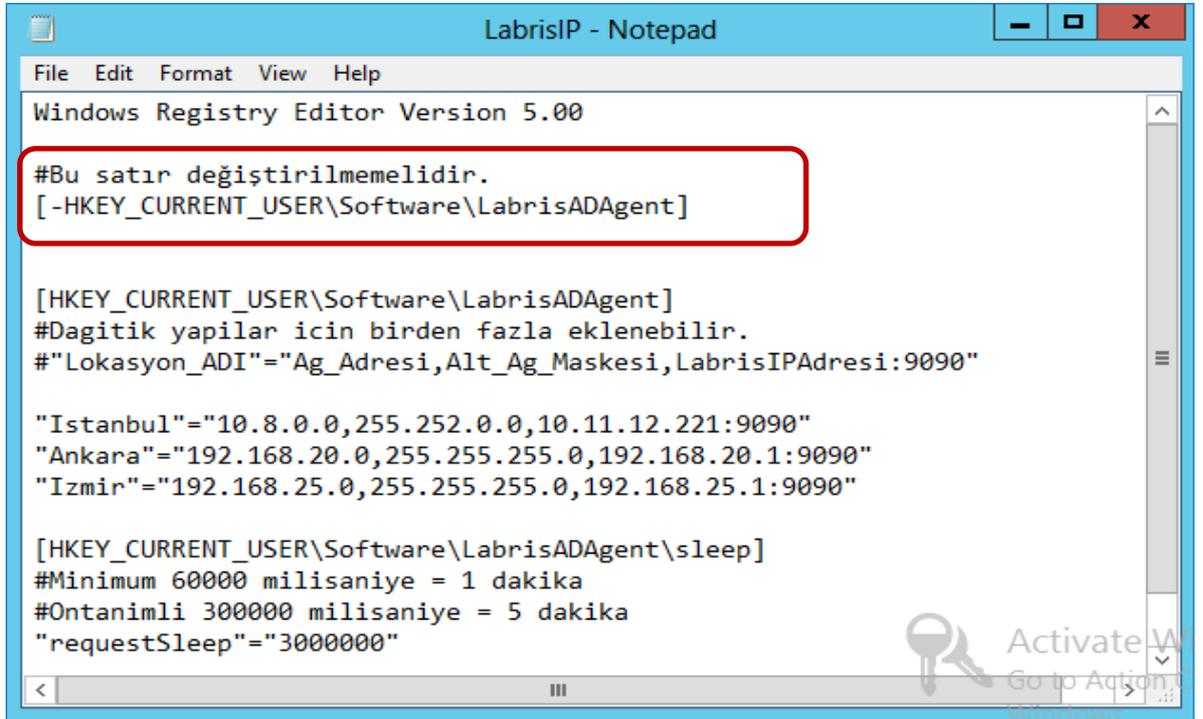


Attached files are copied to this area.



- b. **networksettings registry file is edited for the network settings.**
Right button + edit are clicked on **networksettings** file.
Appropriate definitions are made to your network settings in registry file opened.

If the regedit file is not set, the gateway of computer sends requests to the IP address by default. If the default gateway is Labris device, it works without any problems.



The screenshot shows a Notepad window titled "LabrisIP - Notepad" containing the text of a registry file. The text is as follows:

```
Windows Registry Editor Version 5.00

#Bu satır deđiřtirilmemelidir.
[-HKEY_CURRENT_USER\Software\LabrisADAgent]

[HKEY_CURRENT_USER\Software\LabrisADAgent]
#Dagitik yapilar icin birden fazla eklenebilir.
#"Lokasyon_ADI"="Ag_Adresi,Alt_Ag_Maskesi,LabrisIPAdresi:9090"

"Istanbul"="10.8.0.0,255.252.0.0,10.11.12.221:9090"
"Ankara"="192.168.20.0,255.255.255.0,192.168.20.1:9090"
"Izmir"="192.168.25.0,255.255.255.0,192.168.25.1:9090"

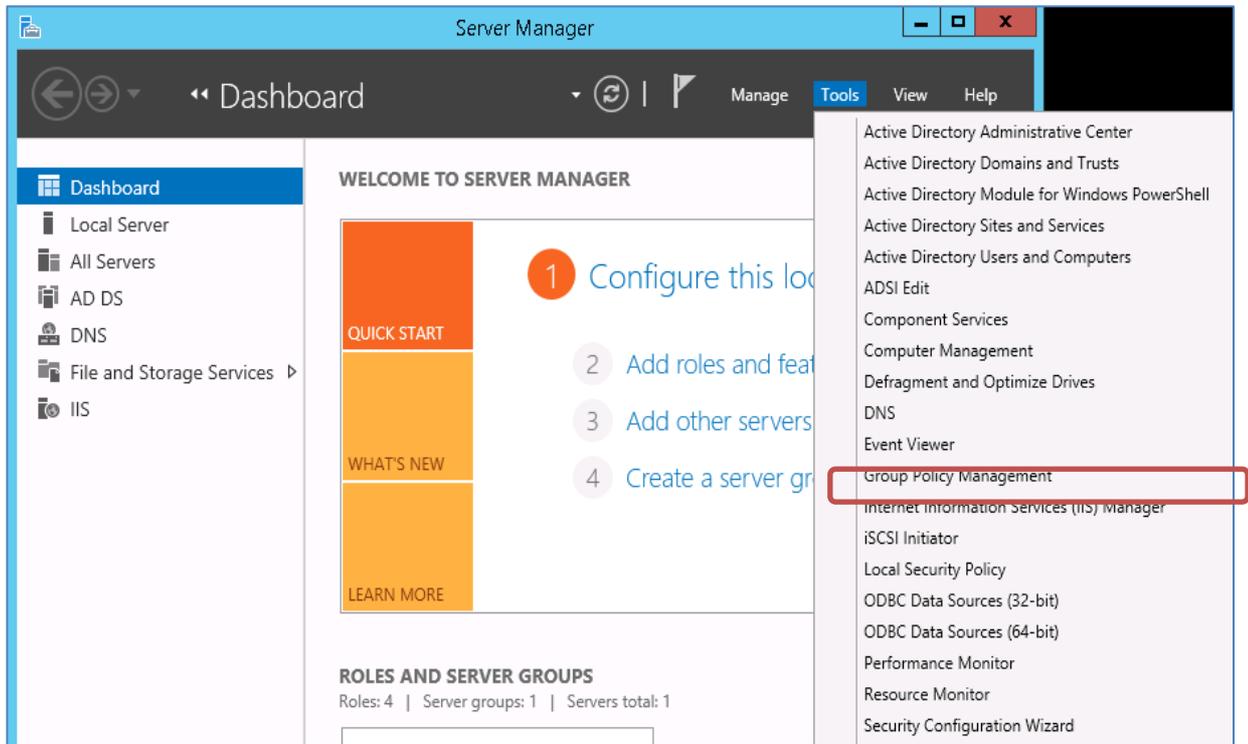
[HKEY_CURRENT_USER\Software\LabrisADAgent\sleep]
#Minimum 60000 milisaniye = 1 dakika
#Ontanimli 300000 milisaniye = 5 dakika
"requestSleep"="3000000"
```

Parameter Description

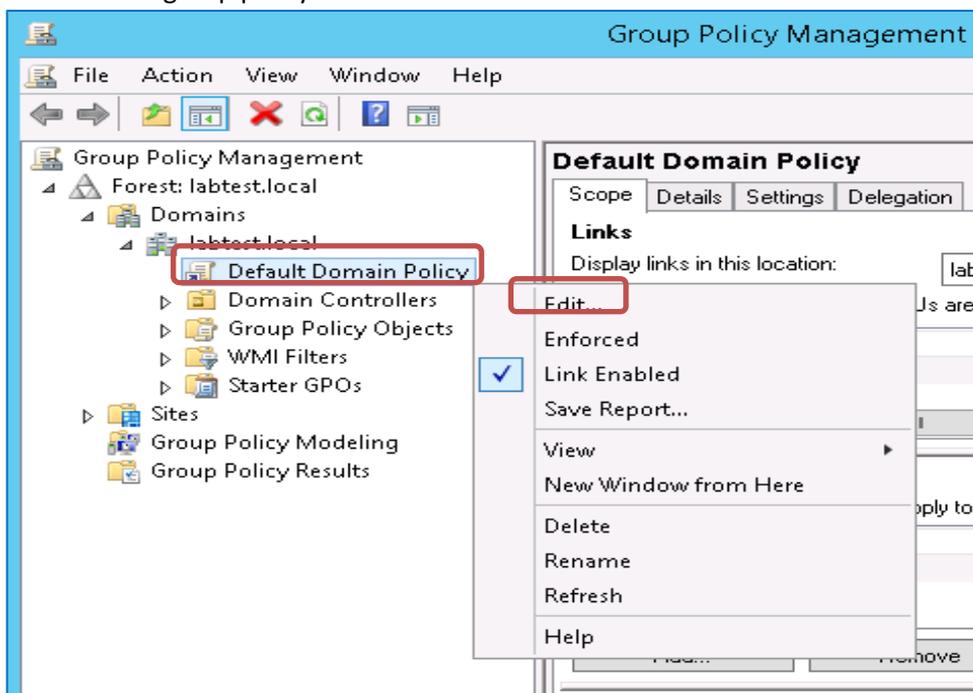
No	Parameter	Value	Description
1	Location Name	Istanbul	The location name to be made network identification.
2	Network Address	192.168.20.0	Network address of the Labris device location is written.
3	Subnet Mask	255.255.255.0	The subnet mask belongs to network address specified is defined.
4	Labris IP address	192.168.20.1	Labris device's IP address in location is written.
5	Labris Port	9090	The port accepting requests on Labris. TCP 9090
6	requestsleep	3000000	It is set that it will make communicate with Labris device in how many milliseconds. It is set 5 minutes by default. It can be set so as to at least 1 minute.

Step 2: Active Directory Group Policy settings are made.

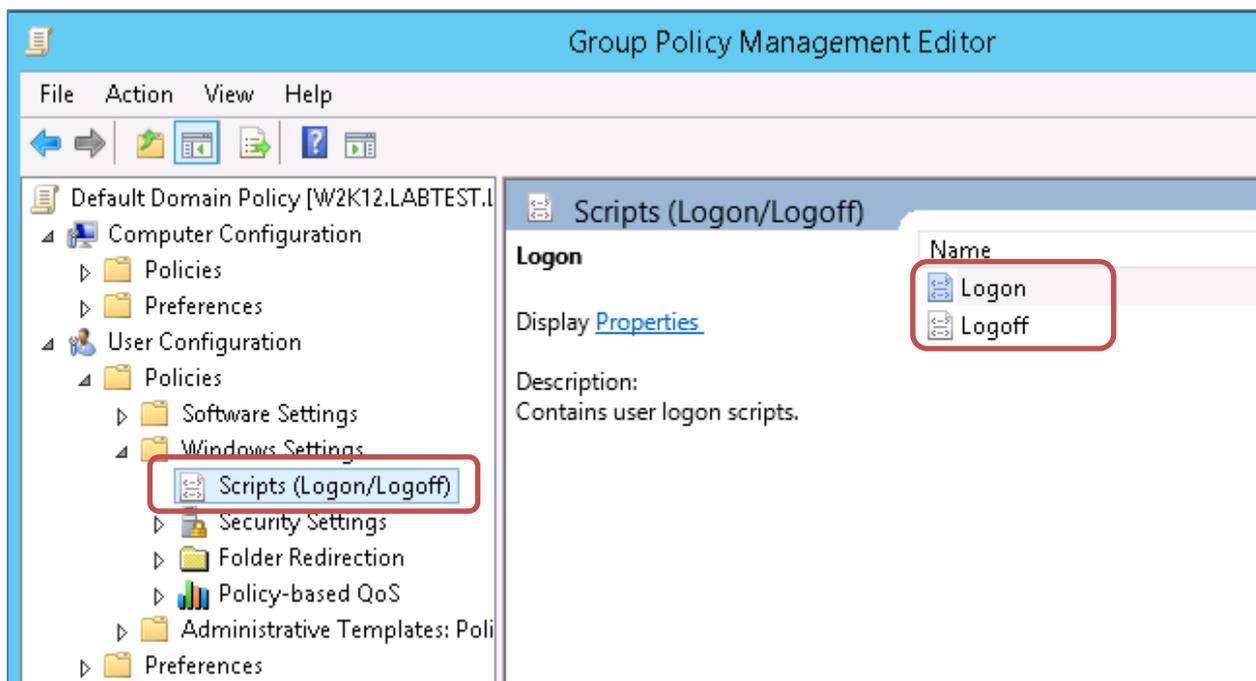
It is entered in the **Group Policy** Management window.



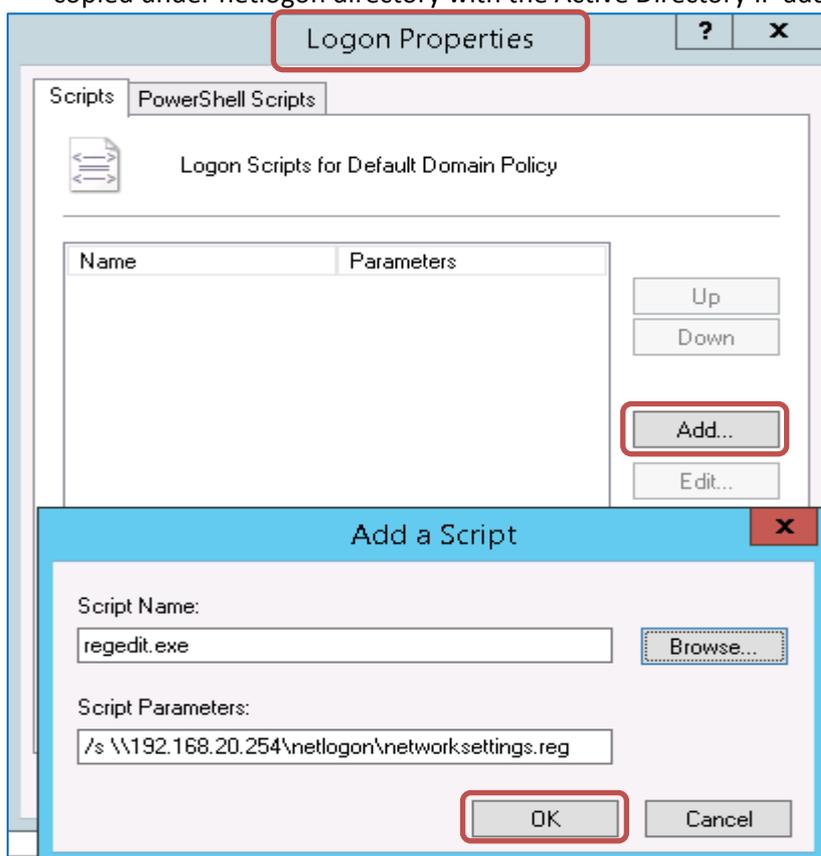
Default Domain Policy is set. If desired, settings can also be made here by creating a different group policy.



Script Settings section opens.



- a. **Logon** settings open. Add is clicked in the window appeared. regedit file displays, which we copied under netlogon directory with the Active Directory IP address.



Parameter Description

No	Parameter	Value	Description
1	Script name	regedit.exe	Registry editing tool in which will run registry file that we set.

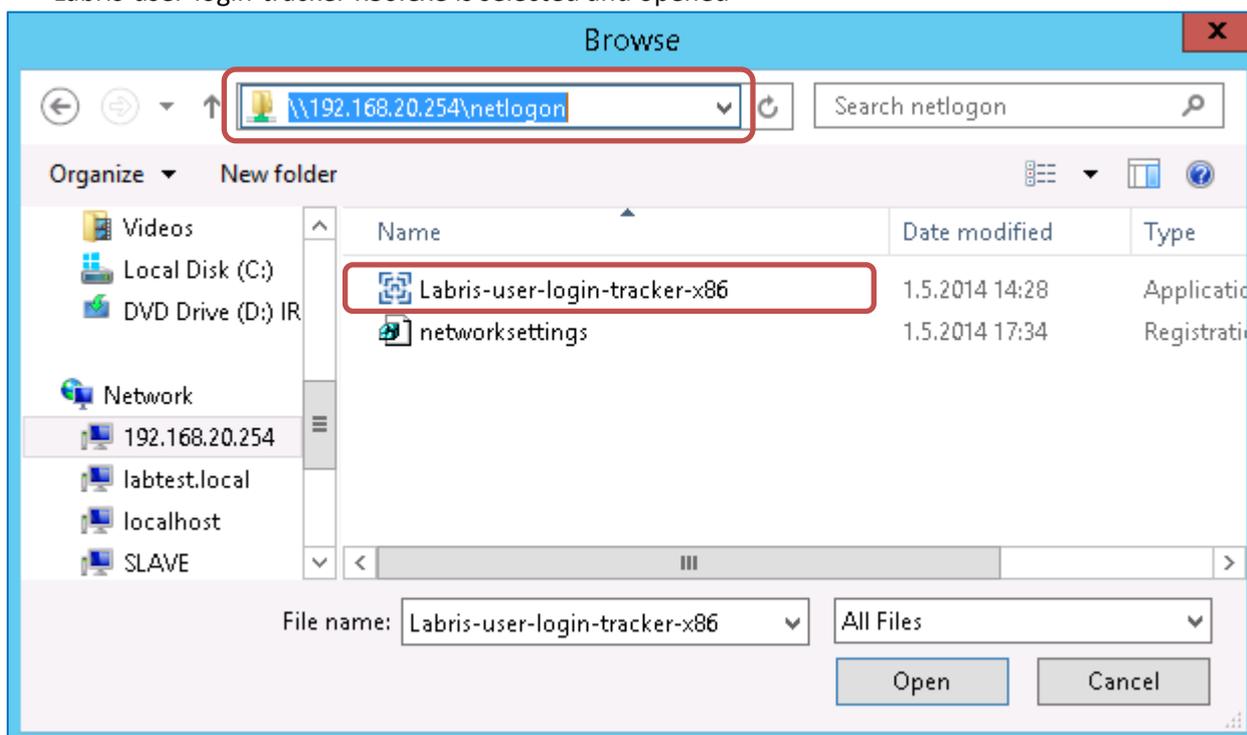
2	Script Parameters 1	/s	It will not be displayed while applying registry record in user computers.
3	Script Parameters 2	\\192.168.20.254\netlogon\networksettings.reg	The path of networksettings.reg file is displayed, which we copied to netlogon directory of active directory server.

Labris User logon tracker settings are made.

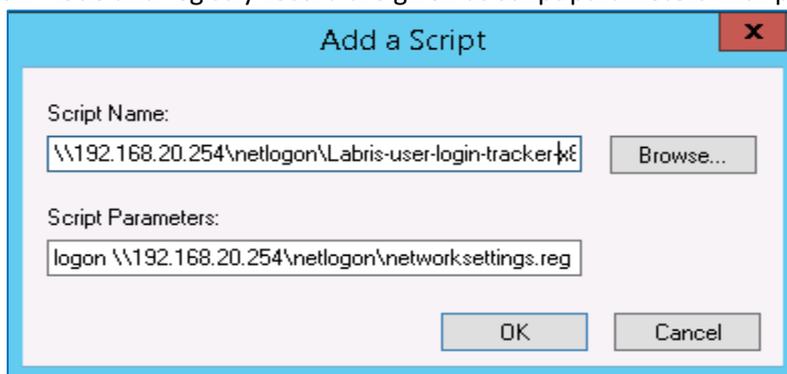
Add Again and Browse is clicked on Logon script settings

\\SunuculP\netlogon\ is written to the address line of window appeared and entered.

Labris-user-login-tracker-x86.exe is selected and opened



Operation mode and registry record are given as script parameters with path on the server.

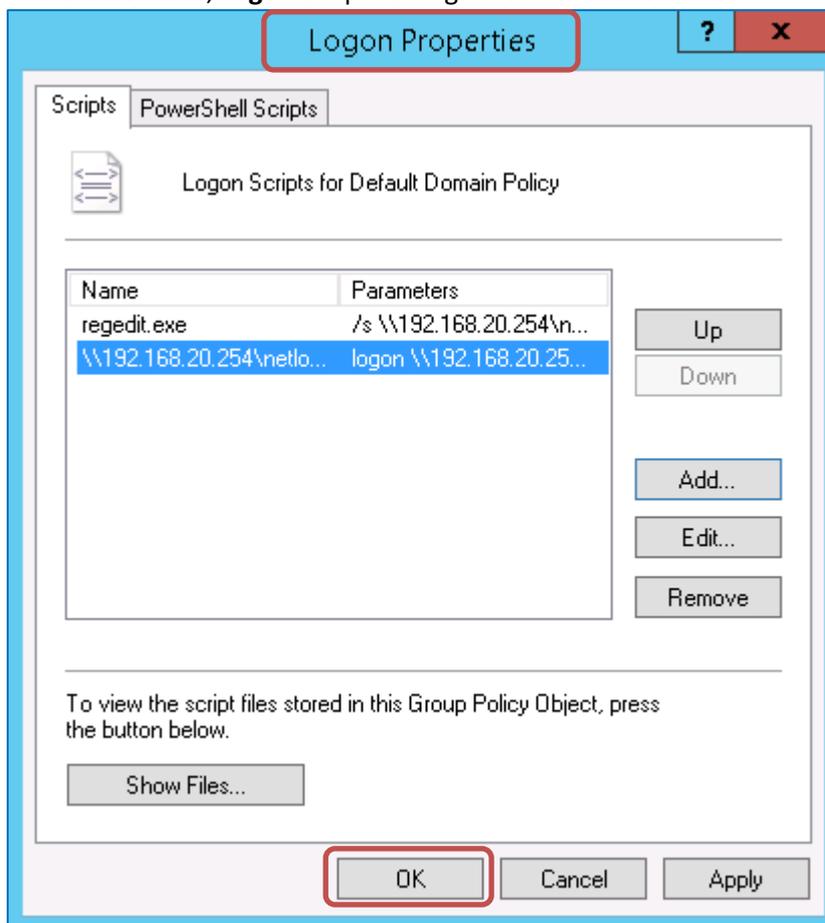


Parameter Description

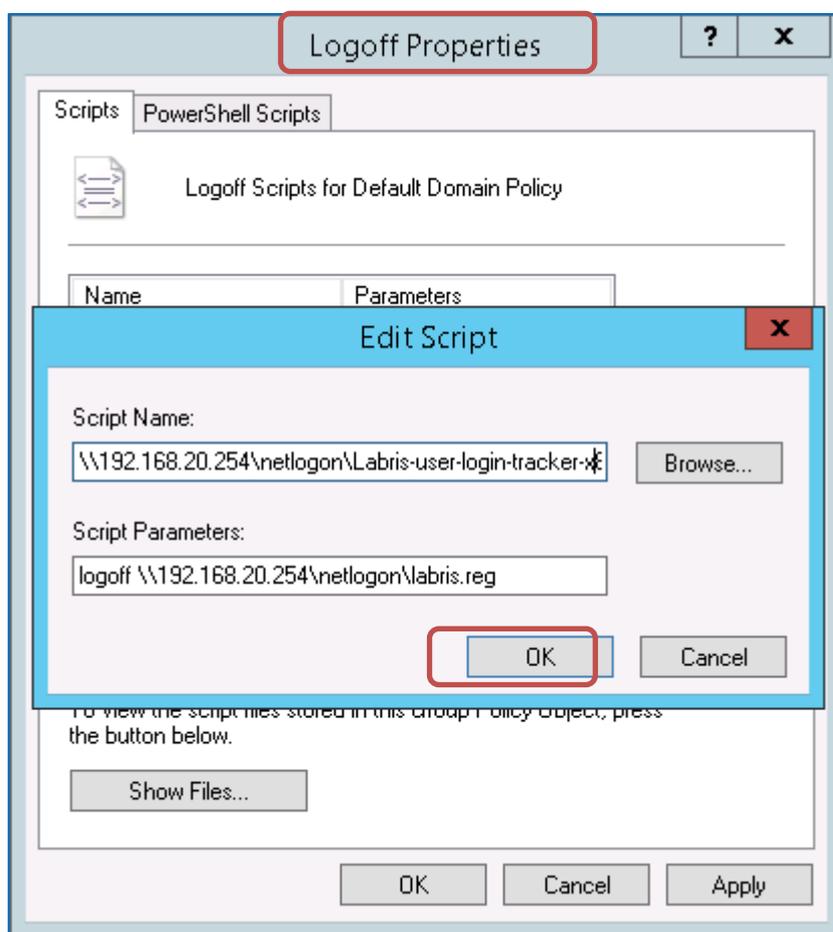
No	Parameter	Value	Description
1	Script name	\\192.168.20.254\netlogon\Labris-user-login-tracker-x86.exe	File path definition is made for Labris user logon tracker program.
2	Script Parameters 1	logon	When the user logs on, the operating mode of the logon tracker is set as logon.
3	Script Parameters 2	\\192.168.20.254\netlogon\networksettings.reg	In case of failure writing of the registry record to the user's computer, logon tracker tries to perform settings by reading the registry file

		here. It is written with a space after the value of Script parameters 1.
--	--	--

In the latter case, **Logon** Script settings should be as follows.



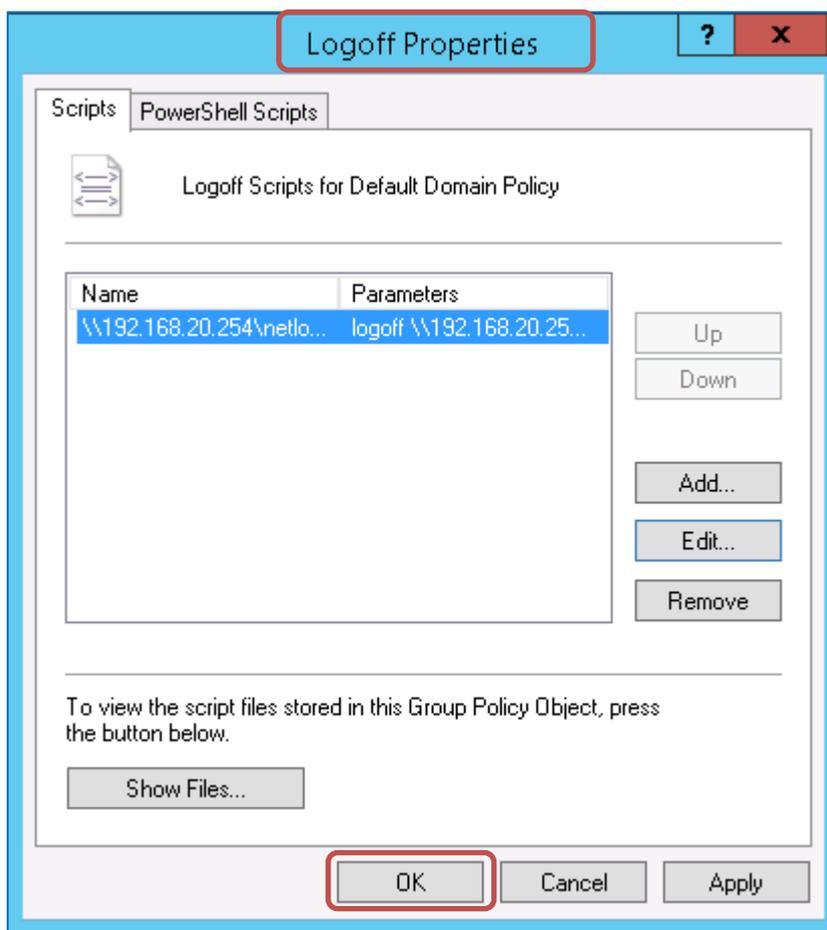
- b. **Logoff** settings are clicked and then Add is clicked.
As in the setting of logon, **Labris-user-login-tracker-x86.exe** is selected and script parameters are written.



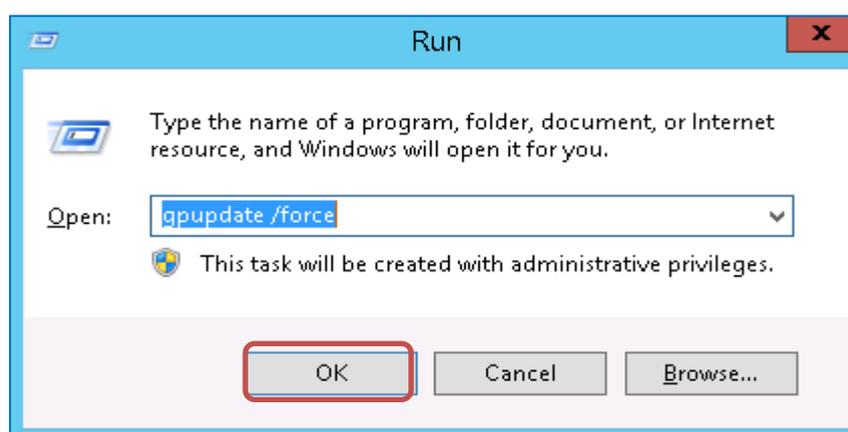
Parameter Description

No	Parameter	Value	Description
1	Script name	\\192.168.20.254\netlogon\Labris-user-login-tracker-x86.exe	File path definition is made for Labris user logon tracker program.
2	Script Parameters 1	logoff	When the user logs off, the operating mode of the logon tracker is set as logoff.
3	Script Parameters 2	\\192.168.20.254\netlogon\networksettings.reg	In case of failure writing of the registry record to the user's computer, logon tracker tries to perform settings by reading the registry file here. It is written with a space after the value of Script parameters 1.

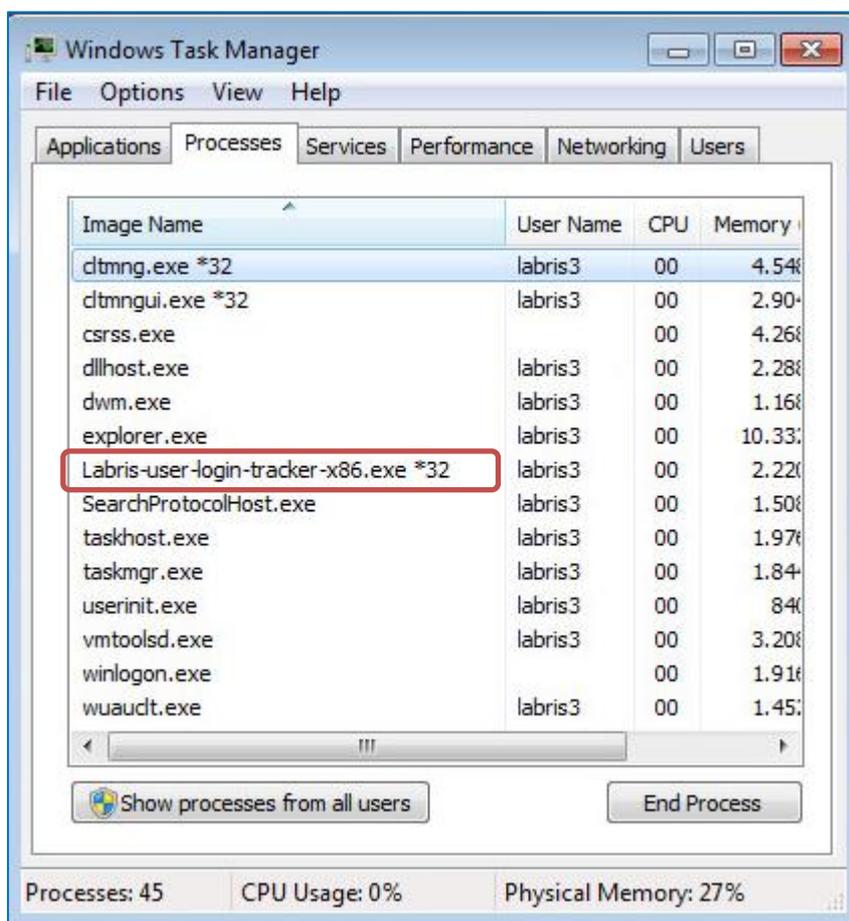
In the latter case, **Logoff** Script settings should be as follows.



- c. Group Policy settings are applied.
For the changes to be valid, Group Policy settings will be updated for all users.
Run opens by using "**Windows + R**" keys.
The settings are applied by giving **gpupdate / force** command to this area.



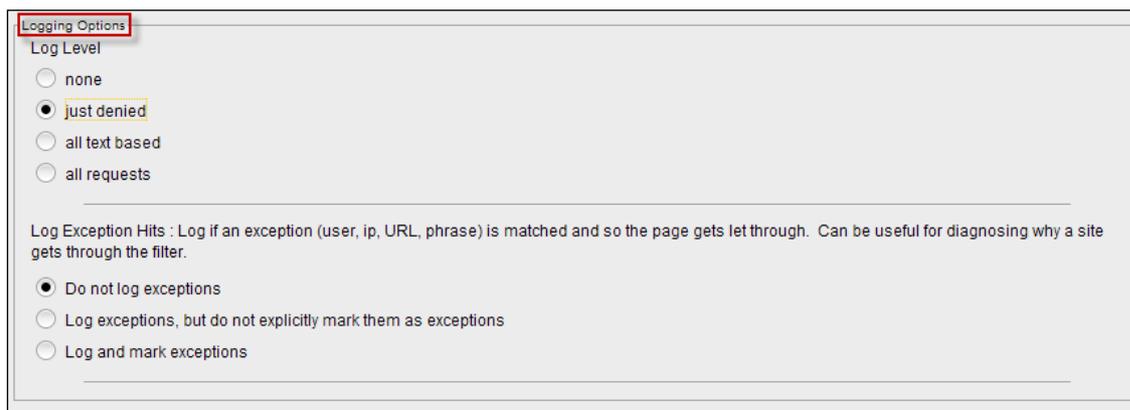
- d. Control of the settings is made.
The user computer is log off and logon again after settings successfully applied. It can be seen that **Labris-user-logon-tacker-x86.exe** is running in task manager (ctrl + shift + esc) application.



To provide control over Labris;
"**labrisdb_user_manager.py -getall-ip**" command is written on the command line and it is seen that the IP addresses of users came.

94. Logging Options

Log Level and Log Exception Hits tabs are displayed.



Network Settings

Network settings consists of four fields. They are Filter IP , Filter Port, Proxy IP and Proxy Port. Give appropriate Filter IP, Filter Port, Proxy IP and Proxy Port.

Network Settings

Filter IP : The IP that Labris Web Filter listens on. If left blank filter will listen on all IPs. That would include all NICs, loopback, modem, etc. Normally you would have your firewall protecting this, but if you want you can limit it to only 1 IP. Yes only one.

Filter Port : The port that filter listens to.

Proxy IP : The ip of the proxy. (default is the loopback - i.e. this server)

Proxy Port : The port filter connects to proxy on

Weighted Phrase Settings

In the Weighted Phrases Settings we can choose Weighted Phrase Mode.

If it is on then the phrases found that made up the total which exceeds the naughtiness limit will be logged, if the level is high enough reported.

WeightedPhrase Settings

If enabled then the phrases found that made up the total which exceeds the naughtiness limit will be logged and, if the reporting level is high enough, reported.

on
 off

Weighted Phrase Mode

off = do not use the weighted phrase feature
 on, normal = normal weighted phrase operation.
 on, singular = each weighted phrase found only counts once on a page

Cache Settings

We can view and change Cache Settings.

Cache Settings

Positive result caching for text URLs. Caches good pages so they don't need to be scanned again (0 = off (recommended for ISPs with users with dissimilar browsing), 1000 = recommended for most users, 5000 = suggested max upper limit)

Age before they are stale and should be ignored in seconds. (0 = never, 900 = recommended = 15 mins)

Fork Pool Settings

We can view and change Fork Pool Settings.

Fork Pool Settings

Sets the maximum number of processes to spawn to handle the incoming connections. Max value usually 250 depending on OS. On large sites you might want to try 180.

Sets the minimum number of processes to spawn to handle the incoming connections. On large sites you might want to try 32.

Sets the minimum number of processes to be kept ready to handle connections. On large sites you might want to try 8.

Sets the minimum number of processes to spawn when it runs out. On large sites you might want to try.

Sets the maximum number of processes to have doing nothing. When this many are spare it will cull some of them. On large sites you might want to try 64.

Sets the maximum age of a child process before it croaks it. This is the number of connections they handle before exiting. On large sites you might want to try 10000.

Click on **Save tab** to save the changes.

Filter Groups **Banned Filters** **Exception Filters** **Configuration** **Log Monitoring**

Reporting Options

Web Access Denied Reporting

log, but do not block - Stealth mode

just say 'Access Denied'

report why but not what denied phrase

report fully

use HTML template file (accessdenied addressigned) - recommended

Customize

Authentication

NTLM Authentication

Basic Authentication

IP Authentication

Logging Options

Log Level

none

just denied

all text based

all requests

Log Exception Hits : Log if an exception (user, ip, URL, phrase) is matched and so the page gets let through. Can be useful for diagnosing why a site

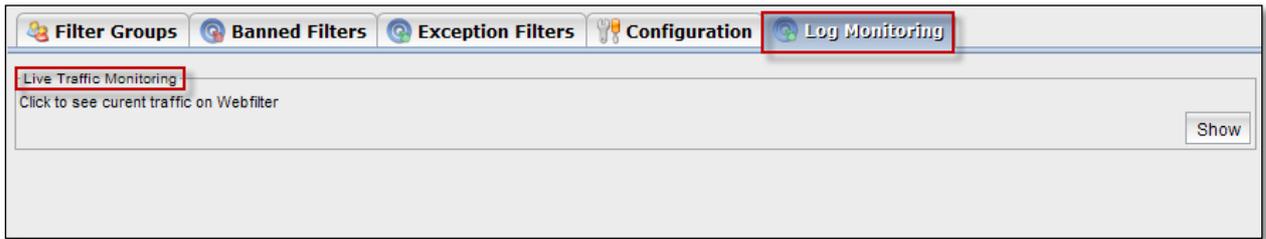
URL/Content Filter Service Status: Running

ected to is: 78.188.50.48

Labris Teknoloji

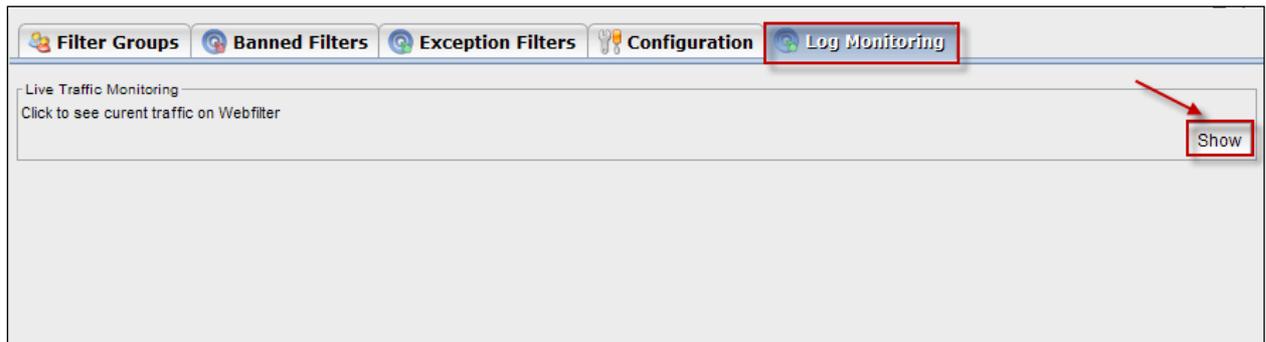
95. Log Monitoring

When we click on **Log Monitoring tab**, Live traffic Monitoring tab appears.



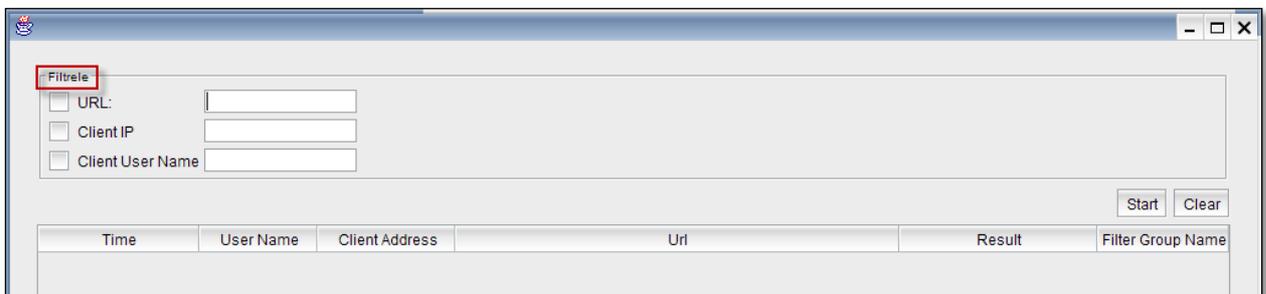
96. Show

Click on **Show tab** to see current traffic on Webfilter.

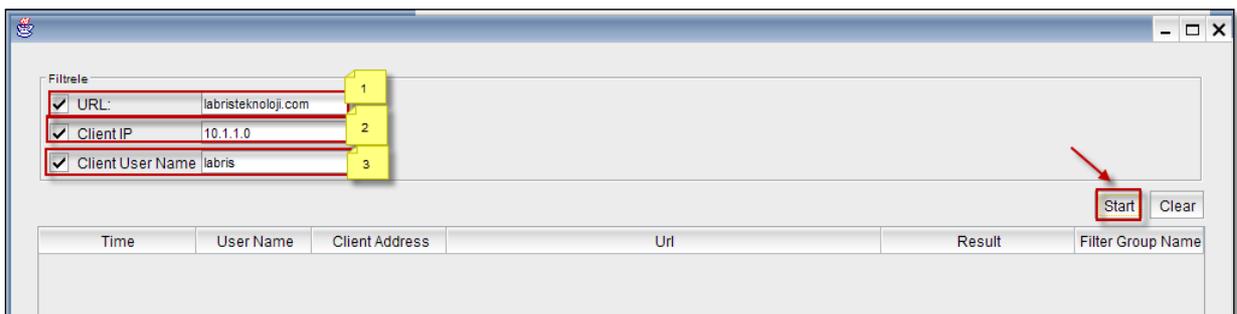


Filter

Below screen appears.



Start

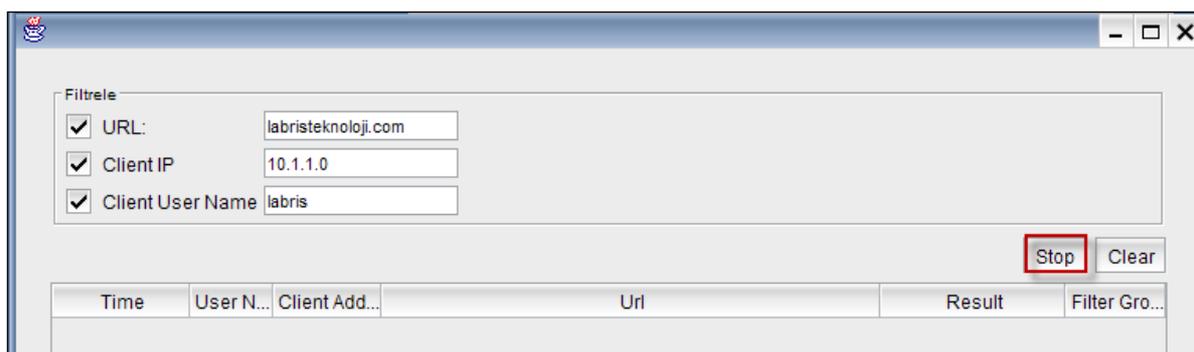


These are the inputs to start

1	URL	Type URL
2	Client IP	Give the client IP Address
3	Client User Name	Type client User Name.

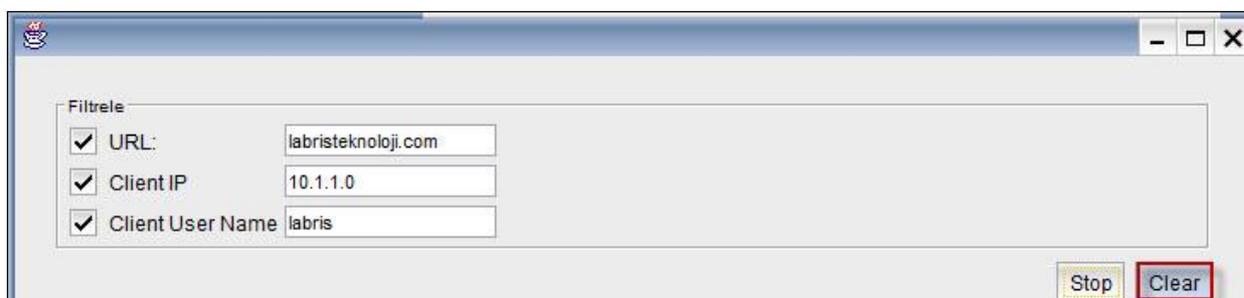
Click on **Start** tab.

In the below screen we can notice service has been started.

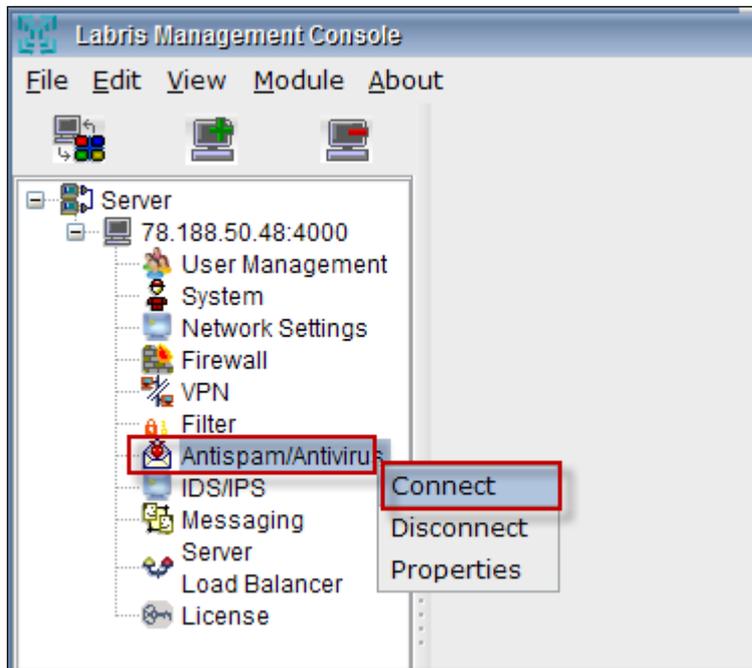


Clear

When we select the log and click on clear button the logs can be cleared from the list. If there are too many rows in the table we can select each one of them and Click on the **Clear** button, to delete a log.

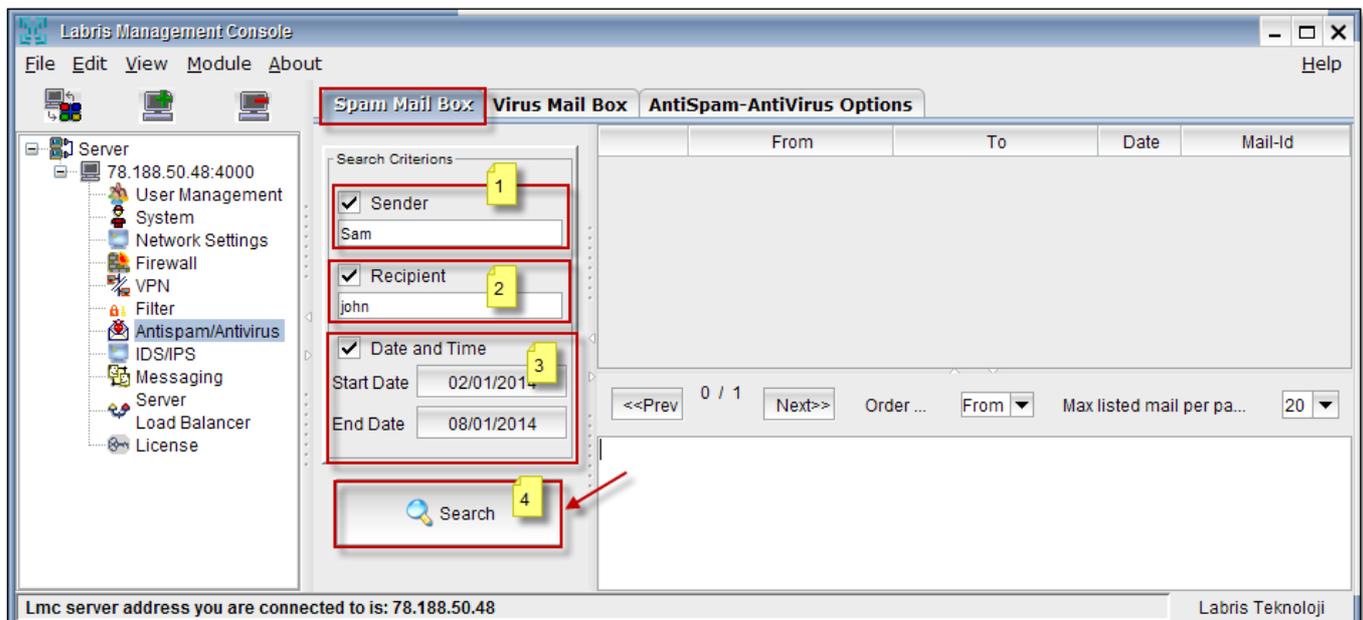


ANTISPAM/ANTIVIRUS



97. Spam Mail Box

Search Criterions

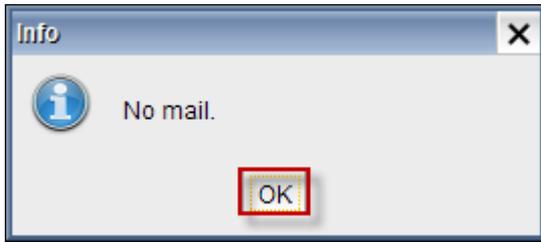


These are the inputs for Spam Mail Box.

1	Sender	Enable Sender and type Sender name
2	Recipient	Enable Recipient and type Recipient name

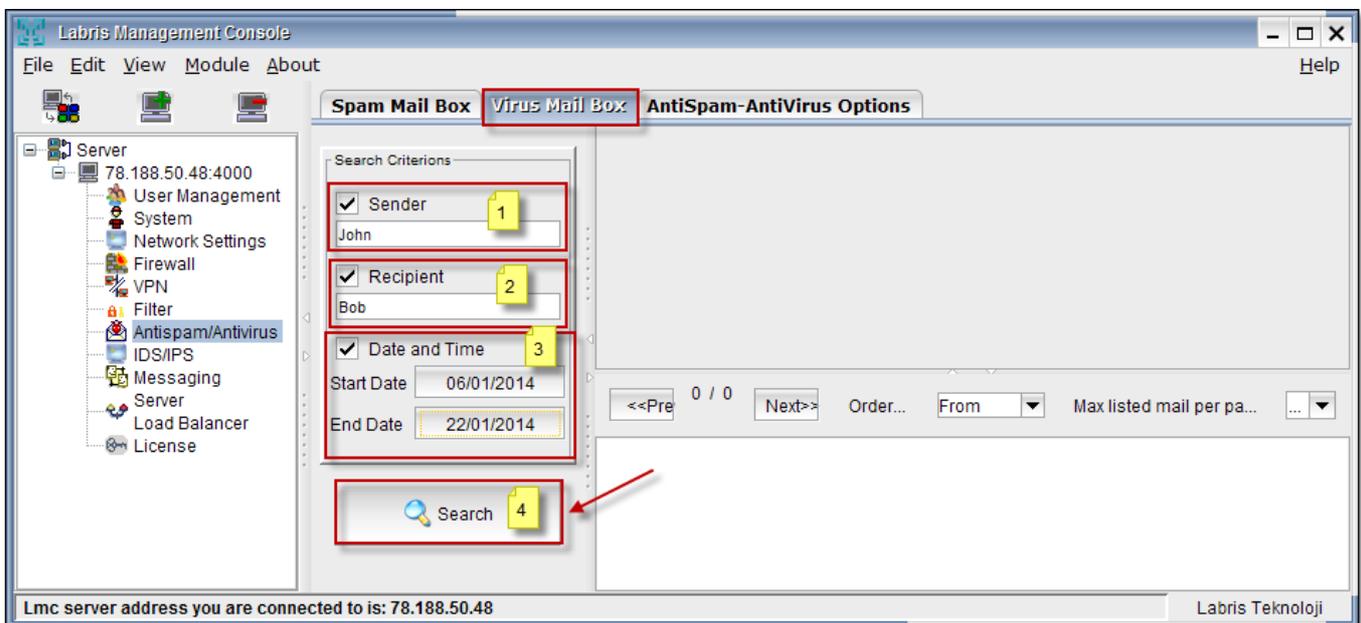
3	Date and Time	Enable Date and Time, choose Start Date and End Date
4	Search	Click on Search tab to find out Mail.

Info tab appears stating No Mail, Since No mail has been sent. Click **Ok**



Virus Mail Box

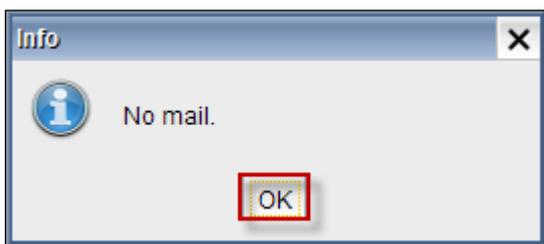
Search Criteria



These are the inputs for Virus Mail Box

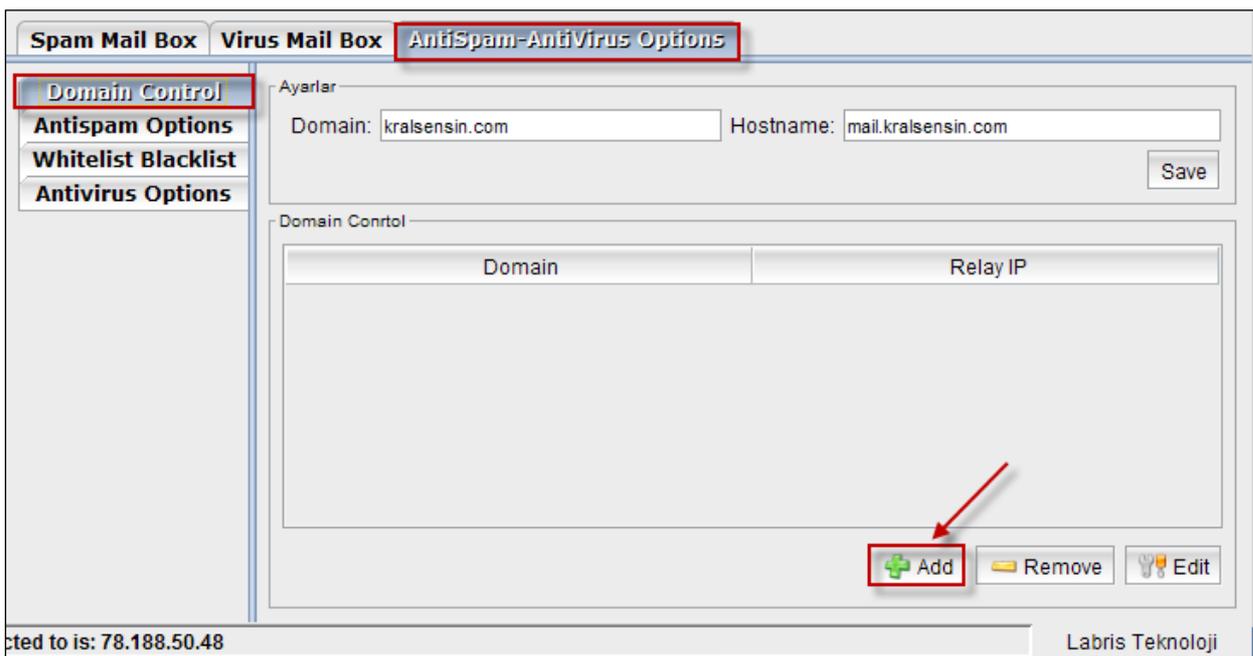
1	Sender	Enable Sender and type Sender name
2	Recipient	Enable Recipient and type Recipient name
3	Date and Time	Enable Date and Time, choose Start Date and End Date
4	Search	Click on Search tab to find out Mail.

Info tab appears stating No Mail, Since No mail has been sent. Click **Ok**



98. Antispam-Antivirus Options

Domain Control



Domain Control tab appears with the fields **Domain** and **Relay IP**

Add New Domain tab appears.

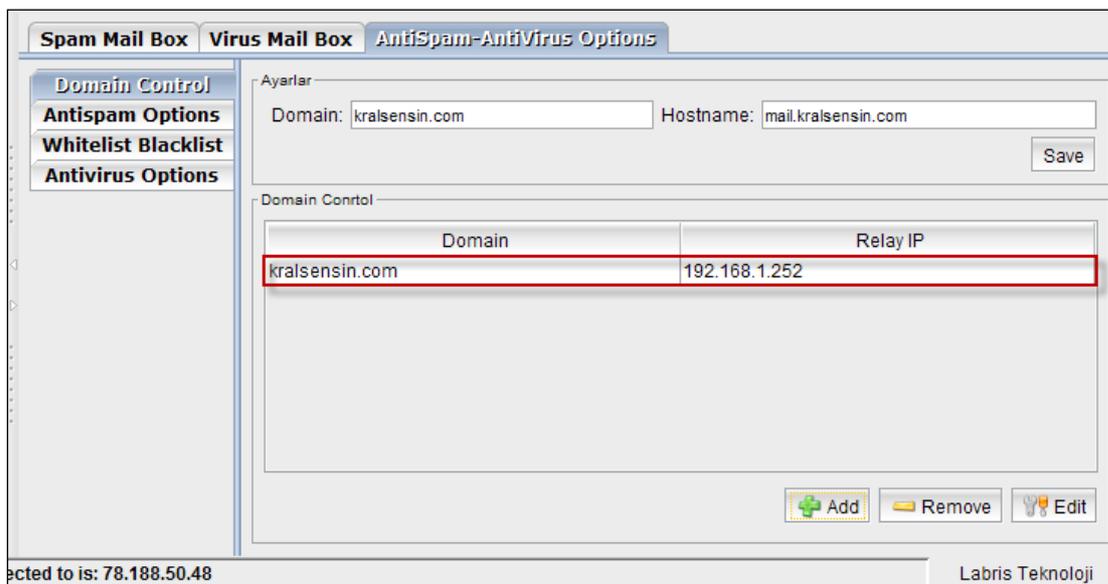
Type **Domain name** and Give **Relay ip address**. Click **Ok**



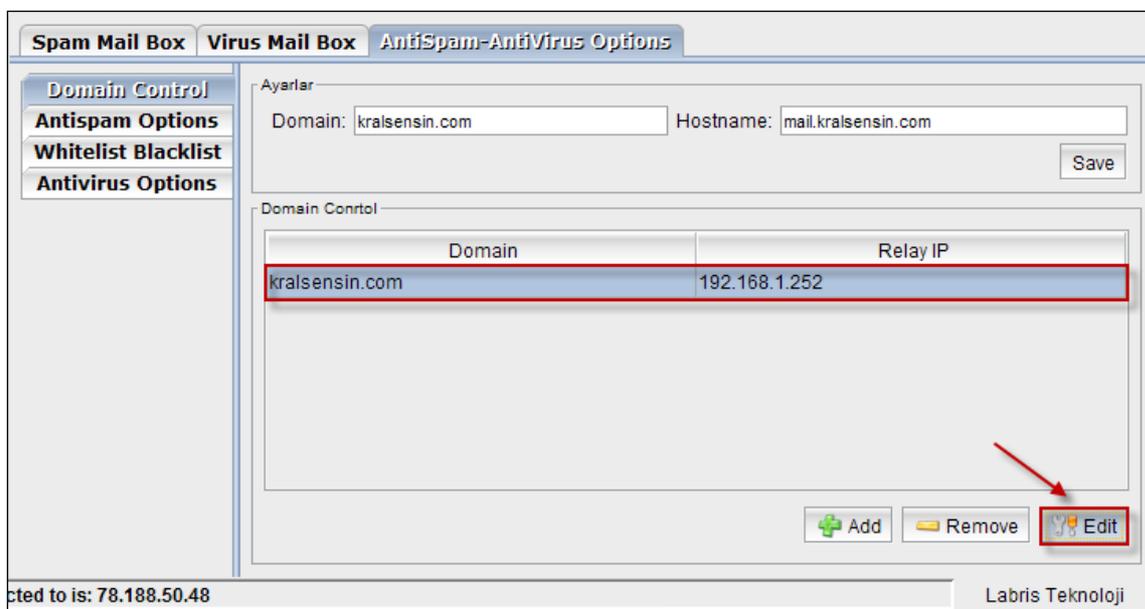
It takes some time to Apply changes.



In the below screen, we can notice New Domain added in the Domain Control tab.



Select the Domain and Click on **Edit** tab.



Edit tab appears.

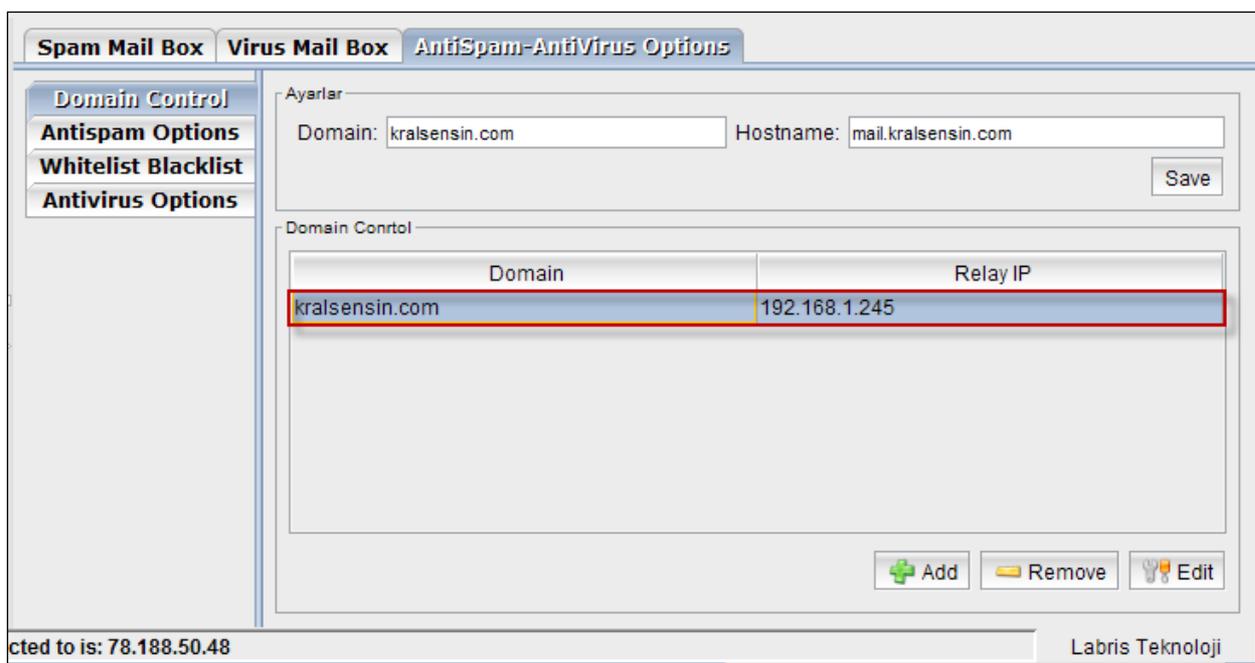
We can edit Domain name and Relay IP address. Click **Ok**.



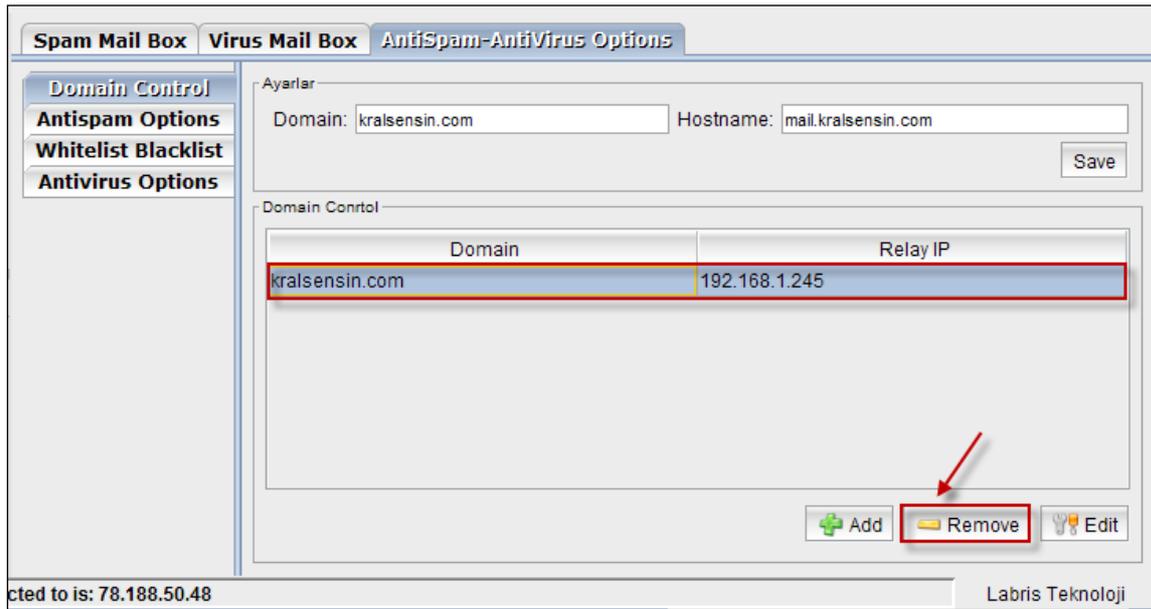
It takes some time to apply changes.



In the below screen, we can notice changes made in the new domain.



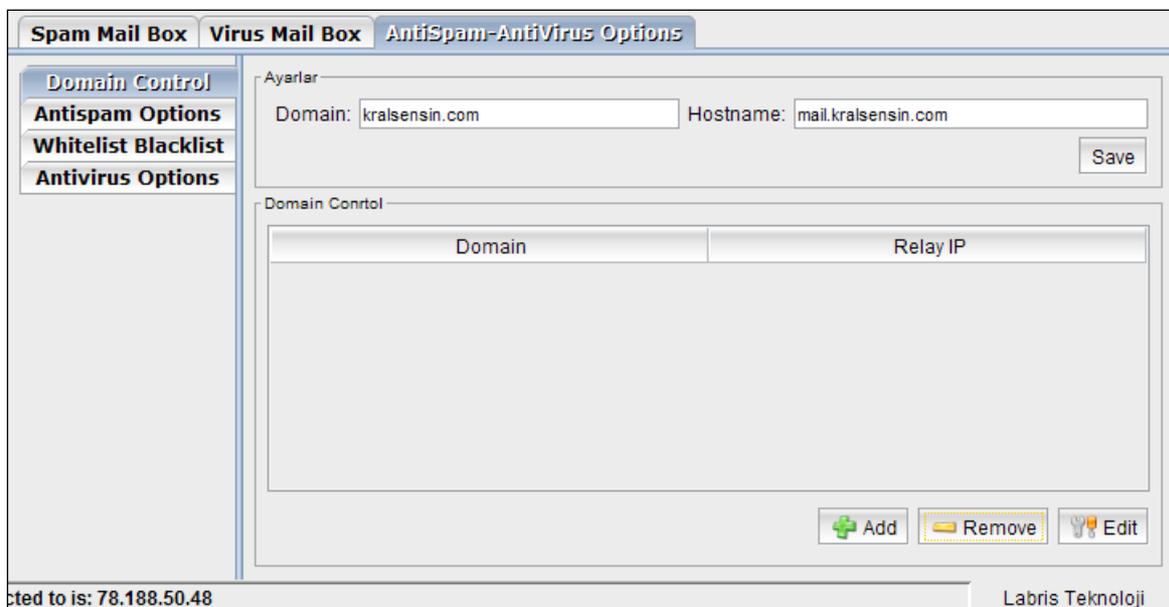
Select the Domain and click on **Remove tab**.



It takes some time to apply changes.



In the below screen, we can notice **Domain** deleted in the Domain Control tab.



Settings

Add a Global policy.

No.	Source	Destination	Service	Action	Schedule	QoS/Band...	Applications	Security P...	Options
0	 Any	 EXCHANGE	 	 Accept	 Any	 Any	 Any	 Any	

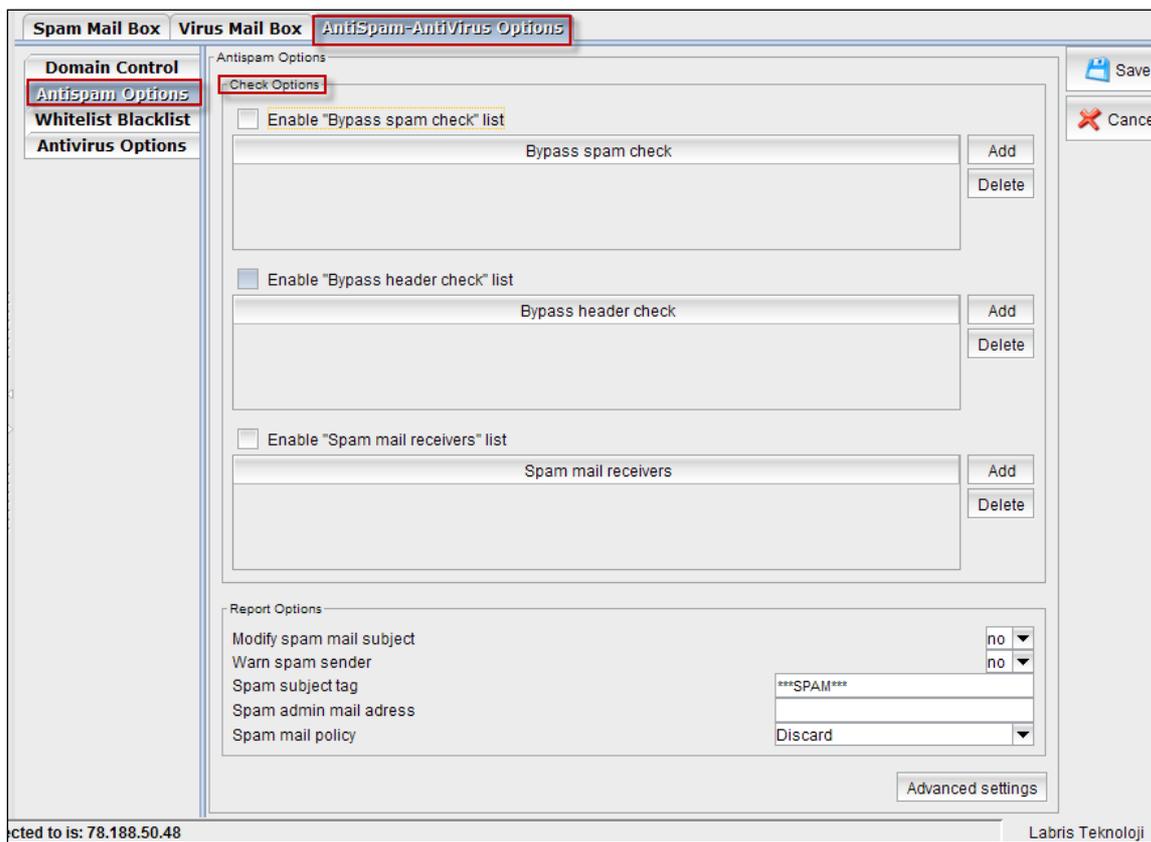
99. Antispam Options

Antispam consists of three fields.

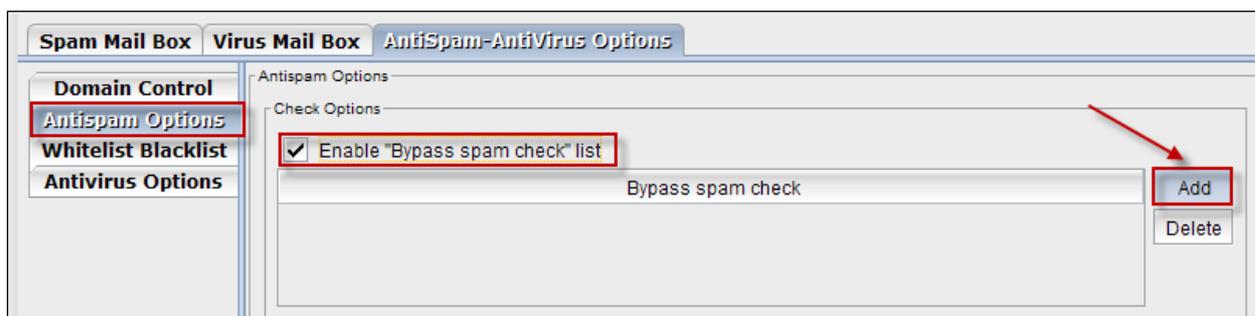
They are Bypass spam check, By pass header check, spam mail receivers.

Check Options

It helps us to enable Bypass spam check, By pass header check, spam mail receivers and perform actions like Add, Delete on check options.

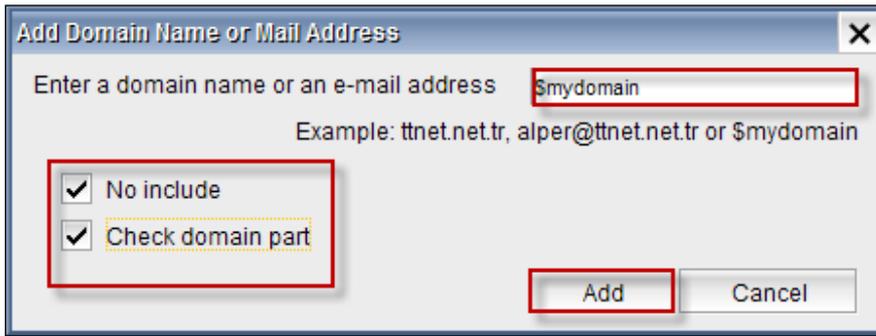


Enable Bypass spam check list and click on **Add** tab.

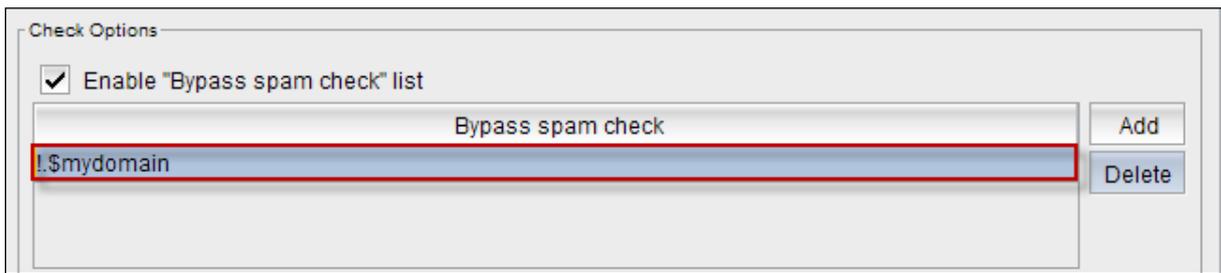


Add Domain Name or Mail Address tab appears.

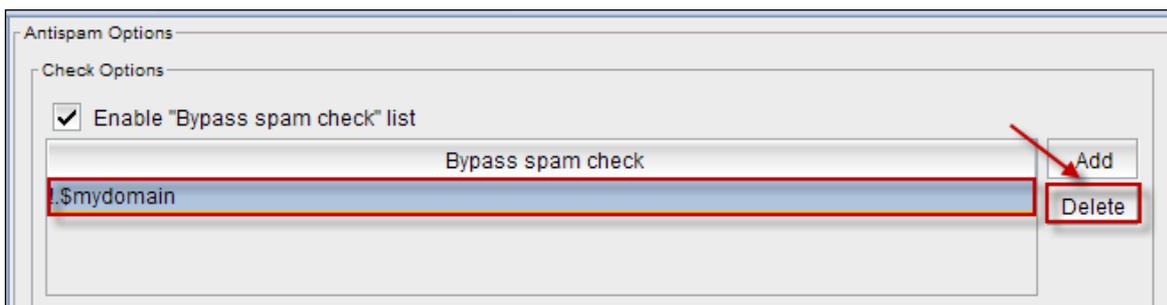
Type Domain name or e-mail address. Enable No include, check domain part and click on **Add** tab.



In the below screen, we can notice domain name added in the spam check list.



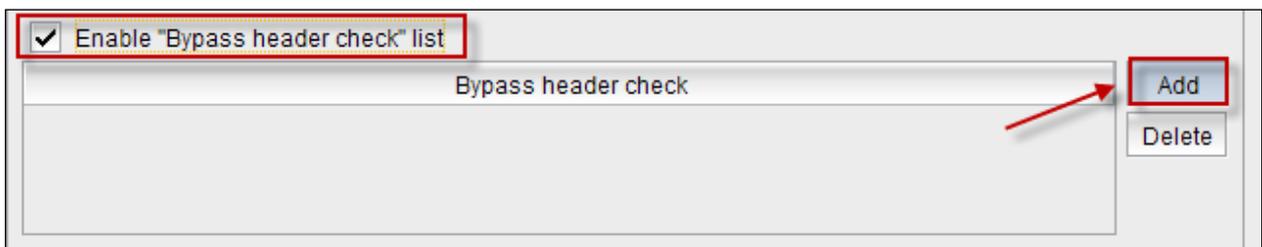
Select domain and click on **Delete** tab.



Warning tab appears stating **Are you sure?** Click on **Yes**



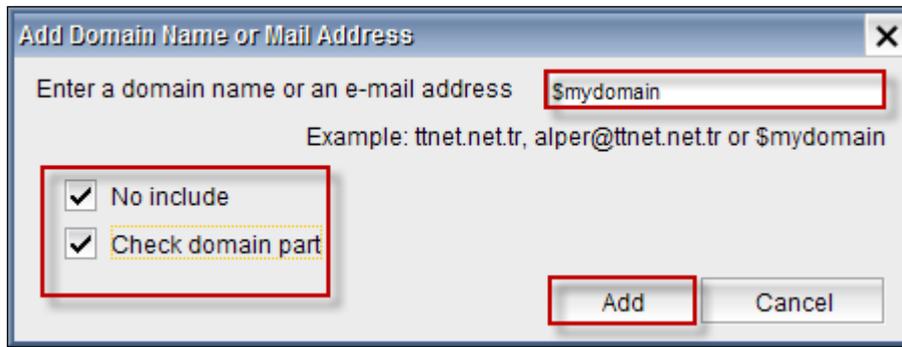
Enable Bypass header check list and click on **Add** tab.



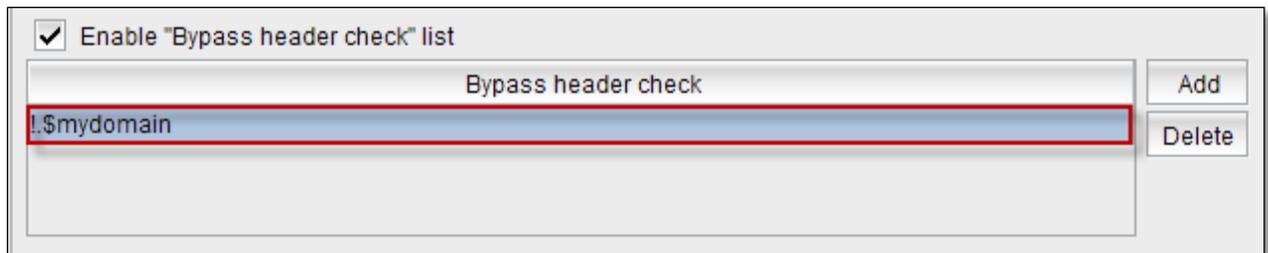
Add Domain Name or Mail Address tab appears.

Type Domain name or e-mail address. Enable No include, check domain part and click on **Add**

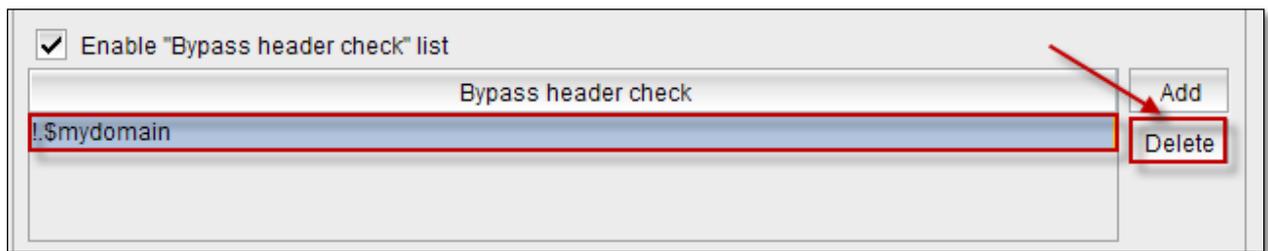
tab.



In the below screen, we can notice domain name added in the header check list.



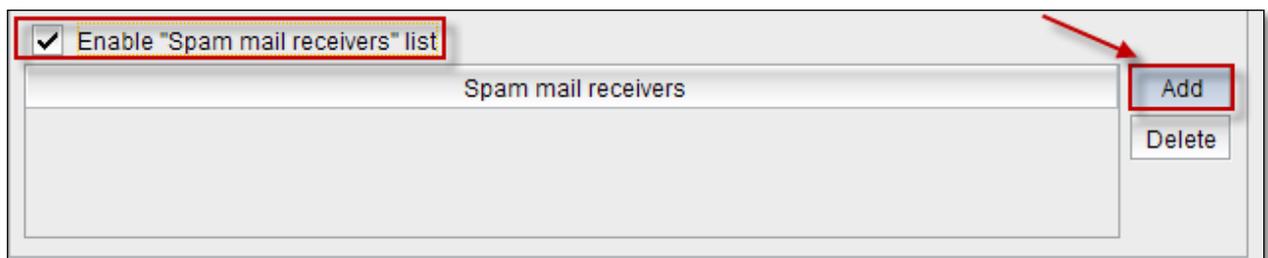
Select domain and click on **Delete** tab.



Warning tab appears stating **Are you sure?** Click on **Yes**

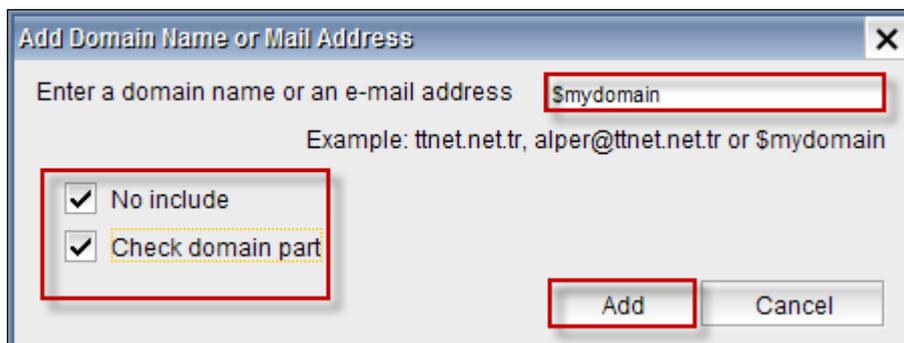


Enable Spam mail receivers list and click on **Add** tab.

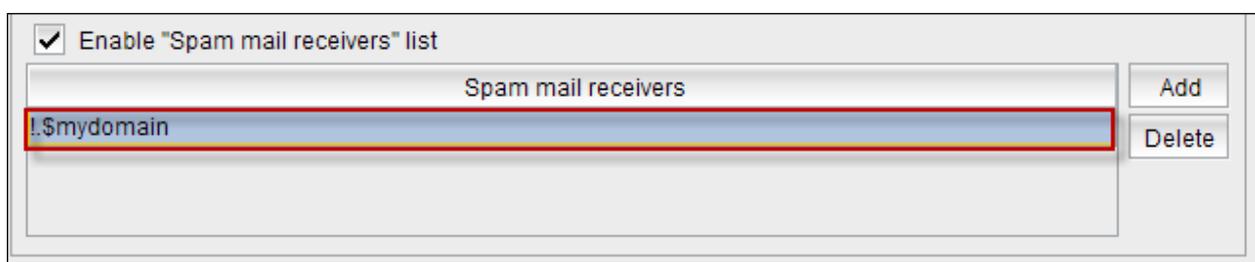


Add Domain Name or Mail Address tab appears.

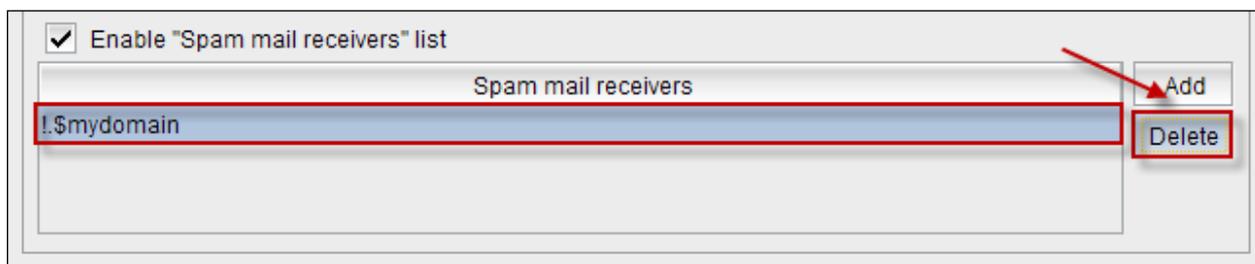
Type Domain name or e-mail address. Enable No include, check domain part and click on **Add** tab.



In the below screen, we can notice domain name added in the Spam mail receivers list.



Select domain and click on **Delete** tab.



Warning tab appears stating **Are you sure?** Click on **Yes**



Report Options

These are the inputs for the Report options.

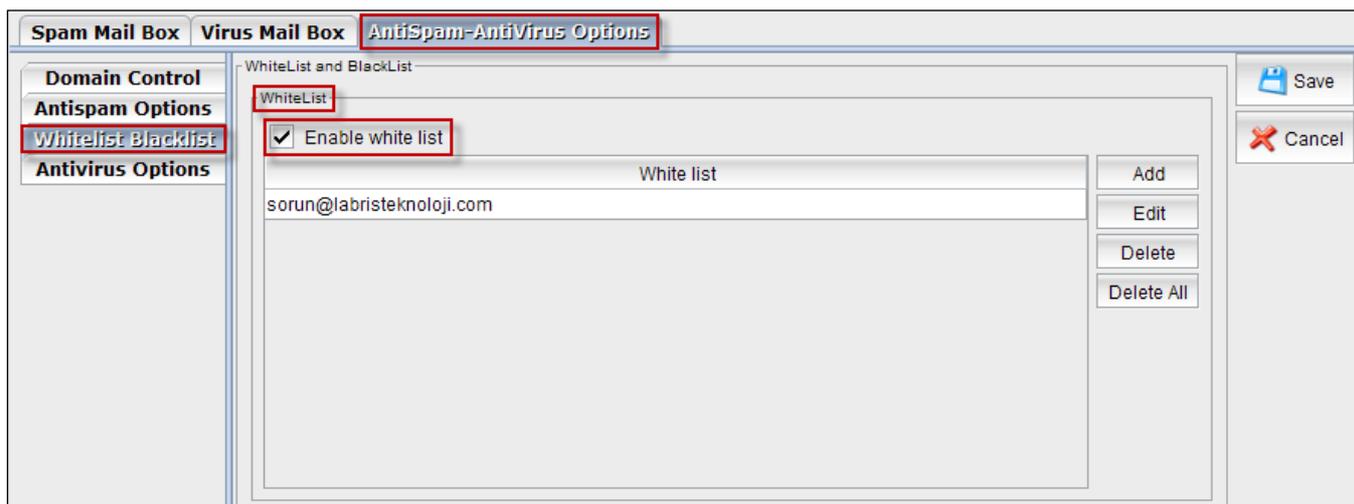
1	Modify spam mail subject	To modify spam mail subject select yes or else no
2	Warn spam sender	To Warn spam sender select yes or else no
3	Spam subject tag	Type tag of Spam subject.
4	Spam admin mail address	Type spam admin mail address
5	Spam mail policy	Select policy from the drop down list.

Click on **Save** tab to save changes made to the AntiSpam-AntiVirus.

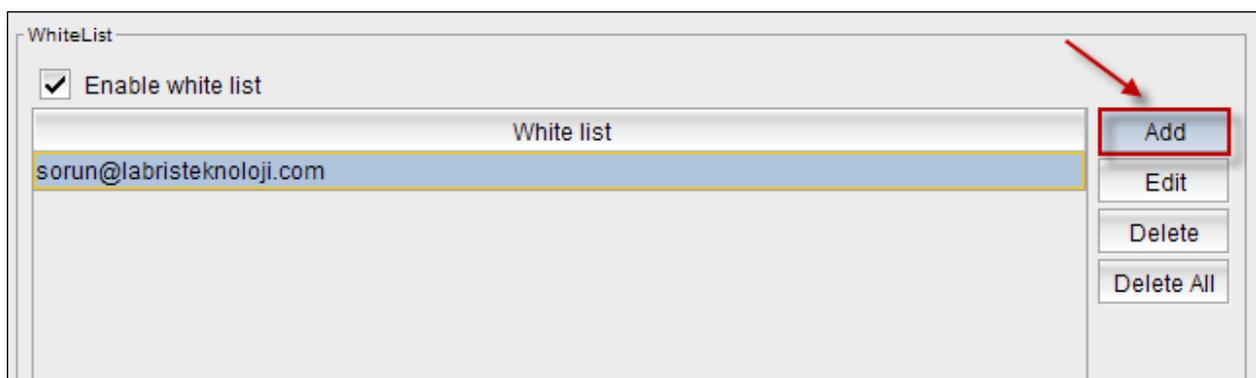
100. Whitelist Blacklist

Enable White List

Enable white list to perform action like Add, Edit, Delete, Delete All Whitelist.

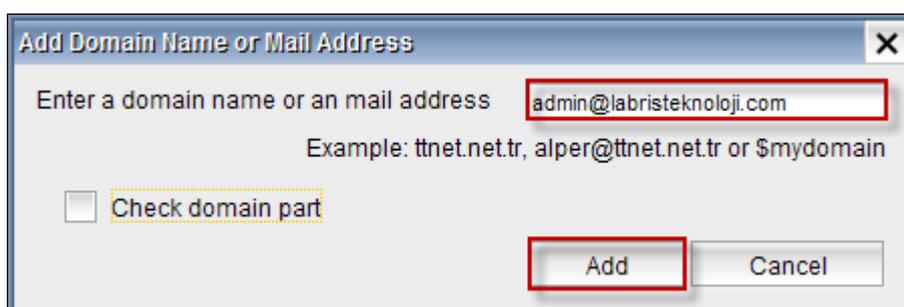


Click on **Add** tab.

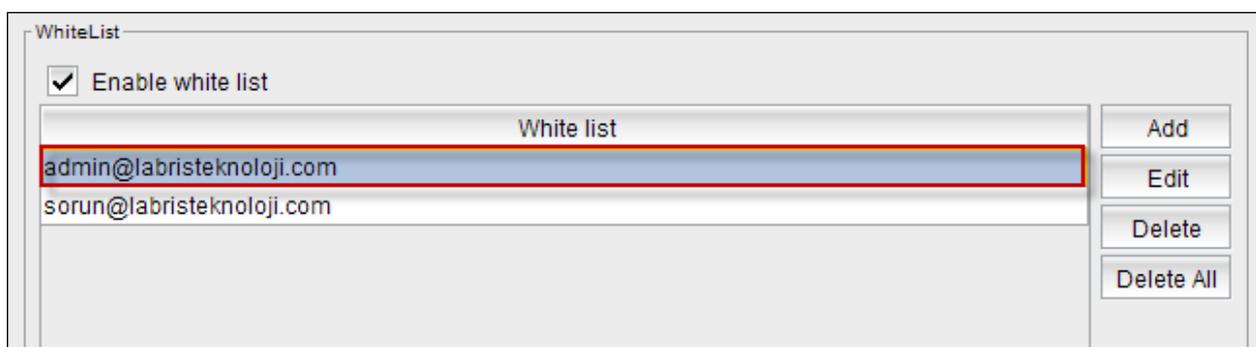


Add Domain Name or Mail Address tab appears.

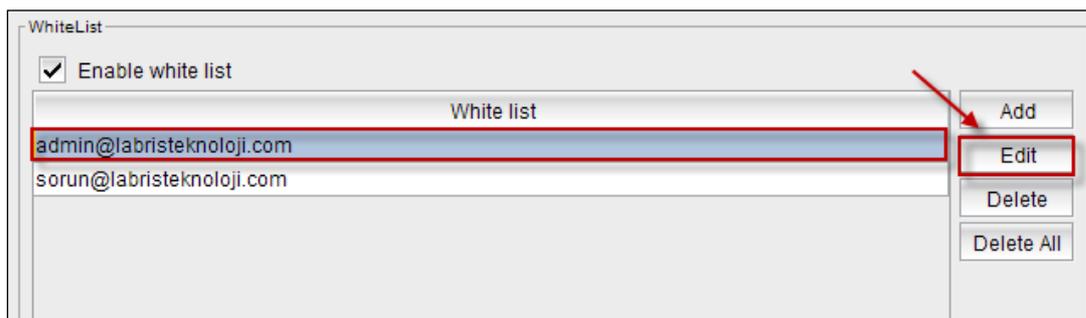
Type Domain name or e-mail address, we can enable Check Domain part if necessary and click on **Add** tab.



In the below screen, we can notice mail address added in the White list.

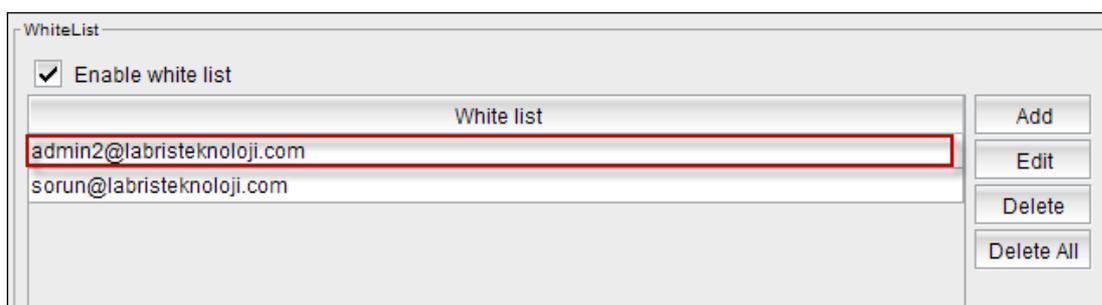


Select mail address and click on **Edit** tab.

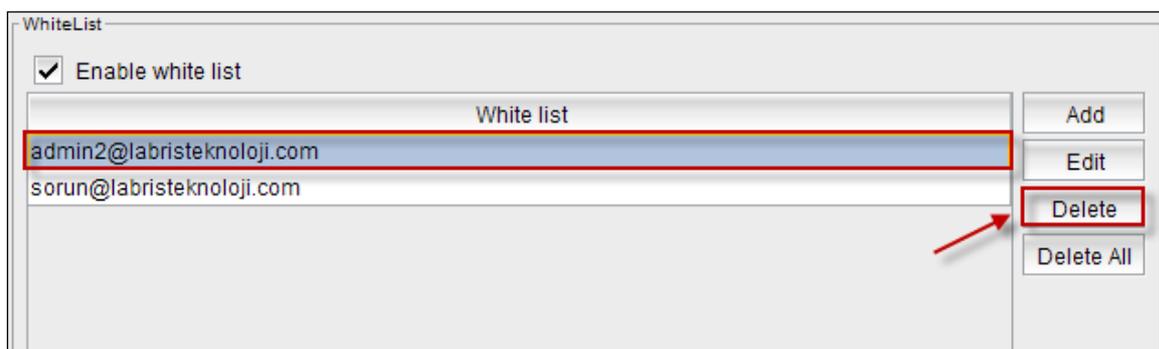


Edit List tab appears, we can edit URL and click on **Save** tab.

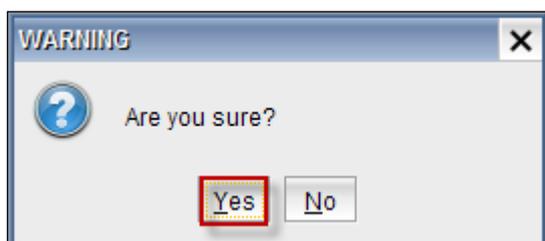
In the below screen, we can notice changes made to the mail address.



Select mail address and click on **Delete** tab.

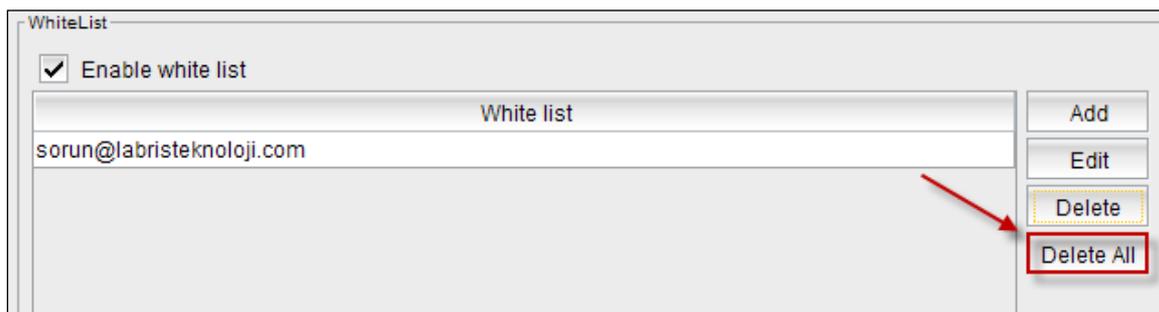


Warning tab appears stating **Are you sure?** Click on **Yes**

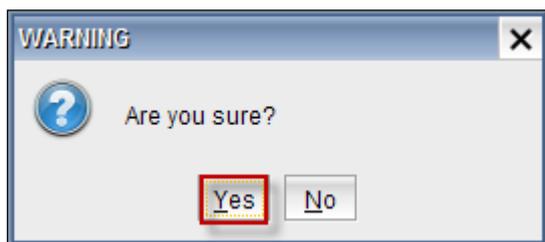


Below screen we can notice selected mail deleted from the white list.

Click on **Delete All** tab to delete all the mail addresses in White list.

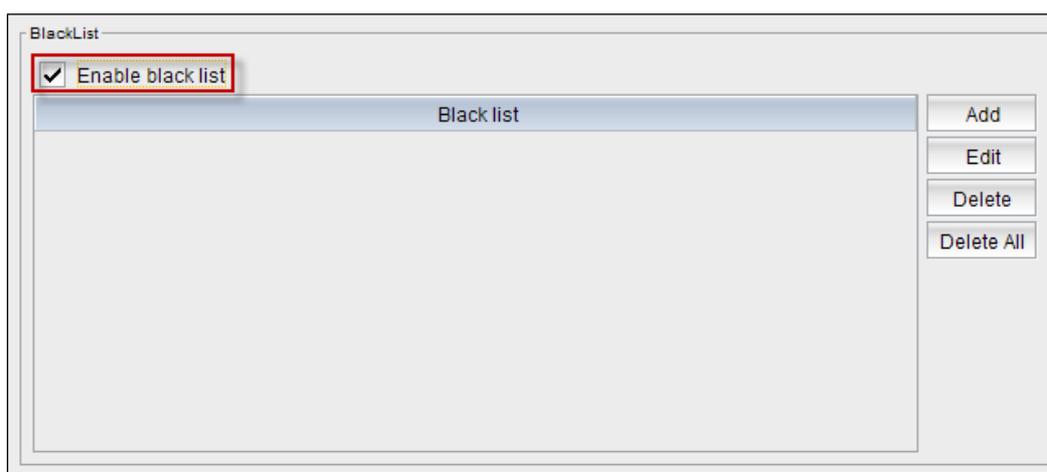


Warning tab appears stating **Are you sure?** Click on **Yes**

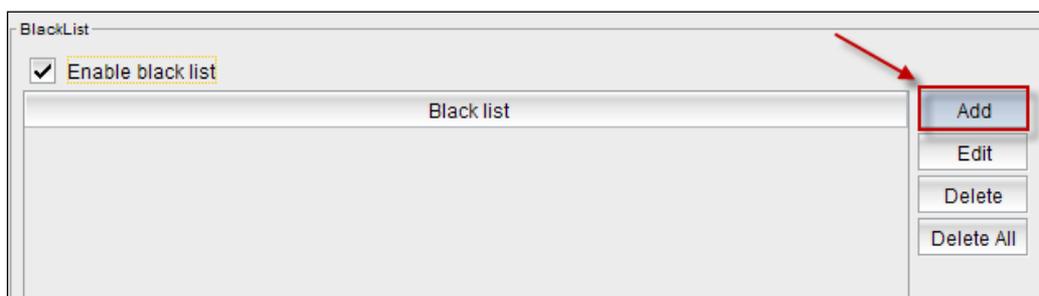


Enable black List

Enable Black List to perform actions like Add, Delete, Delete All in Black list.

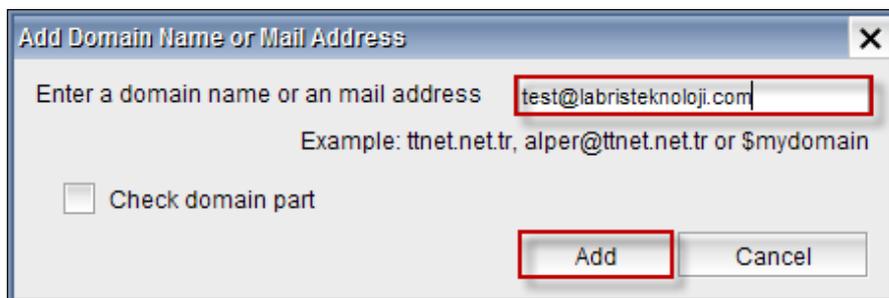


Click on **Add tab**.

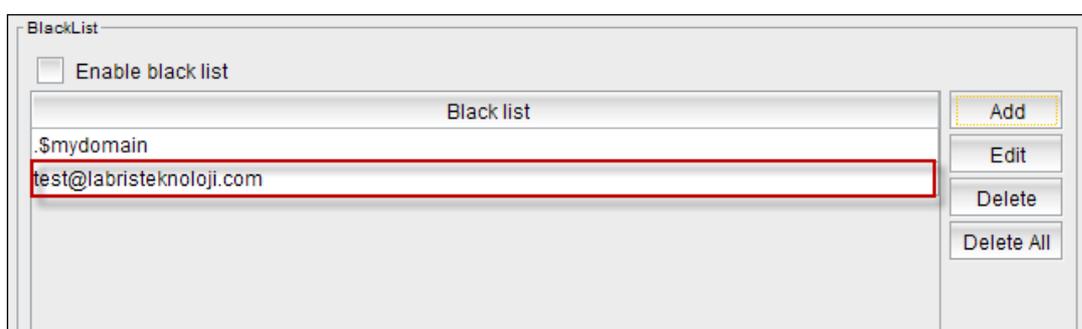


Add Domain Name or Mail Address tab appears.

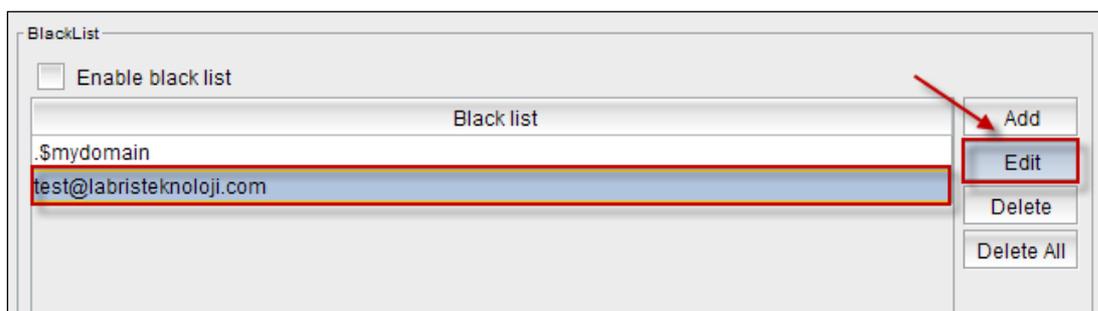
Type Domain name or e-mail address, We can enable Check Domain part if necessary and click on **Add** tab.



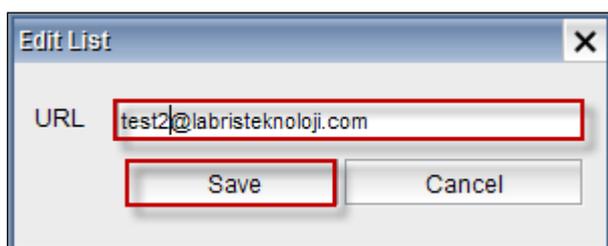
In the below screen, we can notice mail address added to the Black list.



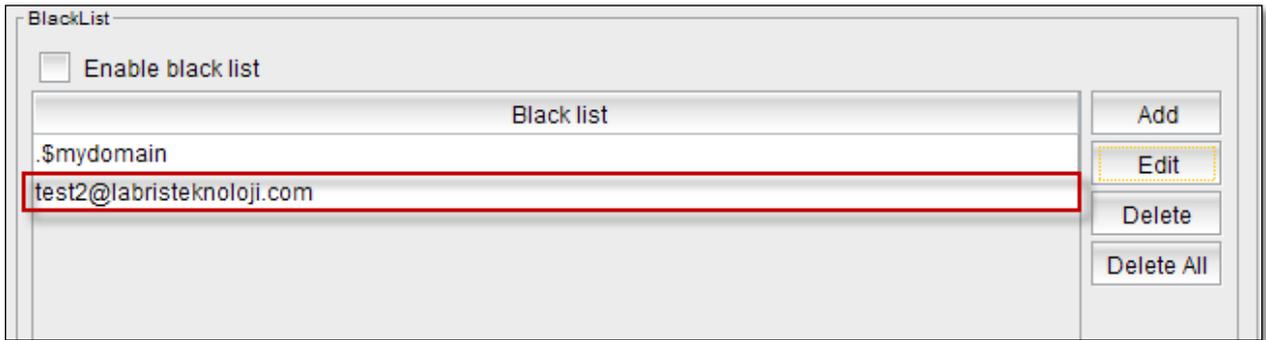
Select mail address and click on **Edit** tab.



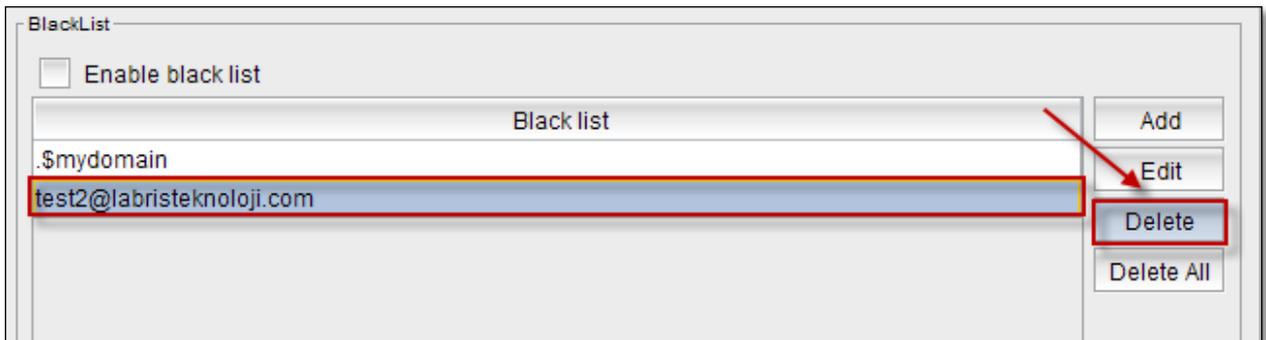
Edit List tab appears, we can edit URL and click on **Save** tab.



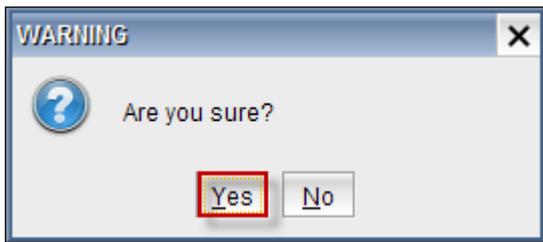
In the below screen, we can notice changes made to the mail address.



Select mail address and click on **Delete** tab.

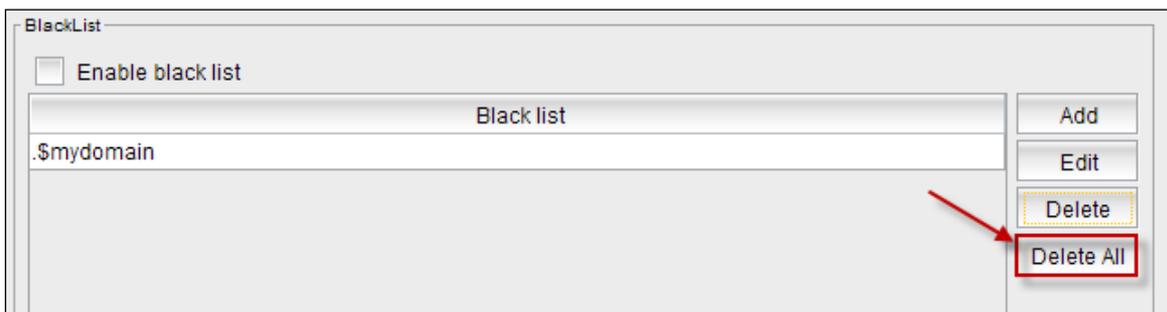


Warning tab appears stating **Are you sure?** Click on **Yes**

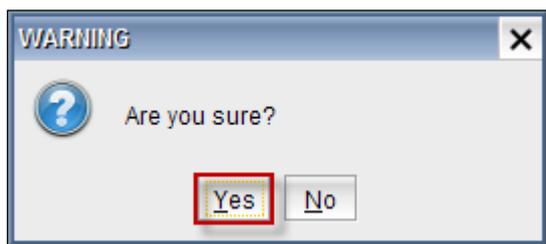


In the below screen we can notice selected mail deleted from the Black list.

Click on **Delete All** tab to delete all the mail addresses in White list.



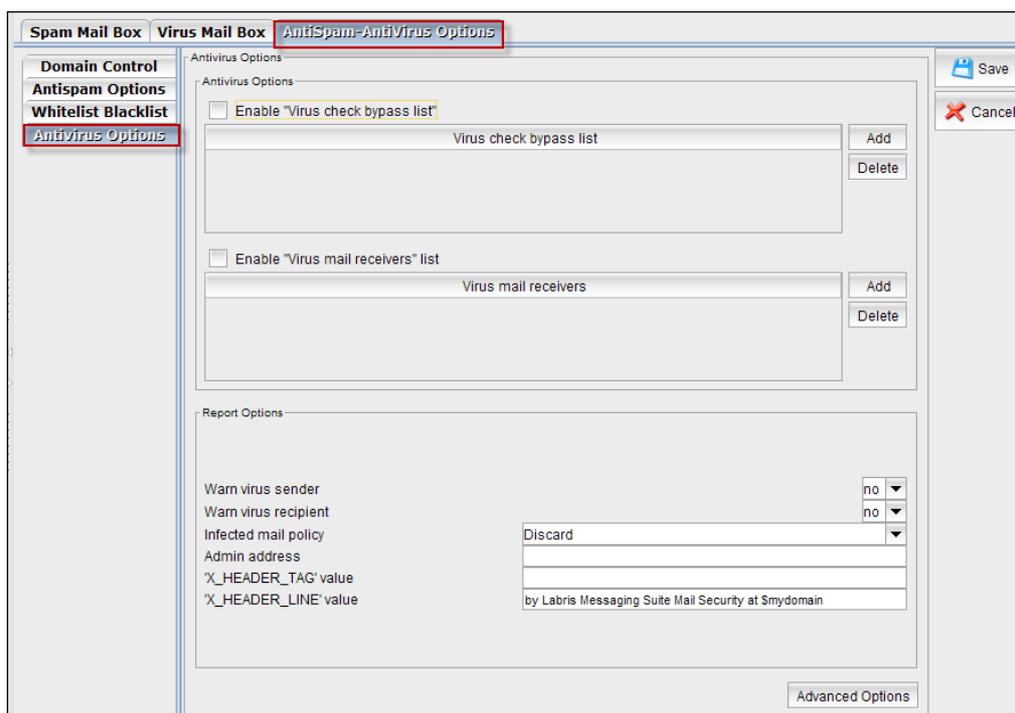
Warning tab appears stating **Are you sure?** Click on **Yes**



101. Antivirus Options

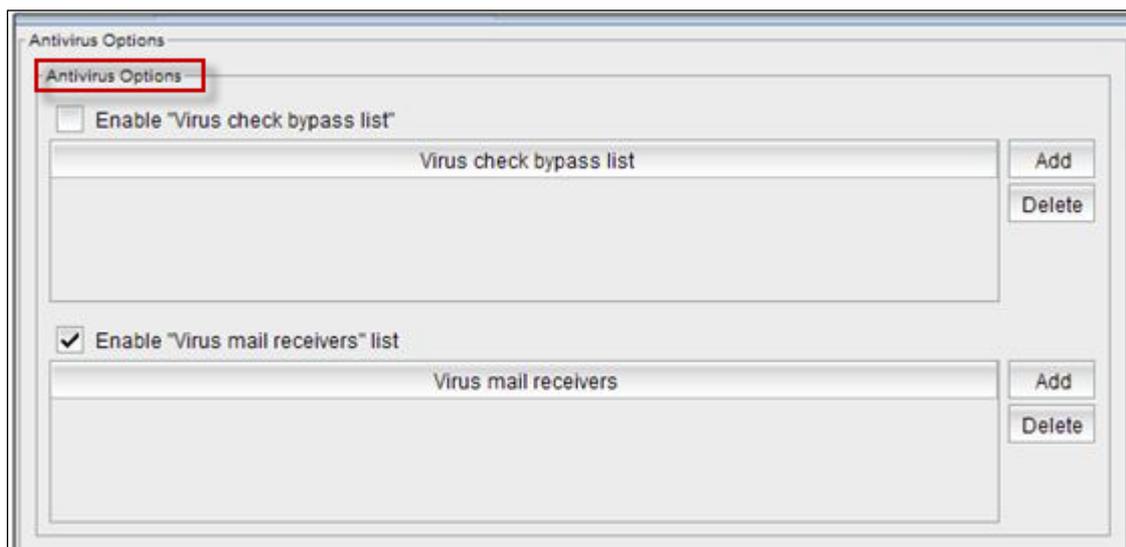
Antivirus consists of two fields.

They are Virus check bypass list and Virus mail receivers list.

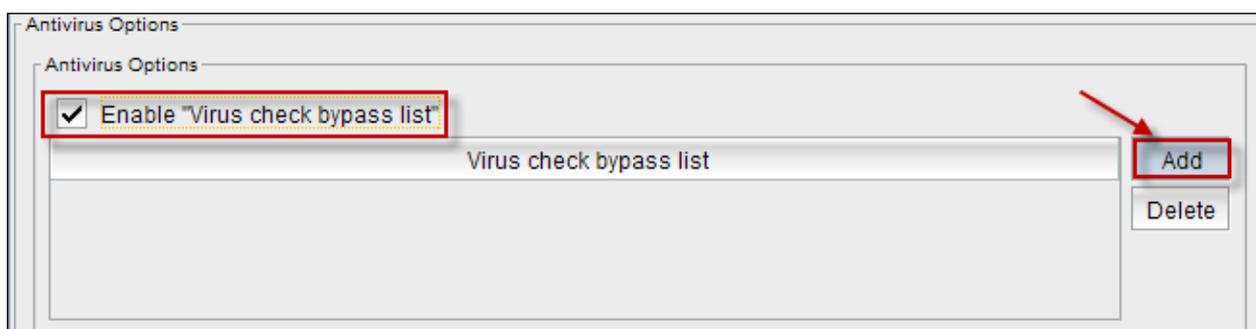


Antivirus Options

It helps us to enable Virus check bypass list and Virus mail receivers list and perform actions like Add, Delete on check options.

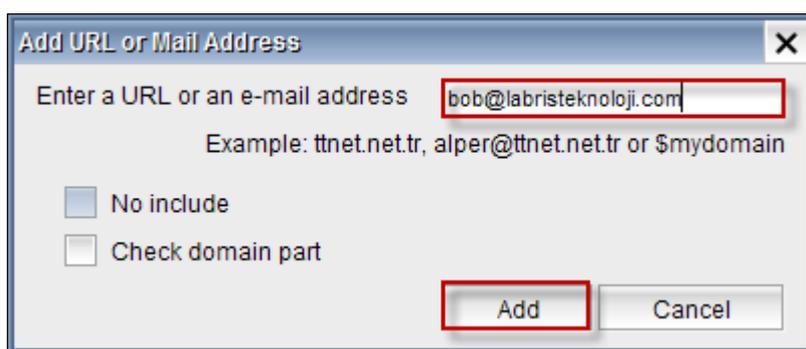


Enable virus check bypass list and click on **Add** tab.

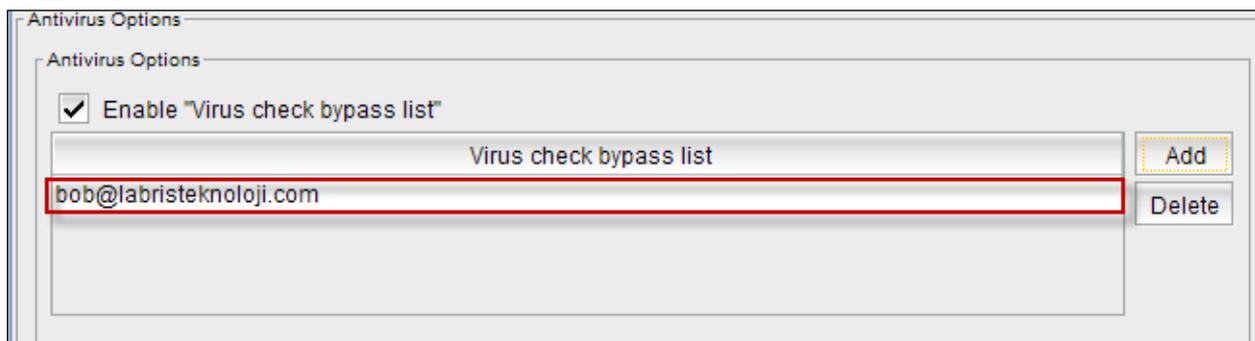


Add URL or Mail Address tab appears.

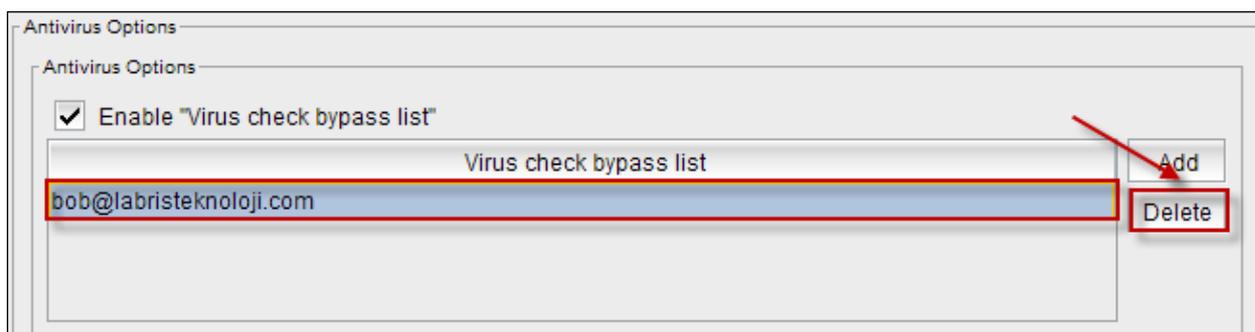
Type **URL or e-mail address**. We can enable No include, check domain part only when we give domain and click on **Add** tab.



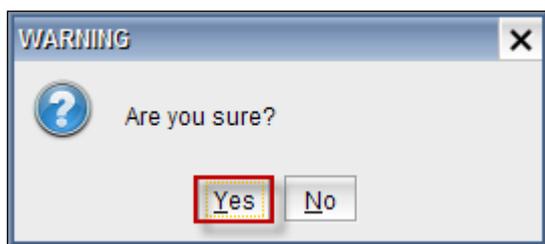
In the below screen, we can notice mail address added in the Virus check bypass list.



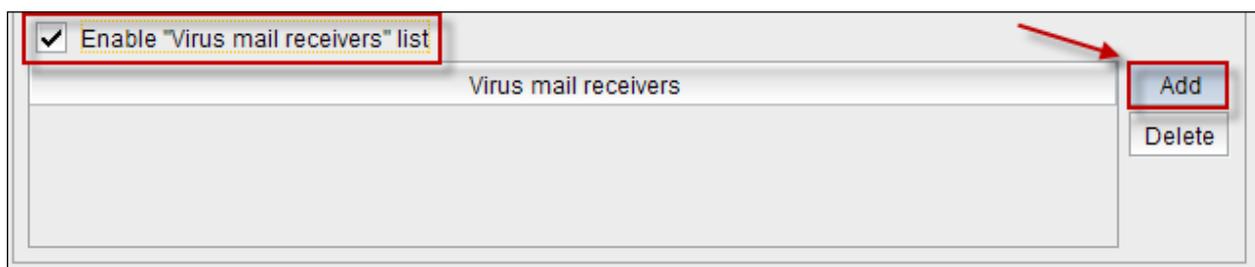
Select mail address and click on **Delete tab**.



Warning tab appears stating **Are you sure?** Click on **Yes**

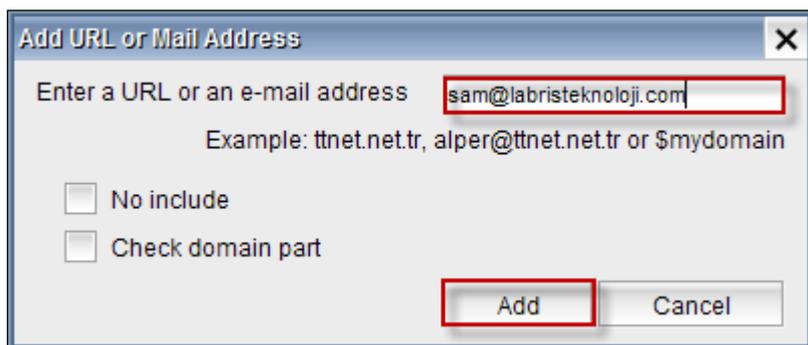


Enable Virus mail receivers list and click on **Add tab**.

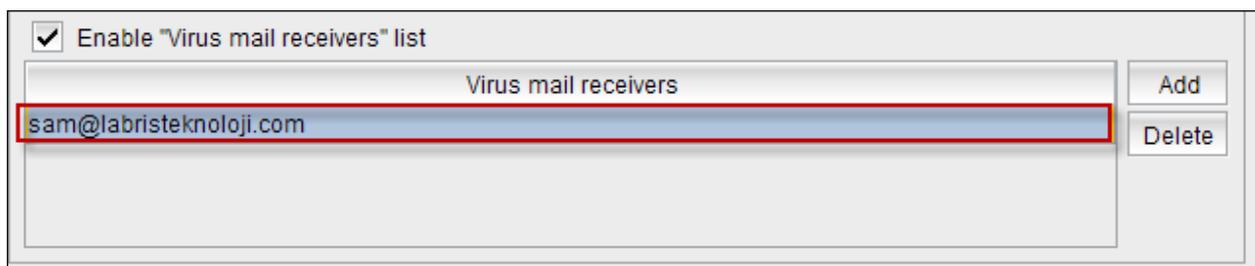


Add URL or Mail Address tab appears.

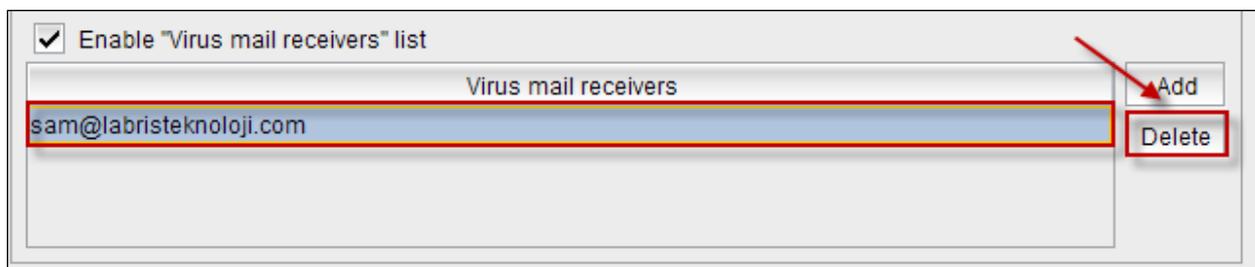
Type **URL or e-mail address**. We can enable No include, check domain part only when we give domain and click on **Add tab**.



In the below screen, we can notice mail address added in the Virus mail receivers.



Select mail address and click on **Delete** tab.



Warning tab appears stating **Are you sure?** Click on **Yes**



Report Options

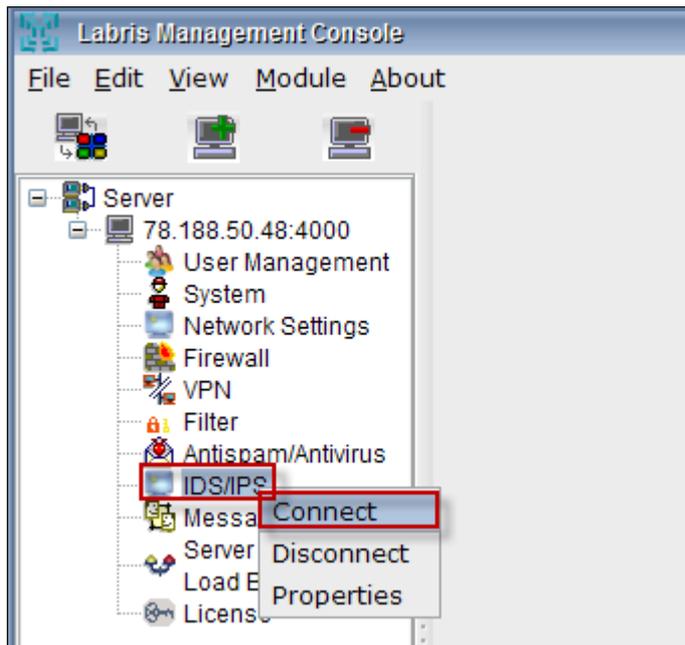
These are the inputs for **Report Options**.

1	Warn virus sender	To Warn virus sender select yes or else no
2	Warn virus recipient	To Warn virus recipient select yes or else no
3	Infected mail policy	Select policy from the drop down list
4	Admin address	Type spam admin mail address
5	'X_HEADER_TAG' value	Give header tag value
6	'X_HEADER_line' value	Give header line value.

Click on **Save** tab to save changes made to the Antivirus options.

IDS/IPS

Right Click on the **IDS / IPS** tab and click on **Connect** to get connected to the IDS/IPS tab

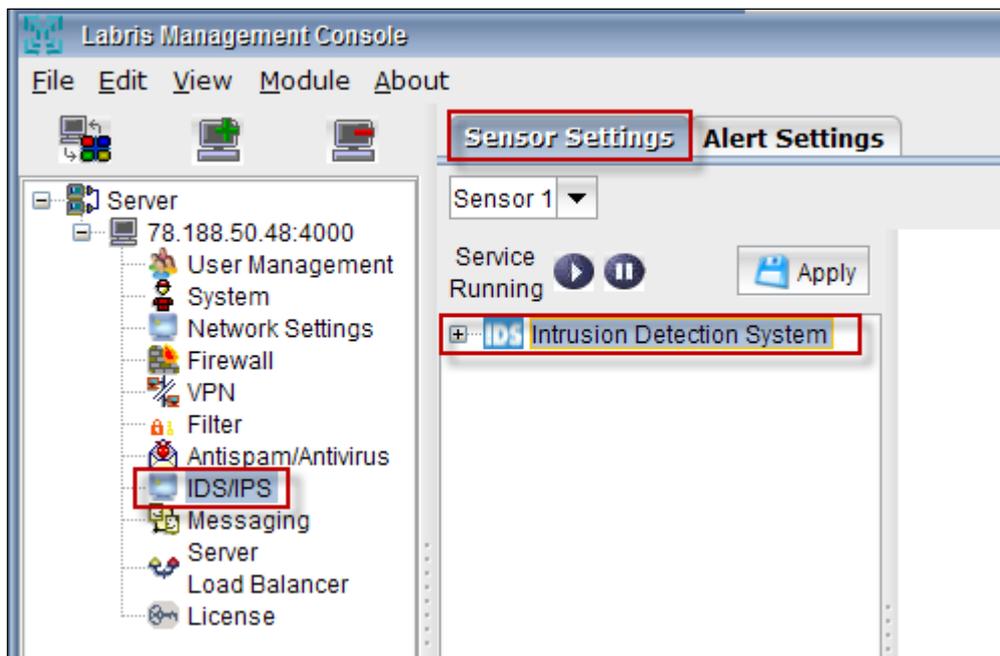


102. Sensor Settings

Once you get connected you can find two options on the top i.e., Sensor settings and alert settings.

Click on **Sensor settings** , in that tab you can find **Intrusion detection system**

Intrusion Detection System



103. Settings

Network Settings

Under Intrusion Detection System we find options like **Settings > Network settings**

Sensor Settings | Alert Settings

Sensor 1 configuration: listening all interfaces

Service Running [Apply]

- Intrusion Detection System
 - Settings
 - Network Settings**
 - Interface
 - Rulesets

Variable	Value	Control/Status
HOME_NET	10.1.1.0/24	Disabled
HOME_NET	\$eth0_ADDRESS	Disabled
HOME_NET	10.1.1.0/24, 192.168.1.0/24	Disabled
HOME_NET	any	Enabled
EXTERNAL_NET	any	Enabled
DNS_SERVERS	\$HOME_NET	Enabled
SMTP_SERVERS	\$HOME_NET	Enabled
HTTP_SERVERS	\$HOME_NET	Enabled
SQL_SERVERS	\$HOME_NET	Enabled
TELNET_SERVERS	\$HOME_NET	Enabled
SNMP_SERVERS	\$HOME_NET	Enabled
HTTP_PORTS	8081	Disabled

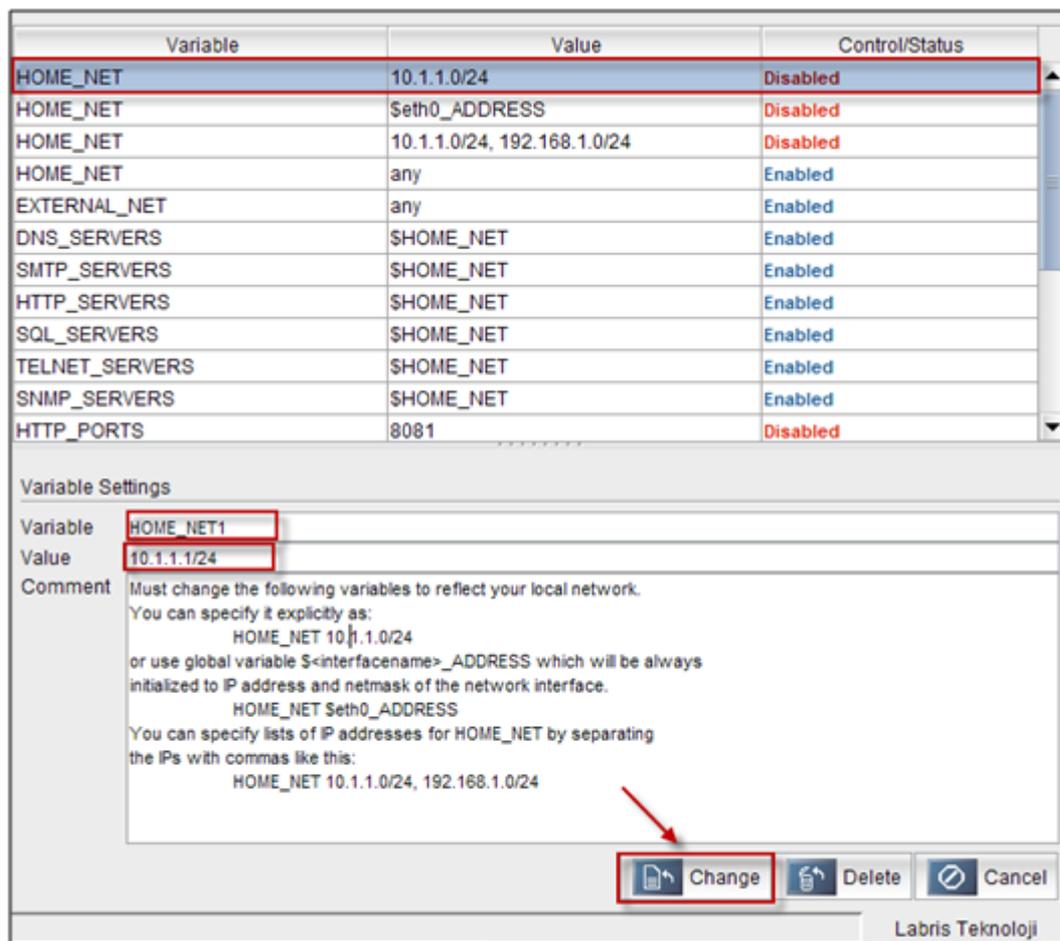
Variable Settings

Variable: HOME_NET
Value: 10.1.1.0/24
Comment: Must change the following variables to reflect your local network.
You can specify it explicitly as:
HOME_NET 10.1.1.0/24
or use global variable \$<interfacename>_ADDRESS which will be always initialized to IP address and netmask of the network interface.
HOME_NET \$eth0_ADDRESS
You can specify lists of IP addresses for HOME_NET by separating the IPs with commas like this:
HOME_NET 10.1.1.0/24, 192.168.1.0/24

[Change] [Delete] [Cancel]

Changing variable

Select one of the variable from the list in the right pane, below you can **edit** the contents of the variables in variable settings tab and click on **Change**.



The screenshot displays the Labris UTM interface. At the top, there is a table with three columns: 'Variable', 'Value', and 'Control/Status'. The first row is highlighted in blue and contains 'HOME_NET', '10.1.1.0/24', and 'Disabled'. Below the table is a 'Variable Settings' dialog box. The 'Variable' field contains 'HOME_NET1' and the 'Value' field contains '10.1.1.1/24'. The 'Comment' field contains instructions on how to specify the variable value. At the bottom of the dialog box, there are three buttons: 'Change', 'Delete', and 'Cancel'. A red arrow points to the 'Change' button.

Variable	Value	Control/Status
HOME_NET	10.1.1.0/24	Disabled
HOME_NET	Seth0_ADDRESS	Disabled
HOME_NET	10.1.1.0/24, 192.168.1.0/24	Disabled
HOME_NET	any	Enabled
EXTERNAL_NET	any	Enabled
DNS_SERVERS	\$HOME_NET	Enabled
SMTP_SERVERS	\$HOME_NET	Enabled
HTTP_SERVERS	\$HOME_NET	Enabled
SQL_SERVERS	\$HOME_NET	Enabled
TELNET_SERVERS	\$HOME_NET	Enabled
SNMP_SERVERS	\$HOME_NET	Enabled
HTTP_PORTS	8081	Disabled

Variable Settings

Variable: HOME_NET1

Value: 10.1.1.1/24

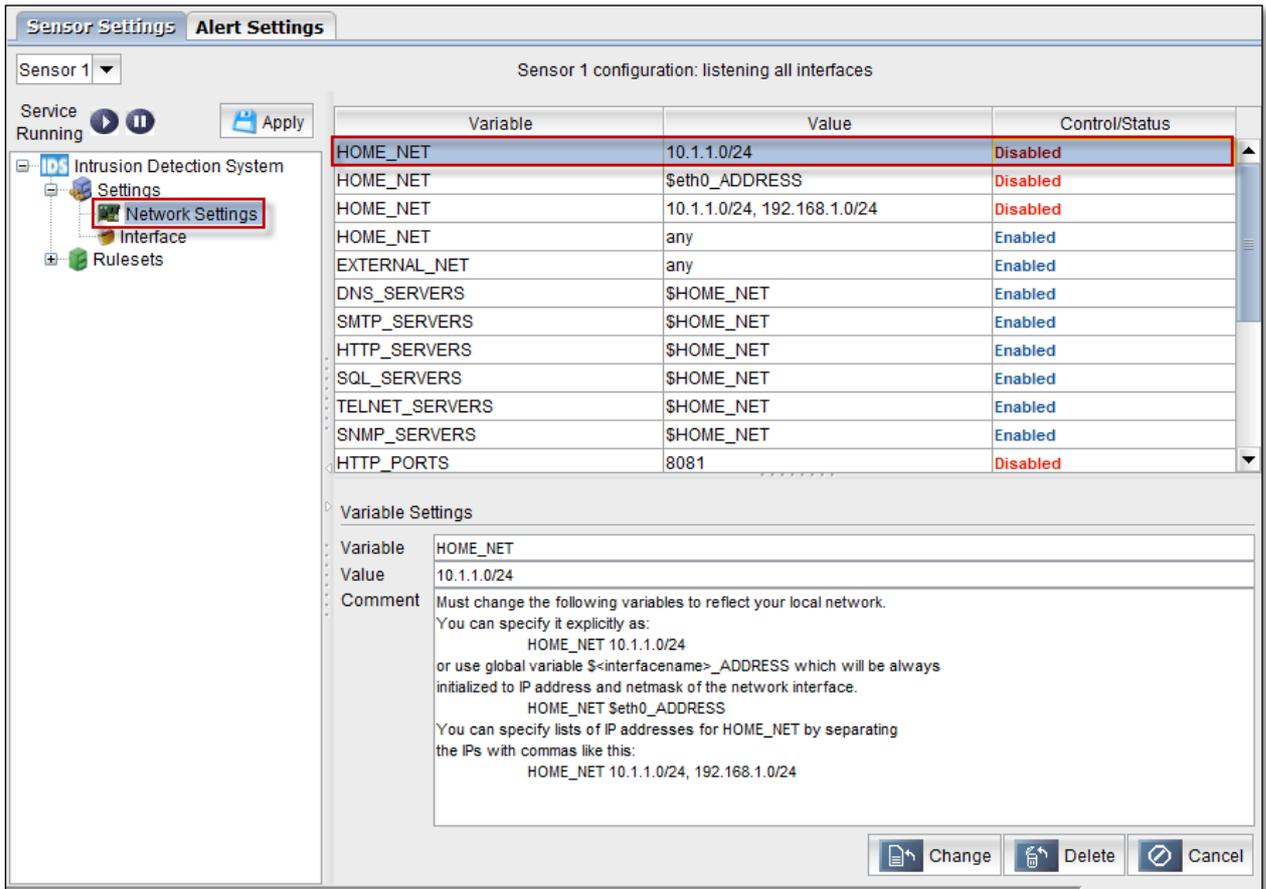
Comment: Must change the following variables to reflect your local network.
You can specify it explicitly as:
HOME_NET 10.1.1.0/24
or use global variable \$<interfacename>_ADDRESS which will be always initialized to IP address and netmask of the network interface.
HOME_NET Seth0_ADDRESS
You can specify lists of IP addresses for HOME_NET by separating the IPs with commas like this:
HOME_NET 10.1.1.0/24, 192.168.1.0/24

Change Delete Cancel

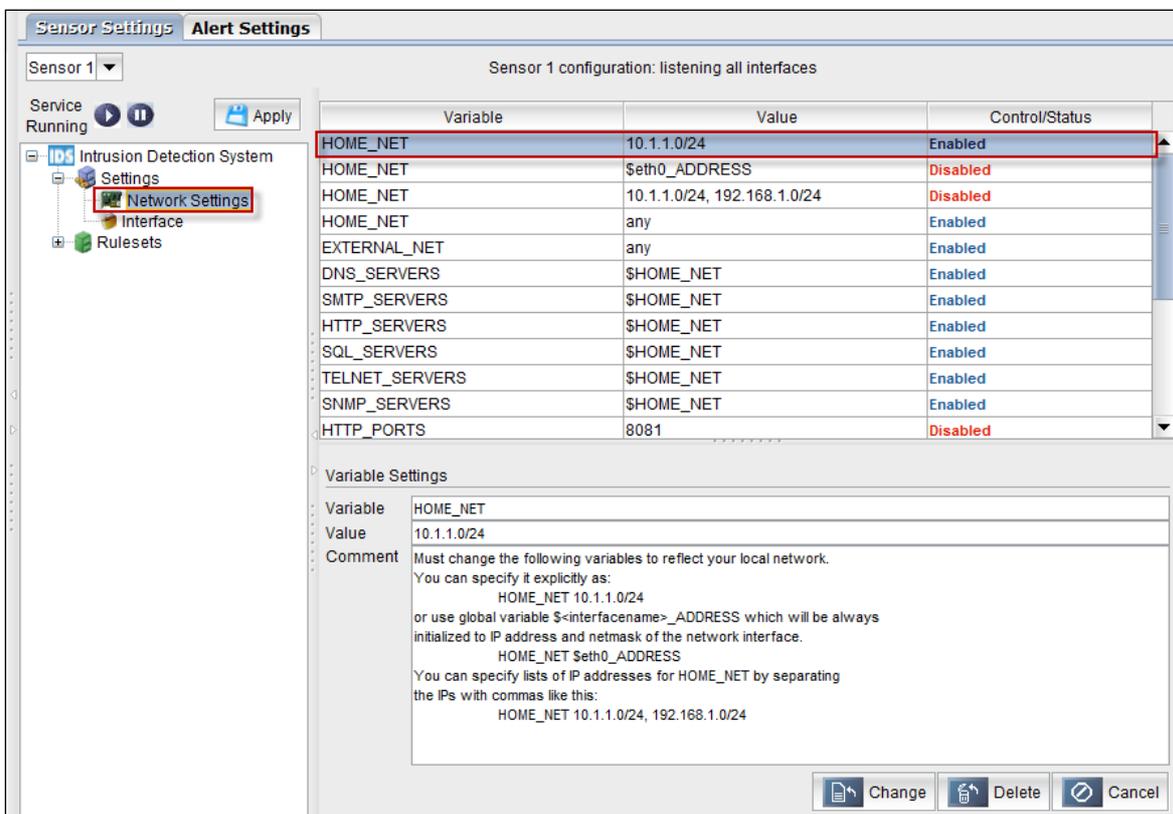
Labris Teknoloji

Changes are applied to the variables immediately. We can notice in the below screen.

Select the variable and double click on Control/Status to make the Variable Enable.



Changes are applied to the variables immediately. We can notice in the below screen.



Deleting variable

Select one of the variables from the list right pane and click on **Delete**.

Selected variables are deleted from the list immediately.

Sensor 1 configuration: listening all interfaces

Variable	Value	Control/Status
HOME_NET1	10.1.1.1/24	Disabled
HOME_NET	\$eth0_ADDRESS	Disabled
HOME_NET	10.1.1.0/24, 192.168.1.0/24	Disabled
HOME_NET	any	Enabled
EXTERNAL_NET	any	Enabled
DNS_SERVERS	\$HOME_NET	Enabled
SMTP_SERVERS	\$HOME_NET	Enabled
HTTP_SERVERS	\$HOME_NET	Enabled
SQL_SERVERS	\$HOME_NET	Enabled
TELNET_SERVERS	\$HOME_NET	Enabled
SNMP_SERVERS	\$HOME_NET	Enabled
HTTP_PORTS	8081	Disabled

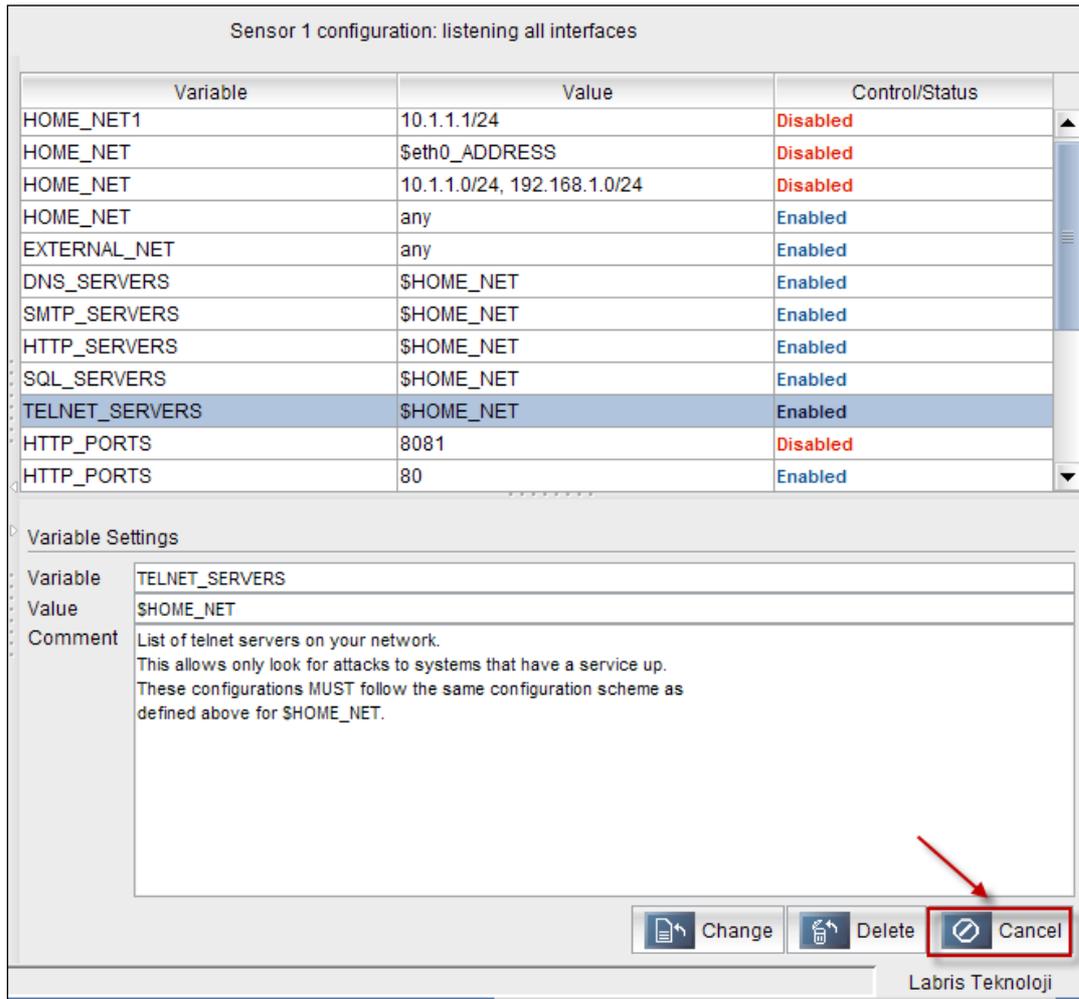
Variable Settings

Variable	SNMP_SERVERS
Value	\$HOME_NET
Comment	???.SNMP_SERVERS???

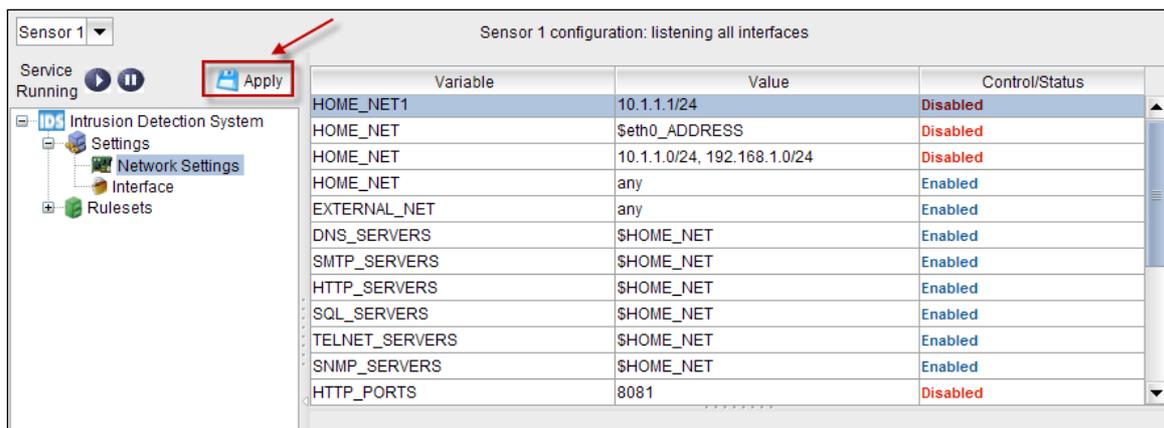
Change Delete Cancel

Cancel

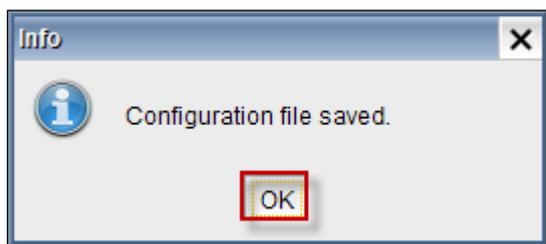
Click on **Cancel** tab to **revert back** to the same settings as before.



Click on **Apply** tab to **apply the modified settings** in Network settings tab

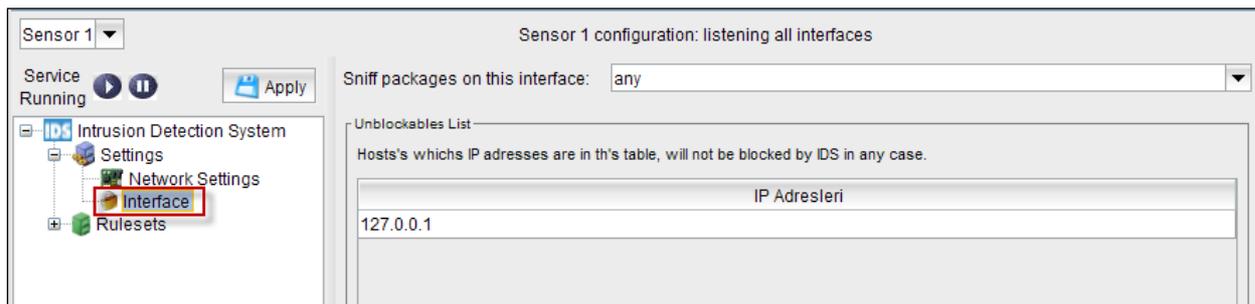


Click **Ok** to save the changes

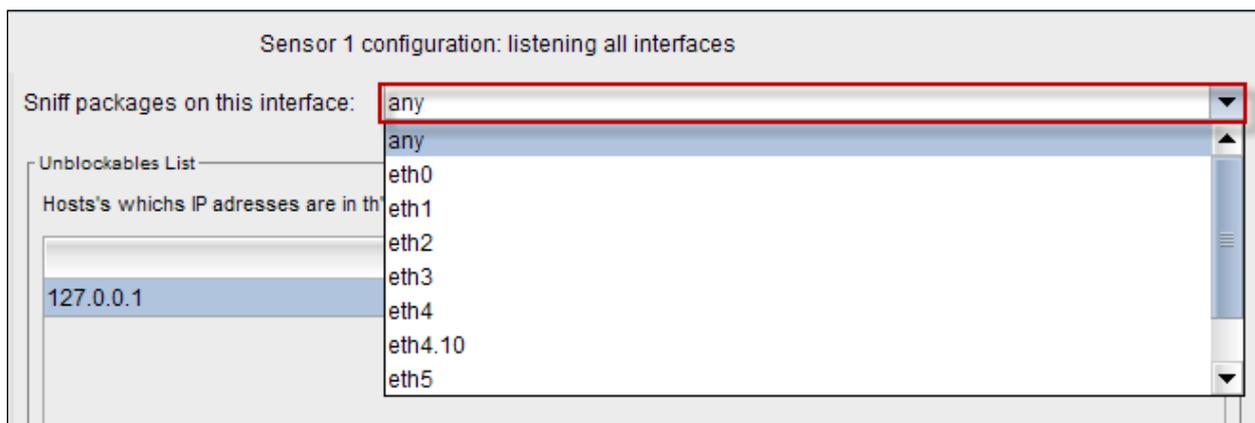


Interface

Select **Interface** tab from the left pane

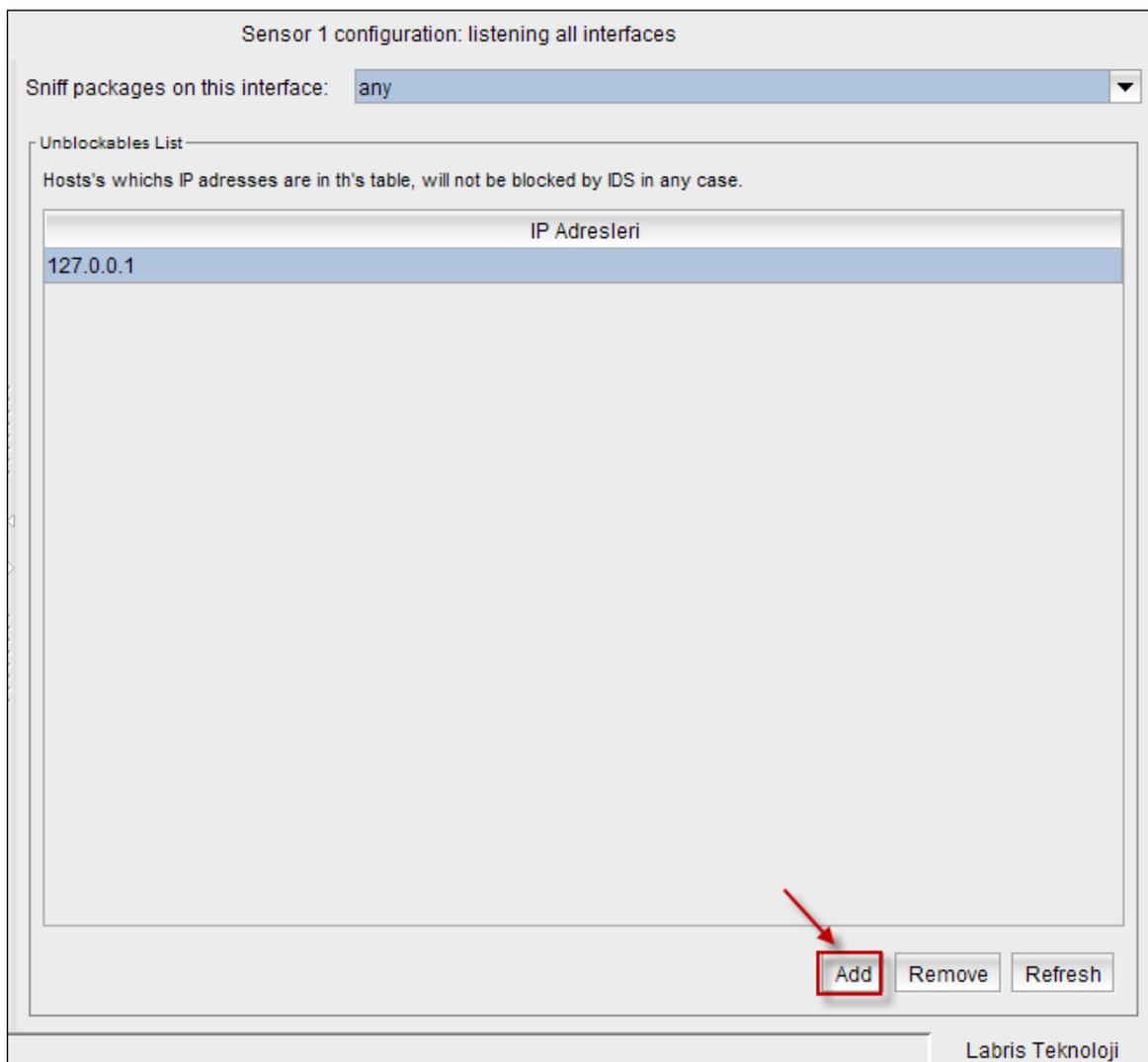


From the **drop down list** select any one of the required **Ethernet** type

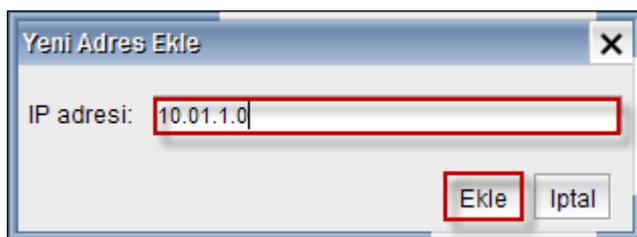


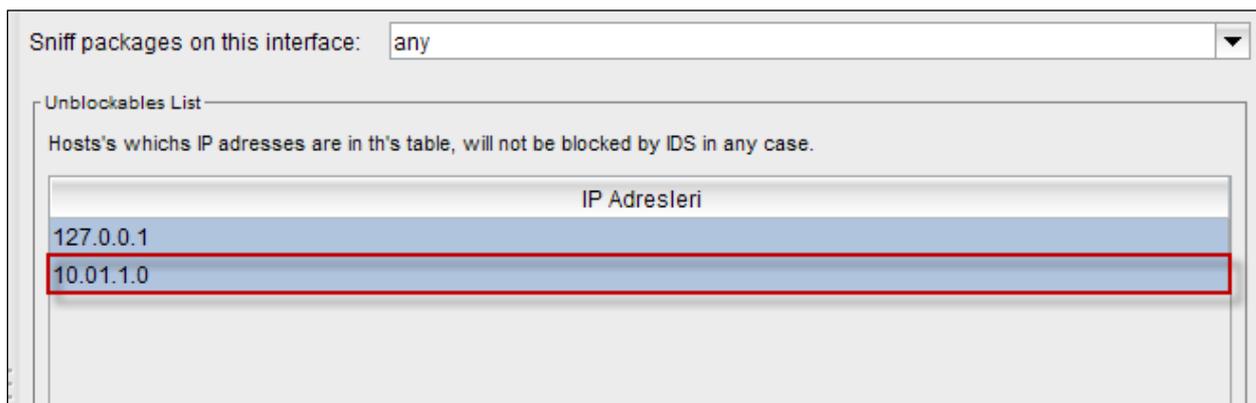
Adding IP

Click on **Add** tab to Add the new IP Address to the **unblockable list**



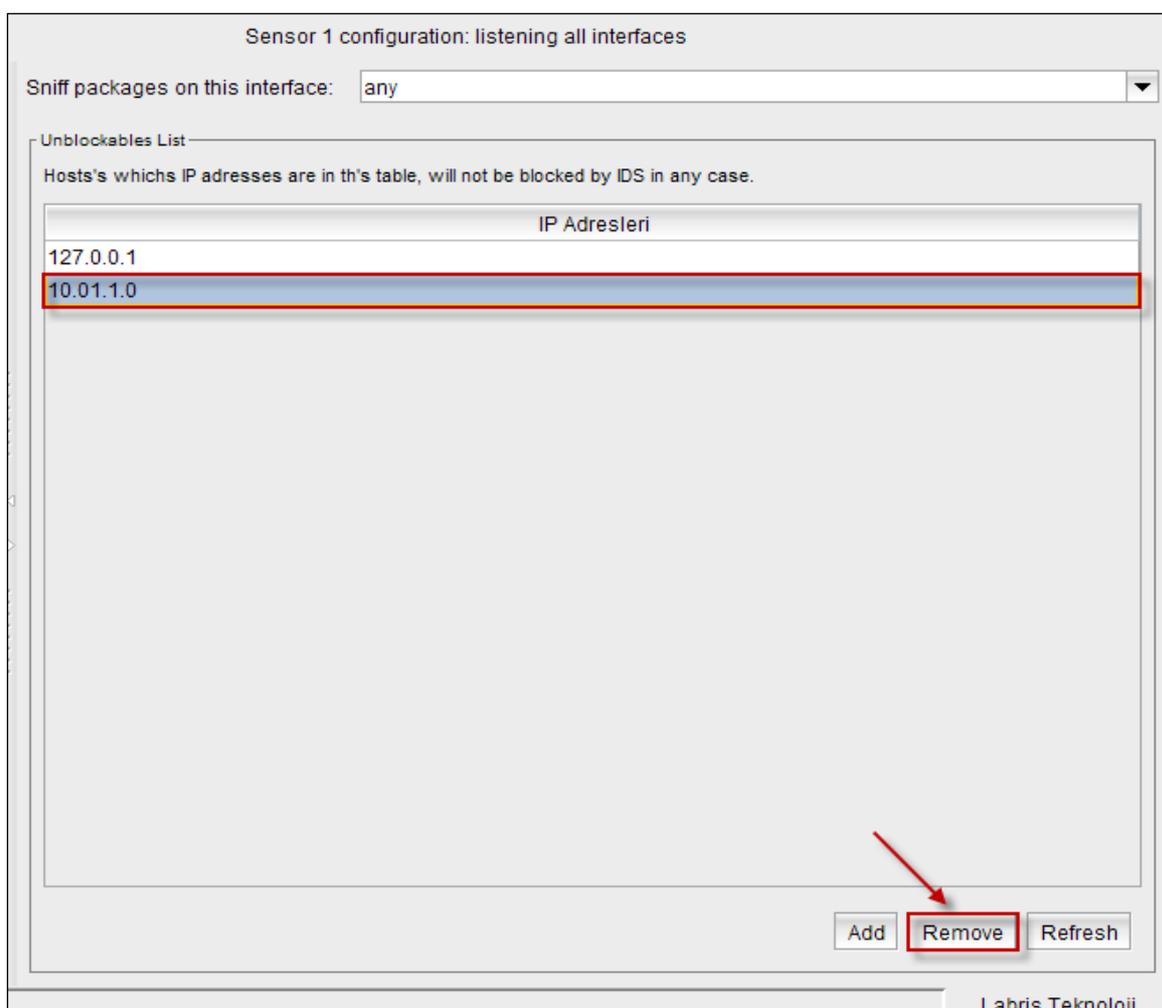
Enter the **IP Address** which you wanted to add to the list and click on **“EKLE”**



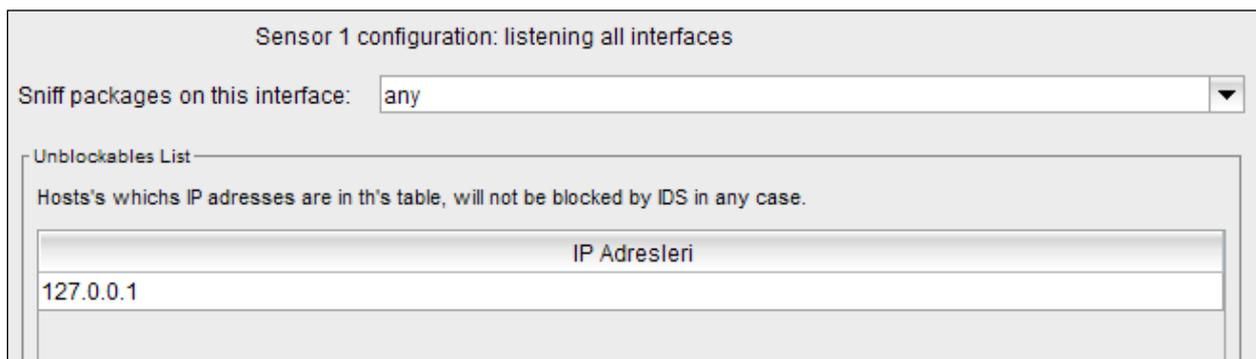


Delete

Select one of the **IP Address** which you want to remove from the list and click on **Remove** tab.

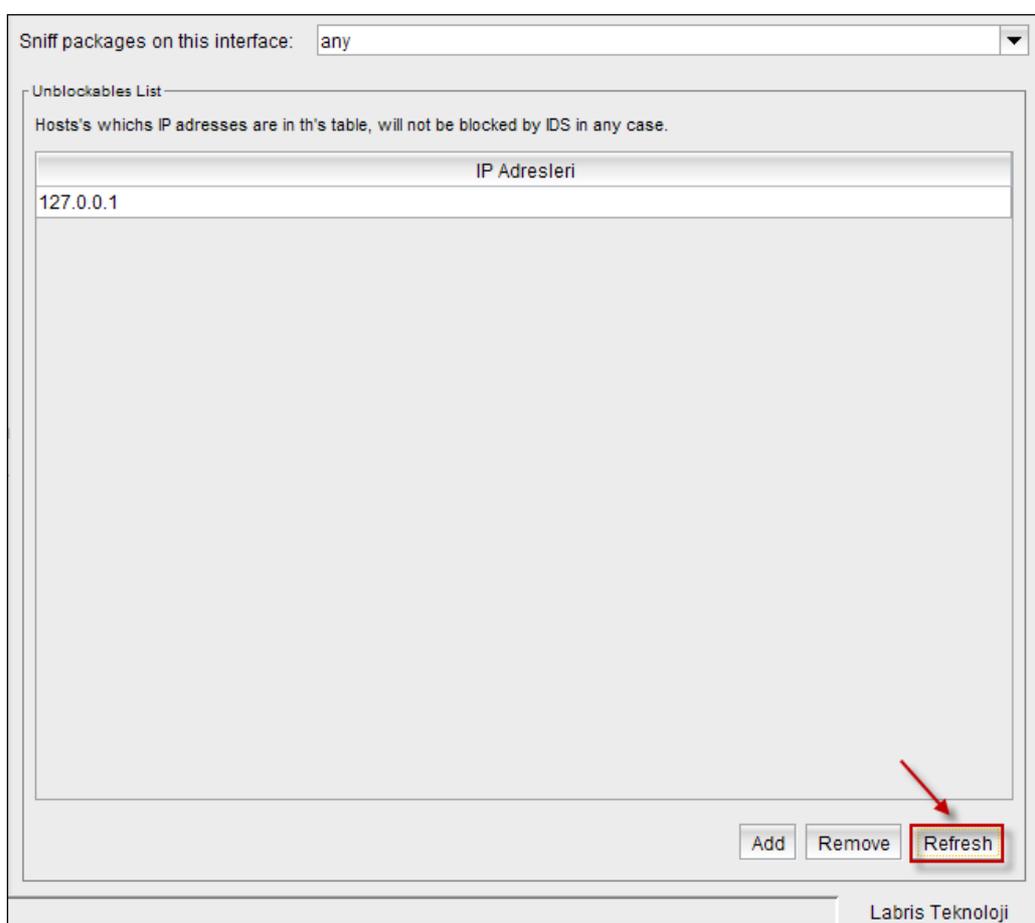


Selected IP Address is removed from the list immediately, which you can notice from the below screen.



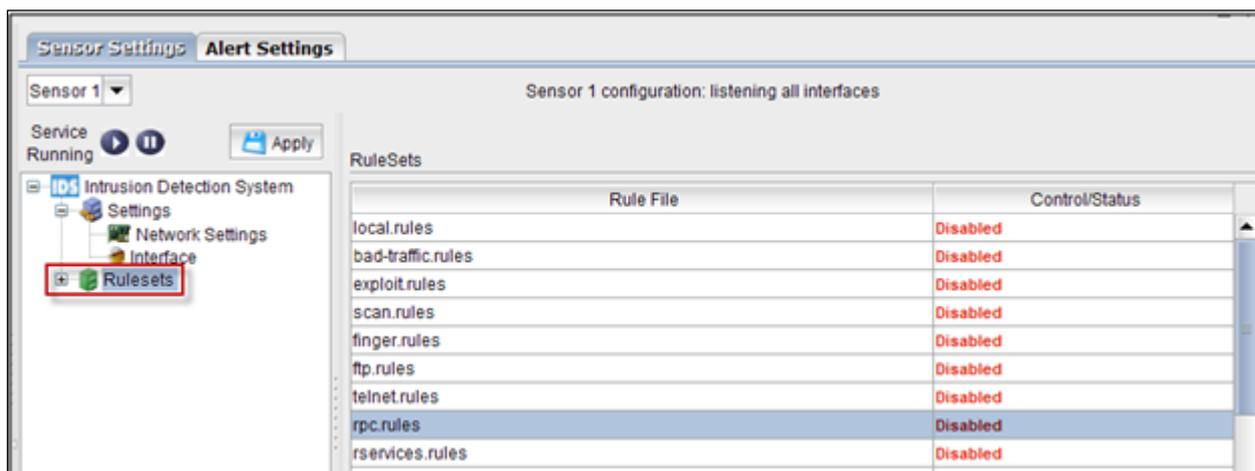
Refresh

Click on **Refresh** Tab to refresh the entire tab.

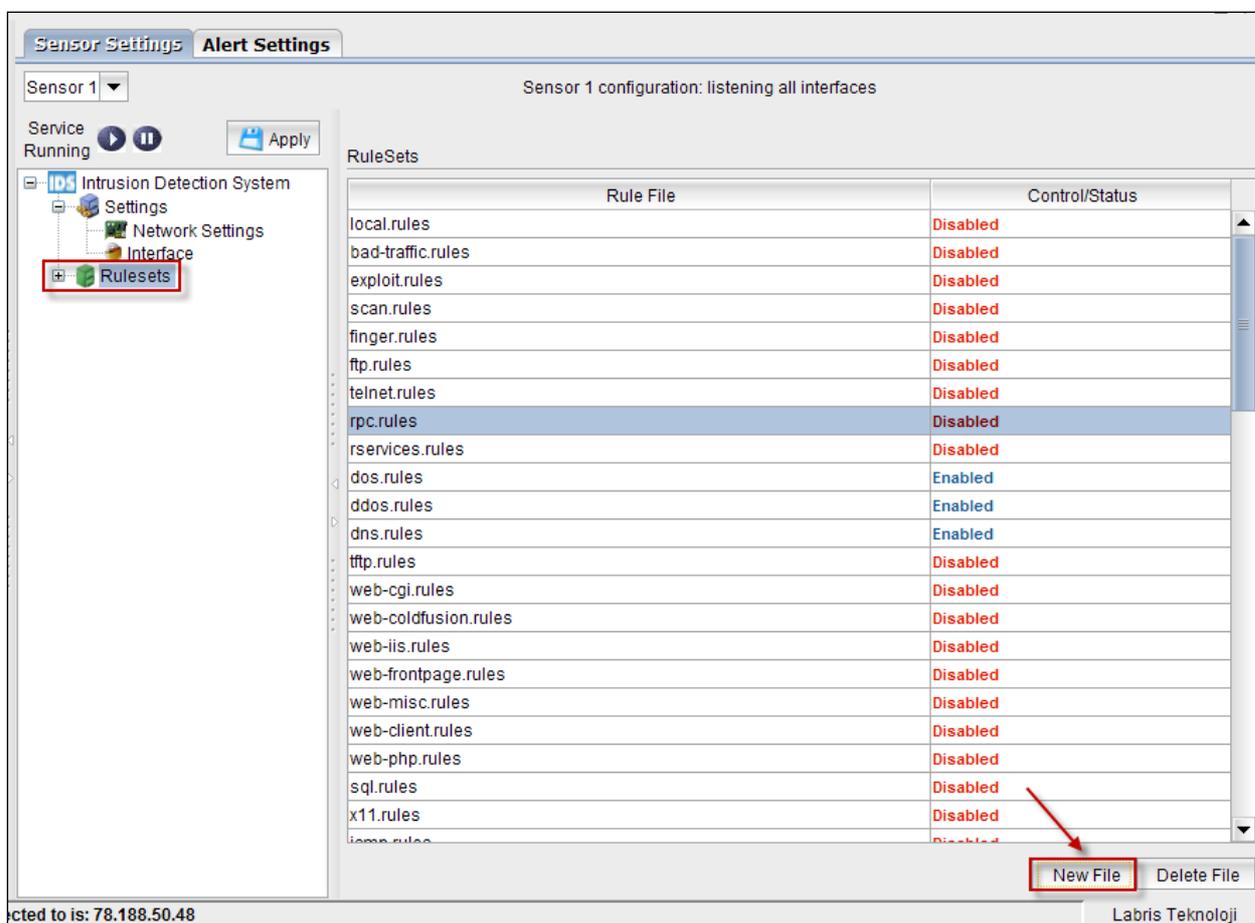


Rule sets

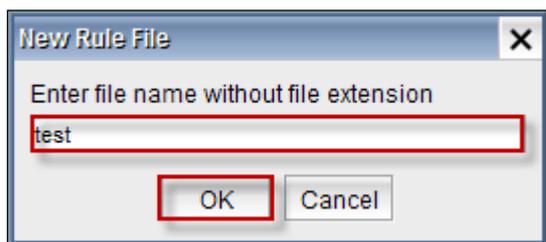
Select **Rulesets** tab from the left pane.



Click on **New File** to create a **new rule file**.



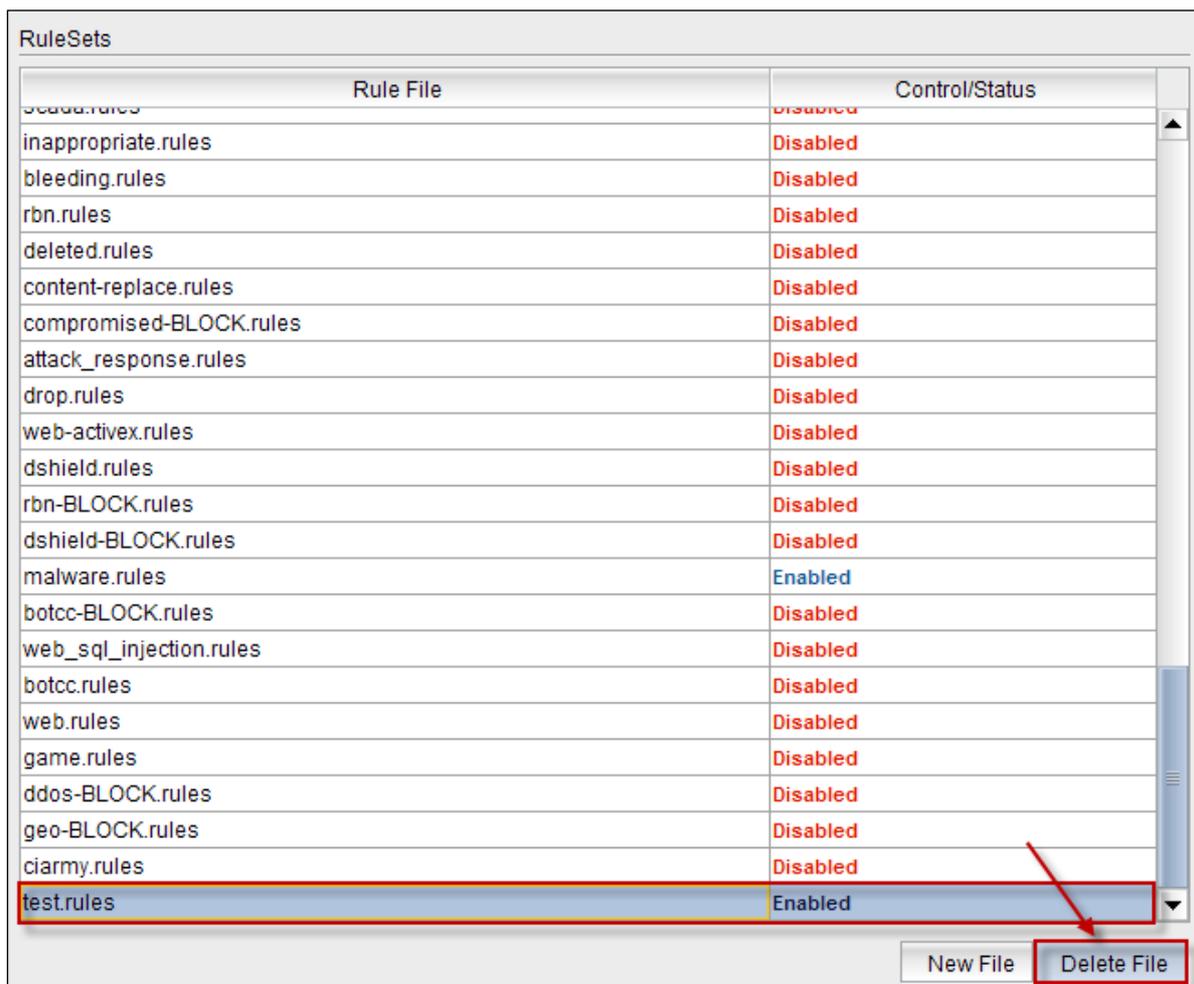
Give the **name** of the file without any extension and click **Ok**.



You can notice that the new file with the name **test** is **added** to the list.

Rule File	Control/Status
default.rules	Disabled
inappropriate.rules	Disabled
bleeding.rules	Disabled
rbn.rules	Disabled
deleted.rules	Disabled
content-replace.rules	Disabled
compromised-BLOCK.rules	Disabled
attack_response.rules	Disabled
drop.rules	Disabled
web-activex.rules	Disabled
dshield.rules	Disabled
rbn-BLOCK.rules	Disabled
dshield-BLOCK.rules	Disabled
malware.rules	Enabled
botcc-BLOCK.rules	Disabled
web_sql_injection.rules	Disabled
botcc.rules	Disabled
web.rules	Disabled
game.rules	Disabled
ddos-BLOCK.rules	Disabled
geo-BLOCK.rules	Disabled
ciarmy.rules	Disabled
test.rules	Enabled

Select the required file from the list and click on **delete file** tab to remove the file from the list.



Rule File	Control/Status
30000.rules	Disabled
inappropriate.rules	Disabled
bleeding.rules	Disabled
rbn.rules	Disabled
deleted.rules	Disabled
content-replace.rules	Disabled
compromised-BLOCK.rules	Disabled
attack_response.rules	Disabled
drop.rules	Disabled
web-activex.rules	Disabled
dshield.rules	Disabled
rbn-BLOCK.rules	Disabled
dshield-BLOCK.rules	Disabled
malware.rules	Enabled
botcc-BLOCK.rules	Disabled
web_sql_injection.rules	Disabled
botcc.rules	Disabled
web.rules	Disabled
game.rules	Disabled
ddos-BLOCK.rules	Disabled
geo-BLOCK.rules	Disabled
ciarmy.rules	Disabled
test.rules	Enabled

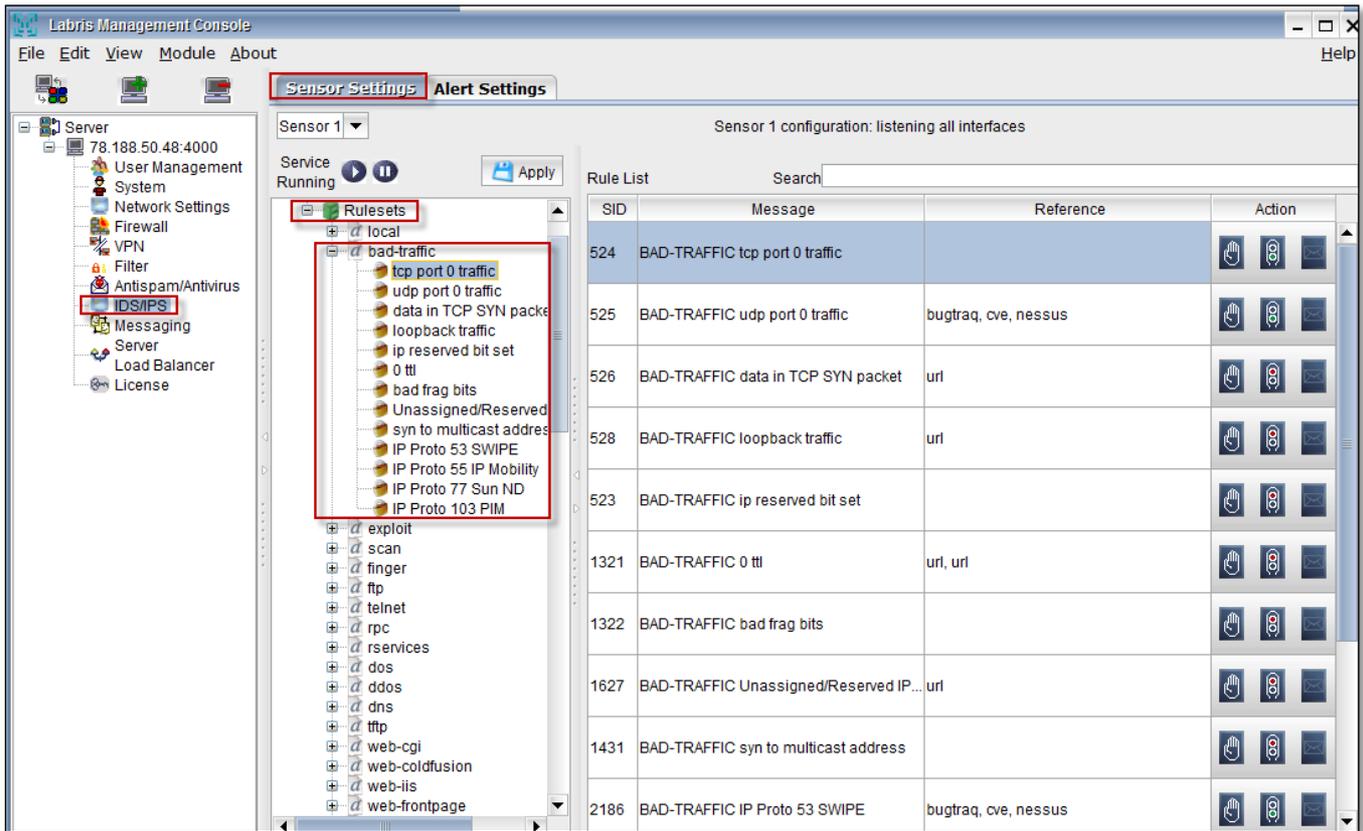
New File Delete File

Rulesets List

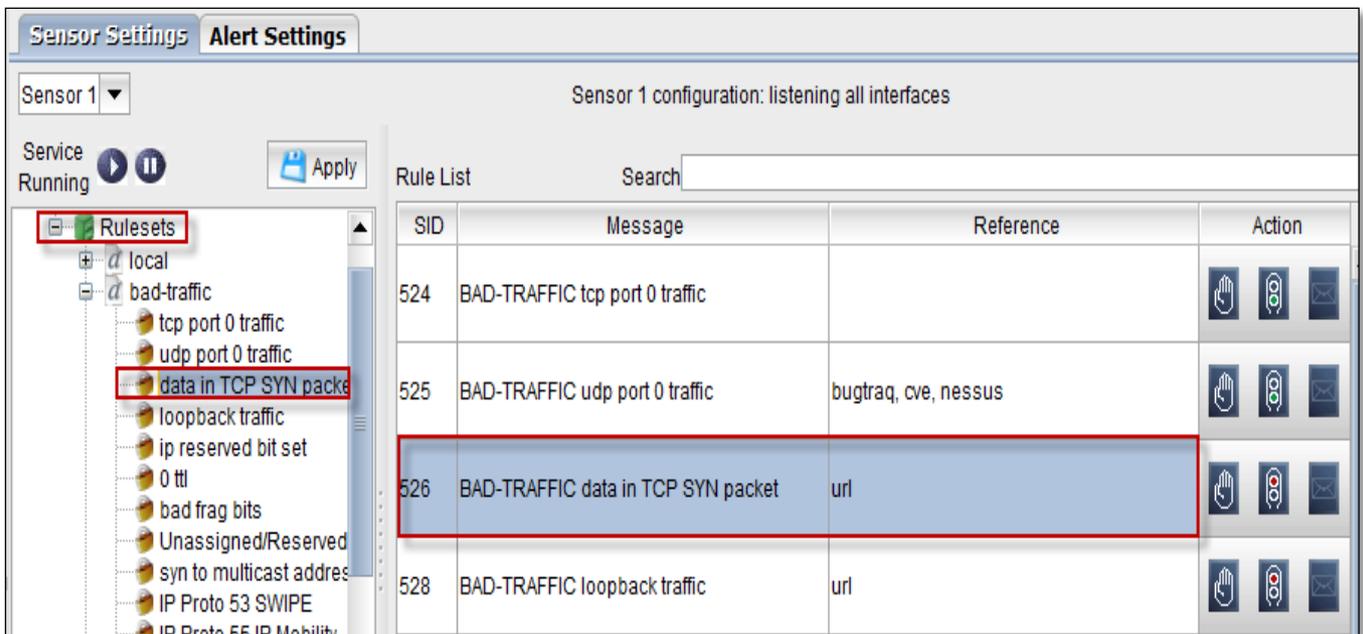
Expand **Rulesets** from the Leftpane.

We can find different list of Rulesets.

Expand any one of the Rulesets as shown in the below figure.



Select any one of the Rule from the **RuleList**.



Click on
Rule.



the icon from the Action Tab to **Block** , **UnBlock** or **cancel** the selected Rule.

The screenshot shows the 'Sensor Settings' window for 'Sensor 1'. The 'Alert Settings' tab is active. On the left, a tree view shows 'Rulesets' with categories like 'local', 'bad-traffic', 'exploit', 'scan', etc. The 'bad-traffic' category is expanded, showing rules like 'tcp port 0 traffic', 'udp port 0 traffic', and 'data in TCP SYN packet'. The 'Rule List' table on the right contains the following data:

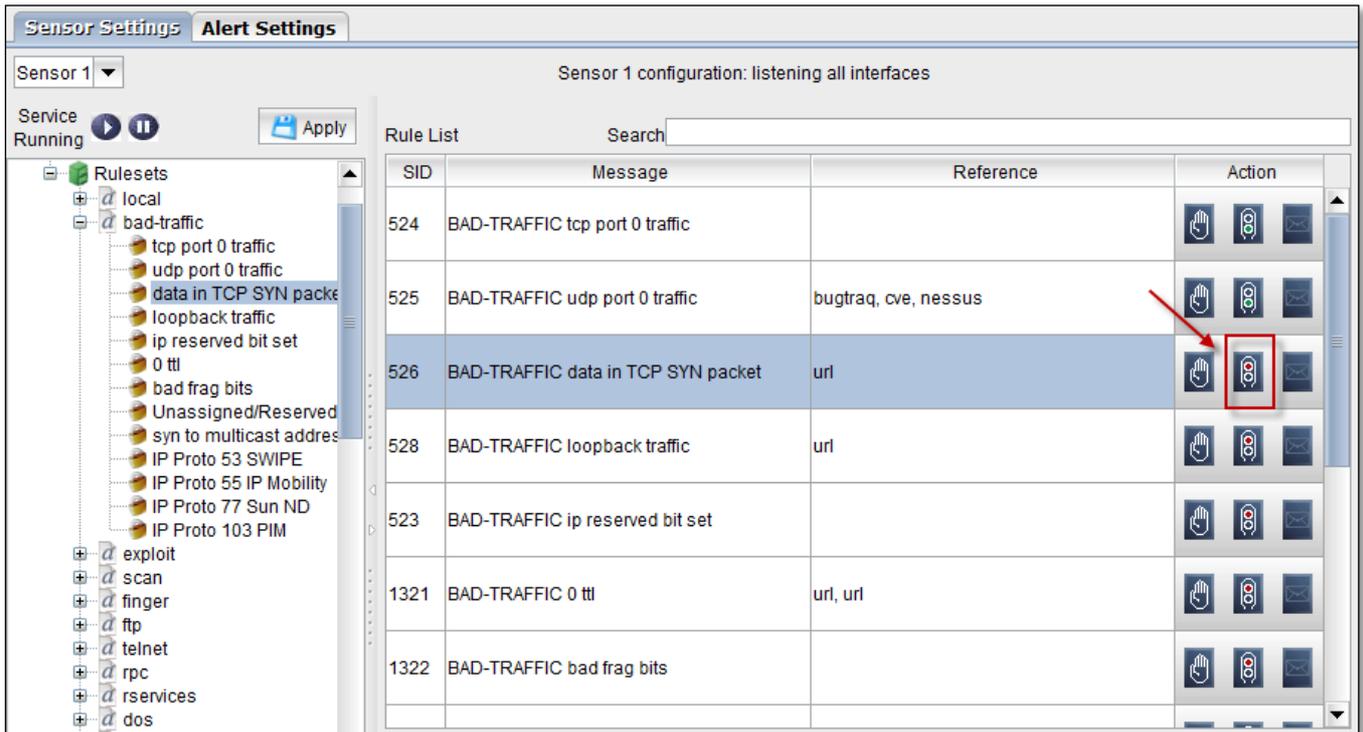
SID	Message	Reference	Action
524	BAD-TRAFFIC tcp port 0 traffic		[Hand icon] [Light icon] [Envelope icon]
525	BAD-TRAFFIC udp port 0 traffic	bugtraq, cve, nessus	[Hand icon] [Light icon] [Envelope icon]
526	BAD-TRAFFIC data in TCP SYN packet	url	[Hand icon] [Light icon] [Envelope icon]
528	BAD-TRAFFIC loopback traffic	url	[Hand icon] [Light icon] [Envelope icon]
523	BAD-TRAFFIC ip reserved bit set		[Hand icon] [Light icon] [Envelope icon]
1321	BAD-TRAFFIC 0 ttl	url, url	[Hand icon] [Light icon] [Envelope icon]
1322	BAD-TRAFFIC bad frag bits		[Hand icon] [Light icon] [Envelope icon]

Below the table, the 'Rule Block' section is visible, with a red box around the 'Rule Block' label. The 'Rule apply to' dropdown is set to 'src', 'How apply(optional)' is empty, and 'Time(day:hr:min:sec)' is '00:00:00'. At the bottom right, there are three buttons: 'Block' (with a green light icon), 'Unblock' (with a red light icon), and 'Cancel' (with a red 'X' icon). A red arrow points to the 'Hand' icon in the 'Action' column of the row for rule 526.

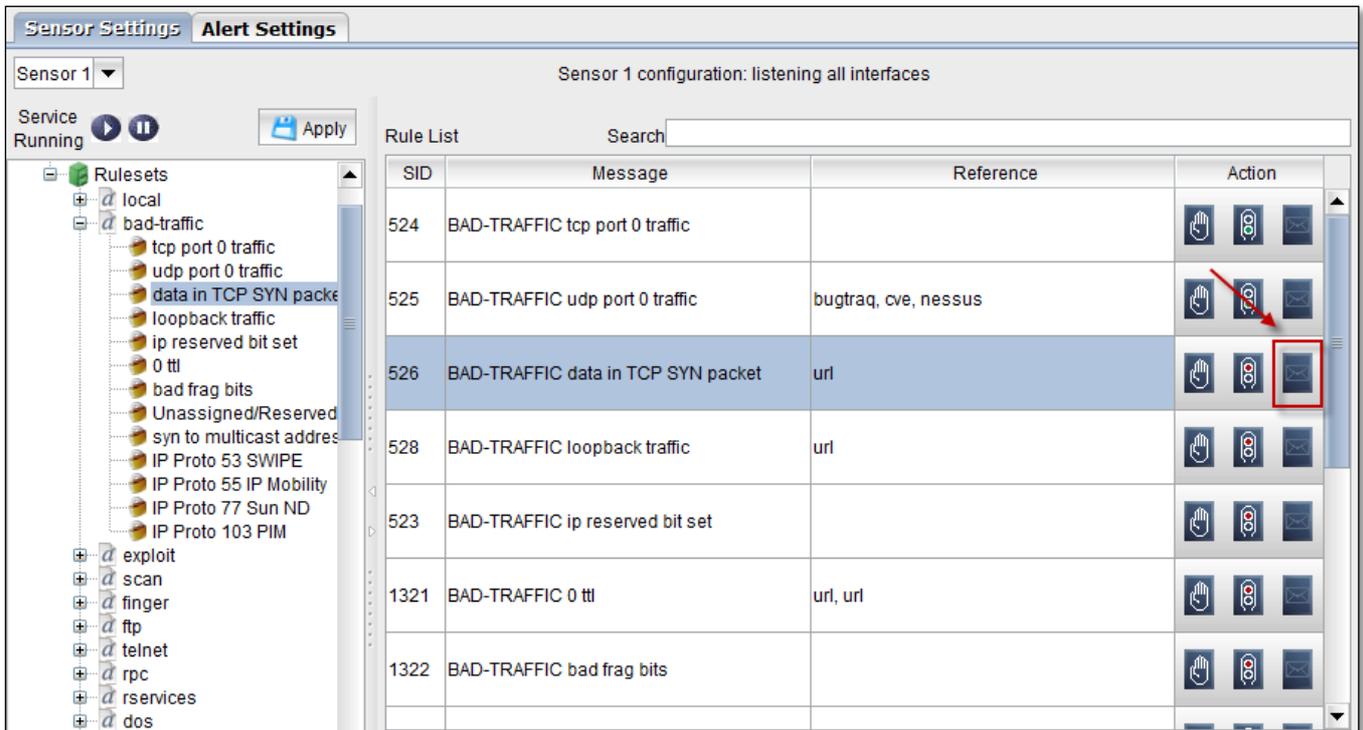
Click on the highlighted icon to **Start / Stop** the Rule.

Red Light – Stop

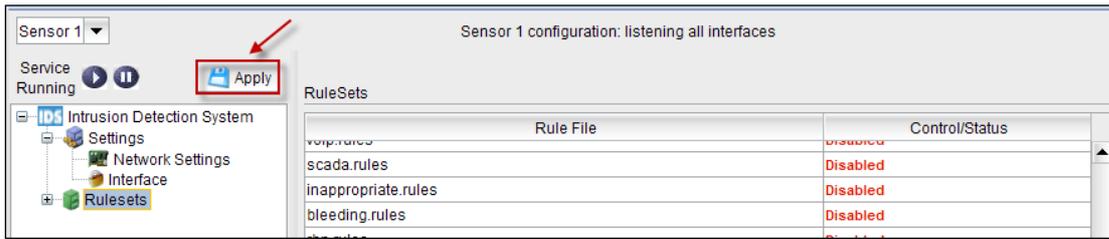
Green Light - Start



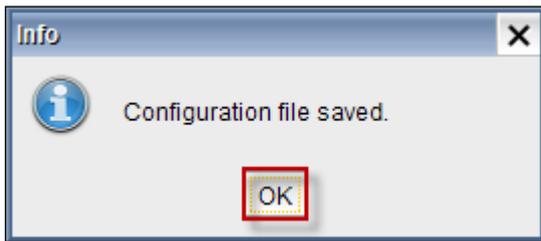
Click on the highlighted icon to redirect to the reference URL which is specified in the list.



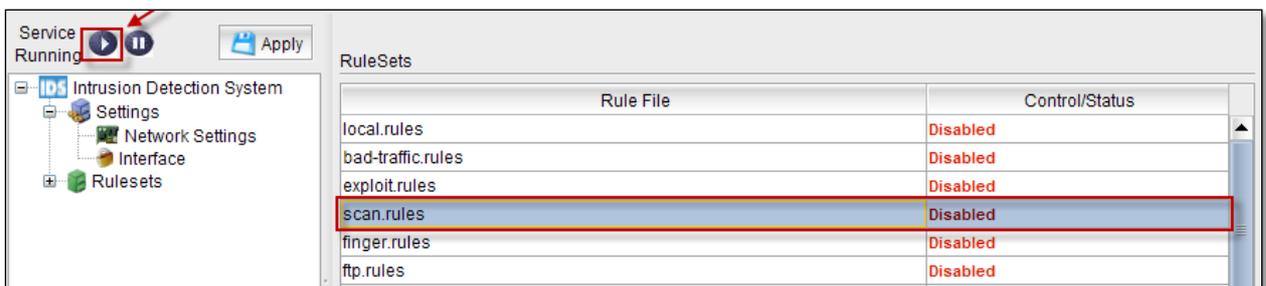
Click on **Apply** tab to **apply the modified settings** in Rulesets tab.



Click on **Ok** to save the changes.



Click on the **Start** tab as shown in the screen to start the IDS Service for chosen sensor



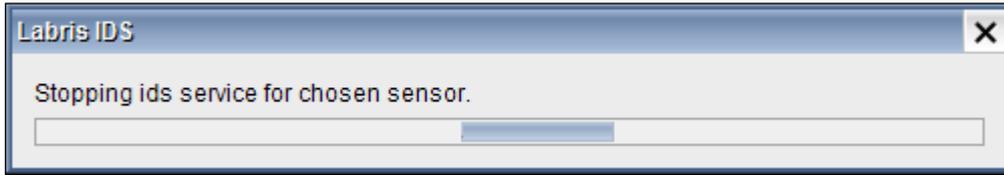
Below screen appears stating that Starting IDS service is in progress.



Click on the **Stop** tab as shown in the screen to stop the IDS Service for chosen sensor.

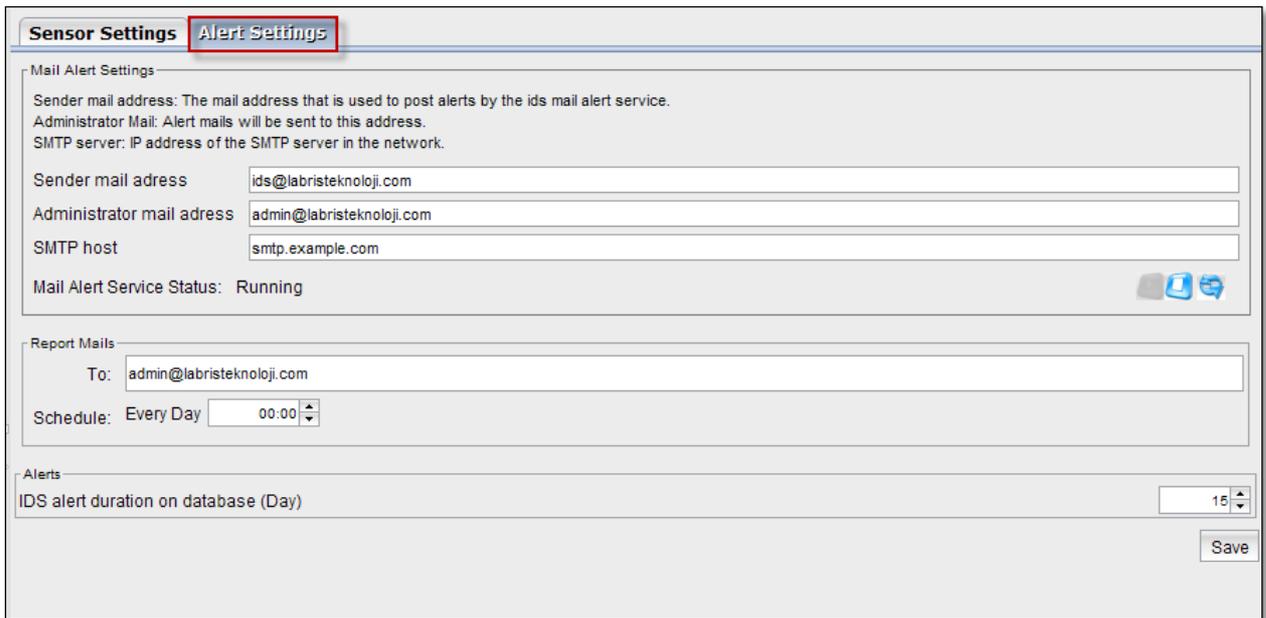


Below screen appears stating that Stopping IDS service is in progress.



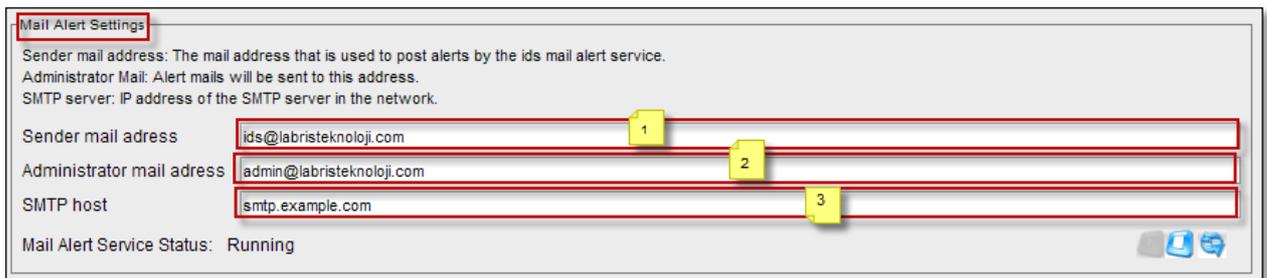
104. Alert Settings

In the **Alert** tab we can find options like **Mail Alert Settings**, **Report Mails** and **Alerts**.



Mail Alert Settings

Give the inputs in the below fields.



1	Sender mail address	In this field give the sender mail address
2	Administrator mail address	In this field give the administrator mail address
3	SMTP host	In this field give the details of the SMTP server

Report Mails

In the Report mails tab specify the **To address** and **Schedule time** to send mails.



The screenshot shows a configuration window titled "Report Mails". It contains two main fields: "To:" with the value "admin@labristeknoloji.com" and "Schedule:" with the value "Every Day" and a time selector set to "01:00". Red boxes highlight the "Report Mails" title, the "To:" field, and the "Schedule:" field.

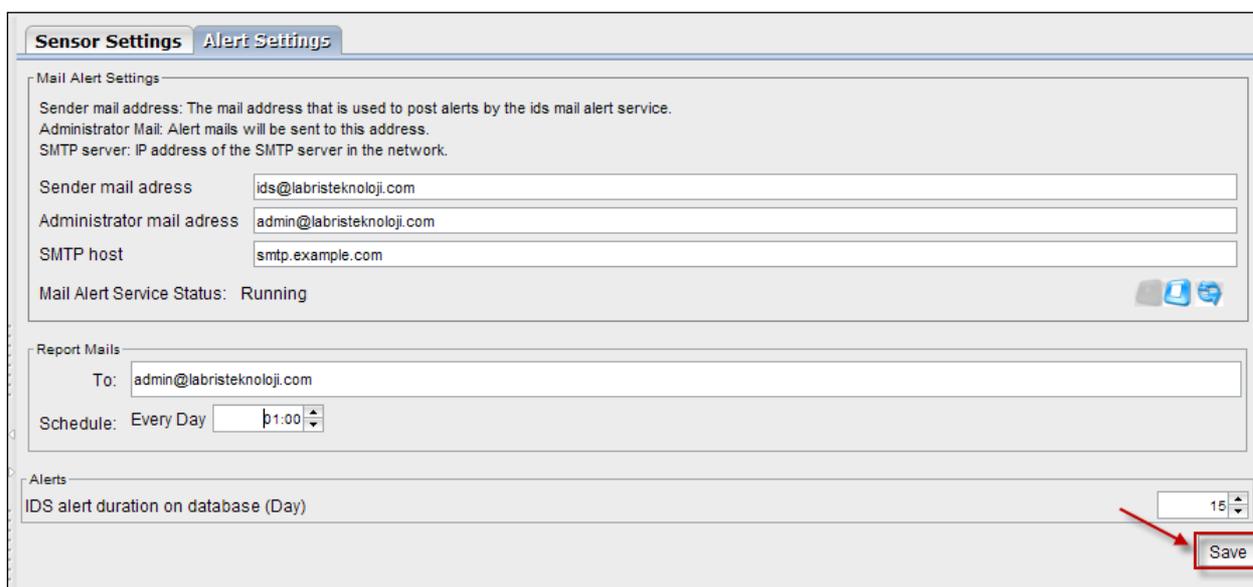
Alerts

In the **Alerts** tab, we can change the **IDS Alert Duration** depending on the requirement.



The screenshot shows a configuration window titled "Alerts". It contains a single field: "IDS alert duration on database (Day)" with a value of "15". A red box highlights the "Alerts" title and another red box highlights the "15" value in the input field.

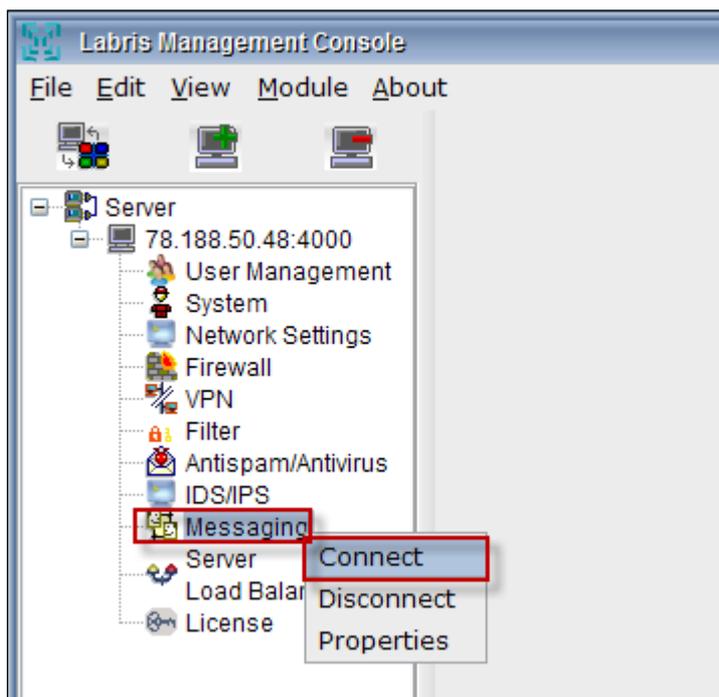
Click on **save** tab to save the modified settings



The screenshot shows a configuration page with two tabs: "Sensor Settings" and "Alert Settings". The "Alert Settings" tab is active. It contains several sections: "Mail Alert Settings" with fields for "Sender mail address" (ids@labristeknoloji.com), "Administrator mail address" (admin@labristeknoloji.com), and "SMTP host" (smtp.example.com); "Report Mails" with "To:" (admin@labristeknoloji.com) and "Schedule:" (Every Day, 01:00); and "Alerts" with "IDS alert duration on database (Day)" (15). A red arrow points to a "Save" button in the bottom right corner.

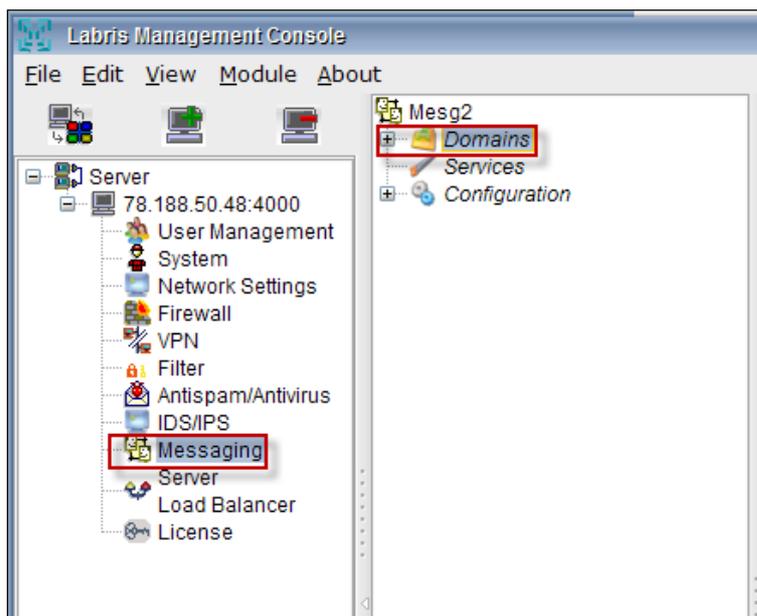
MESSAGING

Right click on **Messaging**, Select **Connect**.



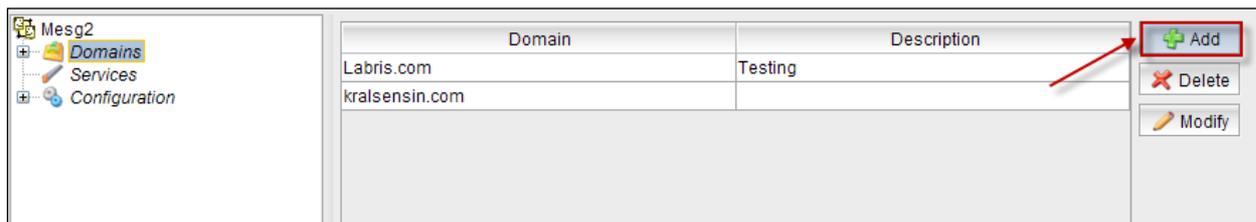
105. Domains

When we get connected to Messaging, we can notice **Domains** in the right pane.



Domain

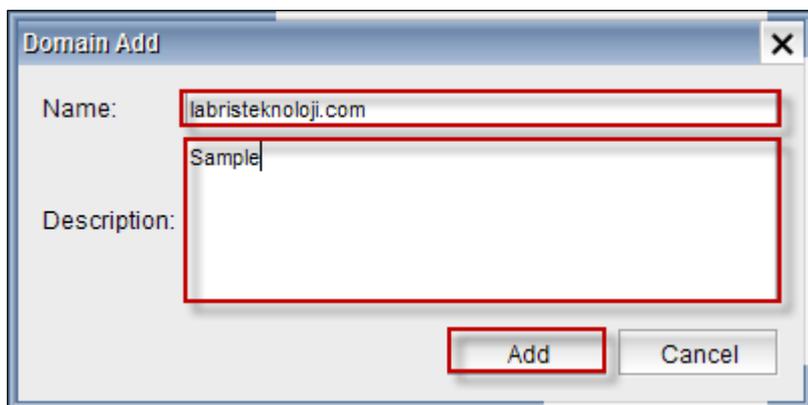
Click on **Add** tab to add new Domain to Messaging.



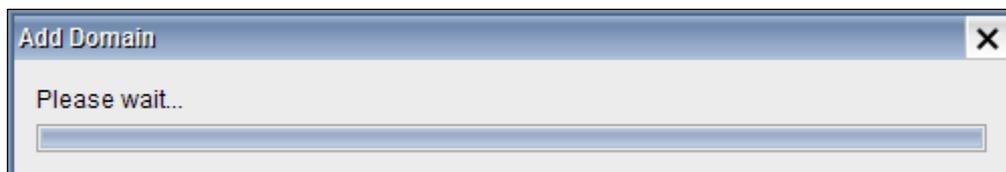
Domain Add tab appears.

Type the **name of domain** and give information regarding Domain in the **Description** column.

Click on **Add** tab.



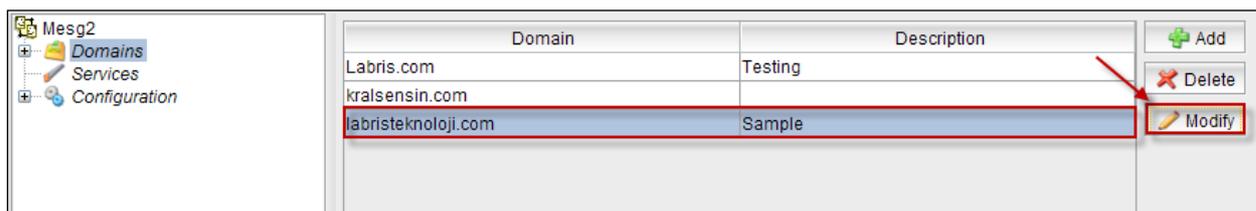
Below screen appears stating that Adding Domain process is in progress.



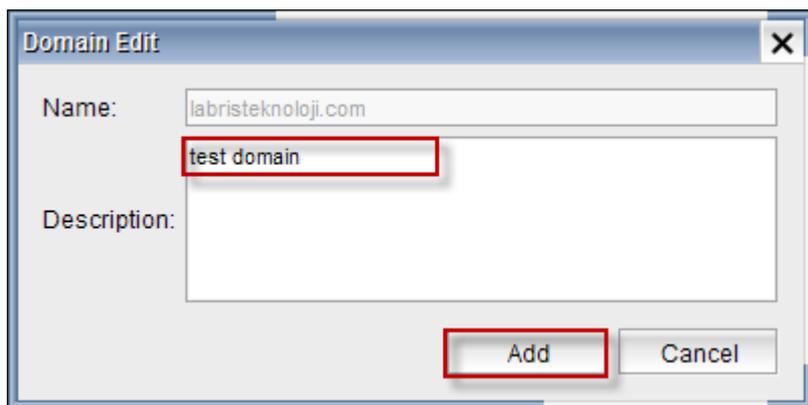
In the below screen, we can notice new Domain added.



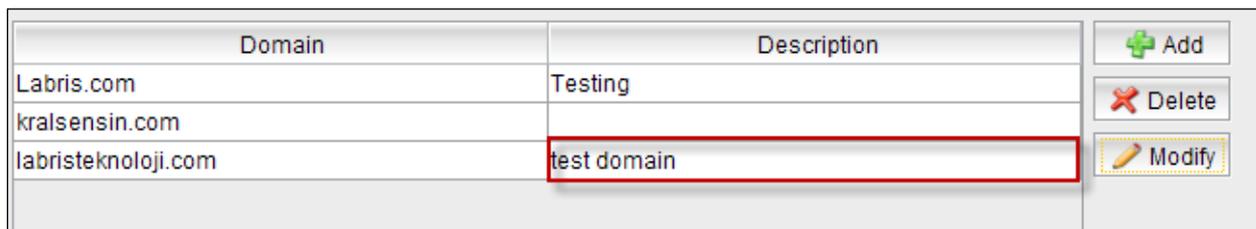
Click on **Modify** tab to make any changes to the Domain.



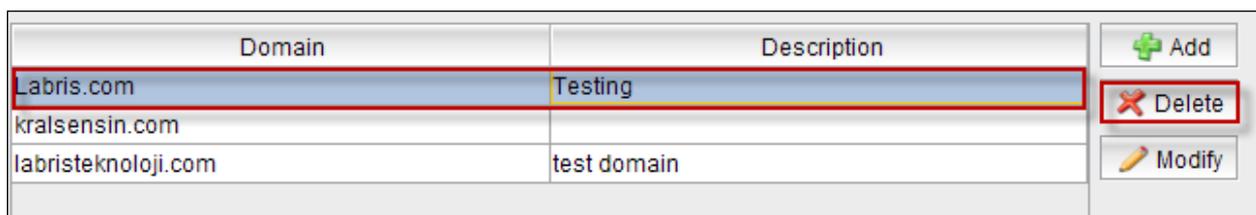
Domain Edit tab appears, we can modify Description of the Domain and click on **Add tab**.



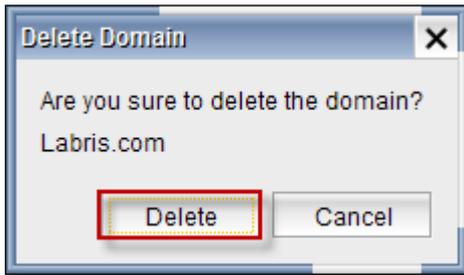
In the below screen, we can notice changes made to the Domain.



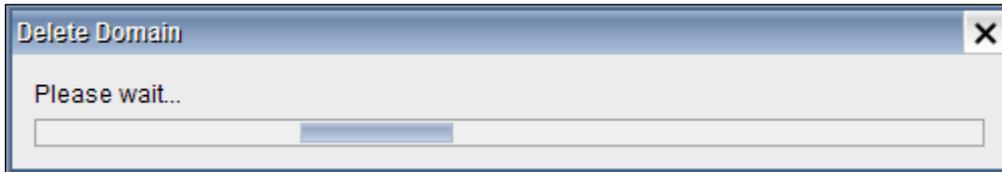
Select the Domain and click on **Delete tab**.



Delete Domain tab appears stating **Are you sure to delete the domain?** Click on **Delete tab**.



Below screen appears stating that Deleting Domain process is in progress.

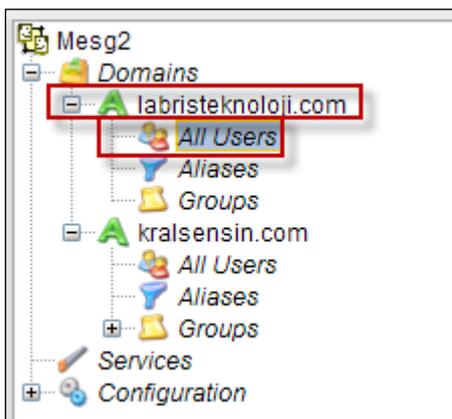


When we click on Domain in the right pane, details of that particular domain is displayed.



All Users

When we expand domain, we can find options like **All Users, Aliases, Groups**

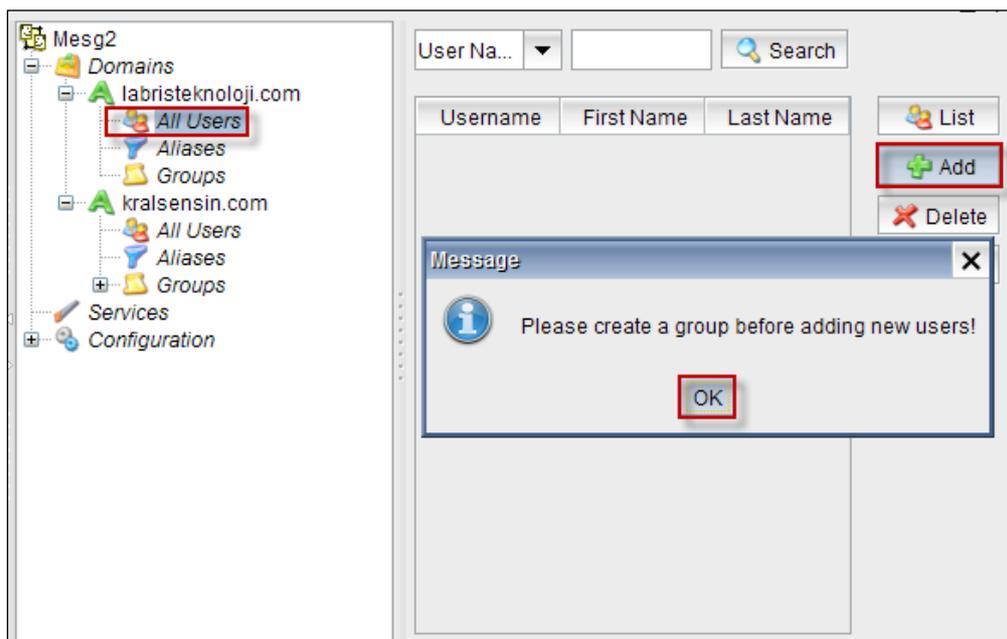


Select **All Users**, Click on **Add tab** to add new User.

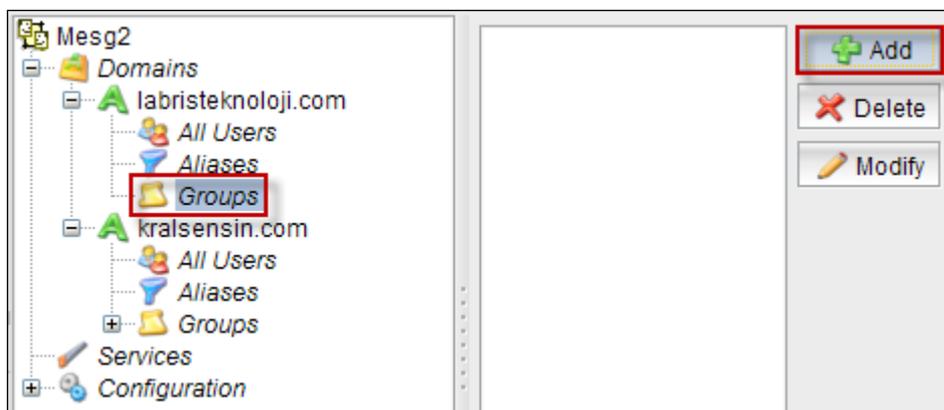
When we click on Add tab, Message is displayed stating **Please create a group before adding new users!**

Click **Ok**.

Before adding new user, we must create a Group in the domain.

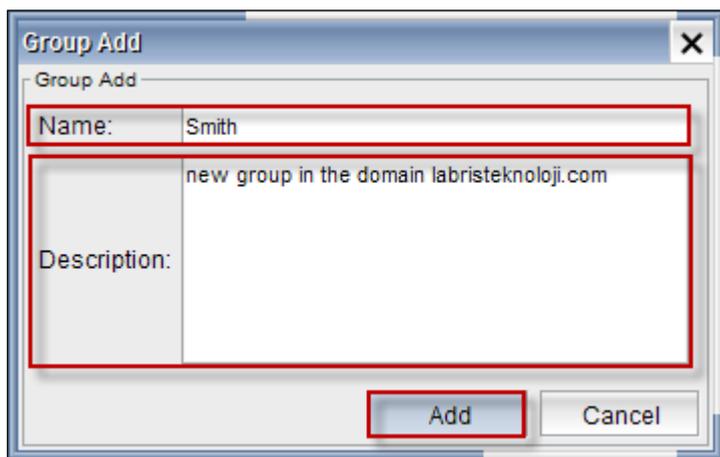


Select Groups and click on **Add tab**.

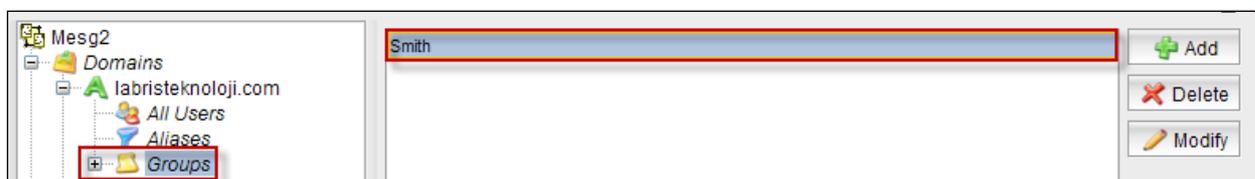


Group Add tab appears, Type the name of the Group and give the information regarding Group in the Description column.

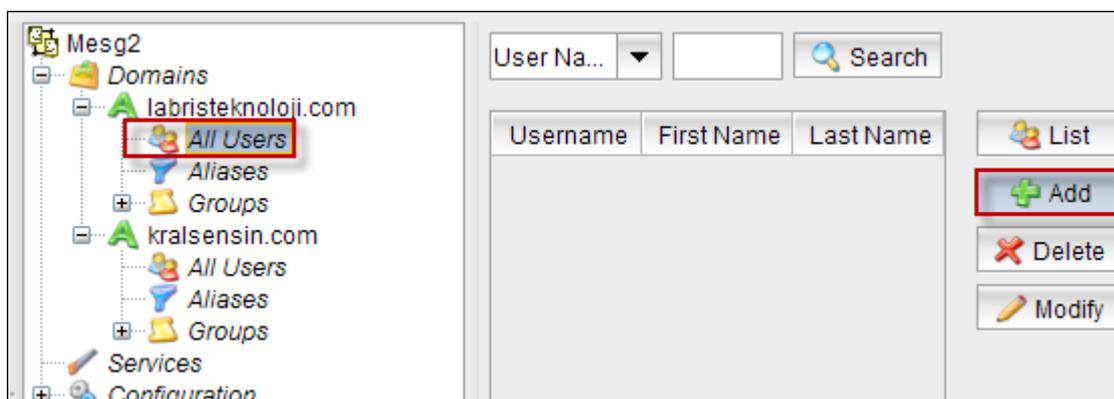
Click on **Add tab**.



In the below screen, we can notice new Group added to the Domain.



Now select All Users and click on **Add tab**.



Add New User tab appears.

The screenshot shows a dialog box titled "Add New User" with the following fields and values:

- User Name: James (1)
- First Name: William (2)
- Last Name: James (3)
- Title: SmithGroupUser (4)
- Group: Smith (5)
- Description: testuser (6)
- Employee Number: 030 (7)
- Telefon Number: 9959496730 (8)
- Alternative E-mail: James.William@rediff.com (9)
- Quota: Total Size: 30 (10), Number of emails: 2 (11)
- Forwarding: (12)
- Password: (13)
- Re-type Password: (14)

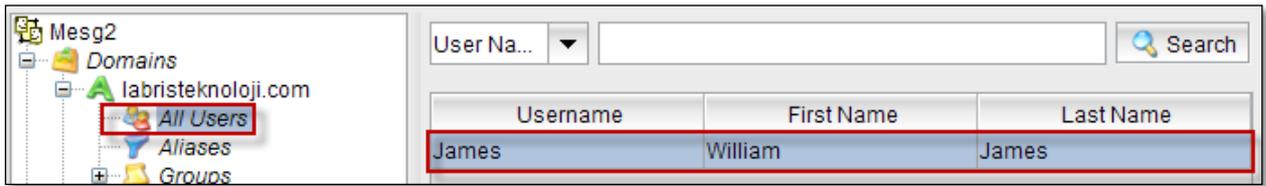
These are the inputs to add New User.

1	User Name	Type the User Name
2	First Name	Type the First Name
3	Last Name	Type the Last Name
4	Title	Give the Title of the User
5	Group	Choose Group from the drop down list
6	Description	Give the Description of the User
7	Employee Number	Type Employee Number
8	Telephone Number	Type the Telephone Number
9	Alternative E-mail	Give the Alternate E-mail Address
10	Total Size	Choose the required Size
11	Number of emails	Type the Number of emails
12	Forwarding	Give the Forwarding E-mail Address if necessary
13	Password	Give the Password for the User
14	Re-type Password	Re-type Password for Confirmation.

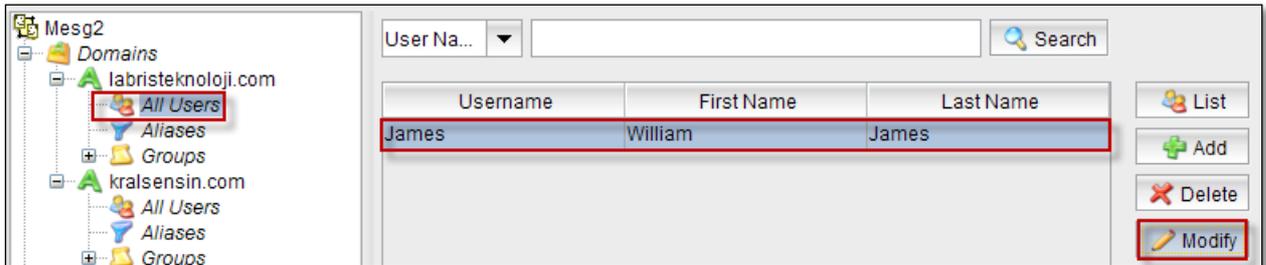
Adding User process is in progress.



In the below screen we can notice New User added to All Users.



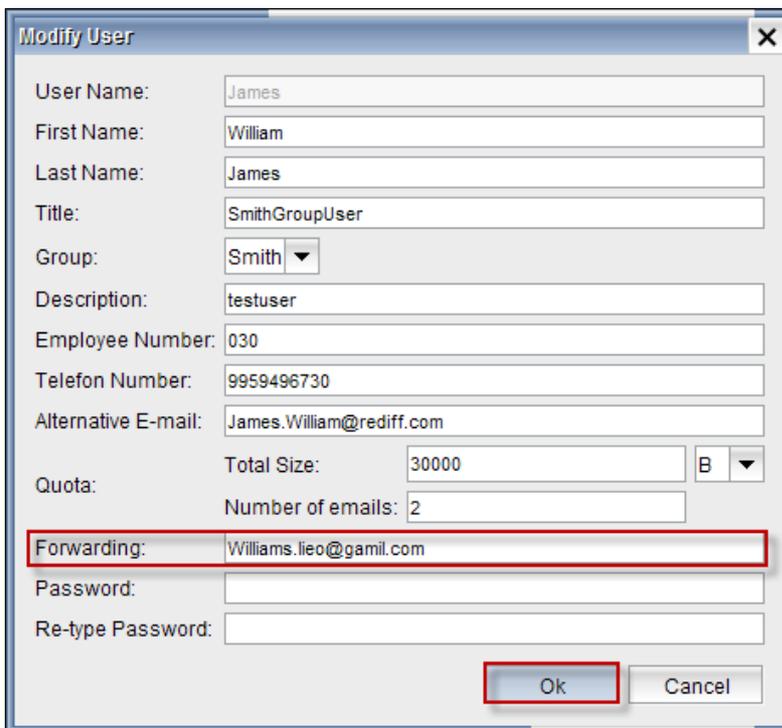
Select the User and click on **Modify** tab to make any changes to the User.



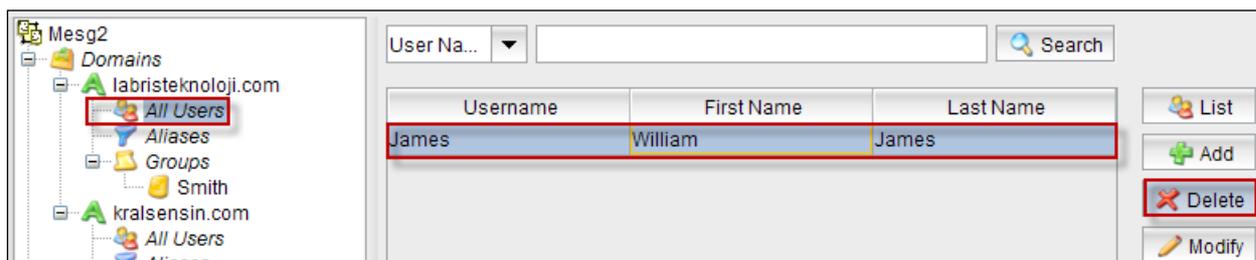
Modify User tab appears.

Except User Name all the remaining fields can be modified.

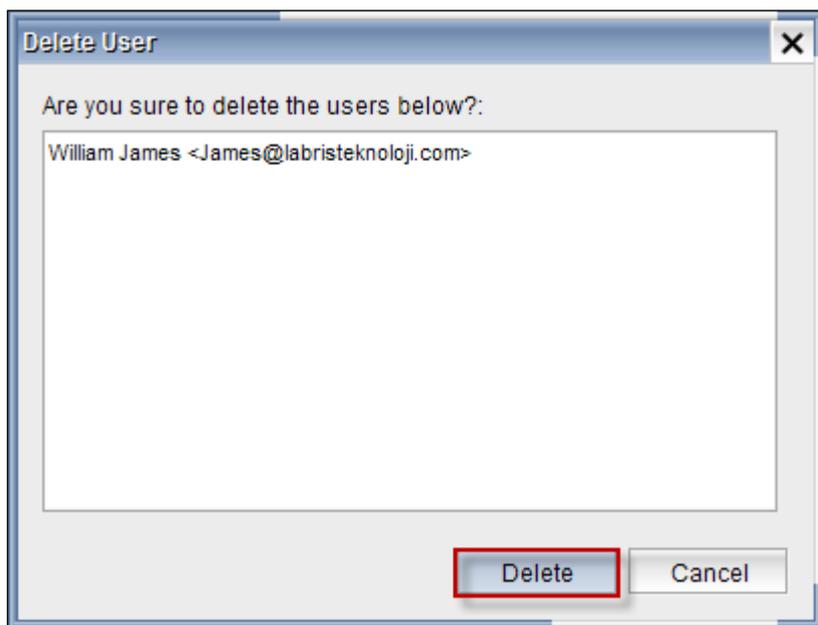
Click **Ok**.



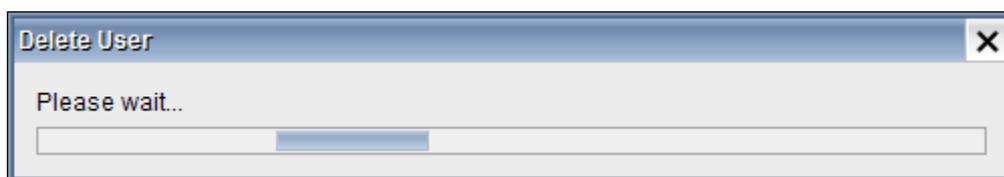
Select User and click on Delete tab to delete an User.



Delete User tab appears stating **Are you sure to delete the Users below?** Click on **Delete** tab.

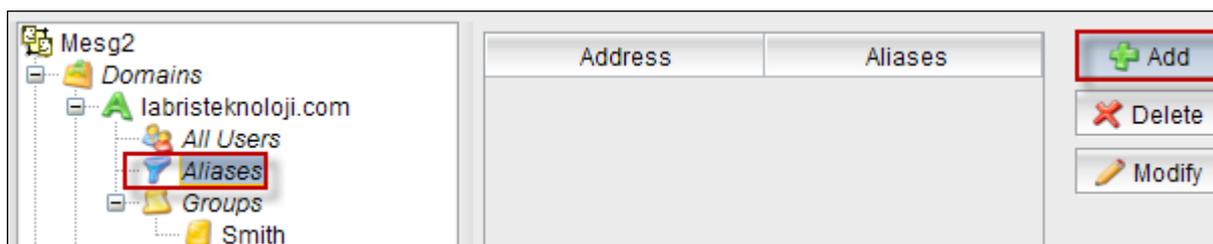


Deleting User process is in progress.



Aliases

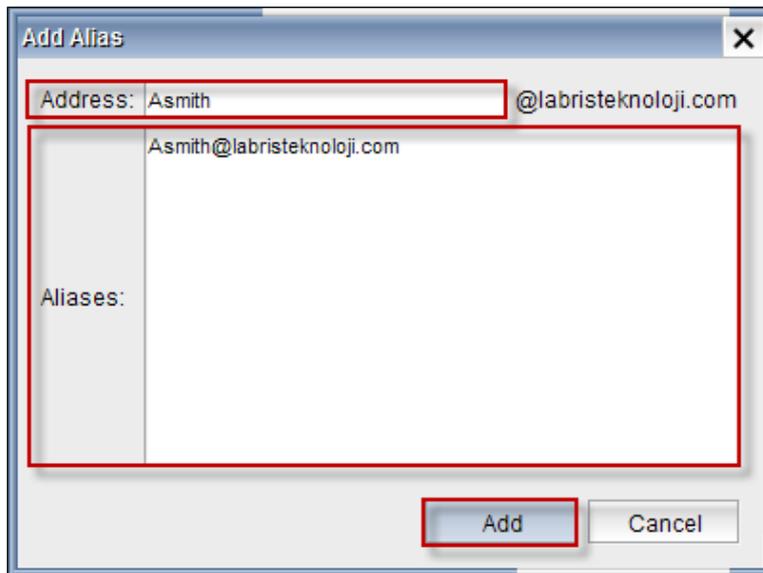
Select Aliases and click on **Add** tab.



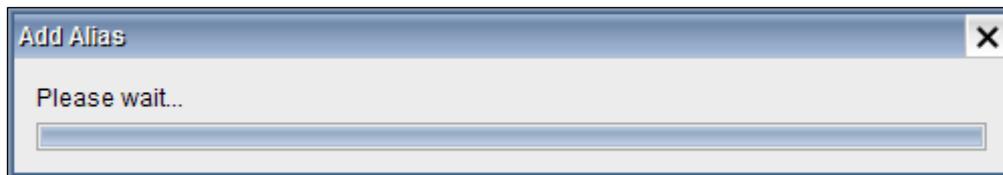
Add Aliases tab appears.

Type the Address and Aliases.

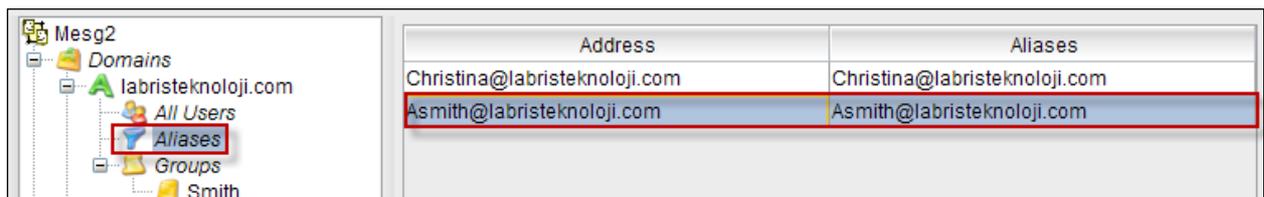
Click on **Add tab**.



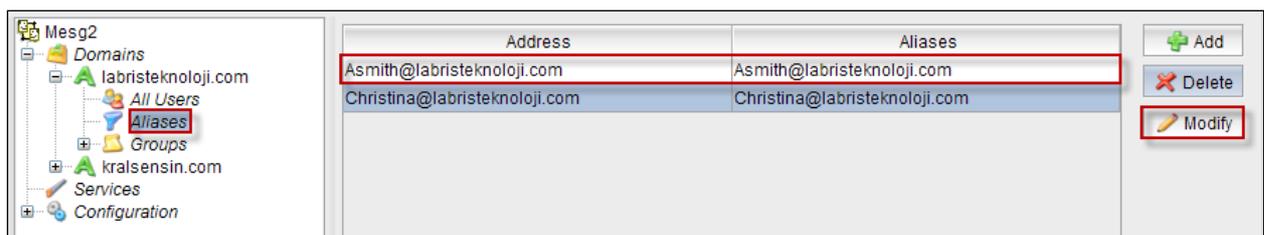
Adding Alias process is in progress.



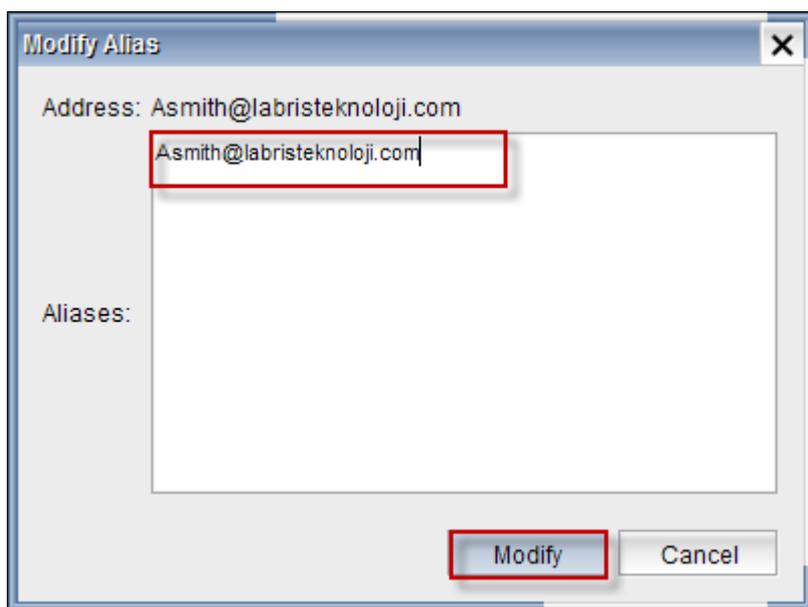
In the below screen, we can notice New Alias added.



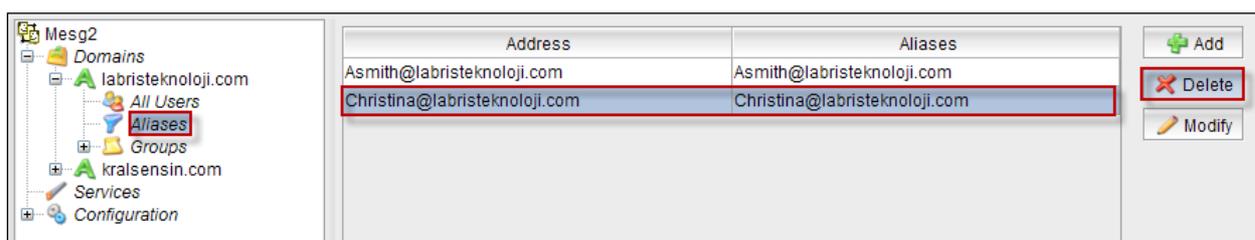
Select the Alias and click on **Modify tab** to make any changes t the Alias.



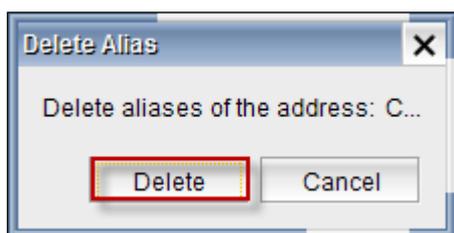
Modify Alias tab appears, we can modify Aliases column and click on **Modify**



Select the Alias and click on **Delete tab** to delete an Alias.



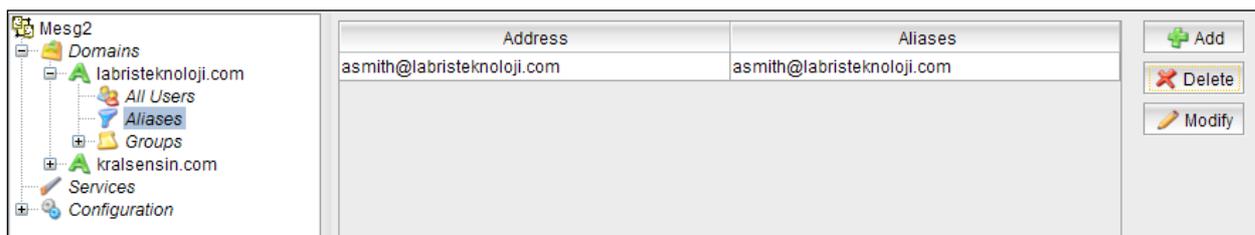
Delete Alias tab appears, click on **Delete**.



Deleting Alias process is in progress.



In the below screen, we can notice Aliases deleted.



Groups

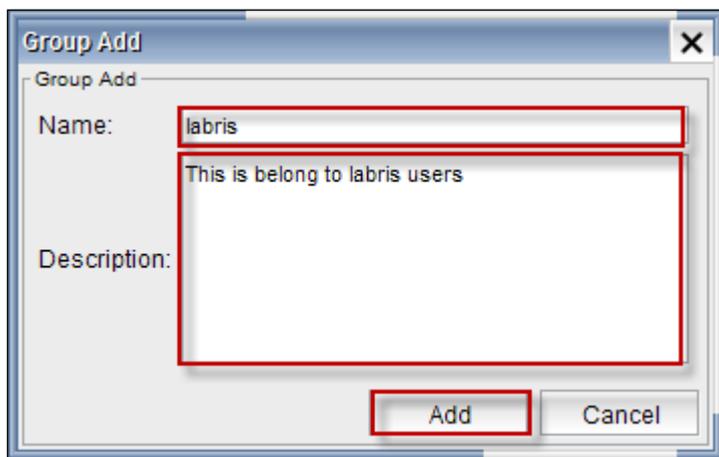
Select Groups and click on **Add tab**.



Group Add tab appears.

Type the Name of the Group and give information regarding Group in the Description column.

Click on **Add tab**.



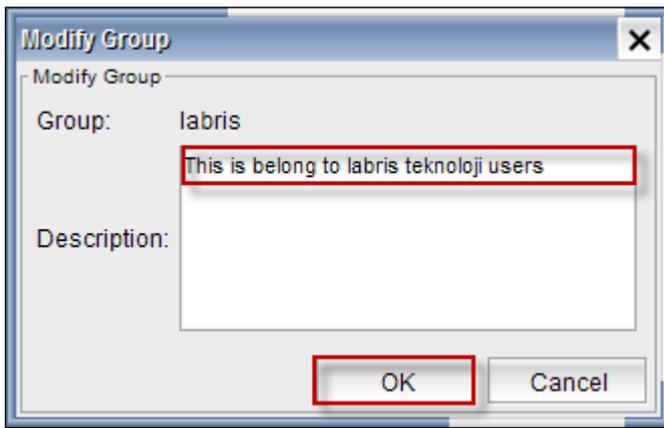
In the below screen, we can notice New Group added.



Select the Group and click on **Modify** tab.



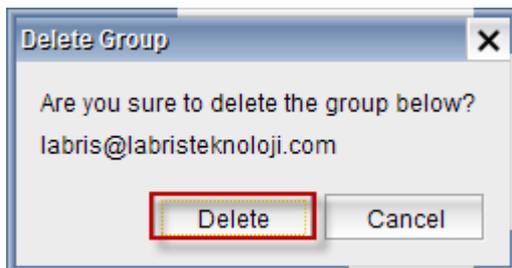
Modify Group tab appears ;we can modify Description of the Group and click **Ok**.



Select the Group and click on **Delete** tab.



Delete Group tab appears stating **Are you sure to delete the group below?** Click on **Delete** tab.



106. Services

Services help us to know the status of the Messaging. It also enables us to start, stop the Service.



Select Services and click on the highlighted icon to the stop Service.



Mesg2 tab appears stating **Stopping service, Please wait...**

Stopping services process is in progress.



In the below screen, we can notice **mes2 Service Status: Stopped**.



Select Services and click on the highlighted icon to the start the Service.



Mesg2 tab appears stating **Starting service, Please wait...**

Starting Services process is in progress.



In the below screen, we can notice **mes2 Service Status: Running**.

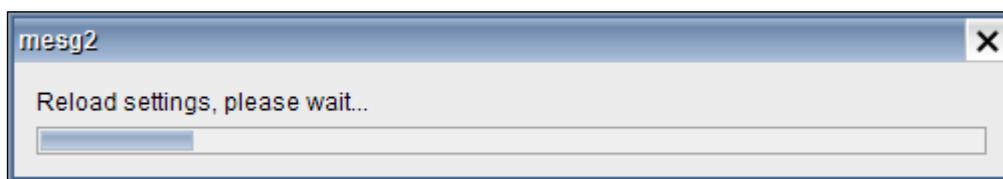


Select Services and click on the highlighted icon to the Reload Service.



Mesg2 tab appears stating **Reload settings, please wait...**

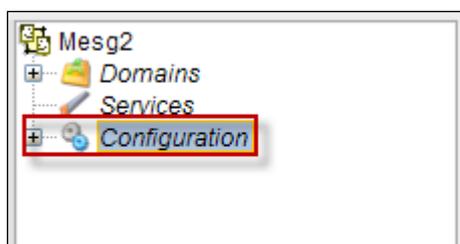
Reload settings process is in progress.



In the below screen, we can notice **mes2 Service Status: Reloaded**.



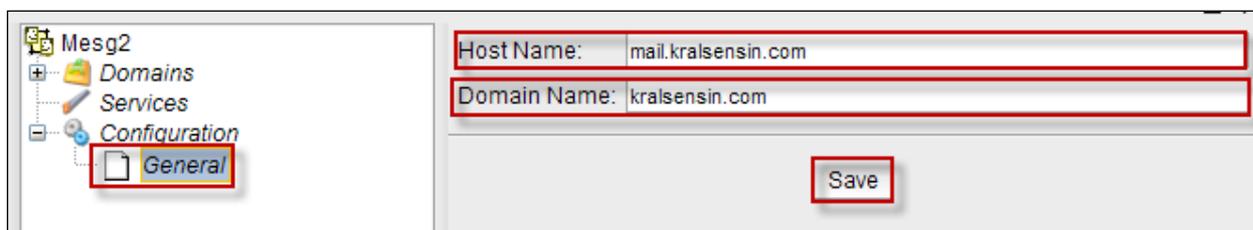
107. Configuration



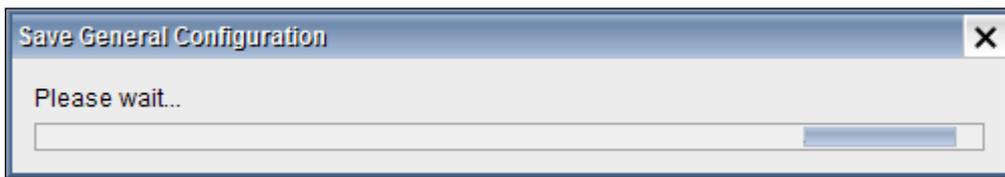
When we expand Configuration tab only General is displayed.

Click on **General** tab, Host Name and Domain Name are appeared.

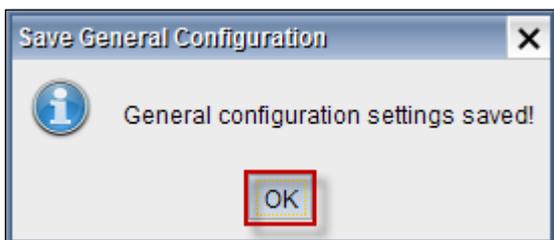
Click on **Save** tab.



Saving General Configuration process is in progress.

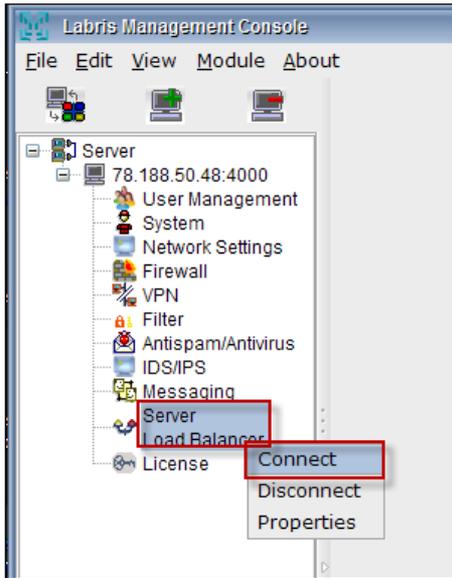


Below screen appears stating **General configuration settings saved**, Click **Ok**.

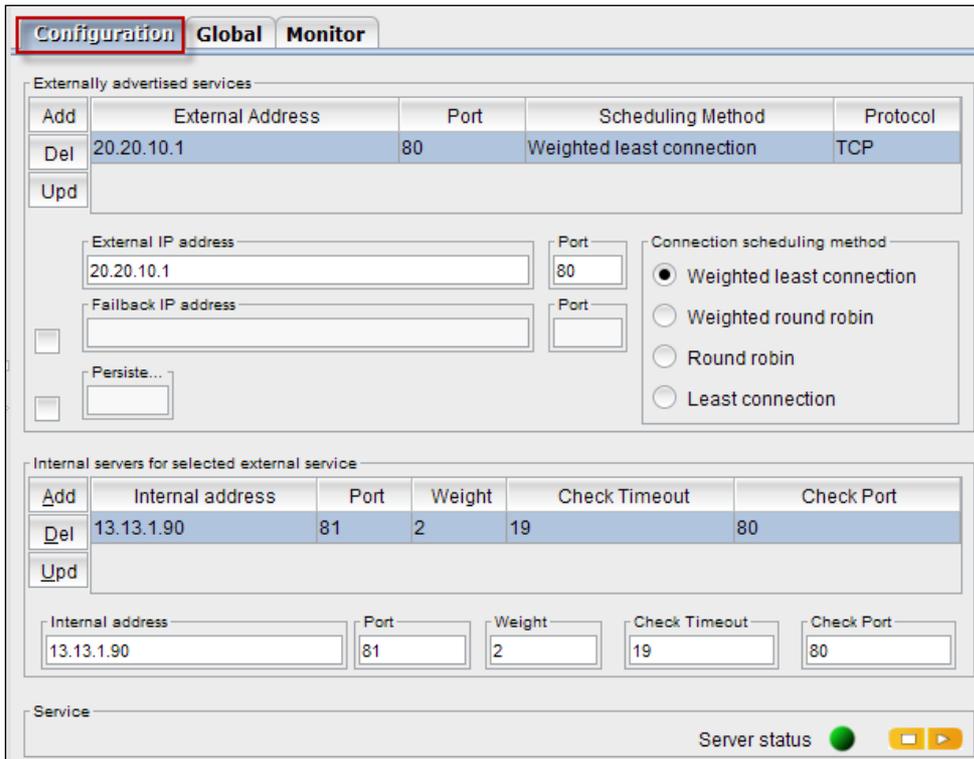


Load Balancer

Right click on Server Load Balancer, select **connect**.



When we get connected to Server Load Balancer below screen appears.



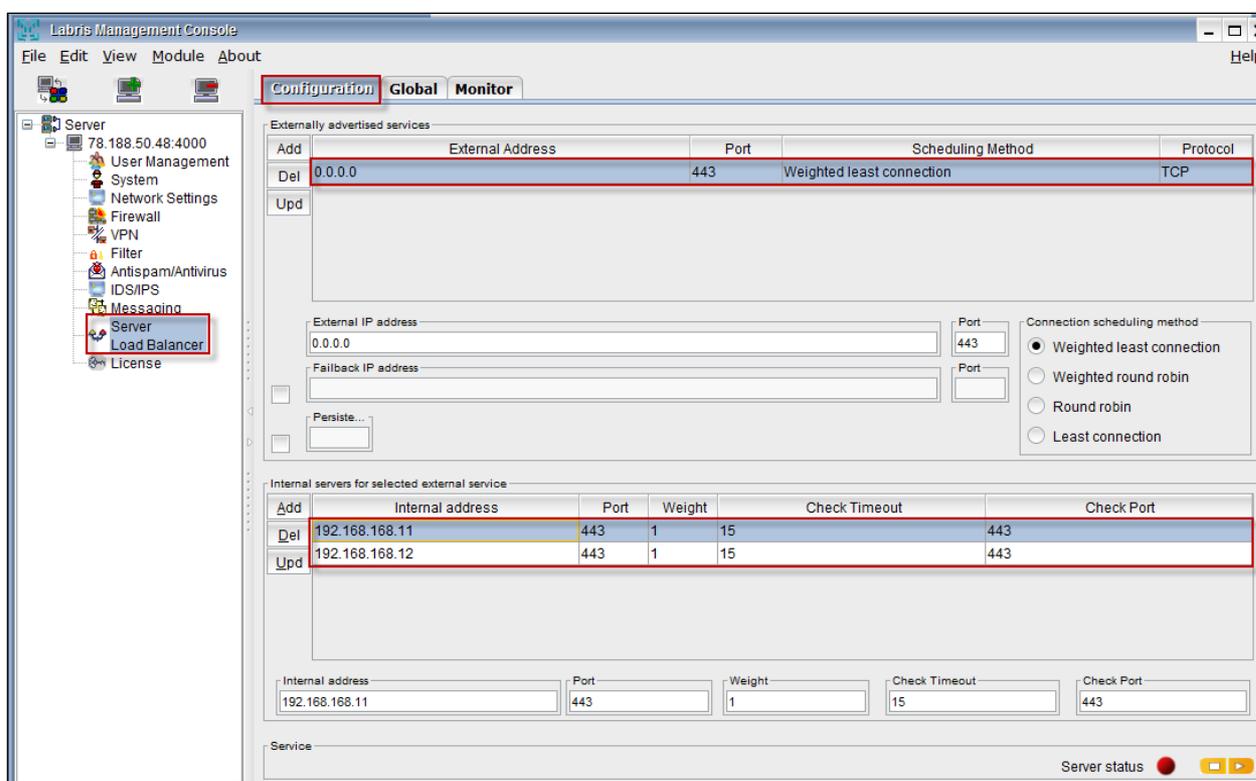
108. Configuration

Load balance service open to outside servers, outside-in line with the demands of a specified weight values is used to send the request packets to servers.

For example, there is a web site, and you experience performance issues on the server because of the intense traffic. In such cases, you can use the same web resources can come in a second web server and load balance property between the two servers can share a server densities according to the packages.

In the below screen, we can notice external source Address.

In the internal servers field we can find two piece of the same source files in the background using the server providing the same background via request packets on port 443, respectively one among them, is the intensity of the request packet weight.



Externally Advertised Services

It enables us to Add, Delete and Update Externally advertised services

The screenshot shows the 'Configuration' page with the 'Externally advertised services' section. A table lists the current service configuration:

	External Address	Port	Scheduling Method	Protocol
Del	0.0.0.0	80	Weighted round robin	TCP

Below the table are form fields for adding a new service:

- External IP address: 0.0.0.0
- Port: 80
- Failback IP address: (empty)
- Port: (empty)
- Persiste...: (empty)
- Connection scheduling method: Weighted round robin, Weighted least connection, Round robin, Least connection

To add new service.

Mention External IP address and its Port number.

Mention Failback IP address and its Port number.

Choose the type of the Connection scheduling method and enter Persiste value.

After providing all the inputs, click on **Add** tab.

The screenshot shows the 'Configuration' page with the 'Externally advertised services' section. The 'Add' button is highlighted in red. The table now shows the updated service configuration:

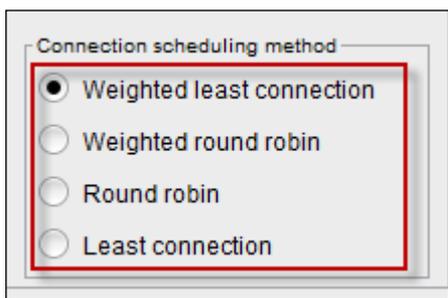
	External Address	Port	Scheduling Method	Protocol
Del	0.0.0.0	80	Weighted round robin	TCP

Below the table are form fields for adding a new service:

- External IP address: 11.11.11.1
- Port: 80
- Failback IP address: 10.10.10.1
- Port: 80
- Persiste...: 5
- Connection scheduling method: Weighted least connection, Weighted round robin, Round robin, Least connection

Connection scheduling methods

These are four types of server load balancing methods which are also known as “scheduling methods” or “algorithms”.



Round Robin

Round Robin is one of load balancing algorithm. It maintains a list of servers and forwards a new connection to the next server in the member list. Round robin is simple and effective method of distribution. This method functions best if all the servers have similar resource capacity.

Weighted Round Robin

The weighted Round robin algorithm maintains a weighted list of servers and forwards new connections in proportion to the weight of each server.

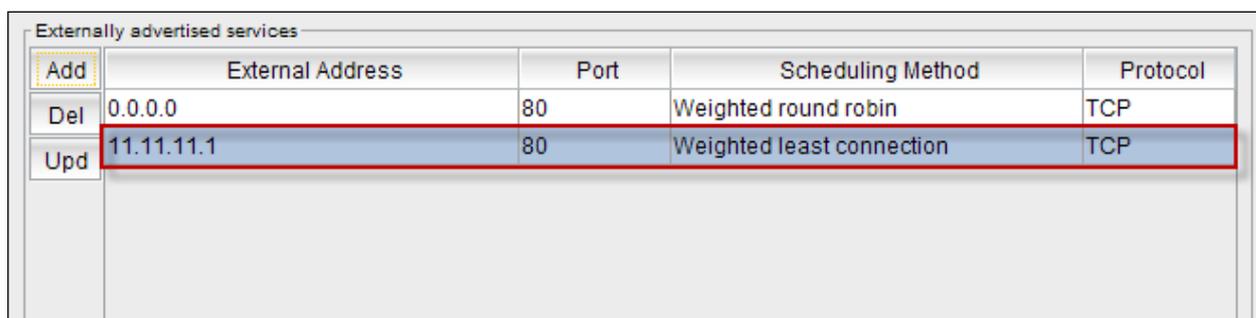
Least connection

Least Connection is one of load balancing algorithm. This Algorithm maintains a record of active server connections and forwards a new connection to the server with least number of active connections. Least connection method functions best in environments where the servers have similar capabilities.

Weighted Least connection

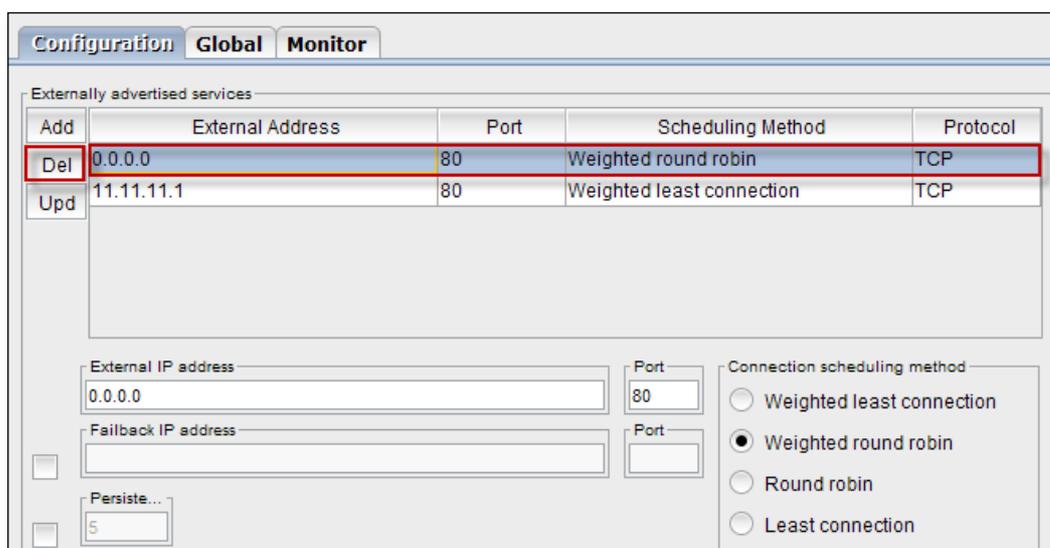
The weighted least connection algorithm maintains a weighted list of application servers with their number of active connections and forwards a new connection to an application server based on a combination of its proportion to the weight and number of active connections. Like the least connections methods, these load balancing methods select pool members or nodes based on the number of active connections. This method work best in environments where the servers have different capacities.

In the below screen, we can notice New service added.



	External Address	Port	Scheduling Method	Protocol
Add				
Del	0.0.0.0	80	Weighted round robin	TCP
Upd	11.11.11.1	80	Weighted least connection	TCP

Select the service and click on **Delete tab**.



Configuration Global Monitor

Externally advertised services

Add	External Address	Port	Scheduling Method	Protocol
Del	0.0.0.0	80	Weighted round robin	TCP
Upd	11.11.11.1	80	Weighted least connection	TCP

External IP address: 0.0.0.0 Port: 80

Failback IP address: Port:

Persiste...: 5

Connection scheduling method:

- Weighted least connection
- Weighted round robin
- Round robin
- Least connection

To Update the service, Select the service.

We can modify External IP address and its port number, Connection scheduling method type.
After making necessary changes, Click on **Update** tab.

Configuration Global Monitor

Externally advertised services

Add	External Address	Port	Scheduling Method	Protocol
Del	11.11.11.1	80	Weighted least connection	TCP

Upd

External IP address: 20.20.10.1 Port: 80

Failback IP address: Port:

Persiste...: 5

Connection scheduling method:

- Weighted least connection
- Weighted round robin
- Round robin
- Least connection

In the below screen, we can notice Updated server.

Externally advertised services

Add	External Address	Port	Scheduling Method	Protocol
Del	20.20.10.1	80	Weighted least connection	TCP

Upd

Internal Servers for Selected External Service

Internal Address

It enables us to Add, Delete and Update Inter server for selected external service.

Internal servers for selected external service

Add	Internal address	Port	Weight	Check Timeout	Check Port
-----	------------------	------	--------	---------------	------------

Del

Upd

Internal address: Port: Weight: Check Timeout: Check Port:

To add Internal server.

Mention Internal address, port number, weight, Check timeout and Check port.

After providing all inputs click on **Add** tab.

Internal servers for selected external service

	Internal address	Port	Weight	Check Timeout	Check Port
Add					
Del					
Upd					

Internal address: 192.168.10.5 Port: 80 Weight: 22 Check Timeout: 12 Check Port: 80

In the below screen, we can notice Internal server added.

Internal servers for selected external service

	Internal address	Port	Weight	Check Timeout	Check Port
Add					
Del	192.168.10.5	80	22	12	80
Upd					

Select the server and click on **Delete** tab.

Internal servers for selected external service

	Internal address	Port	Weight	Check Timeout	Check Port
Add					
Del	192.168.10.5	80	22	12	80
Upd	10.10.0.1	81	1	20	81

Internal address: 10.10.0.1 Port: 81 Weight: 1 Check Timeout: 20 Check Port: 81

To Update the server, Select the server.

We can modify internal IP address, Port, Weight, Check Timeout and Check Port.

After making necessary changes, Click on **Update** tab.

Internal servers for selected external service

Add	Internal address	Port	Weight	Check Timeout	Check Port
Del	192.168.10.5	80	22	12	80

Upd

Internal address: 13.13.1.90 Port: 81 Weight: 2 Check Timeout: 19 Check Port: 80

In the below screen, we can notice Updated server.

Internal servers for selected external service

Add	Internal address	Port	Weight	Check Timeout	Check Port
Del	13.13.1.90	81	2	19	80

Upd

Service

Service tab enables us to know the status of the service.

Service

Server status ●  

Click on the highlighted icon to stop the service.

Service

Server status ●  

In the below screen, we can notice Red color status which indicates Server stopped.

Service

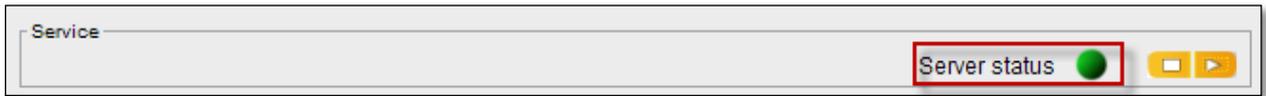
Server status ●  

Click on the highlighted icon to start the service.

Service

Server status ●  

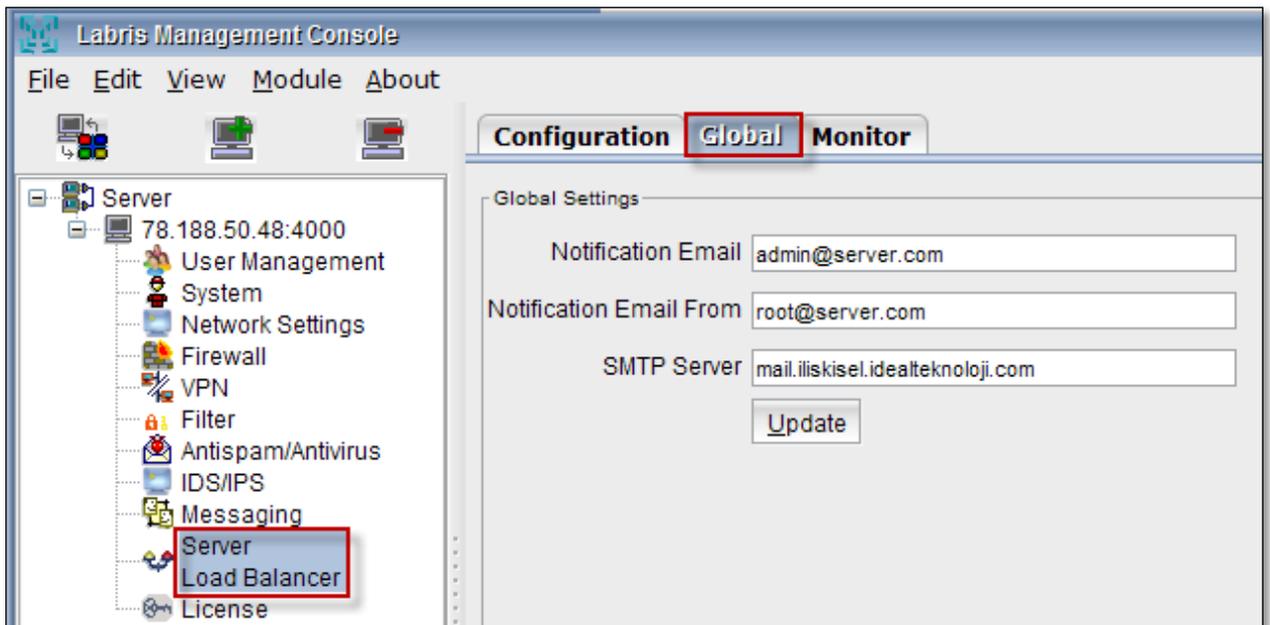
In the below screen, we can notice Green color status which indicates Server stopped.



109. Global

Global Settings

Click on **Global** tab.



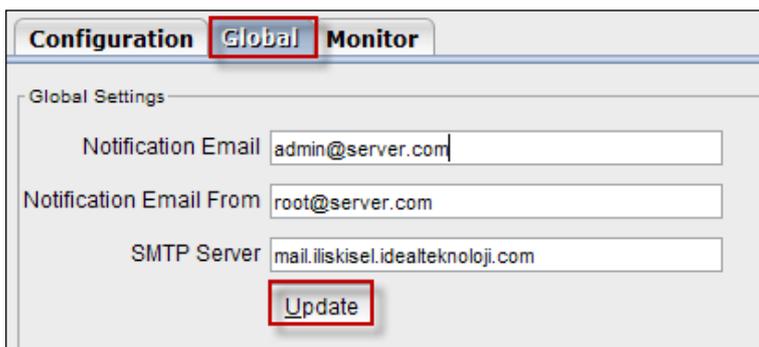
It enables us to view and change the Global Settings.



These are the inputs for **Global**.

1	Notification Email	Give the Notification Email address
2	Notification Email From	Give the From address Notification Email
3	SMTO Server	Give the SMTO Server address

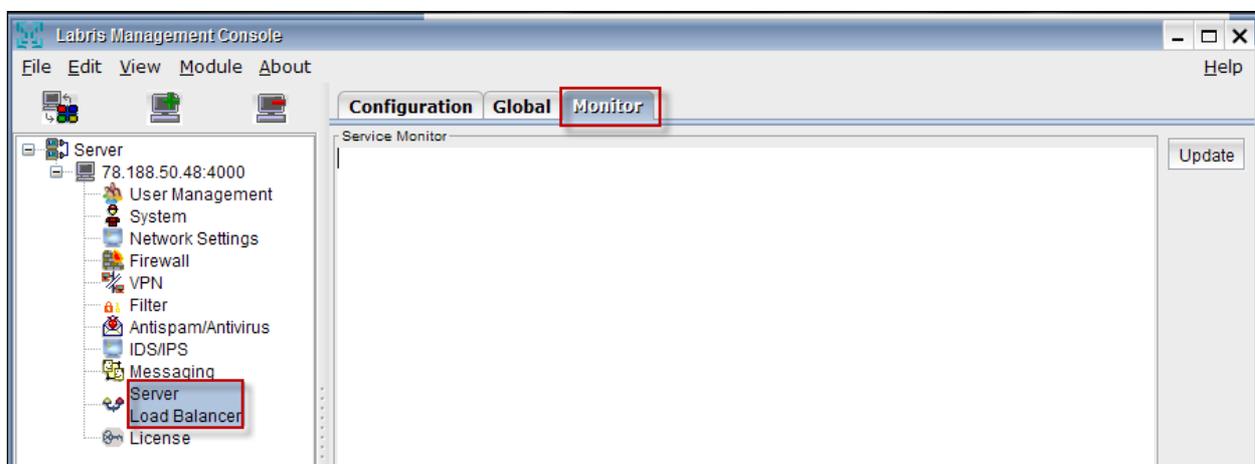
Click on **Update** tab.



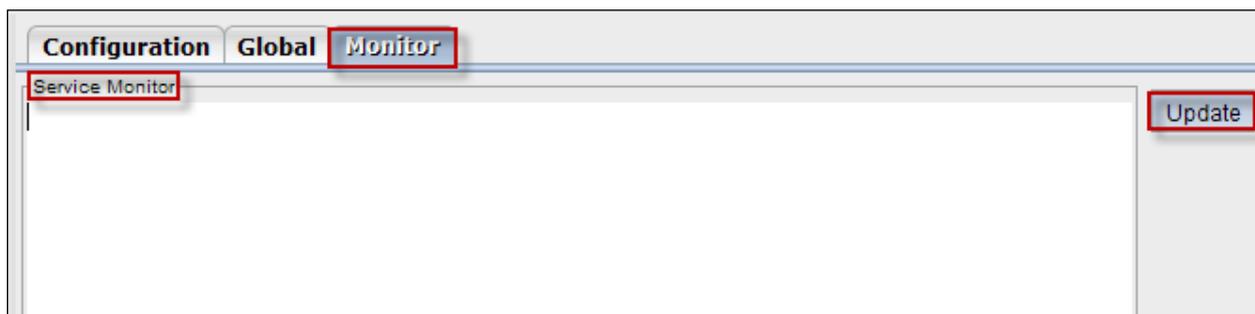
110. Monitor

Service Monitor

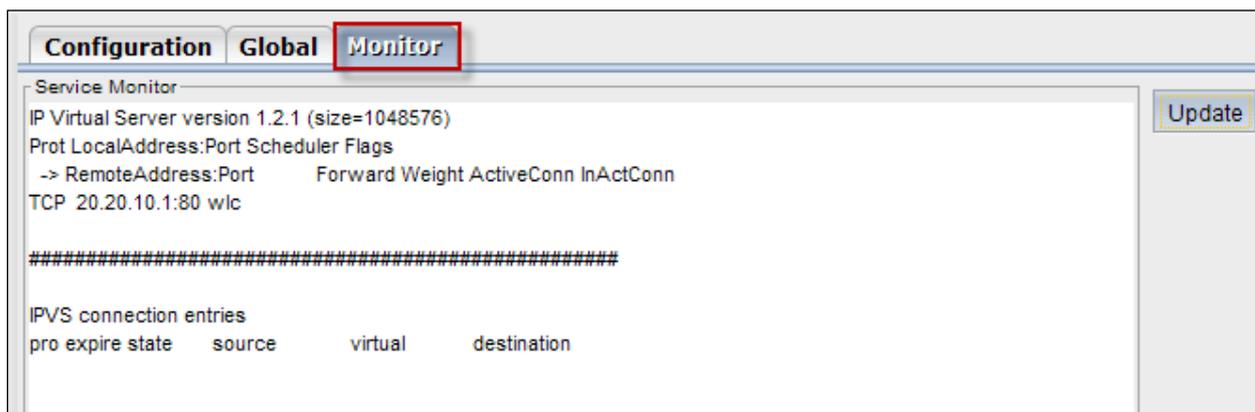
Select **Monitor** tab



Click on **Update** tab to update the information

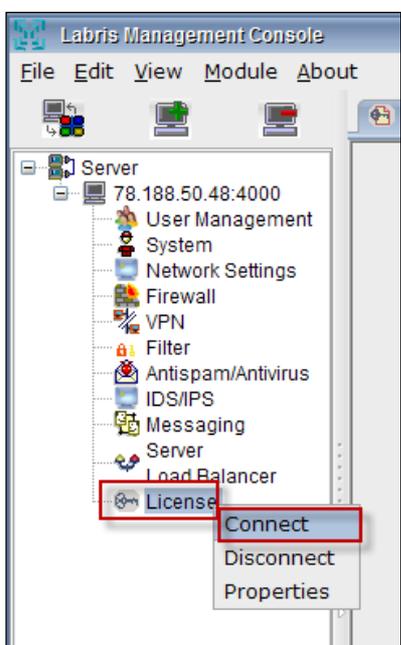


You can notice that information is updated in this tab



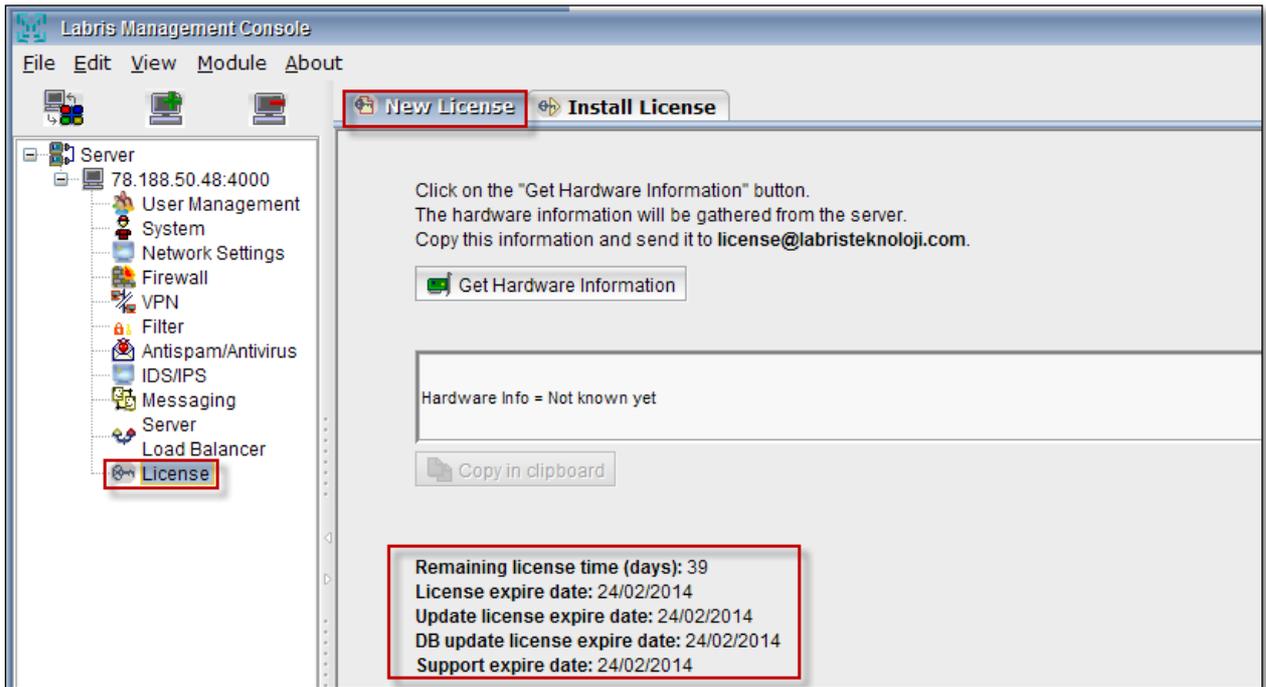
License

Right click on License and select **connect**.

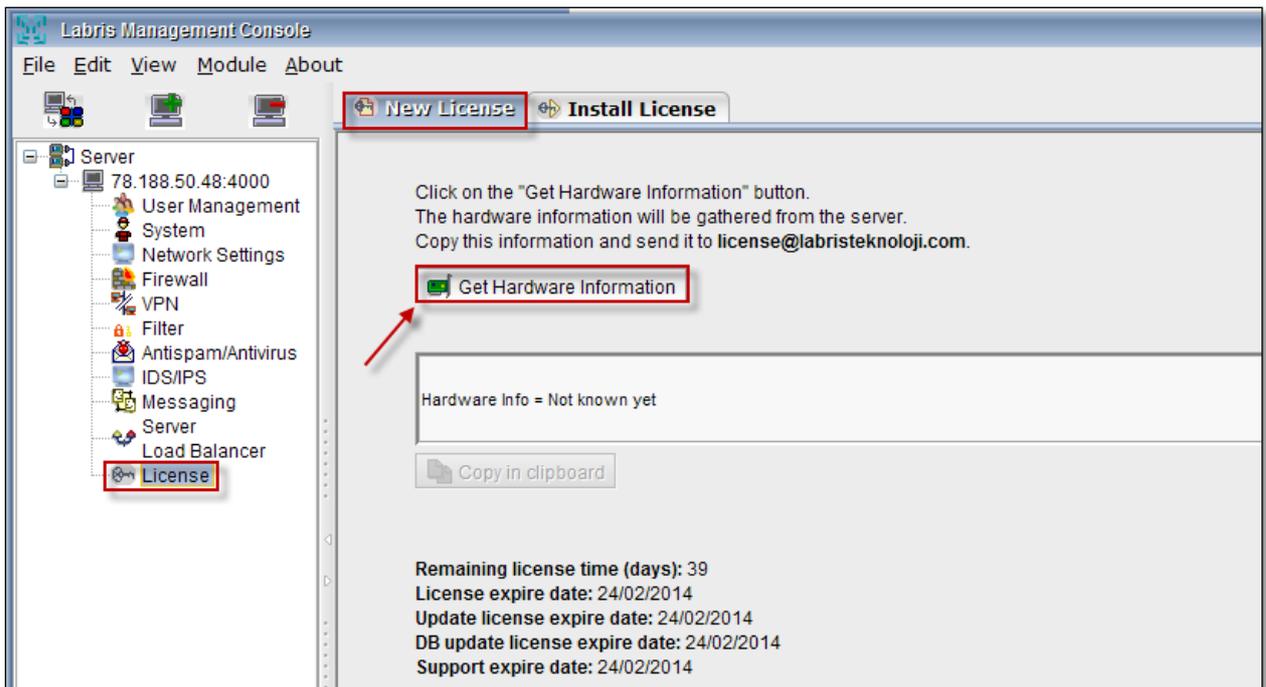


New License

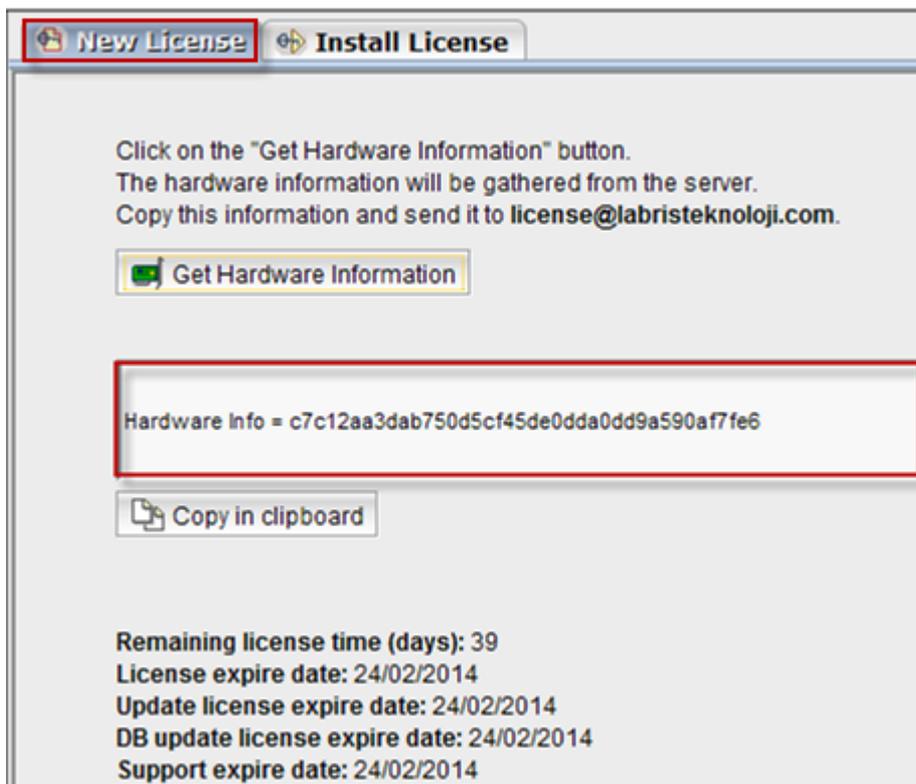
Click on **New License**, Information regarding License is being displayed.



Click on **Get Hardware Information** button.



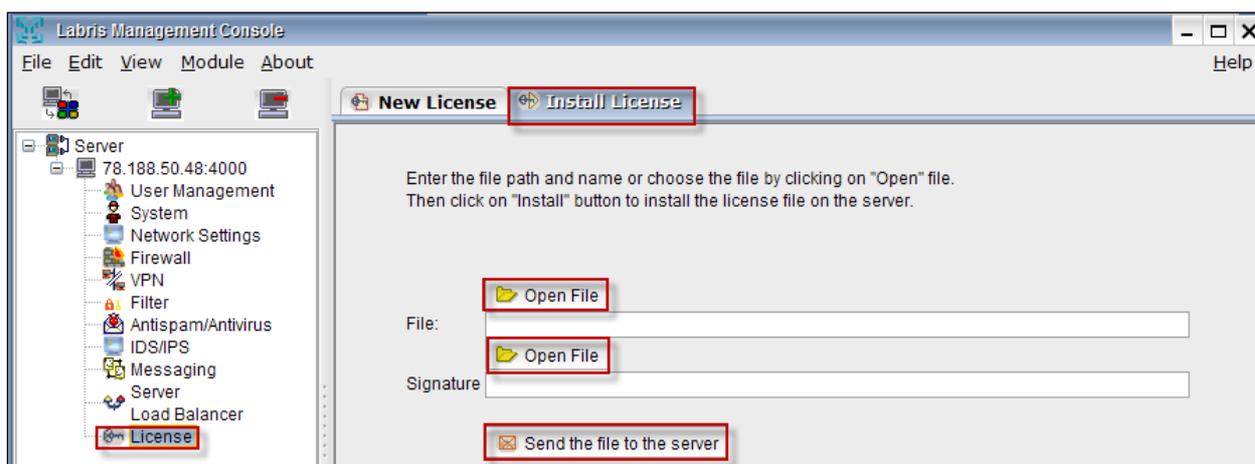
In the below screen, we can notice **Hardware Information** gathered from server is displayed.



Install License

Enter file name or choose **Open file** if we have a license file.

Signature of the file should be mentioned or choose **Open file** if we have a Signature and click on **Send the file to the server**.



Note

For License file, please request from the service provider.

111. Glossary

DHCP	Dynamic Host Configuration Protocol
DNAT	Destination Network Address Translation
DNS	Domain Name System
DOS	Denial of service
DDOS	Distributed Denial of service
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
LMC	Labris Management Console
L2TP	Layer 2 Tunneling Protocol
MIME	Multi Purpose Internet Mail Extensions
NAT	Network Address Translation
PAT	Port Address Translation
QOS	Quality of service
SNAT	Secure Network Address Translation
SSL VPN	Secure Socket Layer Virtual Private Network
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTM	Unified Threat Management
VPN	Virtual Private Network
WAN	Wide Area Network
WAUTH	Wireless Authentication

112. Labris Firewall Messages

lfp DROP IN ethN OTHER SRC	Blocking occurred because the source address of the packets incoming from an interface which is defined as external interface overlaps with either the network address of an internal interface or the internal networks defined under this internal interface.
lfp DROP IN ethN 127.x SRC	Blocking occurred because the source address of a packet incoming from external interface belongs to 127.0.0.0/8 network.
lfp DROP IN ethN BCAST SRC	Blocking occurred because the source address of a packet incoming from external interface belongs to Broadcast type.
lfp DROP IN ethN BCAST PKT	Blocking occurred because the packet type of a packet incoming from external interface is Broadcast.
lfp DROP IN MNG FWD	The packet forwarding process is blocked because the relevant interface has been defined as management interface.
lfp DROP OUT MNG FWD	The packet forwarding process is blocked because the relevant interface has been defined as management interface.
lfp DROP IN MNG LMCS	Access to LMCS service port numbered 4000 from an interface except Management Interface is blocked.

lfp DROP OUT MNG LMCS	Response access from LMCS service port numbered 4000 towards an interface except Management Interface is blocked.
lfp DROP IN MNG WEB	Access to LRMS service port numbered 81 from an interface except Management Interface is blocked.
lfp DROP OUT MNG WEB	Response access from LRMS service port numbered 81 towards an interface except Management Interface is blocked.
lfp DROP IN MNG SSH	Access to SSH service port numbered 22 from an interface except Management Interface is blocked.
lfp DROP OUT MNG SSH	Response access from SSH service port numbered 22 towards an interface except Management Interface is blocked.
lfp DROP IN MNG IF	A management request connection which does not have management permission is blocked.
lfp DROP OUT MNG IF	Response to a management request connection which does not have management permission is blocked.
lfp DROP IN CONSOLE	Access to management ports is blocked.
lfp DROP OUT CONSOLE	Access response from management ports is blocked.
lfp DROP IN IF BAD SRCIP	Blocking occurred because the source address of the packets incoming from the relevant internal interface does not overlap with neither the network address of the internal interface nor the internal networks defined under this internal interface.
lfp DROP IN ethN OWN SRCIP	B locking is done because the source address of the packet incoming from any overlaps with the IP address of one of the interfaces defined on the device.
lfp DROP ICMP DoS	ICMP: Blocking occurred due to fragment or invalid session state.
lfp DROP TCP DoS	TCP: Blocking occurred due to fragment or invalid session state.
lfp DROP UDP DoS	UDP: Blocking occurred due to fragment or invalid session state.
lfp DROP TCP Scan	TCP: Packets which are coming with scanning purpose and have packet flags which are expected to be absent normally, are blocked. FIN,URG,PSH / ALL SYN,RST,ACK,FIN,URG / ALL NONE / ALL ALL / ALL FIN / ALL SYN,RST / SYN,RST SYN,RST / SYN,RST tcp-option 64 tcp-option 128

lfp DROP FRAG Scan	TCP Fragment Scan: Packets which are coming with scanning purpose and have packet flags which are expected to be absent normally, are blocked. FIN,URG,PSH / ALL SYN,RST,ACK,FIN,URG / ALL NONE / ALL ALL / ALL FIN / ALL SYN,RST / SYN,RST SYN,RST / SYN,RST tcp-option 64 tcp-option 128
lfp DROP SESSIONLESS PKT	Communication packets coming with a purpose other than opening session although there's no session are blocked.
lfp DROP PKT Too small	UDP, TCP, ICMP packets which are smaller than they should be are blocked.
lfp DROP LRMS Abuse	Extremely fast connection request to LRMS management service port is blocked.
lfp DROP SSH Abuse	Extremely fast connection request to SSH management service port is blocked.
lfp DROP WAUTH INPUT	Packets belonging to an unauthorized IP although WAUTH is active are blocked.
lfp DROP WAUTH FORWARD	Packets belonging to an unauthorized IP although WAUTH is active are blocked.
lfp DROP Default	Packets are blocked with the predefined blocking rule running after all the rules added by the user.
lfp Default --DENY	Packets are blocked with the predefined blocking rule running after all the rules added by the user.
lfp Default_ ethN -- DENY	Packets are blocked with the predefined blocking rule running after all the rules added by the user.
lfp Rule NNN -- ACCEPT	Permitted with the rule numbered NNN defined through LMC.
lfp Rule NNN -- DROP	Blocked with the rule numbered NNN defined through LMC.
lfp Rule NNN -- REJECT	Actively rejected with the rule numbered NNN defined through LMC.
lfp Rule NNN -- LOG	Only logged with the rule numbered NNN defined through LMC, no other process is performed.
lfp USER DEFINED PREFIX:	Logged with "USER DEFINED PREFIX" name specified by system administrator in a rule defined through LMC. ACCEPT, DROP state shall be specified by user.

lfp IPMAC_MAXCONN:	Blocking occurred because the maximum number of connections assigned per IP is exceeded.
lfp IPMAC_ABUSE	Blocking occurred because of contrary situation to IP-MAC mapping rules.
lfp i PROXYCONNLIMIT_DROP	Blocking occurred because number of sessions limit from internal clients to proxy system on the device is exceeded.
lfp i FLOODCONTROL_DROP: _lfp_ f FLOODCONTROL_DROP	Temporary blocking occurred because an internal client exceeded the connection limits to a single destination.
lfp i CLIENTFLOOD_DROP: _lfp_ f CLIENTFLOOD_DROP:	Temporary blocking occurred because an internal client exceeded the defined packet speed limits.
lfp i CONNLIMIT_DROP: _lfp_ f CONNLIMIT_DROP:	Temporary blocking occurred because an internal client exceeded the defined number of sessions limits.

2013.7.31-3:33:12 USER IP URL *EXCEPTION* You_have_privileged_username. GET 0 0 - 2 304 - GRUP - TCP_MISS/304 13 DEFAULT_PARENT/127.0.0.1	URL is permitted.
SCANNED POST	A sent web POST request is scanned and permitted. Blocking occurred because the source address of a packet incoming from external interface belongs to 127.0.0.0/8 network.
CONTENTMOD GET	The incoming content is replaced with regular expressions.
URLMOD GET	The outgoing request URL is replaced with regular expressions. For example with the purpose of forcing to Safe Search
DENIED Banned_file_extension:_.exe GET 0 0 Banned extension	Access is blocked due to a banned file extension (exe)
*DENIED*Banned_Site:_facebook.com GET	Access is blocked due to a banned site.
DENIED Banned_URL:_adfarm.mediaplex.com/ad GET	Access is blocked due to a banned URL.

DENIED Banned_MIME_Type:_video/mp4 GET 0 0 Banned MIME Type	Video (mp4) content is blocked due to a banned MIME Type.
*EXCEPTION*You_have_accessed_to_a_privileged_site. GET	Access permission is given to a site that is added to exceptions.
*DENIED*Banned_irregular_expression_(URL)	Blocking occurred because URL matched with a blocked pattern.
*SCANNED**DENIED*Limit_of_blocked_expressions_is_exceeded:_50 _	Blocking occurred because web page content contains blocked expressions above the limit.
*SCANNED**DENIED*Banned_words_are_found	Blocking occurred because banned words are found in the web page content.

1. Labris Logview User Guide

1. Introduction

Labris Logview is a project which aims to make monitoring the system wide logs easier to system admins. User can see all logs for entire:

1	Firewall	Firewall Network Logs View
2	Access	Access Logs View
3	Operational	Operational Logs View
4	Administrative	Administrative Logs View
5	Wireless Authentication	Wireless Authentication Logs View
6	IPMAC	IPMAC Logs View
7	DHCP	DHCP Logs View

system sources.

Logview allows user to define different log sources and regarding columns. Users can easily access new logs via “Live Monitoring” and reach older records for a given date range.

The screenshot displays the Labris Logview interface with the 'FIREWALL LOGS' table selected. The table contains the following columns: Date / Time, Source, Source User, Source Port, Destination, Destination User, Rule, Action, Protocol, Application, and Mac Address. The data shows various network events, including accepted and dropped connections, with specific details on source and destination IP addresses, ports, and the rules applied.

Logview Records table while streaming with some sample logs

The screenshot displays the Labris Logview interface with the 'ACCESS LOGS' table selected. The table contains the following columns: Date / Time, User, Source, Mac Address, Destination, URL, Decision, HITNESS, and Category. The data shows a series of access attempts, all of which were 'SCANNED' and resulted in a 'TCP_DENIED403' status, indicating blocked access to various URLs.

Figure Logview records table with some historical logs

2. Parts & Tools

Logview has some easy-to-use parts and useful tools:

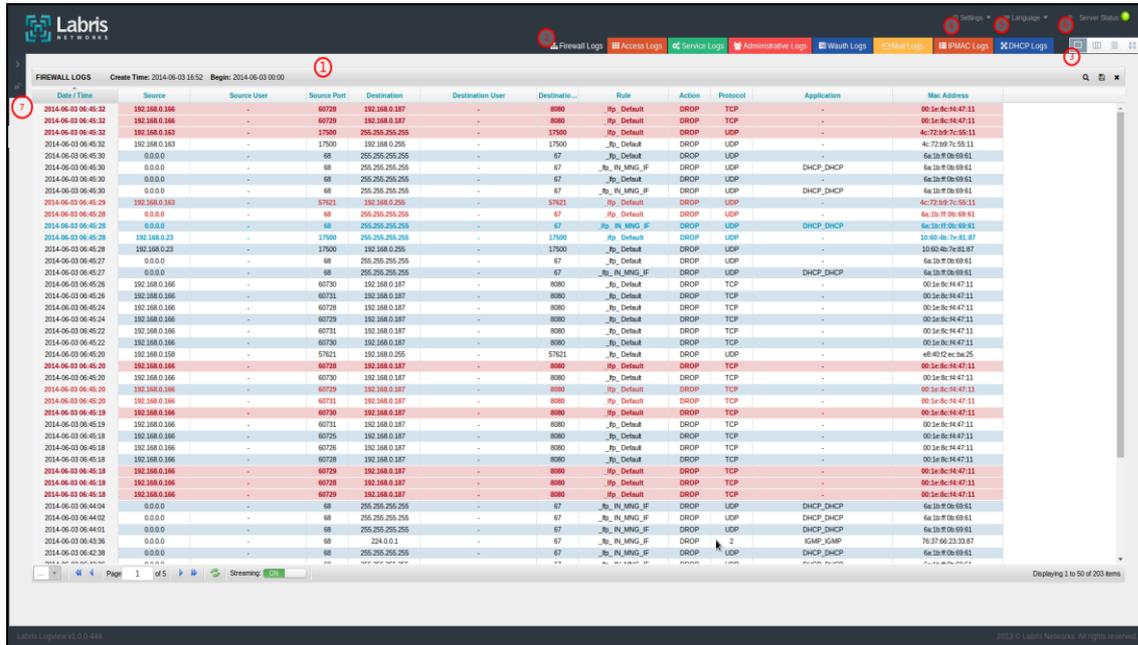
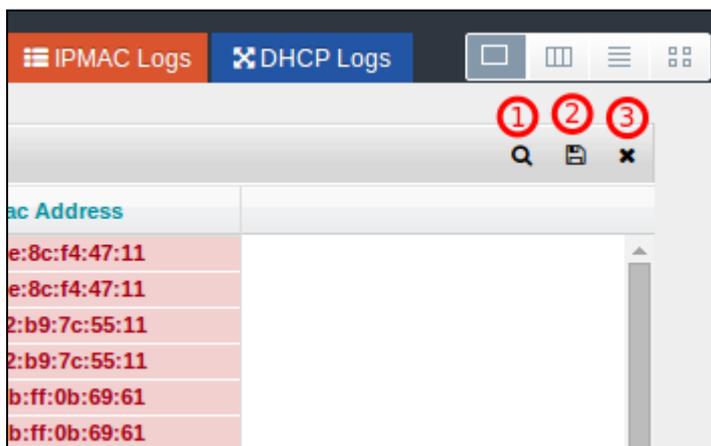


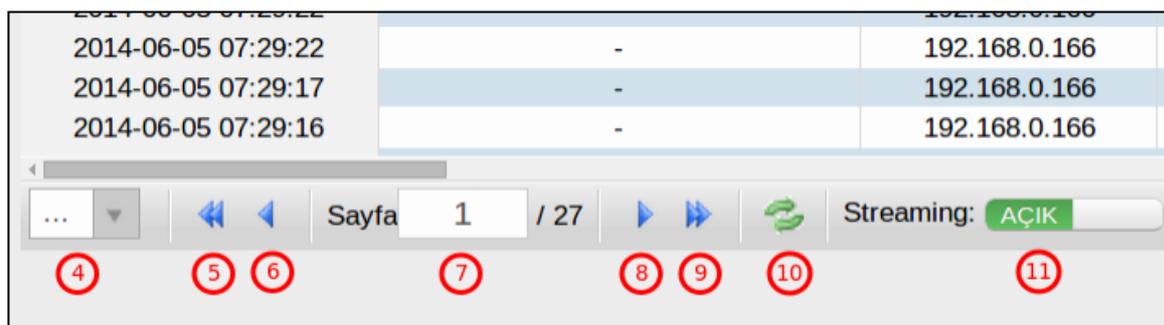
Figure Parts & Tools on main display

1 . Records tables

1	Show / Hide Column Filtering	Select Show or Hide Column Filtering
2	Export Filtered Records	Select Export Filtered Records
3	Remove Table	Select Remove Table



4	Table Length	Select Table Length
5	Backward Pages by 10	Select Backward Pages
6	Previous Page	Select Previous Page
7	Go to Page Number	Write Go to Page Number
8	Next Page	Go to Next Page
9	Forward Pages by 10	Select Forward Pages
10	Refresh The Table	Refresh The Table Button
11	Switch on/off	Switch on/off Live Monitoring



2 . Live monitoring shortcuts



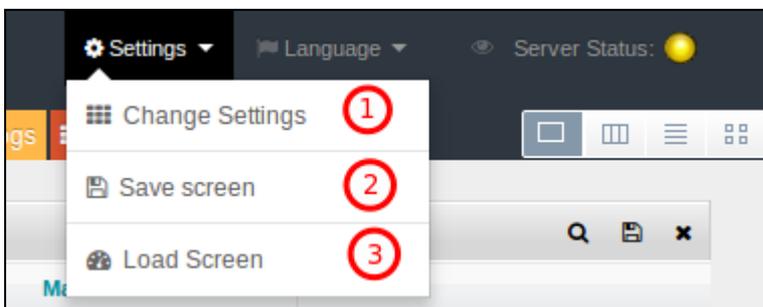
1	Firewall	Firewall Network Logs View
2	Access	Access Logs View
3	Operational	Operational Logs View
4	Administrative	Administrative Logs View
5	Wireless Authentication	Wireless Authentication Logs View
6	IPMAC	IPMAC Logs View
7	DHCP	DHCP Logs View
8	Mail	Mail Logs View

3 .Layout options



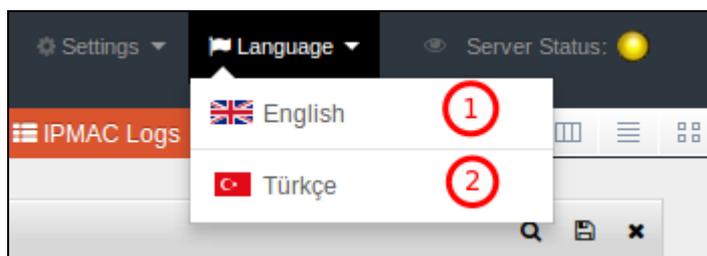
1	Single View	Select Single View
2	Column View	Select Column View
3	List View	Select List View
4	Grid View	Select Grid View

4 . Settings



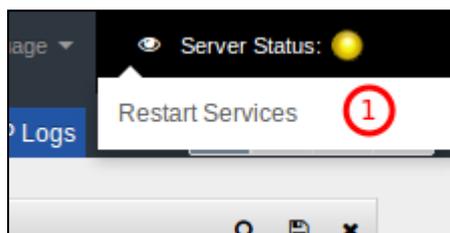
1	Change Settings	Select Change Settings
2	Save Screen	Save Screen
3	Load Screen	Load Screen

5 . Language selector



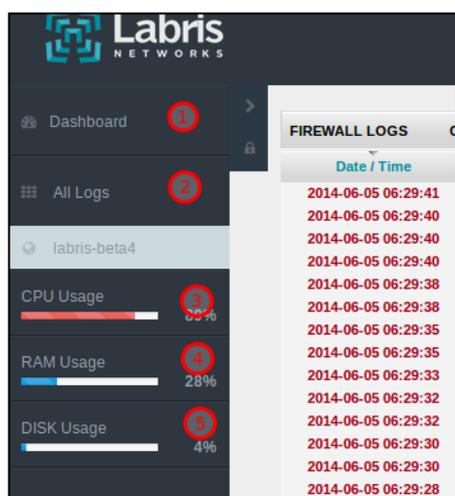
1	English	Select English Language
2	Turkish	Select Turkish Language

6 . Server status & service controller



1	Restart Services	Restart all Services
---	------------------	----------------------

7 . Sidebar



1	Dashboard	Select Dashboard for Dashboard Screen
2	All Logs	Select All Logs
3	CPU Usage	CPU Usage Info
4	RAM Usage	RAM Usage Info
5	Disk Usage	Disk Usage Info

3. Instructions

Logview is a web-based application and the only thing you could run it is a Web browser. We advice you to mostly use Chrome, Safari or Firefox. Logview does not support IE versions before 8.0.

Logview uses Websocket and most of near future Web technologies; therefore the browser you would use must support all these technologies.

4. Records Table

Records table shows records from your UTM device that is gathers all logs from defined sources. You can see any log data, which is gathered from given date range and given, source. You can access column filter feature just by clicking 1.1 Show / Hide column filtering button and you can make a search by typing any keyword regarding column data.

The picture shows a table that its column filter is not enabled yet:

Date / Time	User	Source	Mac Address	Destination	URL	Decision	HIT/MISS	Category	Filter C
2014-06-05 13:13:52		192.168.2.156	-	-		*EXCEPTION*Ayricakli_br_steye_girdiz.	TCP_MISS/200		kullu
2014-06-05 13:13:52		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:52		192.168.2.156	-	-			TCP_MISS/304		kullu
2014-06-05 13:13:52		192.168.0.153	-	-		*EXCEPTION*Ayricakli_br_steye_girdiz.	TCP_MISS/206		kullu
2014-06-05 13:13:52		192.168.2.161	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:52		192.168.2.156	-	-			TCP_MISS/200		kullu
2014-06-05 13:13:51		192.168.0.153	-	-		*EXCEPTION*Ayricakli_br_steye_girdiz.	TCP_MISS/206		kullu
2014-06-05 13:13:51		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:50		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:50		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:50		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:50		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:50		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:50		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:50		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:50		192.168.0.153	-	-		*EXCEPTION*Ayricakli_br_steye_girdiz.	TCP_MISS/206		kullu
2014-06-05 13:13:50		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:49		192.168.0.153	-	-		*EXCEPTION*Ayricakli_br_steye_girdiz.	TCP_MISS/206		kullu
2014-06-05 13:13:49		192.168.2.156	-	-			TCP_MISS/200		kullu
2014-06-05 13:13:48		192.168.2.161	-	-			TCP_MISS/200		kullu
2014-06-05 13:13:48		192.168.2.161	-	-			TCP_MISS/200		kullu
2014-06-05 13:13:47		192.168.2.156	-	-			TCP_MISS/200		kullu
2014-06-05 13:13:47		192.168.0.153	-	-		*EXCEPTION*Ayricakli_br_steye_girdiz.	TCP_MISS/206		kullu
2014-06-05 13:13:47		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:47		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:46		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:46		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:46		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:46		192.168.2.156	-	-		*SCANNED*	TCP_MISS/302		kullu
2014-06-05 13:13:46		192.168.2.156	-	-			TCP_MISS/200		kullu
2014-06-05 13:13:46		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:46		192.168.2.156	-	-			TCP_MISS/200		kullu
2014-06-05 13:13:46		192.168.0.153	-	-		*EXCEPTION*Ayricakli_br_steye_girdiz.	TCP_MISS/206		kullu
2014-06-05 13:13:46		192.168.2.156	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:46		192.168.0.198	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:46		192.168.2.156	-	-			TCP_MISS/200		kullu
2014-06-05 13:13:46		192.168.2.156	-	-			TCP_MISS/200		kullu
2014-06-05 13:13:46		192.168.0.153	-	-			TCP_MISS/200		kullu
2014-06-05 13:13:46		192.168.2.132	-	-		*SCANNED*	TCP_MISS/200		kullu
2014-06-05 13:13:45		192.168.2.156	-	-			TCP_MISS/200		kullu
2014-06-05 13:13:45		192.168.2.156	-	-			TCP_MISS/200		kullu

And by clicking 1.1 Show / Hide Column Filtering button you will see the filters, even they are already filtered:

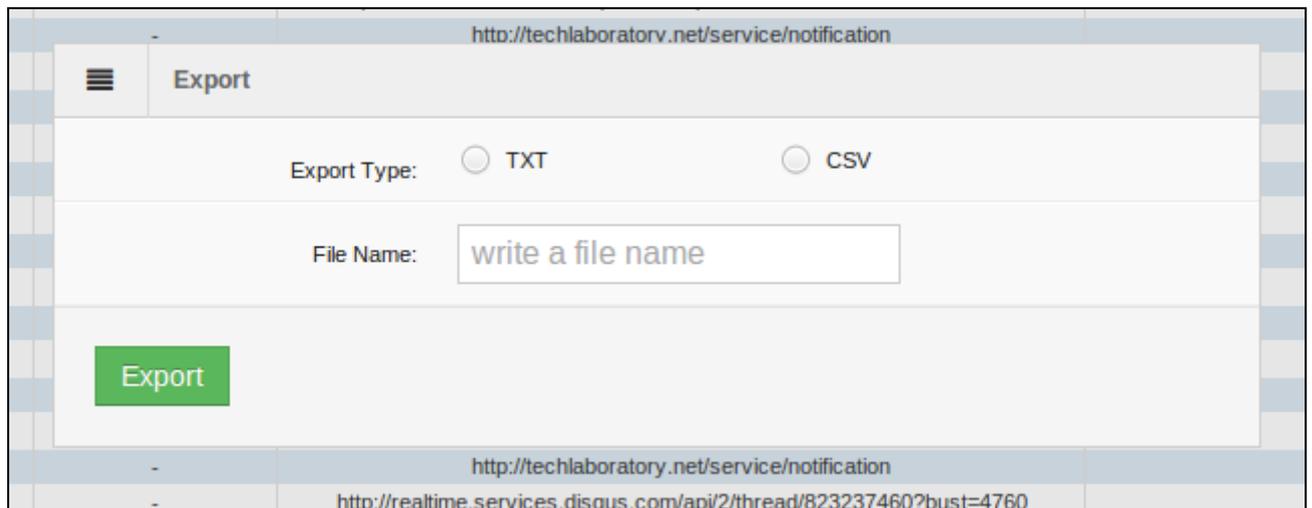
Date / Time	User	Source	Mac Address	Destination	URL	Decision
2014-06-05 13:21:45		192.168.0.155	-	-		*SCANNED*
2014-06-05 13:21:44		192.168.6.173	-	-		*SCANNED*
2014-06-05 13:21:43		192.168.6.173	-	-		*SCANNED*
2014-06-05 13:21:43		192.168.6.173	-	-		*SCANNED*
2014-06-05 13:21:43		192.168.6.173	-	-		*SCANNED*
2014-06-05 13:21:43		192.168.6.173	-	-		*SCANNED*
2014-06-05 13:21:43		192.168.6.173	-	-		*SCANNED*
2014-06-05 13:21:42		192.168.6.173	-	-		*SCANNED*
2014-06-05 13:21:41		192.168.6.173	-	-		*SCANNED*
2014-06-05 13:21:41		192.168.6.173	-	-		*SCANNED*
2014-06-05 13:21:41		192.168.6.173	-	-		*SCANNED*
2014-06-05 13:21:41		192.168.6.173	-	-		*SCANNED*
2014-06-05 13:21:41		192.168.6.173	-	-		*SCANNED*

It can be search by using some operators:

- “=” use it for define an equation such as for User column use like “user@domain” or type “=username@domain”
- “!=” use it for User column use like “user@domain” or type “=username@domain”
- “&&” use it for “and” keywords such as for User column use like “=user@domain && !=anotheruser@domain”
- “||” use it for “or” keywords such as for User column use like “=user@domain || !=anotheruser@domain”

In records table you can export your filtered data by clicking 1.2 Export filtered records as CSV

or TXT file formatted.



And you can remove the table by clicking 1.3 Remove table button.

Records table also has a footer, which includes:

- record length: use it to set content length of a table by page 10, 15, 20, 30 and 50



- backward- forward buttons: use it to shift pages by 10 forward  or backward 

- previous- next buttons: use it to shift pages one by one  

- reload buttons: use it to reload the page if you think something goes wrong about the



table

- streaming on/off button: enable or disable stream, it is better to stop stream when



filtering data.

Records tables also have nice user-friendly features. You can resize columns by pulling the next line to the column and leave it when you reach the size you want. Initially records tables have own predefined size to provide best-fit size for the data inside the column. You can also order historical records table just by clicking the header of the column you would like to sort by; and also you can show or hide columns by clicking the down-arrow on the column heading as show

in figure.

Another feature tables have is “replacing columns”. You can replace columns by drag and drop. Drag a column you want to move then drop to put where you want.

4.1. Real-time Monitoring

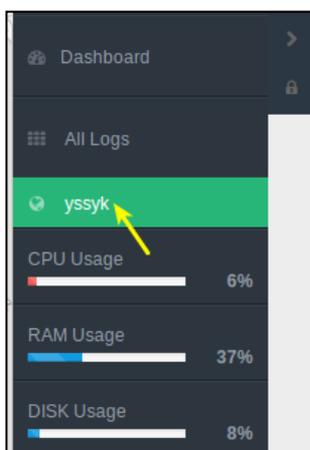
Logview provides a real-time monitoring for streaming logs. You can just click the shortcut buttons and it fires an event to create real-time logs monitoring tables.



1	Firewall Log	View All Firewall Logs
2	Access Logs	Internet Access Logs
3	Service Logs	Device Service Logs
4	Administrative Logs	Administrative Logs for This Device
5	Wireless Authentication Logs	Wireless Authentication Logs
6	Mail Logs	Mail Logs for SMTP, IMAP and POP3
7	IP-MAC Logs	IP AND MAC Address Logs
8	DHCP Logs	DHCP Logs

Real-time monitoring tables allow you to track real time logs. Even if you want to filter them then it still keeps streaming

Historical Logs



Historical logs are all logs that are retrieved from older logs. You can create a historical records table from sidebar.

After you click the domain name you will see a window like below:

As we see in the figure, there are log sources and regarding fields which will be defined as columns when the table is created. We can select which column will be shown or hidden. In date range selection section, there are predefined date ranges 1 day, 3 days, 1 week. In another case, you can also select date range by manually.

The screenshot shows a web interface titled "Table" for configuring a historical log table. It includes the following sections:

- Select Log Source:** Radio buttons for Firewall Logs, Service Logs, Wauth Logs, IPMAC Logs, Access Logs (selected), Administrative Logs, Mail Logs, and DHCP Logs.
- Select Log Fields:** Checkboxes for Date / Time, Mac Address, Decision, Host, Response Code, Client Host, Method, User, Destination, Undefined, Domain, User Agent, Duration, Source, URL, Category, Filter Group, Size, and Mime Type.
- Default Ranges:** Buttons for 1 day (selected), 3 days, and 1 week.
- From:** Text input field containing "2014-05-29 16:09".
- To:** Text input field containing "2014-06-05 16:09".
- CREATE TABLE:** A green button at the bottom left.

Figure: Create Historical Log Table

The screenshot shows a web-based configuration interface titled "Table". It is divided into several sections:

- Select Log Source:** Radio buttons for "Firewall Logs" (unselected) and "Access Logs" (selected). Other options include "Administrative Logs", "Mail Logs", and "DHCP Logs".
- Select Log Fields:** A list of fields with checkboxes: "Source" (checked), "URL" (checked), "Category" (checked), "Filter Group" (checked), "Size" (unchecked), and "Mime Type" (unchecked).
- Calendar:** A calendar for May 2014. The date range is set from May 29 (highlighted in orange) to May 31 (highlighted in blue).
- Time Selection:** A "Time" field set to "16:09". Below it are sliders for "Hour" and "Minute".
- Default Ranges:** A "Now" button and a "Done" button.
- Date Range:** "From:" field contains "2014-05-29 16:09" and "To:" field contains "2014-06-05 16:09".
- CREATE TABLE:** A green button at the bottom left.

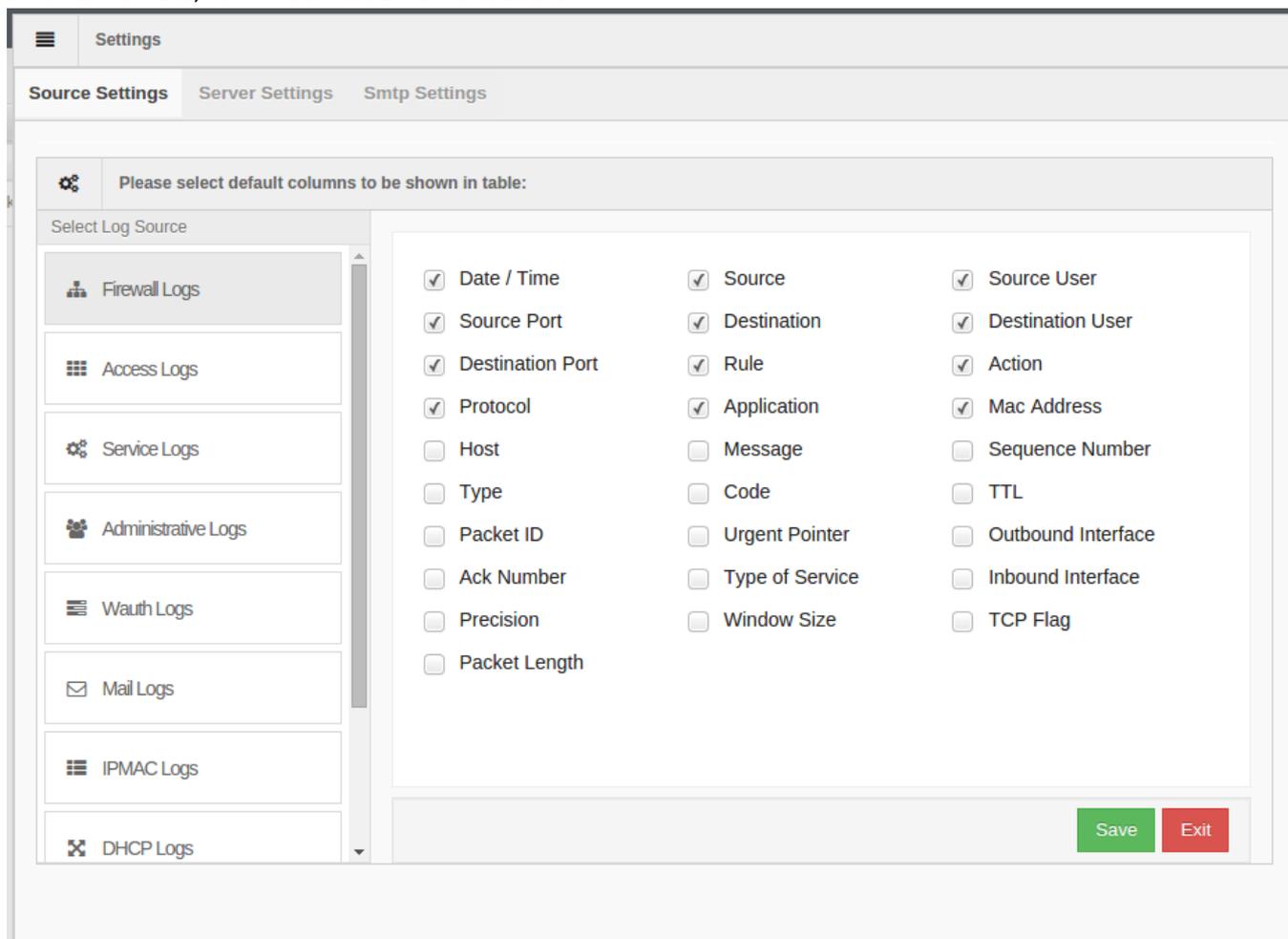
Figure: Create Historical Log Table - Pick Date Range

5. Utilities

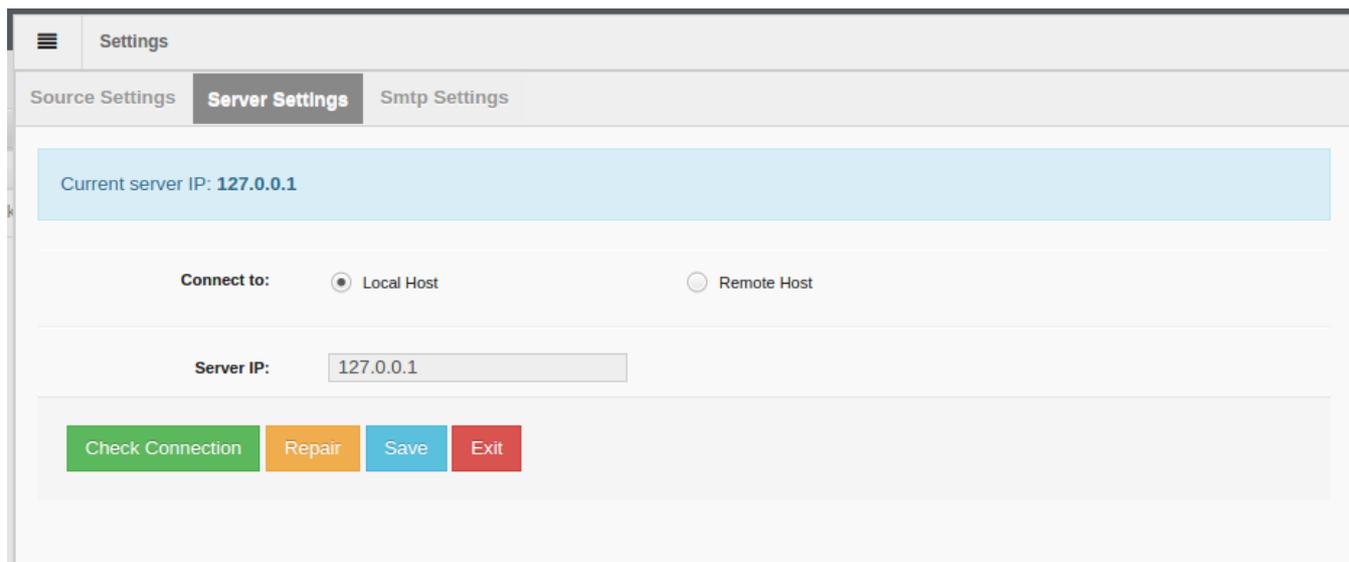
5.1. Settings

Settings section lets you change settings along Logview. By clicking 4.1 Change Settings you will be able to set default behavior of columns to be shown or hidden.

If you check any field on this window, it will be shown in records table as shown column. If you uncheck a field, it will be hidden on the table.



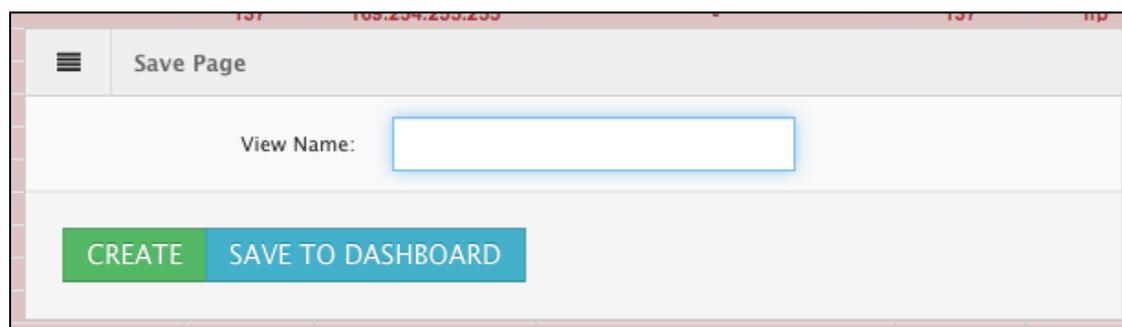
Choosing Default Log Fields which, are shown as predefined column in the table



Settings Data Store to retrieve data from localhost or remote host

5.2. Save Screen

Logview allows you to save different views depending on your needs. You can create different widgets for different log sources, you can resize columns, set filters, change layouts and then you can click on “Save Screen” and give it a name. The page automatically saves the view after some critical events.



5.3. Load Screen

Logview stores your saved screen with any parameters and settings you asdf, as mentioned above. You can make a search then you fill find all saved screens and select which one you would like to load.

FIND A VIEW

NAME:

FROM:

TO:

View name	Table count
-----------	-------------

FIND

FIND A VIEW

NAME:

FROM:

TO:

View name	Table count	
view 2	4	Load Delete
dashboard	4	Load Delete

FIND

5.4. SMTP Settings

It can be set SMTP settings by new version of Logview. You can either provide your own SMTP server settings or set any other SMTP server provider settings to send email(s) from Labris appliances. As it is shown in the figure below, there are mandatory fields you have to set and you have a “Test Connection”

Tarih / Zaman	Kaynak	Kaynak Kullanici	Kaynak Portu	Hedef Adresi	Hedef Kullanici	Hedef Portu	Kural	Karar	Protokol
2014-06-06 10:53:07	169.254.1.1	-	138	169.254.255.255	-	138	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:53:06	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:53:05	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:53:04	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:53:02	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:53:01	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:53:00	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:59	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:57	169.254.1.1	-	138	169.254.255.255	-	138	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:57	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:55	169.254.1.1	-	138	169.254.255.255	-	138	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:53	169.254.1.1	-	138	169.254.255.255	-	138	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:51	169.254.1.1	-	138	169.254.255.255	-	138	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:50	169.254.1.1	-	138	169.254.255.255	-	138	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:39	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:36	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP
2014-06-06 10:52:36	169.254.1.1	-	137	169.254.255.255	-	137	Ifb OUT MNG IF	DROP	UDP

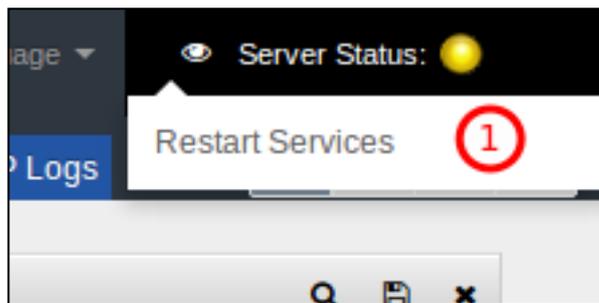
Main display in Turkish

7. Service Monitoring

You can monitor background service's status of Logview. The status indicator will be green if all background services work fine, but the indicator will be yellow if some of services are ok but some have problem. If you see yellow indicator you should see system logs. If the indicator is red you should talk with the technical support.

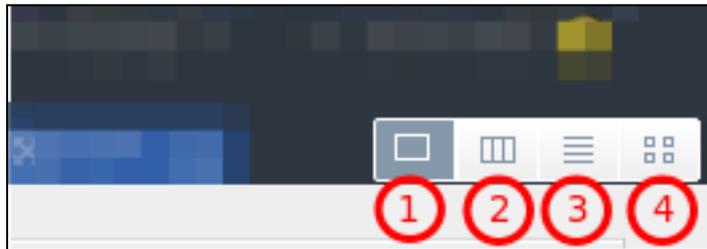


There is also a service controlling option under the Server Status menu to restart services. If you see yellow indicator you may go through to try restarting services. If it may keep staying in the yellow status please contact the technical support.



8. Layout Options

Logview is a single page application that supports widgetizing the layout. You can monitor 4 different log sources in different records table. There are 4 layout option to placed widgets in the page:



1	Single Widget View	Single Widget View Button
2	Column View	Select Column View
3	List View	Select List View
4	Grid View	Select Grid View

Logview starts with a single widget if there is no dashboard saved and if the dashboard has no widget on it. So, Logview loads a firewall records table in single widget view. You can change the widgets, view option, columns, filters and then save the dashboard or save it with a different name.

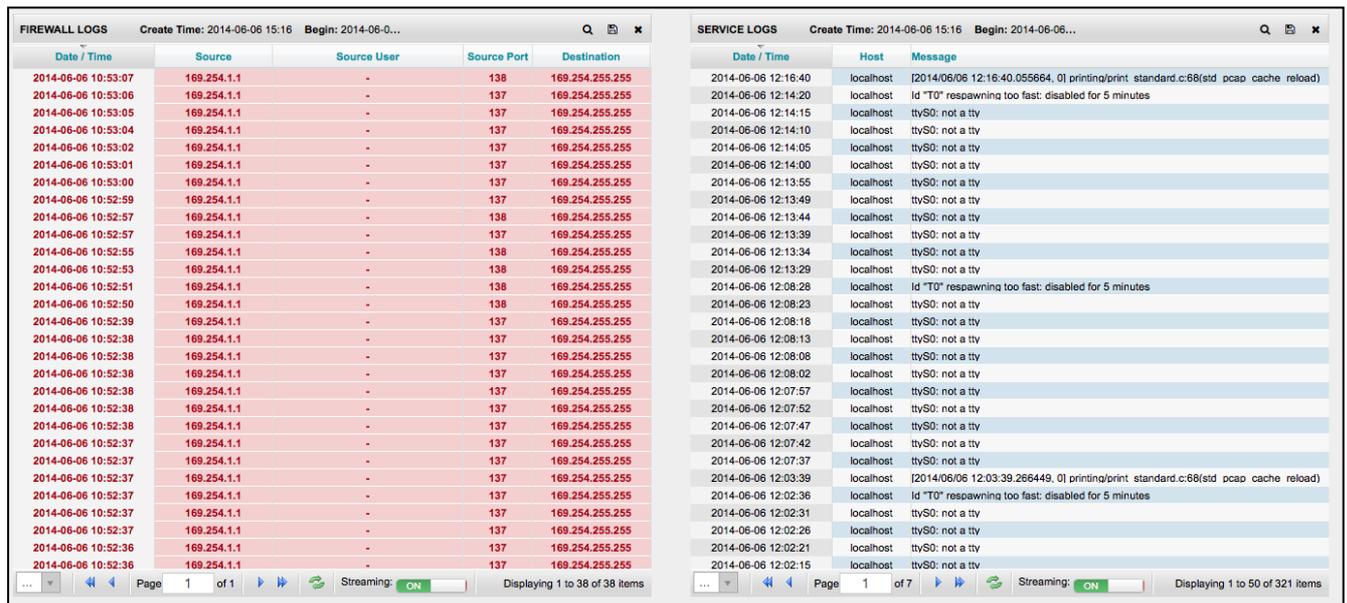
8.1. Single Widget View

In single widget view layout you can see only one widget at a time. If you pick a streaming records table or create a historical records table it will replace the previous widget with itself. In another case, if you have more than one widget in a different view then you select the single view, the layout option will remove all widget except the one that added last.

Date / Time	Source	Source User	Source Port	Destination	Destination User	Destinatio...	Rule	Action	Protocol	Application
2014-06-06 10:53:07	169.254.1.1	-	138	169.254.255.255	-	138	lfp OUT MNG IF	DROP	UDP	CIFS CIFS
2014-06-06 10:53:06	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:53:05	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:53:04	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:53:02	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:53:01	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:53:00	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:59	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:57	169.254.1.1	-	138	169.254.255.255	-	138	lfp OUT MNG IF	DROP	UDP	CIFS CIFS
2014-06-06 10:52:57	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:55	169.254.1.1	-	138	169.254.255.255	-	138	lfp OUT MNG IF	DROP	UDP	CIFS CIFS
2014-06-06 10:52:53	169.254.1.1	-	138	169.254.255.255	-	138	lfp OUT MNG IF	DROP	UDP	CIFS CIFS
2014-06-06 10:52:51	169.254.1.1	-	138	169.254.255.255	-	138	lfp OUT MNG IF	DROP	UDP	CIFS CIFS
2014-06-06 10:52:50	169.254.1.1	-	138	169.254.255.255	-	138	lfp OUT MNG IF	DROP	UDP	CIFS CIFS
2014-06-06 10:52:39	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:36	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:36	169.254.1.1	-	137	169.254.255.255	-	137	lfp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar

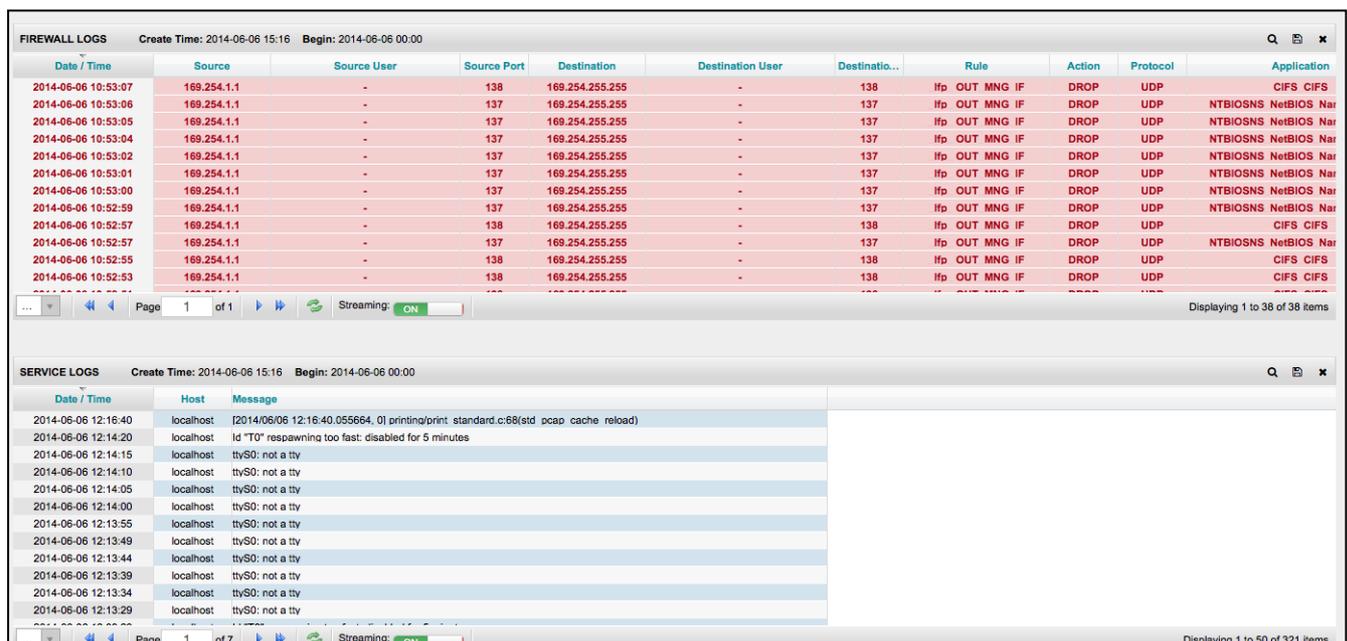
8.2. Column View

In column view you can put widgets in columns and vertically display them.



8.3. List View

In list view you can put widgets in an horizontal order.



It is easy to track log records while you have two streaming records table to compare some data. You can select columns and watch logs while the records table streams.

8.4. Grid View

Grid view has a wide gallery-like view and puts widgets in a 4 piece grid layout.

The screenshot displays the Logview interface with four log sources arranged in a 2x2 grid. Each source has a table view and a streaming control.

Top Left: FIREWALL LOGS
 Create Time: 2014-06-06 15:17 Begin: 2014-06-0...
 Columns: Date / Time, Source, Source User, Source Port, Destination
 Data (rows):
 2014-06-06 10:53:07 | 169.254.1.1 | - | 138 | 169.254.255.255
 2014-06-06 10:53:06 | 169.254.1.1 | - | 137 | 169.254.255.255
 2014-06-06 10:53:05 | 169.254.1.1 | - | 137 | 169.254.255.255
 2014-06-06 10:53:04 | 169.254.1.1 | - | 137 | 169.254.255.255
 2014-06-06 10:53:02 | 169.254.1.1 | - | 137 | 169.254.255.255
 2014-06-06 10:53:01 | 169.254.1.1 | - | 137 | 169.254.255.255
 2014-06-06 10:53:00 | 169.254.1.1 | - | 137 | 169.254.255.255
 2014-06-06 10:52:59 | 169.254.1.1 | - | 137 | 169.254.255.255
 2014-06-06 10:52:57 | 169.254.1.1 | - | 138 | 169.254.255.255
 2014-06-06 10:52:57 | 169.254.1.1 | - | 137 | 169.254.255.255
 2014-06-06 10:52:55 | 169.254.1.1 | - | 138 | 169.254.255.255
 2014-06-06 10:52:53 | 169.254.1.1 | - | 138 | 169.254.255.255
 Streaming: ON | Displaying 1 to 38 of 38 items

Top Right: ADMINISTRATIVE LOGS
 Create Time: 2014-06-06 15:17 Begin: 20...
 Columns: Date / Time, Host, Message
 Data (rows):
 2014-06-06 11:01:37 | localhost | Accepted password for root from 10.7.100.102 port 58930 ssh2
 2014-06-06 11:01:37 | localhost | pam_unix(sshd:session): session opened for user root by (uid=0)
 2014-06-06 10:53:00 | localhost | pam_unix(login:session): session opened for user root by LOGIN(uid=0)
 2014-06-06 10:53:00 | localhost | ROOT LOGIN ON tty1
 Streaming: ON | Displaying 1 to 4 of 4 items

Bottom Left: FIREWALL LOGS
 Create Time: 2014-06-06 15:16 Begin: 2014-06-0...
 Columns: Date / Time, Source, Source User, Source Port, Destination
 Data (rows):
 2014-06-06 10:53:07 | 169.254.1.1 | - | 138 | 169.254.255.255
 2014-06-06 10:53:06 | 169.254.1.1 | - | 137 | 169.254.255.255
 2014-06-06 10:53:05 | 169.254.1.1 | - | 137 | 169.254.255.255
 2014-06-06 10:53:04 | 169.254.1.1 | - | 137 | 169.254.255.255
 2014-06-06 10:53:02 | 169.254.1.1 | - | 137 | 169.254.255.255
 2014-06-06 10:53:01 | 169.254.1.1 | - | 137 | 169.254.255.255
 2014-06-06 10:53:00 | 169.254.1.1 | - | 137 | 169.254.255.255
 2014-06-06 10:52:59 | 169.254.1.1 | - | 137 | 169.254.255.255
 2014-06-06 10:52:57 | 169.254.1.1 | - | 138 | 169.254.255.255
 2014-06-06 10:52:57 | 169.254.1.1 | - | 137 | 169.254.255.255
 2014-06-06 10:52:55 | 169.254.1.1 | - | 138 | 169.254.255.255
 2014-06-06 10:52:53 | 169.254.1.1 | - | 138 | 169.254.255.255
 Streaming: ON | Displaying 1 to 38 of 38 items

Bottom Right: SERVICE LOGS
 Create Time: 2014-06-06 15:16 Begin: 2014-06-06...
 Columns: Date / Time, Host, Message
 Data (rows):
 2014-06-06 12:16:40 | localhost | [2014/06/06 12:16:40.055664.0] printing/print_standard.c:68(std_pcap_cache_reload)
 2014-06-06 12:14:20 | localhost | ld "TO" respawning too fast: disabled for 5 minutes
 2014-06-06 12:14:15 | localhost | ttvS0: not a tty
 2014-06-06 12:14:10 | localhost | ttvS0: not a tty
 2014-06-06 12:14:05 | localhost | ttvS0: not a tty
 2014-06-06 12:14:00 | localhost | ttvS0: not a tty
 2014-06-06 12:13:55 | localhost | ttvS0: not a tty
 2014-06-06 12:13:49 | localhost | ttvS0: not a tty
 2014-06-06 12:13:44 | localhost | ttvS0: not a tty
 2014-06-06 12:13:39 | localhost | ttvS0: not a tty
 2014-06-06 12:13:34 | localhost | ttvS0: not a tty
 2014-06-06 12:13:29 | localhost | ttvS0: not a tty
 Streaming: ON | Displaying 1 to 50 of 321 items

This view helps you to compare or watch 4 different log sources in tables.

9. Reports

By a new version 1.2.0-84 of Logview, we provide a brand new reporting module. Since, our products have already reporting module ERM, by this new module we add improving features listed below:

- Enables custom query writing,
- PDF report generation,
- Table and chart(PIE chart only for recent version) displaying in PDF,
- Report template add/edit/remove features,
- Schedule report generation by user,
- Email and FTP upload feature,
- Manually upload or email generated report to given destination,

9.1. Create Template

The figure shown below helps you create a “Report Template” which, defines “Report” fields, data set, chart set, schedule settings, email settings and FTP settings. In this view you can use **All** records in a log table or write your own custom query based on SQL syntax. See details in the figure below:

The screenshot shows the 'Create New Report Template' interface. The 'Report Name' is 'Firewall Weekly Application Report'. The 'Description' is 'This report contains weekly application filter regarding provided query'. The 'Output Format' is 'PDF' and the 'Report Language' is 'English'. The 'Data Source' is 'Firewall' and the 'Period' is 'This Week'. The 'Report Query' is set to 'Custom' with the query 'application = "HTTP_HTTP"'. The 'Create Report' button is green and the 'Exit' button is red.

This screenshot shows the same 'Create New Report Template' interface, but with a dropdown menu open over the 'Report Query' field. The dropdown lists suggestions: 'date', 'source', 'source_user', 'source_port', 'destination', 'destination_user', 'destination_port', 'rule', 'action', and 'protocol'. The 'Save Report' button is green and the 'Exit' button is red.

Write custom SQL query and Logview suggest column names and basic SQL keywords.

The screenshot shows the 'Create New Report Template' form with the 'Table Settings' tab selected. The form includes fields for 'Report Name' (Firewall Weekly Application Report), 'Description' (This report contains weekly application filter regarding provided query), 'Output Format' (PDF), and 'Report Language' (English). The 'Table Settings' tab contains a grid of checkboxes for selecting columns to display in the report table. The 'Show in Table' dropdown is set to 'Top 30'. At the bottom right, there are 'Create Report' and 'Exit' buttons.

Table Columns	Source	Email Settings
<input checked="" type="checkbox"/> Date / Time	<input checked="" type="checkbox"/> Source	<input type="checkbox"/> Source User
<input type="checkbox"/> Source Port	<input type="checkbox"/> Destination	<input type="checkbox"/> Destination User
<input type="checkbox"/> Destination Port	<input checked="" type="checkbox"/> Rule	<input checked="" type="checkbox"/> Action
<input type="checkbox"/> Protocol	<input checked="" type="checkbox"/> Application	<input checked="" type="checkbox"/> Mac Address
<input type="checkbox"/> Host	<input type="checkbox"/> Message	<input type="checkbox"/> Sequence Number
<input type="checkbox"/> Type	<input type="checkbox"/> Code	<input type="checkbox"/> TTL
<input type="checkbox"/> Packet ID	<input type="checkbox"/> Urgent Pointer	<input type="checkbox"/> Outbound Interface
<input type="checkbox"/> Ack Number	<input type="checkbox"/> Inbound Interface	<input type="checkbox"/> Precision
<input type="checkbox"/> Window Size	<input type="checkbox"/> TCP Flag	<input type="checkbox"/> Packet Length

Select columns which, are will be shown in the report table.

The screenshot shows the 'Create New Report Template' form with the 'Chart Settings' tab selected. The form includes fields for 'Report Name' (Firewall Weekly Application Report), 'Description' (This report contains weekly application filter regarding provided query), 'Output Format' (PDF), and 'Report Language' (English). The 'Chart Settings' tab contains dropdown menus for 'Chart Type' (Pie Chart), 'Chart Field' (Source), and 'Show in Chart' (Top 5). At the bottom right, there are 'Create Report' and 'Exit' buttons.

Select chart field to be shown in Pie chart

The screenshot shows the 'Create New Report Template' interface. The 'Schedule Settings' tab is selected and highlighted. The form contains the following fields and controls:

- Report Name:** Firewall Weekly Application Report
- Description:** This report contains weekly application filter regarding provided query (Max. 500 character)
- Output Format:** PDF
- Report Language:** English
- Enable:**
- Generate Report Every:** 1 Weeks
- Schedule Start:** 2015-12-14 09:44
- Schedule End:** (empty field)

At the bottom right, there are two buttons: 'Create Report' (green) and 'Exit' (red).

Schedule settings tab

The screenshot shows the 'Create New Report Template' form with the 'Email Settings' tab selected. The form contains the following fields and settings:

- Report Name:** Firewall Weekly Application Report
- Description:** This report contains weekly application filter regarding provided query (Max. 500 character)
- Output Format:** PDF
- Report Language:** English
- Enable:**
- Subject:** Firewall Weekly Application Repr
- Recipients:** murat.bulbul@labrisnetworks.com, cem.yapalak@labrisnetworks.com (Note: Write email addresses with comma between them.)
- Message:** This report contains weekly application filter regarding provided query

At the bottom right, there are two buttons: 'Create Report' (green) and 'Exit' (red).

Email Settings Tab

The screenshot shows the 'Create New Report Template' form with the 'FTP Settings' tab selected. The form contains the following fields and settings:

- Report Name:** Firewall Weekly Application Report
- Description:** This report contains weekly application filter regarding provided query (Max. 500 character)
- Output Format:** PDF
- Report Language:** English
- Enable:**
- Server:** ftp.myserver.com
- User:** anonymous
- Password:** *****
- Directory:** home/reports/firewall

At the bottom right, there are two buttons: 'Create Report' (green) and 'Exit' (red).

FTP Settings Tab

	Name	Description	Period	Created Date	Reports	Manage
1	Firewall Weekly Application Report	This report contains weekly application filter regarding provi...	This Week	Monday, 14 December 2015, 09:47		

Page of 1 1 Records per page: 20 Displaying 1 to 1 of 1 items.

The figure above, contains all report templates which, are created by user or pre-defined by Labris regarding most required report enquiries. Some buttons and details can be seen in a template row: name, description, period, created date, show reports grid and generate a new report, edit and remove template.

Reports	Manage

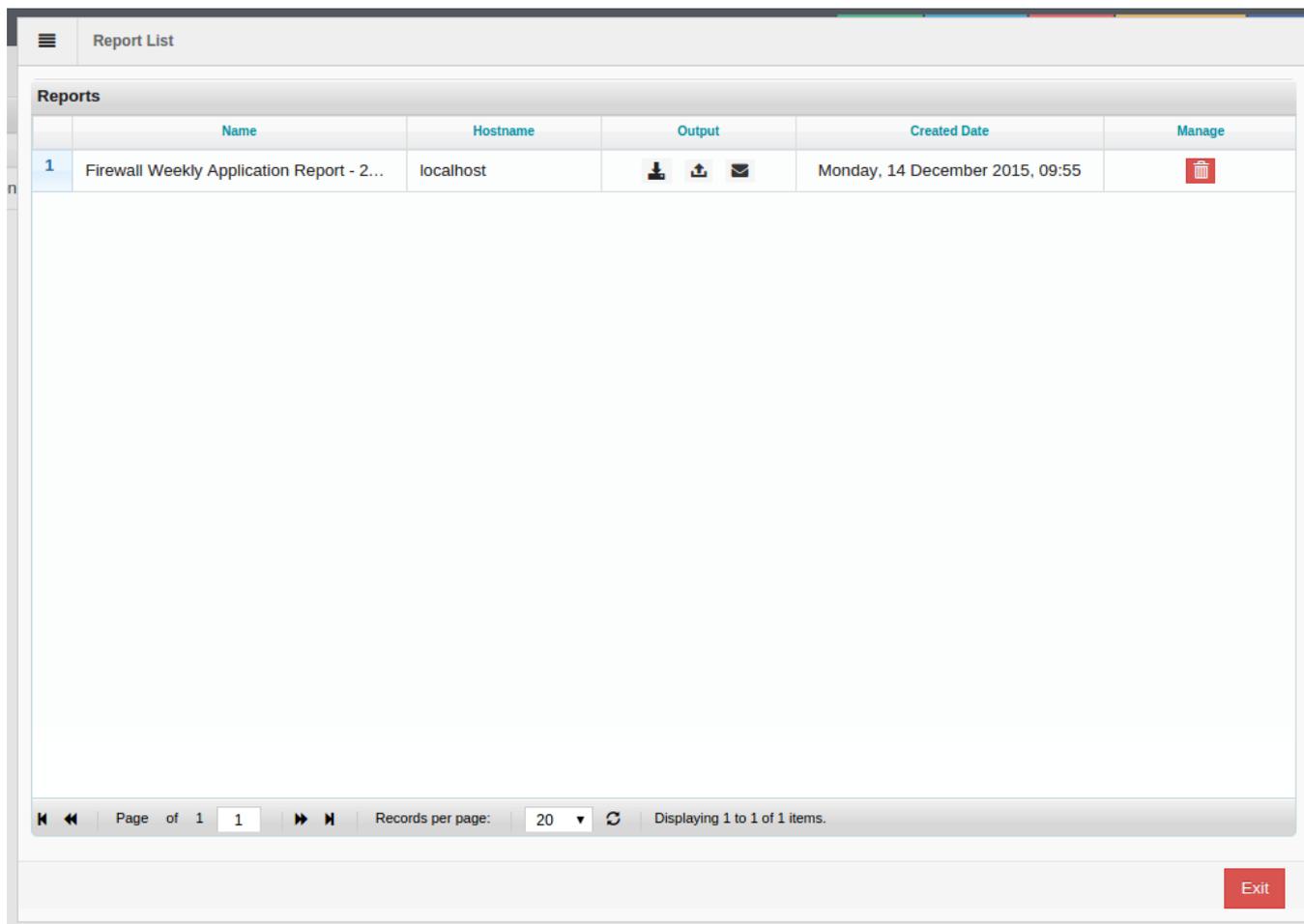
There are helper tooltips on every single buttons placed in a row. It helps you about what its click event.

Show Report Table: Open a popup and show reports listed in a table that belong to the template.

Generate New: Generates a new report depending provided details such as data set, table settings, chart settings, schedule settings, emails settings and FTP settings.

Edit: Helps you edit the template details.

Remove: Delete the template and all reports generated previously by the template details.

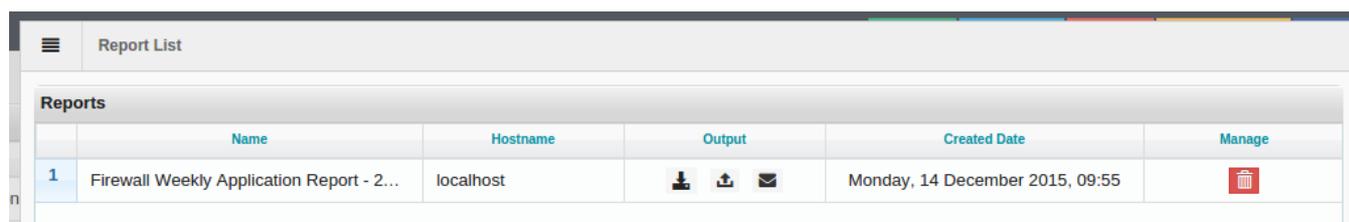


The screenshot shows a web interface titled "Report List". It contains a table with the following data:

	Name	Hostname	Output	Created Date	Manage
1	Firewall Weekly Application Report - 2...	localhost	  	Monday, 14 December 2015, 09:55	

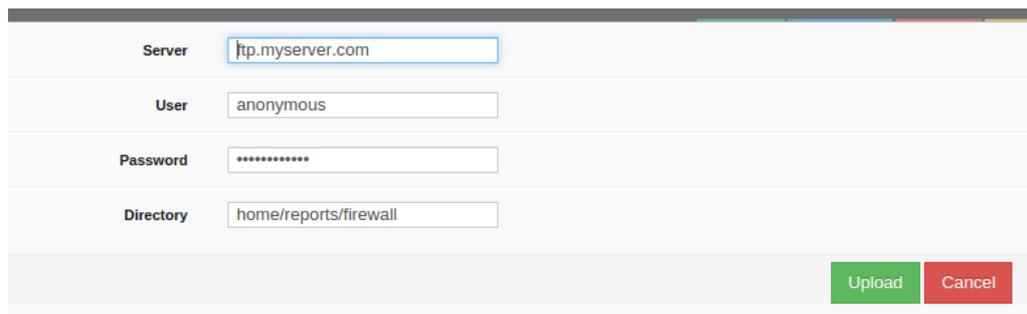
Below the table is a pagination bar showing "Page of 1 1", "Records per page: 20", and "Displaying 1 to 1 of 1 items." An "Exit" button is located in the bottom right corner.

Reports Grid shows all generated reports



This screenshot is identical to the one above, showing the "Report List" interface with a single report entry in the table.

In reports table you can download, upload or send email manually. You can leave FTP and email settings as given previously or write new settings to deliver the report separately to different email addresses or FTP destinations.

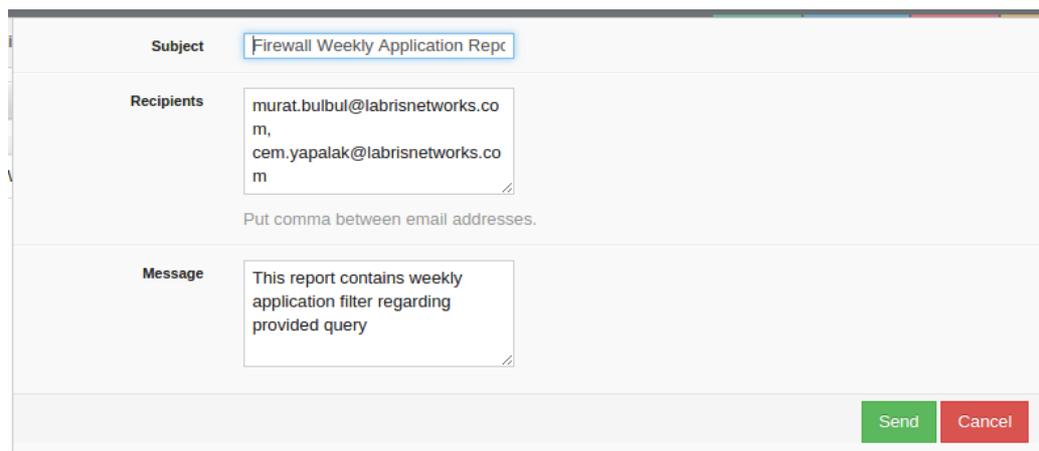


The image shows an FTP Upload popup form with the following fields and values:

Server	ftp.myserver.com
User	anonymous
Password	*****
Directory	home/reports/firewall

At the bottom right, there are two buttons: "Upload" (green) and "Cancel" (red).

FigureFTP Upload popup

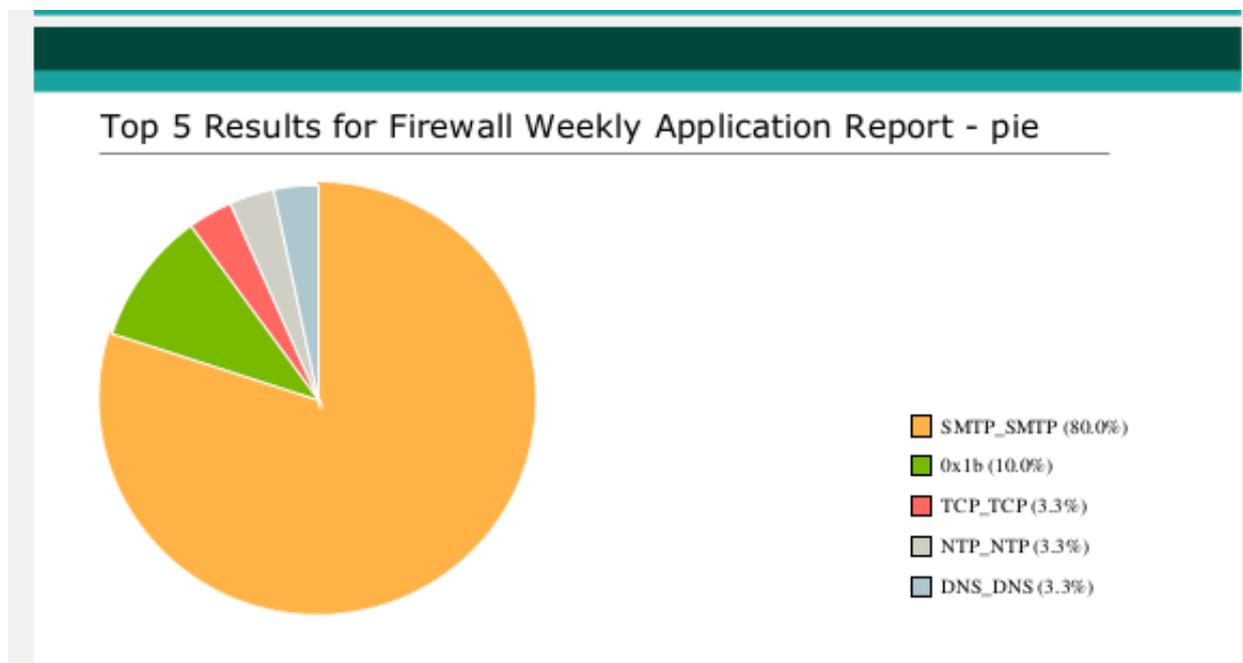


The image shows a Send email popup form with the following fields and values:

Subject	Firewall Weekly Application Repc
Recipients	murat.bulbul@labrisnetworks.com, cem.yapalak@labrisnetworks.com
Message	This report contains weekly application filter regarding provided query

Below the recipients field, there is a note: "Put comma between email addresses." At the bottom right, there are two buttons: "Send" (green) and "Cancel" (red).

Send email popup



Pie Chart result which, is shown in the report

