



Labris
N E T W O R K S

Administration Guide for Labris LOG

Logging, Guest Authentication (Wauth), Monitoring and Reporting System
Version 3.4.2

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

Tel: +90 850 455 4555



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.

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.

Table of Contents

Copyright.....	1
Disclaimer.....	1
About Labris Networks Inc.	8
About LABRIS LOG.....	10
How to Purchase LABRIS LOG	10
LABRIS LOG Appliance Deployment Architecture.....	11
Plug And Play.....	11
Bridge Mode.....	12
Port mirror/Span port mode.....	13
Router mode	14
Logging with SNMP	14
Connecting Appliance	15
Accessing the Web Admin Console.....	15
LRMS into the LABRIS LOG Appliance	16
Accessing LABRIS LOG through LMC.....	19
Labris Management Console (LMC).....	20
Menu	20
User Management	30
Users	30
Adding User.....	30
Deleting User.....	33
Changing password / Editing User	34
Groups.....	35
Adding Group	36
Deleting Group.....	39
Editing Group	40
Wauth	43
Deleting WAUTH policy.....	46
Editing WAUTH Policy	48
Wauth Web Admin Portal.....	49
Settings.....	49

General Settings	49
Settings of Hotel Authentication.....	53
Settings of SMS Authentication	55
Active Directory Authentication	57
User Interface Customize.....	Hata! Yer işareti tanımlanmamış.
Creating WAUTH User.....	66
Online Users.....	67
All Users (User editing).....	67
WAUTH Welcome Screen	69
Login.....	71
Change User Password.....	72
Obtain Password	76
Registering with SMS	76
System.....	81
Users	82
Adding User.....	83
Deleting User.....	84
Change Password / Editing User	85
DHCP	89
DNS.....	105
Diagnostic Tools	110
Configuration Backup / Restore.....	116
Update	126
Automatic Update.....	127
Logs	128
Date / Time Settings.....	129
Console Access Settings.....	129
General Settings.....	133
Trusted Time Stamp.....	134
Certificate Management	135
Restart and Shutdown	138
Network Settings.....	139

IP Configuration	139
IP Alias (ADD, Edit, Delete, Status, Enable/disable)	139
ADSL (Add, Edit, Delete, Status, Enable/Disable)	147
Bridge (Add, Edit, Delete, Status, Enable/disable)	152
3G (ADD, Edit, Delete, Status, Enable/disable)	155
Vlan (Add, Edit, Delete, Status, Enable/disable)	159
Routes	162
Default Gateway	163
Static Route	163
Add (Static Route)	163
Delete (Static Route)	165
Load Balance	165
Add (Load Balance Route)	166
Edit (Load Balance Route)	167
Delete (Load Balance Route)	168
Advanced/ Policy Based Routing	168
Link Configuration	169
Decision Table	170
WAN Load Balancing	174
WAN Failover using CLI	176
Log Settings	183
Sensor Configuration	183
Syslog Receiver	185
Syslog Sender	187
Windows Log Receiver	188
Simple Network Management Protocol (SNMP)	191
Windows Labris Log Sender	193
Labris Log Sender Pre-Setup and Software Agreement	193
How to use Log Sender Installation?	193
1 st Step – Language Selection;	194
2 nd Step – Starting Installation Wizard;	194
3 rd Step – Selecting the Installation Directory;	195

How to use Log Sender Configuration?	197
Log Configuration.....	198
Server Configuration	201
Labris LOG Server Configuration	202
Port mirroring	205
3Com Switch Port Mirroring	205
Cisco Switch Port Mirroring	205
HP Switch Port Mirroring	205
Juniper Switch Port Mirroring.....	207
Logview	208
Introduction	208
Parts & Tools	209
Instructions	213
Records Table.....	213
Real-time Monitoring.....	215
Utilities	218
Settings.....	218
Save Screen	218
Load Screen.....	219
Regional Settings.....	219
Service Monitoring.....	221
Layout Options.....	221
Single Widget View	222
Column View	222
List View	223
Grid View.....	223
Network Visibility.....	225
Firewall.....	229
Make a new firewall object.....	229
Objects	235
Network Objects	236
Hosts	237

Networks	241
Address Ranges	244
Object Groups	247
Users	250
Services	253
ICMP	254
IP	256
TCP	258
UDP	260
Service Groups	262
DoS/DDoS.....	265
General.....	266
SYN Flood	267
UDP Flood	267
CONN Flood.....	268
ICMP Flood	268
ICMPv6 Flood	269
Notes	269
QoS/Bandwidth.....	271
General.....	272
Notes.....	273
Schedule.....	274
Standard.....	274
User Defined	276
General.....	276
Start.....	277
Stop	278
Notes	278
Application Control	280
User Defined	280
Firewall.....	282
Labris Firewall Management.....	283

Install, Save (create a new policy object for first setup), Install Policy.....	283
Add Next Generation Firewall.....	285
Firewall Properties	286
Global Policy table.....	290
NAT (Network Address Translate) Policy table	295
Interfaces	298
Firewall Application.....	301
Network Address Translate (NAT)	301
What is the NAT?	302
Why it is made?.....	302
NAT Types	302
SNAT.....	302
DNAT	302
PAT	302
Port Forwarding/Port Mapping.....	302
Labris Firewall Messages.....	303
IDS/IPS.....	307
Sensor Settings.....	307
Intrusion Detection System.....	307
Settings.....	307
Network Settings.....	307
Interface.....	313
Rule sets	317
Alert Settings.....	325
Mail Alert Settings.....	325
Report Mails.....	325
Alerts	326
License.....	327
New License	327
Install License	329
NTLM Authentication AD Configuration	330
Active Directory Integration.....	330

Windows Labris Logon Tracer 337

Logon Script Configuration 337

CLI Access 346

Glossary..... 348

About Labris Networks Inc.

Since 2002, Labris Networks Inc. has been an R&D focused and rapidly-growing provider of network security solutions through its globally-proven products. Labris ensures ultimate network security through its extensive product line including Firewall/VPN, Web Security, E-Mail Security, Lawful Interception and Availability Protection solutions on LABRIS UTM, Labris LOG and Harpp DDoS Mitigator

appliances. Next-generation solutions are developed to detect, identify all kinds of real-time threats, applications providing a smart shield against intrusions, viruses, spam, malware and availability attacks.

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

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

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

About LABRIS LOG

Labris LOG ensures compliance to logging regulations and that network logs are kept without needing to change the network topology. Labris LOG also keeps additional data like web access logs, which are not enforced by the law, but provides an insight about the network and its security. But before using this feature, do not forget to have your users sign an agreement by consulting your legal adviser which informs that the network traffic is logged. Labris Networks does not accept any responsibility or liability with regard to the usage of this product.

How to Purchase LABRIS LOG

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

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

LABRIS LOG Appliance Deployment Architecture

Labris LOG is designed to keep network logs and differently from many other products it does not need any configuration changes in third party systems to sniff the network and get the logs. With this capability it can also function as a sensor collecting network logs for SIEM product families.

Providing a logging and reporting structure for itself, Labris LOG also provides multiple methods for retrieving logs from other third party systems and acts as log storage. Labris LOG product family is categorized by network traffic size and log record count.

Plug And Play

Labris LOG is ready for operation when out of box. Logging settings are already configured. This way, without the need of additional configuration changes, logging process starts immediately in bridge and port mirroring modes.

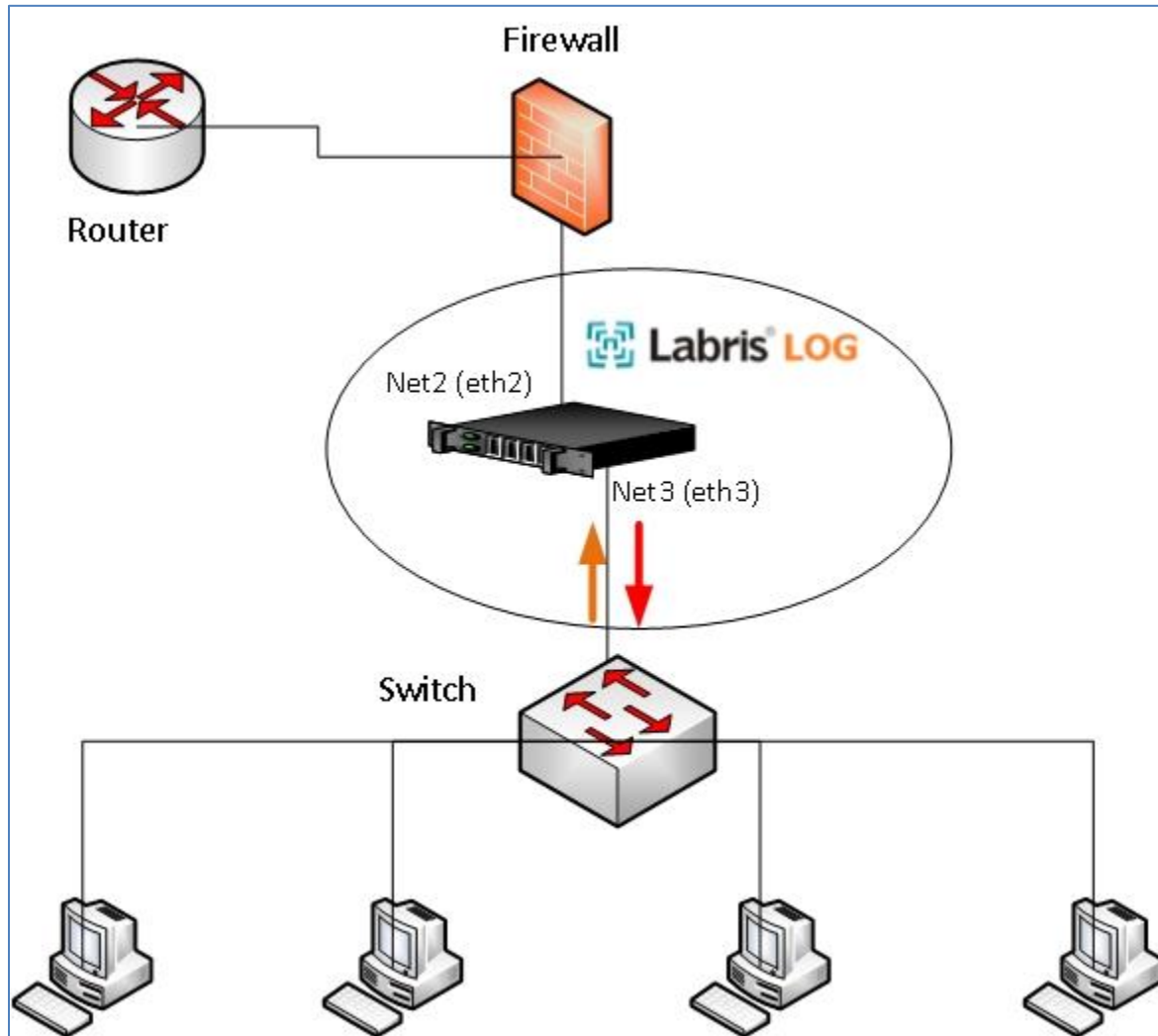
For bridge mode, eth2 and eth3 ports comes configured on default. Sensor is active on eth2 port.

For mirror mode, after an ethernet cable is plugged to the eth2 port and the switch is configured for port mirroring, logging process will start.

Traffic sniffing and Logging Methods

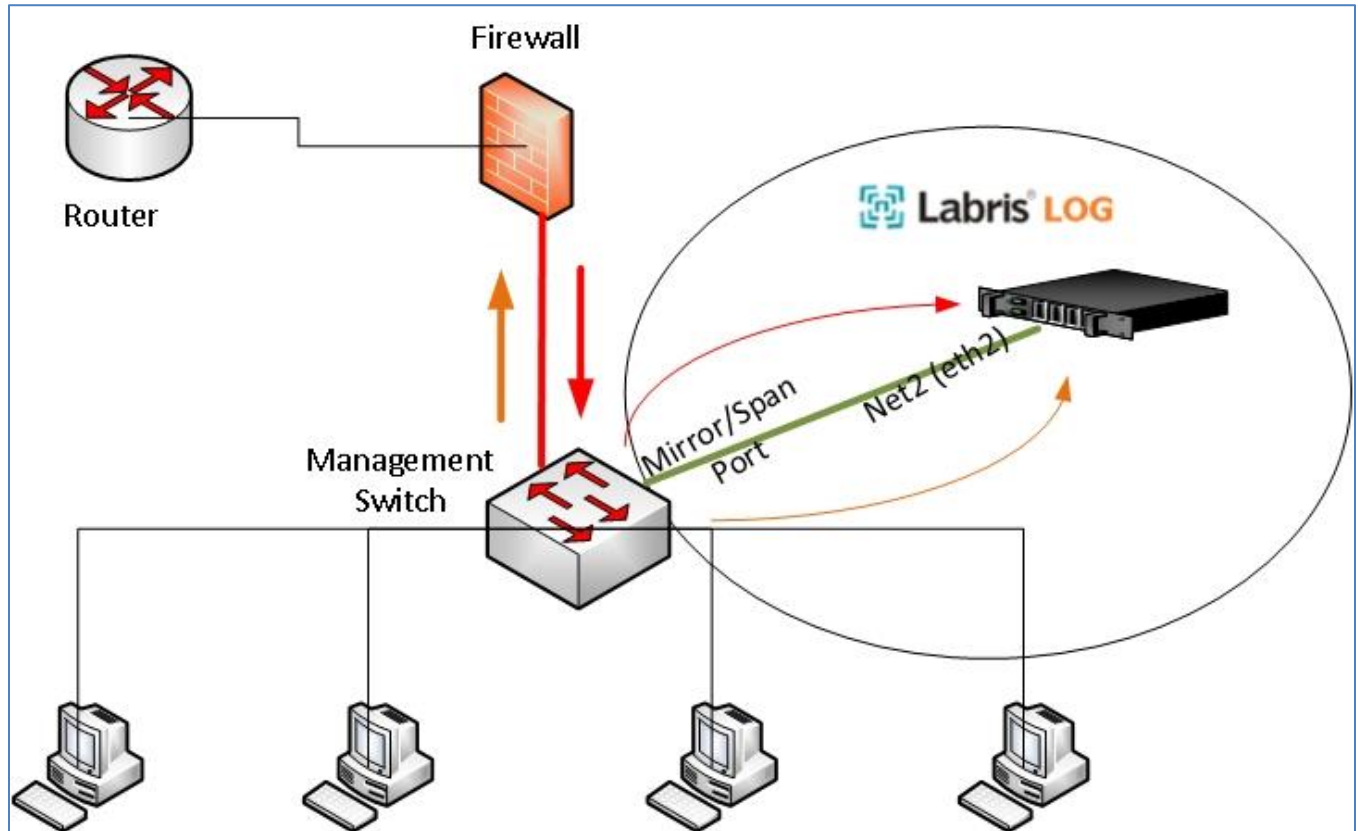
Bridge Mode

In this configuration the device logs the needed data by intercepting the traffic on the cable. Usually the cable connecting the network firewall to the switch is the cable where users' traffic flows, so Labris LOG can be placed here between the switch and the firewall.



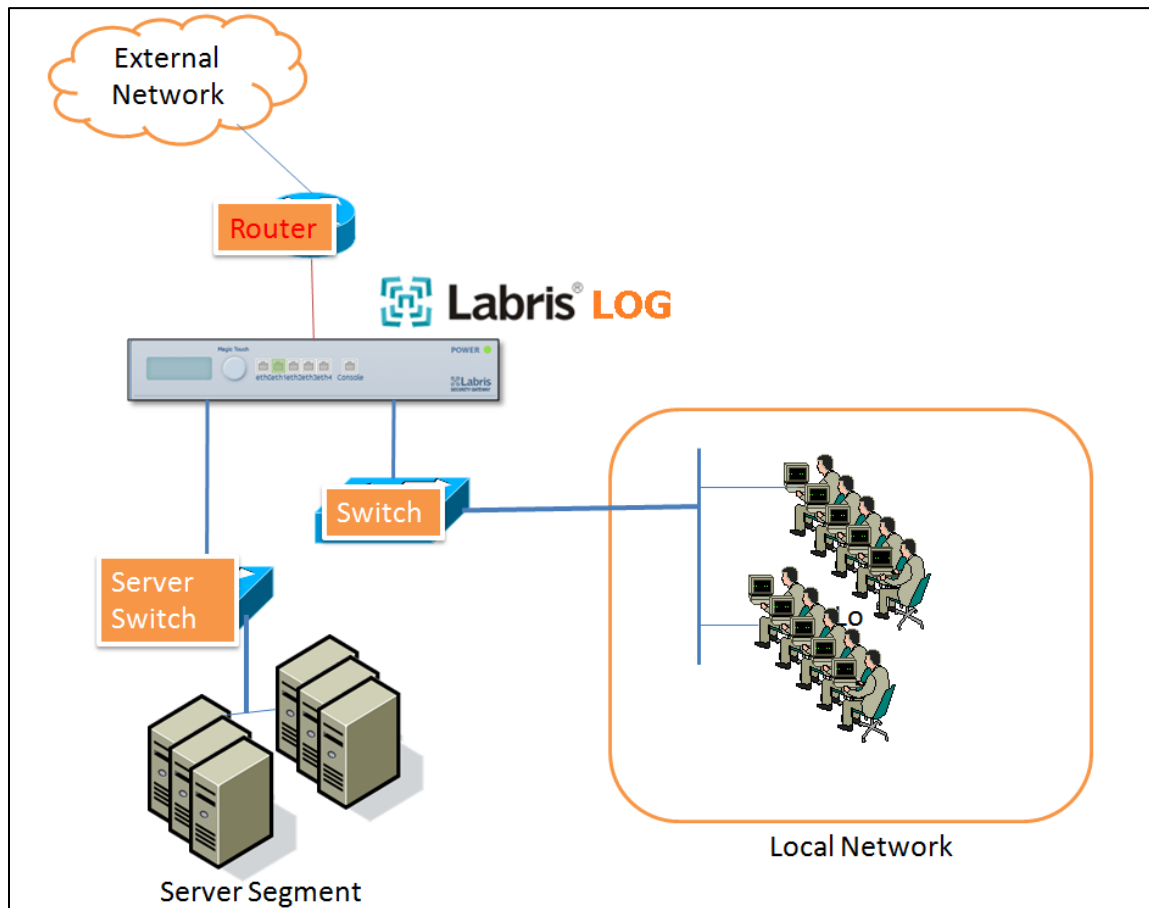
Port mirror/Span port mode

This configuration uses the port mirroring capability on configurable switches. Switches provide methods with the names “port mirror”, “port monitor” or “span port” which are used to transfer a copy of the traffic on a port/ports to another listening port. With this way, a copy of the traffic from the uplink port of a firewall/router is transferred to a listening port of the network switch and Labris LOG is connected to this port of the switch.



Router mode

In this configuration Labris LOG can take on the routing responsibility and easily log the traffic directed to it. For example, in Wauth configurations, Labris LOG will log the Wauth traffic with this method.



Logging with Syslog

With the de facto log sending and receiving protocol syslog, Labris LOG can receive the logs generated by third party systems over TCP or UDP and store each of them in different storage locations.

Logging with SNMP

With the standard information sending and receiving protocol SNMP, Labris LOG can receive the logs generated by third party systems and store each of them in different storage locations.

Receiving logs from Windows based systems via Labris Log Sender

With this method the logs are transferred to Labris LOG via the Labris Log Sender tool which is created for Windows systems which do not support syslog. Labris Log Sender periodically checks for log files under user defined folders and sends them. Thus it is possible to capture IIS, Exchange, and Windows

DHCP logs and send them to Labris LOG.

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 LOG device in eth0 and other end to computer.

Note

•Labris LOG Device will provide default IP address

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 LOG** 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

LRMS into the LABRIS LOG Appliance

LRMS – Labris Report and Monitoring Service

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

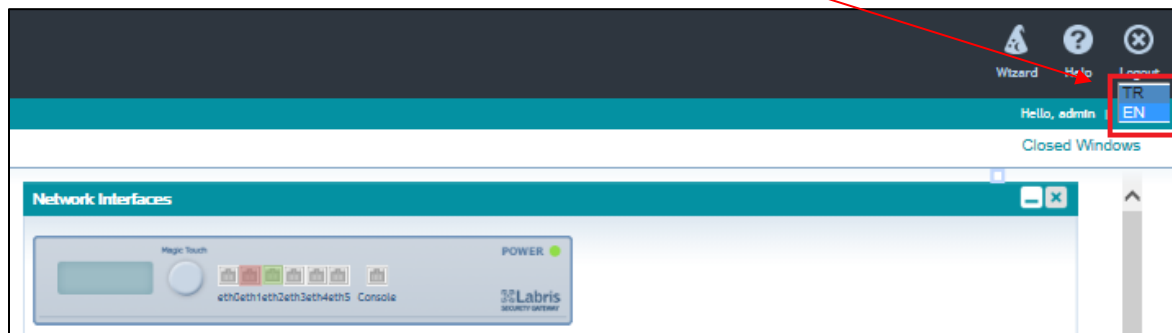
It has a login screen as well as languages selection screen

These are the inputs for LABRIS LOG 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

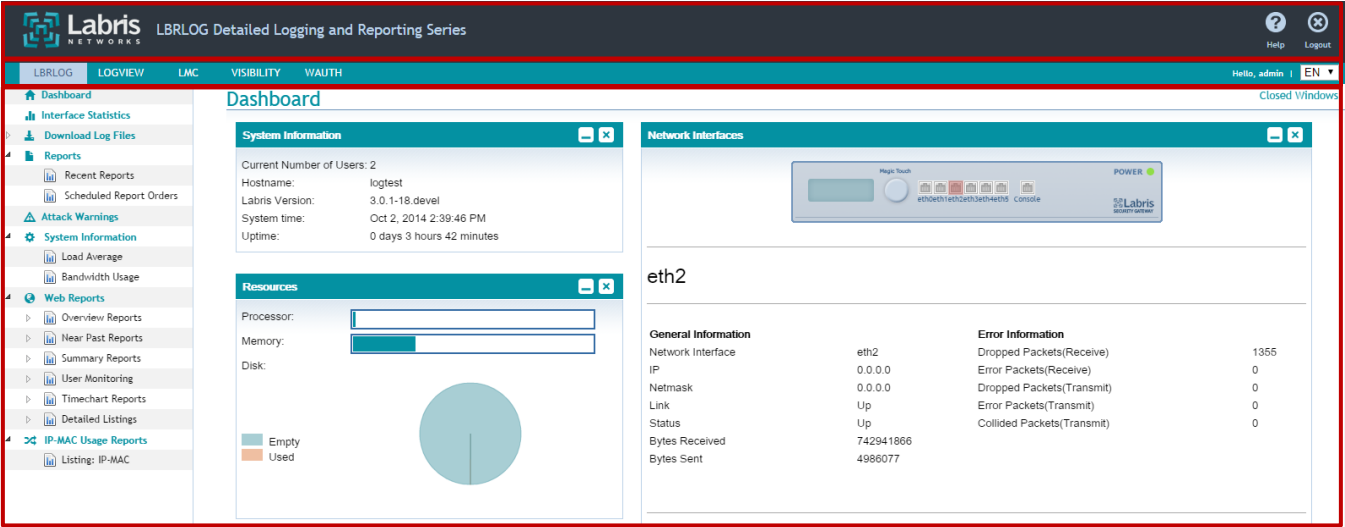
Note

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



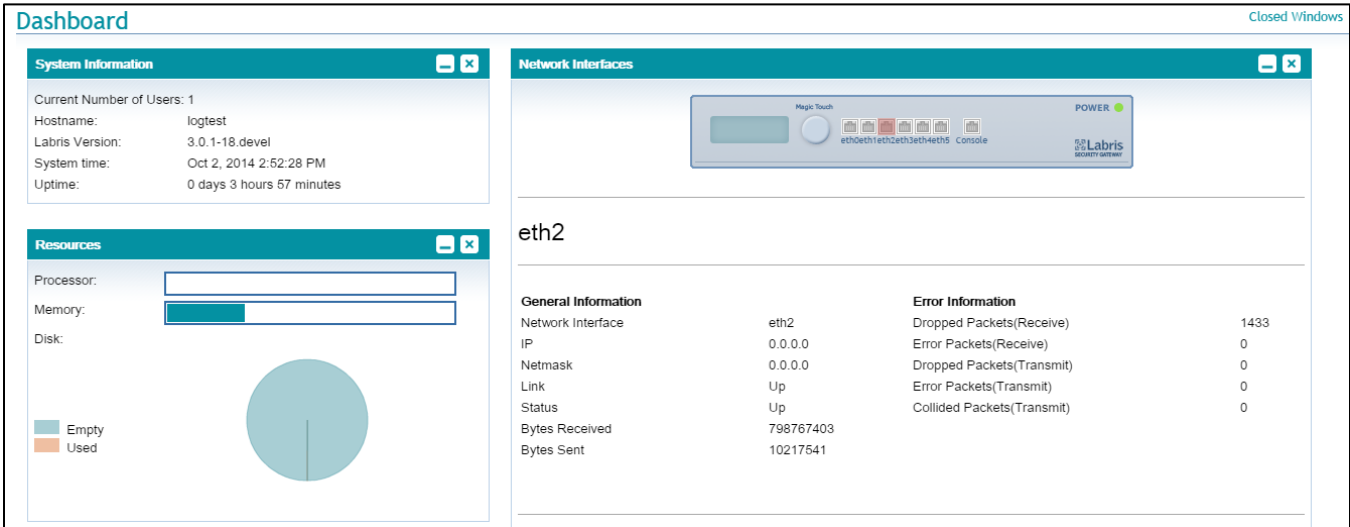
Understanding your landing page or home screen

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



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

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

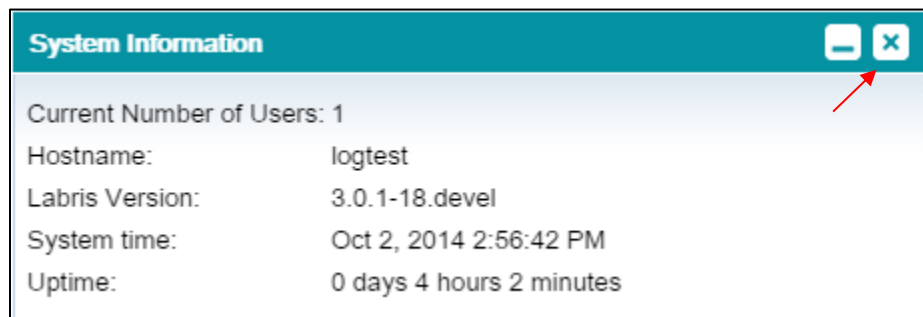


1	System Information	System Information field in the dashboard displays information on the No.of users , Host Name , Labris Version , System Time and Uptime
2	Resources	Resources field displays information on resources(Processors , Memory , Disk) and their utilization levels with diagrams which makes us to understand easily.
3	Network Interfaces	General Information 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 .

How to delete / Enable widgets on the Main Dashboard

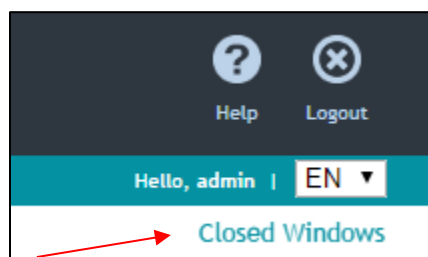
You can delete and redisplay these widgets on the main dashboard based on your need.

To delete the widget click on the “X” icon on each widget as show below.

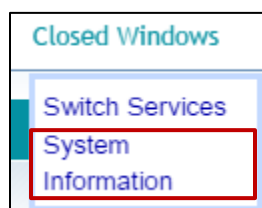


To re-display, you can always click on the <“**Closed windows**” > Choose the widget you would like to see on Dashboard again.

Step1: Click on the “**Closed Windows**”

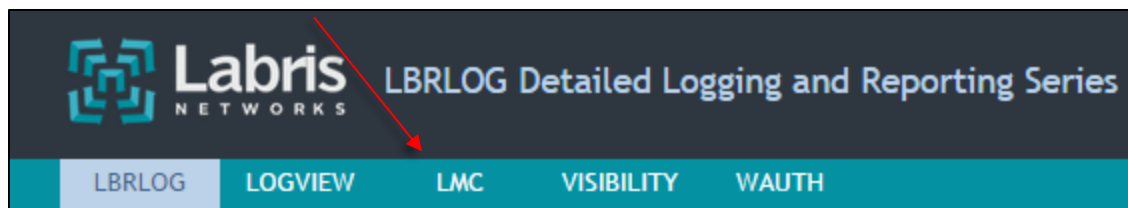


Step2: Select the widget again, which you would like to see on the main dashboard.



Accessing LABRIS LOG through LMC

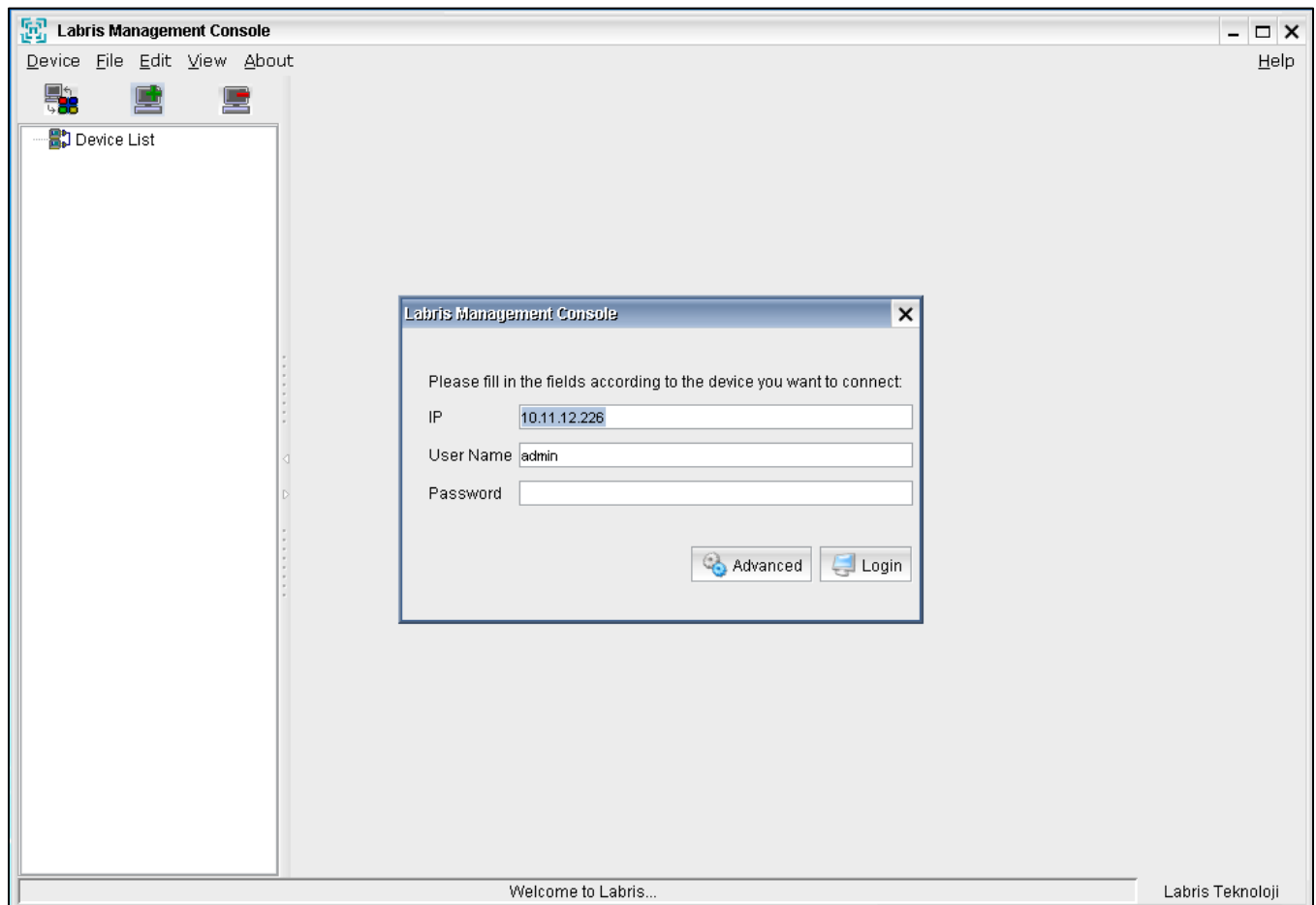
Click on **LMC** tab (Labris Management Console) from the Dashboard.



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

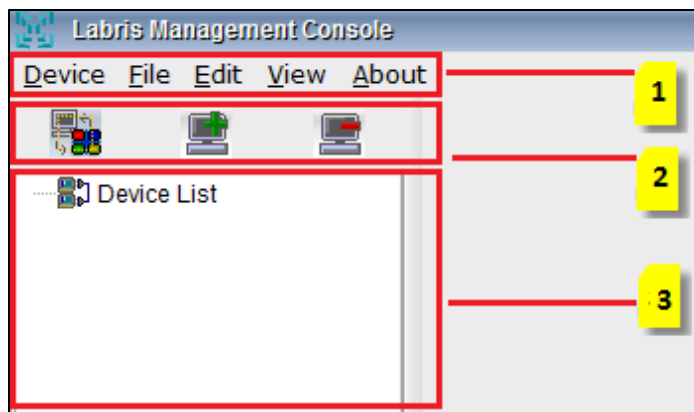
After all the validation and verification, the following LMC screen appears.



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

Labris Management Console (LMC)

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



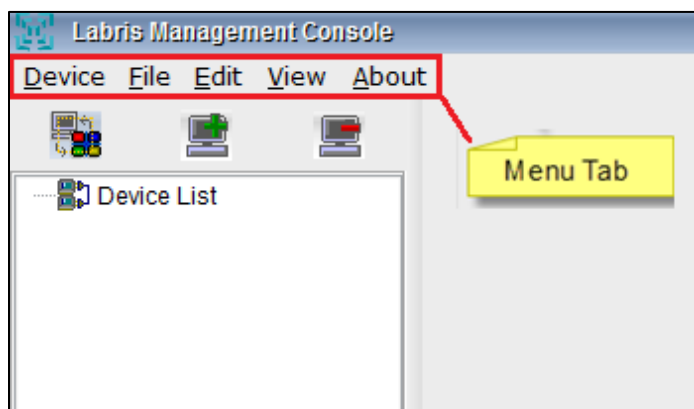
In Labris Management Console we will find three sections.

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

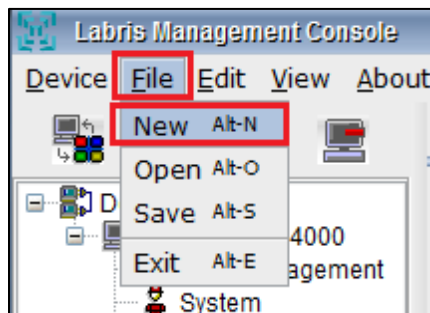
Under **File Menu** we find the following options

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

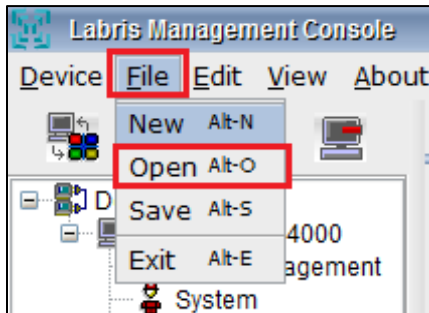
1. Go to **File>New**
2. **New** Options helps us to connect to the **New** Labris Management Console (LMC).

When we click on New the following screen appears.

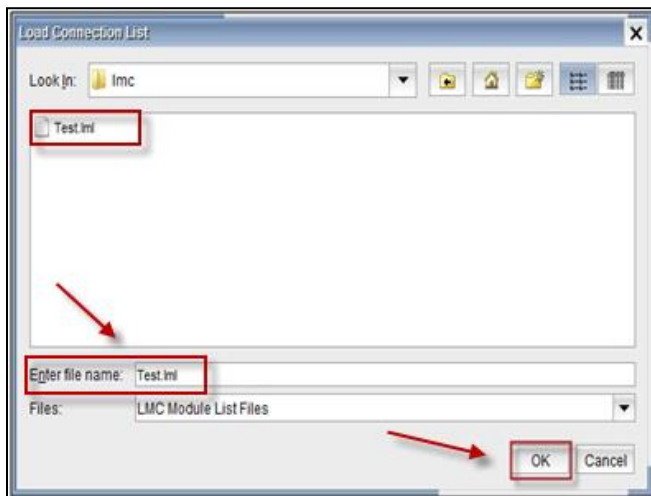


Opening an existing file using LMC

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

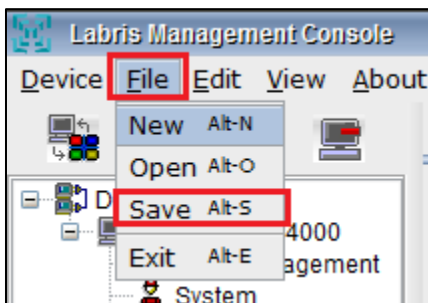


3. Browse the path of the file, Select the **File** and click **Ok**



Saving the files in LMC

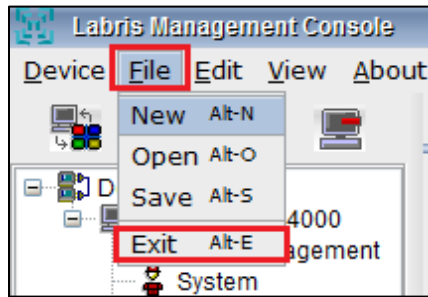
1. Go to **File>Save**



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

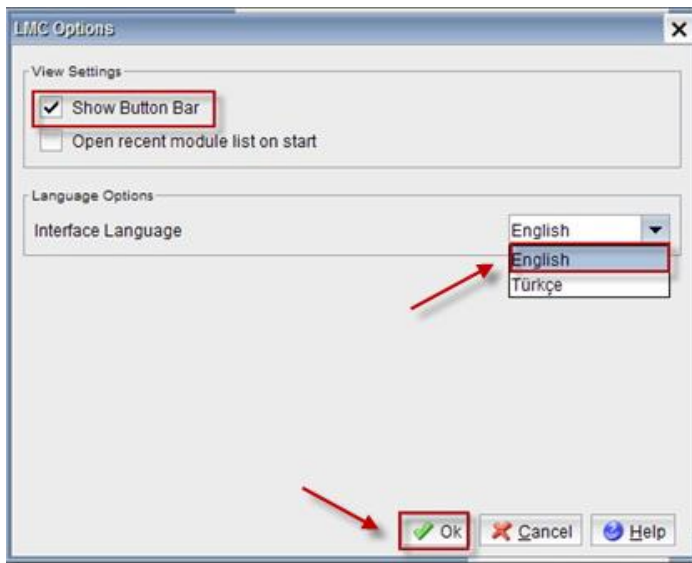
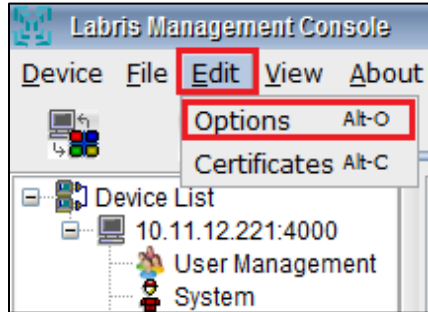
Under **Edit Menu** we find the following options

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

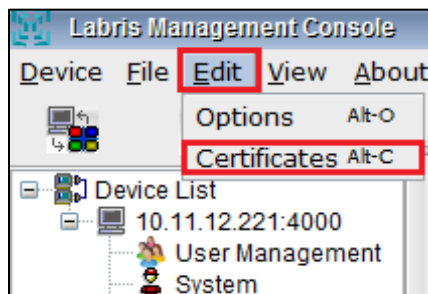
1. Go to **Edit>Options**
2. Using **Options** we can view settings and select interface language in LMC and click “**Ok**” to apply settings.

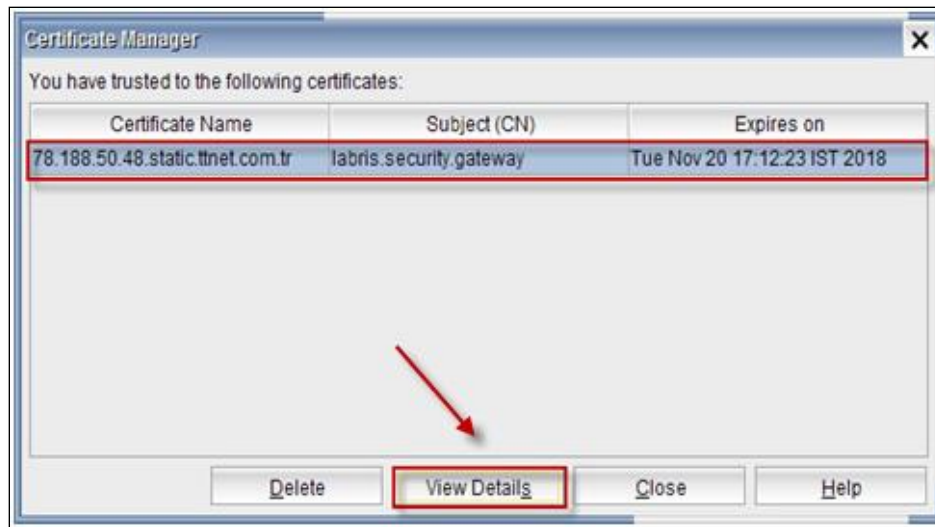
1	View settings	View Settings consists of show button bar and open module list on start. Choose appropriate option
2	Language options	This option enables us to choose preferred language either English or Turkish
3	OK	Select OK to apply the settings
4	Cancel	Select Cancel if we don't want to apply these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



Certificates details in LMC

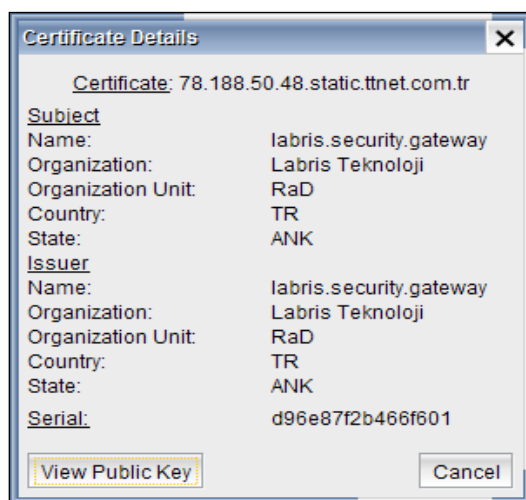
1. Go to **Edit>Certificates**
2. When we click on **“Certificates”** the Certificate manager console gets opened, where we can manage the Certificate using options like Delete, View Details, Close, Help





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

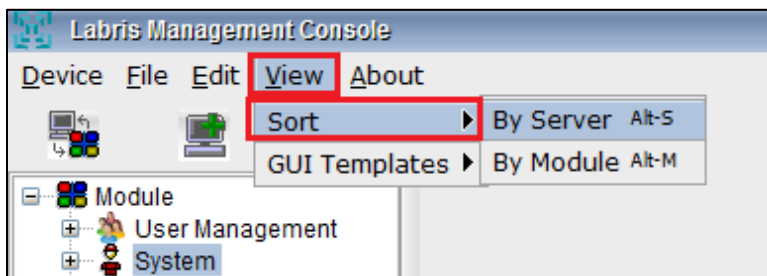
View Menu is one of the option in Menu Tab. **View Menu** helps us to view the contents in different modes depending on the options available in LMC.

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

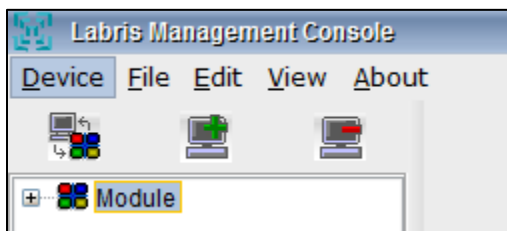
1	Sort	This option helps to sort by server or module
2	GUI Templates	This option helps to change the view of LMC to Aero mode or MacWin mode

Sorting Labris management console

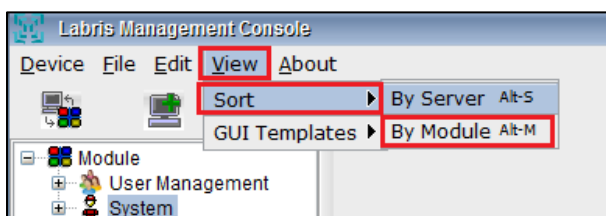
1. Go to **View>Sort> By Server**



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

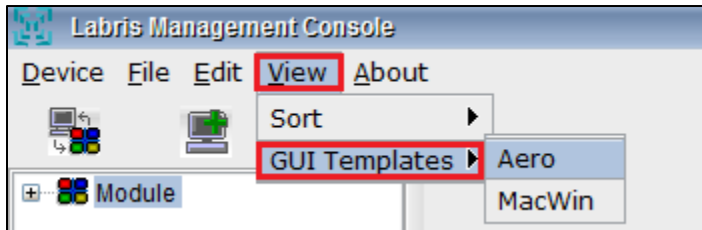


1. Go to **View>Sort> BY Module**
2. When we sort by module the view of the LMC changes as below



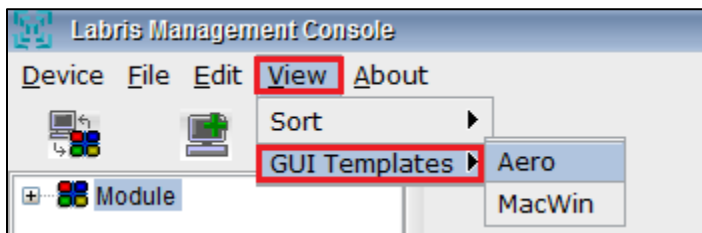
View using GUI Templates option in Aero Mode

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**

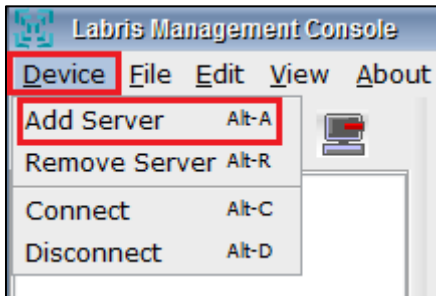
Under **Device Menu** we find the following options

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.

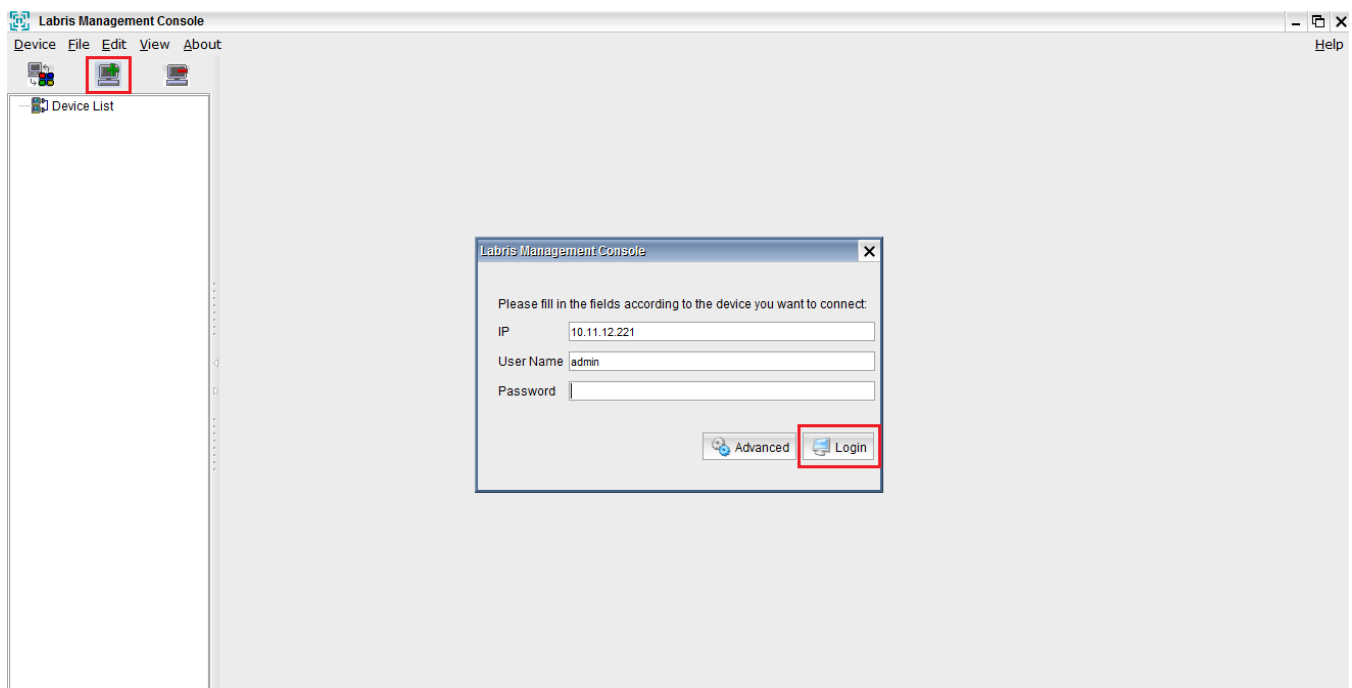
1. Go to **Device>Add server**



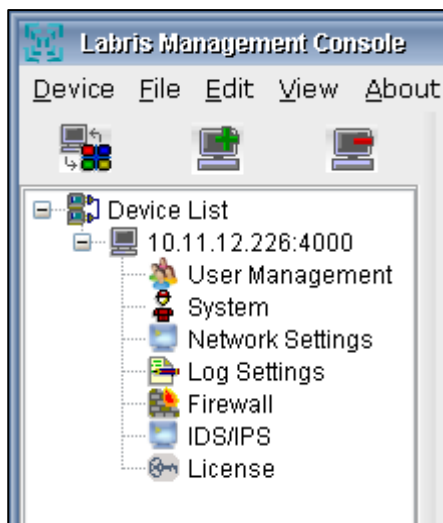
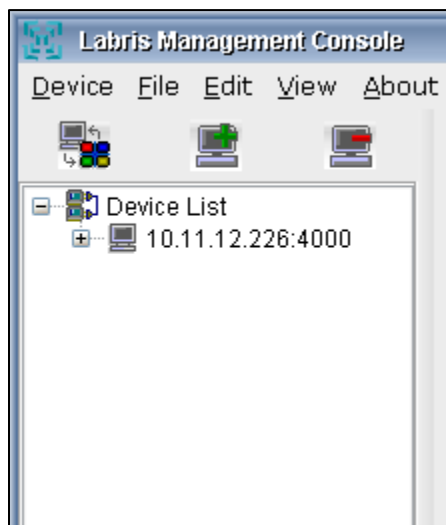
Note

- 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



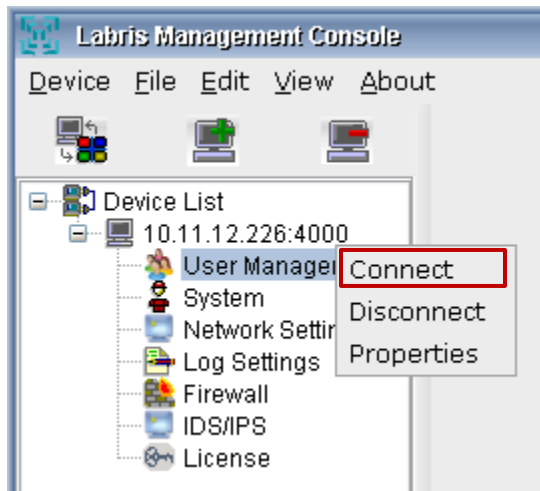
2. After successful authentication process, you will notice your new appliance appearing on LMC's Server list as shown in the following images.



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

Users

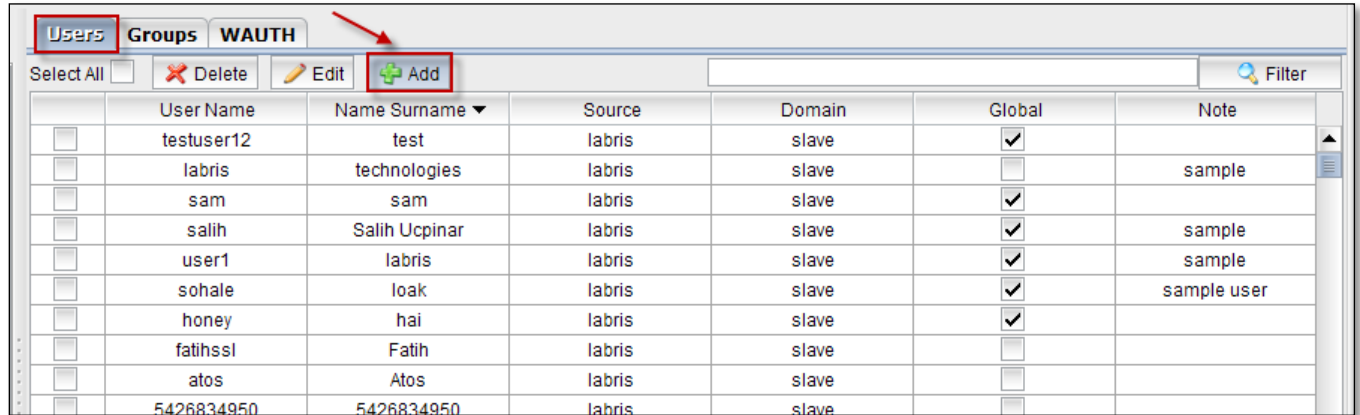
Users Tab in LMC enables us to **Add** new User, **Edit** existing Users, **Delete** User in User Management Section in LMC.

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



Add User

1 User Name sam

2 Name Surname sam

3 Password *****

4 Password Again *****

5 Domain slave

6 ☒ Global

7 Comment

☒ Select Group istpaz 8

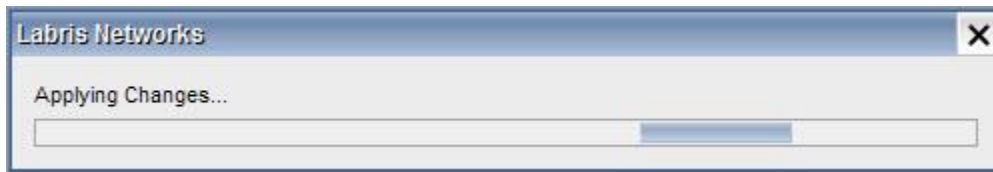
OK Cancel

These are the inputs for adding New User

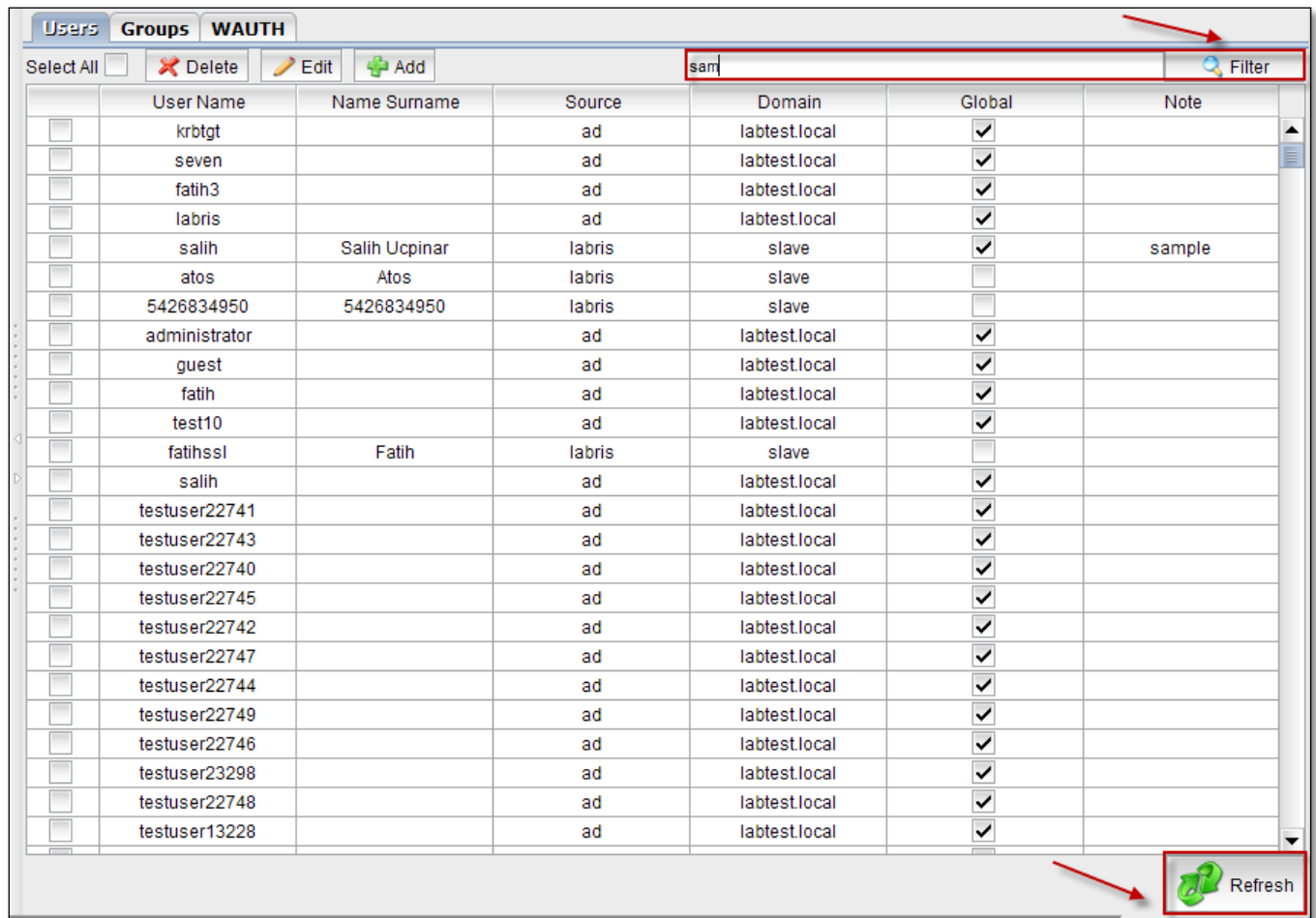
1	User Name	Type the name of the new User
2	Name Surname	Type the Surname of the new User
3	Password	Type Password of the new User s
4	Password Again	Re type the same Password for confirmation
5	Domain	By default Slave is being selected in Domain

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 LOG device.
7	Comment	Type reason for the User creation (Optional)
8	Select Group	You can make a user, member of a group

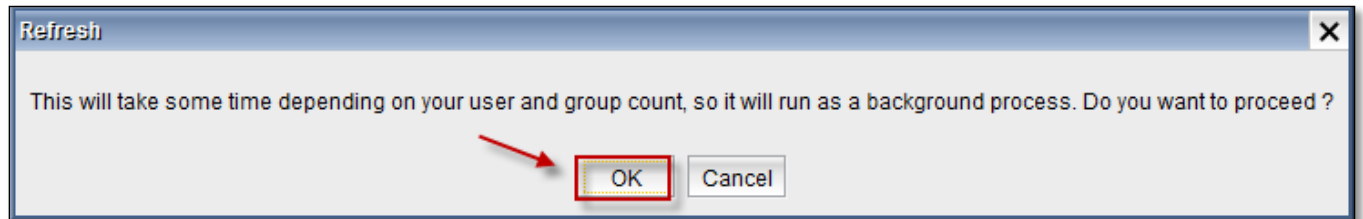
Global, Comment and Select Group fields can be selected according to the User requirement and click on **OK** to apply these settings.



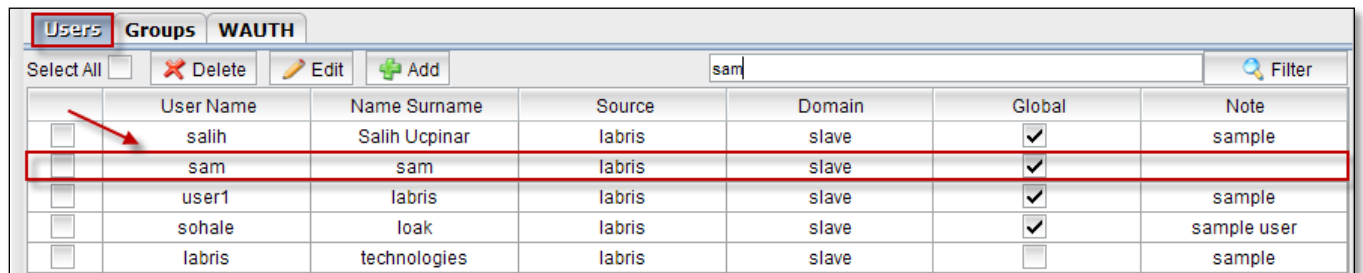
Type the name of the User in the **Filter Tab** to check whether the user is added to the list or not. If the user is not added click on **Refresh** button.



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



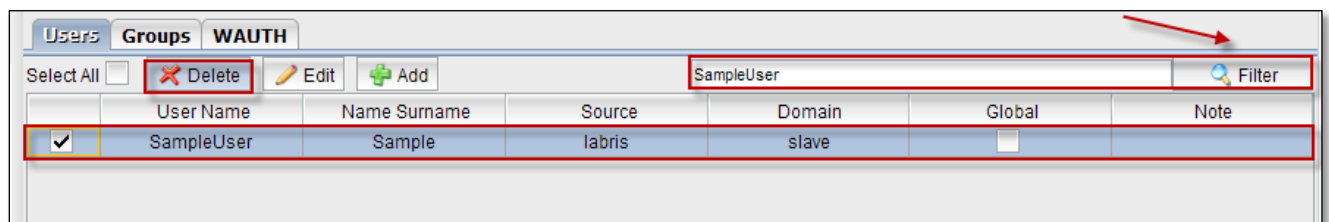
After completing Refresh process type the name of the User in the **Filter tab**, then you can notice the **New User** displaying in the User's list



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**



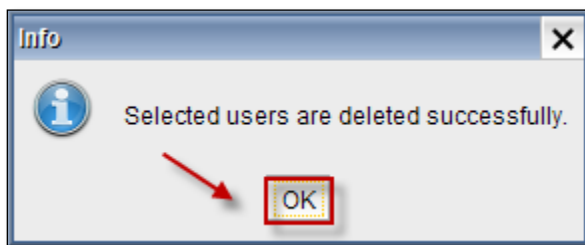
Then the below screen appears, Click **OK** to delete a User in User Management in LMC



It takes some time to **delete** a **User** from User's list

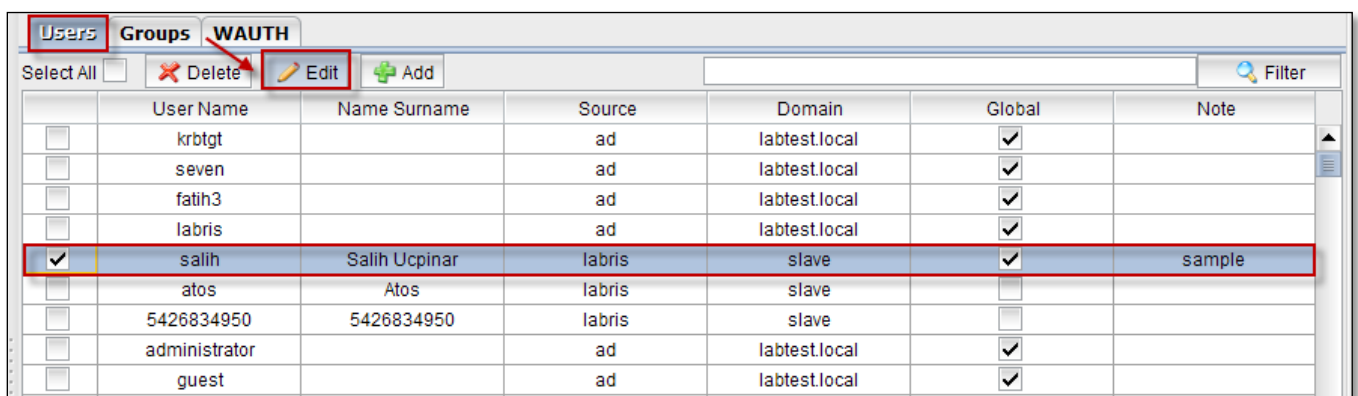


Below screen gives information that the selected User is deleted successfully. Click **OK**



Changing password / Editing User

Select a User from the User's list and click on **Edit Tab**



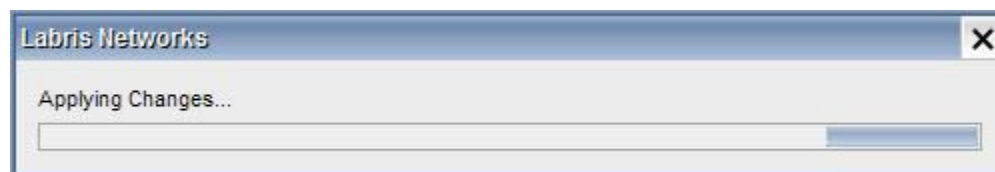
Edit option helps us to change the password of the existing User and edit the comment.

The 'Edit User' dialog box contains the following fields and controls:

- User Name: salih
- Name Surname: Salih Ucpinar
- Password: ***** (Callout 1)
- Password Again: ***** (Callout 2)
- Domain: slave
- ☒ Global
- Comment: sample (Callout 3)
- OK button
- Cancel button

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.

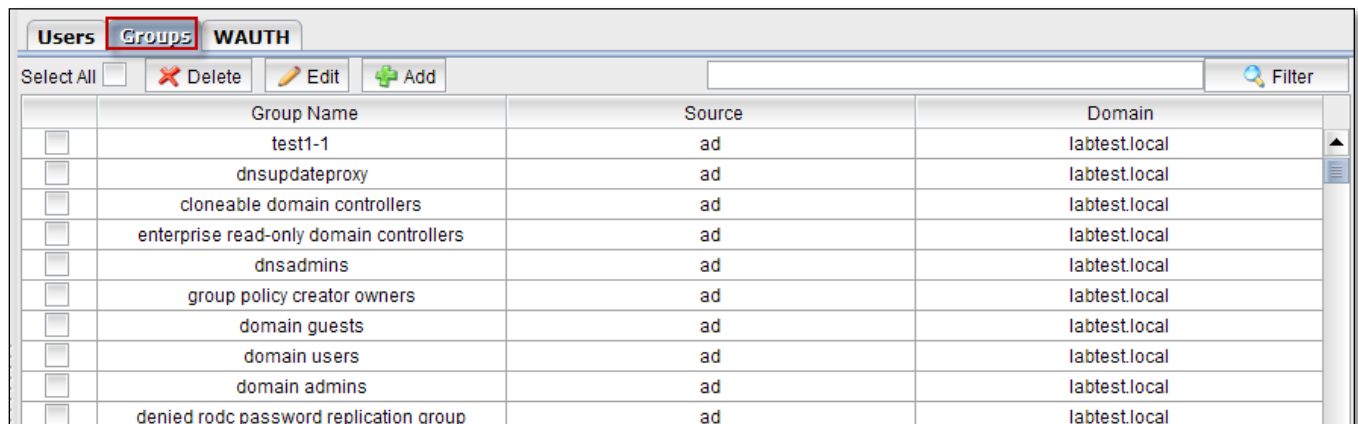





Groups

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**, and **Delete Groups** in User Management Section in LMC.

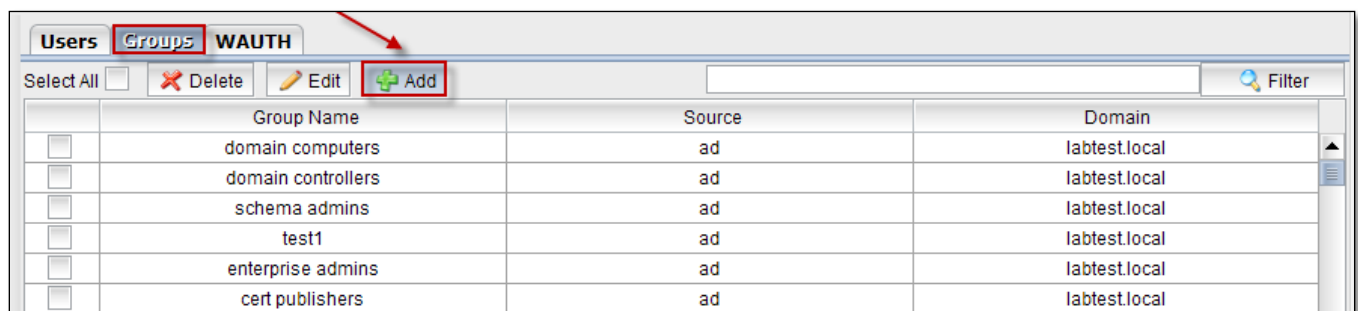
When we click on **Groups Tab** all the existing groups are displayed with the fields **Group Name**, **Source**, **Domain**.






Users Groups WAUTH			
Select All <input type="checkbox"/>	 Delete	 Edit	 Add
			<input type="text"/> Filter
<input type="checkbox"/>	Group Name	Source	Domain
<input type="checkbox"/>	test1-1	ad	labtest.local
<input type="checkbox"/>	dnsupdateproxy	ad	labtest.local
<input type="checkbox"/>	cloneable domain controllers	ad	labtest.local
<input type="checkbox"/>	enterprise read-only domain controllers	ad	labtest.local
<input type="checkbox"/>	dnsadmins	ad	labtest.local
<input type="checkbox"/>	group policy creator owners	ad	labtest.local
<input type="checkbox"/>	domain guests	ad	labtest.local
<input type="checkbox"/>	domain users	ad	labtest.local
<input type="checkbox"/>	domain admins	ad	labtest.local
<input type="checkbox"/>	denied rodc password replication group	ad	labtest.local

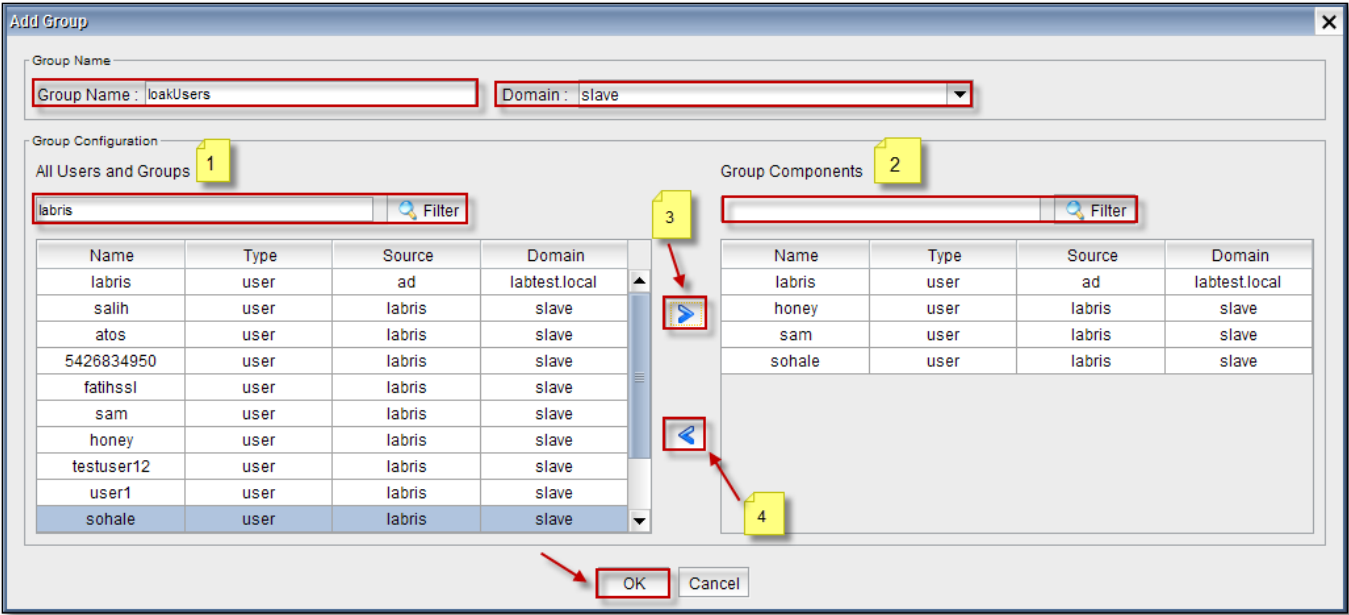
Adding Group

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



Users Groups WAUTH			
Select All <input type="checkbox"/>	 Delete	 Edit	 Add
			<input type="text"/> Filter
<input type="checkbox"/>	Group Name	Source	Domain
<input type="checkbox"/>	domain computers	ad	labtest.local
<input type="checkbox"/>	domain controllers	ad	labtest.local
<input type="checkbox"/>	schema admins	ad	labtest.local
<input type="checkbox"/>	test1	ad	labtest.local
<input type="checkbox"/>	enterprise admins	ad	labtest.local
<input type="checkbox"/>	cert publishers	ad	labtest.local



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



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

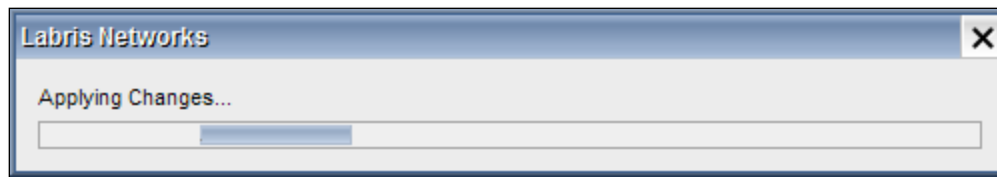
1	Group Name	Type name of the New Group
2	Domain	In this field slave is selected by default

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

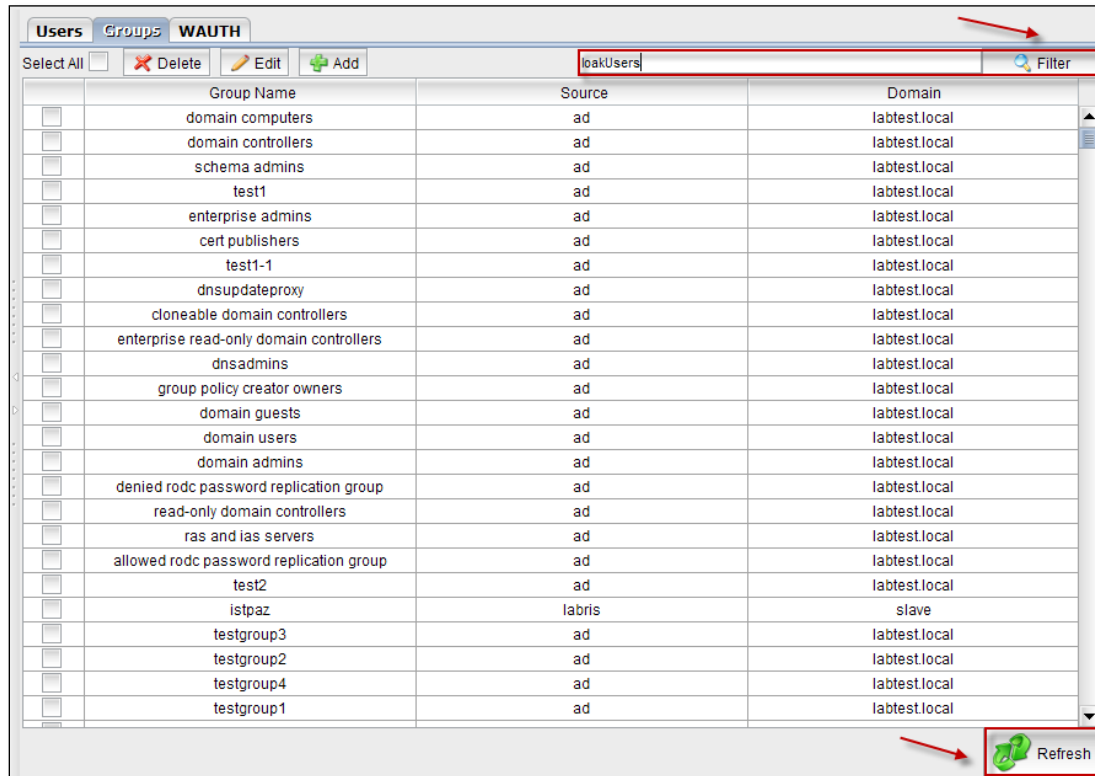
1	All Users and Groups	All the users and groups are displayed in this field
2	Group Components	Users in specific Group are displayed in this field
3		Click this icon to add Users in to Group Components
4		Click this icon to delete Users from the Group Components

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

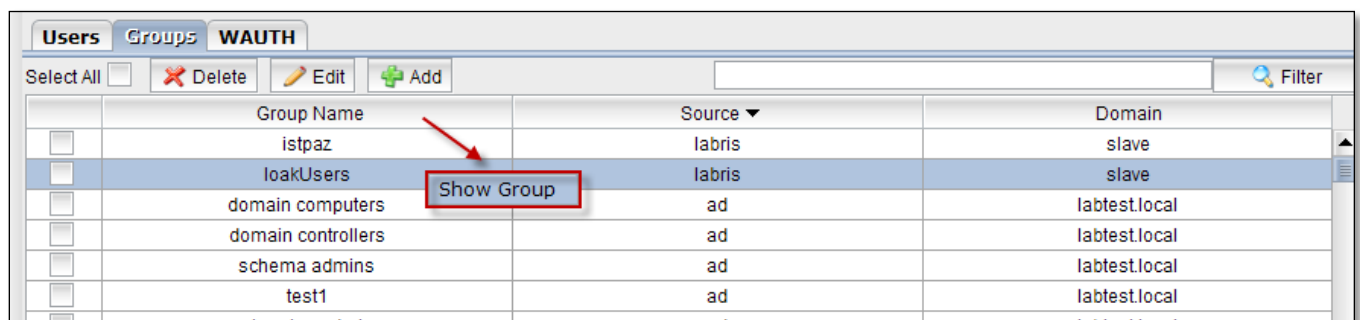
It takes some time to apply changes.



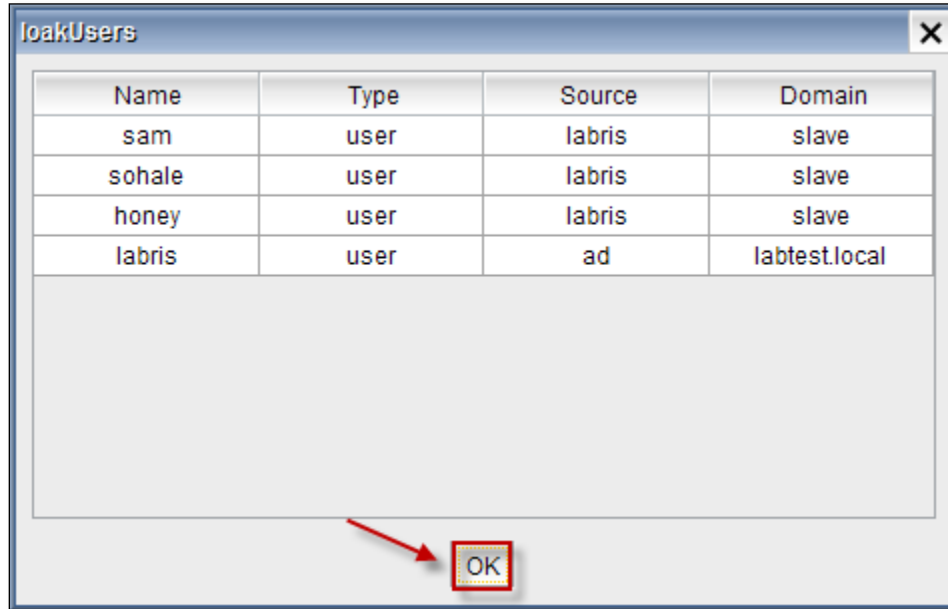
Type the **New Group** name in the **Filter** tab and click **Refresh** to find out the **New Group** in the **Group's** list is added or not.



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

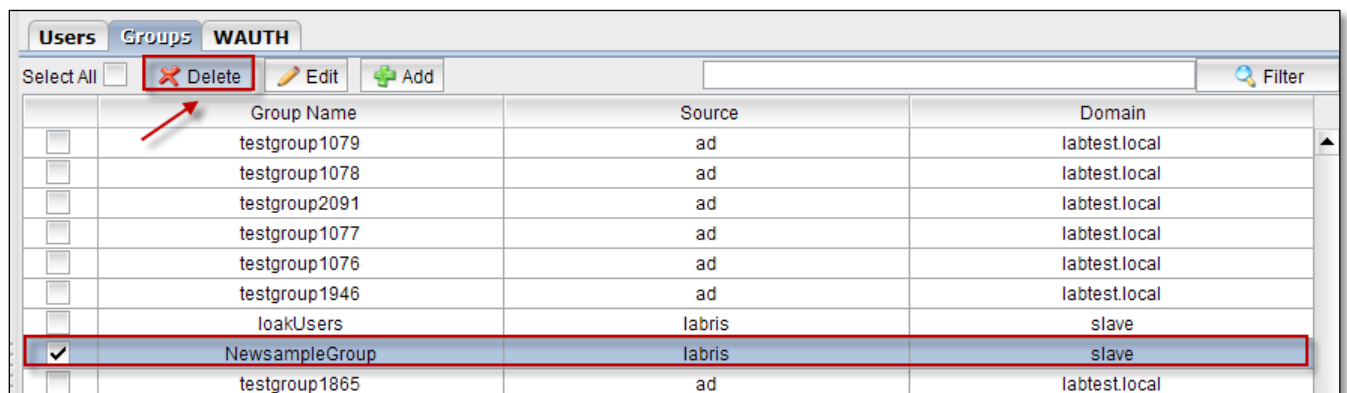


When you click on **Show Group**, Users in that **group** are displayed. Click **OK** to close the current tab.

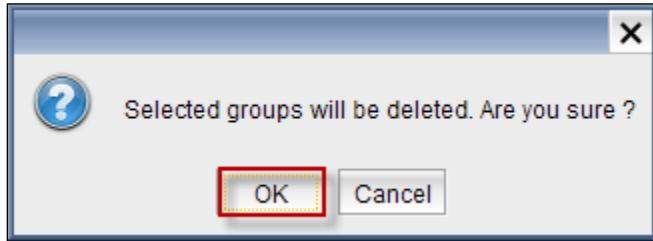


Deleting Group

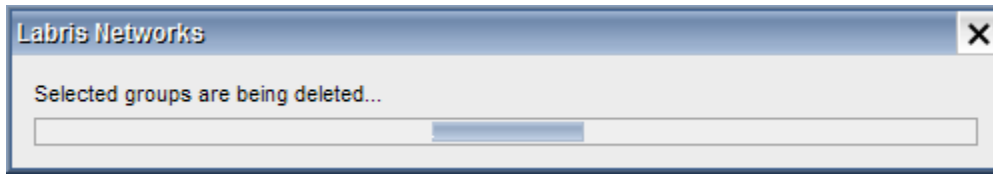
Select the Group from the Group's list and click on **Delete** Tab.



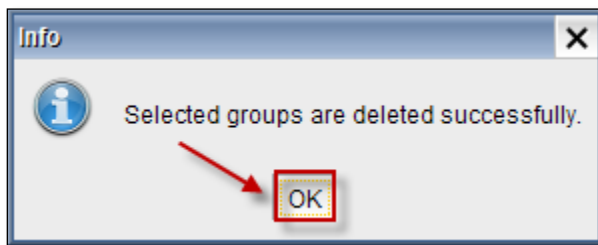
Warning screen is displayed; Click **OK** to delete a Group from the LMC.



Deleting process is in progress.

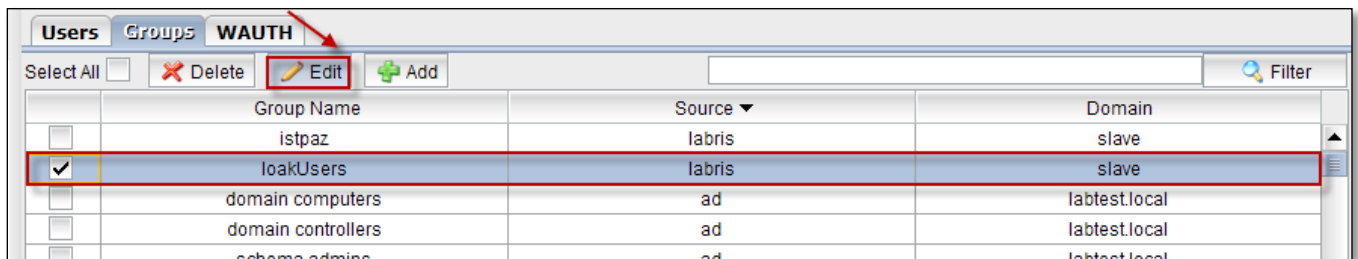


Below screen appears stating that the selected Group is **deleted** successfully & click **OK** to close the current tab



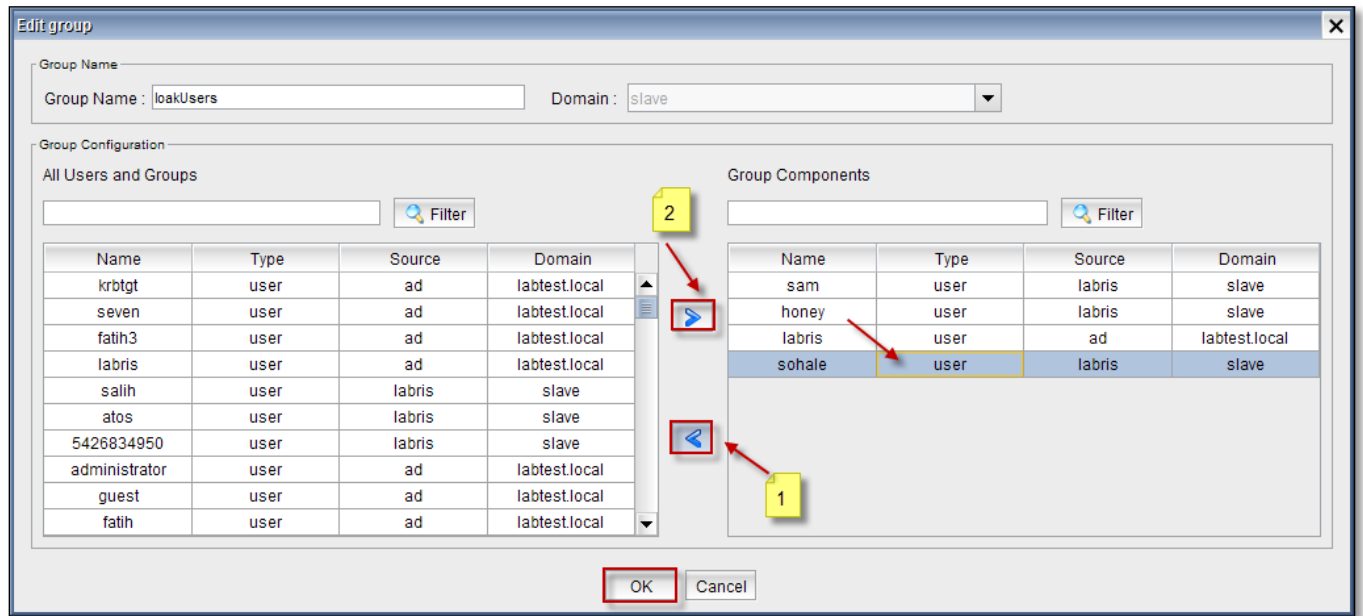
Editing Group

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

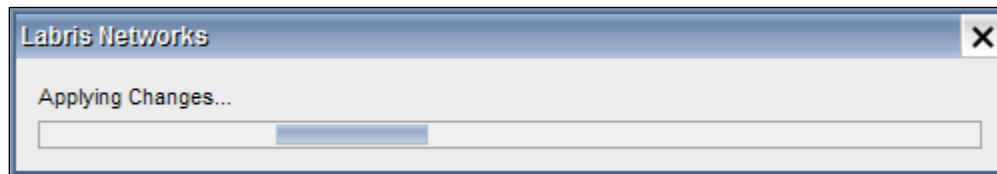


Select the User from the **Group** components list and click on the **icon 1** to remove User from the **Group** Components and click **OK**

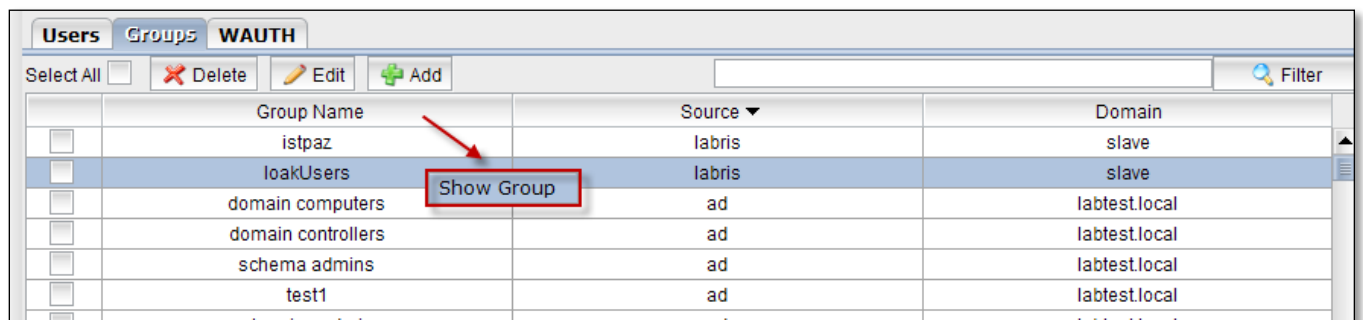
Select the **User** from All Users and **Groups** field and click on the **icon 2** to add Users in to Group Components list and click **OK**



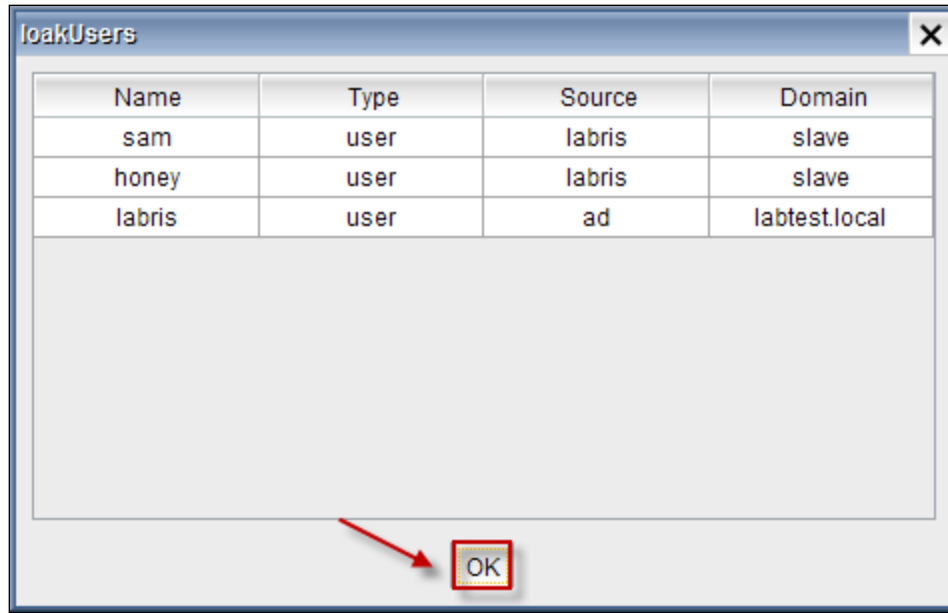
It takes some time to apply the changes.



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



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



Wauth

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

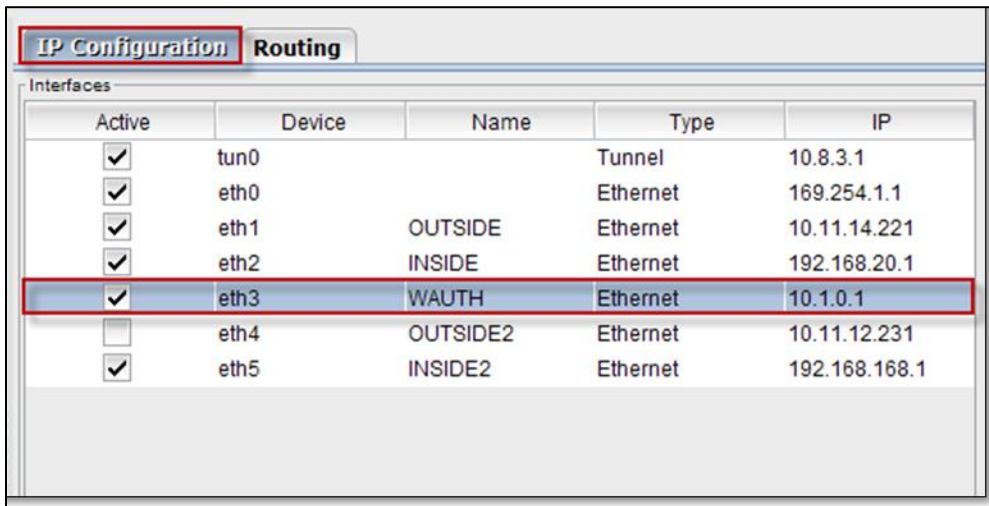
WAuth (Wireless Authentication) in LMC enables us to **Add New WAuth Interface, Edit existing WAuth Interface, and Delete WAuth Interface** in User Management Section in LMC.

Your device configuration for WAUTH

First Step:

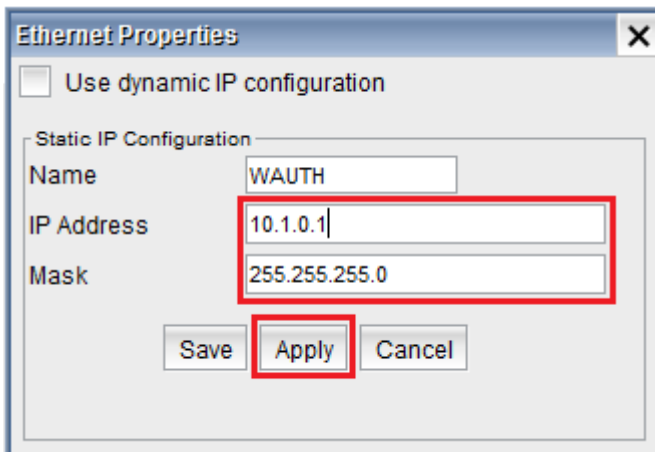
Add a separate Network for WAuth in the Network settings module. Select Network settings for selected interface.

Choose the interface you want to choose for enabling WAuth.



Active	Device	Name	Type	IP
<input checked="" type="checkbox"/>	tun0		Tunnel	10.8.3.1
<input checked="" type="checkbox"/>	eth0		Ethernet	169.254.1.1
<input checked="" type="checkbox"/>	eth1	OUTSIDE	Ethernet	10.11.14.221
<input checked="" type="checkbox"/>	eth2	INSIDE	Ethernet	192.168.20.1
<input checked="" type="checkbox"/>	eth3	WAUTH	Ethernet	10.1.0.1
<input type="checkbox"/>	eth4	OUTSIDE2	Ethernet	10.11.12.231
<input checked="" type="checkbox"/>	eth5	INSIDE2	Ethernet	192.168.168.1

- Edit Interface IP address or Name;



Ethernet Properties

☐ Use dynamic IP configuration

Static IP Configuration

Name: WAUTH

IP Address: 10.1.0.1

Mask: 255.255.255.0

Buttons: Save, Apply, Cancel

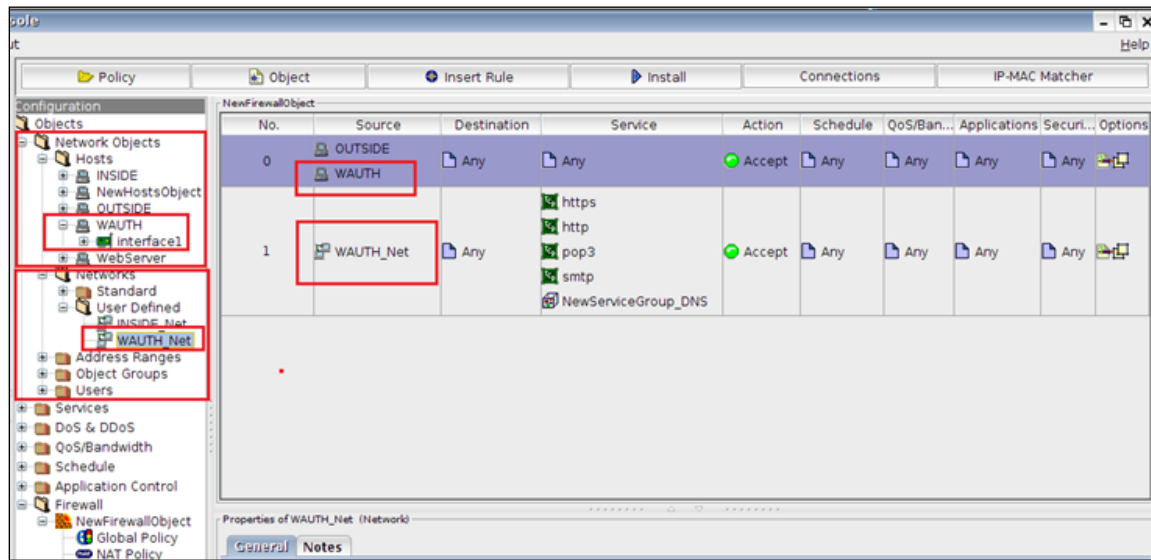
Second Step:

Create a DHCP Server for WAUTH;

[Click for DHCP configuration.](#)

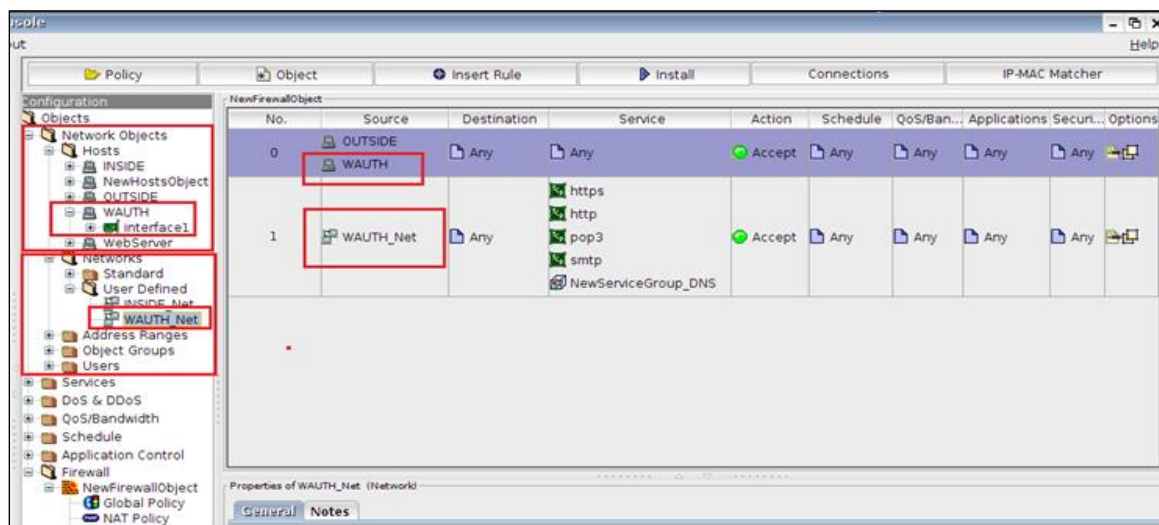
Third Step:

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)



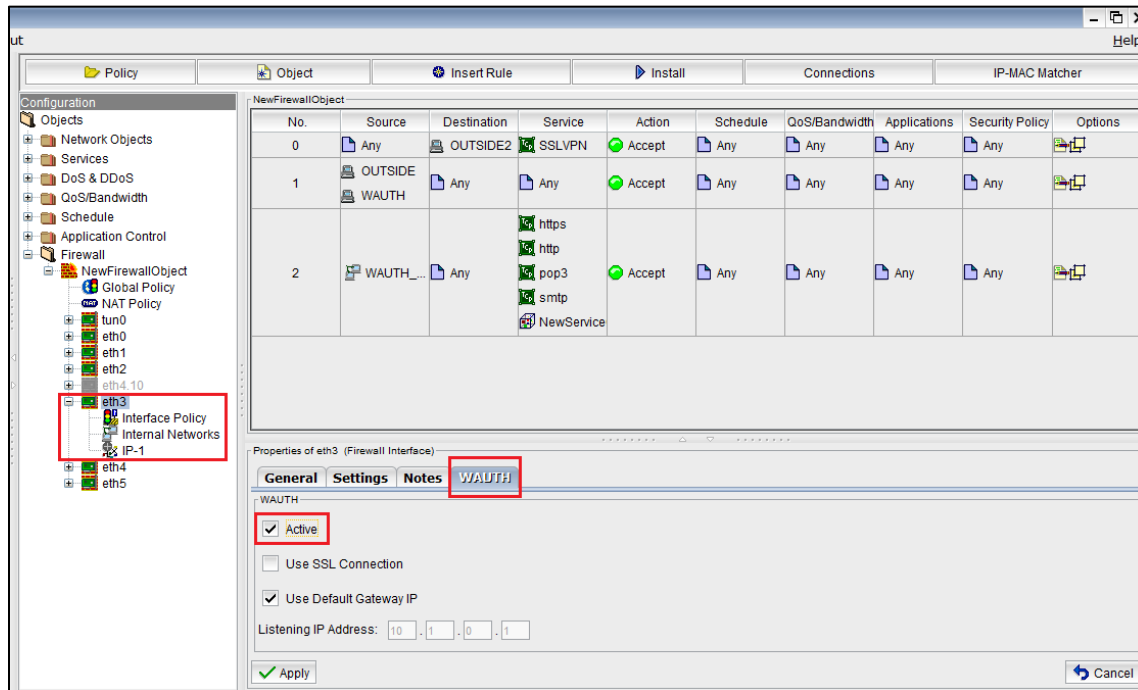
Fourth Step:

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.



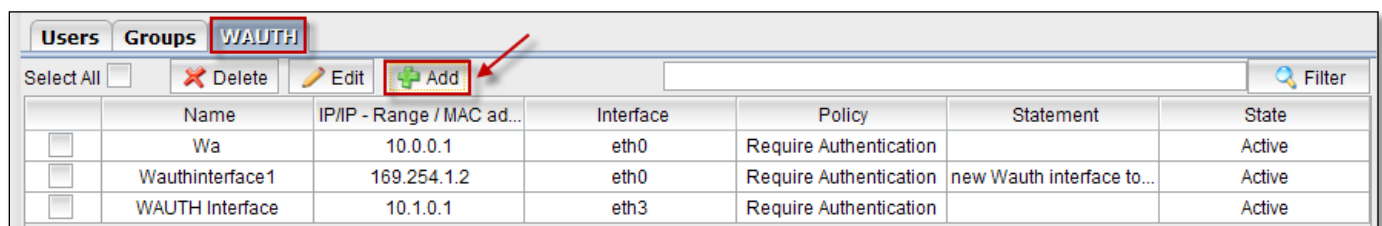
Sixth Step:

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)

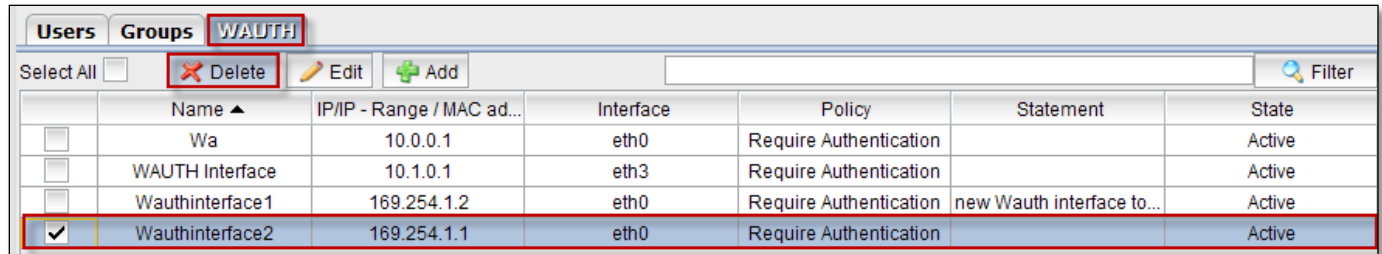
Click **Ok**.

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

Users Groups WAUTH						
Select All	<input type="checkbox"/>	Delete	Edit	Add		Filter
	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"/>	Wauthinterface1	169.254.1.2	eth0	Require Authentication	new Wauth interface to...	Active
<input type="checkbox"/>	Wauthinterface2	169.254.1.1	eth0	Require Authentication		Active
<input type="checkbox"/>	WAUTH Interface	10.1.0.1	eth3	Require Authentication		Active

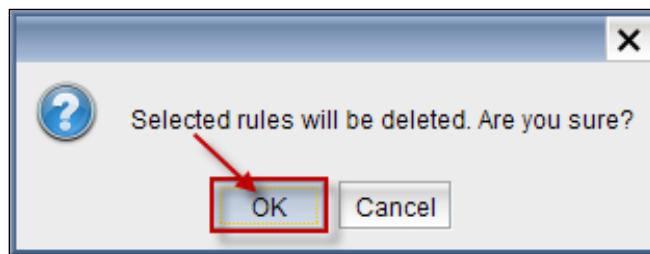
Deleting WAUTH policy

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

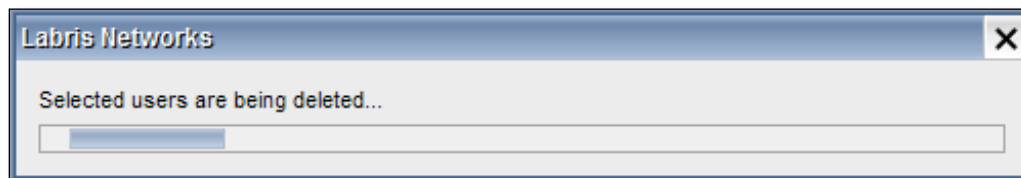


	Name ▲	IP/IP - Range / MAC ad...	Interface	Policy	Statement	State
<input type="checkbox"/>	Wa	10.0.0.1	eth0	Require Authentication		Active
<input type="checkbox"/>	WAUTH Interface	10.1.0.1	eth3	Require Authentication		Active
<input type="checkbox"/>	Wauthinterface1	169.254.1.2	eth0	Require Authentication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

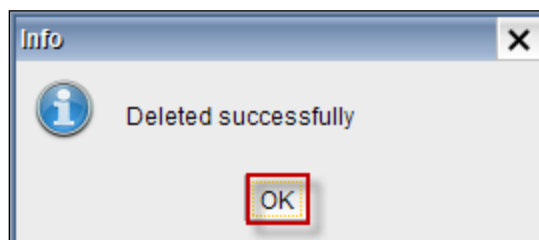
Warning screen is displayed, Click **OK** to delete the Interface



Deleting process is in progress.

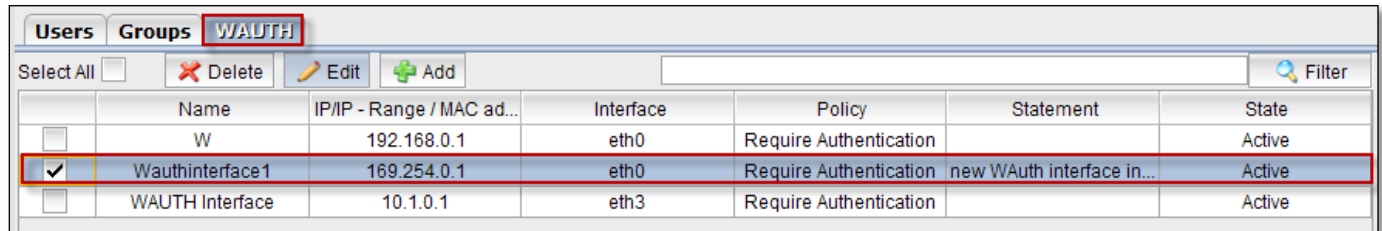


Below screen appears stating that **Deleted** successfully & click **OK** to close the current tab.



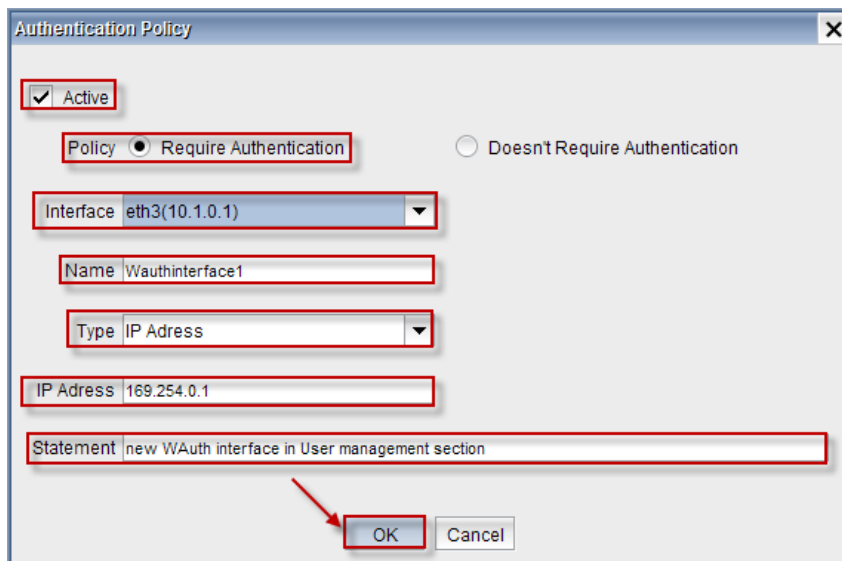
Editing WAUTH Policy

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 Address

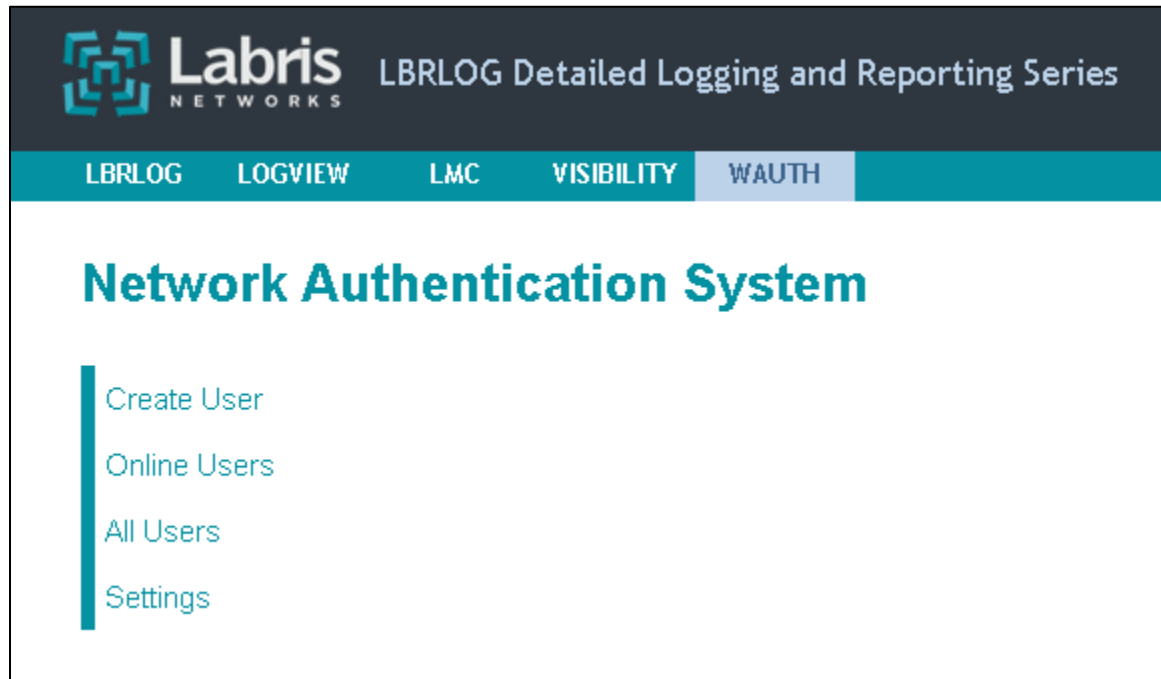
IP Address: 169.254.0.1

Statement: new WAuth interface in User management section

OK Cancel

Click **Ok**.

Wauth Web Admin Portal



Settings

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

Default

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	Welcome message is displayed in English
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.

The screenshot shows a web interface for configuring subnet rules. At the top, there's a tab labeled 'Settings - Default'. Below it, a 'Setting Rule:' dropdown menu is set to 'Default'. A horizontal tab bar contains five tabs: 'Subnet Rules' (which is highlighted in a darker teal), 'General', 'UI', 'ACL', and 'TCKN Wauth'. The main content area is divided into two sections. The top section has a 'Rule name:' label followed by a text input field containing 'Default'. Below this is a 'Subnet list:' label followed by a text input field containing '0.0.0.0/0.0.0.0'. A large, light gray rectangular area with a small diagonal handle in the bottom right corner is positioned below the subnet list input, likely for adding or editing multiple subnets. At the bottom of the main content area, there is a teal 'Save' button.

General Settings

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

Authentication methods in WAUTH is configured in General tab.

Labris

Labris Güvenlik Ağ Geçidi

LSGSLOGVIEWLMCVISIBILITYWAUTHSSLVPNAVAS

Network Authentication System

Create User

Online Users

All Users

Settings

Settings - Default

Setting Rule: Default

Subnet Rules

General

UI

ACL

TCKN Wauth

Welcome message:

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

1

Welcome message (EN):

Your access to the system is granted. By using the address bar of your browser, you can now start surfing.

2

Local Authent. Format:

TC Identification

3

SMS Wauth:

Disable

4

Active Directory Authent.

Disable

5

Hotel Integration:

Disable

6

TC Identity NVI Confirmation:

Enable

7

Passport Wauth:

Disable

8

Agreement Enable/Disable:

☐

9

Agreement:

Show Agreement

10

Agreement (EN):

Show Agreement (EN)

11

Timeout Enable/Disable:

☒

12

Timeout Period:

2

(minutes)

13

Authentication Type:

MAC

14

Ingress Session Enable/Disable:

☐

15

Reference Emails/Domains:

Enter your input here

Add

16

Reference Timeout (seconds):

7200

17

Smtp Server Address:

18

Smtp Mode:

Normal

19

Smtp Port:

20

Smtp Username:

21

Smtp Password:

22

Smtp Mail From:

23

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	Smtp Server Address	We can set smtp server address
19	Smtp Mode	We can choose smtp mode (TLS, SSL, Normal
20	Smtp Port	We can set port number for smtp protocol
21	Smtp Username	We can set username for smtp server
22	Smtp Password	We can set password for smtp server
23	Smtp Mail From	We can set mail from field in sent mail

Click on **Save** to save the changes

Settings of Hotel Authentication

Select **Hotel** tab

The screenshot shows the 'Hotel' tab in the settings interface. It contains the following fields and controls:

- 1. Default: Default (dropdown)
- 2. Hotel Name: HOTEL1 (text)
- 3. Product Type: Fidelio (OracleDB) (dropdown)
- 4. MAC Address: 112233445566 (text)
- 5. Machine Port: (text)
- 6. Real Name: DB_Hotel (text)
- 7. Real Name: DB_Users (text)
- 8. Username: dbadmin (text)
- 9. Password: (password)
- 10. Username Field Name: (text)
- 11. Password Field Name: (text)
- 12. Name Field Name: (text)
- 13. Surname Field Name: (text)
- 14. Departure Date: (text)
- 15. Timeout: 0 (mins) (text)
- 16. Infinite timeout: ☐ (checkbox)
- 17. Multiple Login: ☐ (checkbox)

Buttons: Test, Save

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	Departure Date (optional)
15	Timeout	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 tab 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.

Settings

General

Hotel

SMSWauth

AD

UI

Default: Default

1

Account Quota: 1440 (mins)

2

Account Expiration Date: 24 (hours)

3

Timeout: 1440 (mins)

4

Cust. Serv. Tel: 0500000000

5

Comp. Mobile***: 5426834950

6

Cust. Serv. Email: destek@labrisnetworks.c

7

Common Key Enable/Disable: ☒

8

CK Option: Automatic

9

CK Period: 1440 (mins)

10

Common Key: QGMV8M

11

CK Username: test

12

CK Password: ****

13

TC Identification: SMS ile kayıt
olabilmek için lütfen
danışmadan ortak
anahtarını temin ediniz.

14

TC Identification: For registering with
SMS, please get the
common key from
advisory.

15

SMS sending will be afforded by the
company*: ☐

16

Help page for SMS authentication: ☐

17

Title of SMS authentication help page: Labris Networks

18

Subtitle of SMS authentication help
page: Wauth Ağ Yetkilendirme

19

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

20

Remained Token**: 0

Buy tokens

21

Show Common Key

22

Save

***If only corporate and foreign numbers (numbers, which are not permitted to use Mobile Sale) SMS payments wanted to be afforded, this option should not be checked

***When remained token is 50 or 25, an SMS will be send to company mobile phone, which will be suggesting to buy tokens.

***A phone number, that is permitted for the use of Mobile Sale, which will be used for buying tokens.

For more token purchasing demand, please click [here](#).

1	Default	Select User Group
2	Account Quota	Mention Account Quota
3	Account Expr. Date	Mention Account expiration date
4	Timeout	Mention Timeout Period
5	Cust. Serv. Tel	Type Customer Service Telephone number
6	Comp. Mobile	Type Company Mobile Name
7	Cust. Serv. Email	Type Customer Service Email address
8	Common Key	We can enable or disable Common Key
9	CK Option	We can Automatic or Manuel Common Key
10	CK Period	Expiration time for common key
11	Common Key	Mention Common Key
12	CK Username	Type Common Key Username
13	CK Password	Type Common Key Password
14	CK Instructions	Common Key Instructions displayed in Turkish
15	CK Instructions (EN)	Common Key Instructions displayed in English
16	SMS	Enable or disable SMS sending.
17	Help	Enable or disable Help page for SMS authentication
18	Title	Title of SMS authentication help page
19	Subtitle	Subtitle of SMS authentication help page
20	Message	Message of SMS authentication help page
21	Buy Tokens	Buy Tokens web page to open
22	Show Common Key	Common Key web page to open

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

Active Directory Authentication

Labris LOG should be integrated with Active Directory before using Wauth AD Authentication mode. Use this document's [NTLM Authentication AD Configuration](#) part for this configuration. Follow the steps below after integration:

Select **AD** (Active Directory tab)

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

Settings

General

Hotel

SMSWauth

AD

UI

AD Domain Name:

1

Disable Group Name:

☐

2

AD Workgroup:

3

AD Group Name:

4

Timeout:

Unlimited

(hours)

5

Infinite timeout:

☒

6

AD Quota:

Unlimited

(hours)

7

Infinite quota:

☒

8

AD Expire After:

Unlimited

(hours)

9

Infinite Expr Time:

☒

10

Test

Save

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: (eng)

9

Login Page Header:

10

Login Page Header: (eng)

11

Login Page Footer:

12

Login Page Footer: (eng)

13

Username Caption:

14

Username Caption: (eng)

15

Password Caption:

16

Password Caption: (eng)

17

Login Button Caption:

18

Login Button Caption: (eng)

19

Logout Button Caption:

20

Logout Button Caption: (eng)

21

Background Color:

22

Header/Footer Font Color:

23

Page Title Background Color:

24

Page Title Font Color:

25

Default Domain Choice:

26

Save

Preview

Reset Color Schema


Reset All Settings

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 an 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.


Labris
NETWORKS

Labris Güvenlik Ağ Geçidi

LSGS
LOGVIEW
LMC
VISIBILITY
WAUTH
SSLVPN
AVAS

Network Authentication System

Create User
Online Users
All Users
Settings

Settings - Default

Setting Rule: Default

Subnet Rules
General
UI
ACL
TCKN Wauth

Default Group: Default 1

Multiple Login: 2

Infinite Quota: 3

Account Quota: 1440 (mins) 4

Infinite Account: 5

Timeout: 1440 (mins) 6

Account Expiration Date: 24 (hours) 7

Cust. Serv. Tel: 3122101490 8

Cust. Serv. Email: support@labrisnetworks.co 9

Reference Approval: 10

Request Mobil Number: 11

Use GSM Number for Username: 12

Send Password With SMS: 13

Common Key Enable/Disable: 14

CK Option: Automatic 15

CK Period: (mins) 16

Common Key: None 17

CK Username: None 18

CK Password: **** 19

CK Instructions: Tc No ile kayıt olabilmek için lütfen danışmadan ortak anahtarı temin ediniz. 20

CK Instructions (EN): For registering with Tc No, please get the common key from advisory. 21

Show Common Key

Save

1	Default Group	User signed up with this method will be a member of this group
2	Multiple Login	We can enable or disable option
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	We can set time to delete user account
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	Common Key Disable/Enable	We can enable or disable common key configuration
15	CK Option	We can automatic or manual common key
16	CK Period	Expiration time for common key
17	Common Key	Password Instructions is displayed in English
18	CK Username	Type common key username
19	CK Password	Type common key password
20	CK Instruction	Common key instructions displayed in Turkish
21	CK Instruction (EN)	Common key instructions displayed in English

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.

Settings - Default

Setting Rule: Default

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

Default Group: Default **1**

Multiple Login: ☐ **2**

Infinite Quota: ☐ **3**

Account Quota: 1440 (mins) **4**

Infinite Account: ☐ **5**

Timeout: 1440 (mins) **6**

Account Expiration Date: 24 (hours) **7**

Cust. Serv. Tel: 3122101490 **8**

Cust. Serv. Email: support@labrisnetworks.co **9**

Reference Approval: ☒ **10**

Request Mobil Number: ☒ **11**

Use GSM Number for Username: ☒ **12**

Send Password With SMS: ☒ **13**

Common Key Enable/Disable: ☐ **14**

CK Option: Automatic **15**

CK Period: (mins) **16**

Common Key: None **17**

CK Username: None **18**

CK Password: **** **19**

CK Instructions: Pasaport numarası ile kayıt olabilmek için lütfen danışmadan ortak anahtarı temin ediniz. **20**

CK Instructions (EN): For registering with Passport Number, please get the common key from advisory. **21**

[Show Common Key](#)

[Save](#)

1	Default Group	User signed up with this method will be a member of this group
2	Multiple Login	We can enable or disable option
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	We can set time to delete user account
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	Common Key Disable/Enable	We can enable or disable common key configuration
15	CK Option	We can automatic or manual common key
16	CK Period	Expiration time for common key
17	Common Key	Password Instructions is displayed in English
18	CK Username	Type common key username
19	CK Password	Type common key password
20	CK Instruction	Common key instructions displayed in Turkish
21	CK Instruction (EN)	Common key instructions displayed in English

Access Control List

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

Subnet RulesGeneralUIACL

IP Addresses:

1

Rule choice:

2

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

Select Members:

MembersAll Users

3

Filter

Remove Members

Add Members

« Prev Next »

Select Groups:

Member GroupsAll Groups

4

Filter

Remove Groups

Add Groups

« Prev Next »

Save

1	Ip Addresses	Comma separated list of ips
---	--------------	-----------------------------

65

Labris Networks

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 dash board and click on **Create User tab**

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.

Online Users						
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.

All Users									
Search Results									
User Name	Real Name	Account Expiration Date	Expired In	Creation Time	MAC Address	Multiple Login	Quota (min)	Notes	User Name
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.

Edit User

Username: Salih@slave 1

Real Name: Salih Ucpinar 2

Expiration Date: Date: 3000-01-29 Today 3
Time: 01:59:59 Now 3

MAC Address(Optional): 4

Allow Multiple Logins: ☒ 5

Quota: Unlimited 6

Infinite quota: ☒ 7

Notes: Guest User 8

Password: 9

Edit User

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

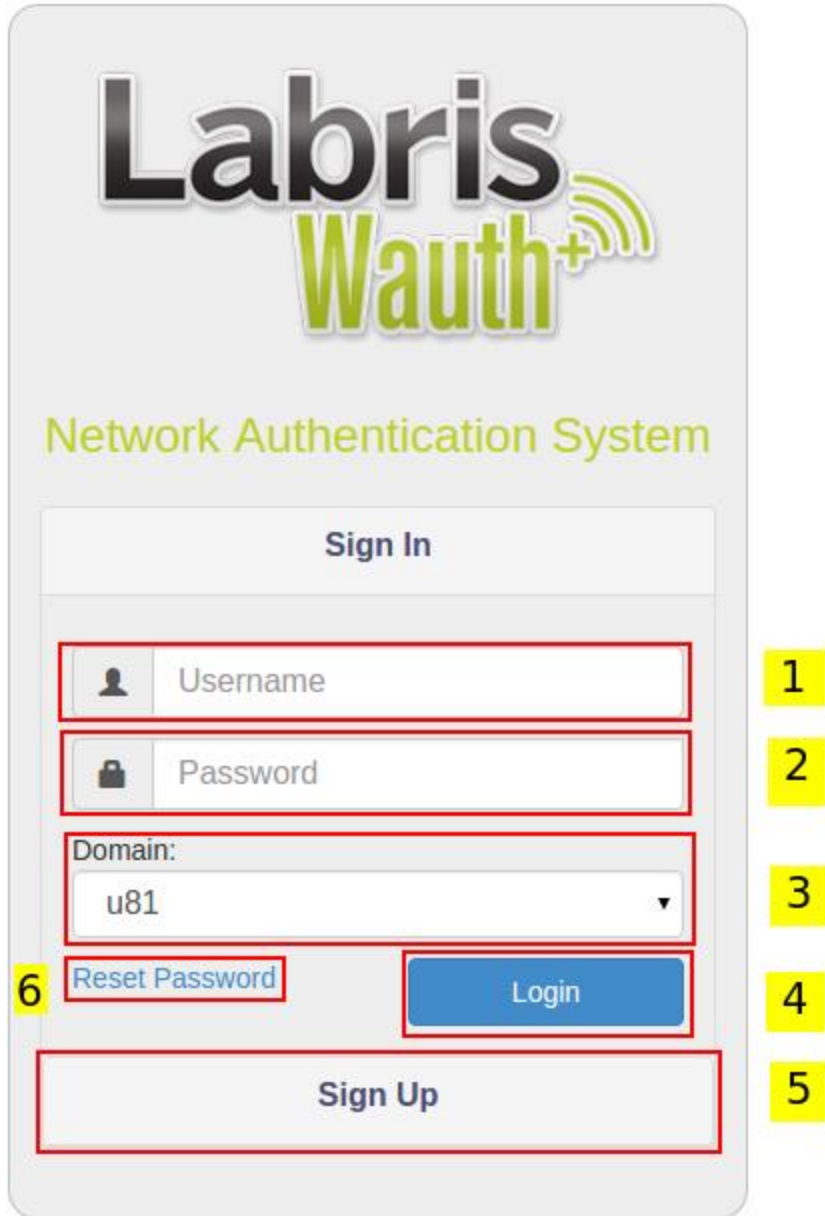
The guest or user is expected to authenticate him/her to the system with given credential information or credential information they get through SMS messages.

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.

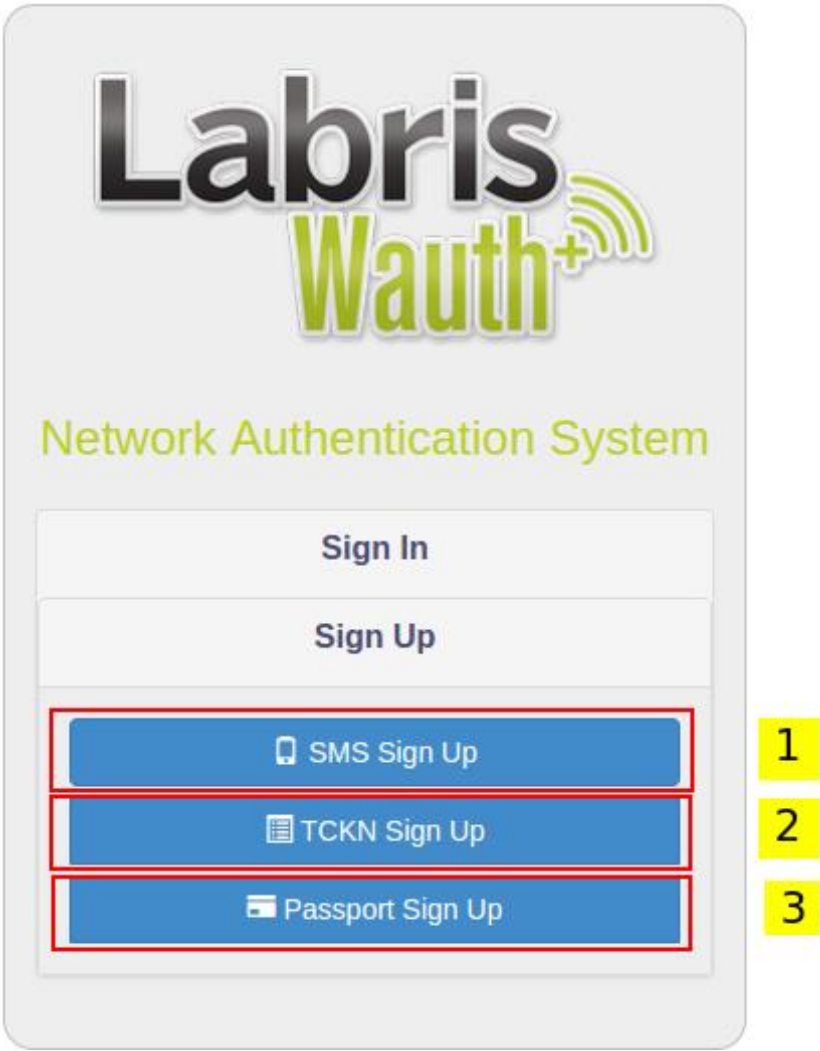
This welcome screen can be shown in different languages according to internet browser's language settings.

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	Obtain Password	SMS Authentication Button
6	Reset Password	Reset forgot password

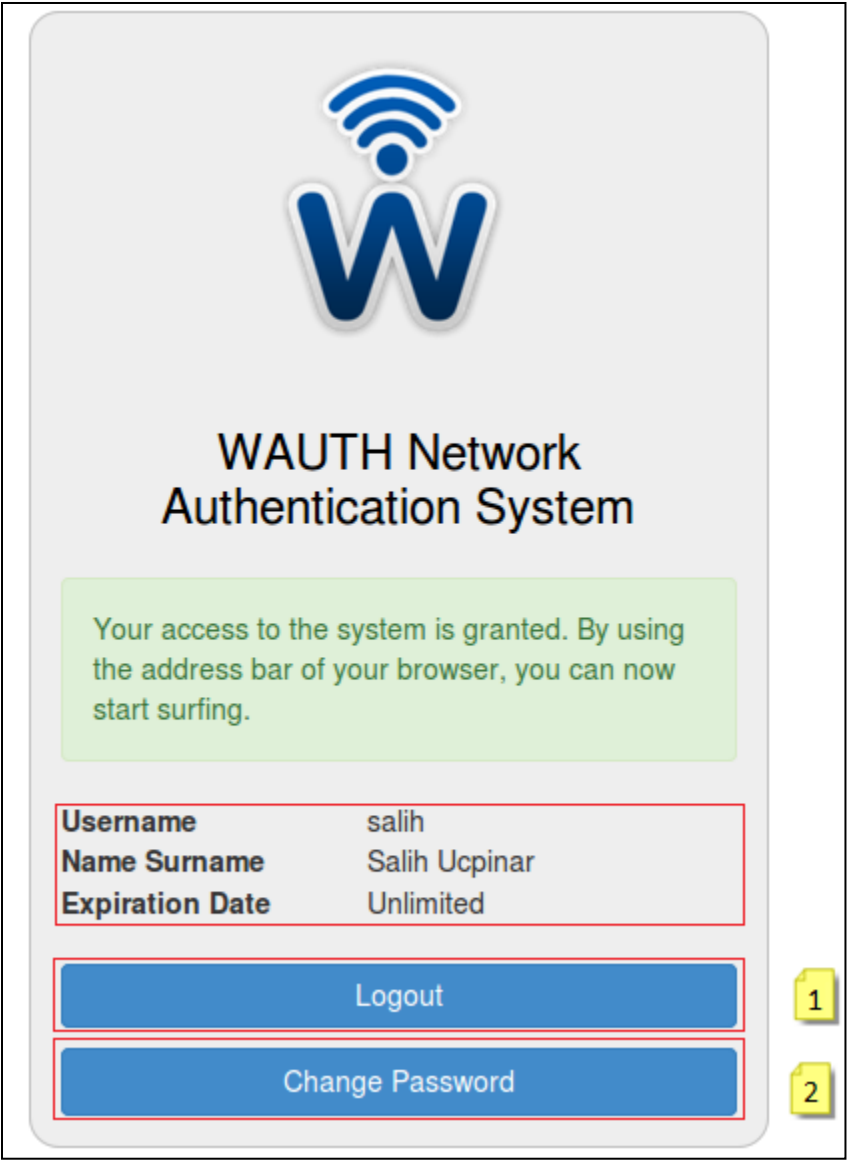
Alternative Sign Up Methods



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

Login

Post-entry Screen



1	Logout	Logout Button
2	Change Password	Change Password Button

Change User Password

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

Change Password

Current password

New password

Verify password

Confirmation

Back

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

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.

Labris

Wauth+

Network Authentication System

Name

1

Surname

2

Year of Birth

3

E-Mail

4

TC Identity Code

5

Back

Next

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

Reset Password - Set new password step

Labris
Wauth+

Network Authentication System

New Password

1

Confirm Password

2

Back

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.




SMS Sign Up

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 Wi-Fi guest internet access. This common key is enabled and set in SMSWauth screen. If CK is enabled, guest is wanted to enter it.




WAUTH Network Authentication System

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.

Answer the SMS, which will come to you, as 'Evet'.



Mobile Number



Common Key

Continue

Back

Customer Services
Phone: 0500000000
E-Mail: destek@labrisnetworks.com

For registering with SMS, please get the common key from advisory.

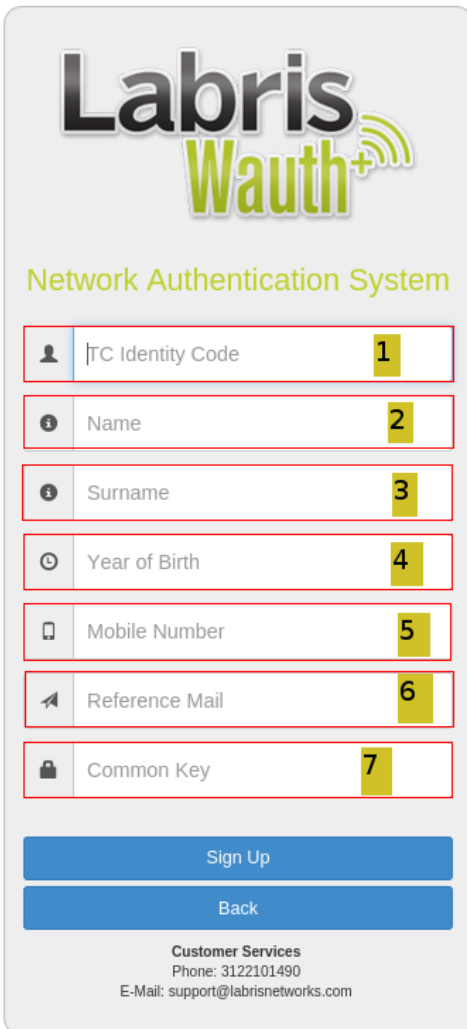
1

2

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

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.



The image shows a mobile application interface for 'Labris Wauth+' Network Authentication System. The form contains seven input fields, each with a red border and a yellow number in the top right corner indicating a sequence: 1. TC Identity Code (with a person icon), 2. Name (with an 'i' icon), 3. Surname (with an 'i' icon), 4. Year of Birth (with a clock icon), 5. Mobile Number (with a mobile phone icon), 6. Reference Mail (with an envelope icon), and 7. Common Key (with a lock icon). Below the fields are two blue buttons: 'Sign Up' and 'Back'. At the bottom, there is a 'Customer Services' section with the phone number 3122101490 and the email 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 field 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

Passport Sign Up

Users may sign up using their Passport Number.

Labris

Wauth+

Network Authentication System

Passport Number

1

Name

2

Surname

3

Year of Birth

4

Mobile Number

5

Reference Mail

6

Common Key

7

Sign Up

Back

Customer Services

Phone:

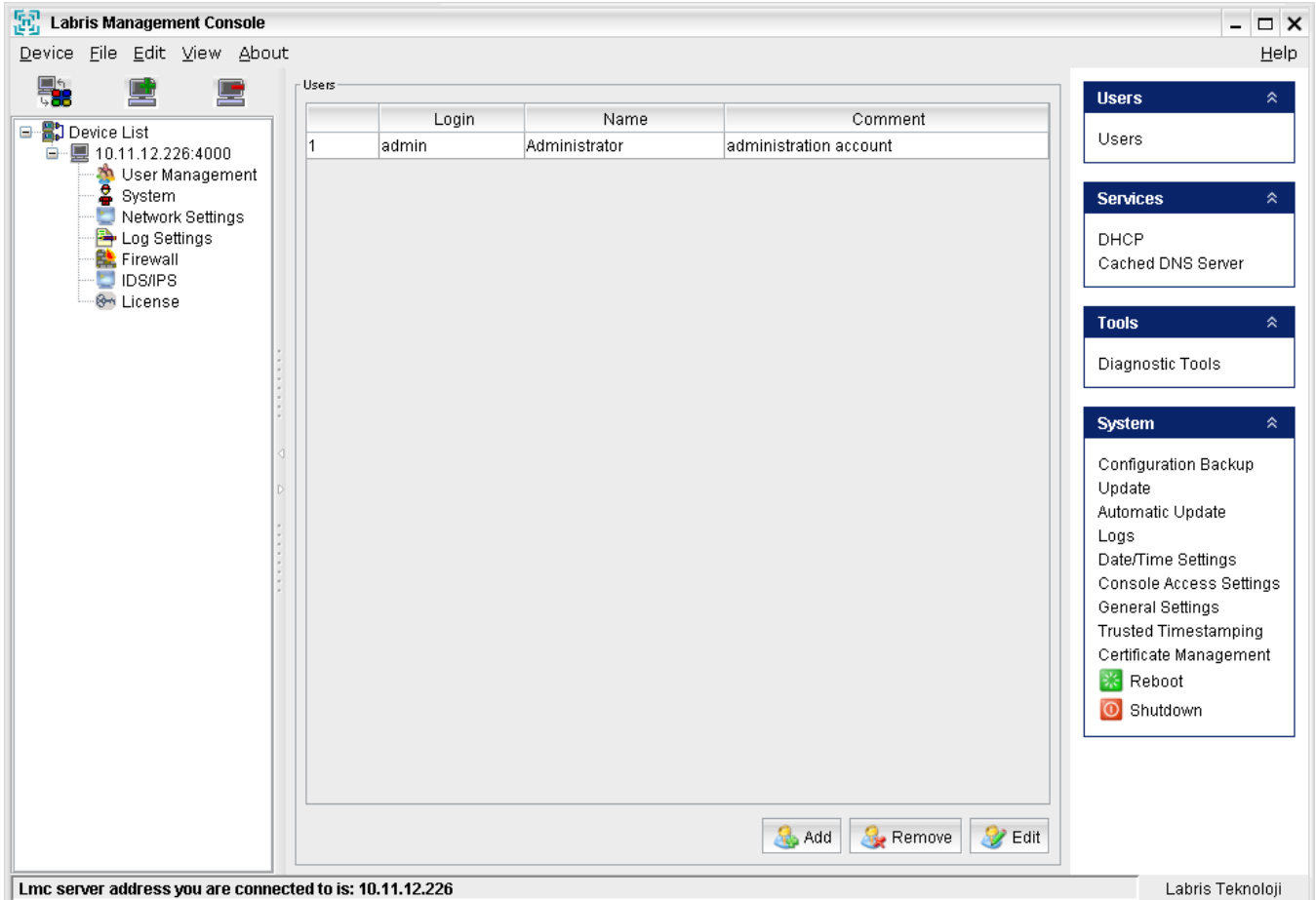
E-Mail:

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

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.

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.

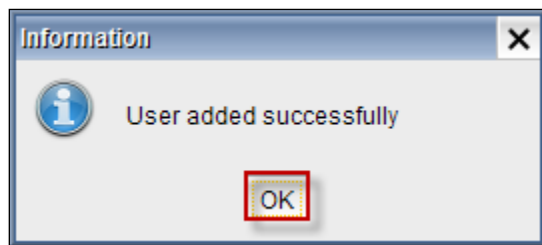
The 'Add User' dialog box contains the following fields and values:

Field	Value
Username	SystemUser1
Password
Re-type
Name	User1
Comment	TestUser

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

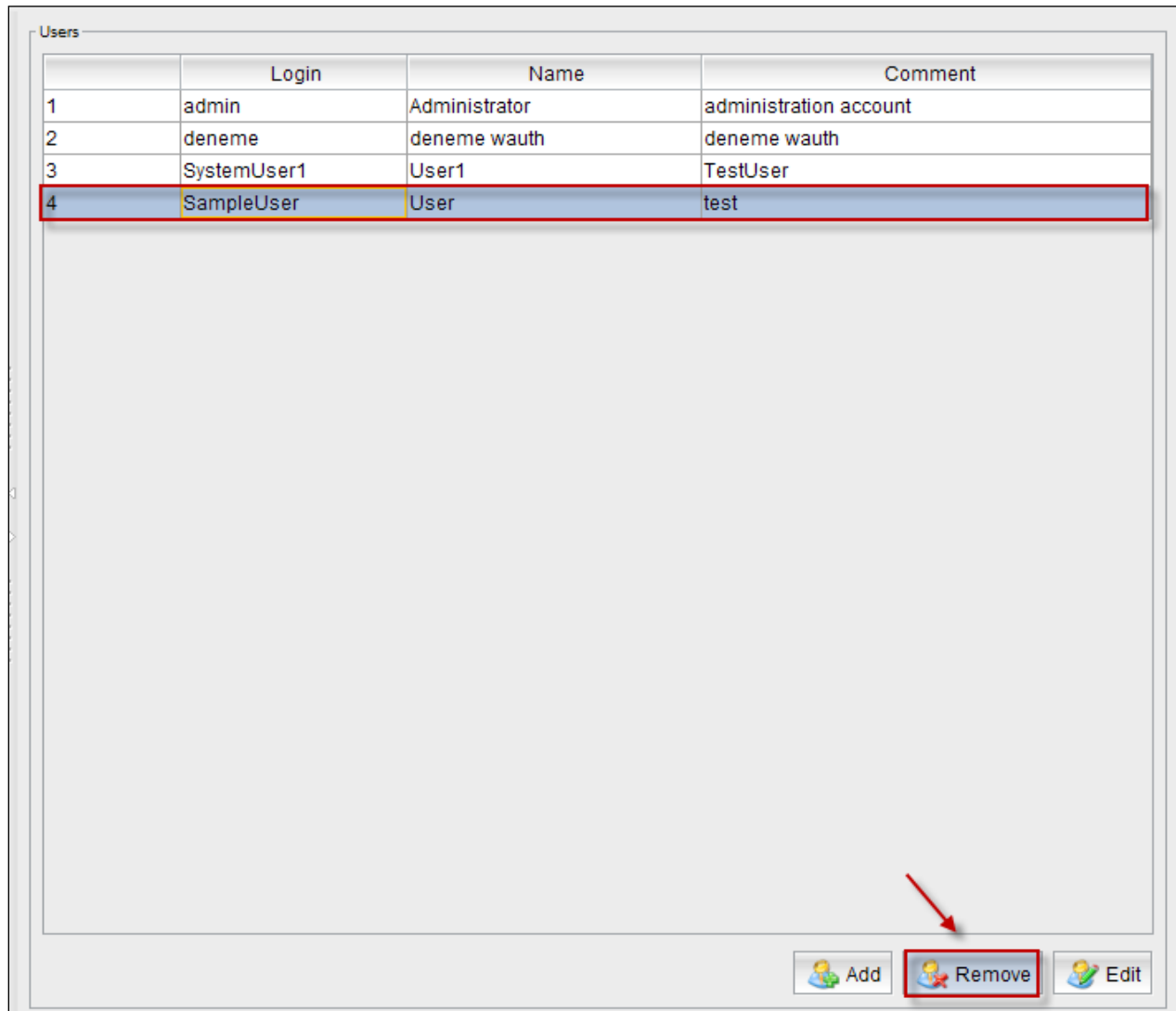


We can notice **new User** added in the **User's** list of **System Module**

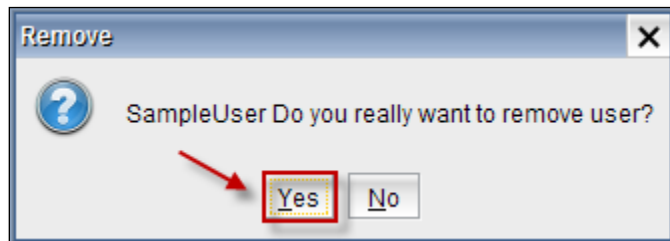
	Login	Name	Comment
1	admin	Administrator	administration account
2	deneme	deneme wauth	deneme wauth
3	SystemUser1	User1	TestUser

Deleting User

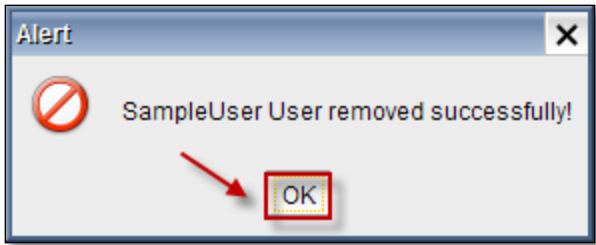
Select User and click on **Remove Tab** to delete a User.



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

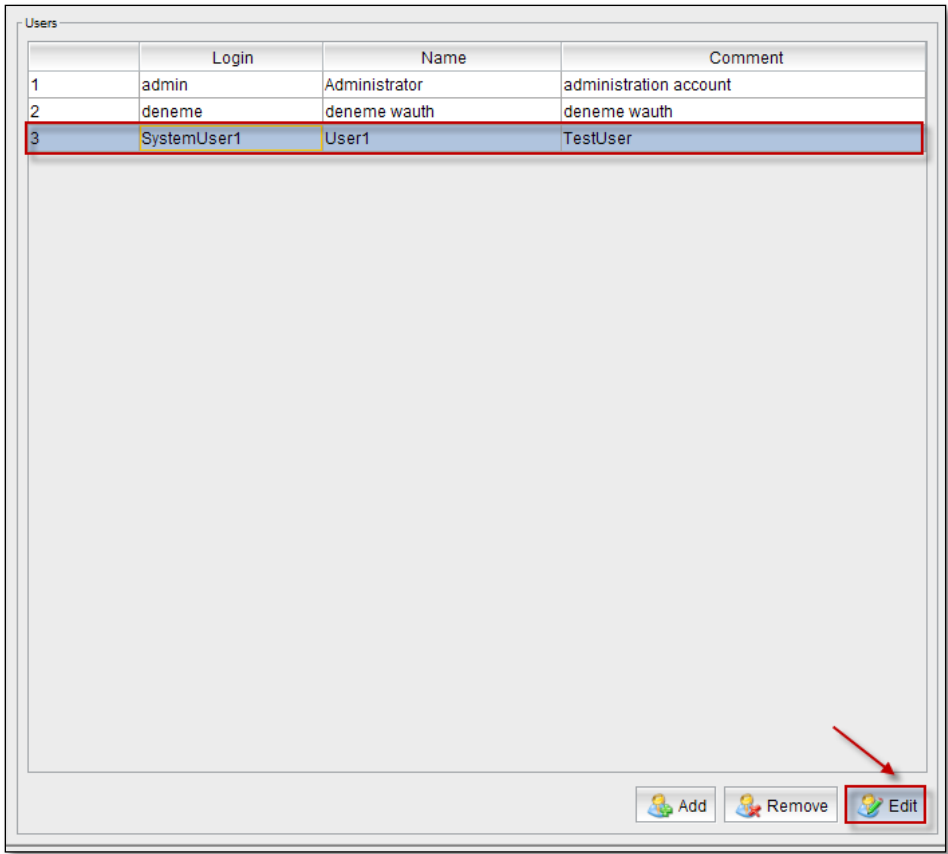


Alert screen appears displaying User removed successfully; click **Ok** to close the current tab.



Change Password / Editing User

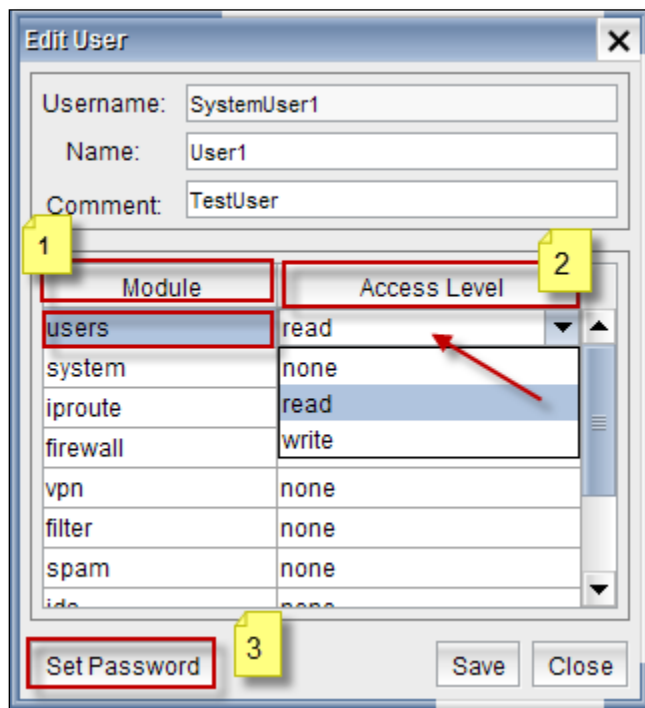
Select the user from the list and click on **Edit**



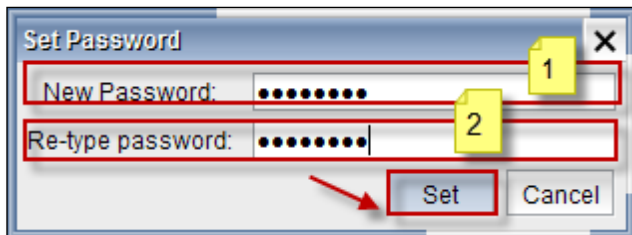
Viewing options in Edit User

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.

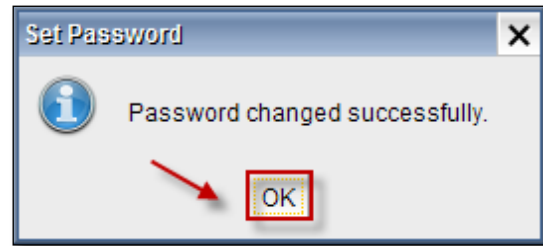


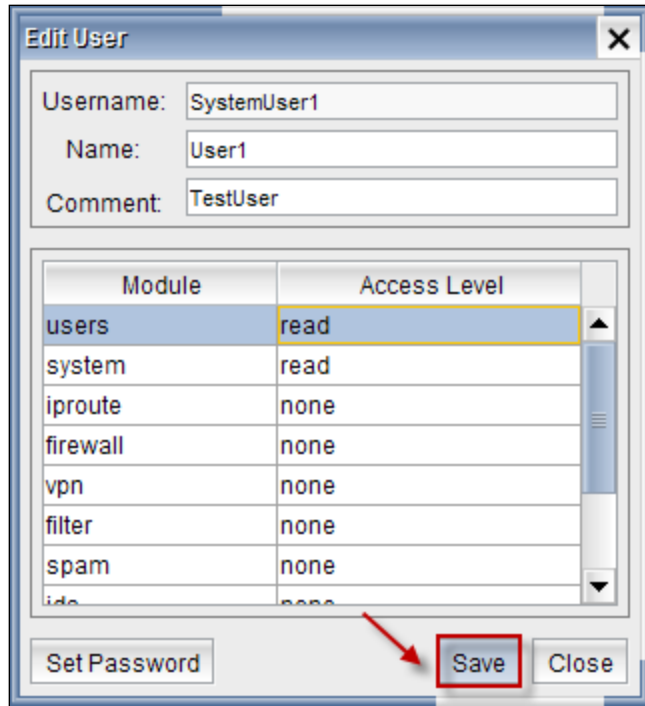
1	New Password	Type password of the User
2	Re-type Password	Re-type Password of the User for confirmation

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.





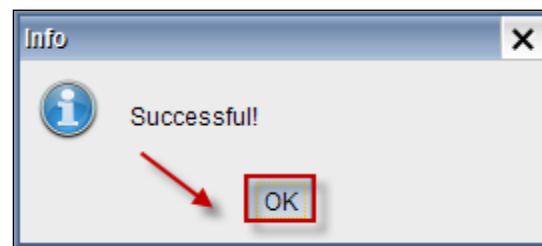
The 'Edit User' dialog box contains the following fields and table:

Username: SystemUser1
Name: User1
Comment: TestUser

Module	Access Level
users	read
system	read
iproute	none
firewall	none
vpn	none
filter	none
spam	none
ids	none

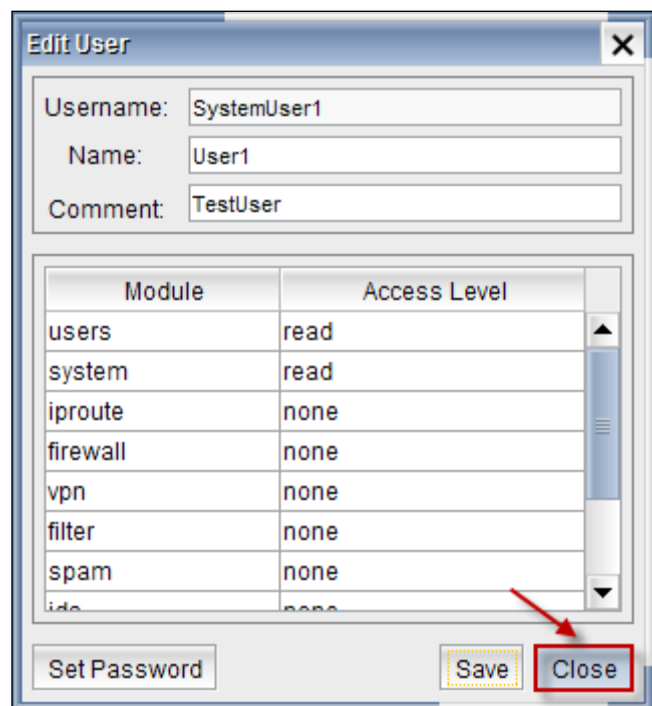
Buttons: Set Password, Save, Close. A red arrow points to the 'Save' button.

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



The 'Info' dialog box displays a message icon and the text 'Successful!'. A red arrow points to the 'OK' button.

Click on **Close Tab**



The 'Edit User' dialog box contains the following fields and table:

Username: SystemUser1
Name: User1
Comment: TestUser

Module	Access Level
users	read
system	read
iproute	none
firewall	none
vpn	none
filter	none
spam	none
ids	none

Buttons: Set Password, Save, Close. A red arrow points to the 'Close' button.

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

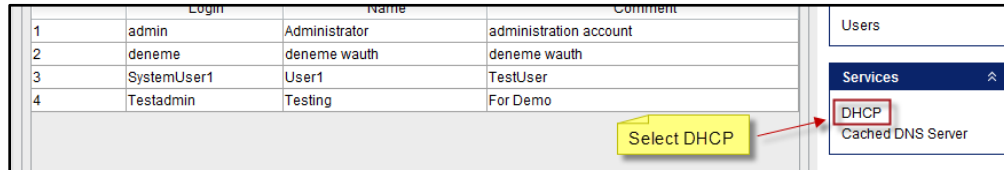
DHCP is a server which assigns IPs automatically to the clients requested from a range of IPs.

IP leasing process:

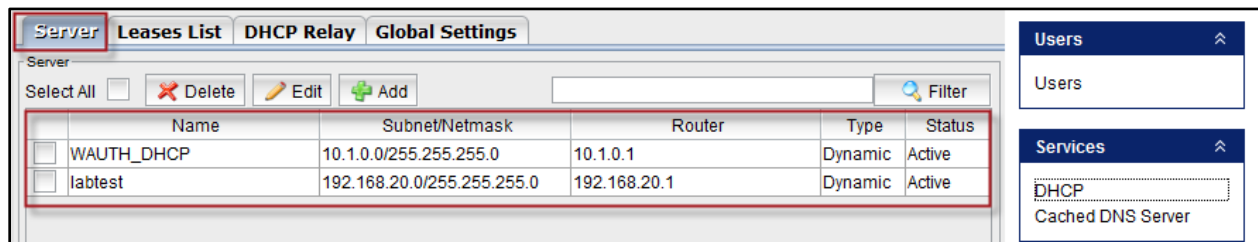
1. **DHCP discover:** The client machine when turned on, broadcasts the network id, broadcast id and MAC address on Network for discovering **DHCP** server.
2. **Offer:** The **DHCP** server listening to the request made by the client offers a pool of IP addresses to the client machine.
3. **Selection:**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

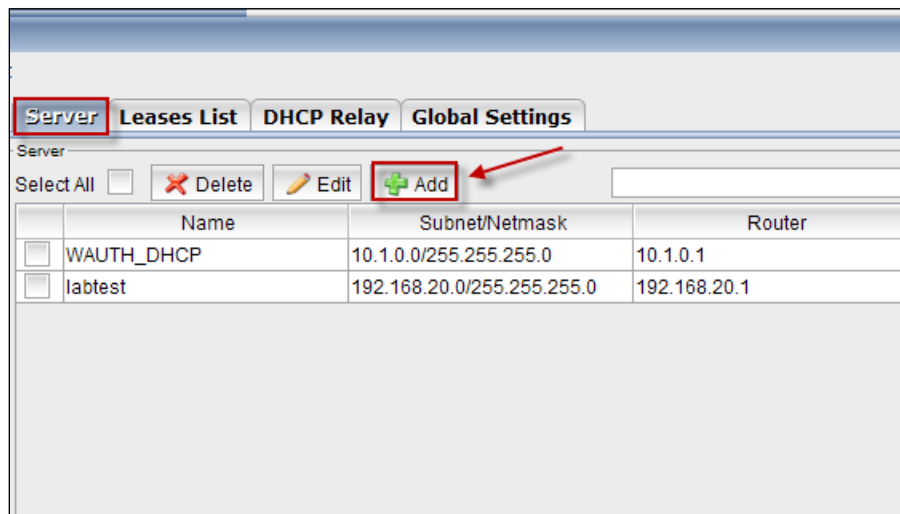
Select **DHCP** option under services.



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

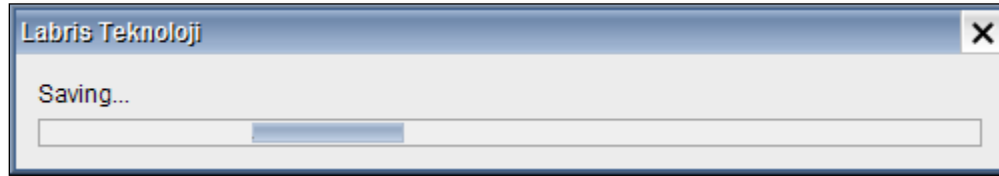
Click on **Add Tab** to add an IP Range

The screenshot shows the 'Add Dhcp Scope' dialog box. The 'Settings' tab is selected. The 'Active' checkbox is checked. The 'Type' is set to 'Dynamic'. The 'Scope Name' is 'TestScope'. The 'Interface' is 'tun0 - 10.8.3.1'. The 'IP Address' checkbox 'Use interface's IP address as subnet' is checked. The 'Netmask' is '/24 (255.255.255.0)'. The 'IP Range' is '10.8.3.10 - 10.8.3.80'. The 'Add' button is highlighted. The 'Router' checkbox 'Use interface's IP address as router' is checked.

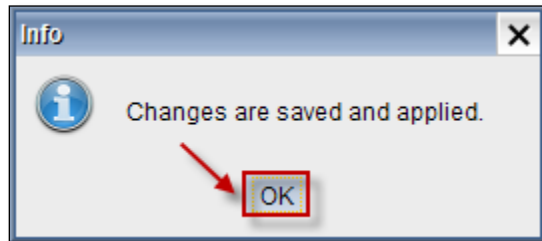
Continuation to the above screen, choose **Lease Time & Maximum Lease Time** from the scope and type **Domain Name**, Click on **Save Tab**.

The screenshot shows the DHCP configuration screen. The 'Lease Time' is set to 1440 minutes. The 'Maximum Lease Time' is set to 2880 minutes. The 'Domain Name' is 'loak.com'. The 'DNS' checkbox 'Use router's IP address as DNS' is checked. The 'Primary DNS' and 'Secondary DNS' fields are empty. The 'Save' button is highlighted with a red arrow.

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"/> Delete Edit Add <input type="text"/> 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**.

Server Leases List DHCP Relay Global Settings

Select All ☐

	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 *

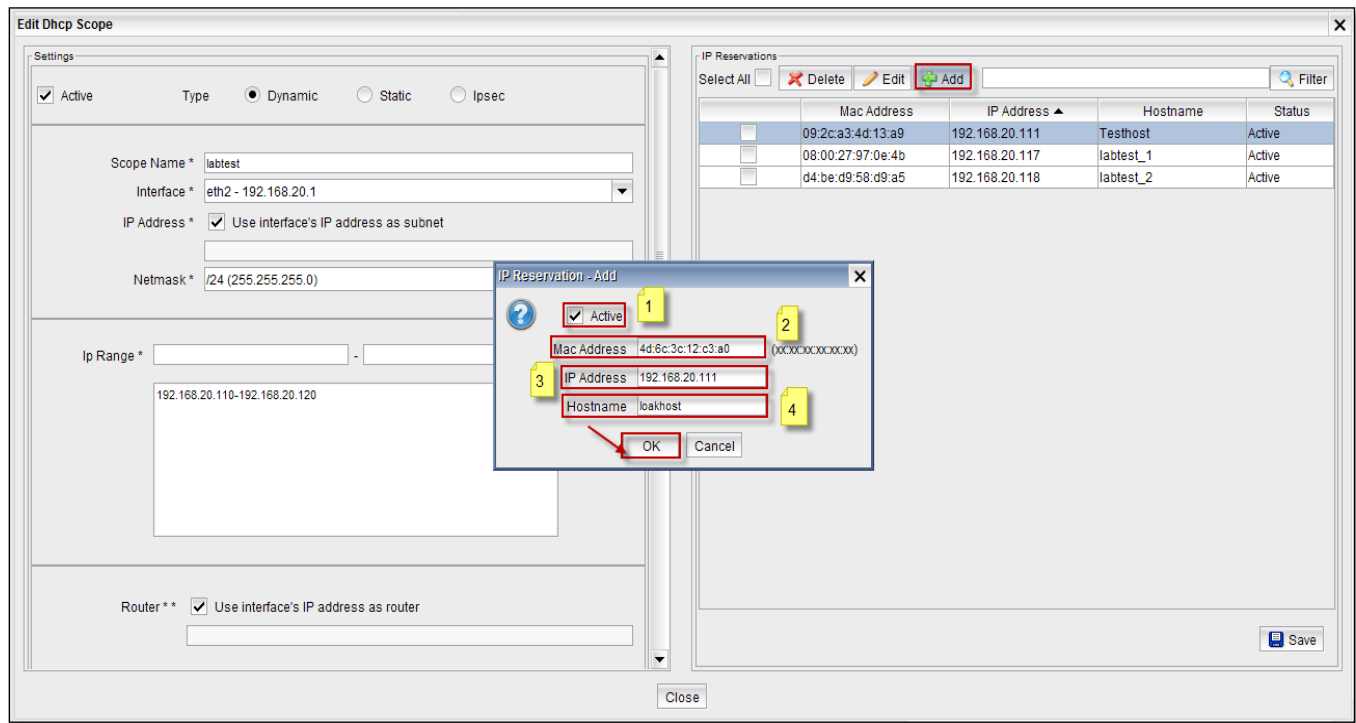
IP Address * ☒ Use interface's IP address as subnet

Netmask *

Ip Range * -

Router ** ☒ Use interface's IP address as router

Adding IP Reservation to DHCP scope

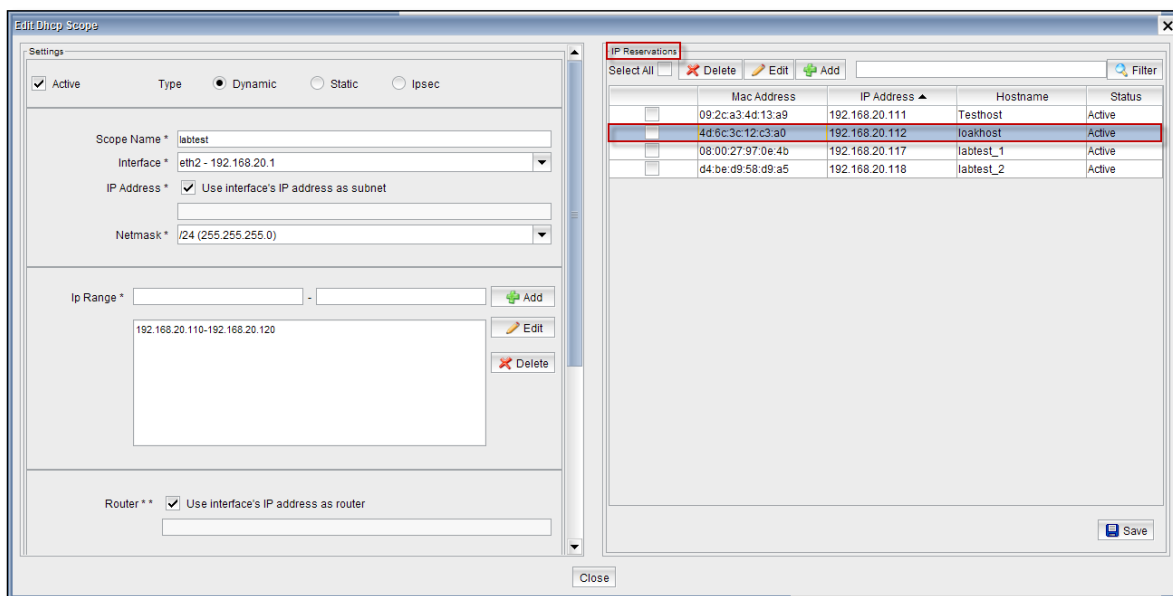


These are the inputs for adding IP Reservation

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**

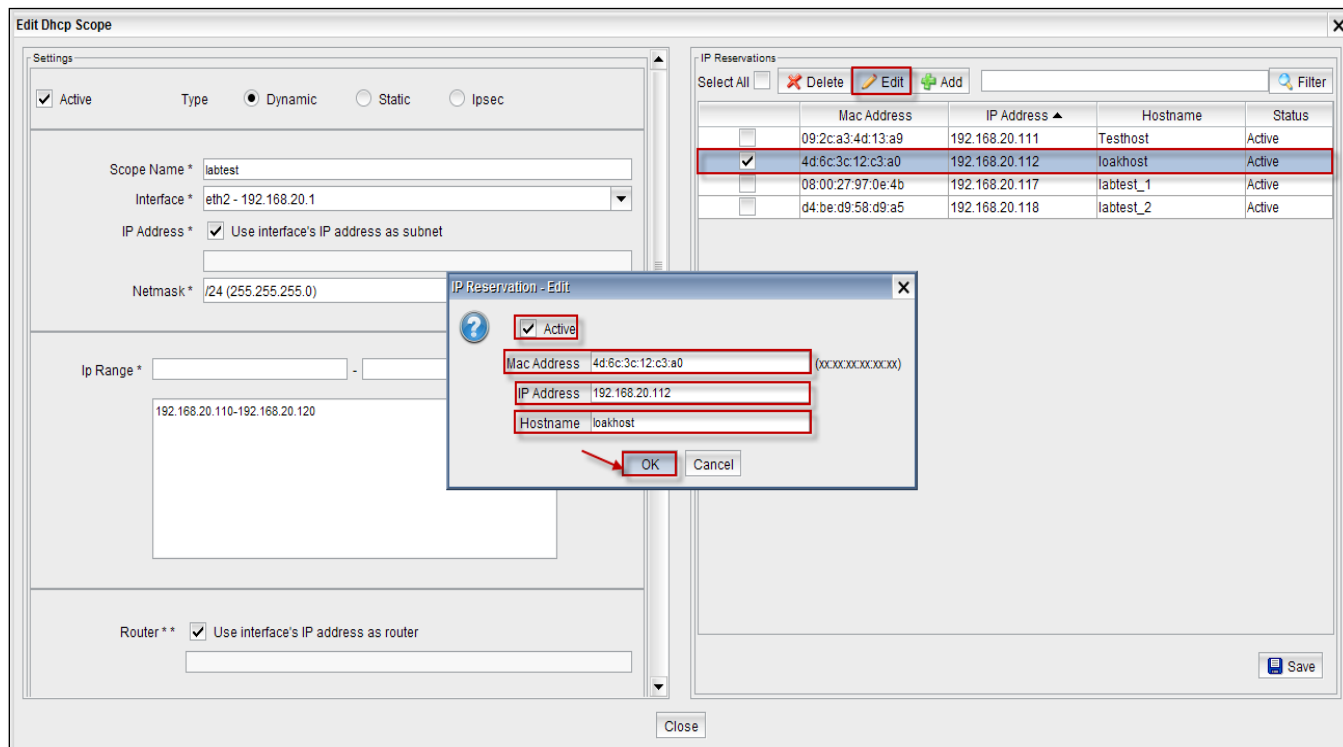
In the below screen we can notice **IP Reservation** added to the DHCP Server



Editing IP Reservation

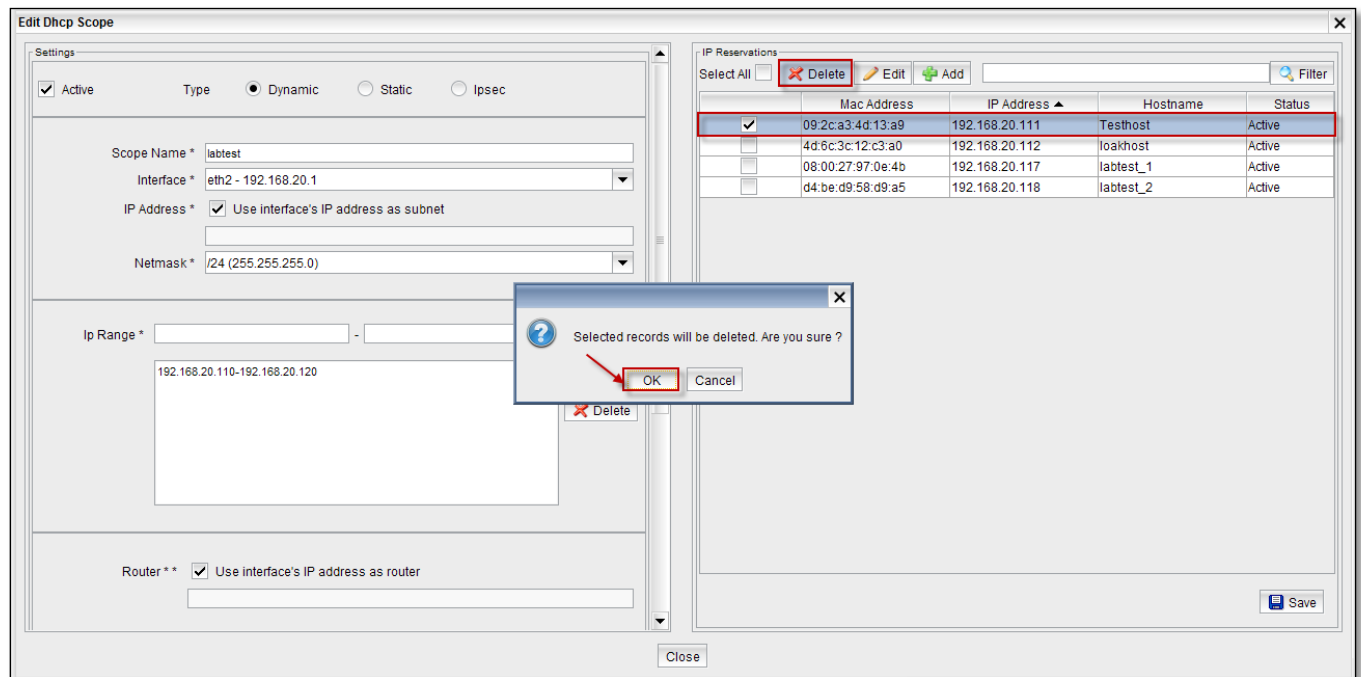
Select IP and click on **Edit** tab

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

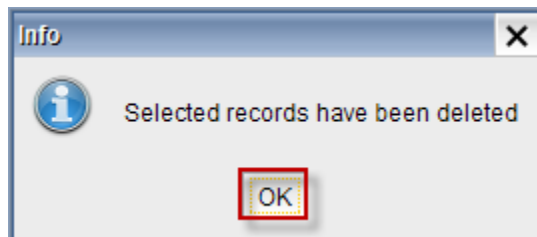


Deleting IP Reservation

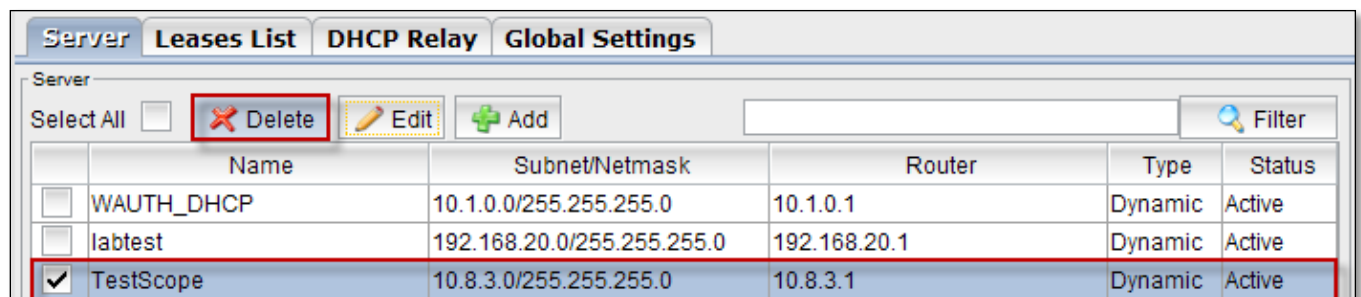
Select the IP and click on **Delete tab**, Click **Ok** to delete.



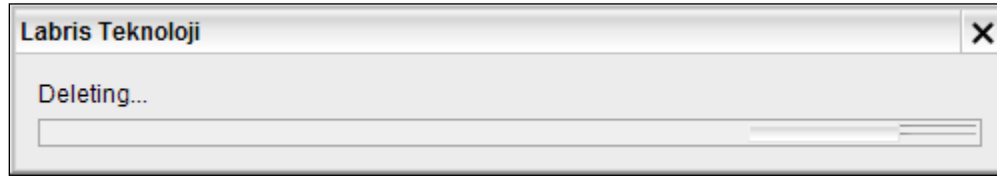
Below screen appears stating that selected records have been deleted. Click **Ok** to close the current tab.



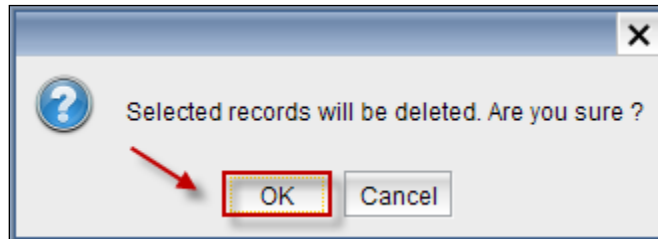
Select the **Server** from the list and click on **Delete Tab** to delete the **DHCP Server**.



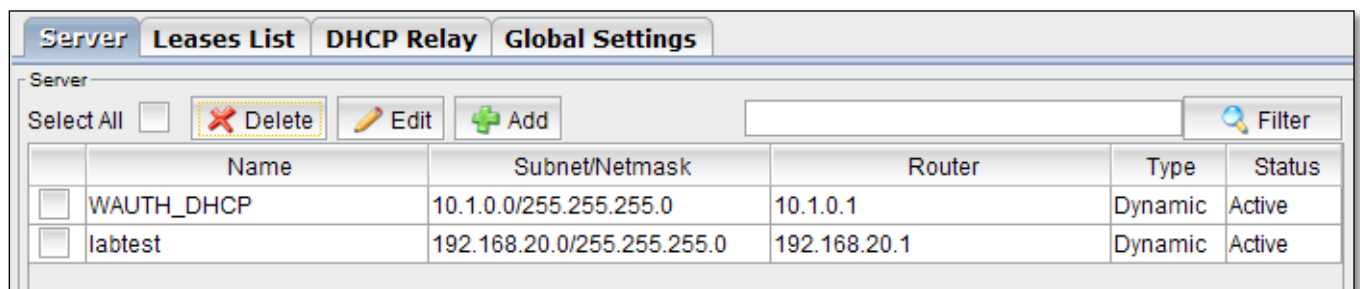
Deleting process is in progress.



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

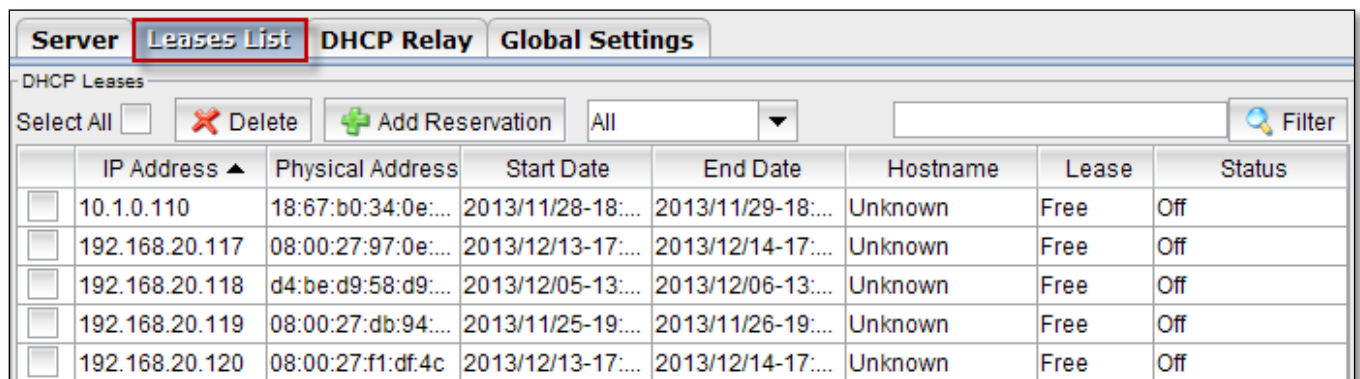


We can notice that the selected **Server** is **deleted** from the Servers list.

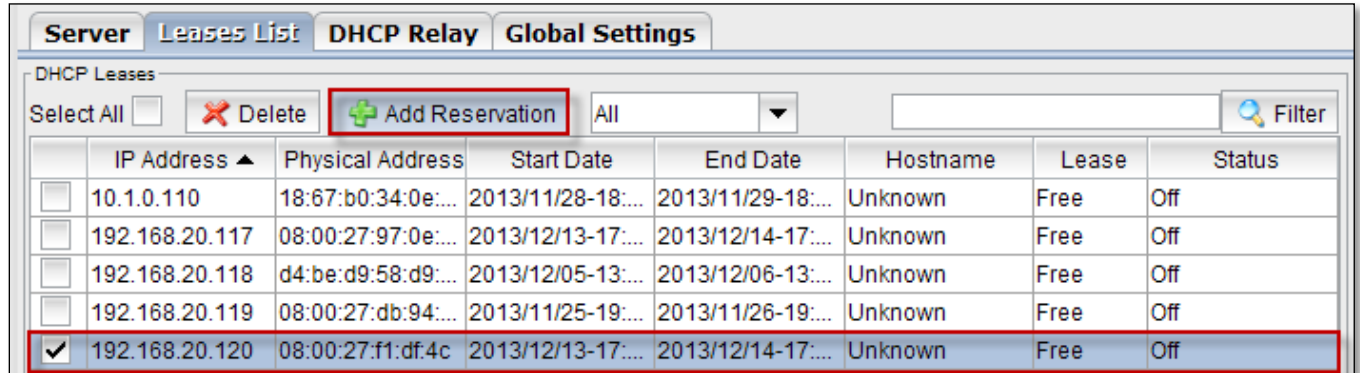


Lease list options

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



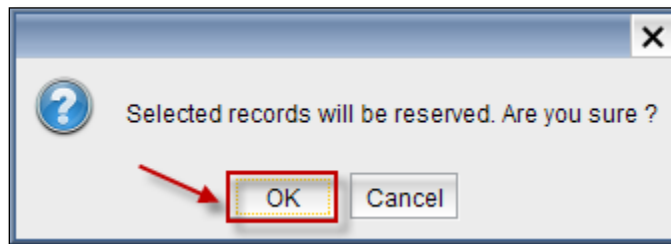
Choose **IP Address** and click on **Add Reservation Tab**.



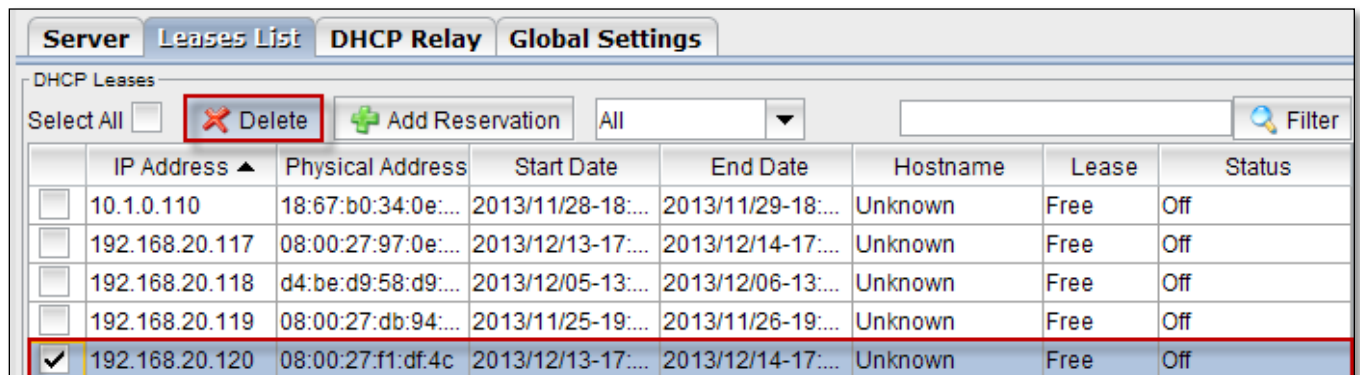
The screenshot shows the 'DHCP Leases' window with tabs for 'Server', 'Leases List', 'DHCP Relay', and 'Global Settings'. The 'Leases List' tab is active. At the top, there are buttons for 'Select All', 'Delete', and 'Add Reservation' (highlighted with a red box). A dropdown menu is set to 'All'. Below the buttons is a table with columns: IP Address, Physical Address, Start Date, End Date, Hostname, Lease, and Status. The table contains five rows of lease data. The last row, with IP address 192.168.20.120, is selected and highlighted with a red border.

	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**.



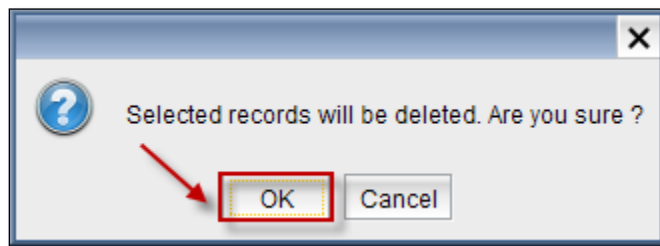
Select the **IP Address** and click on **delete** tab to delete the selected lease list.



The screenshot shows the 'DHCP Leases' window with the 'Delete' button highlighted with a red box. The table below is identical to the one in the previous screenshot, with the last row (IP 192.168.20.120) selected.

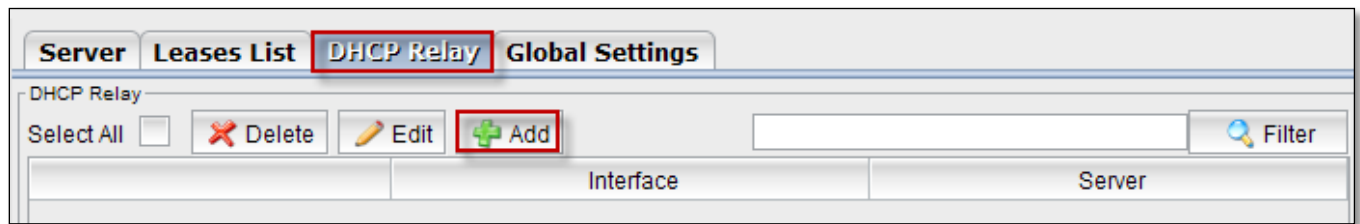
	IP Address ▲	Physical Address	Start Date	End Date	Hostname	Lease	Status
<input type="checkbox"/>	10.1.0.110	18:67:b0:34:0e:...	2013/11/28-18:...	2013/11/29-18:...	Unknown	Free	Off
<input type="checkbox"/>	192.168.20.117	08:00:27:97:0e:...	2013/12/13-17:...	2013/12/14-17:...	Unknown	Free	Off
<input type="checkbox"/>	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

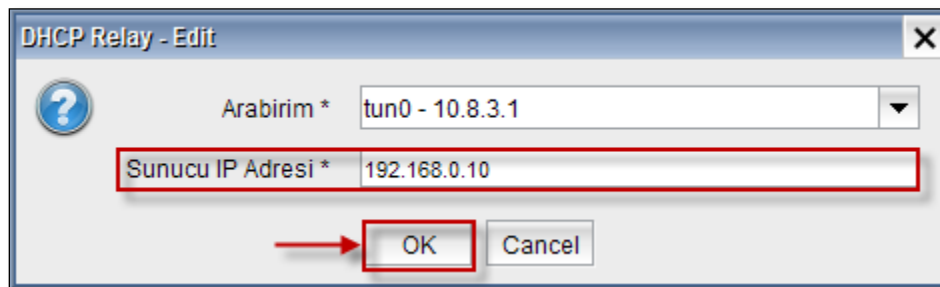


DHCP Relay options

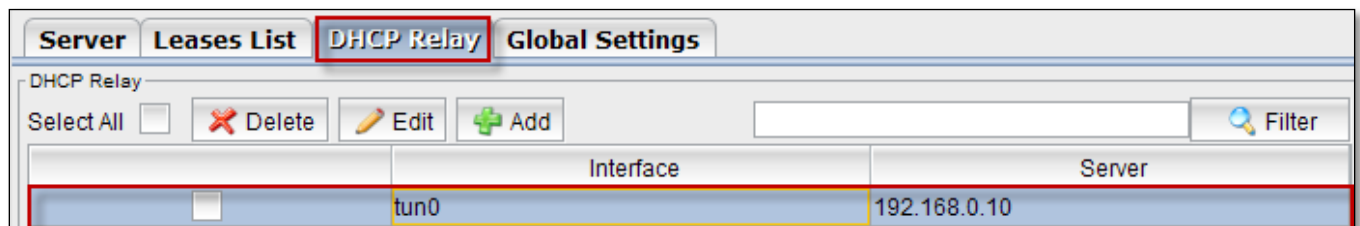
Select **DHCP Relay** and click on **Add Tab**.



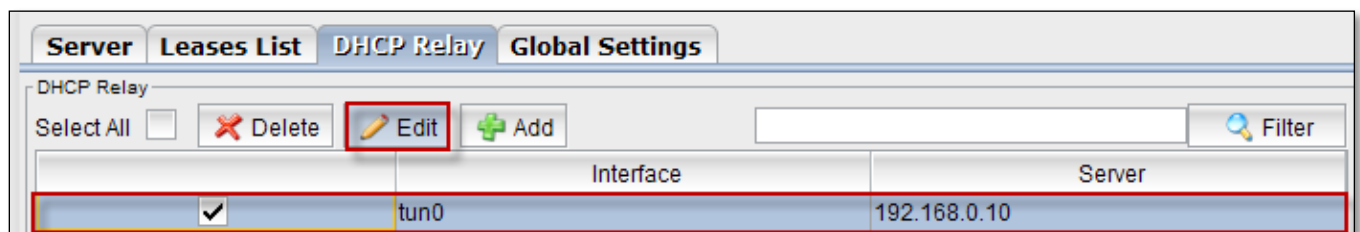
Give the server IP Address and click **OK**.



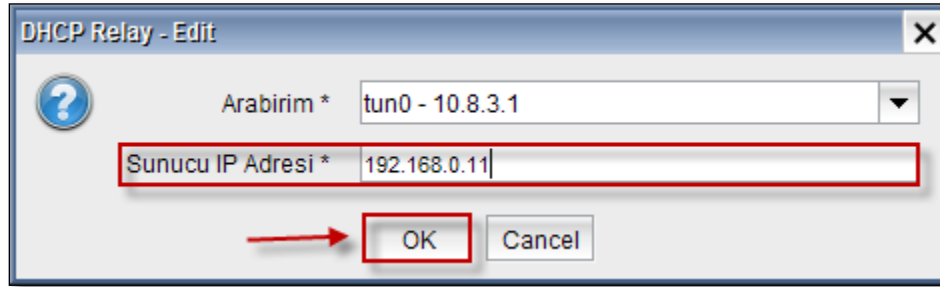
We can notice that **Server** is added in the **DHCP Relay**.



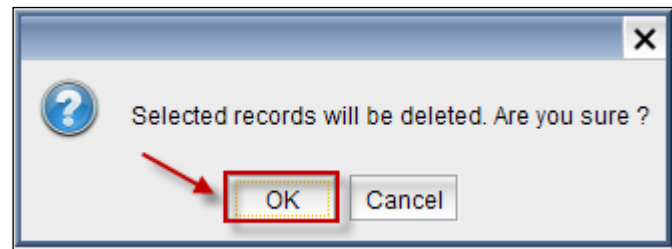
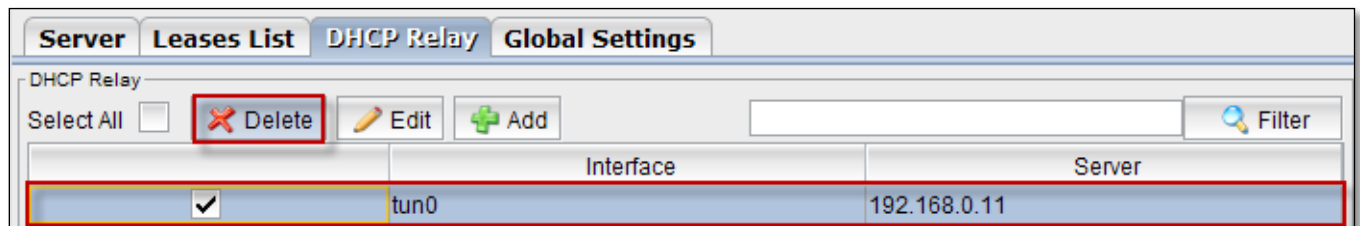
Select the **Server** and click on **Edit Tab**.



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

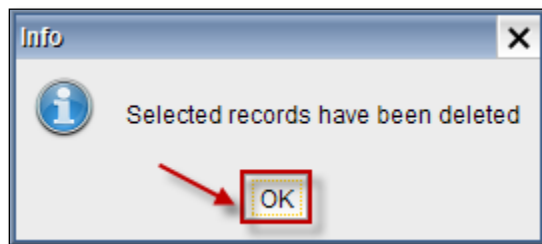


Select the **Server** and click on **Delete Tab** to delete server from the DHCP Relay.



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

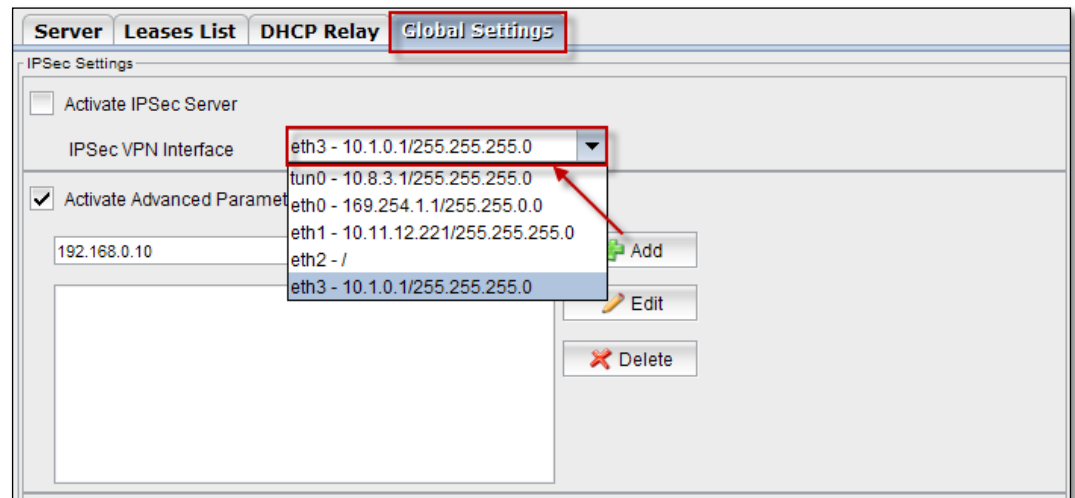
Below screen appears stating that Selected **Records** have been deleted, click **Ok** to close the current tab.



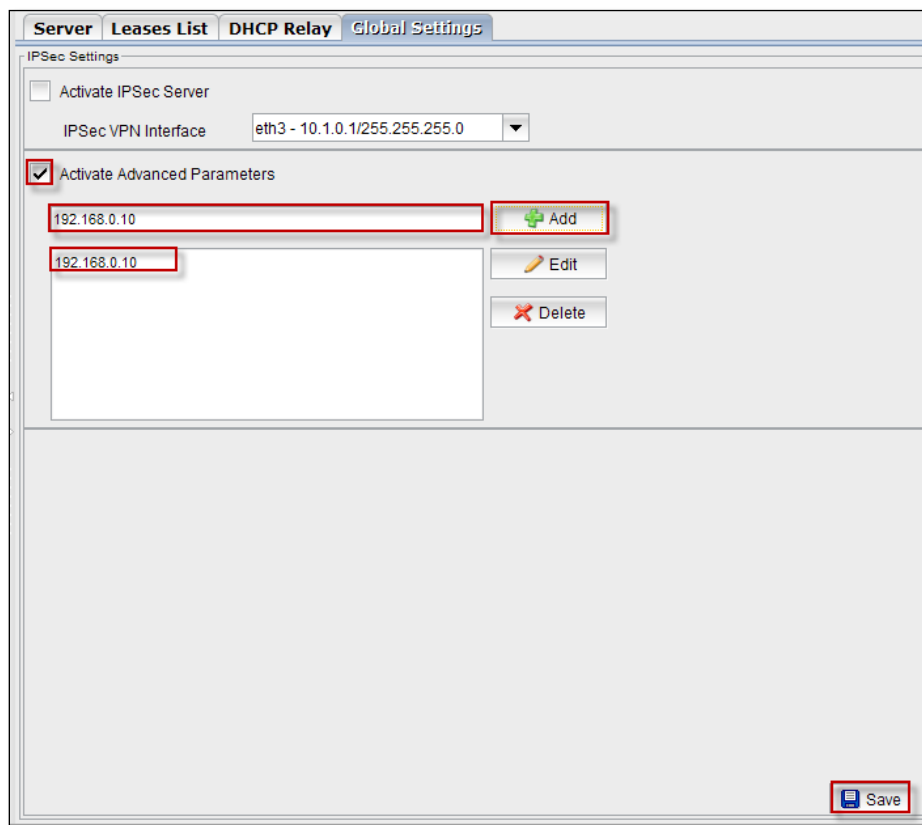
Global Settings options

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

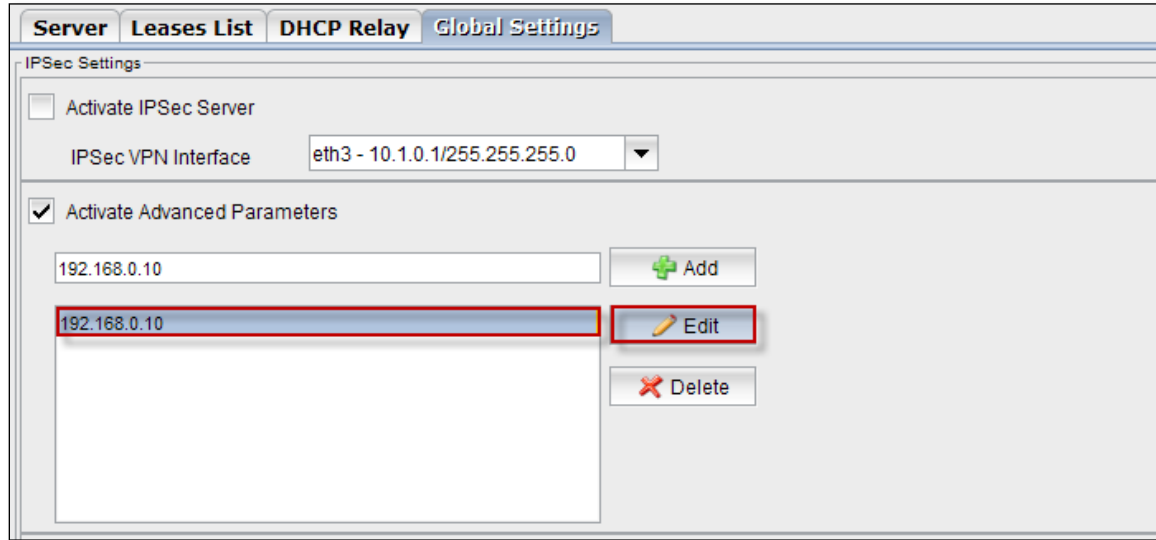
From the **IPSec VPN Interface** drop down list select the Ethernet adapter.



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

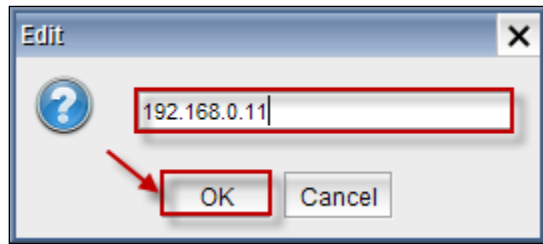


Select the **IP Address** and click on **Edit tab** to edit **IP Address**.



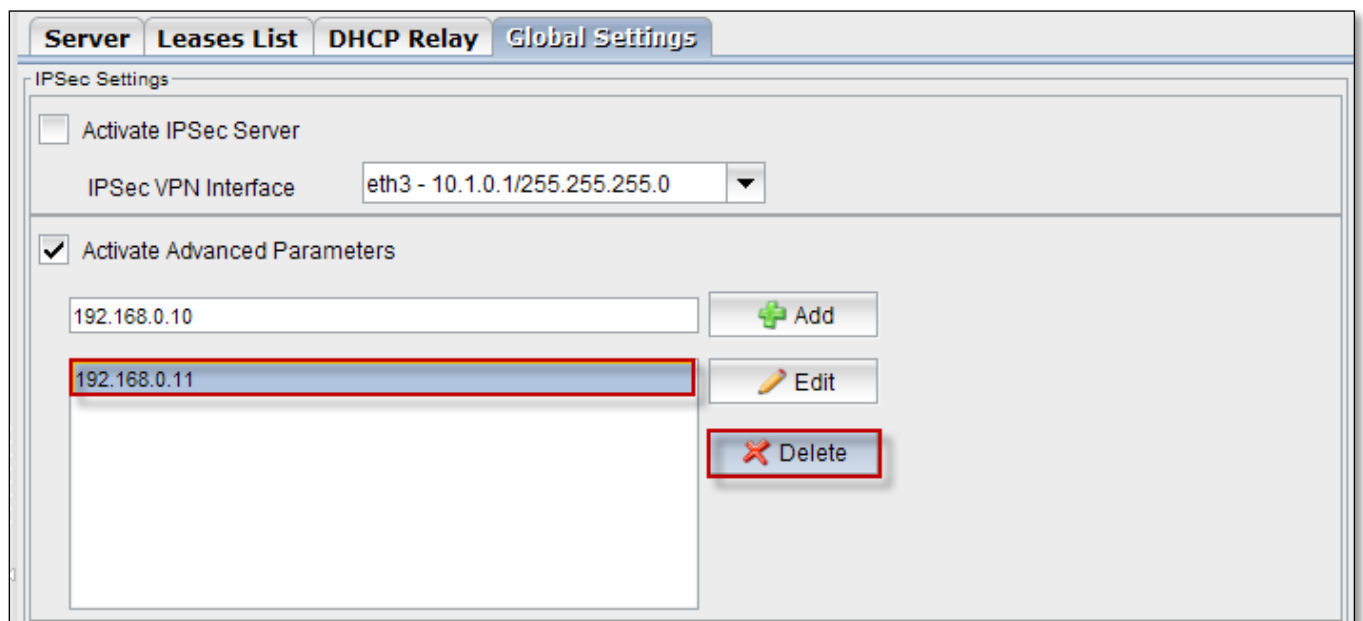
The screenshot shows the 'Global Settings' tab of the 'IPsec Settings' window. The 'Activate IPsec Server' checkbox is unchecked. The 'IPsec VPN Interface' dropdown is set to 'eth3 - 10.1.0.1/255.255.255.0'. The 'Activate Advanced Parameters' checkbox is checked. Below this, there is a list of IP addresses. The first entry is '192.168.0.10'. The second entry, '192.168.0.10', is selected and highlighted with a blue background. To the right of the list, there are three buttons: 'Add' (green plus icon), 'Edit' (pencil icon), and 'Delete' (red X icon). The 'Edit' button is highlighted with a red border.

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



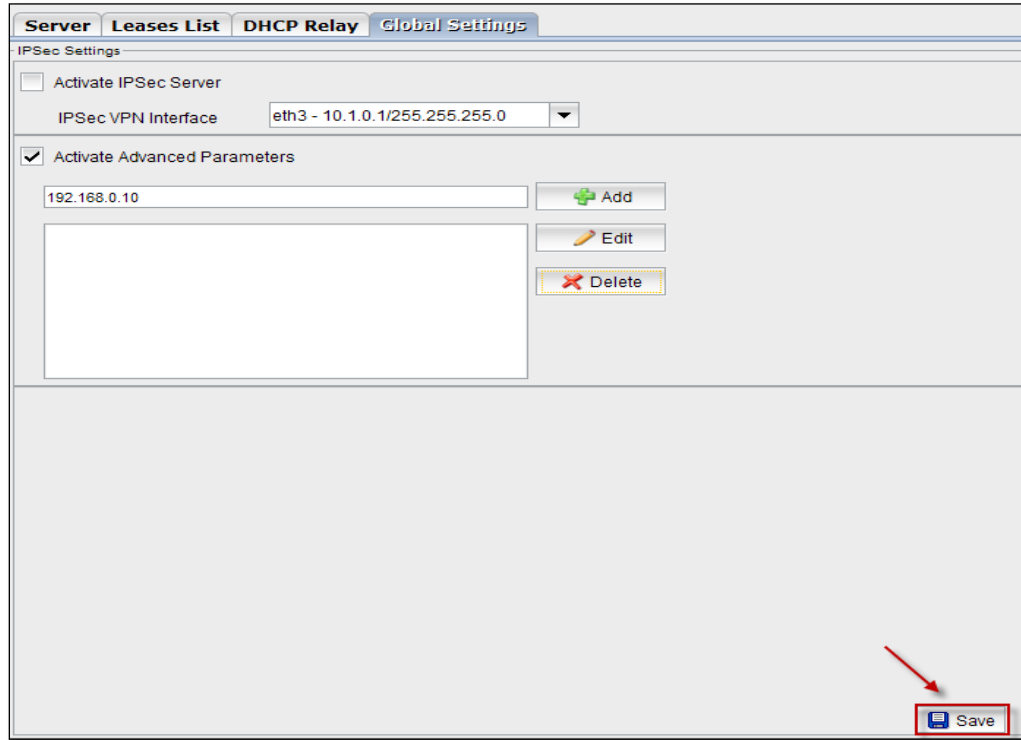
The screenshot shows an 'Edit' dialog box. It has a title bar with 'Edit' and a close button (X). Inside, there is a question mark icon on the left. A text input field contains the IP address '192.168.0.11'. Below the input field, there are two buttons: 'OK' and 'Cancel'. The 'OK' button is highlighted with a red border and a red arrow points to it from the left.

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

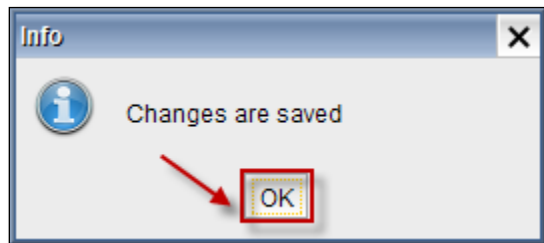


The screenshot shows the 'Global Settings' tab of the 'IPsec Settings' window. The 'Activate IPsec Server' checkbox is unchecked. The 'IPsec VPN Interface' dropdown is set to 'eth3 - 10.1.0.1/255.255.255.0'. The 'Activate Advanced Parameters' checkbox is checked. Below this, there is a list of IP addresses. The first entry is '192.168.0.10'. The second entry, '192.168.0.11', is selected and highlighted with a blue background. To the right of the list, there are three buttons: 'Add' (green plus icon), 'Edit' (pencil icon), and 'Delete' (red X icon). The 'Delete' button is highlighted with a red border.

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.

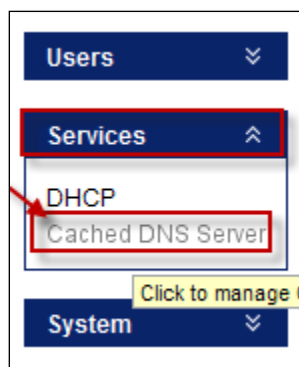


DNS

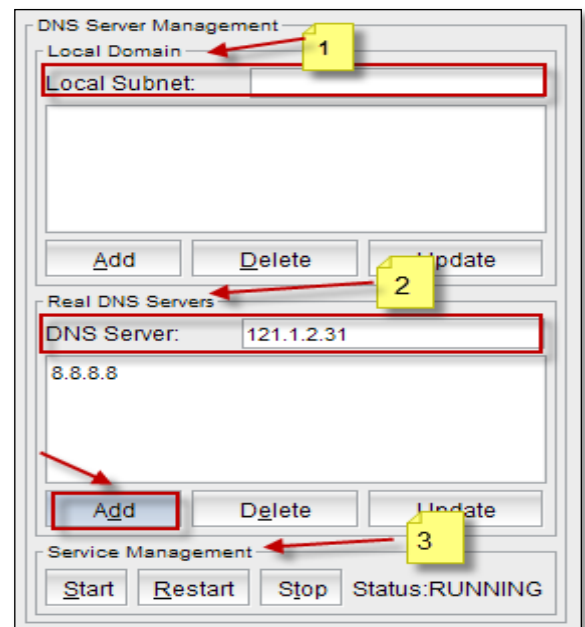
Domain Name System (DNS) is the name resolution protocol for TCP/IP networks, such as the Internet. DNS translates Internet domain and host names to IP addresses. DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites.

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**.



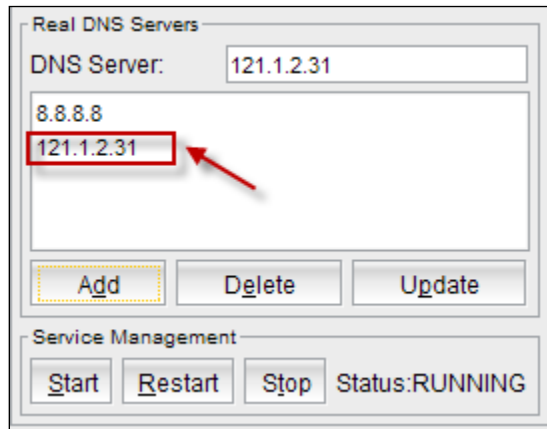
In the **DNS Server Management** tab we find different options like Local Subnet, Real DNS Servers. In the Real DNS Servers give the **IP Address** of the **DNS server** and click on **Add**.



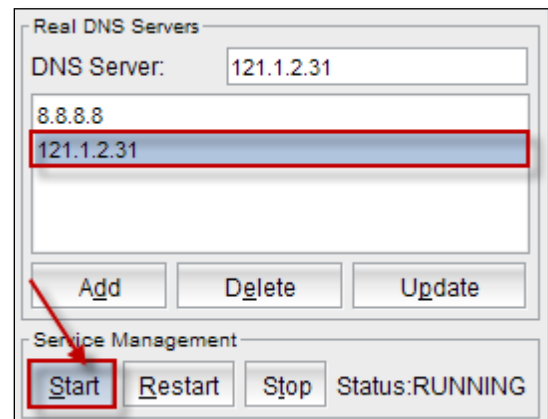
Viewing fields in DNS

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

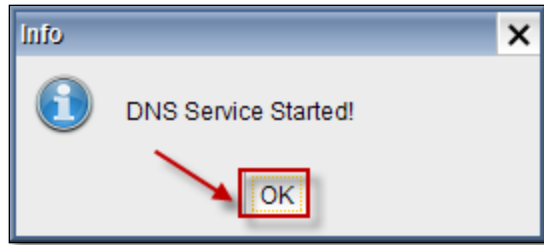
In the below screen we can notice **DNS Server** is added.



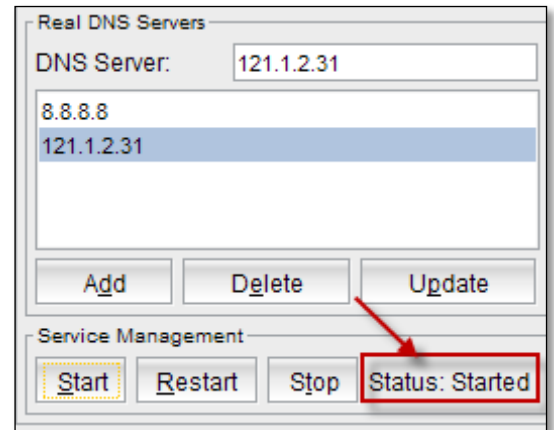
Select the server and click on **Start tab** to start the services of **DNS Server**.



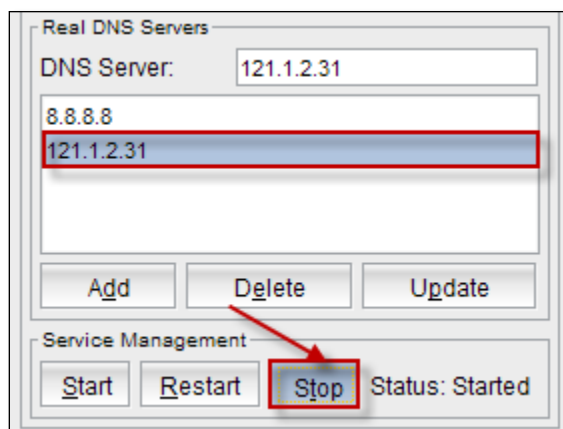
Below screen appears stating that **DNS Service Started**, click **Ok** to close the current tab.



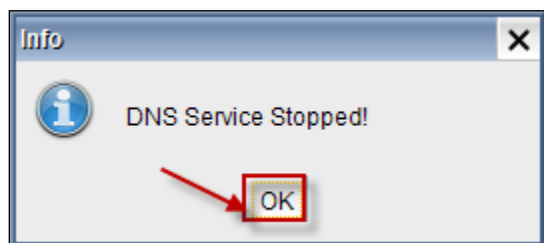
In the below screen we can notice the **Status** of the **DNS Server** is shown as **Started**.



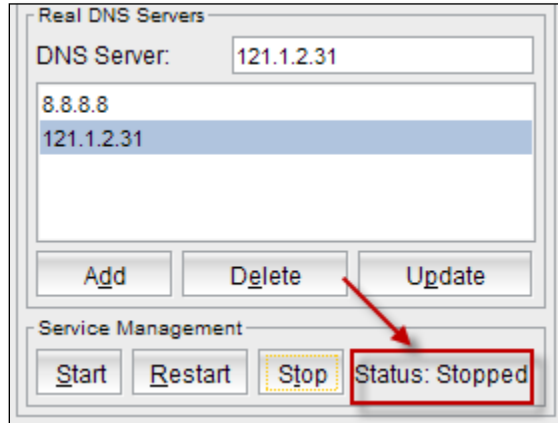
Select the Server and click on **Stop** button to stop the services of **DNS Server**.



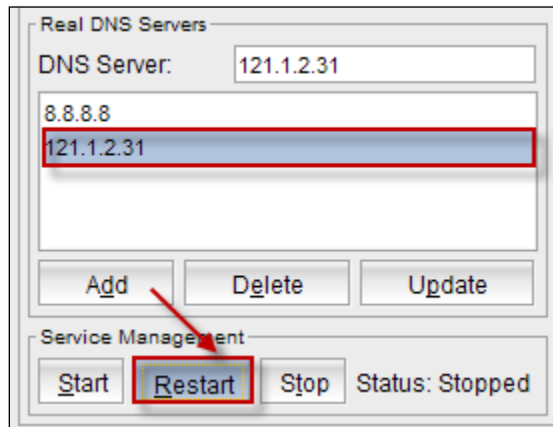
Below screen appears stating that **DNS Service Stopped**, click **OK** to close the current tab.



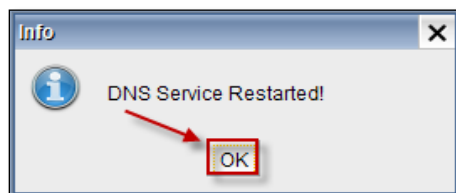
In the below screen we can notice the status of the **DNS Server** is shown as **Stopped**.



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

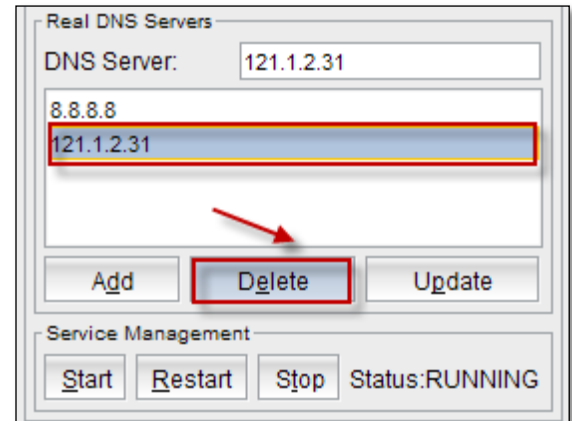
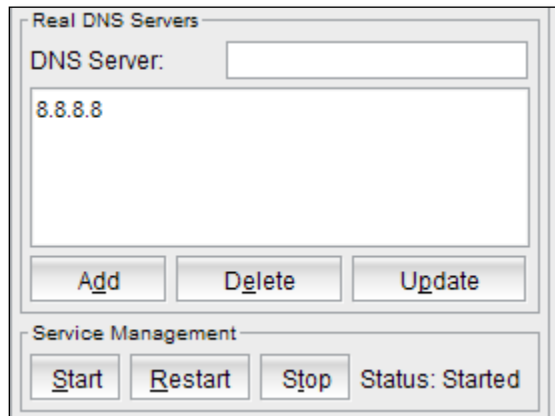


Below screen appears stating that **DNS Service Restarted**, click **OK** to close the current tab.



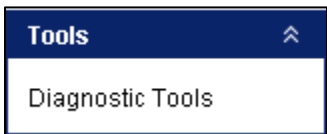
Select the Server and click on **Delete** button to delete a **DNS Server**.

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

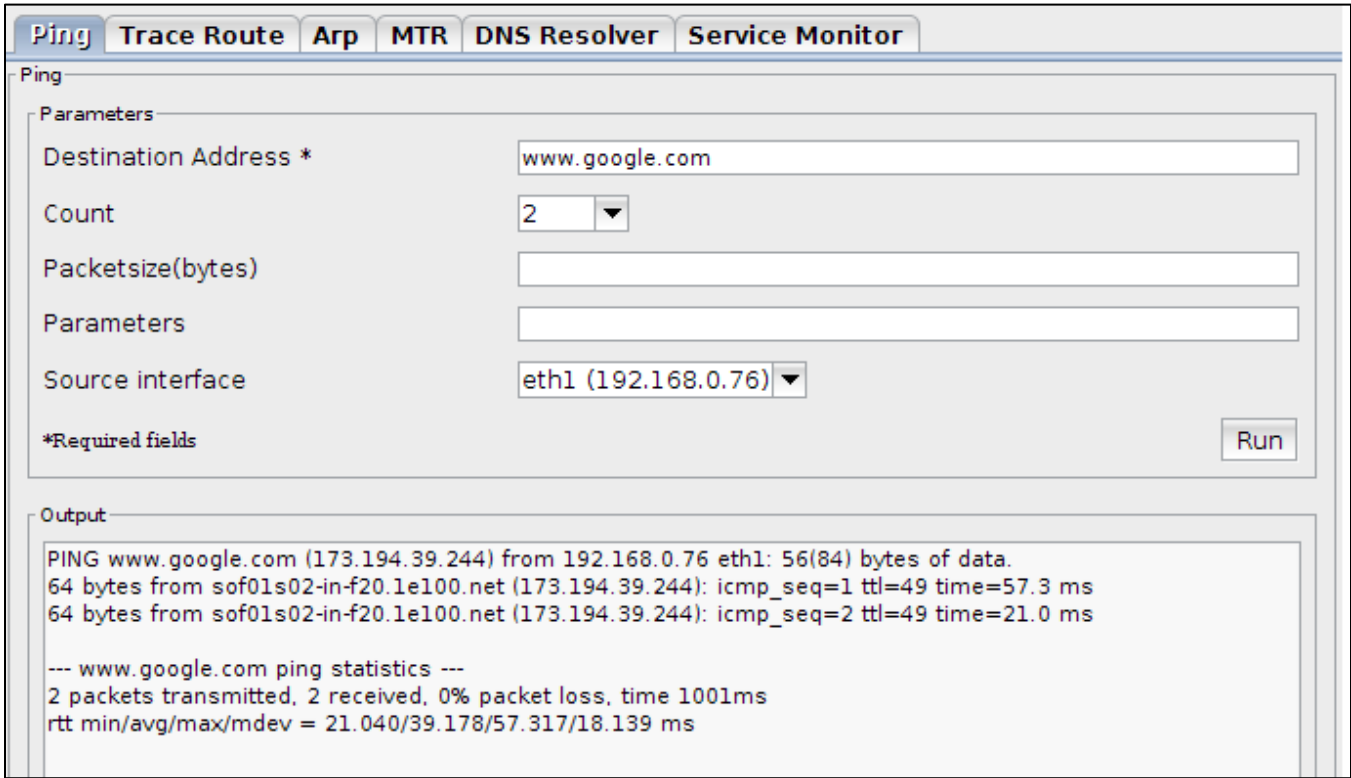


Diagnostic Tools

Several diagnostic tools are provided in LMC GUI. Sample tools and their uses in shown in the following screenshots.



Ping



1	Destination Address	IP address, computer name or domain name to be tested.
2	Count	Packet count to be sent during ping test.
3	Packet Size(bytes)	Packet size (in bytes) to be used in ping test.
4	Parameters	Other ping parameters. (GNU/Linux ping parameters)
5	Source Interface	Ping packets are sent to the destination over given interface.
6	Run	Test is started with given options.
7	Output	Test result.

Trace Route

Ping
Trace Route
Arp
MTR
DNS Resolver
Service Monitor

Trace Route

Parameters

Destination Address *
www.google.com

Parameters

Source interface
Automatic selection

☒ Do not resolve addresses to host names

*Required fields
Run

Output

```

traceroute to www.google.com (173.194.39.243), 30 hops max, 40 byte packets
 1 192.168.0.1 0.489 ms 0.348 ms 0.313 ms
 2 10.2.0.1 0.858 ms 0.562 ms 0.614 ms
 3 192.168.1.11 0.987 ms 1.100 ms 0.794 ms
 4 37.202.55.129 5.173 ms 4.486 ms 4.417 ms
 5 37.202.55.97 4.455 ms 6.157 ms 5.973 ms
 6 37.202.55.66 5.698 ms 6.469 ms 6.982 ms
 7 213.74.194.253 7.254 ms 7.057 ms 6.830 ms
 8 10.36.2.222 12.234 ms 10.36.1.61 12.019 ms 10.36.1.49 11.804 ms
 9 10.36.2.93 11.532 ms 11.140 ms 10.764 ms
10 10.36.1.118 9.854 ms 8.862 ms 8.636 ms
11 72.14.242.230 23.275 ms 23.028 ms 22.850 ms
12 72.14.235.79 20.803 ms 22.841 ms 20.407 ms
13 173.194.39.243 22.046 ms 22.452 ms 18.888 ms

```

1	Destination Address	IP address, computer name or domain name to be tested.
2	Parameters	Other traceroute parameters. (GNU/Linux traceroute parameters)
3	Source Interface	Traceroute packets are sent to the destination over given interface. If "Automatic selection" is chosen interface is determined using routing table.
4	Do Note Resolve addresses to host names	Do not resolve hostname of routers on the path to destination host. (Disable reverse lookup)
5	Run	Test is started with given options.
6	Output	Test result.

Arp

PingTrace RouteArpMTRDNS ResolverService Monitor

Arp

Parameters

☐ IP Address*

☐ Mac Address*

Parameters

Source interface

*Output can be filtered ip address or mac address

eth1 (192.168.0.76)

Run

Output

Address	HWtype	HWaddress	Flags	Mask	Iface
192.168.0.63	ether	08:00:27:53:86:d9	C		eth1
192.168.0.157	ether	4c:72:b9:7c:55:69	C		eth1
192.168.0.1	ether	00:90:0b:2f:a9:09	C		eth1

Entries: 3 Skipped: 0 Found: 3

1	IP address	IP address to be filtered.
2	Mac Address	MAC address to be filtered.
3	Parameters	Other arp parameters. (GNU/Linux arp parameters)
4	Source Interface	ARP listing is done on given interface.
5	Run	Test is started with given options.
6	Output	Test result.

112

Labris Networks

Mtr

Ping
Trace Route
Arp
MTR
DNS Resolver
Service Monitor

MTR

Parameters

Destination Address *
www.google.com

Packet Size (bytes)
20

Interval Between ICMP Echo Request(sec)
2

Ping Count (max 100)
5

Source interface
Automatic selection ▼

☒ Do not resolve addresses to host names

*Required fields
Run

Output

Host	Loss%	Last	Avg	Best	Wrst	StDev
192.168.0.1	0.0%	0.5	0.6	0.5	0.6	0.0
10.2.0.1	0.0%	0.6	0.6	0.5	0.8	0.1
192.168.1.11	0.0%	0.8	0.9	0.8	1.1	0.1
37.202.55.129	0.0%	6.7	4.9	4.2	6.7	1.1
37.202.55.97	0.0%	6.0	5.8	3.9	10.1	2.5
37.202.55.66	0.0%	4.6	6.3	4.6	8.8	2.0
213.74.194.253	0.0%	6.5	6.5	5.6	7.9	0.9
10.36.1.49	0.0%	13.8	13.0	9.8	18.2	3.4
10.36.2.93	0.0%	18.6	15.3	10.2	22.2	5.1
82.222.224.81	0.0%	9.5	16.2	9.5	41.1	13.9
72.14.242.230	0.0%	20.3	23.0	18.6	33.0	6.0
72.14.235.79	0.0%	22.2	20.9	19.3	24.0	2.1
173.194.39.242	0.0%	23.4	20.8	18.4	23.4	2.0

1	Destination Address	IP address, computer name or domain name to be tested.
2	Packet size (bytes)	Packet size (in bytes) to be used in ping test.
3	Interval Between ICMP echo request (sec)	Pause in seconds between two consecutively sent packets.
4	Ping Count (Max 100)	Count of packets to be sent for testing. After all packets are sent and test is done results are shown.
5	Source Interface	MTR packets are sent to the destination over given interface. If "Automatic selection" is chosen interface is determined using routing table.
4	Do Not Resolve addresses to host names	Do not resolve hostname of routers on the path to destination host. (Disable reverse lookup)
5	Run	Test is started with given options.
6	Output	Test result.

DNS Resolver

DNS Resolver

Parameters

Destination Address/IP *

☐ Query Over Specific Nameserver

Query Type

*Required fields

Output

```
--DNS Resolver Results--
www.google.com has address 173.194.39.241
www.google.com has address 173.194.39.242
www.google.com has address 173.194.39.243
www.google.com has address 173.194.39.244
www.google.com has address 173.194.39.240
www.google.com has IPv6 address 2a00:1450:4017:801::1012

--Forwarder DNS Health Check--
checking 8.8.8.8 195.175.39.40      DNS Servers; against test domains www.labristeknoloji.com www.google.c
DNS 8.8.8.8 positive
DNS 195.175.39.40 negative
```

1	Destination Address / IP	IP address, computer name or domain name to be tested.
2	Query Over specific name server	Name resolution test is done on given name server.
3	Query Type	Name resolution test's query type. By default A record lookup is done for test.
5	Run	Test is started with given options.
6	Output	Test result. DNS Resolver Results: Result got from remote name server. Forwarder DNS Health Check: Health status of the name servers defined in Labris Log device.















Service Monitor


Running state of Labris services are show on the table below.

Ping
Trace Route
Arp
MTR
DNS Resolver
Service Monitor

Service Monitor

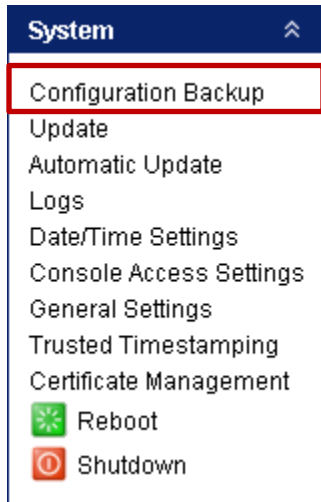
Services

Antivirus	
Directory Service	
SMTP Scanner	
LMC Management Service	
Syslog Server	
Web Filter	
IPS Service	
MTA Service	
IMAP Service	
POP3 Scanner	
Databases	
AD Integration Services	
Web Management Services	
Log Processor	

 Refresh

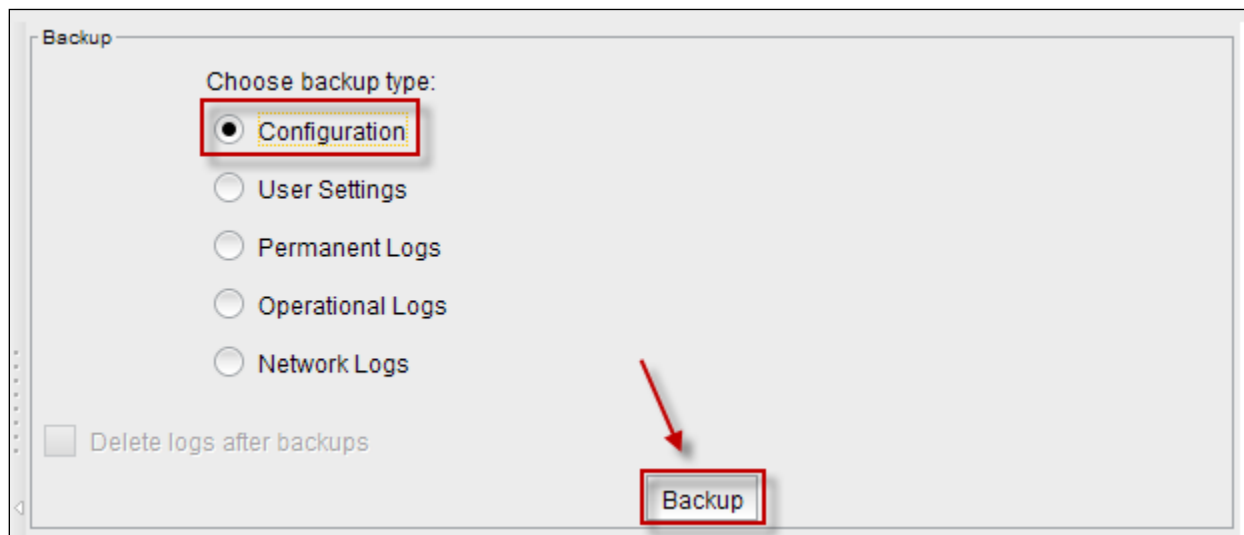
Configuration Backup / Restore

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

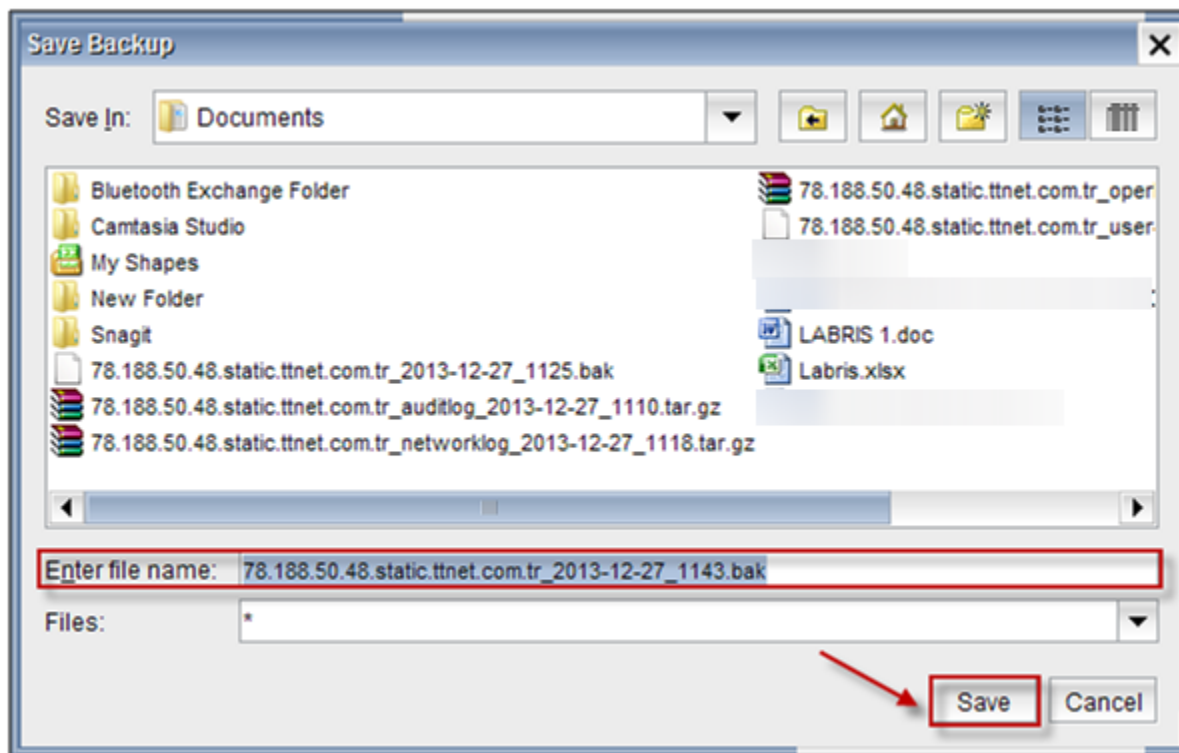


According to user requirement choose any one of the radio button in the below screen and click on **Backup Tab** to start the Backup process.

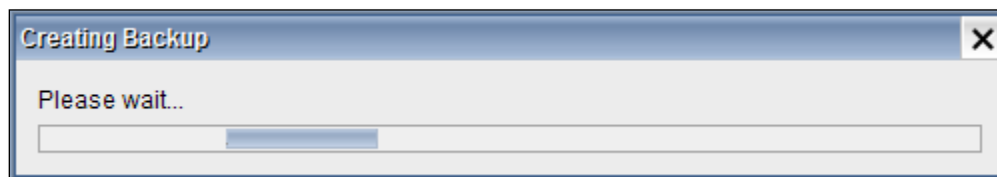
Choose **Configuration** radio button and click on **Backup** button.



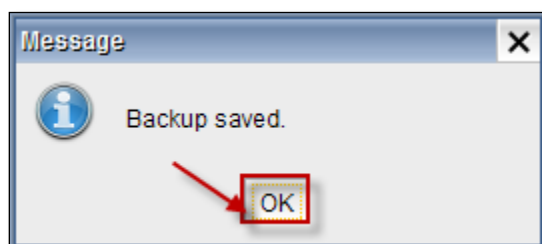
Click on **Save tab** to save the file with **file name.bak** extension in your local machine as in the below screenshot.



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

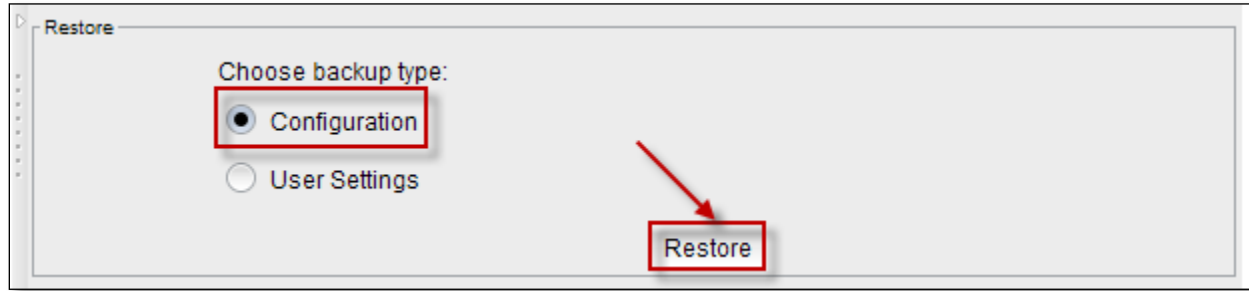


Below screen appears stating that **Backup** saved at the chosen location in your hard drive, click **OK** to close the current tab.

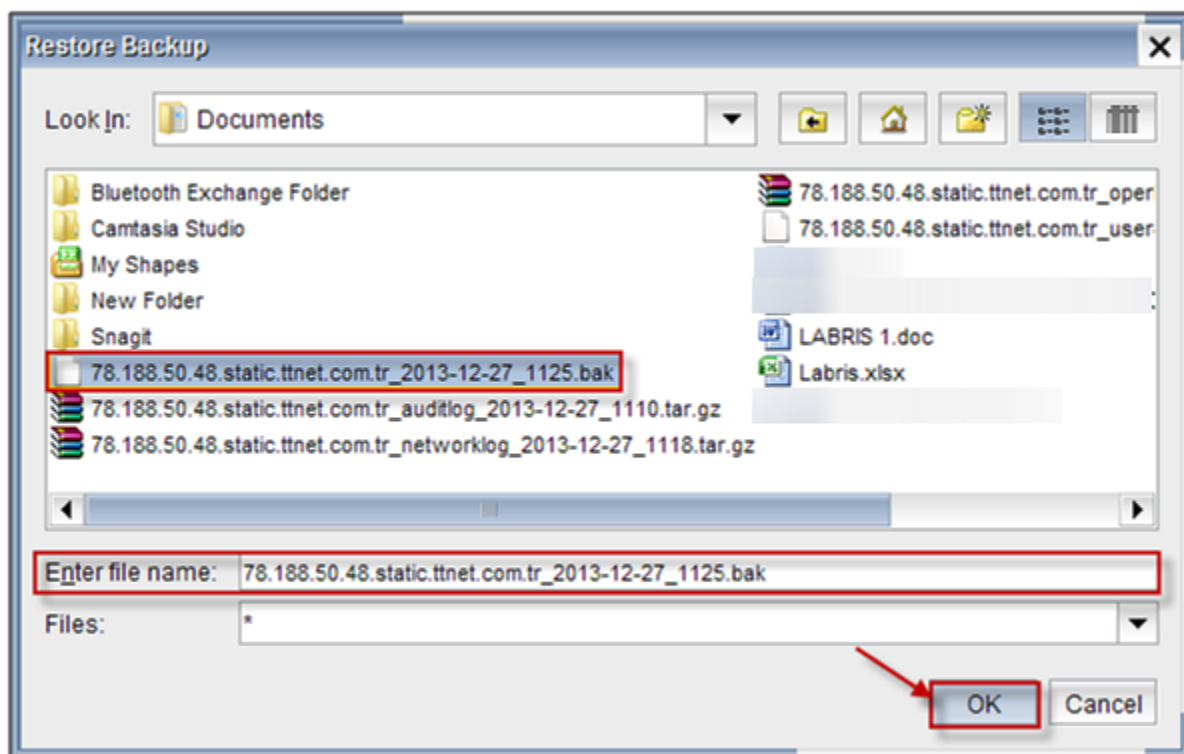


According to user requirement choose any one of the radio button in the below screen and click on **Restore** to start restore process

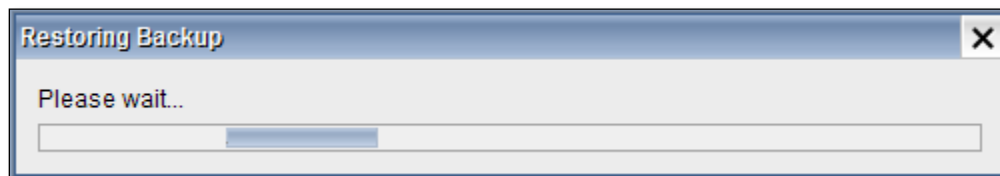
Choose **Configuration** and click on **Restore** button.



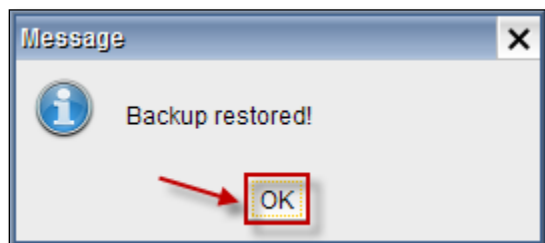
Choose the backup file from the local machine and click **OK** to **Restore Backup**



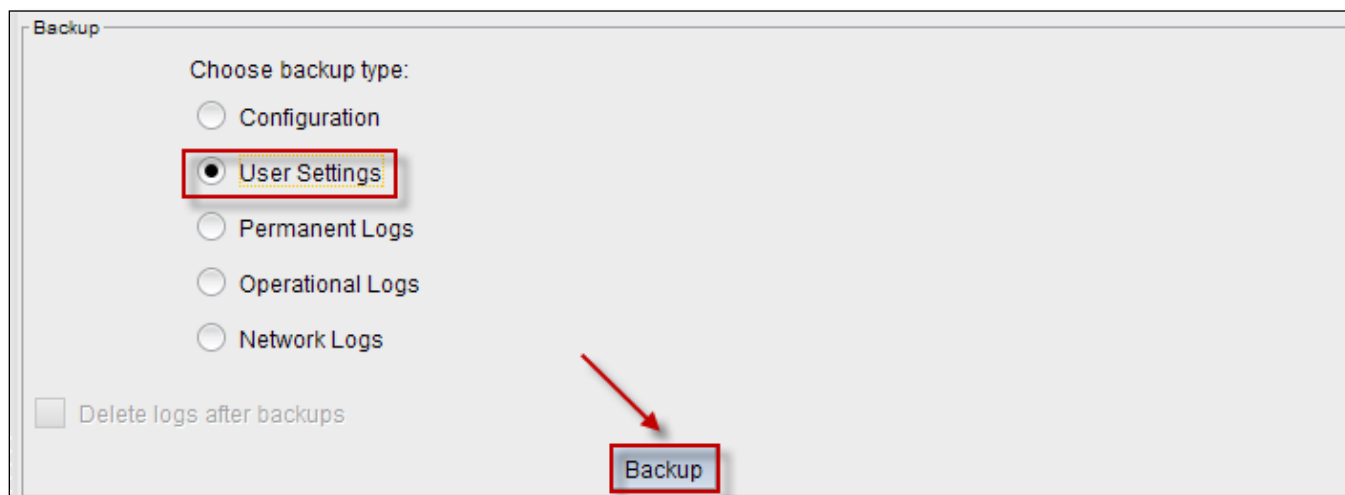
Restoring Backup process for **Configuration** is in progress.



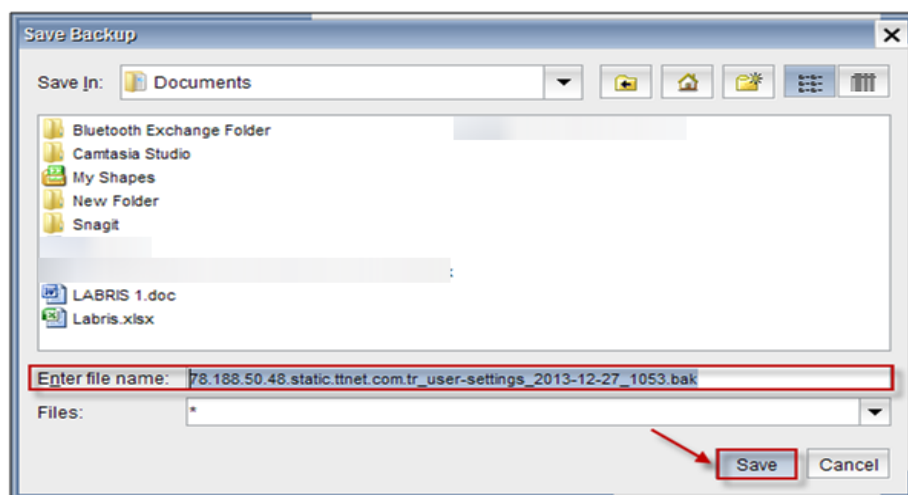
Below screen appears stating that **Backup restored**, click **OK** to close the current tab.



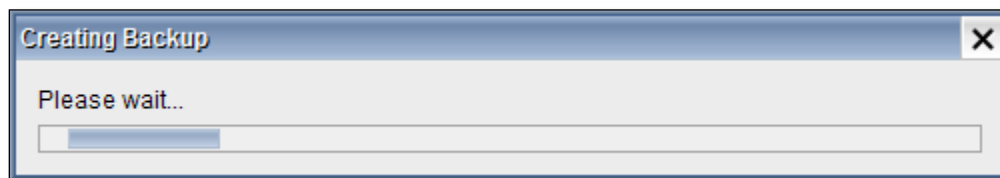
Choose **User Settings** and click on **Backup Tab**



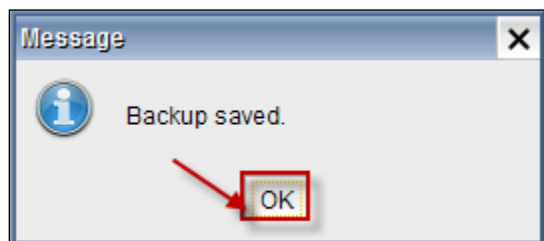
Click on **Save tab** to save the file with **file name.bak** extension in your local machine as shown in the below screen.



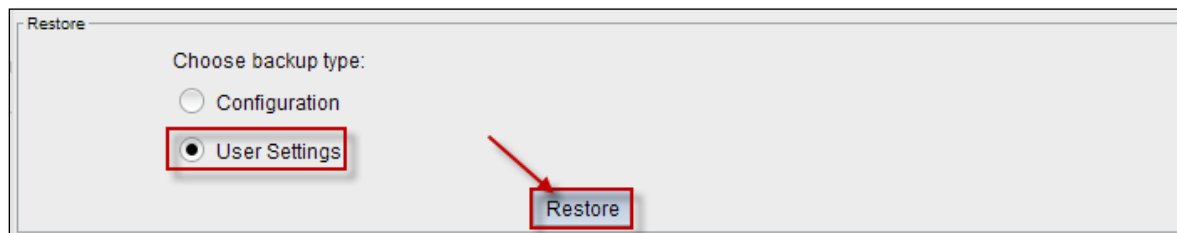
Creating **Backup** process for **User Settings** is in progress.



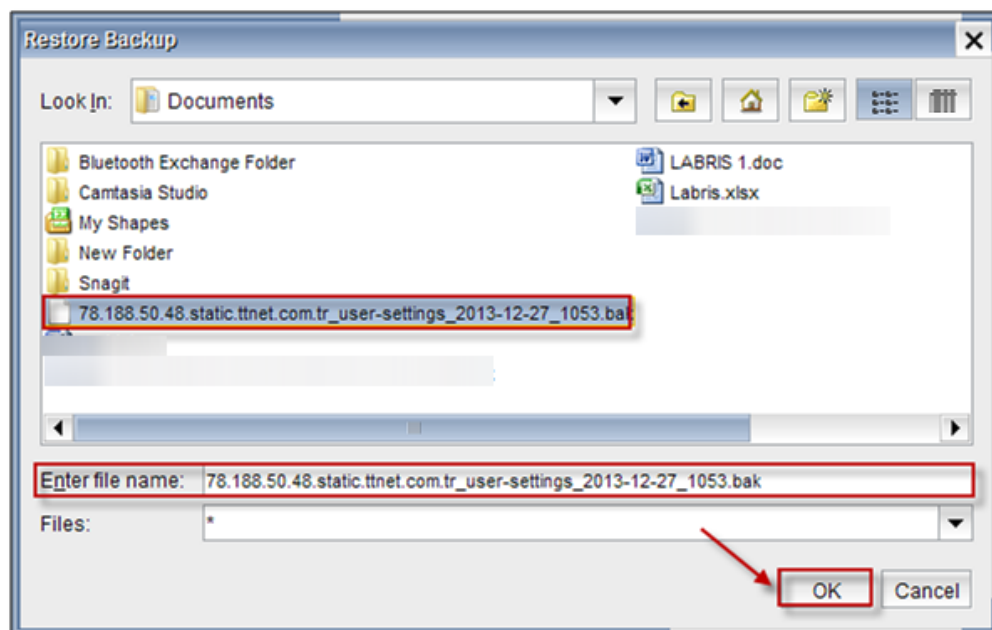
Below screen appears stating that **Backup Saved**, click **OK** to close the current tab.



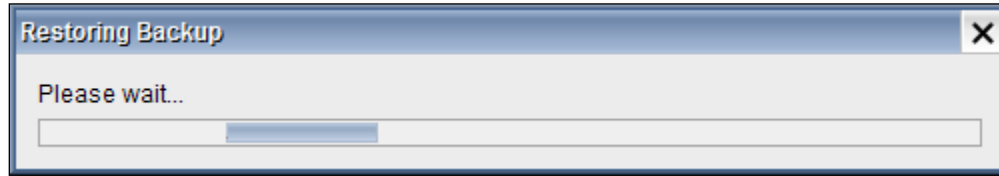
Choose **User Settings** and click on **Restore** button.



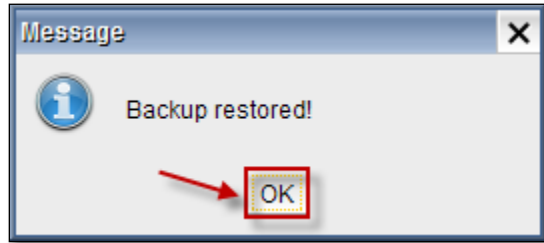
Choose the backup file from the local machine and click **Ok** to **Restore Backup**



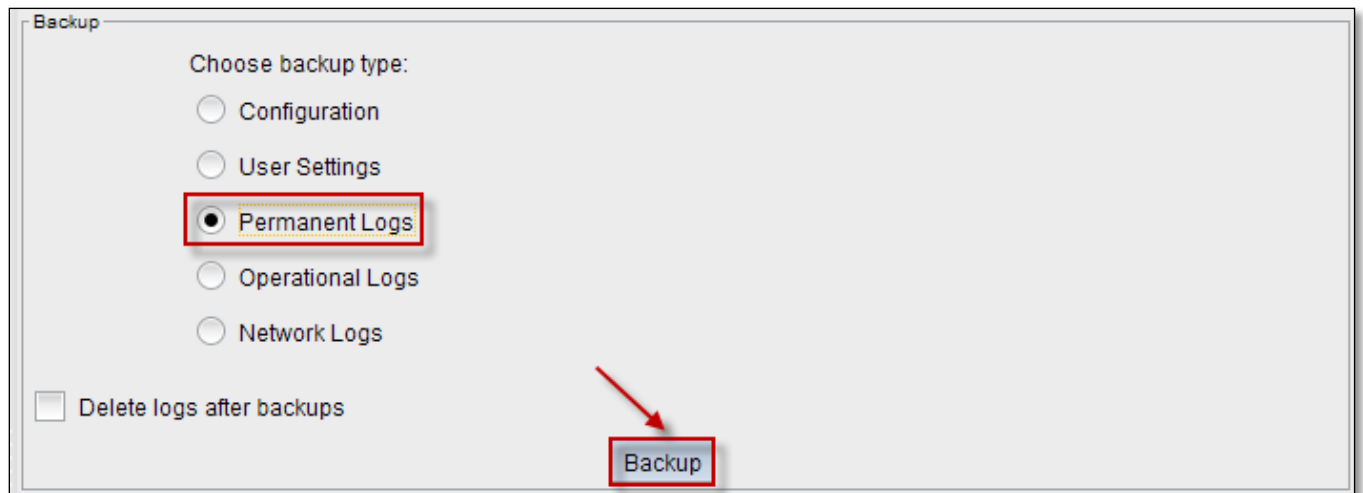
Restoring Backup process for **User Settings** is in progress.



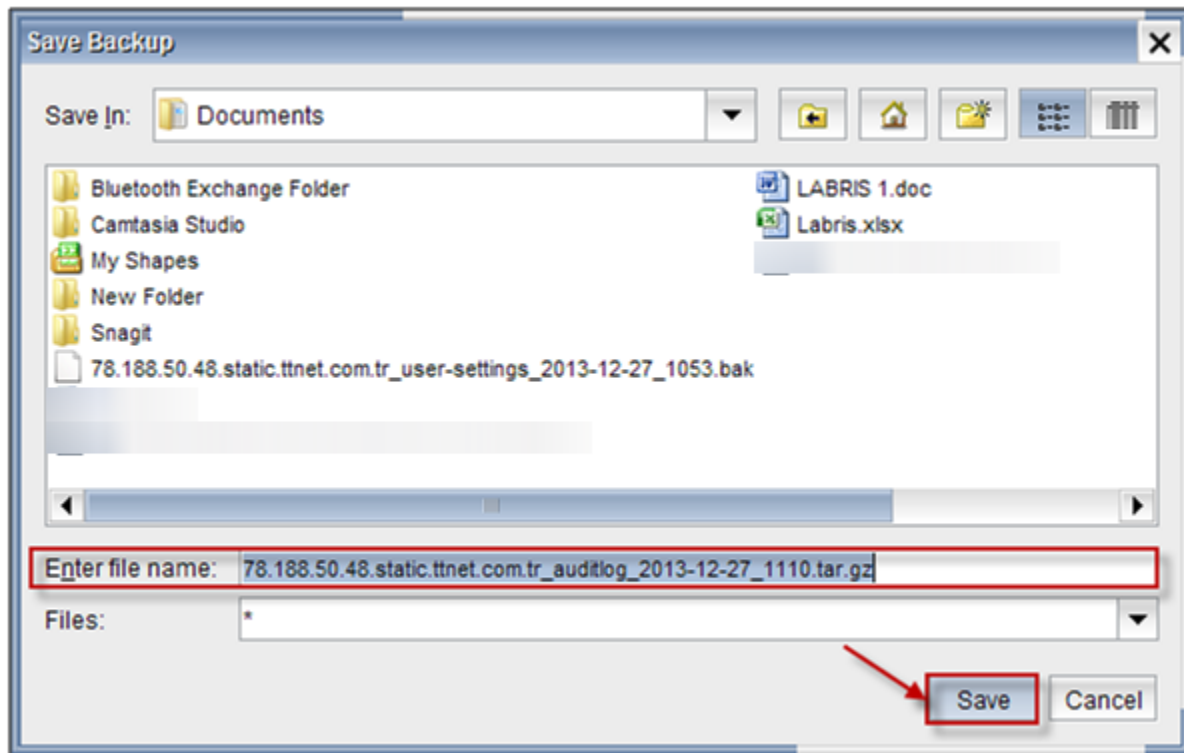
Below screen appears stating that **Backup restored**, click **OK** to close the current tab.



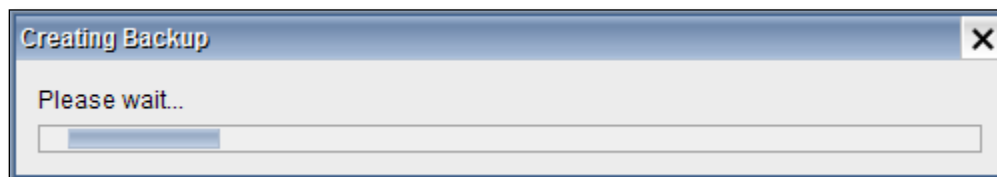
Choose **Permanent Logs** and click on **Backup** button.



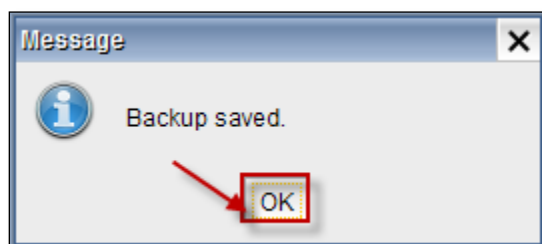
Click on **Save** tab to save the file with **file name. tar.gz** extension in your local machine at your chosen location as shown below.



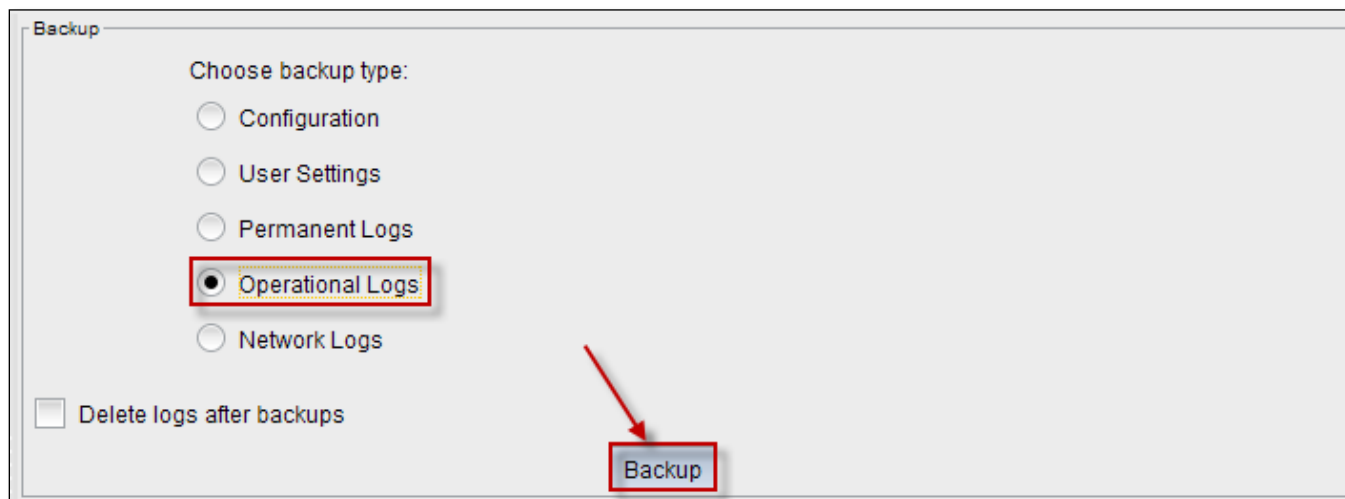
Creating **Backup** process for **Permanent logs** is in progress.



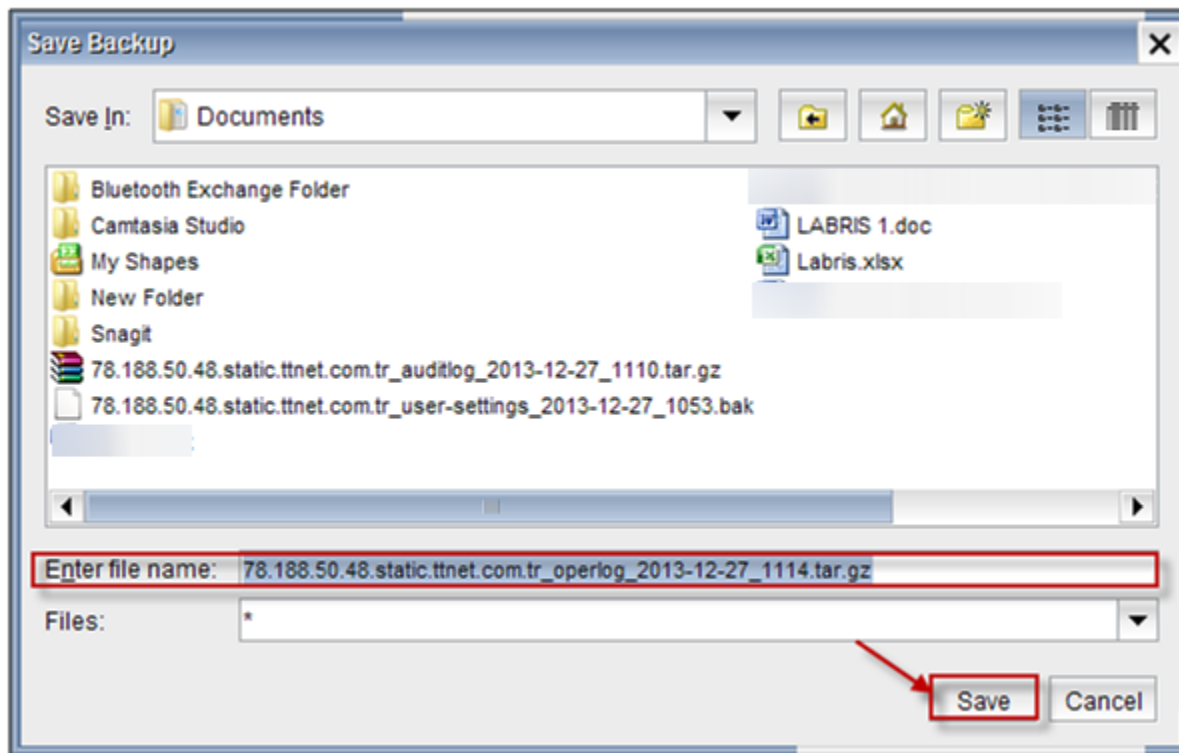
Below screen appears stating that **Backup Saved**, click **OK** to close the current tab.



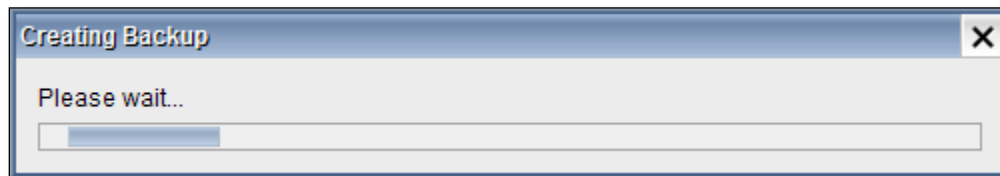
Choose **Operational Logs** and click on **Backup Tab**



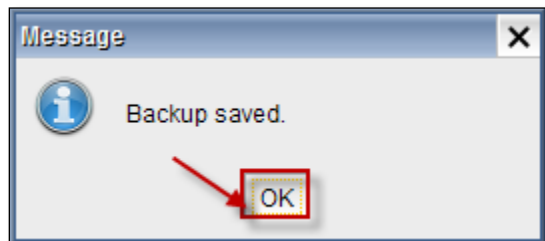
Click on **Save tab** to save the file with **file name .tar.gz** extension in your local machine to save the operational logs as shown below.



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

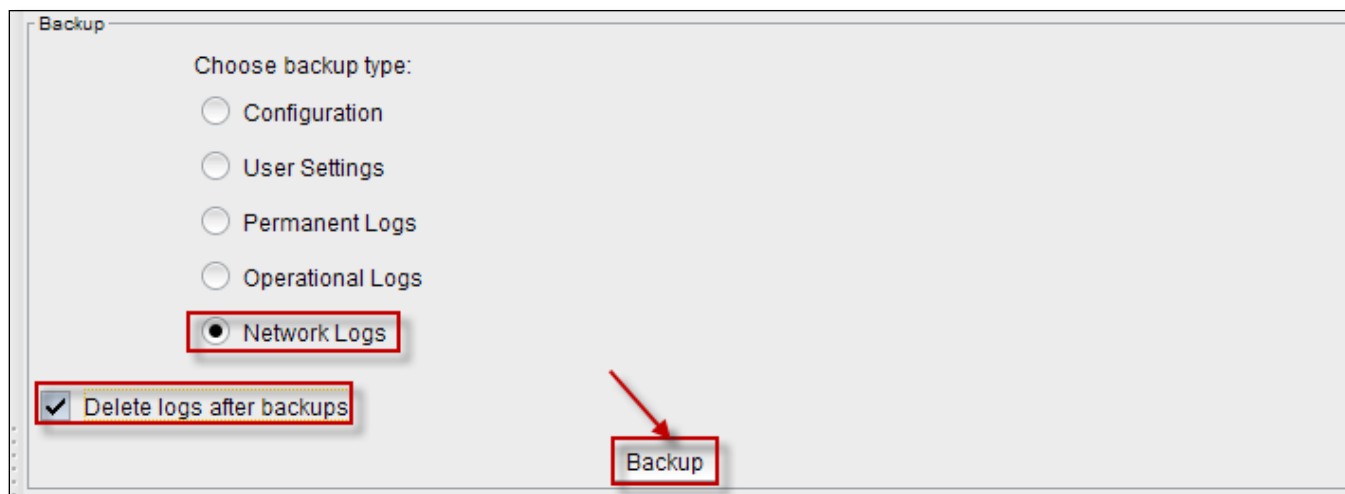


Below screen appears stating that **Backup Saved**, click **OK** to close the current tab.

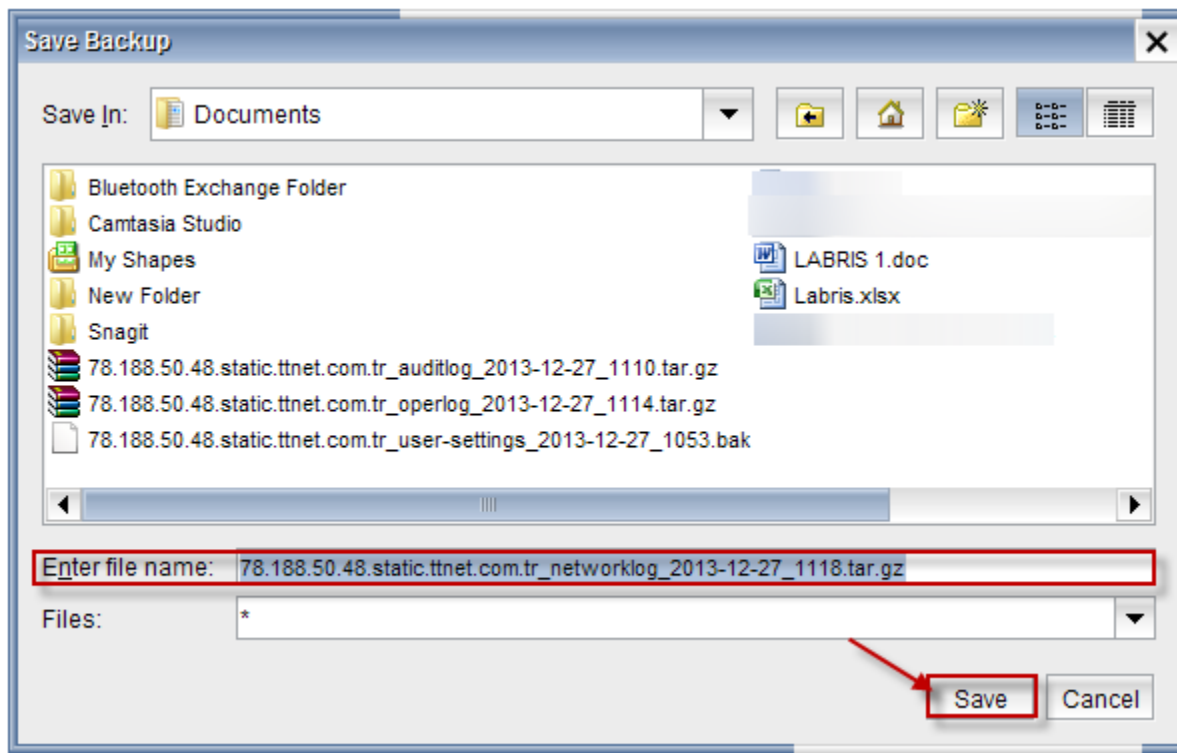


Choose **Network Logs** and click on **Backup Tab**.

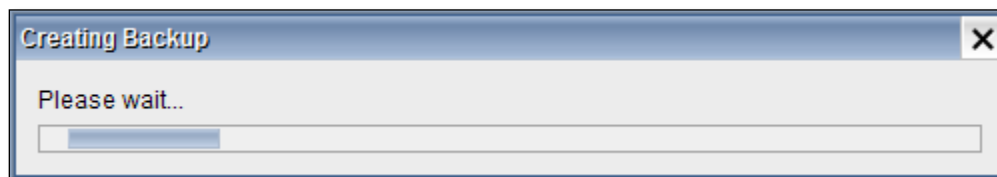
If we want to delete logs after completion of Backups process for each log, Check the **Delete logs after backups** check box.



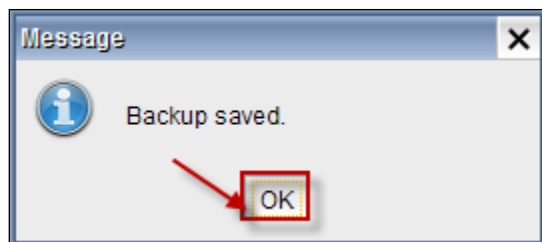
Click on **Save** tab to save the file with **file name .tar. gz** extension in your local machine as shown below.



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

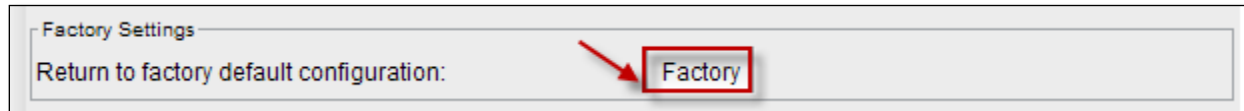


Below screen appears stating that **Backup Saved**, click **OK** to close the current tab.



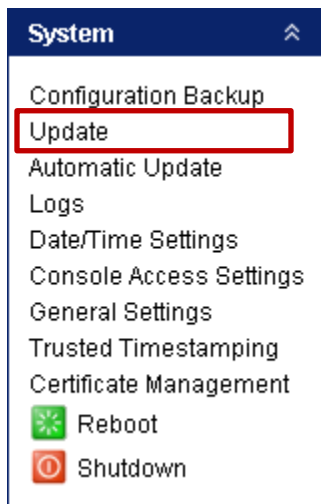
Factory settings

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



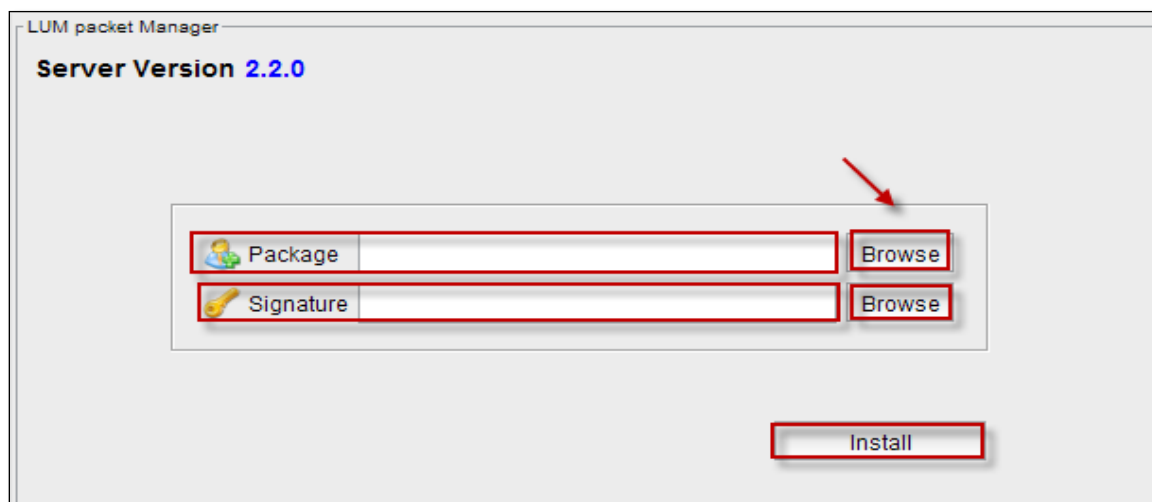
Update

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



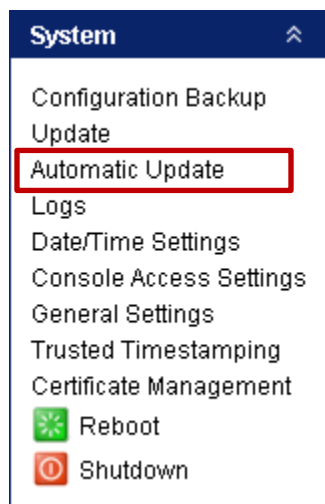
Note – In the below screen if any package is pending for upgrade, please request from the service provider using the mail id or call.

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**



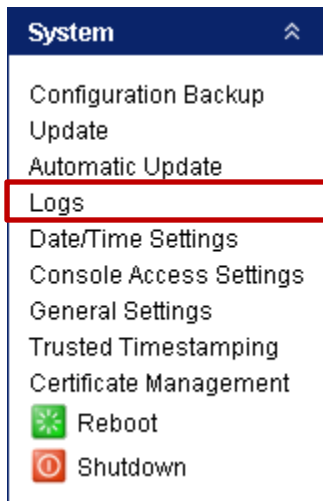
Automatic Update

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



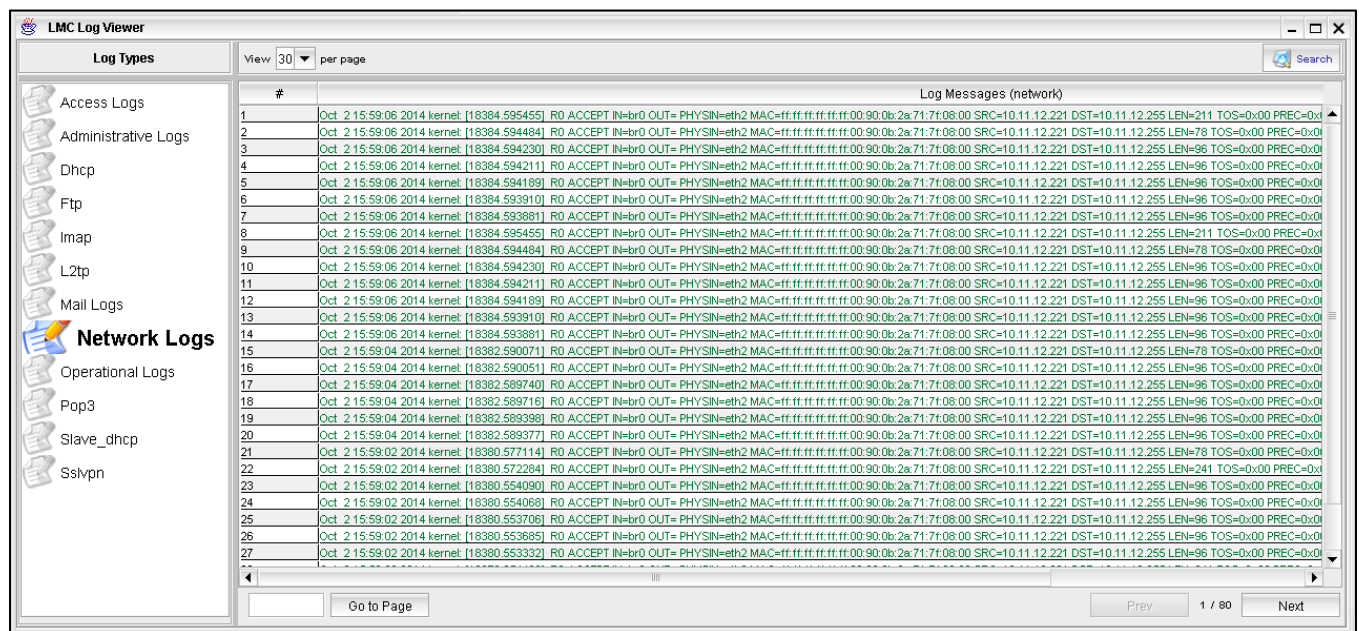
Logs

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.



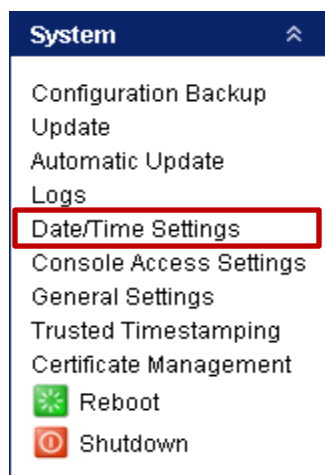
Different types of Logs in LMC.

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

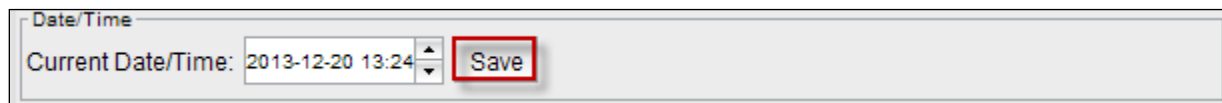
7	Network log	Log messages related to Network log can be viewed
8	Operational	Log messages related to Operational can be viewed
9	SSLVPN	Log messages related to SSLVPN can be viewed
10	Wauth-access.log	Log messages related to Wauth-access can be viewed
11	Slave_dhcp	Log Messages Custom syslog dhcp logs.

Date / Time Settings

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

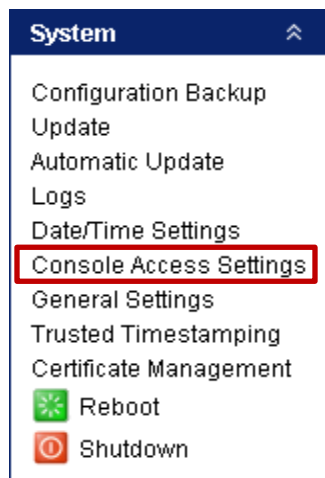


Below screen appears, set the date and time and click **Save** to save the **Current Date/Time**.

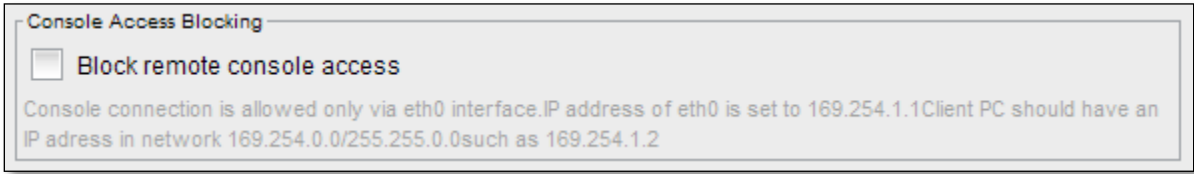


Console Access Settings

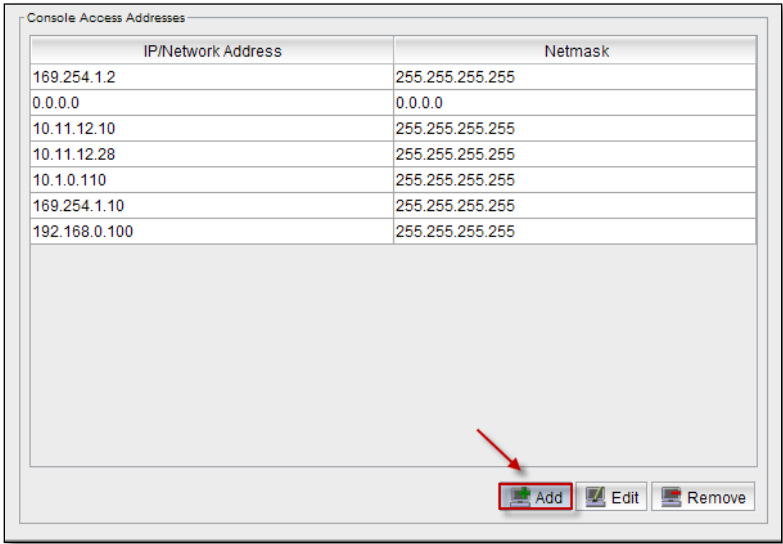
In System Module, right pane under **System Tab** click on **Console Access Settings**.



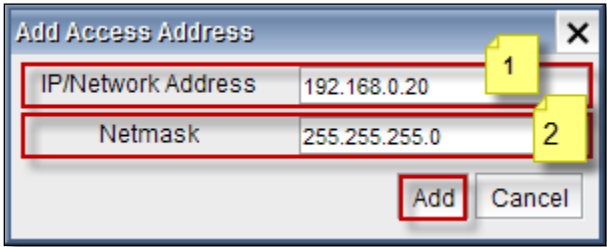
Enable **Block remote console access** check box to block remote access for other users or desktops.



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

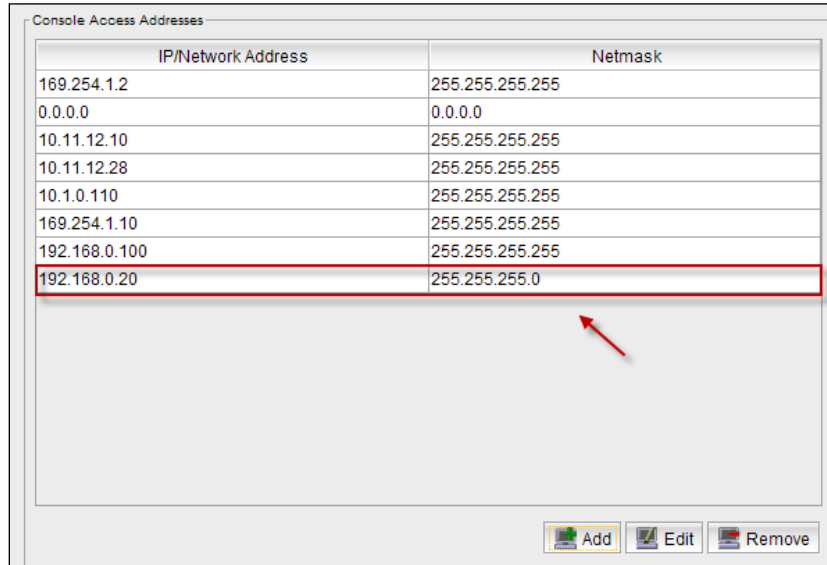


Below screen appears

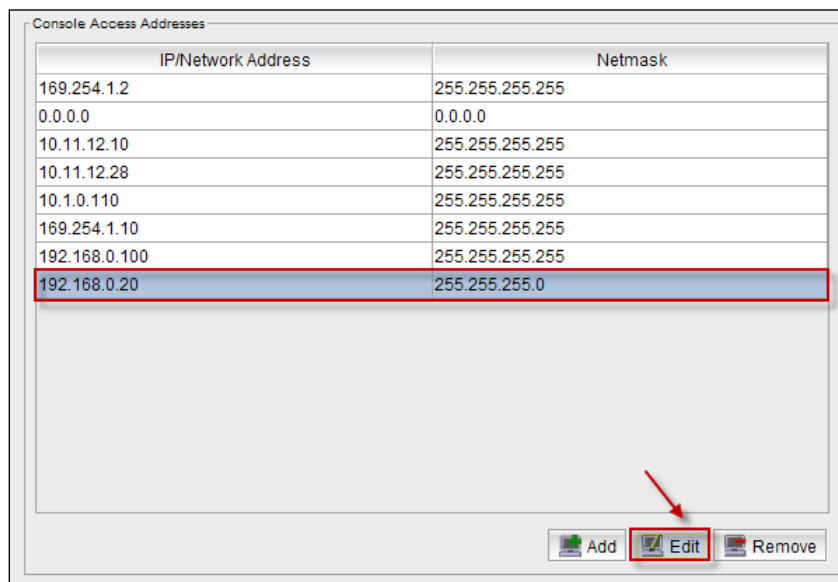


1	IP/Network Address	Type IP/Network Address
2	Netmask	Type Sub Netmask

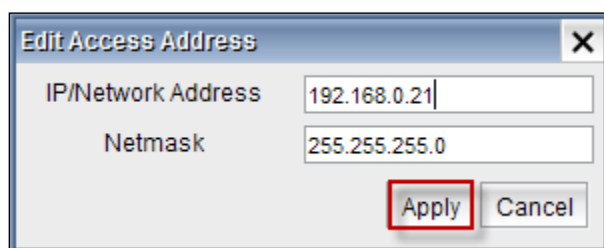
We can notice the **IP/Network** address in the **Console Access Address**



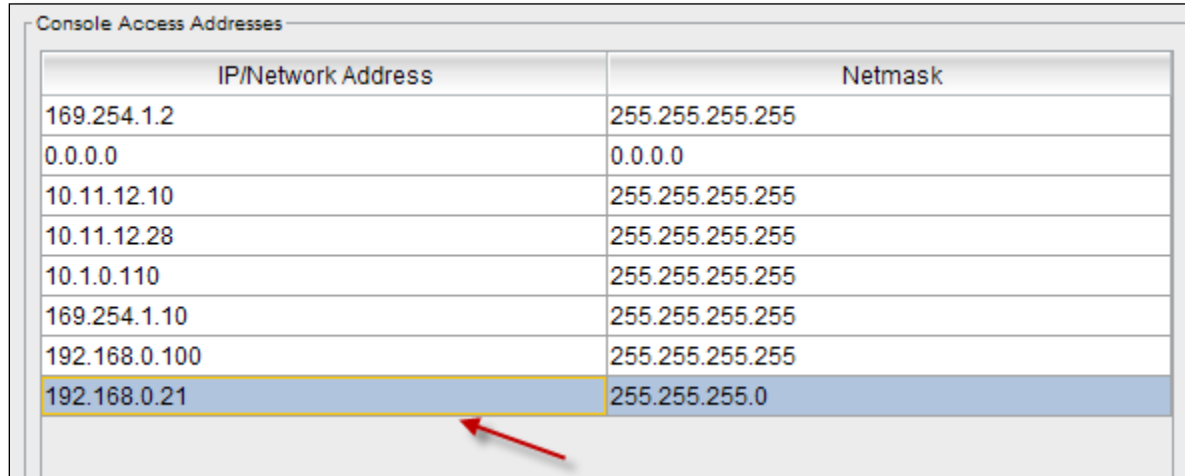
Select the **IP/Network Address** and click on **Edit** button.



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

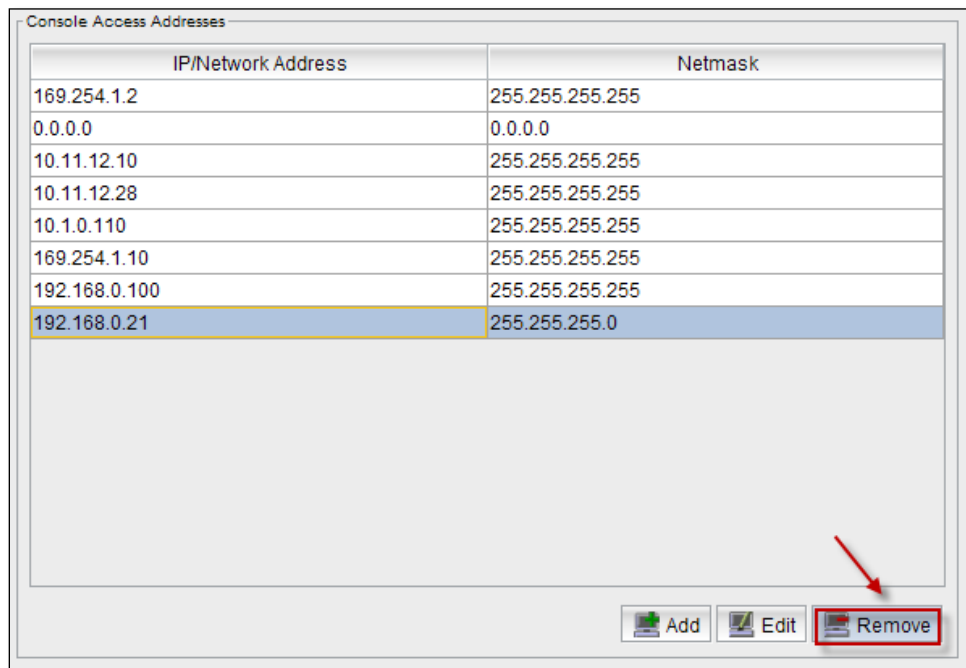


We can notice the applied changes



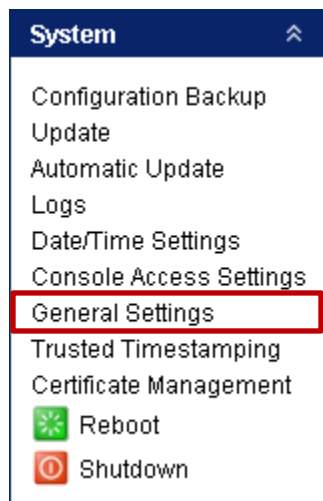
IP/Network Address	Netmask
169.254.1.2	255.255.255.255
0.0.0.0	0.0.0.0
10.11.12.10	255.255.255.255
10.11.12.28	255.255.255.255
10.1.0.110	255.255.255.255
169.254.1.10	255.255.255.255
192.168.0.100	255.255.255.255
192.168.0.21	255.255.255.0

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

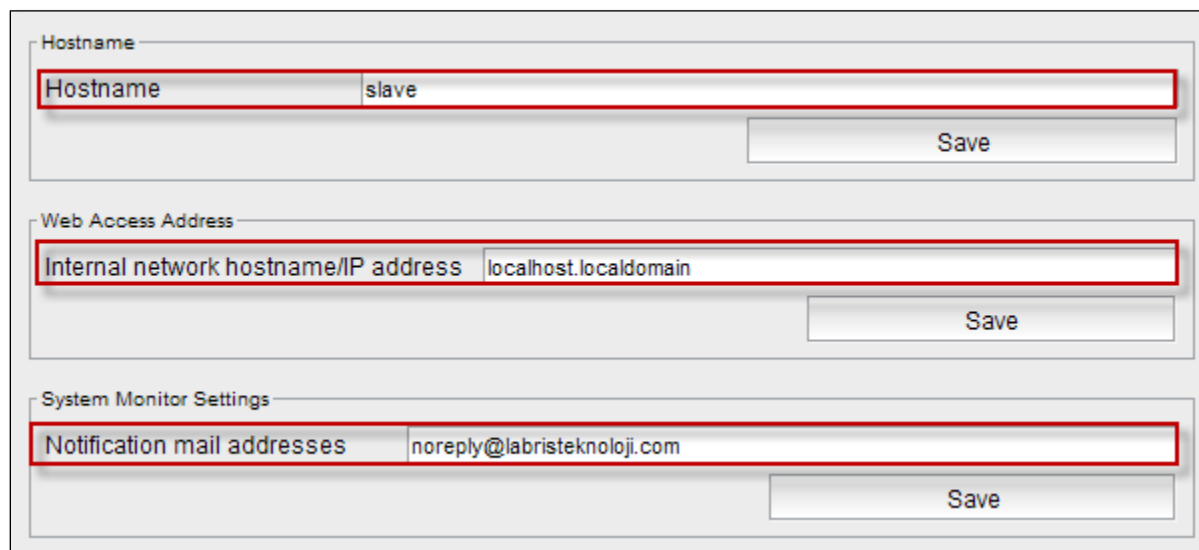


General Settings

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

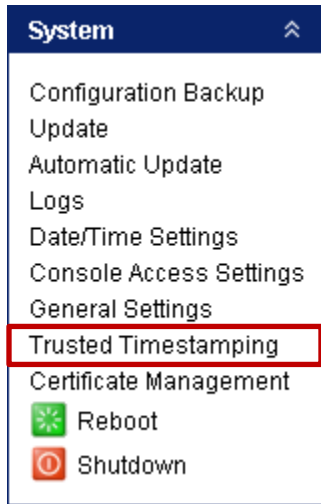


Below screen will appear displaying **Hostname**, **Internal network hostname/IP address**, and **Notification mail address**.

A screenshot of a web-based configuration interface for 'General Settings'. It consists of three vertically stacked sections, each with a title bar and a text input field followed by a 'Save' button. The first section, titled 'Hostname', has an input field containing the text 'slave'. The second section, titled 'Web Access Address', has an input field containing 'localhost.localdomain'. The third section, titled 'System Monitor Settings', has an input field containing 'noreply@labristeknoloji.com'. Each input field is highlighted with a red rectangular border.

Trusted Time Stamp

In **System Module**, right pane 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.

In the case of certain specified property on every day or **wanted periods** 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**

Settings

☒ Turktrust

☐ Local

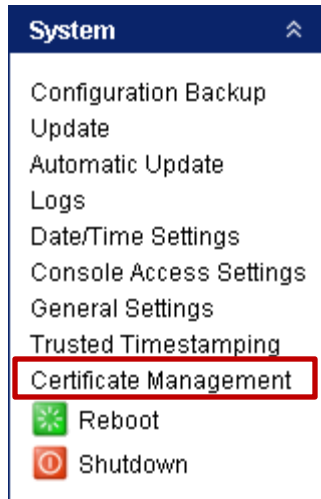
Previous Time Stamped Log Packages

Date	Hash
2013/12/19 03:31:14	dd15edd089aa027db85798fc69a32d8b
2013/12/17 03:31:14	2e8db4c6e7e7c0bb19f62a0c180d1546
2013/12/14 03:31:33	b4a4c86d08b97d6ce8808fbbc31f7035
2013/12/13 03:31:32	f2040007556816e44067321fbc1b0126
2013/12/12 03:31:31	b30f65657d6bb4d2bf93f6dfa562a93a
2013/12/11 03:31:31	dc19a2d1042b4ad8ca4426e494951966
2013/11/28 03:31:29	22653e0793d95a6a745c13839f6e3722
2013/11/27 03:31:36	1a776447b0672bea97f188ea2b5ca541
2013/11/26 03:31:36	42f30a85986d2c1c13e491e678628cff

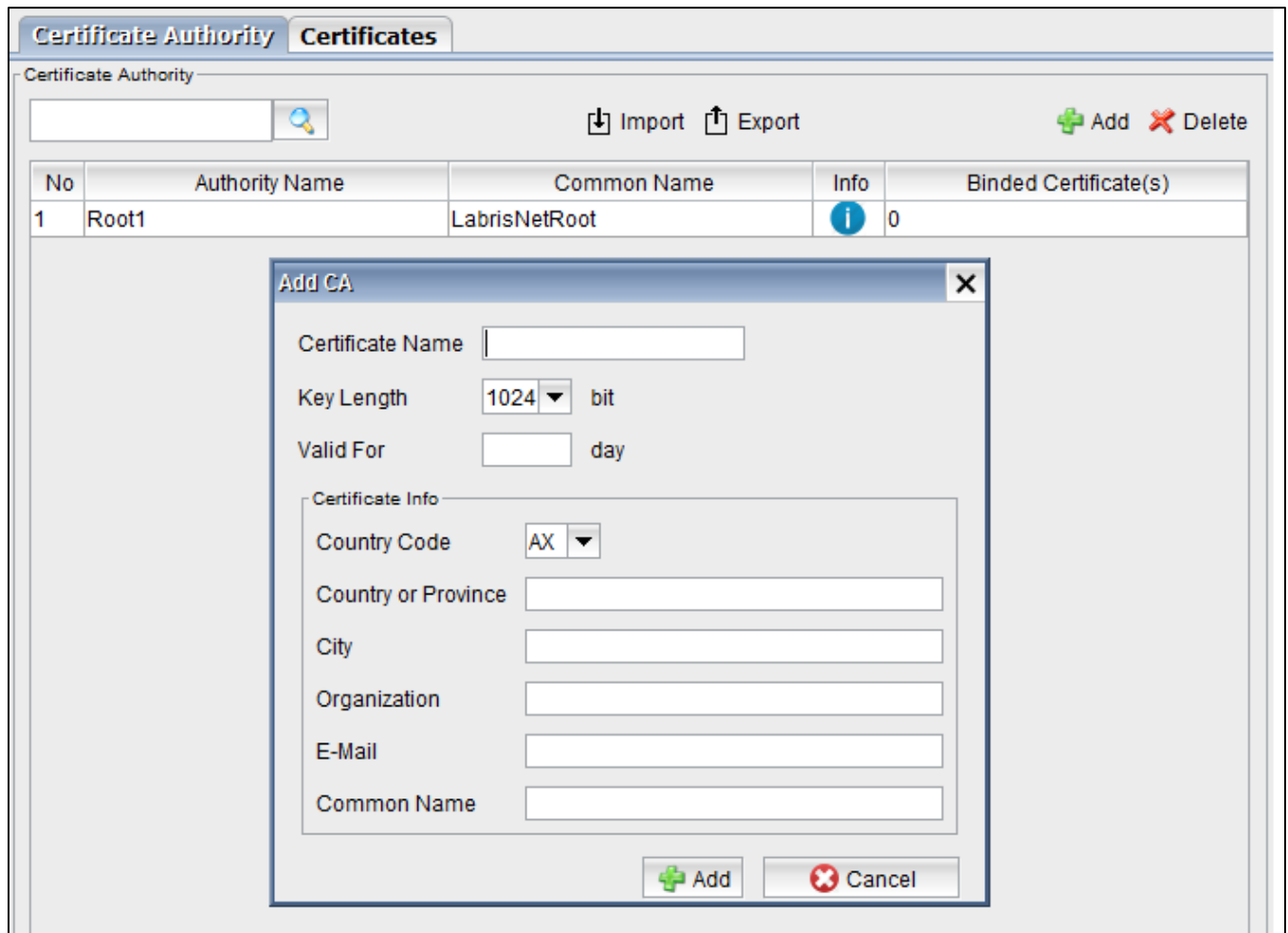
Save

Certificate Management

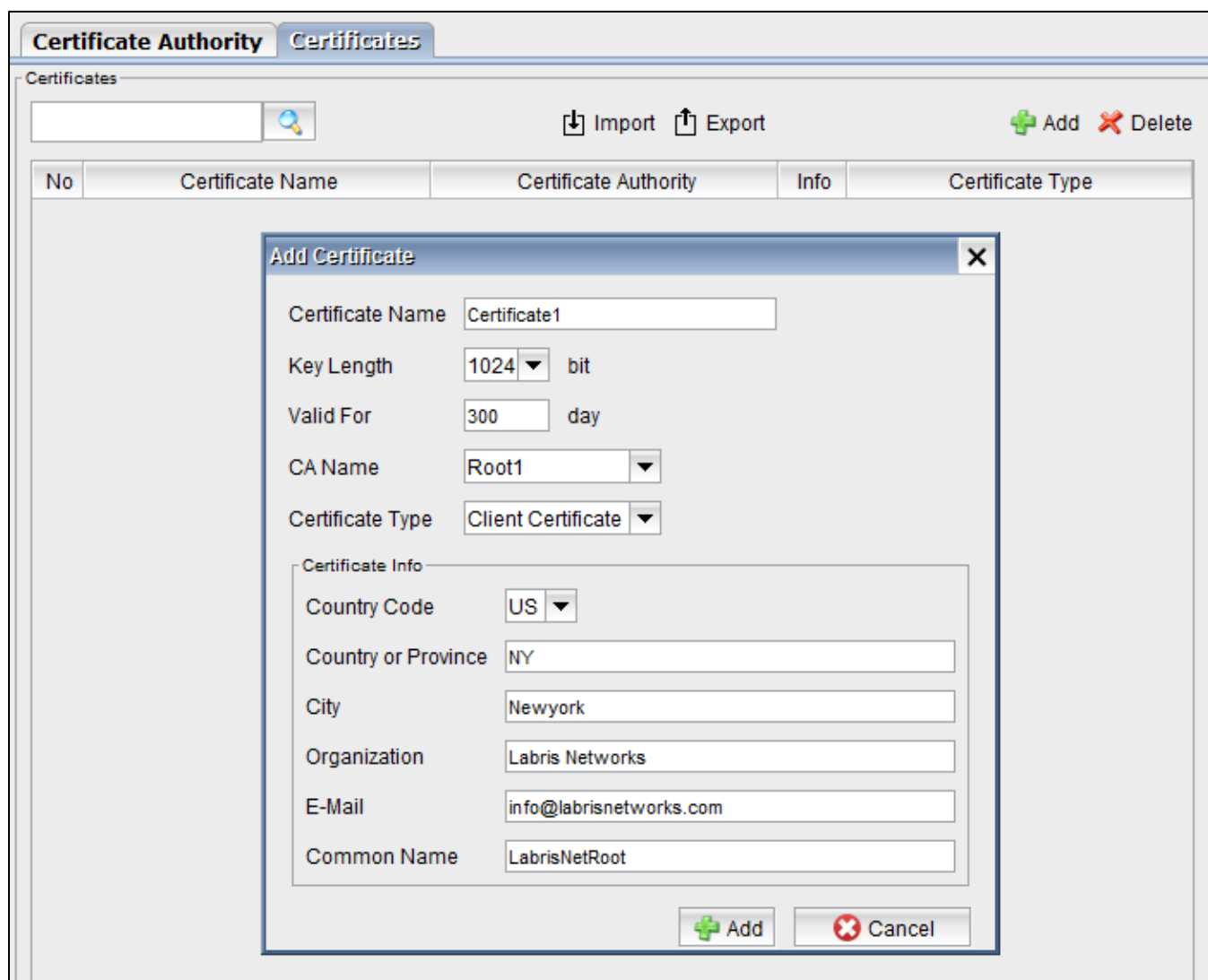
Certificate management tool is provided with this release. This tool provides following use cases:



i- Multiple root certificate generation



ii- Server and User certificate generation

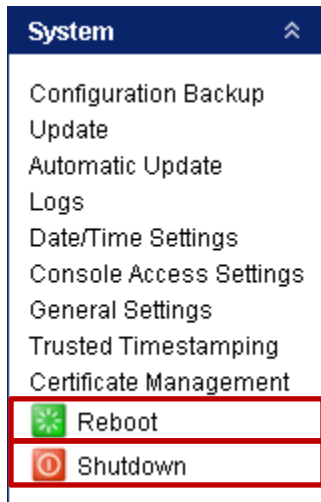


iii- Exporting and importing certificates

Restart and Shutdown

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

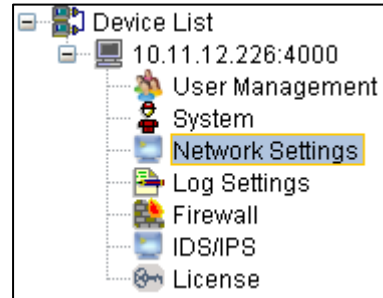
In System Module, under **System Tab** click on **Shutdown** to shutdown the System.



Network Settings

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

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



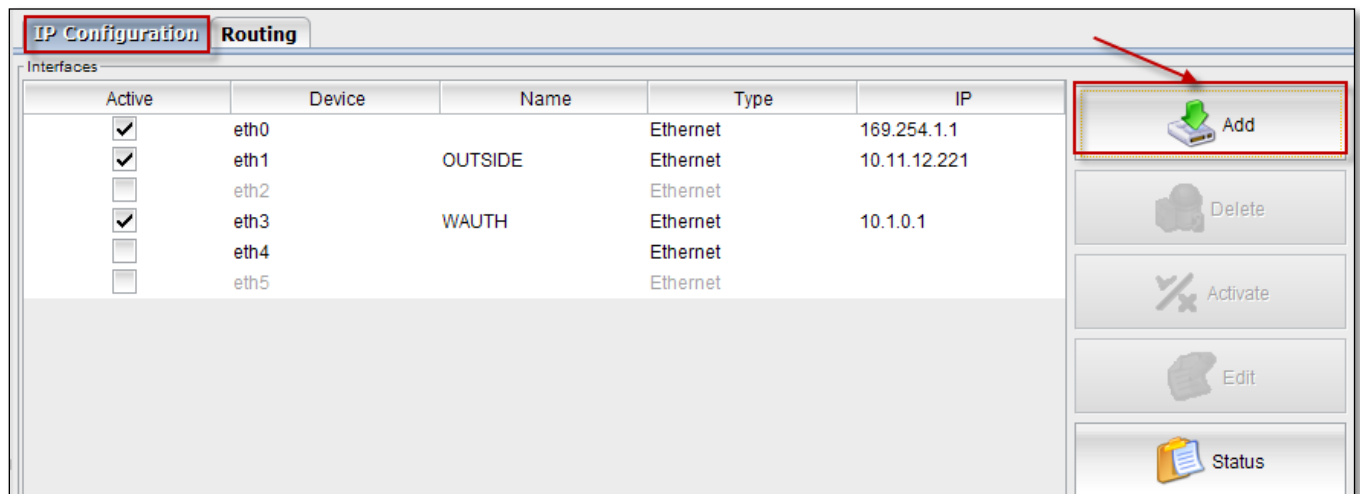
Right click on **Network Settings** and select **Connect**.

IP Configuration

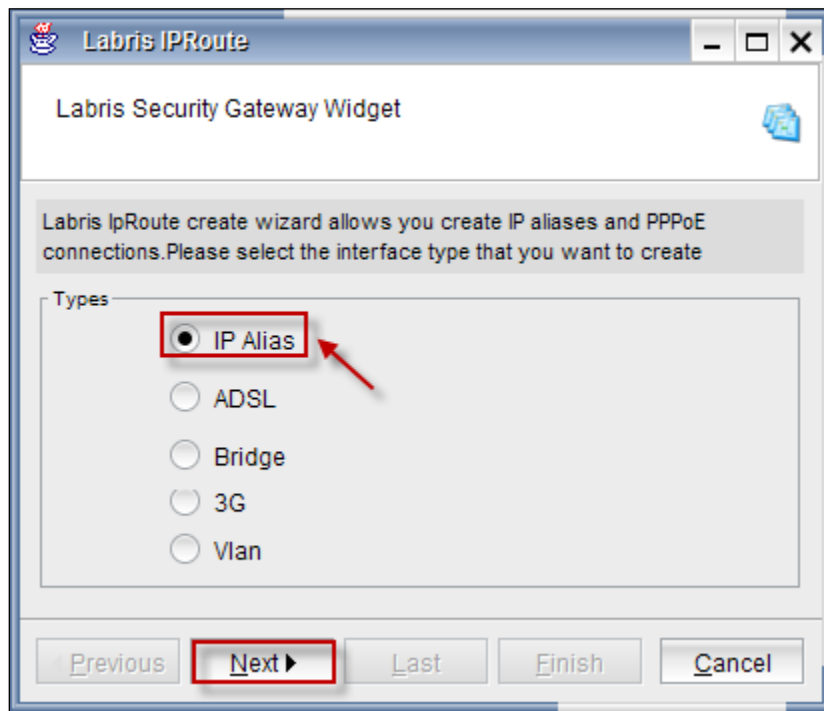
Labris Secure Gateway is a capable router, and it has many Ethernet interfaces both used for security and also routing, load balancing and many other network tasks. IP Routing is used to Configure Ethernet interfaces and routing configuration of Labris Security Gateway.

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

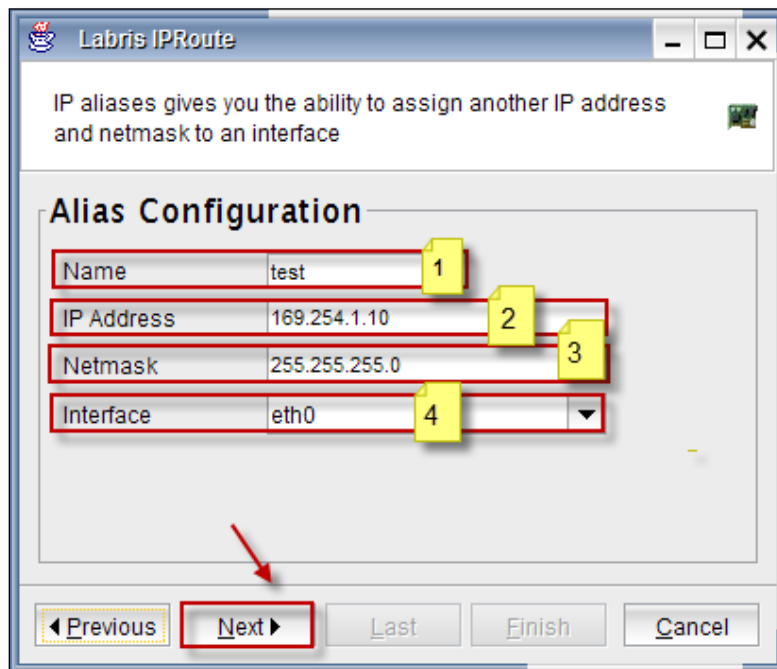
Below screen appears select **IP Configuration**, click on **Add** button.



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



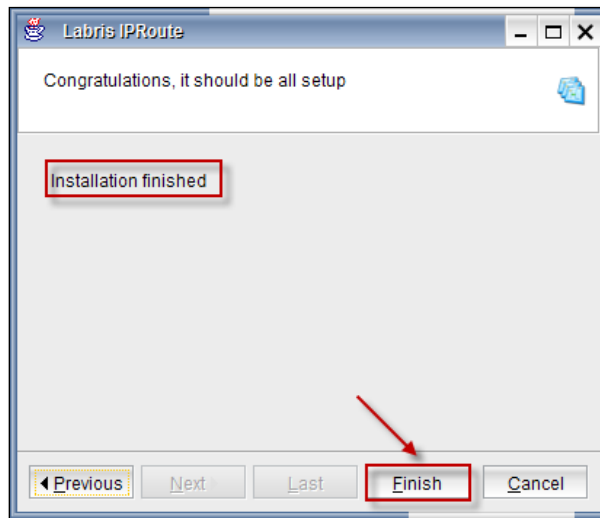
Configuration of the **Alias connection**.



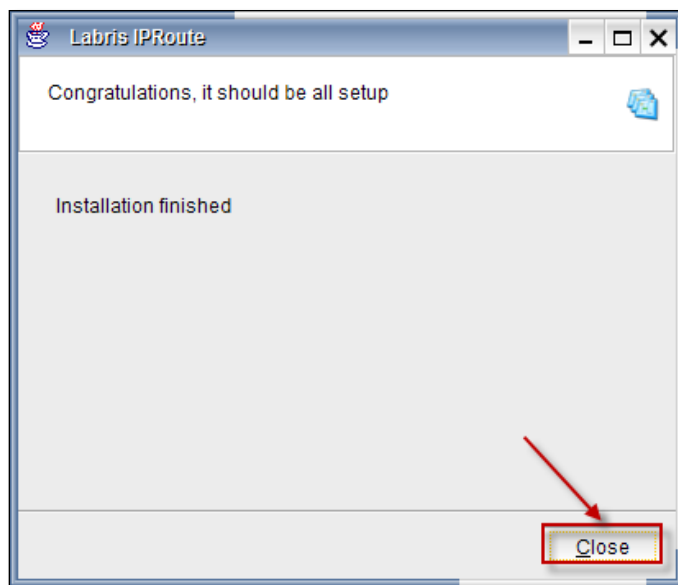
These are the inputs for the Configuration of Interface.

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

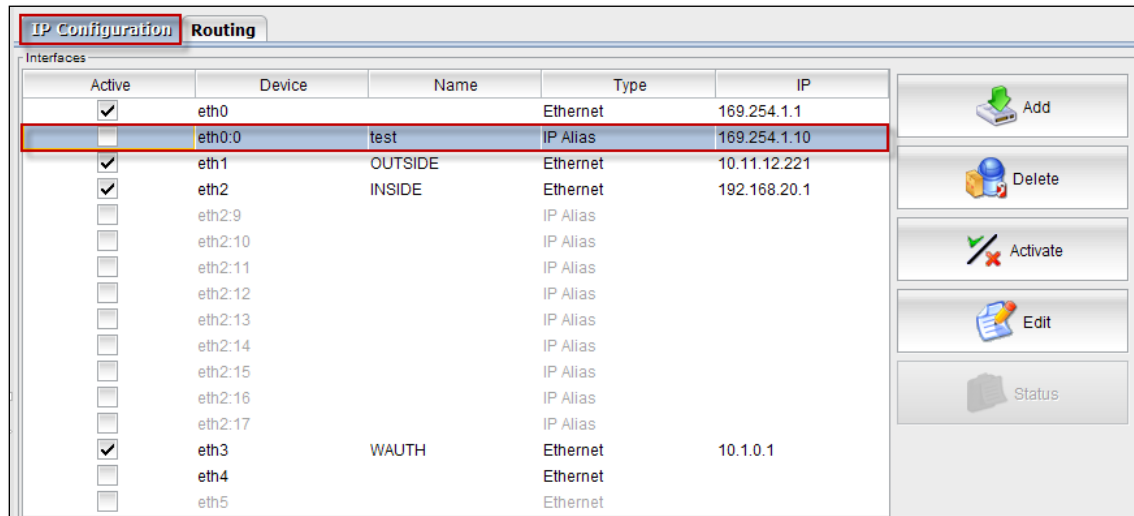
Installation is finished, Click on **Finish** button.



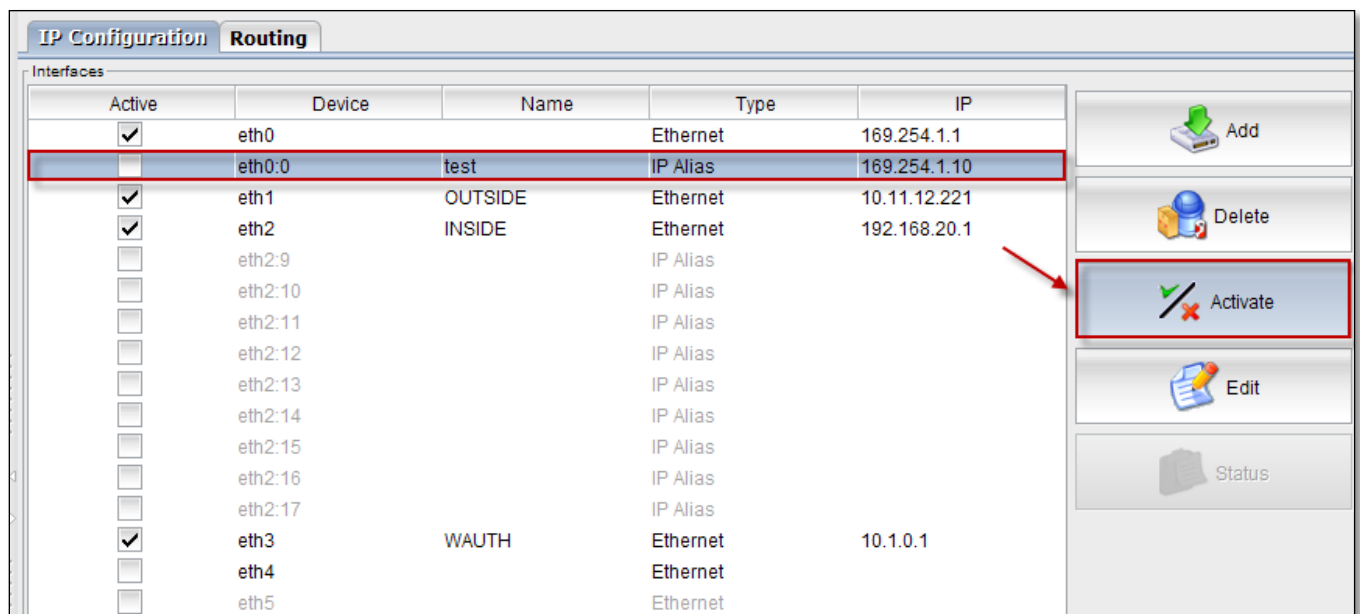
Below screen appears, click on **close** button.



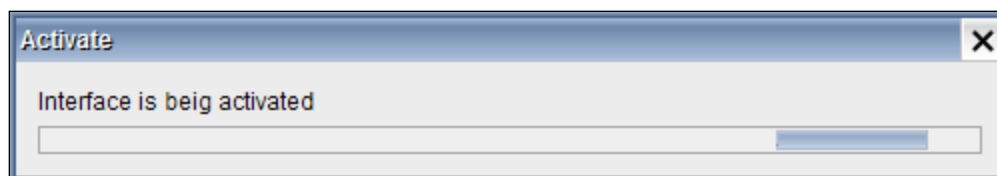
We can notice the New interface added to the Interfaces list with **IP Alias** connection.



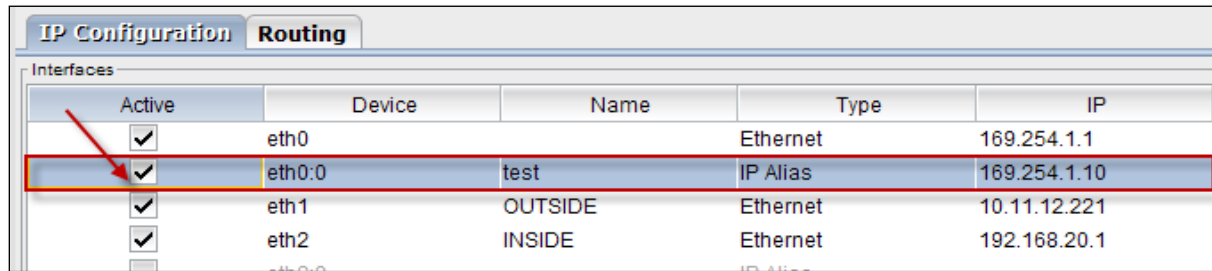
Select the Interface and click on **Activate** button.



Activation process is in progress.



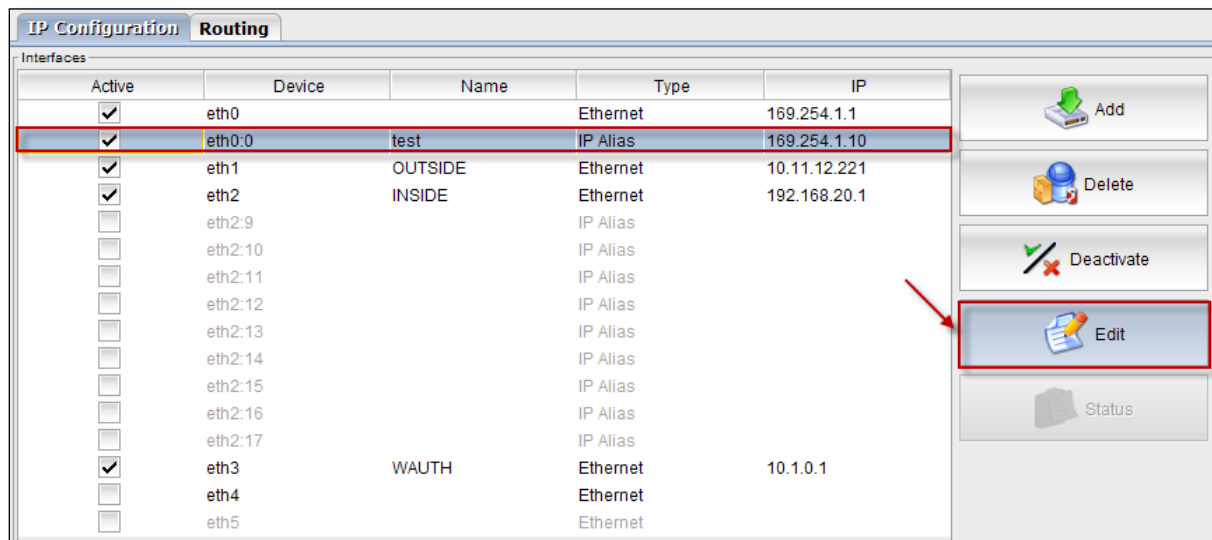
Now we can notice that the newly added Interface is **Active**.



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.

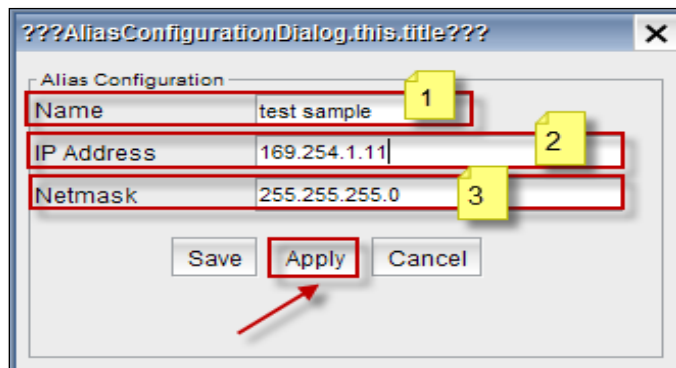


Active	Device	Name	Type	IP
<input checked="" type="checkbox"/>	eth0		Ethernet	169.254.1.1
<input checked="" type="checkbox"/>	eth0:0	test	IP Alias	169.254.1.10
<input checked="" type="checkbox"/>	eth1	OUTSIDE	Ethernet	10.11.12.221
<input checked="" type="checkbox"/>	eth2	INSIDE	Ethernet	192.168.20.1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

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



Alias Configuration

Name: test sample 1

IP Address: 169.254.1.11 2

Netmask: 255.255.255.0 3

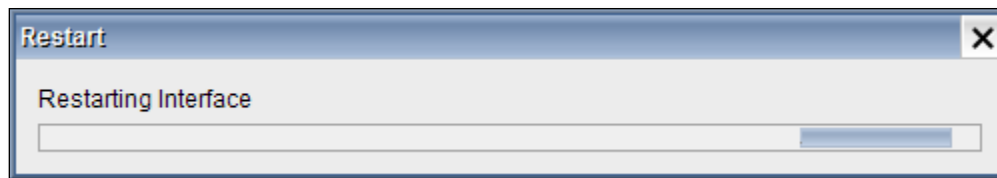
Save Apply Cancel

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.

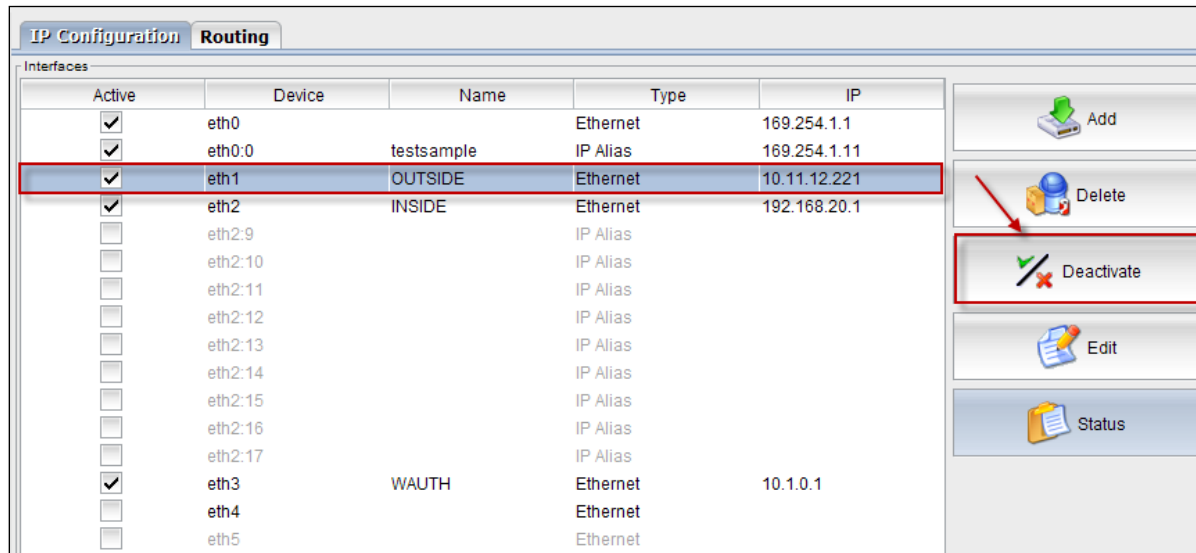


We can notice the changes in the Interface in the **Interfaces** list.

IP Configuration		Routing			
Interfaces					
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		

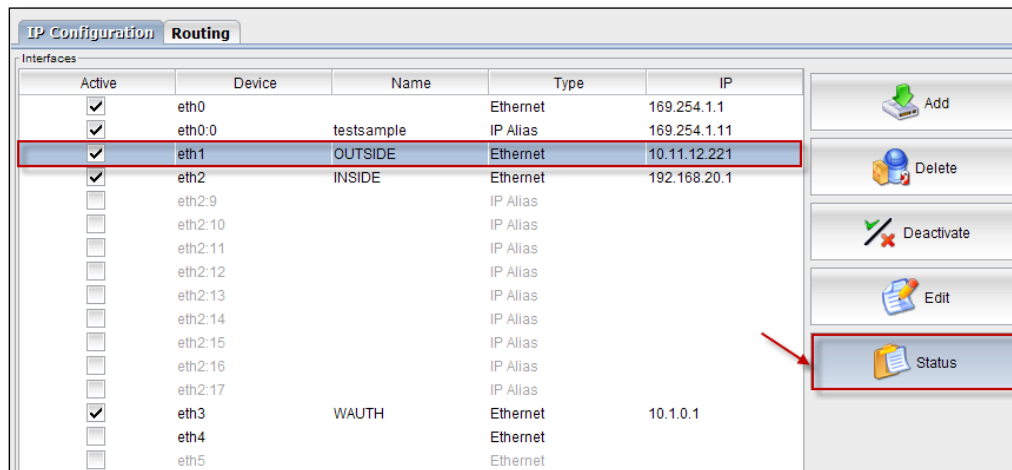
Enable / Disable

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

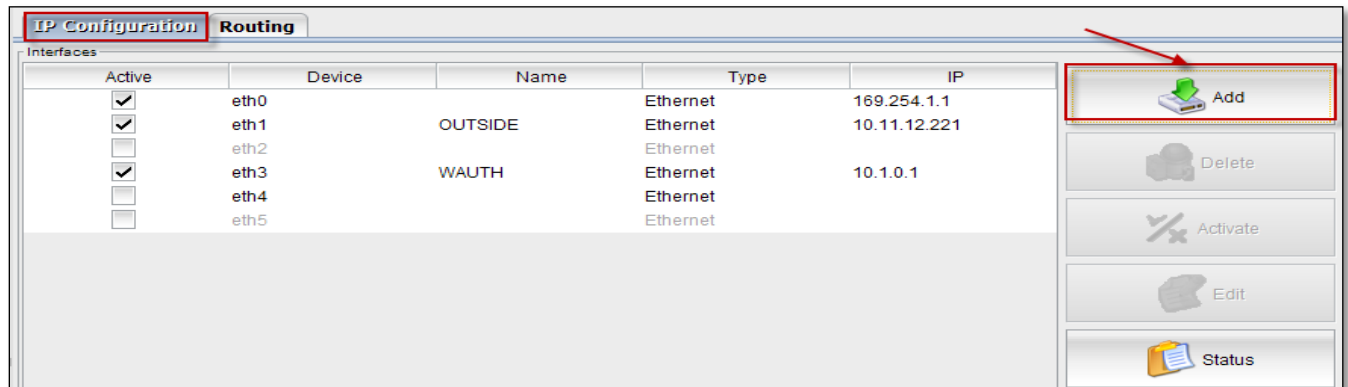
Ethernet Status					
RECIEVED			TRANSMITTED		
Packets	2.04 M	2045867	Packets	971.34 K	971342
Bytes	273.32 MB	286602294	Bytes	445.43 MB	467067233
Error	0		Error	0	
Dropped	244		Dropped	0	
Overruns	0		Overruns	0	
Frame	0		Carrier	0	

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

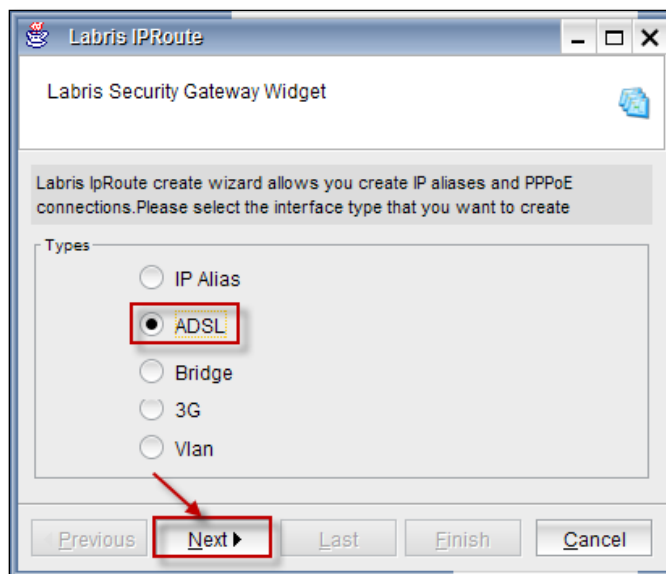
IP Configuration Routing					
Interfaces					
Active	Device	Name	Type	IP	
<input checked="" type="checkbox"/>	eth0		Ethernet	169.254.1.1	
<input checked="" type="checkbox"/>	eth0:0	testsample	IP Alias	169.254.1.11	
<input checked="" type="checkbox"/>	eth1	OUTSIDE	Ethernet	10.11.12.221	
<input checked="" type="checkbox"/>	eth2	INSIDE	Edit	192.168.20.1	
<input type="checkbox"/>	eth2:9		Activate		
<input type="checkbox"/>	eth2:10		Deactivate		
<input type="checkbox"/>	eth2:11		Status		
<input type="checkbox"/>	eth2:12		Delete		
<input type="checkbox"/>	eth2:13		Edit Groups		
<input type="checkbox"/>	eth2:14		Activate Group		
<input type="checkbox"/>	eth2:15		Deactivate Group		
<input type="checkbox"/>	eth2:16				
<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		

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

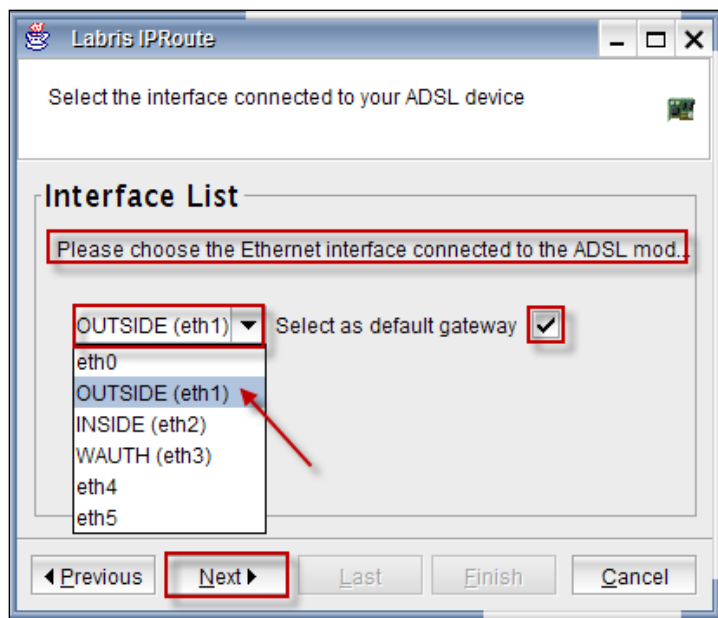
Select **IP Configuration** and click on **Add** button



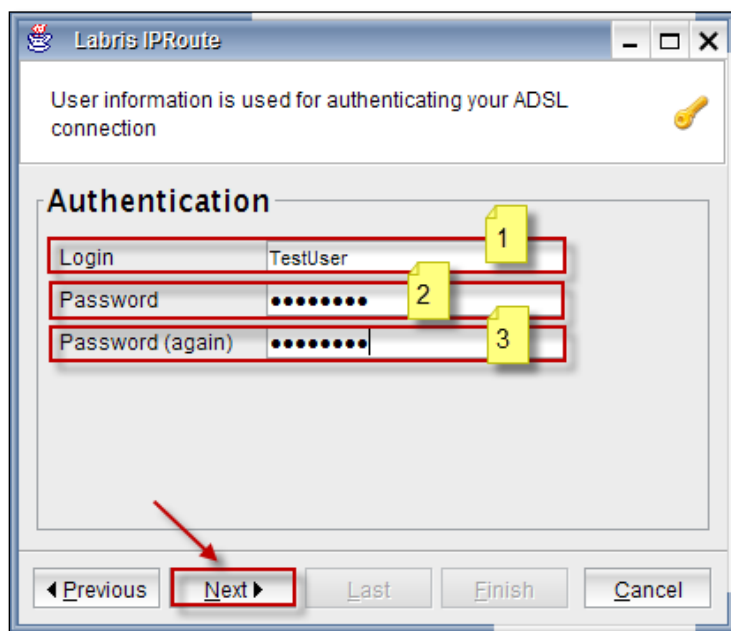
Choose **ADSL** from the types of Interfaces and click on **Next** button to continue.



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

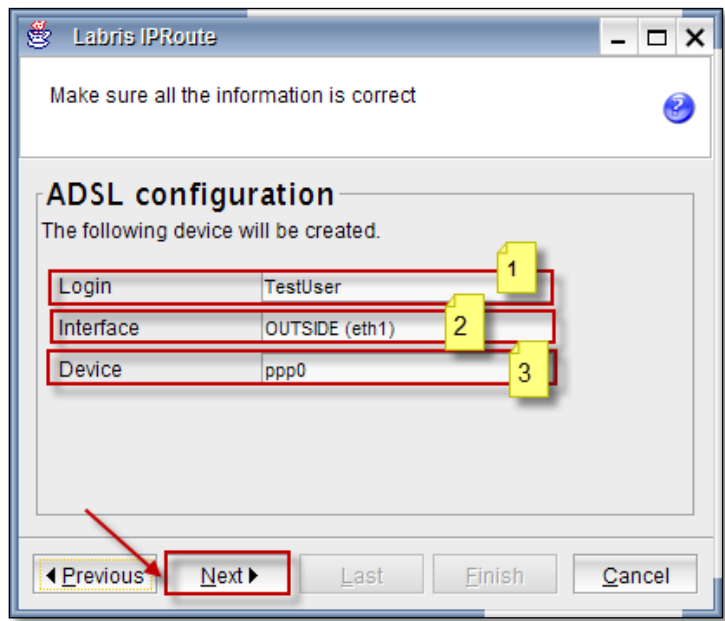


These are the inputs for the User

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

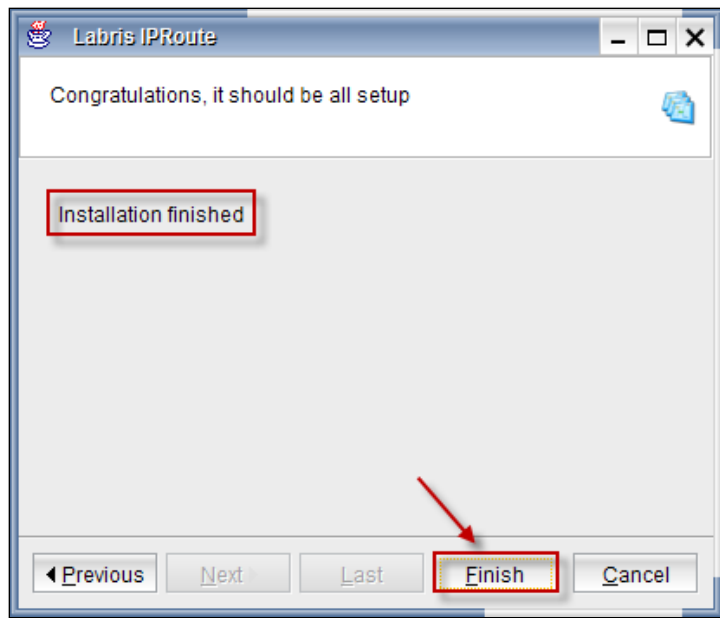
Configuration of ADSL connection.



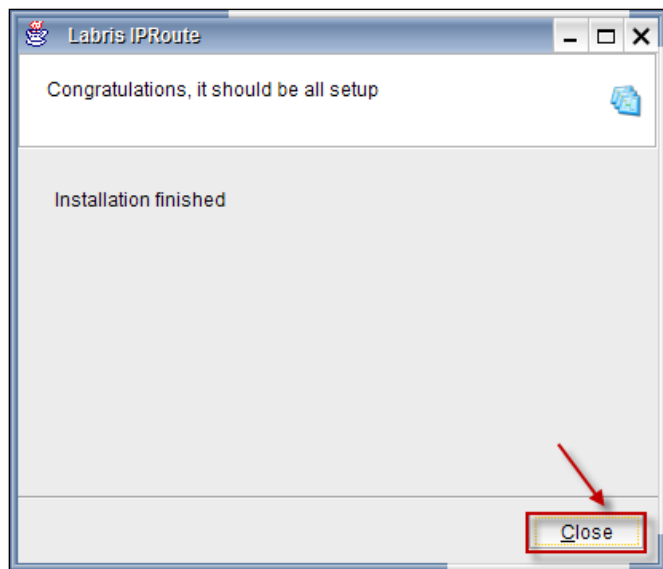
1	Login	It displays Login name of the User
2	Interface	It displays the Interface type
3	Device	It displays device name

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


IP Configuration		Routing			
Interfaces					
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		


IP Configuration


Routing


Interfaces


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	

 Add

 Delete

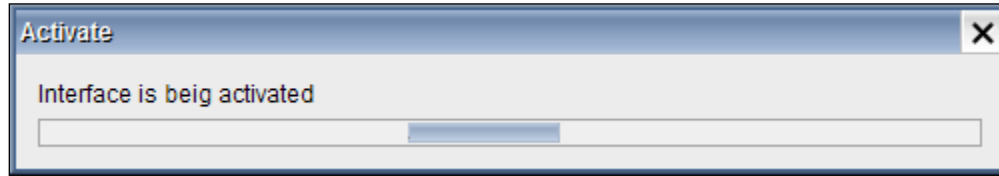
 Activate

 Edit

 Status

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

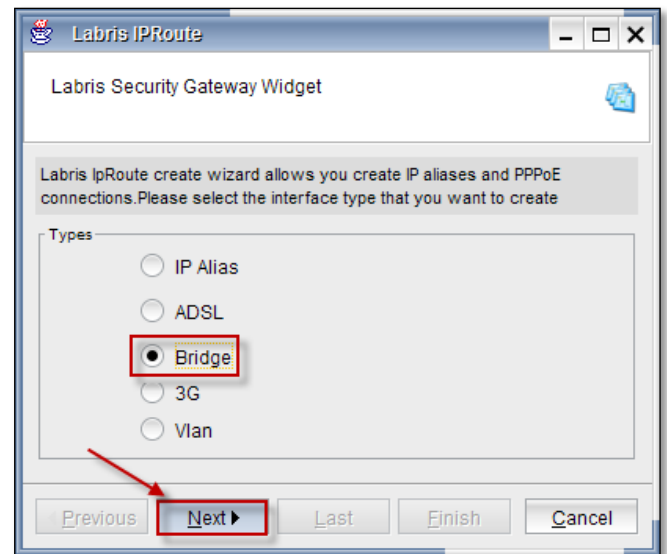
Activation process is in progress



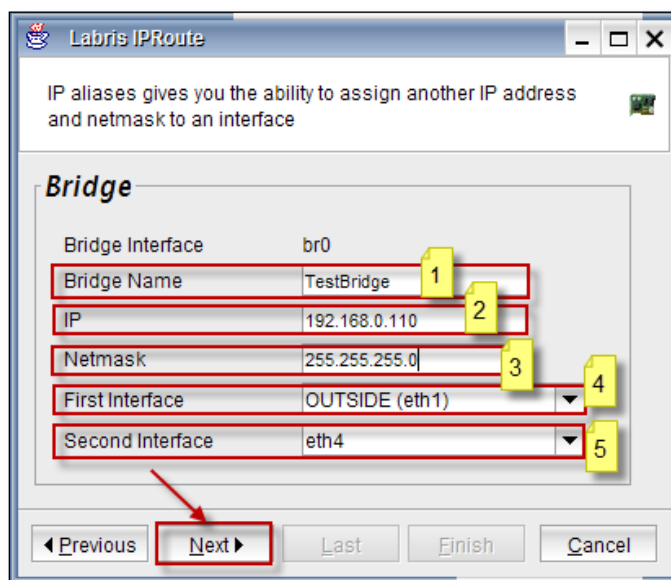
Bridge (Add, Edit, Delete, Status, Enable/disable)

To configure Bridge connection for the Interface.

Select **Bridge radio button** from the types of connection.



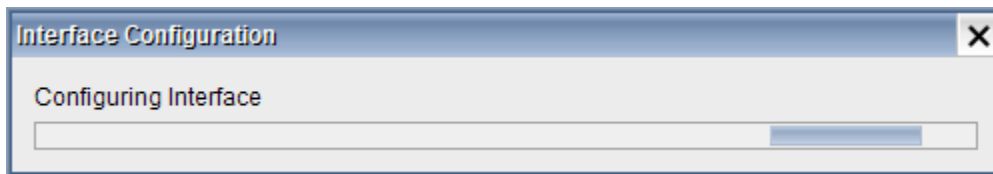
Configuration of Bridge Connection screen.



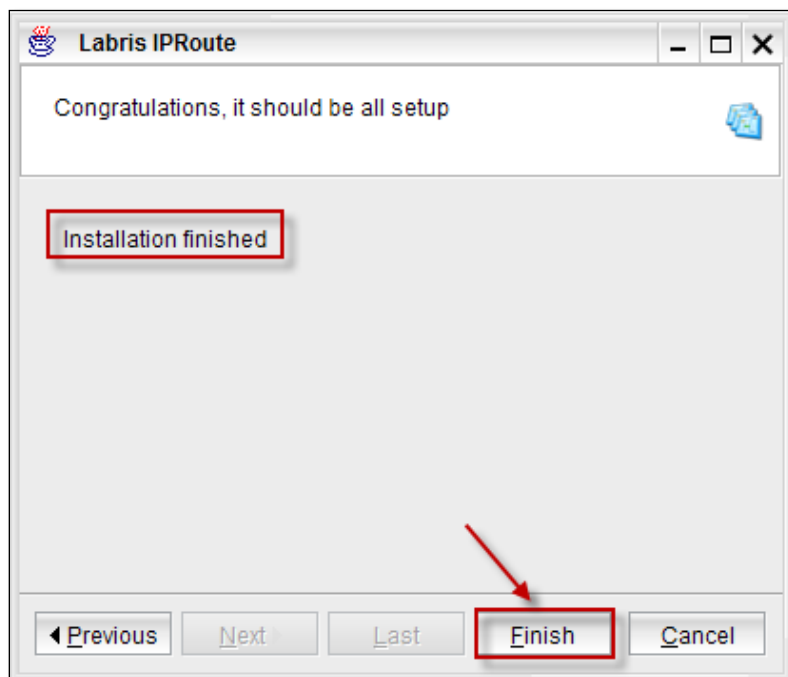
These are the inputs for Bridge connection

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

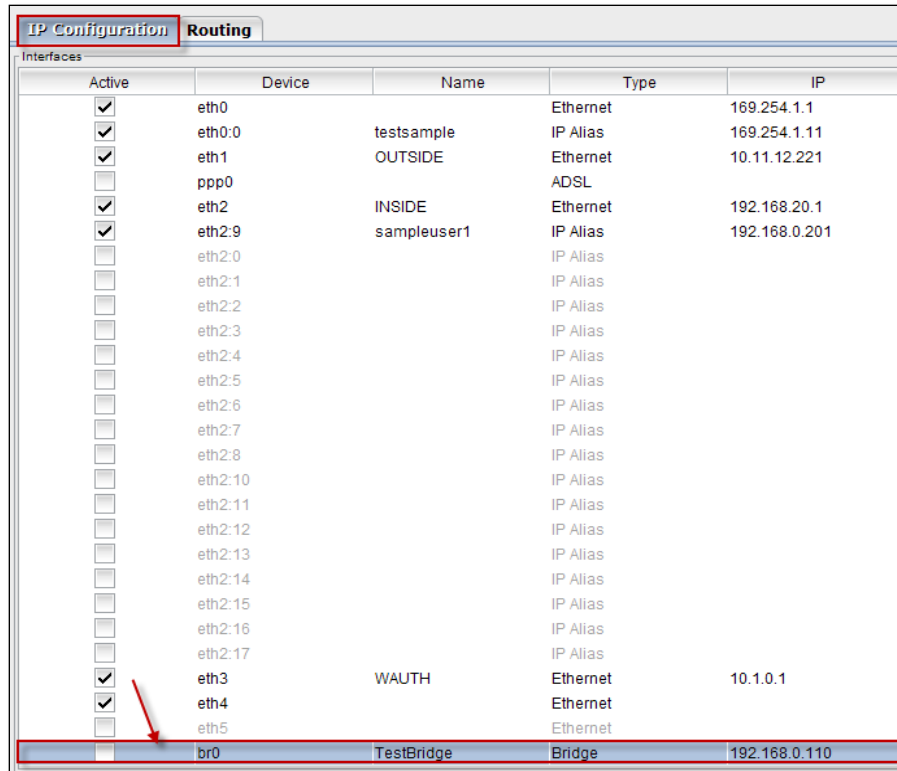
Interface Configuration process is in progress



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

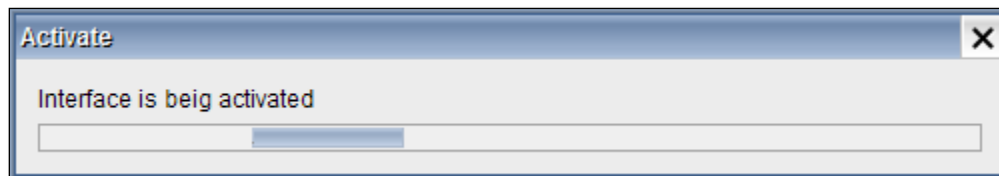


We can notice that the Interface is added in the Interfaces list with **Bridge** type of connection.

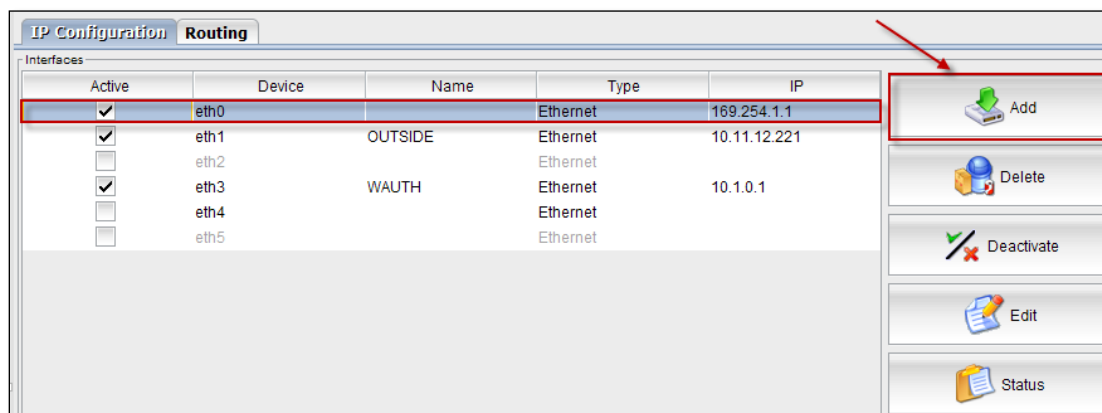


Active	Device	Name	Type	IP
<input checked="" type="checkbox"/>	eth0		Ethernet	169.254.1.1
<input checked="" type="checkbox"/>	eth0:0	testsample	IP Alias	169.254.1.11
<input checked="" type="checkbox"/>	eth1	OUTSIDE	Ethernet	10.11.12.221
<input type="checkbox"/>	ppp0		ADSL	
<input checked="" type="checkbox"/>	eth2	INSIDE	Ethernet	192.168.20.1
<input checked="" type="checkbox"/>	eth2:9	sampleuser1	IP Alias	192.168.0.201
<input type="checkbox"/>	eth2:0		IP Alias	
<input type="checkbox"/>	eth2:1		IP Alias	
<input type="checkbox"/>	eth2:2		IP Alias	
<input type="checkbox"/>	eth2:3		IP Alias	
<input type="checkbox"/>	eth2:4		IP Alias	
<input type="checkbox"/>	eth2:5		IP Alias	
<input type="checkbox"/>	eth2:6		IP Alias	
<input type="checkbox"/>	eth2:7		IP Alias	
<input type="checkbox"/>	eth2:8		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 checked="" type="checkbox"/>	eth4		Ethernet	
<input type="checkbox"/>	eth5		Ethernet	
<input type="checkbox"/>	br0	TestBridge	Bridge	192.168.0.110

Activation process is in progress.



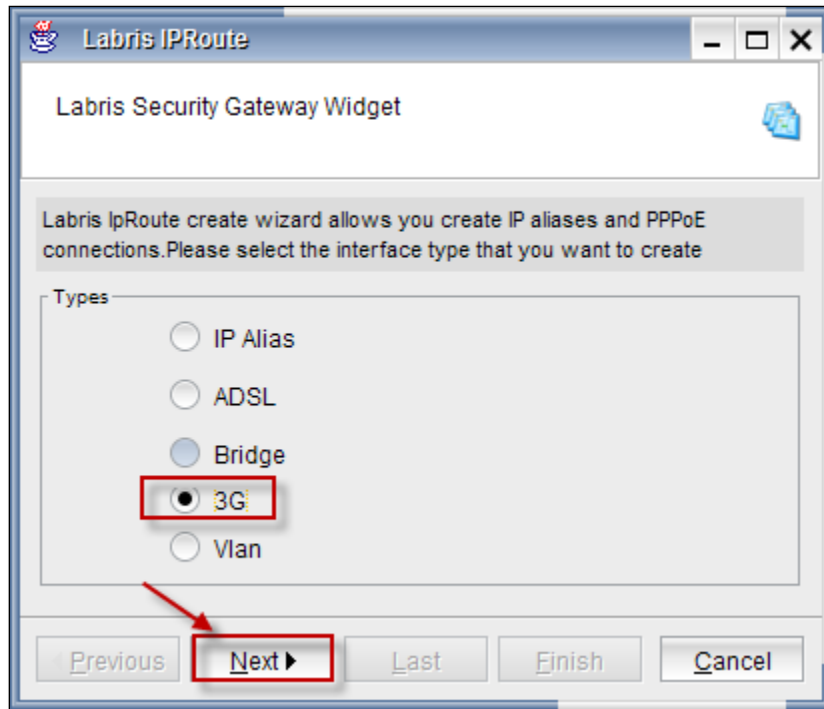
Click on **Add** button to add an interface.



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

To configure 3G connection for the Interface

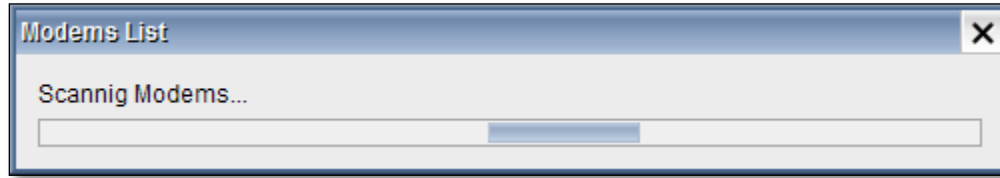
Select **3G** button from the types of connection.



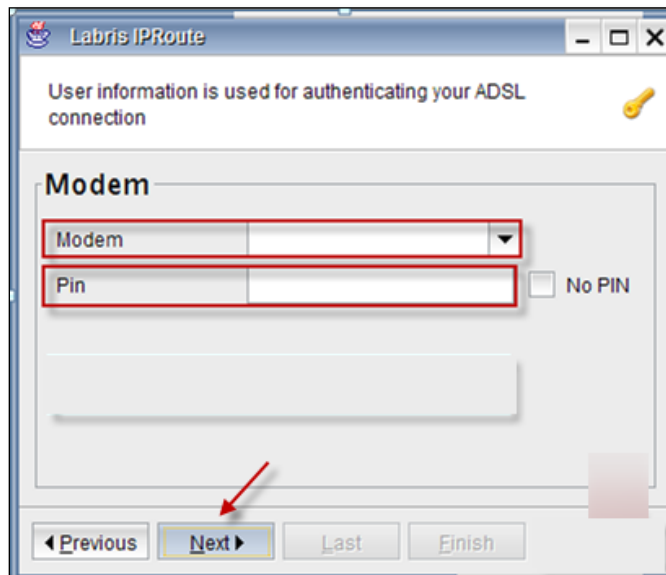
Choose the service provider of the 3G modem from the drop down list, check the default gateway.



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.

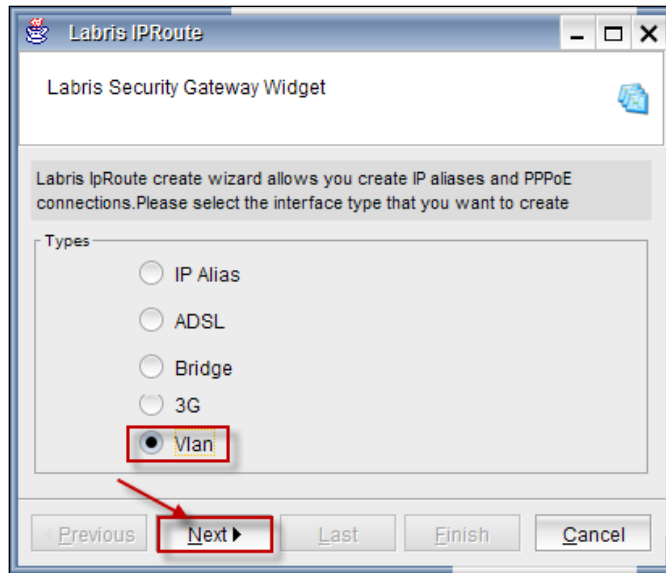
2. **Configuration of new generation 3G modem**

- 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.

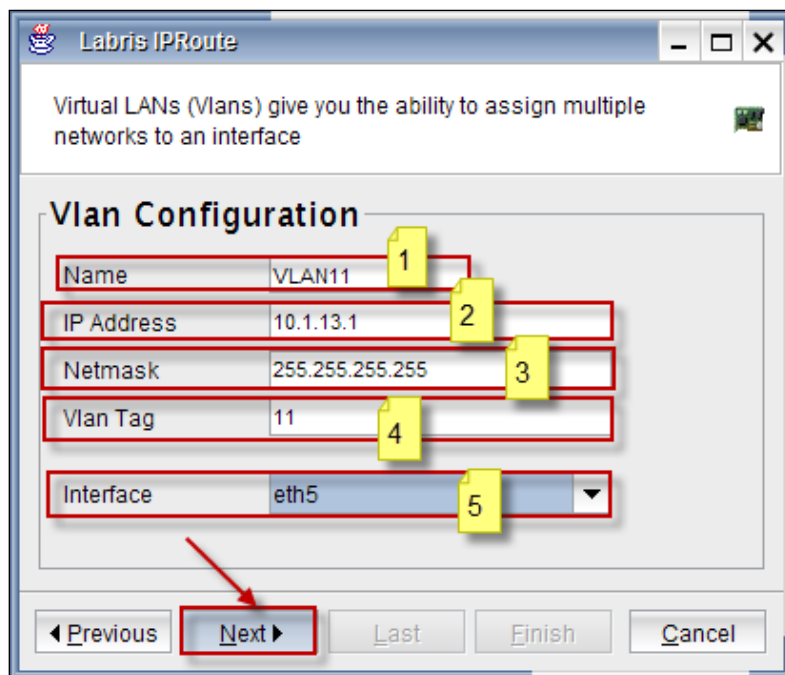
Vlan (Add, Edit, Delete, Status, Enable/disable)

To configure VLAN for the Interface.

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



Configuration of VLAN

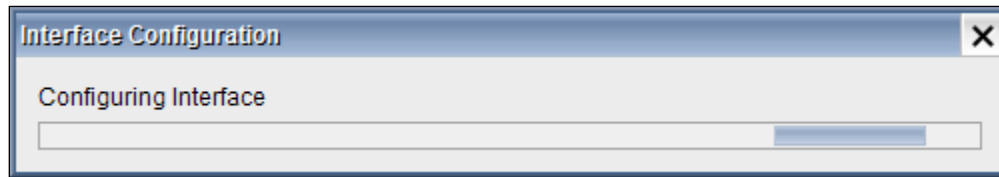


These are inputs for configuration of **VLAN**

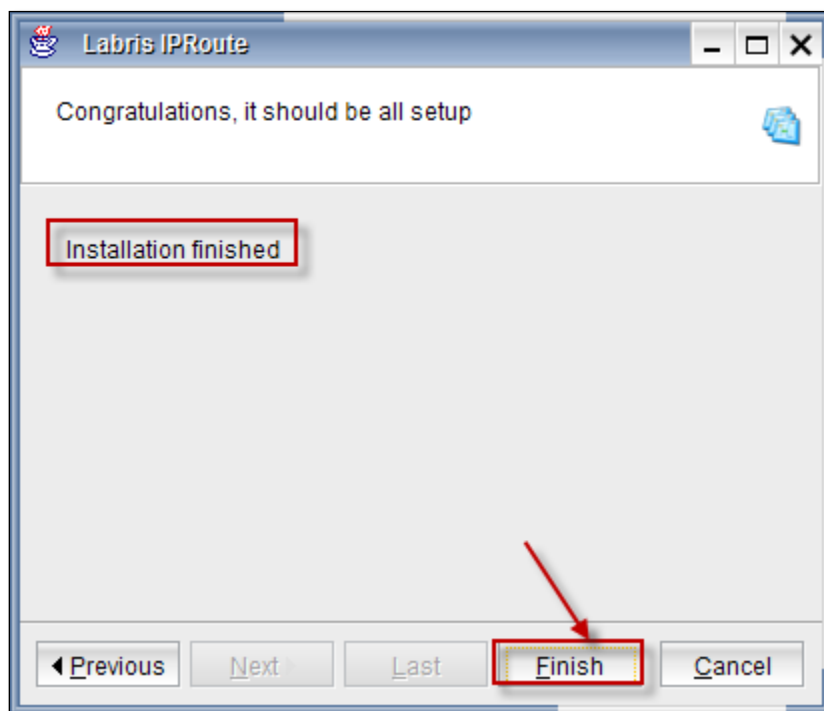
1	Name	Type the Name
2	IP Address	Give the IP Address
3	Netmask	Give the Netmask of the IP Address
4	Vlan Tag	Give the Tag of the Vlan
5	Interface	Choose the Interface from the drop down list

Click on **Next** tab to continue

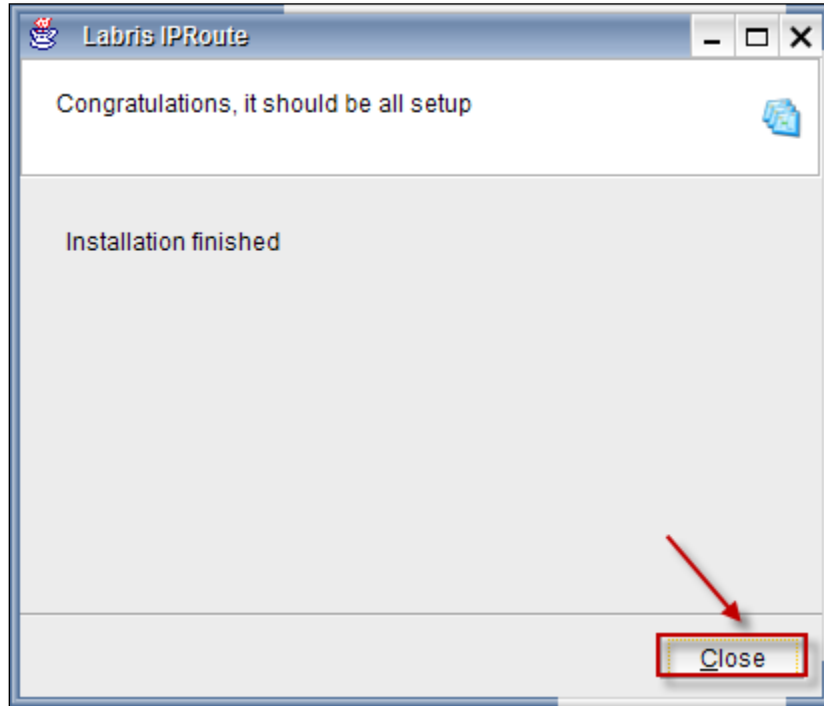
Interface Configuration process is in progress



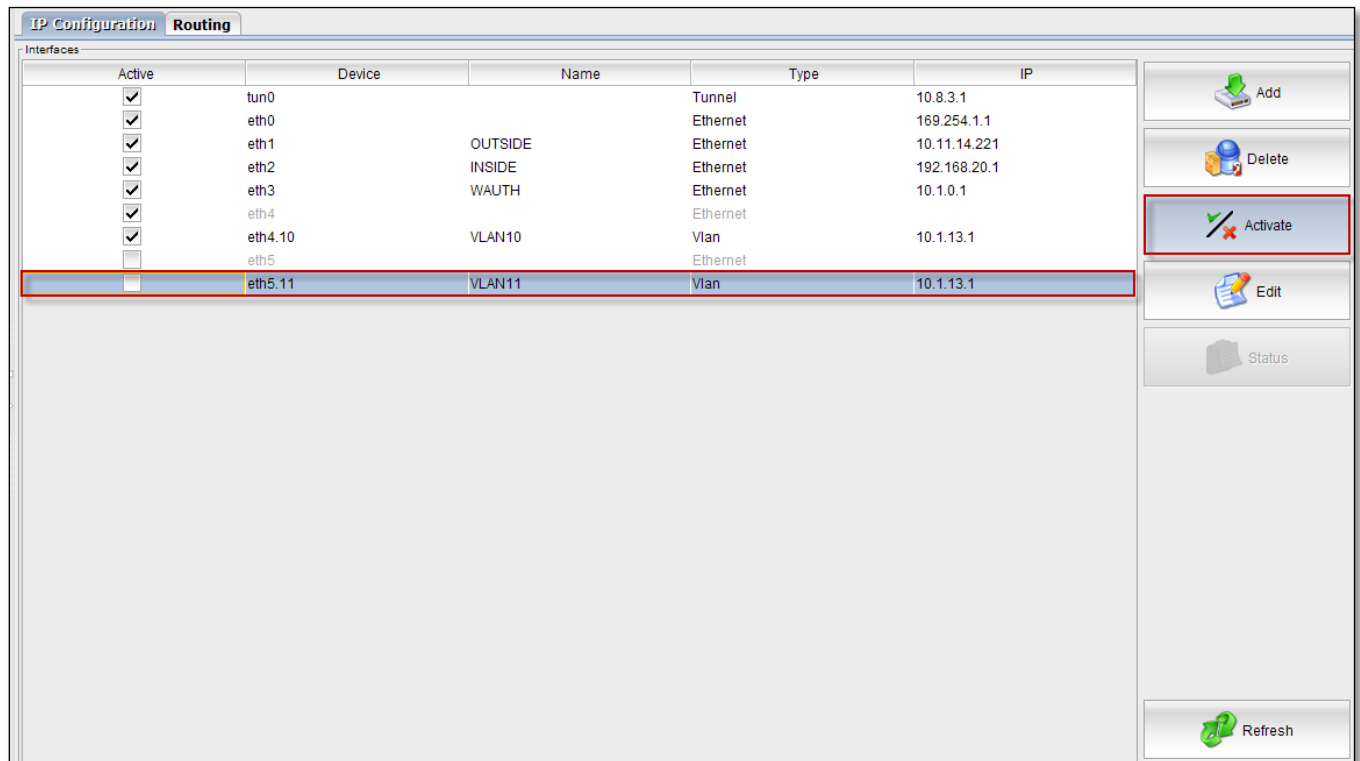
Installation finished click on **Finish** button.



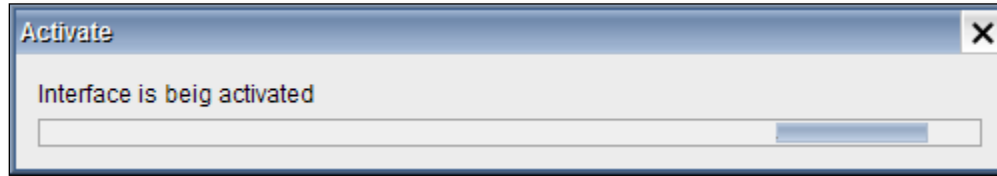
Below screen appears, click on **close** button.



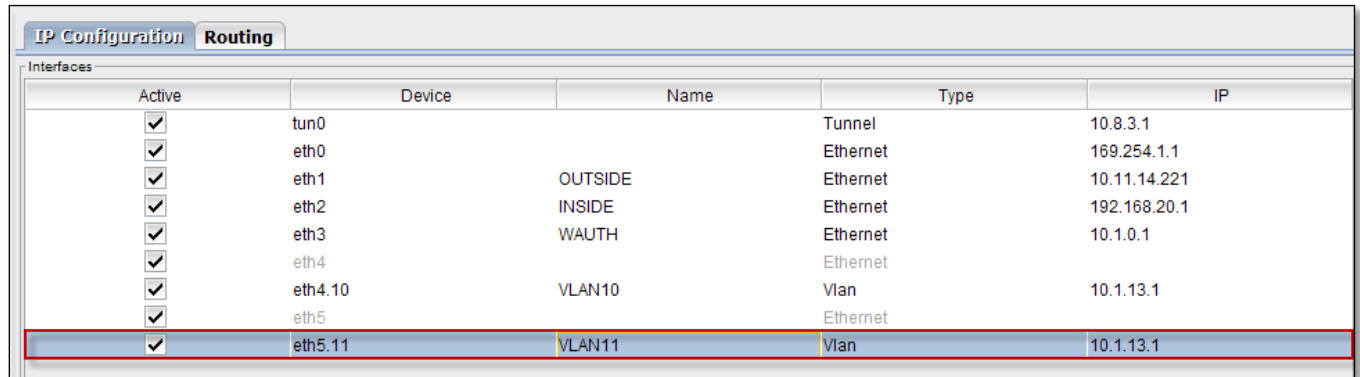
In the below screen we can notice Interface, click on Activate tab to activate the Interface.



Activation process is in progress.



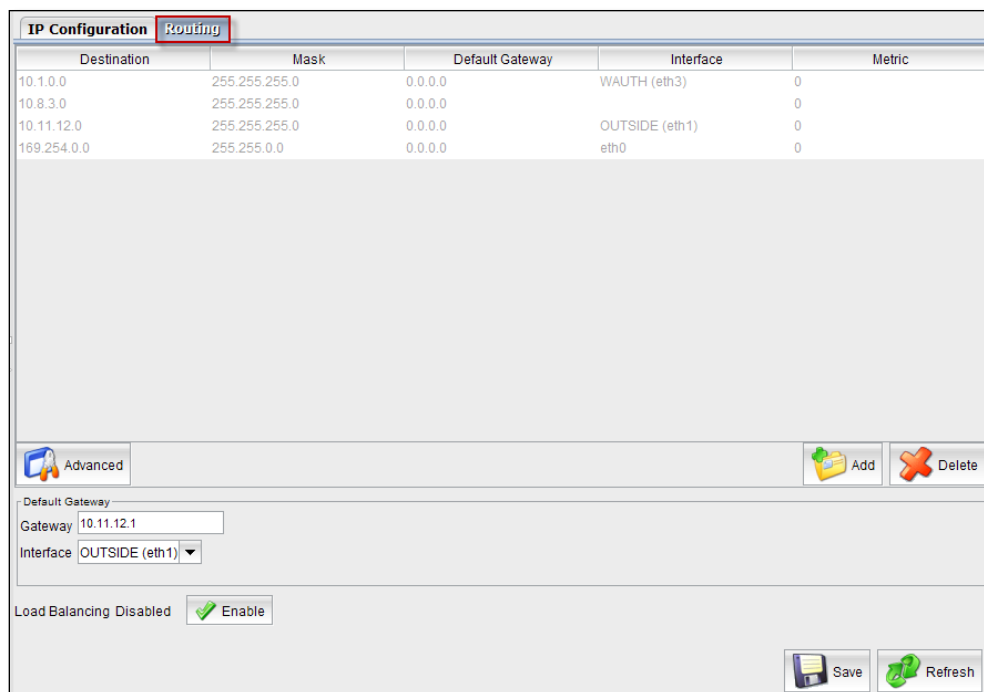
We can notice Interface is Activated in the below screen.



IP Configuration Routing					
Interfaces					
Active	Device	Name	Type	IP	
<input checked="" type="checkbox"/>	tun0		Tunnel	10.8.3.1	
<input checked="" type="checkbox"/>	eth0		Ethernet	169.254.1.1	
<input checked="" type="checkbox"/>	eth1	OUTSIDE	Ethernet	10.11.14.221	
<input checked="" type="checkbox"/>	eth2	INSIDE	Ethernet	192.168.20.1	
<input checked="" type="checkbox"/>	eth3	WAUTH	Ethernet	10.1.0.1	
<input checked="" type="checkbox"/>	eth4		Ethernet		
<input checked="" type="checkbox"/>	eth4.10	VLAN10	Vlan	10.1.13.1	
<input checked="" type="checkbox"/>	eth5		Ethernet		
<input checked="" type="checkbox"/>	eth5.11	VLAN11	Vlan	10.1.13.1	

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.



IP Configuration 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	255.255.255.0	0.0.0.0	eth0	0	

Advanced

AddDelete

Default Gateway
Gateway 10.11.12.1
Interface OUTSIDE (eth1)

Load Balancing Disabled ☒ Enable

SaveRefresh

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: ☒ 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 LOG.

Add (Static Route)

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

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

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

Below screen appears.

The 'Route Add' dialog box contains the following fields and values:

Field	Value
Destination	192.168.0.10
Mask	255.255.255.0
Gateway	192.168.0.1
Device	eth0
Metric	0

The 'Add' button is highlighted with a red arrow.

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

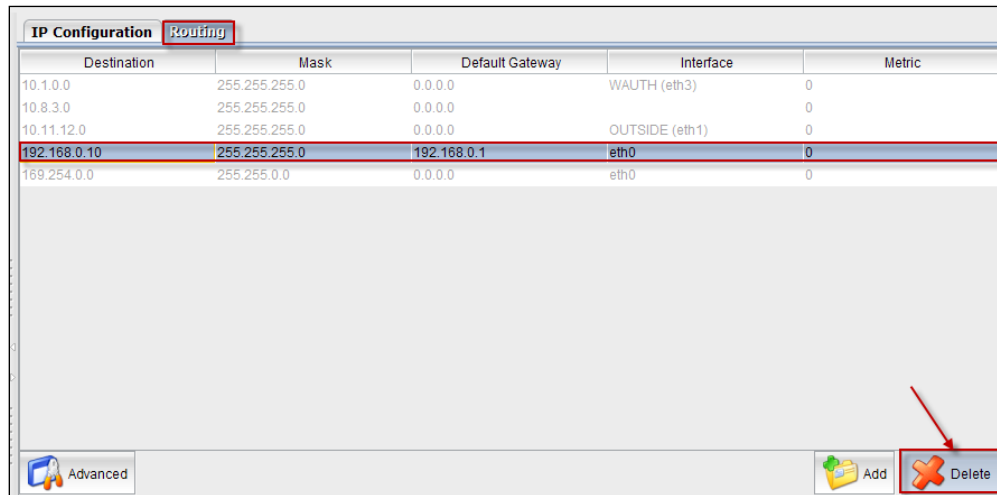
Click on **Add** button.

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

IP Configuration		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
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.

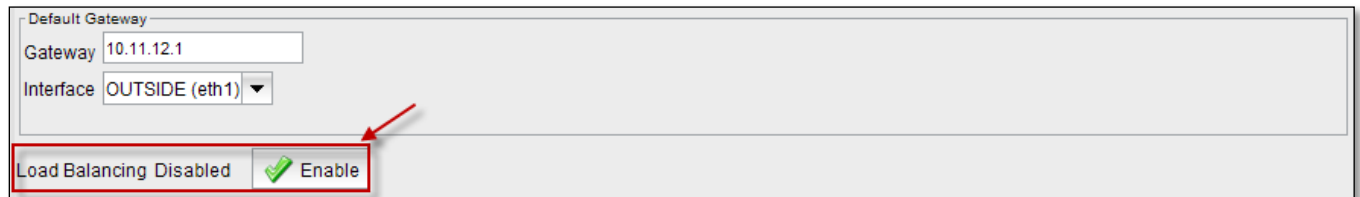


Load Balance

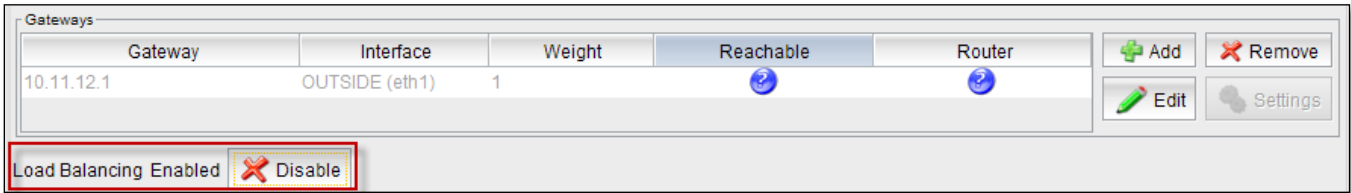
Load balance can be configured based on following types

- 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.

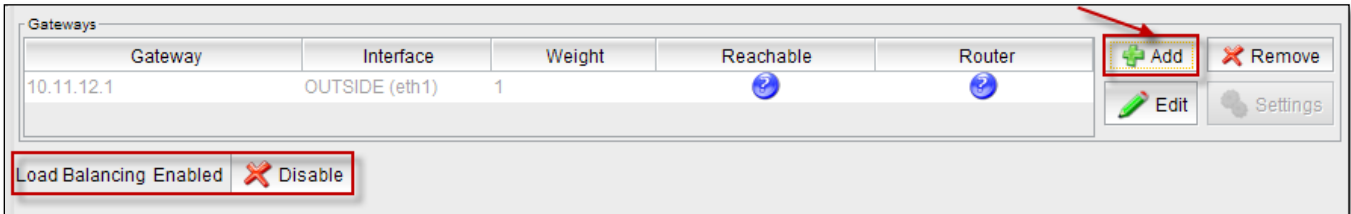


When Load Balance is enabled Gateways section with the fields **Gateway**, **Interface**, **Weight**, **Reachable**, **Router** are seen

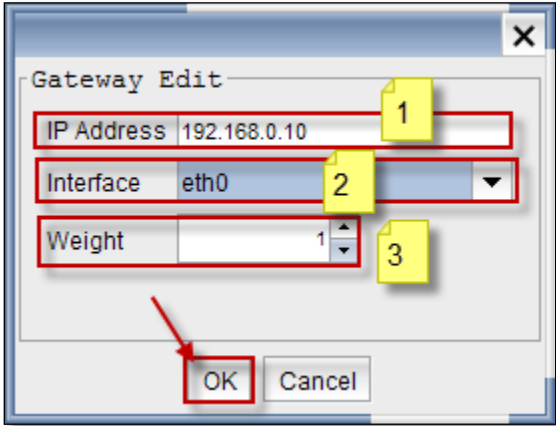


Add (Load Balance Route)

Click on **Add** tab to add Gateway



Below screen appears

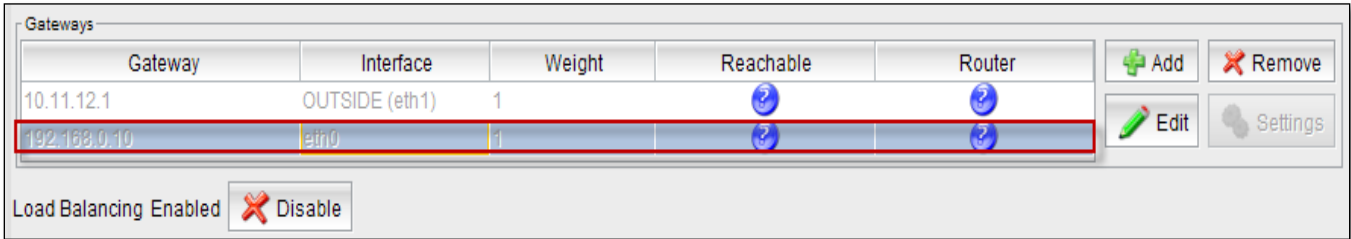


These are the inputs to add Gateway.

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

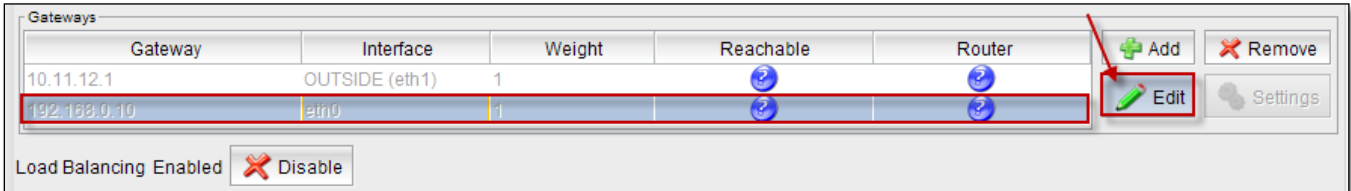
Click **Ok** to add Gateway

We can notice Gateway added in the below screen

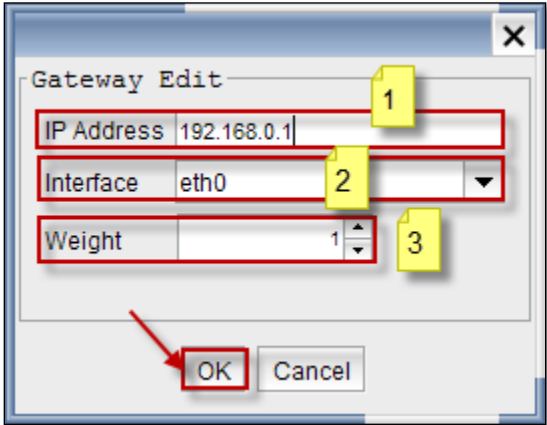


Edit (Load Balance Route)

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



Below screen appears



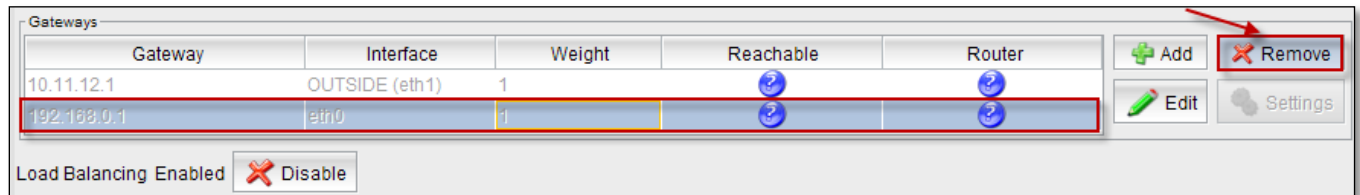
These are the inputs to edit gateway

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)

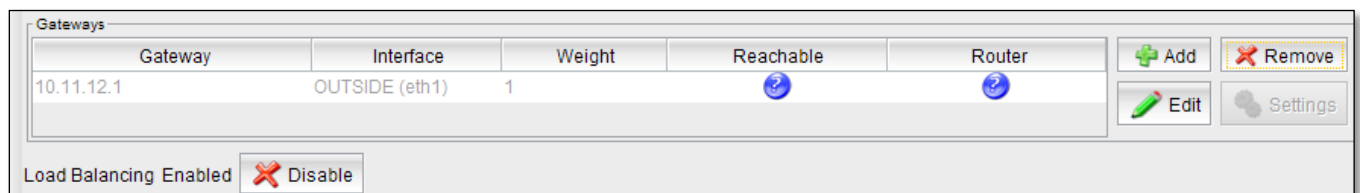
Click **Ok** to apply changes

Delete (Load Balance Route)

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

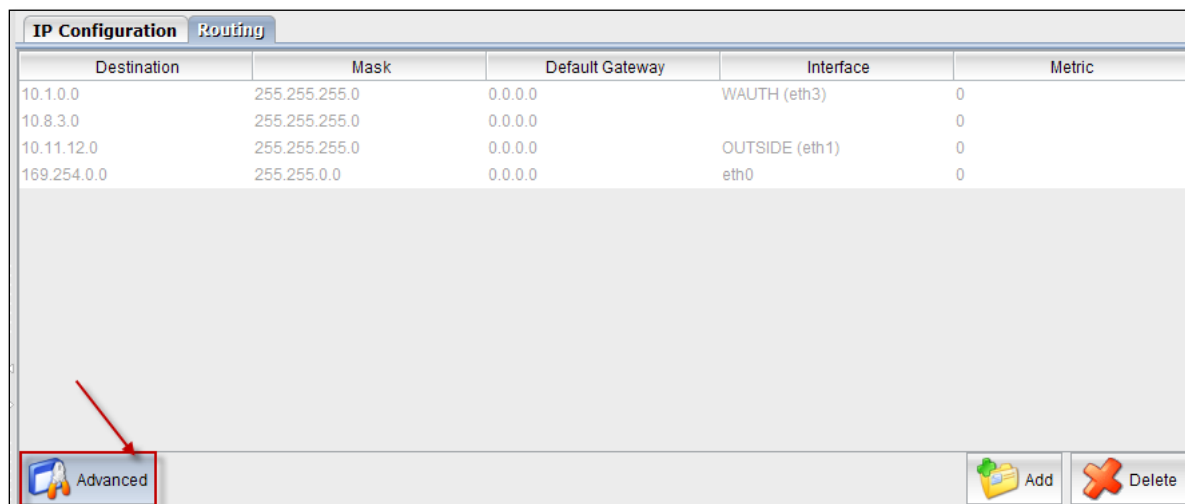


We can notice **Gateway** removed from the list in the below screen



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.

The 'Advanced Routing Table' window contains two main sections:

- Link Configuration:** A table with columns 'Link Name', 'Gateway', and 'Interface'. It contains one entry: 'main' with gateway '10.11.12.1' and interface 'eth1'. To the right are 'Add' and 'Remove' buttons.
- Decision Table:** A table with columns 'Source', 'Destination', and 'Link'. It is currently empty. To the right are 'Add', 'Remove', 'Up', and 'Down' buttons.

At the bottom are 'Save', 'Refresh', and 'Cancel' buttons.

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.

This image shows a close-up of the 'Link Configuration' section. The table has columns 'Link Name', 'Gateway', and 'Interface'. The first row shows 'main', '10.11.12.1', and 'eth1'. The 'Add' button (with a green plus icon) is highlighted with a red box and a red arrow pointing to it. The 'Remove' button is also visible.

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

The 'Link Edit' dialog box is used to create or edit a link. It contains the following fields:

- Link Name:** 'Testlink' (highlighted with a red box and labeled 1).
- Default Gateway:** '192.168.0.1' (highlighted with a red box and labeled 2).
- Interface:** 'eth0' (highlighted with a red box and labeled 3).

At the bottom are 'add' and 'cancel' buttons. A red arrow points to the 'add' button.

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

Link Name	Gateway	Interface
main	10.11.12.1	eth1
Testlink	192.168.0.1	eth0

Buttons: + Add, - Remove

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

Source	Destination	Link
--------	-------------	------

Buttons: + Add, - Remove, Up, Down

Below screen appears

Decision Add

Decision
Please type an ip address or select a user or group

From salih 1 Add User or Group

To testgroup1768 2 Add User or Group

Link main (10.11.12.1) 3

Add Cancel

(OR)

Decision Add

Decision
Please type an ip address or select a user or group

From 192.168.20.0/24 Add User or Group

To 0.0.0.0 Add User or Group

Link Testlink (192.168.0.1)

Add Cancel

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

Decision Table

Source	Destination	Link
salih	testgroup1768	main

+

Add

✖

Remove

▲

Up

▼

Down

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

Advanced Routing Table

Links Configuration

Link Name	Gateway	Interface
main	10.11.12.1	eth1
Testlink	192.168.0.1	eth0

+

Add

✖

Remove

Decision Table

Source	Destination	Link
salih	testgroup1768	main

+

Add

✖

Remove

▲

Up

▼

Down

Save

↻

Refresh

✖

Cancel

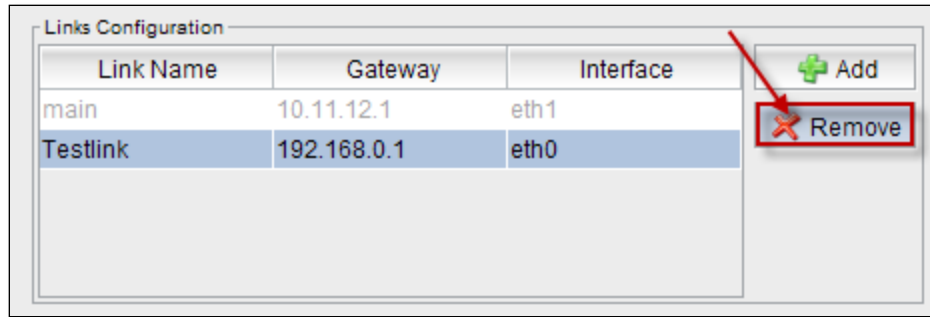
1	Save	It enables us to Save changes made to the Advanced Routing Table
2	Refresh	It enables us to Refresh Advanced Routing Table
3	Cancel	It enables us to Cancel and close the tab

Saving and Applying Links and Decisions is in progress.

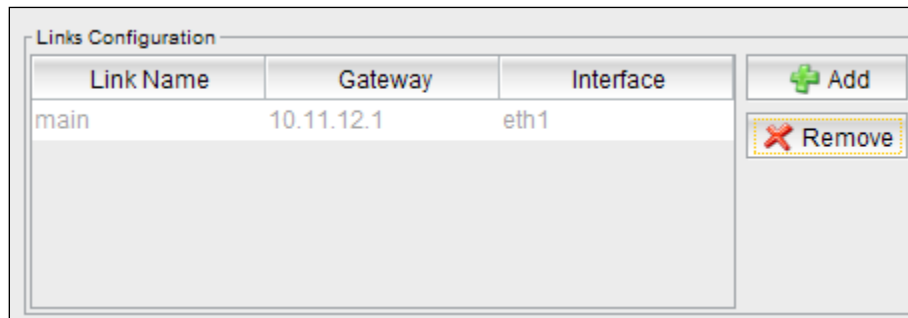
Advanced Routing

Saving and Applying Links and Decisions

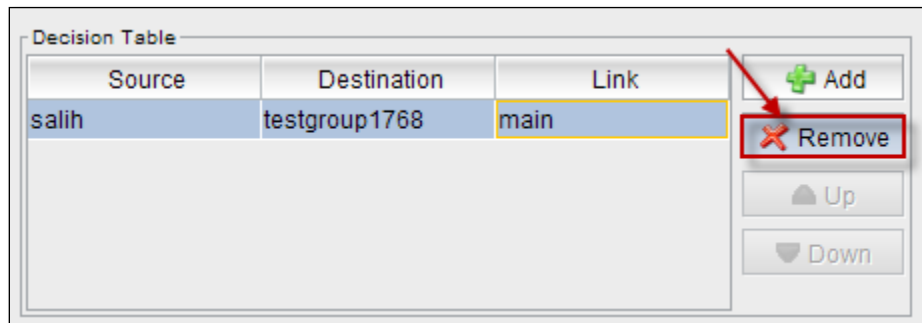
Select the **Link** and click on **Remove** tab to remove **Link** from **Link Configuration**.



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**.

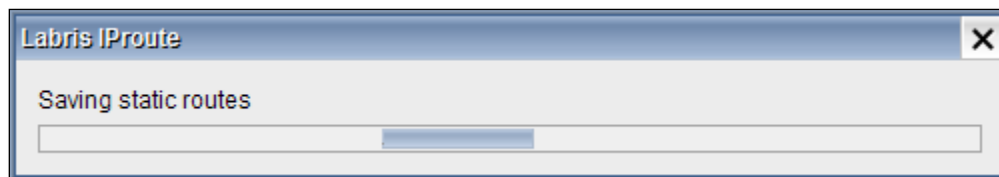
Destination	Mask	Default Gateway	Interface	Metric
10.1.0.0	255.255.255.0	0.0.0.0	WAUTH (eth3)	0
10.8.3.0	255.255.255.0	0.0.0.0		0
10.11.12.0	255.255.255.0	0.0.0.0	OUTSIDE (eth1)	0
169.254.0.0	255.255.0.0	0.0.0.0	eth0	0

Gateway	Interface	Weight	Reachable	Router
10.11.12.1	OUTSIDE (eth1)	1		

Load Balancing Enabled ☒ Disable

Save Refresh

Saving process is in progress



WAN Load Balancing

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

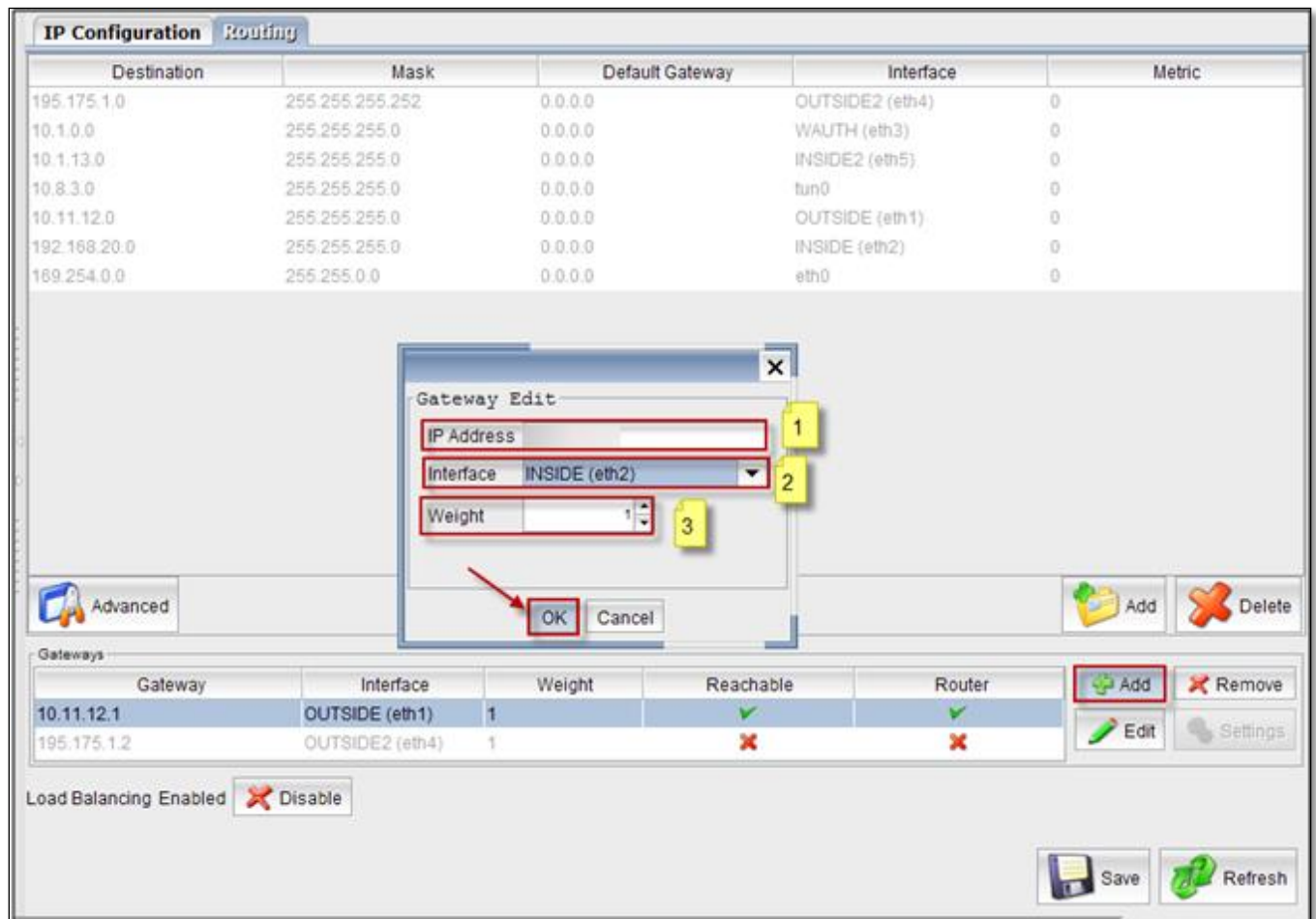
In the below screen we can notice **Load Balance Enabled**

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

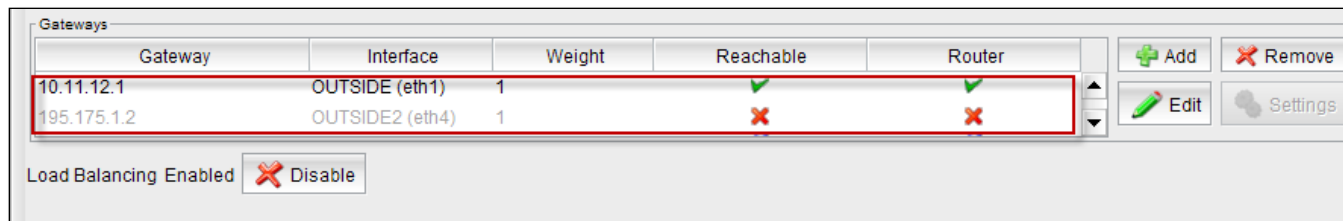


These are the inputs for the Gateway Edit.

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.



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

Load Balancing Enabled ☒ Disable

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 Gateway: 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 gw 20.20.20.1 \
```

#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
```

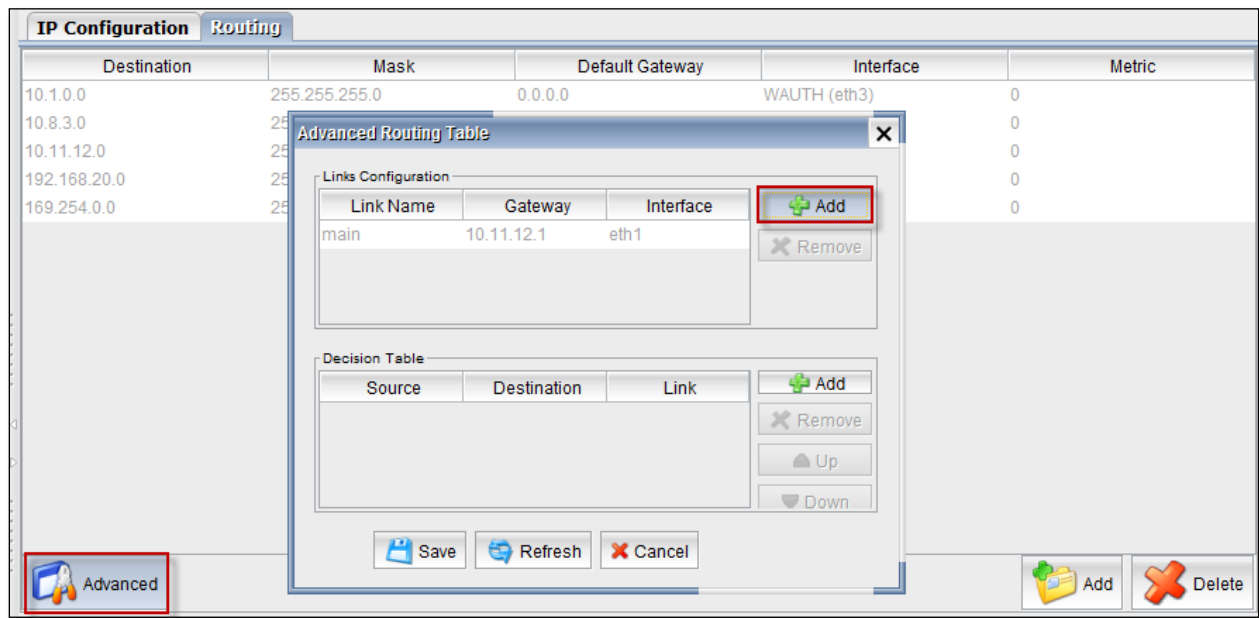
#It's finished

Step 2:

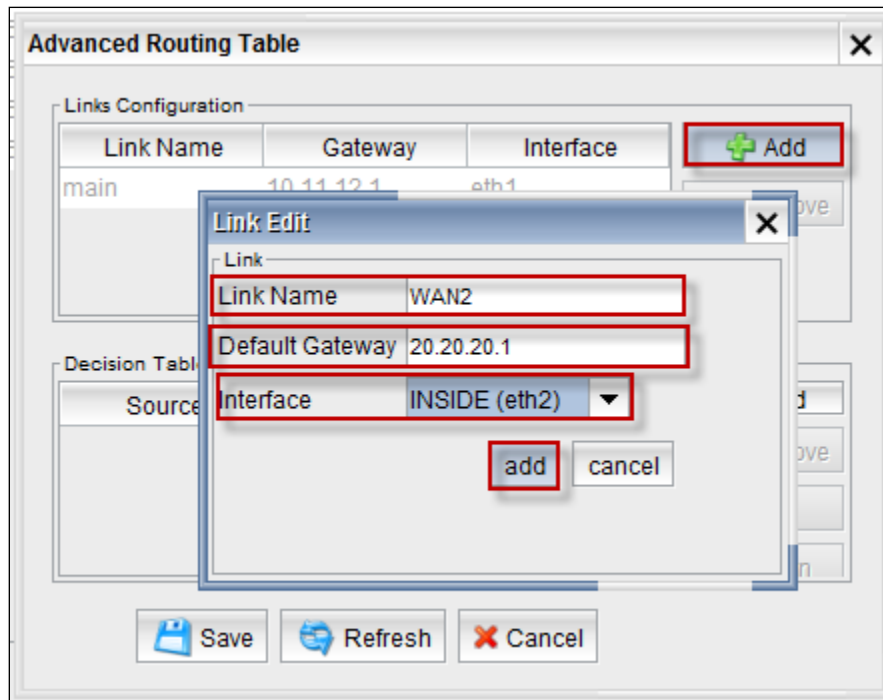
Add Advance routing on the new gateway for wan2.

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.

Advanced Routing Table

Links Configuration

Link Name	Gateway	Interface
main	10.11.12.1	eth1
WAN2	20.20.20.1	eth2

Decision Table

Source	Destination	Link
--------	-------------	------

Buttons: Add, Remove, Up, Down, Save, Refresh, Cancel

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.

Advanced Routing Table

Links Configuration

Decision Add

Decision

Please type an ip address or select a user or group

From

To

Link

Down

Save Refresh Cancel

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

Advanced Routing Table

Links Configuration

Link Name	Gateway	Interface
main	10.11.12.1	eth1
WAN2	20.20.20.1	eth2

Decision Table

Source	Destination	Link
10.0.0.0/24	all	WAN2

Up Down

Save Refresh Cancel

Log Settings

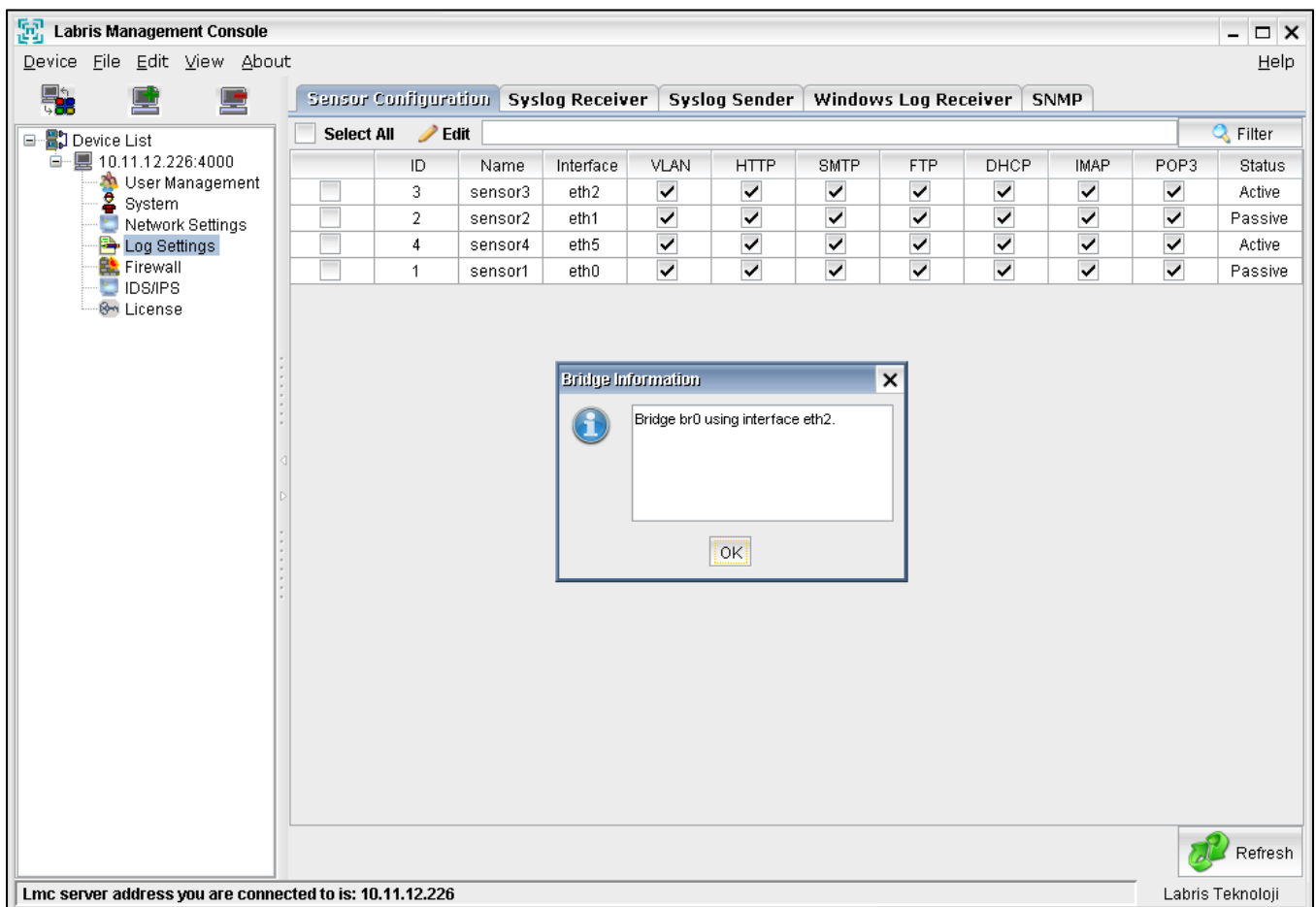
In this module Sensor settings, Syslog, Windows logs and SNMP configurations can be made. Your servers' or network devices' logs are collected on Labris LOG and signed with TurkTrust Time stamp.

Sensor Configuration

Every ethernet on Labris LOG can be configured separately as a sensor.

The desired sensors can be made active or passive via the Sensor Configuration tab in the Log Settings module.

Sensors start running as soon as logs are received on bridge or mirror mode.



The screenshot displays the Labris Management Console interface. On the left, a 'Device List' sidebar shows a tree structure with 'Log Settings' selected. The main window has tabs for 'Sensor Configuration', 'Syslog Receiver', 'Syslog Sender', 'Windows Log Receiver', and 'SNMP'. The 'Sensor Configuration' tab is active, showing a table of sensors. A 'Bridge Information' dialog box is open in the center, displaying the message 'Bridge br0 using interface eth2.' with an 'OK' button. The status bar at the bottom indicates the Lmc server address is 10.11.12.226 and the Labris Teknoloji logo is on the right.

	ID	Name	Interface	VLAN	HTTP	SMTP	FTP	DHCP	IMAP	POP3	Status
<input type="checkbox"/>	3	sensor3	eth2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Active
<input type="checkbox"/>	2	sensor2	eth1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Passive
<input type="checkbox"/>	4	sensor4	eth5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Active
<input type="checkbox"/>	1	sensor1	eth0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Passive

Every single sensor has been designed to sniff 6 different protocols. It can be chosen various protocols on each sensor.

VLAN option can be enabled if there is a VLAN configuration on the network, which its traffic will be listened. There is no restriction to leave it open.

Edit Sensor

☒ Active

Mode *

Standard

Sensor Name *

sensor3

Interface *

eth2

VLAN(802.1Q) *☒

Log Options

☒ HTTP

Records URL addresses.

☒ FTP

Records FTP connections.

☒ DHCP

Records the distribution of the internal network ip addresses.

☒ SMTP

Records E-mail transfers.

☒ POP3

Records E-mail intakes.

☒ IMAP

Records E-mail intakes.

OK

Cancel

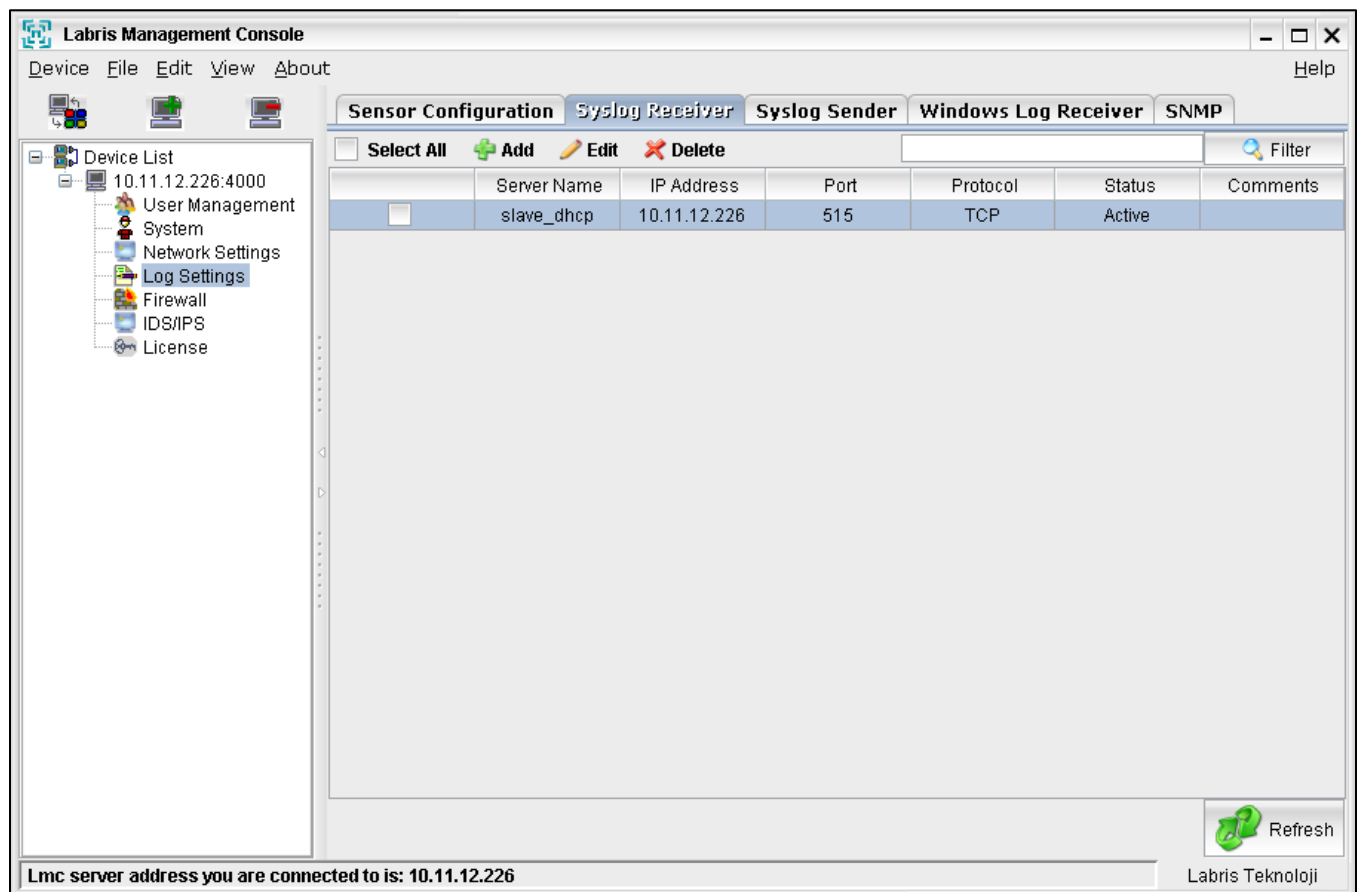
1	Active	Sensor can be set as active / passive.
2	Mode	Standard. Variant options will be available by future.

3	Sensor Name	Name to define regarding sensor.
4	Interface	Interface which is sensor works on it.
5	VLAN (802.1Q)	It can sniff logs on networks, which are VLAN tagged.
6	Log Options	It defines what kind of protocols' logs will be sniffed. Supported protocols: HTTP, FTP, DHCP, SMTP, POP3, IMAP

Syslog Receiver

Logs that formatted as Syslog can be easily recorded by defining Log sender devices via this menu.

Click add button to add new record. It is chosen a name to define the server, an IP address and a port where logs will be sent from. A configuration file is created by given server name and it can be monitored on the monitoring view with that name.



1	Select ALL	All pre-defined configurations can be chosen.
2	Add	It is used to add a new definition.
3	Edit	It is used to edit pre-defined configuration.
4	Delete	It is used to delete pre-defined configuration.
5	Comment	Description field.

Edit Server

☒ Active

Server Name *

IP Address *

Default Port: 514 Protocol: TCP and UDP

Port/Protocol *

Comment

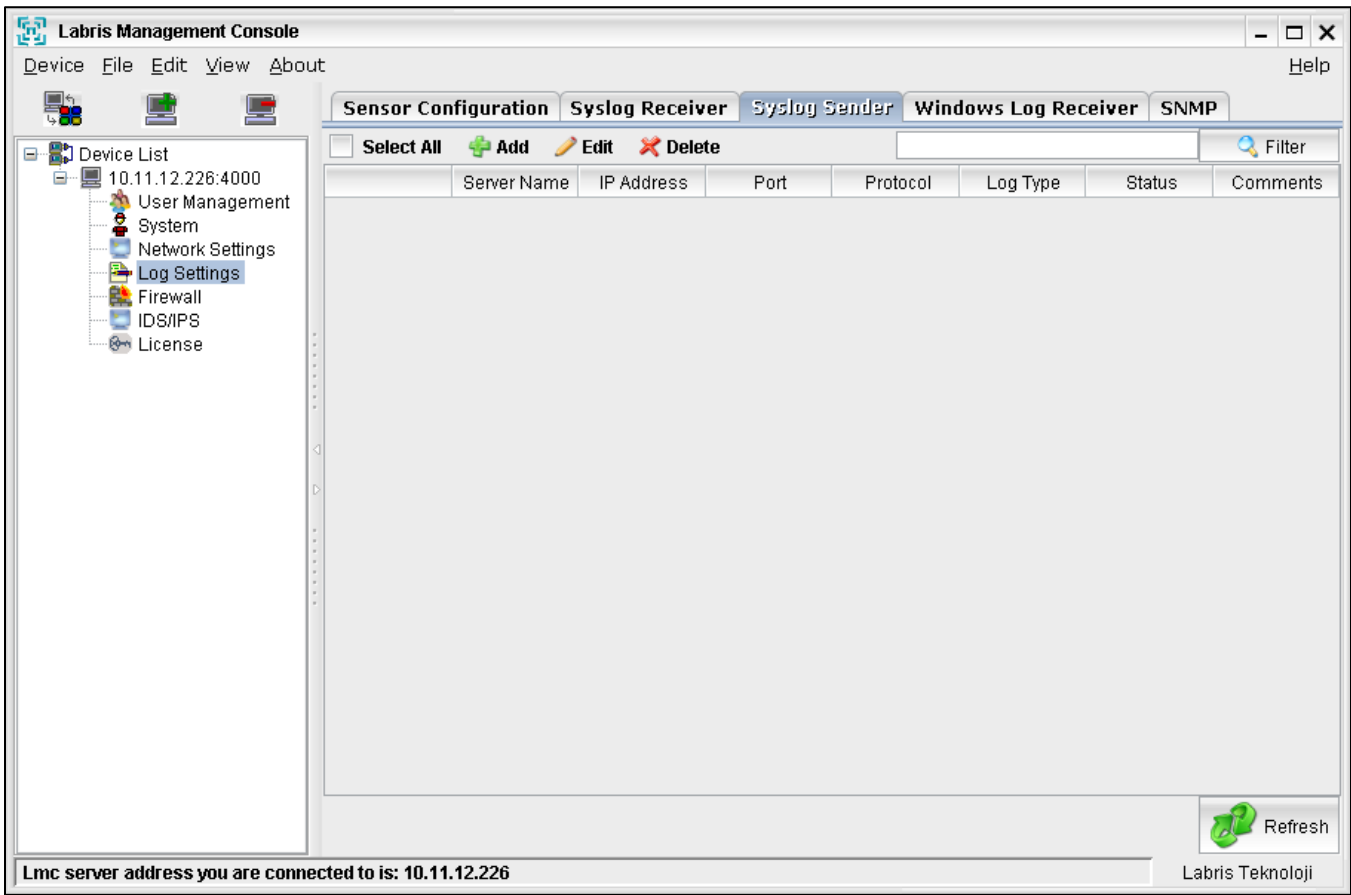
1	Active	Previously defined configurations can be active / passive.
2	Server Name	A name to define the Syslog resource of regarding sensor. Also the configuration file is created with this name.
3	IP Address	IP address of the server which sends logs via Syslog.
4	Port/Protocol	It is used to define which port/protocols will be used to send logs to Labris Log appliance.
5	Comment	Description field.

Syslog Sender

Labris Log appliance can send logs which, retrieved from different sources by different ways, to external log collector devices over Log Sender in Syslog format.

Logs which are sent from the field to the record type that will be sent to the requested records are selected.

Descriptions will be sent to the server is made. All records can be sent if requested. Added later in the records are automatically sent to the server.

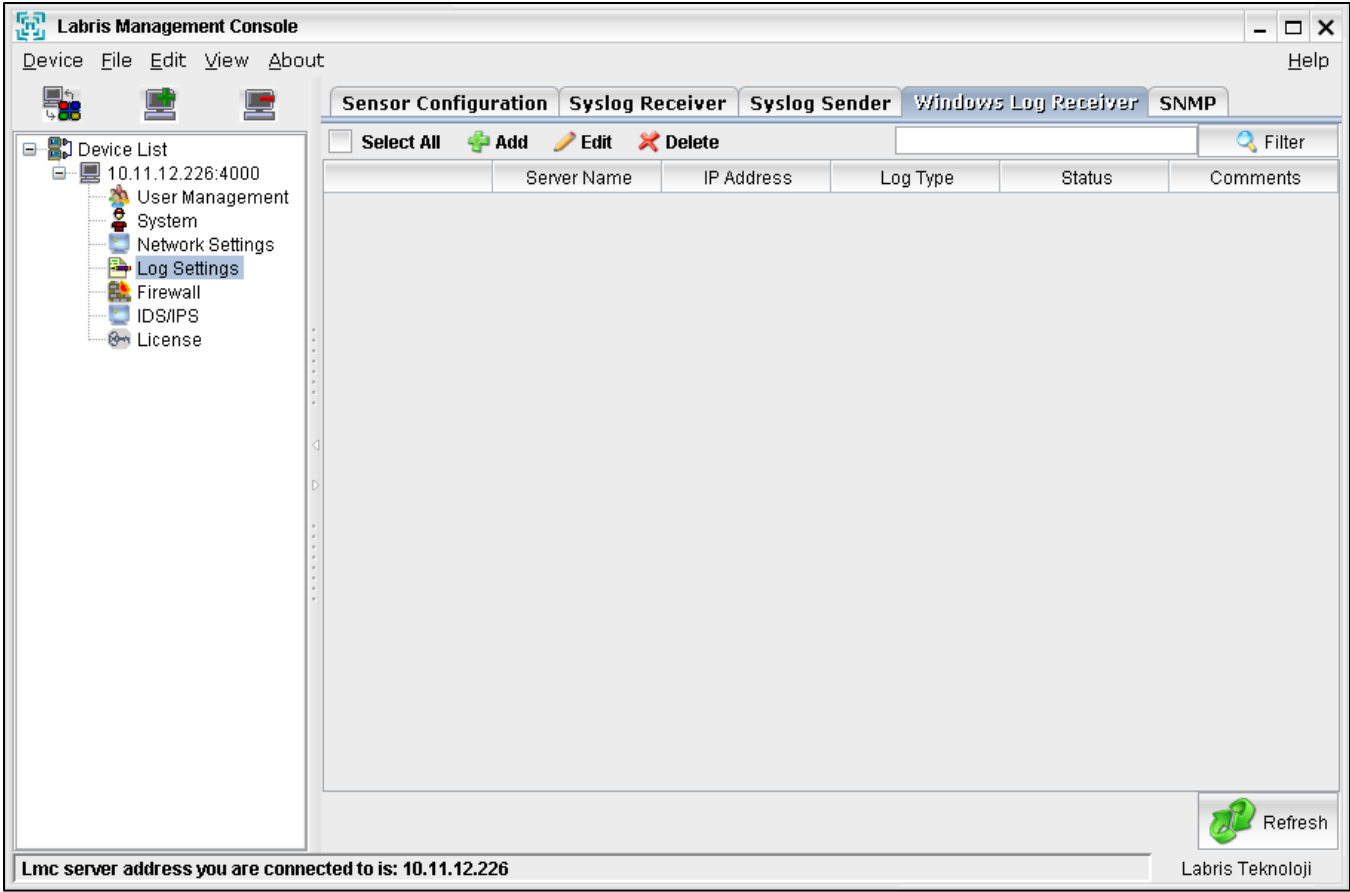


1	Select ALL	All pre-defined configurations can be chosen.
2	Add	It is used to add a new definition.
3	Edit	It is used to edit pre-defined configuration.
4	Delete	It is used to delete pre-defined configuration.
5	Comment	Description field.

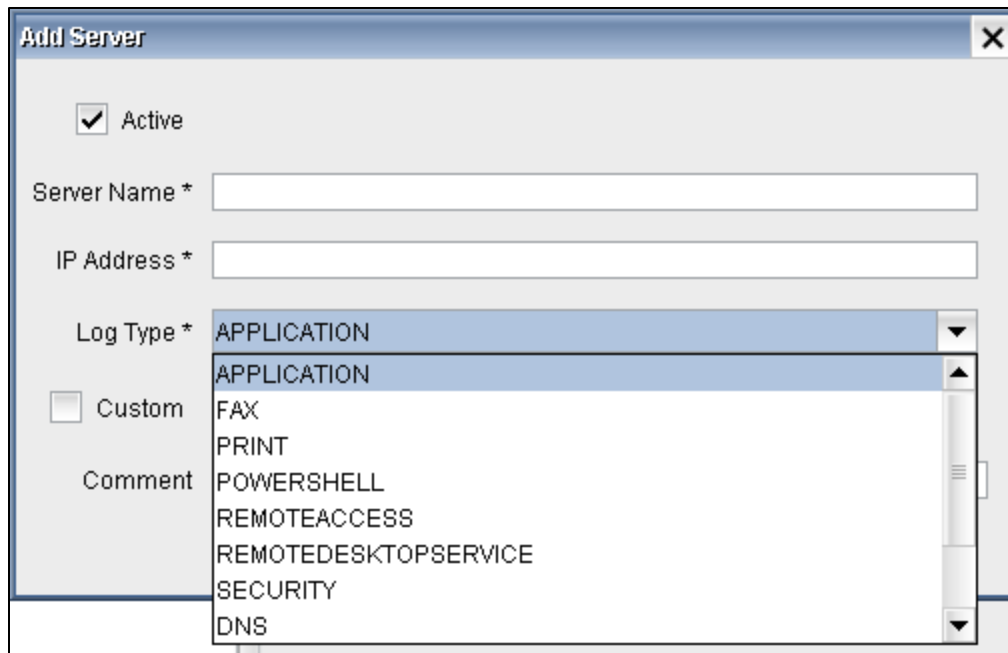
1	Active	Previously defined configurations can be active / passive.
2	Server Name	A name to define the Syslog resource of regarding sensor. Also the configuration file is created with this name.
3	IP Address	IP address of the server which sends logs via Syslog.
4	Log Type ALL	When check this option all received and collected logs will be sent to the external defined server in Syslog format.
5	Custom	All sensor logs and Labris Log own logs will be sent with this name.
6	Syslog Receiver	Logs retrieved from Syslog.
7	Windows Log Receiver	Logs retrieved from Windows Servers by “Windows Log Sender”
8	SNMP	Logs which is retrieved in SNMP format, is sent to the external log collector server.
9	Port/Protocol	It is used to define which port/protocols will be used to send logs to external log collector.
10	Comment	Description field.

Windows Log Receiver

Event logs of Windows servers, DHCP, EXCHANGE, IIS and other text based records can be sent to Labris Log through “Windows Labris Log Sender”. These records can be saved by making changes in settings of Windows Log Receiver.



1	Select ALL	All pre-defined configurations can be chosen.
2	Add	It is used to add a new definition.
3	Edit	It is used to edit pre-defined configuration.
4	Delete	It is used to delete pre-defined configuration.
5	Comment	Description field.



Add Server

☒ Active

Server Name *

IP Address *

Log Type * **APPLICATION**

☐ Custom

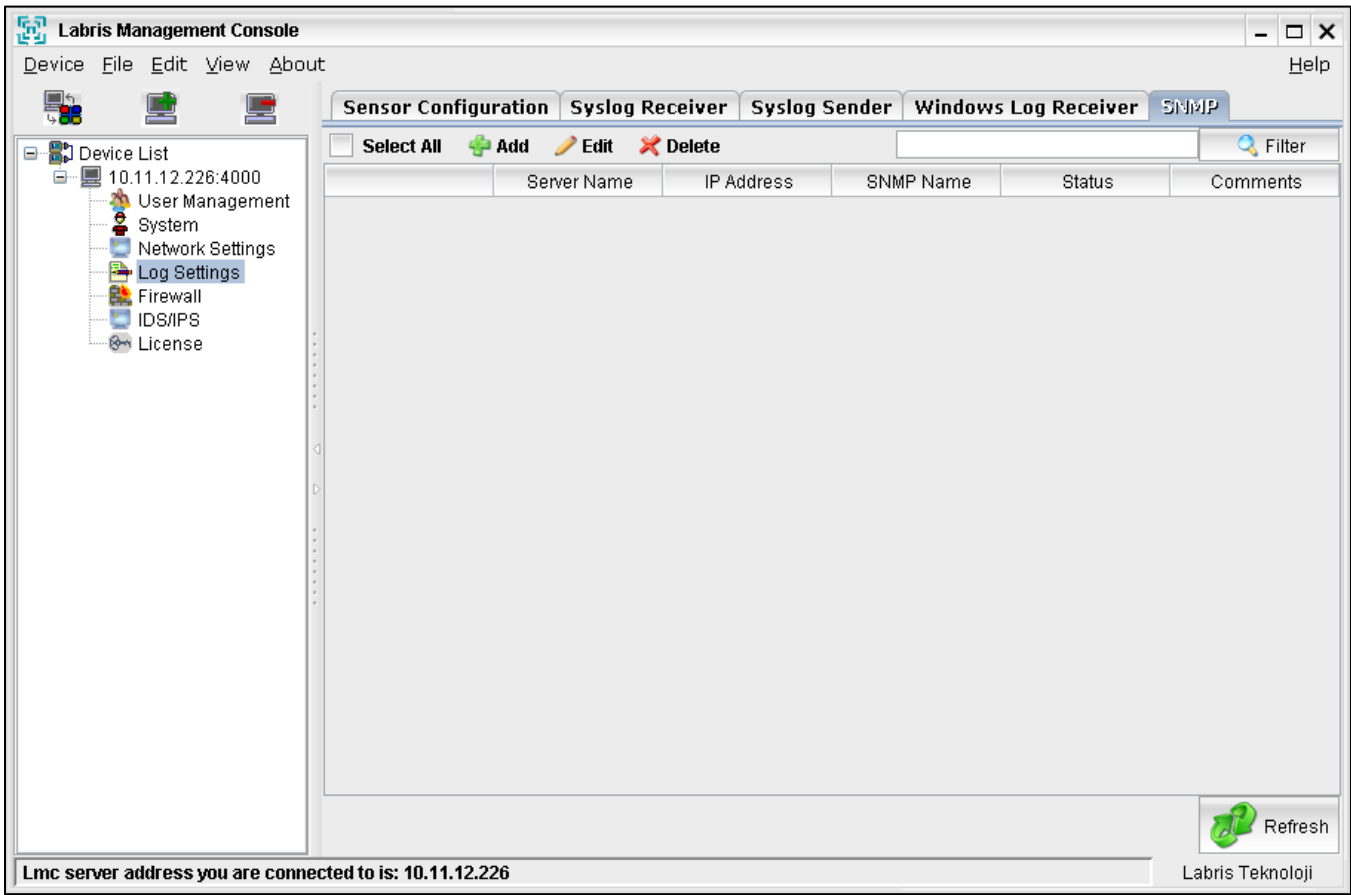
Comment

APPLICATION
FAX
PRINT
POWERSHELL
REMOTEACCESS
REMOTEDESKTOPSERVICE
SECURITY
DNS

1	Active	Defined settings can be set active / passive.
2	Server Name	A name to define Windows server source. At the same time, log files are constructed with that name.
3	IP Address	IP address of the Windows server to take the logs from.
4	Log Type	A definition is made here to be able to keep the logs sent from "Windows Log Sender". Same settings selected and defined on Windows server are applied here.
5	Custom	If this option is selected, a definition is made based on other text content defined on "Windows Log Sender". While making definition on Windows, the definition given as PREFIX is defined here as exactly.
6	Comment	Explanation field.

Simple Network Management Protocol (SNMP)

This option takes the logs of server and network devices having SNMP support. It records the logs by converting into line log formats.



1	Select ALL	All defined settings are selected.
2	Add	To make a new definition, Add button is used.
3	Edit	To make a change on the previously defined configuration, Edit button is used.
4	Delete	To delete defined configuration, Delete button is used.
5	Comment	Explanation field

Add Server

☒ Active

Server Name *

IP Address *

SNMP Name *

Comment

Port: 162 Protocol: UDP

OK

Cancel

1	Active	Defined settings can be set active / passive.
2	Server Name	A name to define related server or network device. At the same time, logs are constructed with this name.
3	IP Address	IP address of the server whom logs will be taken from
4	SNMP Name	SNMP sender's community name is written.
5	Comment	Explanation field.

Windows Labris Log Sender

Labris Log Sender tool provides service to all past logs on servers that have Windows Operating System (to be referred as OS later in this text), DHCP Service, IIS Service, Exchange Server and any other text-based log files from distant Labris LOG Server.

Labris Log Sender tool uses TCP 514 Port for sending logs.

Labris Log Sender tool supports the following OS:

Windows Server 2003 32 bit /64 bit, Server 2008 32 bit /64 bit, Server 2012 64 bit, Windows7 32 bit/64 bit and Windows8 32 bit/64 bit

Labris Log Sender Pre-Setup and Software Agreement

Labris Log Sender tool can be downloaded for your OS from the link shown below:

Click [here](#) for Windows 32 bit OS Server / User Machine Log Sender.

Click [here](#) for Windows 64 bit OS Server / User Machine Log Sender.

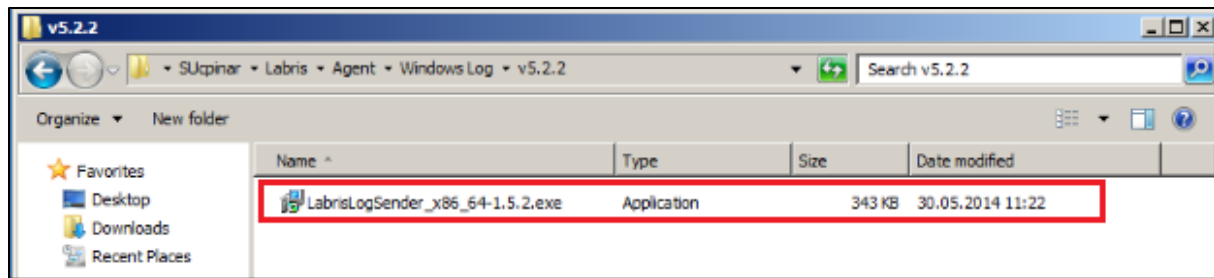
It is important that the user who will setup the software on the computer must have administrator access on the existing OS.

Firewall protection mode must be switched off while Labris Log Sender tool is being setup on Windows OS or you must make sure that TCP 514 port is not banned on the system. If there is a protective antivirus program on the system, default directory of Labris Log Sender tool (default directory C:\Program Files\LabrisLogSender) must be excluded from the protection area.

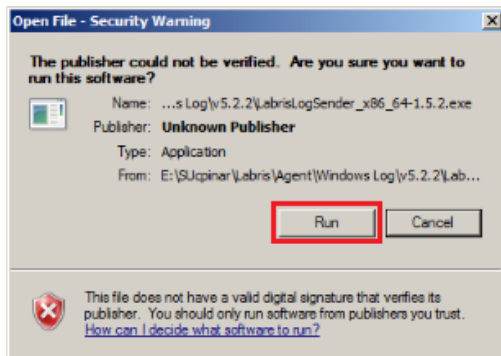
How to use Log Sender Installation?

When Labris Log Sender tool pre-setup conditions are met, you can install it on your Windows OS by following the steps shown below:

You can see the software version and bit information of the OS in the “Name” section.

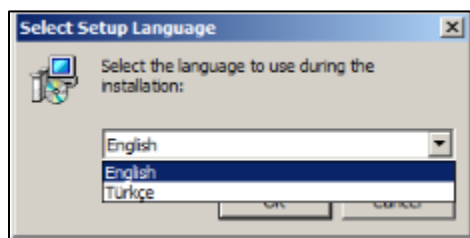


You can start the installation by clicking on the “Run” button.



1st Step – Language Selection;

Labris Log Sender tool has Turkish and English language support for the installation process. Select the suitable language for you and click “OK”. This tool support English language for the post installation process.



2nd Step – Starting Installation Wizard;

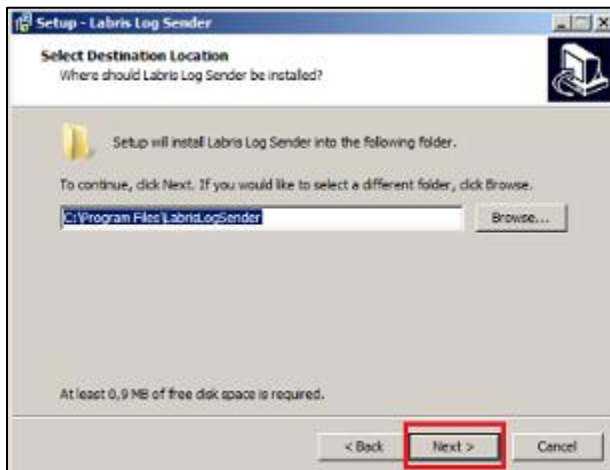
Welcome screen for installation wizard gives you the information about Labris Log Sender tool version and warning about installation. After you read the information shown, you can start installing by clicking “Next”.



3rd Step – Selecting the Installation Directory;

Installation directory is automatically set to C:\Program Files\LabrisLogSender. You can change the directory on your own choice.

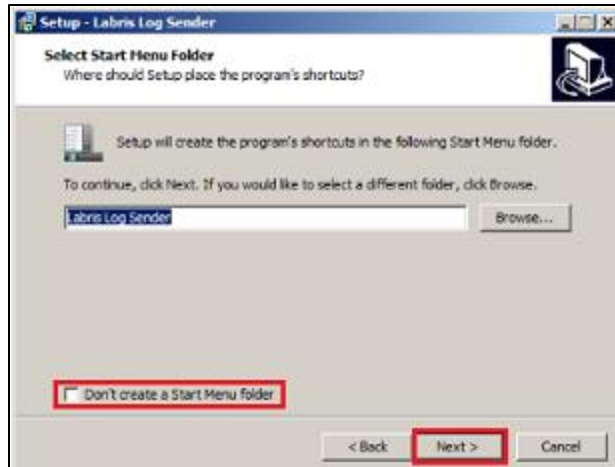
After you complete choosing directory selection, continue to next step by clicking “Next”.



4th Step – Creating Shortcut Name;

Create a shortcut name for Labris Log Sender tool to be shown on the start menu. If you do not want to create a start menu folder, tick “Don’t create a StartMenu folder”.

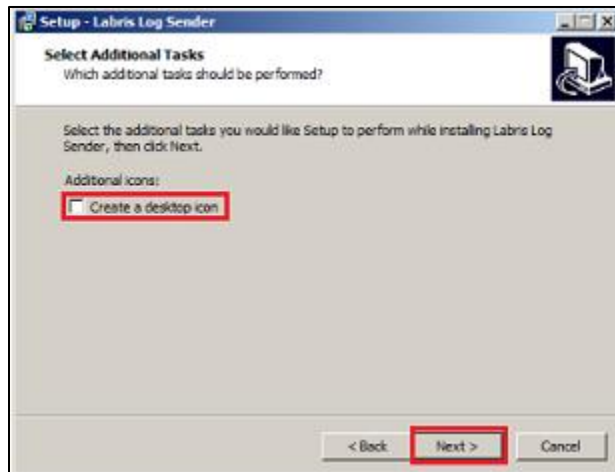
After you finish editing name, continue to next step by clicking “Next”.



5th Step – Creating a Desktop Icon;

Decide about whether you want to create a desktop icon for Labris Log Sender tool on Windows Desktop.

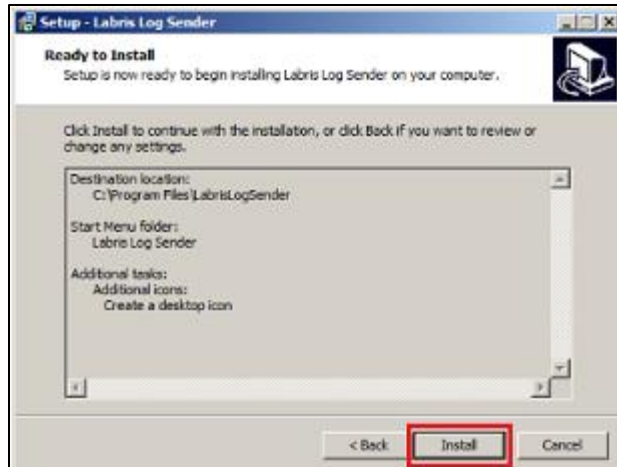
After you decide about it, continue to next step by clicking “Next”.



6th Step – Installing Log Sender tool;

Upon you finish the previous steps, you can start the installation process by clicking “Install”.

If there is a change in the previous steps, click “Back” and edit them.



6th Step – Completing Setup Wizard;

Click “Finish” to end the installation process.



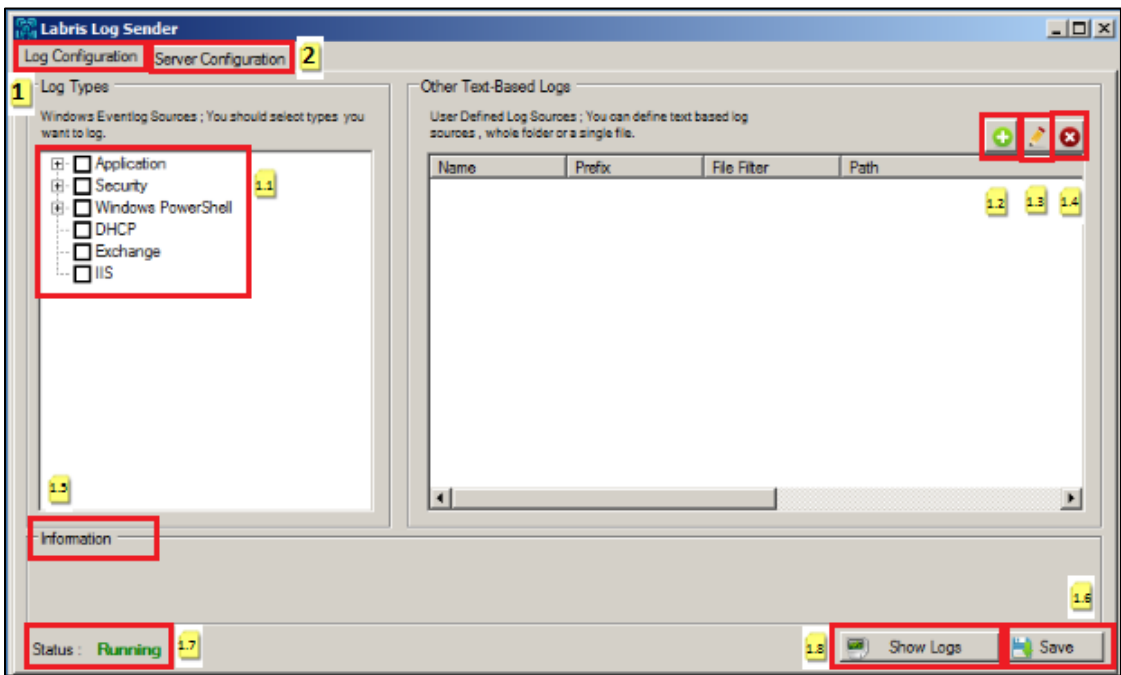
How to use Log Sender Configuration?

After the installation process, open the shortcut either on Windows Desktop or the Start Menu.

If there is no shortcut on any of these, you can start the program by clicking “LabrisLogSender.exe” file from the installation directory (default C:\Program Files\LabrisLogSender)

After you start the shortcut or LabrisLogSender.exe file, screen shown below will welcome you. Detailed information about screen is provided in the following photos and introduction.

The following screen will welcome you upon opening LabrisLogSender.exe or shortcut file. Detailed info is available on the picture below or the text under it.



Log Configuration

1	Log Configuration	Log Configuration Tab
1.1	Log Types	Select Log Type
1.2	Other Text Based Logs	Other Text Based Logs. Add a New Text File
1.3	Other Text Based Logs	Other Text Based Logs. Edit Text File Settings
1.4	Other Text Based Logs	Other Text Based Logs. Delete Text File
1.5	Information	Information for status
1.6	Save	Save all configuration
1.7	Status	Log Sender Service Status
1.8	Show Logs	Show Sender Logs

1/1.1 Log Types;

This is the easy and detailed section for sending the specifications available on Windows OS and event logs to LOG Server.

Event logs are divided into two parts that are Application and Security.

Application; Below status for application logs can be sent to LOG Server.	Security; Below status for security logs can be sent to LOG Server..
---	--

☒ Application

☒ Error

☒ FailureAudit

☒ Information

☒ SuccessAudit

☒ Warning

Windows PowerShell;
Below status for Windows PowerShell logs can be sent to LOG Server.

☒ Windows PowerShell

☒ Error

☒ FailureAudit

☒ Information

☒ SuccessAudit

☒ Warning

☒ Security

☒ Error

☒ FailureAudit

☒ Information

☒ SuccessAudit

☒ Warning

☒ DHCP

☐ Exchange

☐ IIS

☒ Exchange

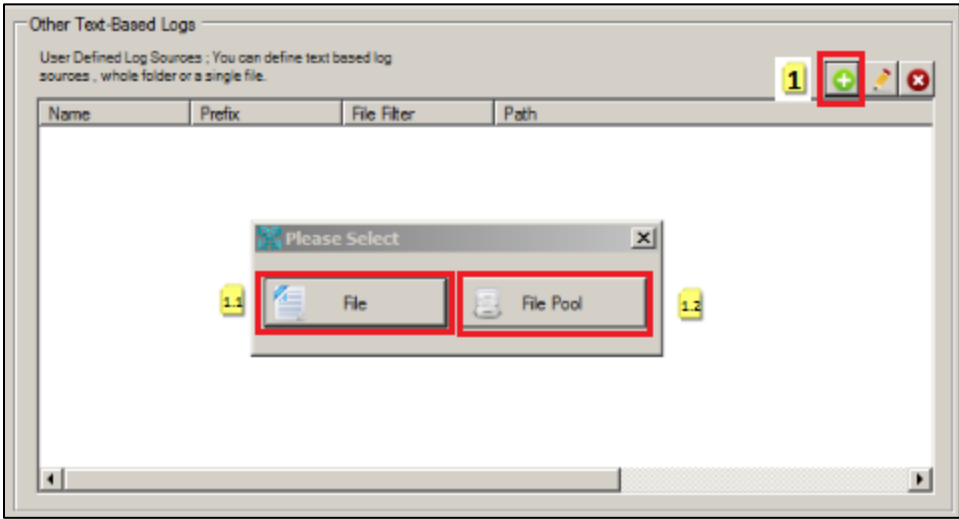
☐ IIS

☒ IIS

Windows Features;
Below status for Windows Features logs can be sent to LOG Server.

[1.2/1.3./1.4 Other Text-Based Logs;](#)

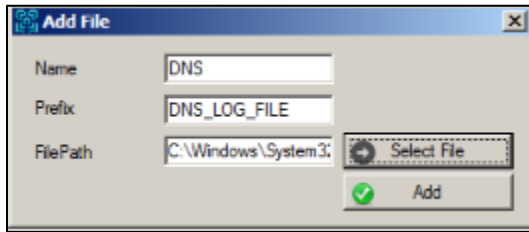
This allows defined text-based log events to be sent to LOG server. Administrator user can view *.txt extension files and C:/Windows/System32/Dhcp/ directory files.



1	Other Text-Based Log Add	Add Text-Based Log
1.1	File	Add Text-Based Log File
1.2	File Pool	Add Text-Based Logs Folder

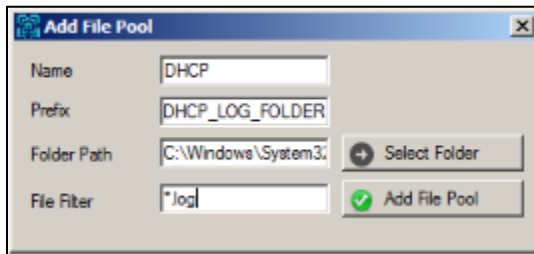
1.1 [Text-Based Logs File;](#)

Click “File” button and file directory is selected correctly.

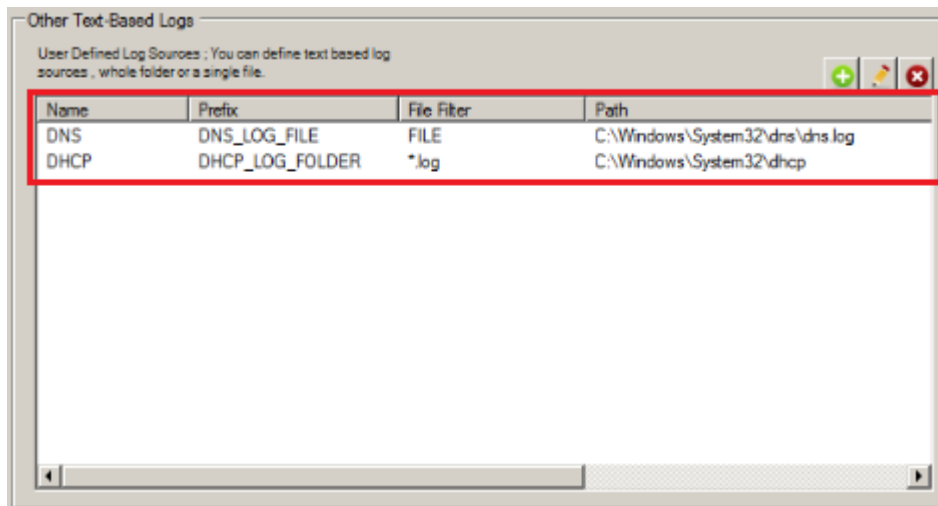


1.2 [Text-Based Logs File Pool;](#)

Click “File Pool” button and file directory is selected correctly.

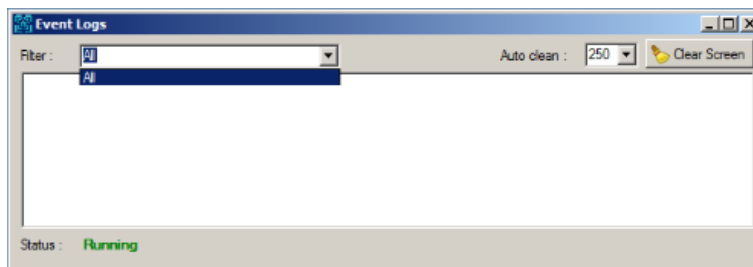


Other Text-Based Logs view will seem like as shown below:



1.8 [Show Logs;](#)

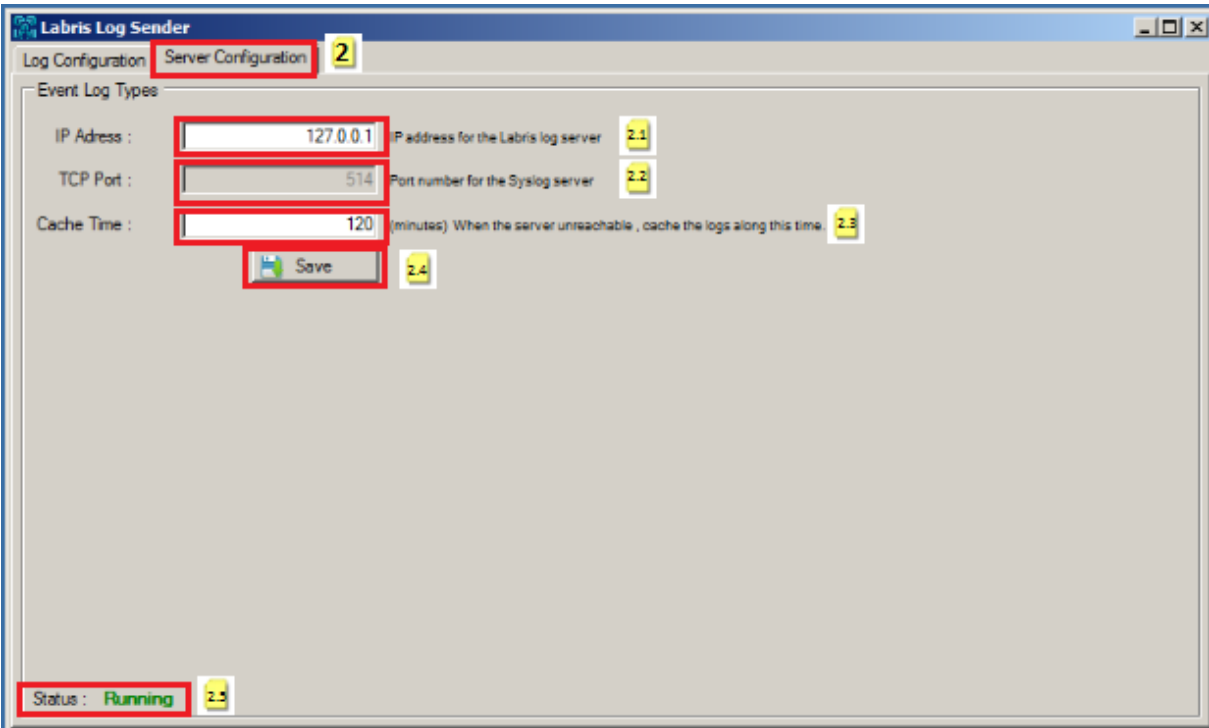
You can view all LOG Server log event that are sent by Log Sender in Show Logs section.



Server Configuration

This is the section for configuration screen for Labris LOG Server information. Default log sending port is automatically set to TCP 514.

Cache Time section is for creating cache memory for log event when the access to LOG Server is unavailable.

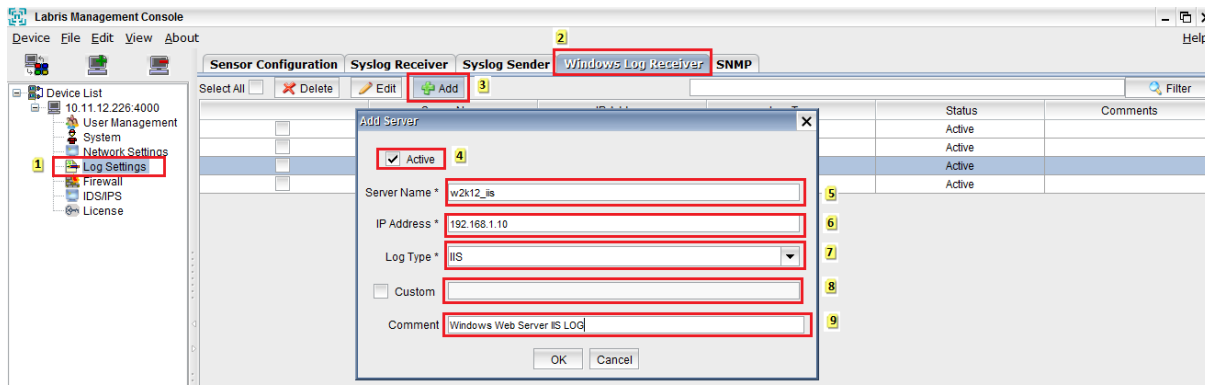


2	Server Configuration	Log Configuration Tab
2.1	IP Address	Labris LOG Server IP Address
2.2	TCP Port	TCP Port Number
2.3	Cache Time	Log Cache Time (Minutes)
2.4	Save	Save Configuration
2.5	Status	Log Sender Service Status

Labris LOG Server Configuration

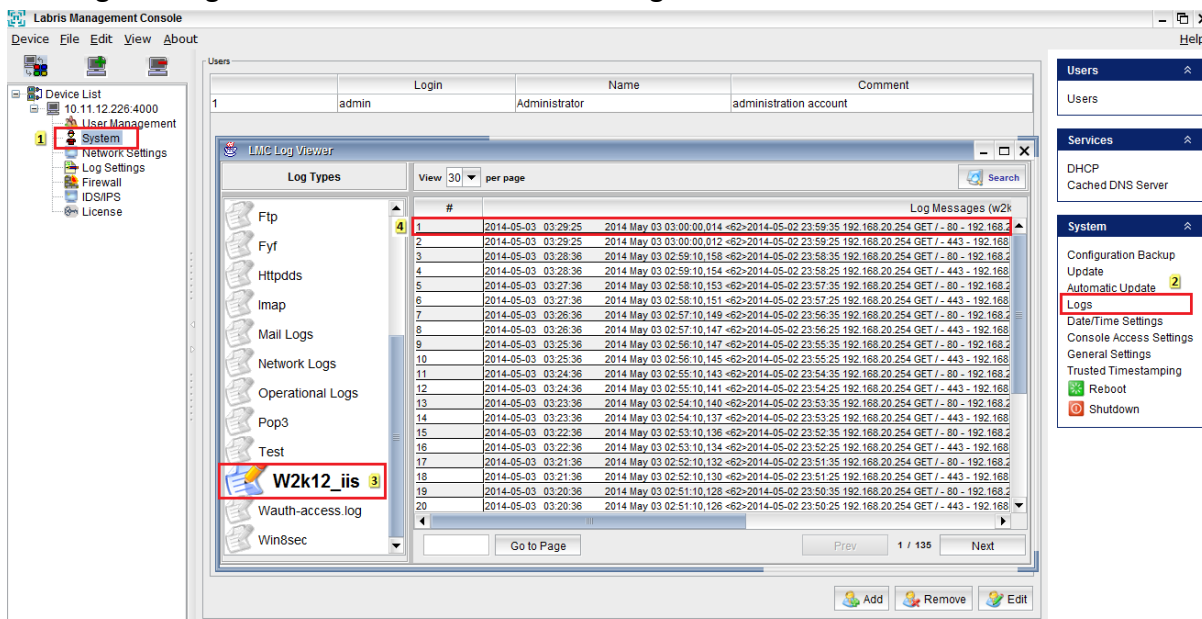
You should make these settings after you finish installation and select the log event for Labris Log Server.

- 1. Identifying Windows device on which Log Sender tool is installed.



1	Log Settings	Log Sender or Receiver Server Configuration Tab
2	Windows Log Receiver	Add Windows Log Receiver Server
3	Add	Add Windows Log Receiver
4	Active (Status)	Log Receiver Status
5	Server Name	Name for Server
6	IP Address	Windows Log Receiver IP Address
7	Log Type	Select a Log Type
8	Custom	Custom Log Type
9	Command	Command for Log Receiver

2. Viewing sent logs of Windows device on which Log Sender tool is installed.



1	System	System Configuration and Log View Tab
2	Logs	All Log File
3	Log Types	Select Log Show
4	Log Rows	Log Sender Logs

Port mirroring

3Com Switch Port Mirroring

To copy traffic of port 1 to port 19:

```
<Sysname> system-view  
[Sysname] interface Ethernet1/0/19  
[Sysname-Ethernet1/0/19] monitor-port  
[Sysname-Ethernet1/0/19] quit  
[Sysname] interface Ethernet1/0/1  
[Sysname-Ethernet1/0/1] mirroring-port both  
[Sysname-Ethernet1/0/1] quit
```

```
<4500> display mirror  
Monitor-port:  
Ethernet1/0/19  
Mirroring-port:  
Ethernet1/0/1      both
```

Cisco Switch Port Mirroring

Kopyalanmasını istediğimiz port: Source Port fa0/3

Hedef Port: Destination Port fa0/4

```
switch(config)#monitor session 1 source interface fa0/3  
switch(config)#monitor session 1 destination interface fa0/4
```

- To copy multiple source ports to destination port;

Source Port fa0/3

Destination Port fa0/5

```
switch(config)#monitor session 2 source interface fa0/3
```

```
switch(config)#monitor session 2 destination interface fa0/5
```

- To display the copied ports on the switch:

```
show monitor session 1
```

```
show monitor session 2
```

HP Switch Port Mirroring

Connect via telnet or console access.

```
#telnet 192.168.2.28
```

Switch to 'Privilege' mode . (You should see '#' instead of '>' .)

```
hp>enable
```

```
hp#
```

Switch to 'configuration' mode.

```
hp#configure terminal
```

Type the port that Labris Log device is connected as monitor port. Some keys has port numbers (A1-12, B13-24, C25-36, D37-48) and some keys are direct port numbers (1-2-3-4-5-6...).

```
hp(config)#mirror-port ethernet 9
```

Enter the settings of the port which will be copied. This port is usually the port that Firewall is connected. By copying source port of network traffic is copied to firewall, all network traffic will be visible.

```
hp(config)#interface ethernet 3
```

Issue monitor command.

```
hp(eth-3)#monitor
```

Exit from ethernet settings.

```
hp(eth-3)# end
```

Save changes.

```
hp#wr mem
```

Juniper Switch Port Mirroring

Firstly, connect to console access interface of Juniper device.
Please type 'edit' to switch edit mode.

Use the commands below to specify the source port(port that router is connected). 'LOG' is typed as a description.

```
# set ethernet-switching-options analyzer LOG input ingress interface ge-0/0/7.0  
# set ethernet-switching-options analyzer LOG input egress interface ge-0/0/7.0
```

After specifying the source port, you should specify destination port (port that Labris LOG device is connected).

Incoming and outgoing traffic in 'ge-0/0/7.0 ethernet' is copied to 'ge-1/0/22.0 ethernet' after typing the command below.

```
# set ethernet-switching-options analyzer LOG output interface ge-1/0/22.0
```

Please type 'commit' to apply your changes.



If a port is used for port mirroring in the switch, it is usually not used for network access. Therefore, use a different port for your Labris LOG device's management port.

Logview

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 system log sources.

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

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.

Date / Time	Source	Source User	Source Port	Destination	Destination User	Destination Port	Rule	Action	Protocol	Application	Mac Address
2014-06-03 08:12:31	192.168.0.165	-	49054	192.168.0.1	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:a0
2014-06-03 08:12:31	192.168.0.165	-	44804	192.168.0.1	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:a0
2014-06-03 08:12:31	192.168.0.165	-	40917	192.168.1.2	-	25	_ftg_Default	DROP	TCP	MARK-HUB35	00:90:0b:2b:a0:94
2014-06-03 08:12:31	192.168.0.165	-	40917	192.168.1.2	-	25	_ftg_Default	DROP	TCP	MARK-HUB35	00:90:0b:2b:a0:94
2014-06-03 08:12:31	192.168.0.165	-	80	192.168.1.2	-	54867	_ftg_Rule	DENY	TCP	-	00:90:0b:2b:a0:94
2014-06-03 08:12:31	192.168.0.165	-	80	192.168.1.2	-	54867	_ftg_Default	DROP	TCP	-	00:90:0b:2b:a0:94
2014-06-03 08:12:30	192.168.2.144	petridyssyk	137	192.168.2.255	-	137	_ftg_Rule	ACCEPT	UDP	MARK-HUB43	5c:f9:ad:4:23:a8
2014-06-03 08:12:30	192.168.2.167	-	58472	192.168.0.1	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	00:15:65:5a:75:7b
2014-06-03 08:12:30	192.168.2.167	-	43040	194.27.44.55	-	123	_ftg_WAULT_FORWARD	DROP	UDP	NTP_NTP	00:15:65:5a:75:7b
2014-06-03 08:12:30	192.168.1.2	-	33138	192.168.1.2	-	80	_ftg_Rule	ACCEPT	TCP	-	-
2014-06-03 08:12:29	192.168.0.165	-	50590	192.168.1.2	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:a0
2014-06-03 08:12:29	192.168.0.165	-	30453	192.168.0.1	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:a0
2014-06-03 08:12:29	192.168.2.247	-	59078	192.168.2.1	-	3127	_ftg_Rule	ACCEPT	TCP	TCP_TCP	00:1a:8c:56:b0:1c
2014-06-03 08:12:29	192.168.1.2	-	60609	5.9.147.90	-	80	_ftg_Rule	ACCEPT	TCP	-	-
2014-06-03 08:12:29	192.168.2.149	-	1752	194.27.44.56	-	123	_ftg_WAULT_FORWARD	DROP	UDP	NTP_NTP	00:15:65:52:23:db
2014-06-03 08:12:29	192.168.1.2	-	33138	192.168.1.2	-	80	_ftg_Rule	ACCEPT	TCP	-	-
2014-06-03 08:12:29	192.168.2.144	petridyssyk	137	192.168.2.255	-	137	_ftg_Rule	ACCEPT	UDP	MARK-HUB43	5c:f9:ad:4:23:a8
2014-06-03 08:12:29	95.6.72.25	-	34766	172.16.1.2	-	25	_ftg_Rule	ACCEPT	TCP	SMTP_SMTP	00:90:0b:2b:a0:94
2014-06-03 08:12:29	192.168.0.165	-	37770	192.168.0.1	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:a0
2014-06-03 08:12:29	192.168.0.165	-	46209	192.168.0.1	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:a0
2014-06-03 08:12:29	192.168.2.144	petridyssyk	55280	192.168.0.1	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	5c:f9:ad:4:23:a8
2014-06-03 08:12:29	192.168.1.2	-	45547	195.175.39.39	-	53	_ftg_Rule	ACCEPT	UDP	-	-
2014-06-03 08:12:29	192.168.2.144	petridyssyk	1739	192.168.2.1	-	3127	_ftg_Rule	ACCEPT	TCP	TCP_TCP	5c:f9:ad:4:23:a8
2014-06-03 08:12:29	192.168.2.144	petridyssyk	1741	192.168.2.1	-	3127	_ftg_Rule	ACCEPT	TCP	TCP_TCP	5c:f9:ad:4:23:a8
2014-06-03 08:12:29	192.168.1.2	-	25086	173.194.70.102	-	80	_ftg_Rule	ACCEPT	TCP	-	-
2014-06-03 08:12:29	192.168.1.139	-	81794	213.180.204.124	-	25	_ftg_WAULT_FORWARD	DROP	TCP	SMTP_SMTP	a0:90:0b:2b:a0:94
2014-06-03 08:12:29	93.186.122.9	-	45572	172.16.1.2	-	25	_ftg_Rule	ACCEPT	TCP	SMTP_SMTP	00:90:0b:2b:a0:94
2014-06-03 08:12:28	192.168.0.190	-	43322	8.8.8.8	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:a0
2014-06-03 08:12:28	192.168.2.144	petridyssyk	64835	192.168.0.1	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	5c:f9:ad:4:23:a8
2014-06-03 08:12:28	192.168.1.2	-	13314	195.175.39.39	-	53	_ftg_Rule	ACCEPT	UDP	-	-
2014-06-03 08:12:28	192.168.2.144	petridyssyk	1735	173.194.70.113	-	443	_ftg_Rule	ACCEPT	TCP	SSL_SSL	5c:f9:ad:4:23:a8
2014-06-03 08:12:28	192.168.0.165	-	46489	192.168.0.1	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:a0
2014-06-03 08:12:28	192.168.0.165	-	36761	192.168.0.1	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:a0
2014-06-03 08:12:28	192.168.0.165	-	44055	192.168.0.1	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:a0
2014-06-03 08:12:28	192.168.0.165	-	35754	192.168.0.1	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:a0
2014-06-03 08:12:28	192.168.0.165	-	54602	192.168.0.1	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:a0
2014-06-03 08:12:28	192.168.0.165	-	33736	192.168.0.1	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:a0
2014-06-03 08:12:28	192.168.0.165	-	40605	192.168.0.1	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:a0
2014-06-03 08:12:28	192.168.0.165	-	49518	192.168.0.1	-	53	_ftg_Rule	ACCEPT	UDP	DNS_DNS	08:00:27:80:1e:a0

Figure Logview records table while streaming with some sample logs

Date/Time	User	Source	Mac Address	Destination	URL	Decision	HTMSS	Category
2014-06-03 08:23:33	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:23:33	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:23:33	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:23:28	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:23:28	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:23:28	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:23:22	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:23:17	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:23:17	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:23:12	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:23:12	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:23:07	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:23:07	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:23:06	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:23:01	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:23:01	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:22:56	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:22:56	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:22:46	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:22:46	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:22:41	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:22:41	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:22:36	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:22:31	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:22:31	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:22:21	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:22:21	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	
2014-06-03 08:22:16	-	192.168.0.156	-	-	http://192.168.0.1.954n	"SCANNED"	TCP_DENIED403	

Figure Logview records table with some historical logs

Parts & Tools

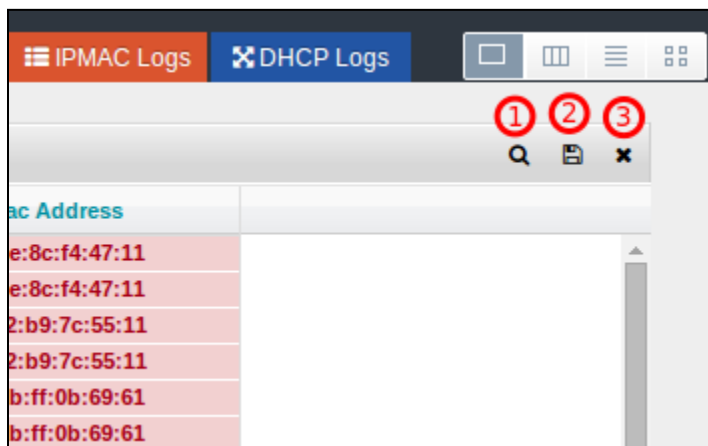
Logview has some easy-to-use parts and useful tools:

Date/Time	Source	Source Port	Destination	Destination User	Destination	Rule	Action	Protocol	Application	Mac Address
2014-06-03 08:45:32	192.168.0.156	-	60728	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:45:32	192.168.0.156	-	60729	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:45:32	192.168.0.153	-	17500	255.255.255.255	-	17500	Drop	UDP	-	4c:72:3d:7a:55:13
2014-06-03 08:45:30	0.0.0.0	-	68	255.255.255.255	-	67	Drop	UDP	-	6a:3a:f7:0b:69:61
2014-06-03 08:45:30	0.0.0.0	-	68	255.255.255.255	-	67	Drop	UDP	-	6a:3a:f7:0b:69:61
2014-06-03 08:45:29	192.168.0.153	-	57621	192.168.0.187	-	57621	Drop	UDP	-	4c:72:3d:7a:55:13
2014-06-03 08:45:28	0.0.0.0	-	68	255.255.255.255	-	67	Drop	UDP	-	6a:3a:f7:0b:69:61
2014-06-03 08:45:28	192.168.0.23	-	17500	255.255.255.255	-	17500	Drop	UDP	-	10:60:40:7c:8c:67
2014-06-03 08:45:27	0.0.0.0	-	68	255.255.255.255	-	67	Drop	UDP	-	6a:3a:f7:0b:69:61
2014-06-03 08:45:27	0.0.0.0	-	68	255.255.255.255	-	67	Drop	UDP	-	6a:3a:f7:0b:69:61
2014-06-03 08:45:26	192.168.0.156	-	60730	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:45:26	192.168.0.156	-	60731	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:45:24	192.168.0.156	-	60728	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:45:24	192.168.0.156	-	60729	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:45:22	192.168.0.156	-	60731	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:45:22	192.168.0.156	-	60730	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:45:20	192.168.0.158	-	57621	192.168.0.187	-	57621	Drop	UDP	-	e8:40:12:4c:3a:25
2014-06-03 08:45:20	192.168.0.156	-	60729	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:45:20	192.168.0.156	-	60730	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:45:20	192.168.0.156	-	60729	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:45:19	192.168.0.156	-	60731	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:45:19	192.168.0.156	-	60725	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:45:19	192.168.0.156	-	60726	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:45:18	192.168.0.156	-	60729	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:45:18	192.168.0.156	-	60729	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:45:18	192.168.0.156	-	60729	192.168.0.187	-	8080	Drop	TCP	-	00:30:8c:94:47:11
2014-06-03 08:44:58	0.0.0.0	-	68	255.255.255.255	-	67	Drop	UDP	-	6a:3a:f7:0b:69:61
2014-06-03 08:44:58	0.0.0.0	-	68	255.255.255.255	-	67	Drop	UDP	-	6a:3a:f7:0b:69:61
2014-06-03 08:44:51	0.0.0.0	-	68	255.255.255.255	-	67	Drop	UDP	-	6a:3a:f7:0b:69:61
2014-06-03 08:44:36	0.0.0.0	-	68	255.255.255.255	-	67	Drop	UDP	-	6a:3a:f7:0b:69:61
2014-06-03 08:44:36	0.0.0.0	-	68	255.255.255.255	-	67	Drop	UDP	-	6a:3a:f7:0b:69:61

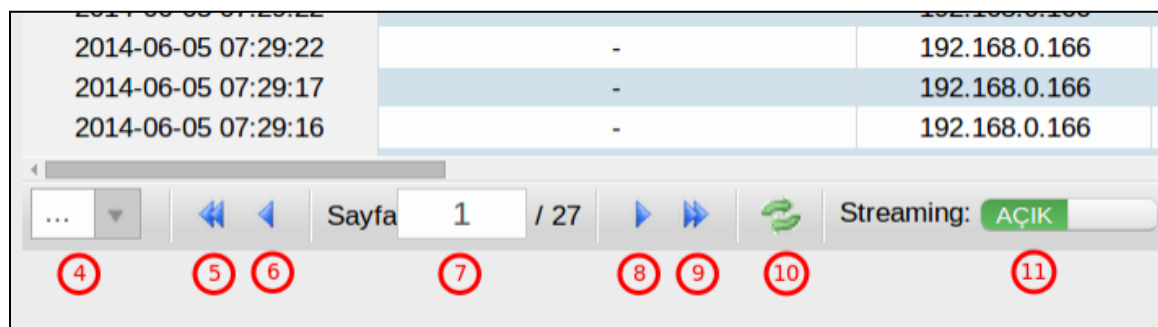
Figure: Parts & Tools on main display

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

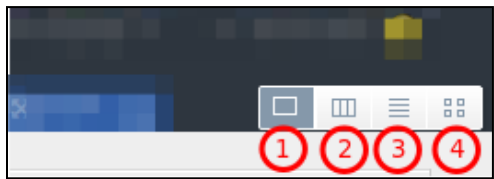


2 . Live monitoring shortcuts



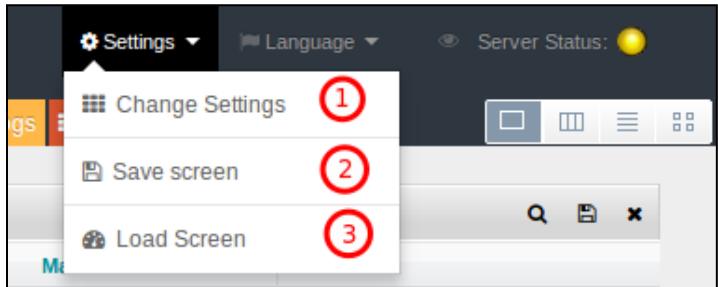
1	Firewall	Firewall Network Logs View
2	Access	Access Logs View
3	Operational	Operational Logs View
4	Administrative	Administrative Logs View
5	Wireless Authentication	Wireless Authentication Logs View
6	IPMAC	IPMAC Logs View
7	DHCP	DHCP Logs View
8	Mail	Mail Logs View

3 . Layout options



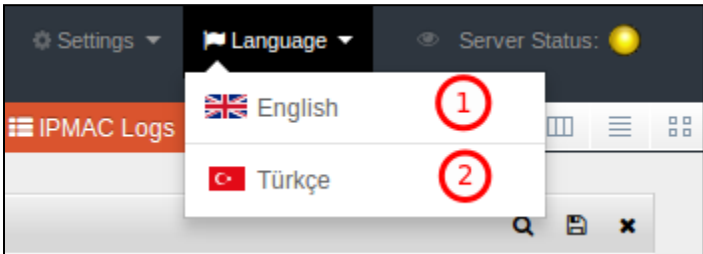
1	Single View	Select Single View
2	Column View	Select Column View
3	List View	Select List View
4	Grid View	Select Grid View

4 . Settings



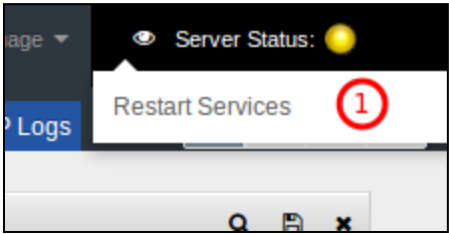
1	Change Settings	Select Change Settings
2	Save Screen	Save Screen
3	Load Screen	Load Screen

5 . Language selector



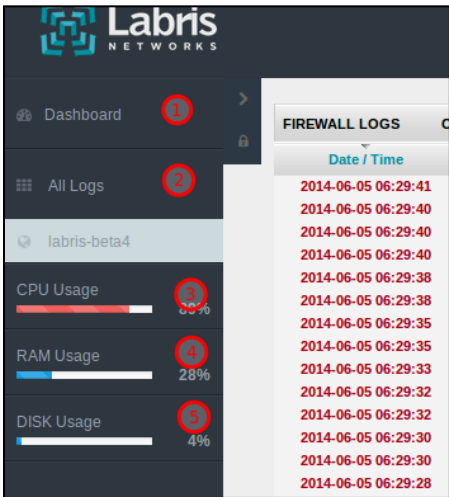
1	English	Select English Language
2	Turkish	Select Turkish Language

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

Instructions

Logview is a web-based application and the only thing you could run it is a Web browser. We advise 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.

Records Table

Records table shows records from your LOG 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:

ACCESS LOGS Create Time: 2014-06-05 13:12 Begin: 2014-06-05 00:00										Q	⊞	×
Date / Time	User	Source	Mac Address	Destination	URL	Decision	HIT/MISS	Category	Filter G			
2014-06-05 13:13:52		192.168.2.156	-	-		*EXCEPTION*Ayrcalkil_bi_sleye_girdniz	TCP_MISS200		kuile			
2014-06-05 13:13:52		192.168.2.156	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:52		192.168.2.156	-	-			TCP_MISS204		kuile			
2014-06-05 13:13:52		192.168.0.153	-	-		*EXCEPTION*Ayrcalkil_bi_sleye_girdniz	TCP_MISS206		kuile			
2014-06-05 13:13:52		192.168.2.161	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:52		192.168.2.156	-	-			TCP_MISS200		kuile			
2014-06-05 13:13:51		192.168.0.153	-	-		*EXCEPTION*Ayrcalkil_bi_sleye_girdniz	TCP_MISS206		kuile			
2014-06-05 13:13:51		192.168.2.156	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:50		192.168.2.156	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:50		192.168.2.156	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:50		192.168.2.156	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:50		192.168.2.156	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:50		192.168.2.156	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:50		192.168.0.153	-	-		*EXCEPTION*Ayrcalkil_bi_sleye_girdniz	TCP_MISS206		kuile			
2014-06-05 13:13:50		192.168.2.156	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:49		192.168.0.153	-	-		*EXCEPTION*Ayrcalkil_bi_sleye_girdniz	TCP_MISS206		kuile			
2014-06-05 13:13:49		192.168.2.156	-	-			TCP_MISS200		kuile			
2014-06-05 13:13:48		192.168.2.161	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:48		192.168.2.161	-	-			TCP_MISS200		kuile			
2014-06-05 13:13:47		192.168.2.156	-	-			TCP_MISS200		kuile			
2014-06-05 13:13:47		192.168.0.153	-	-		*EXCEPTION*Ayrcalkil_bi_sleye_girdniz	TCP_MISS206		kuile			
2014-06-05 13:13:47		192.168.2.156	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:47		192.168.2.156	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:46		192.168.2.156	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:46		192.168.2.156	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:46		192.168.2.156	-	-		*SCANNED*	TCP_MISS202		kuile			
2014-06-05 13:13:46		192.168.2.156	-	-			TCP_MISS200		kuile			
2014-06-05 13:13:46		192.168.2.156	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:46		192.168.2.156	-	-			TCP_MISS200		kuile			
2014-06-05 13:13:46		192.168.0.153	-	-		*EXCEPTION*Ayrcalkil_bi_sleye_girdniz	TCP_MISS206		kuile			
2014-06-05 13:13:46		192.168.2.156	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:46		192.168.0.198	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:46		192.168.2.156	-	-			TCP_MISS200		kuile			
2014-06-05 13:13:46		192.168.2.156	-	-			TCP_MISS200		kuile			
2014-06-05 13:13:46		192.168.0.163	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:46		192.168.2.132	-	-		*SCANNED*	TCP_MISS200		kuile			
2014-06-05 13:13:45		192.168.2.156	-	-			TCP_MISS200		kuile			
2014-06-05 13:13:45		192.168.2.156	-	-			TCP_MISS200		kuile			

And by clicking 1.1 Show / Hide Column Filtering button you will see the filters, even they are already filtered:

ACCESS LOGS Create Time: 2014-06-05 13:12 Begin: 2014-06-05 00:00						
Date / Time	User	Source	Mac Address	Destination	URL	Decision
Set Date Range	User	192.168.0.42	Mac Address	Destination	URL	scanne
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*

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.

http://techlaboratory.net/service/notification

Export

Export Type:

☐ TXT

☐ CSV

File Name:

write a file name







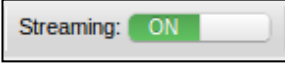
Export

http://techlaboratory.net/service/notification

http://realtime.services.disqus.com/api/2/thread/823237460?bust=4760

And you can remove the table by clicking 1.3 Remove table button.

Records table also has a footer, which includes:

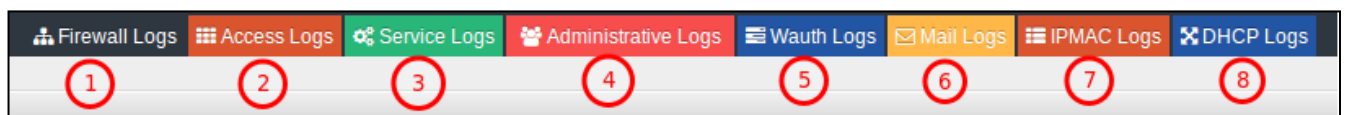
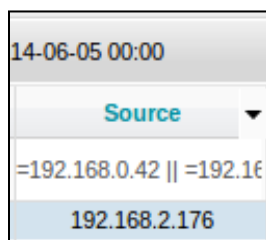
- record  length: use it to set content length of a table by page 10, 15, 20, 30 and 50
- backward-   forward buttons: use it to shift pages by 10 forward or backward
- previous   next buttons: use it to shift pages one by one
- reload buttons:  use it to reload the page if you think something goes wrong 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.

Real-time Monitoring

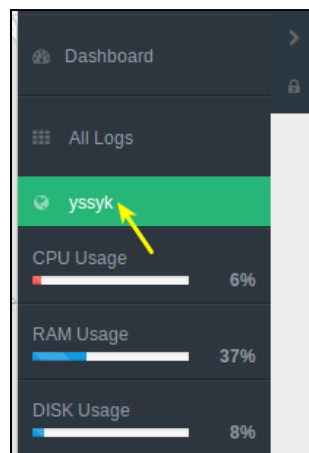
Logview provides a real-time monitoring for streaming logs. You can just click the shortcut buttons and it fires an event to create real-time logs monitoring tables.



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.

Table

Select Log Source

☐ Firewall Logs

☐ Service Logs

☐ Wauth Logs

☐ IPMAC Logs

☒ Access Logs

☐ Administrative Logs

☐ Mail Logs

☐ DHCP Logs

Select Log Fields

☒ Date / Time

☒ Mac Address

☒ Decision

☐ Host

☐ Response Code

☐ Client Host

☐ Method

☒ User

☒ Destination

☒ Undefined

☐ Domain

☐ User Agent

☐ Duration

☒ Source

☒ URL

☒ Category

☒ Filter Group

☐ Size

☐ Mime Type

Default Ranges:

1 day

3 days

1 week

From:

2014-05-29 16:09

To:

2014-06-05 16:09

CREATE TABLE

Table

Select Log Source

☐ Firewall Logs

☒ Access Logs

☐ Administrative Logs

☐ Mail Logs

☐ DHCP Logs

Select Log Fields

☒ Source

☒ URL

☒ Category

☒ Filter Group

☐ Size

☐ Mime Type

Default Ranges:

Now

Done

From:

2014-05-29 16:09

To:

2014-06-05 16:09

CREATE TABLE

May 2014

Su

Mo

Tu

We

Th

Fr

Sa

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

Time

16:09

Hour

Minute

Now

Done

Utilities

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.

The screenshot shows a 'Settings' window with a title bar containing a menu icon and the text 'Settings'. Below the title bar is a section titled 'Please select default columns to be shown in table:'. This section contains a table with columns for different log sources: Firewall ..., Access L..., Service L..., Administ..., Wauth Lo..., Mail Logs, IPMAC L..., and DHCP Logs. Each column has a list of fields with checkboxes. For example, under 'Firewall ...', the fields are 'Date / Time' (checked), 'URL' (checked), 'Domain' (unchecked), and 'Client Host' (unchecked). Under 'Access L...', the fields are 'User' (checked), 'Decision' (checked), 'Filter Group' (checked), and 'Duration' (unchecked). Under 'Service L...', the fields are 'Source' (checked), 'HIT/MISS' (checked), 'Response Code' (unchecked), and 'Mime Type' (unchecked). Under 'Administ...', the fields are 'Mac Address' (checked), 'Category' (checked), 'User Agent' (unchecked), and 'Method' (unchecked). Under 'Wauth Lo...', the fields are 'Destination' (checked), 'Host' (unchecked), and 'Size' (unchecked). At the bottom left of the window is a green 'Save' button.

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.

The screenshot shows a 'Save Page' window with a title bar containing a menu icon and the text 'Save Page'. Below the title bar is a section titled 'View Name:' followed by a text input field. At the bottom of the window are two buttons: a green 'CREATE' button and a blue 'SAVE TO DASHBOARD' button.

Load Screen

Logview stores your saved screen with any parameters and settings you given, 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

Regional Settings

Logview supports multilingual operations. Basically, it comes with English and Turkish. If clients require it, it is easy to add more languages to be supported.

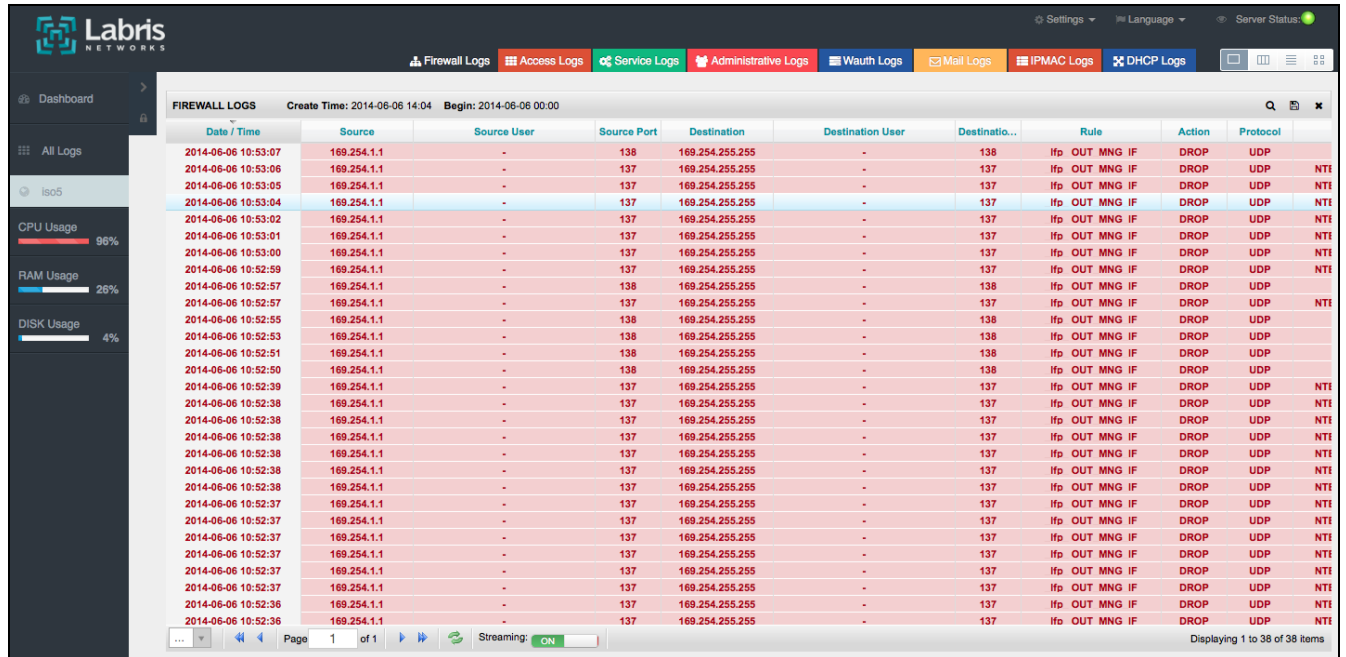


Figure: Main display in English

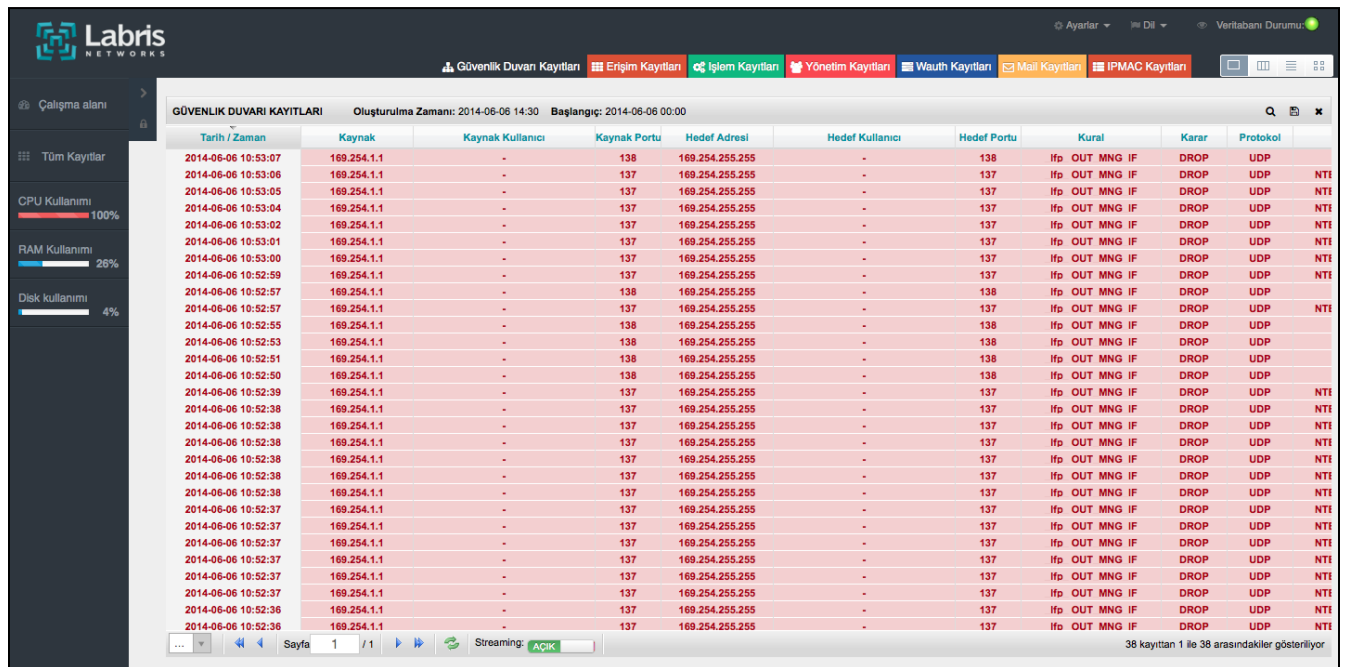


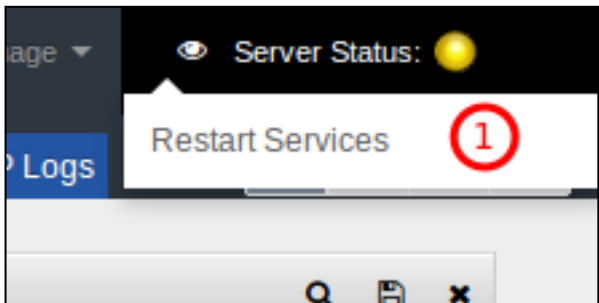
Figure: Main display in Turkish

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.

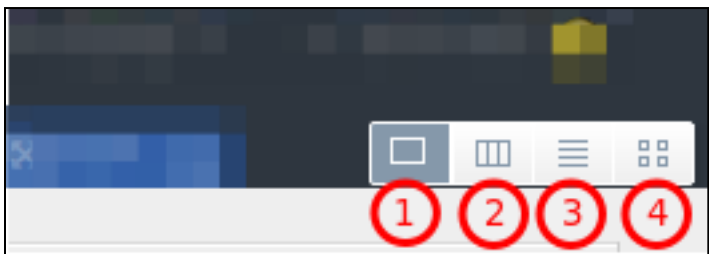


There is also a service controlling option under the Server Status menu to restart services. If you see yellow indicator you may go through to try restarting services. If it may keep staying in the yellow status please contact the technical support.



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 options 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.

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.

FIREWALL LOGS												Q	📄	✖	
Create Time: 2014-06-06 14:59		Begin: 2014-06-06 00:00													
Date / Time	Source	Source User	Source Port	Destination	Destination User	Destination...	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 10:52:37	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					
Page 1 of 1												Streaming: <input checked="" type="checkbox"/>		Displaying 1 to 38 of 38 items	

Column View

In column view you can put widgets in columns and vertically display them.

FIREWALL LOGS					Create Time: 2014-06-06 15:16			Begin: 2014-06-0...					
Date / Time	Source	Source User	Source Port	Destination									
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									
2014-06-06 10:52:51	169.254.1.1	-	138	169.254.255.255									
2014-06-06 10:52:50	169.254.1.1	-	138	169.254.255.255									
2014-06-06 10:52:39	169.254.1.1	-	137	169.254.255.255									
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255									
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255									
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255									
2014-06-06 10:52:38	169.254.1.1	-	137	169.254.255.255									
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255									
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255									
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255									
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255									
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255									
2014-06-06 10:52:37	169.254.1.1	-	137	169.254.255.255									
2014-06-06 10:52:36	169.254.1.1	-	137	169.254.255.255									
2014-06-06 10:52:36	169.254.1.1	-	137	169.254.255.255									
2014-06-06 10:52:36	169.254.1.1	-	137	169.254.255.255									
...					Page 1 of 1			Streaming: ON			Displaying 1 to 38 of 38 items		

SERVICE LOGS			Create Time: 2014-06-06 15:16			Begin: 2014-06-06...					
Date / Time	Host	Message									
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	Id "T0" respawning too fast: disabled for 5 minutes									
2014-06-06 12:14:15	localhost	ttvSO: not a tty									
2014-06-06 12:14:10	localhost	ttvSO: not a tty									
2014-06-06 12:14:05	localhost	ttvSO: not a tty									
2014-06-06 12:14:00	localhost	ttvSO: not a tty									
2014-06-06 12:13:55	localhost	ttvSO: not a tty									
2014-06-06 12:13:49	localhost	ttvSO: not a tty									
2014-06-06 12:13:44	localhost	ttvSO: not a tty									
2014-06-06 12:13:39	localhost	ttvSO: not a tty									
2014-06-06 12:13:34	localhost	ttvSO: not a tty									
2014-06-06 12:13:29	localhost	ttvSO: not a tty									
...			Page 1 of 7			Streaming: ON			Displaying 1 to 50 of 321 items		

List View

In list view you can put widgets in a horizontal order.

FIREWALL LOGS

Create Time: 2014-06-06 15:16

Begin: 2014-06-06 00:00

Q

📄

✕

Date / Time	Source	Source User	Source Port	Destination	Destination User	Destination...	Rule	Action	Protocol	Application
2014-06-06 10:53:07	169.254.1.1	-	138	169.254.255.255	-	138	Ifp OUT MNG IF	DROP	UDP	CIFS CIFS
2014-06-06 10:53:06	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:53:05	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:53:04	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:53:02	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:53:01	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:53:00	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:59	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:57	169.254.1.1	-	138	169.254.255.255	-	138	Ifp OUT MNG IF	DROP	UDP	CIFS CIFS
2014-06-06 10:52:57	169.254.1.1	-	137	169.254.255.255	-	137	Ifp OUT MNG IF	DROP	UDP	NTBIOSNS NetBIOS Nar
2014-06-06 10:52:55	169.254.1.1	-	138	169.254.255.255	-	138	Ifp OUT MNG IF	DROP	UDP	CIFS CIFS
2014-06-06 10:52:53	169.254.1.1	-	138	169.254.255.255	-	138	Ifp OUT MNG IF	DROP	UDP	CIFS CIFS

...

⏪ ⏩

Page 1 of 1

⏪ ⏩

🔄 Streaming: ON

Displaying 1 to 38 of 38 items

SERVICE LOGS

Create Time: 2014-06-06 15:16

Begin: 2014-06-06 00:00

Q

📄

✕

Date / Time	Host	Message
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	Id "T0" respawning too fast: disabled for 5 minutes
2014-06-06 12:14:15	localhost	ttvSO: not a tty
2014-06-06 12:14:10	localhost	ttvSO: not a tty
2014-06-06 12:14:05	localhost	ttvSO: not a tty
2014-06-06 12:14:00	localhost	ttvSO: not a tty
2014-06-06 12:13:55	localhost	ttvSO: not a tty
2014-06-06 12:13:49	localhost	ttvSO: not a tty
2014-06-06 12:13:44	localhost	ttvSO: not a tty
2014-06-06 12:13:39	localhost	ttvSO: not a tty
2014-06-06 12:13:34	localhost	ttvSO: not a tty
2014-06-06 12:13:29	localhost	ttvSO: not a tty

...

⏪ ⏩

Page 1 of 7

⏪ ⏩

🔄 Streaming: ON

Displaying 1 to 50 of 321 items

FIREWALL LOGS

Create Time: 2014-06-06 15:17Begin: 2014-06-0...

Date / Time	Source	Source User	Source Port	Destination
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

Page 1 of 1

Streaming: ON

Displaying 1 to 38 of 38 items

ADMINISTRATIVE LOGS

Create Time: 2014-06-06 15:17Begin: 20...

Date / Time	Host	Message
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

Page 1 of 1

Streaming: ON

Displaying 1 to 4 of 4 items

FIREWALL LOGS

Create Time: 2014-06-06 15:16Begin: 2014-06-0...

Date / Time	Source	Source User	Source Port	Destination
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

Page 1 of 1

Streaming: ON

Displaying 1 to 38 of 38 items

SERVICE LOGS

Create Time: 2014-06-06 15:16Begin: 2014-06-06...

Date / Time	Host	Message
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 "T0" respawning too fast: disabled for 5 minutes
2014-06-06 12:14:15	localhost	tyS0: not a tty
2014-06-06 12:14:10	localhost	tyS0: not a tty
2014-06-06 12:14:05	localhost	tyS0: not a tty
2014-06-06 12:14:00	localhost	tyS0: not a tty
2014-06-06 12:13:55	localhost	tyS0: not a tty
2014-06-06 12:13:49	localhost	tyS0: not a tty
2014-06-06 12:13:44	localhost	tyS0: not a tty
2014-06-06 12:13:39	localhost	tyS0: not a tty
2014-06-06 12:13:34	localhost	tyS0: not a tty
2014-06-06 12:13:29	localhost	tyS0: not a tty

Page 1 of 7

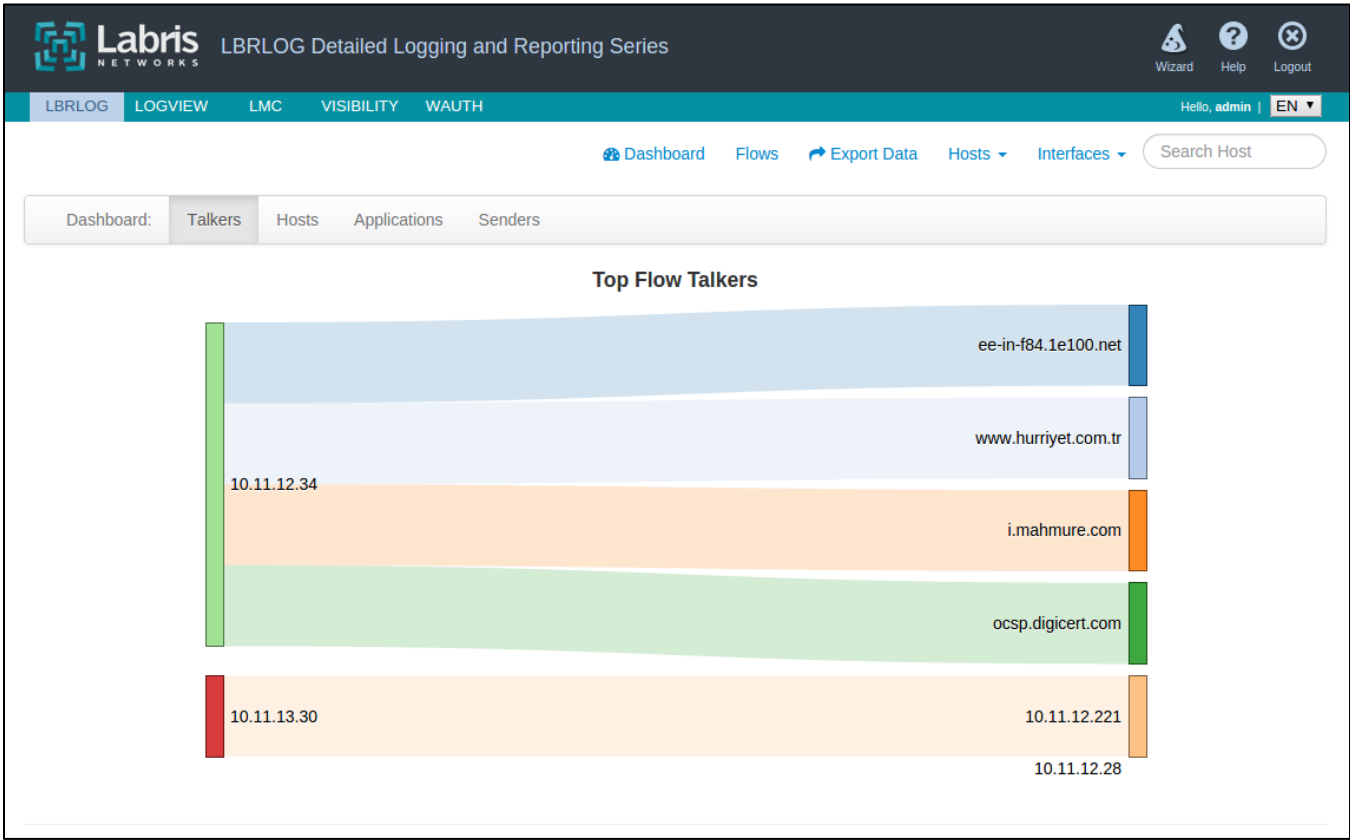
Streaming: ON

Displaying 1 to 50 of 321 items

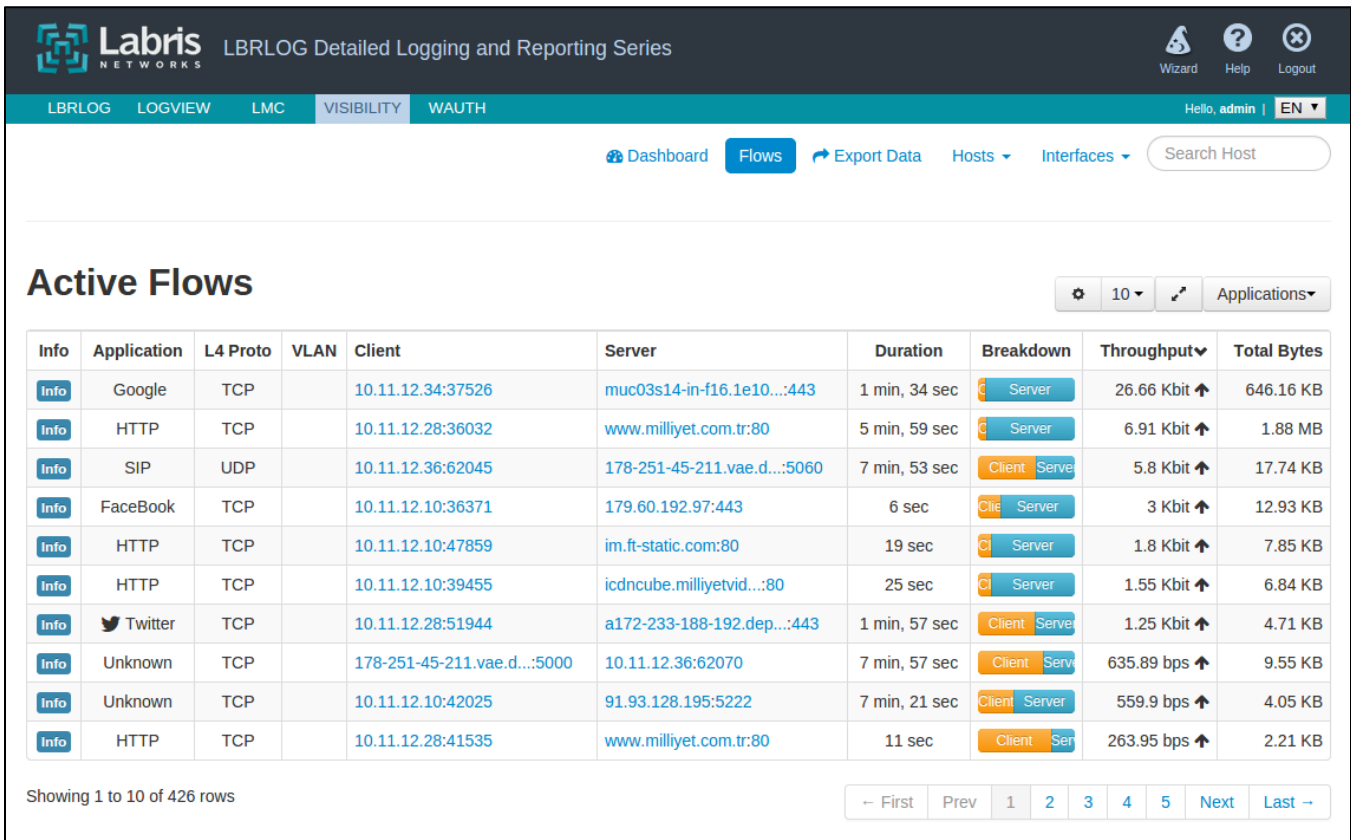
This view helps you to compare or watch 4 different log sources in tables.

Network Visibility

Visibility is the web based tool for monitoring a network. This tool provides visibility for the network, including current traffic, application and more detailed information. Important functionality is listed as below.



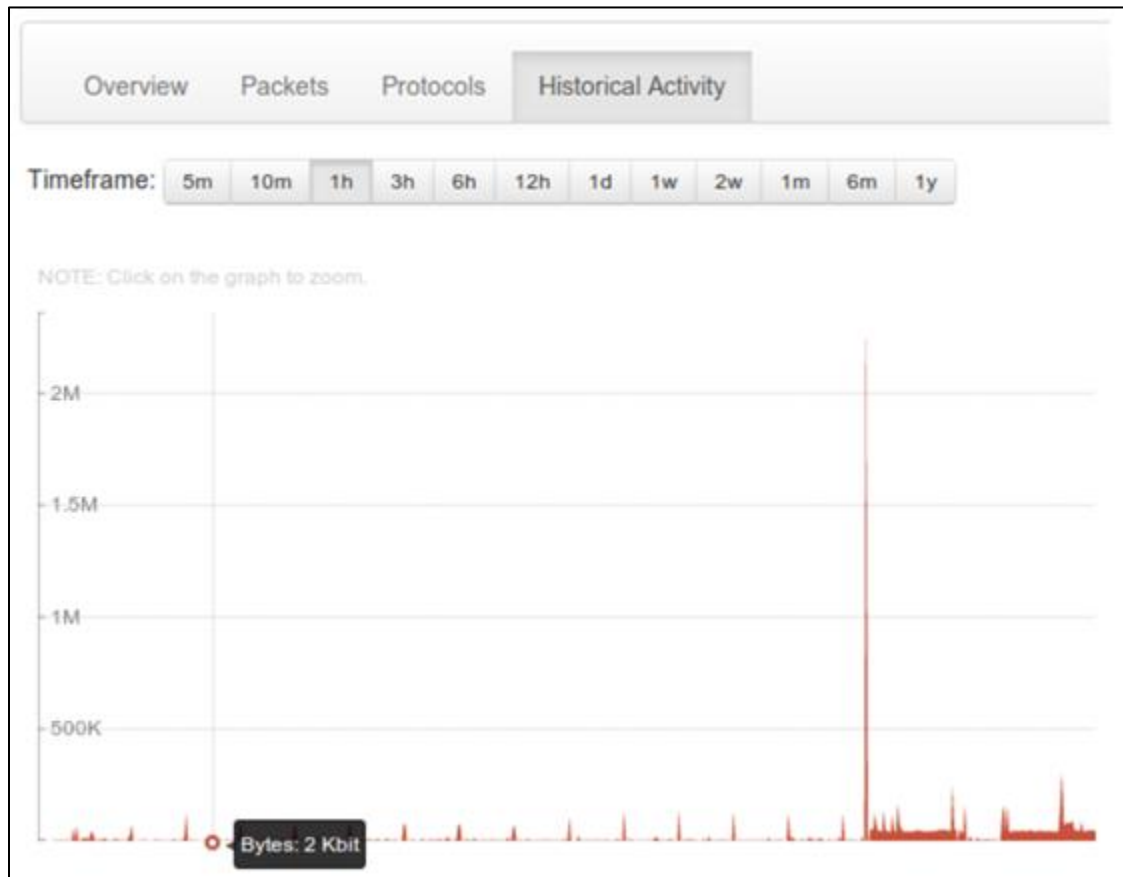
a. All active flows are monitored bi-directionally.



b. Current usage in selected interface:



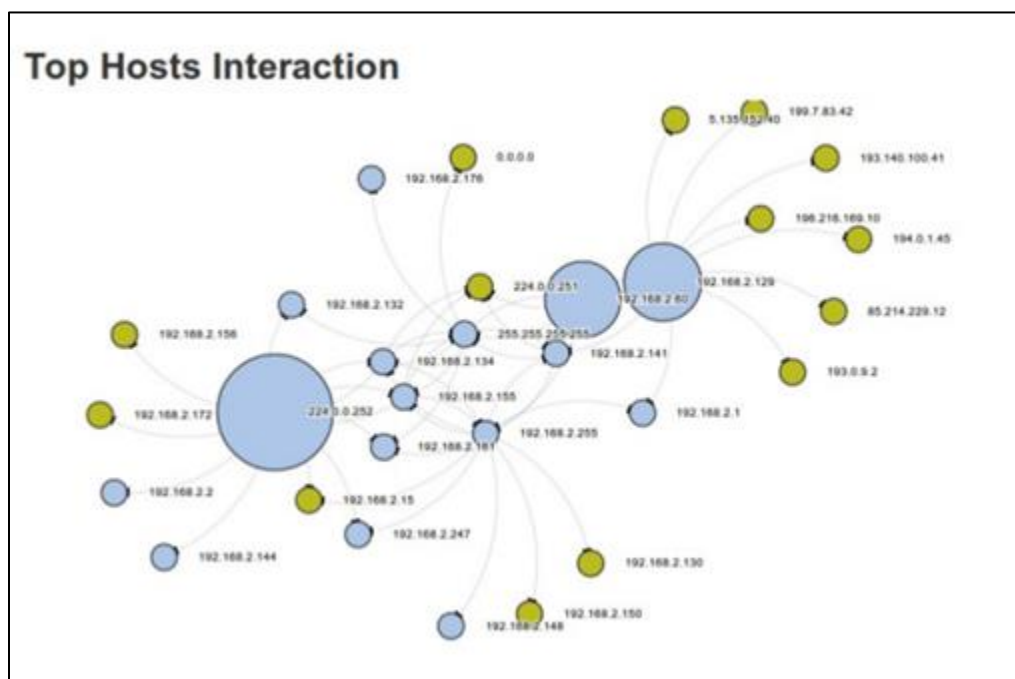
c. Detailed traffic flow in internal and external interface



d. Smart search feature list all traffic generating hosts.



e. All connections are shown in highly interactive graph view.



f. Each IP and hosts has a separate detailed information screen.

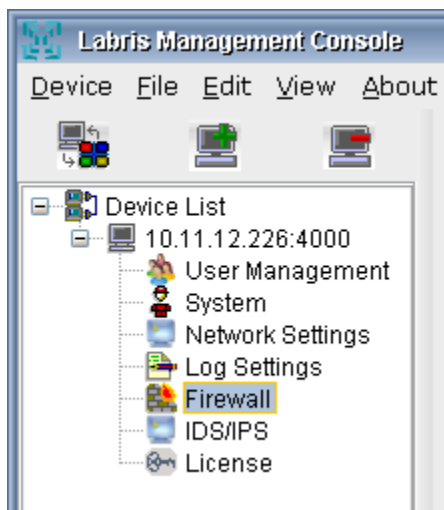
Host: 192.168.2.60		Overview	Traffic	Packets	Protocols	Flows	Talkers	Contacts
(Router) MAC Address	5C:F9:DD:4F:22:18							
IP Address	192.168.2.60							
Name	192.168.2.60 Remote Private IP							
First Seen	03/06/2014 09:09:51 [39 min, 33 sec ago]							
Last Seen	03/06/2014 09:49:25 [< 1 sec ago]							
Sent vs Received Traffic Breakdown	<div><div>Sent</div><div>Rcvd</div></div>							
Traffic Sent	51,352 Pkts / 6.73 MB ↑							
Traffic Received	45,423 Pkts / 6.64 MB ↑							

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**.



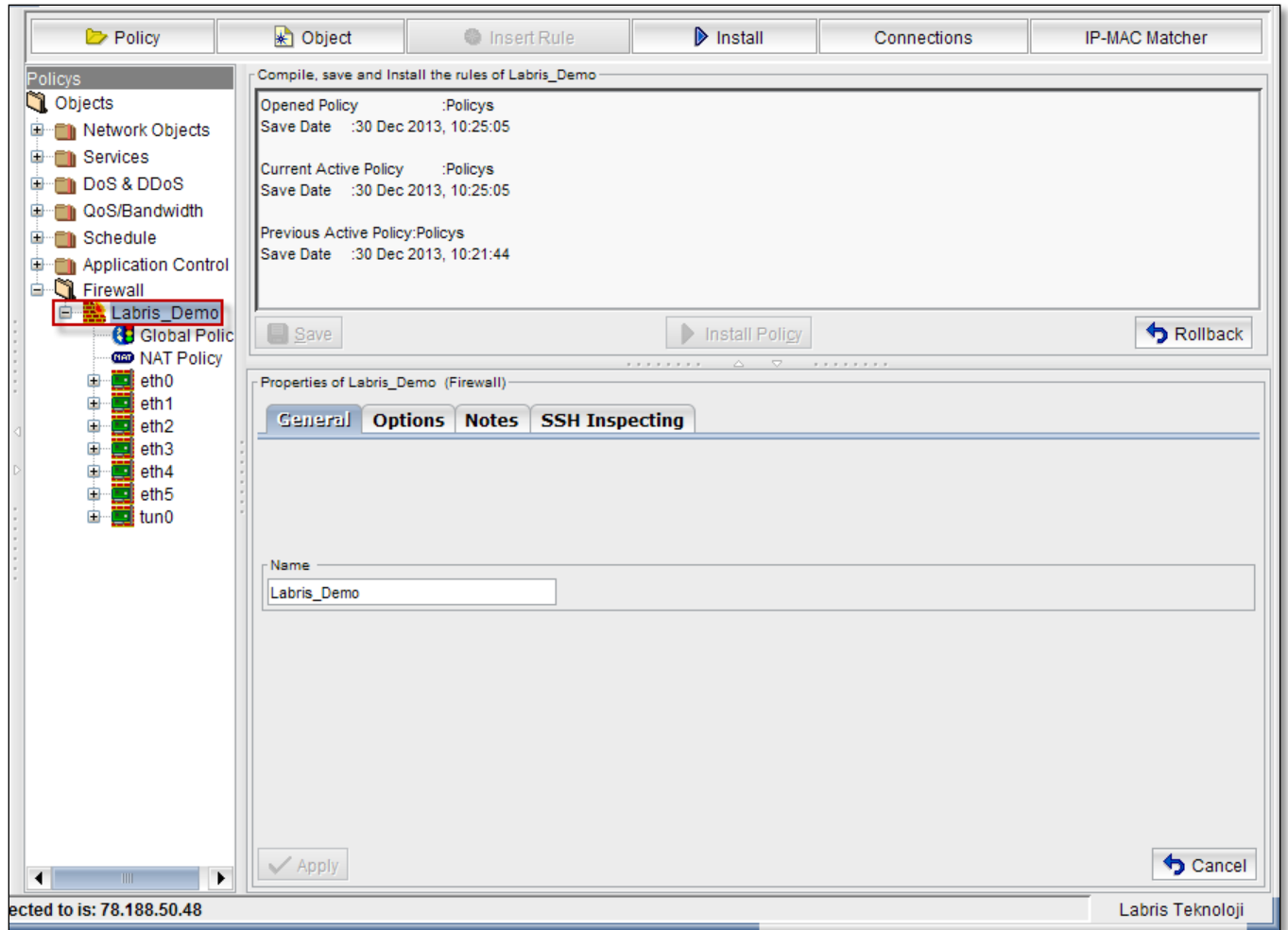
Make a new firewall object

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.

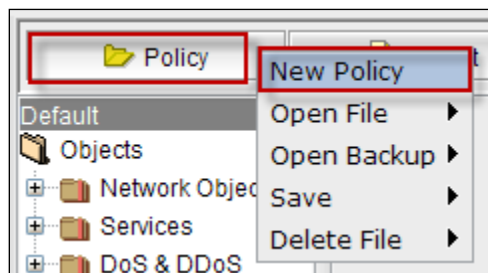
By default, all incoming traffic from outside a network is blocked and without an appropriate firewall rule, no packet is allowed into an instance. You need to set up firewalls to allow incoming network traffic to permit these connections. Each firewall represents a single rule that determines what traffic 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, and Mask** are selected by default.

Click on **Add** tab.

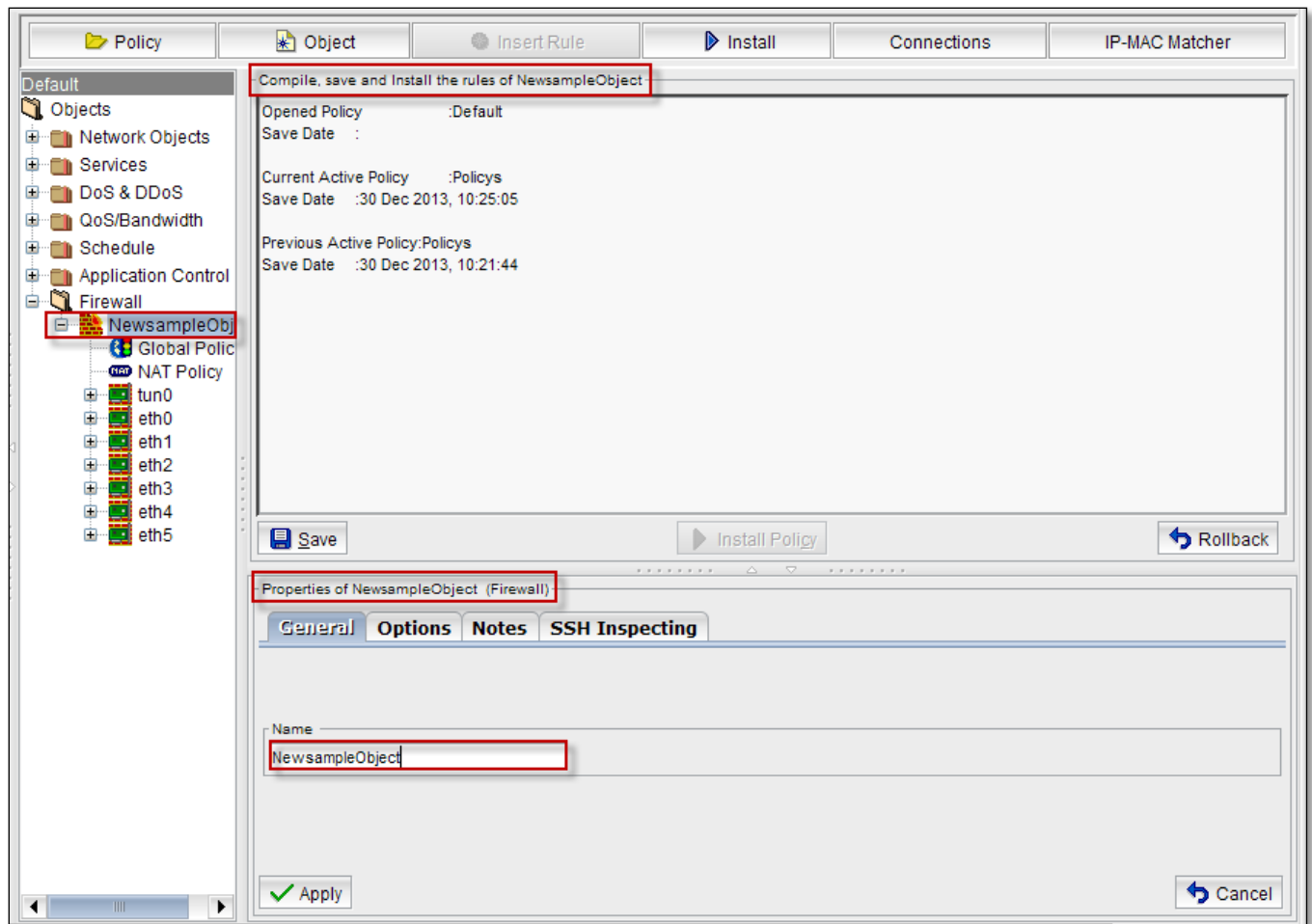
We can notice new firewall object under firewall.

It consists of two fields.

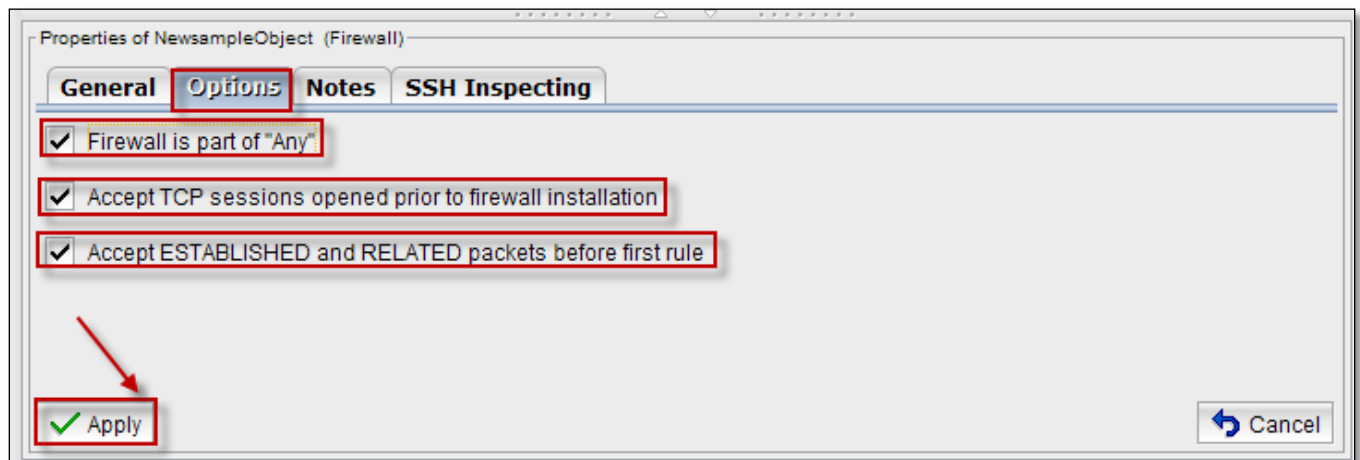
Compile, Save and Install the rules of new firewall object field displays information regarding newly added object to the firewall.

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

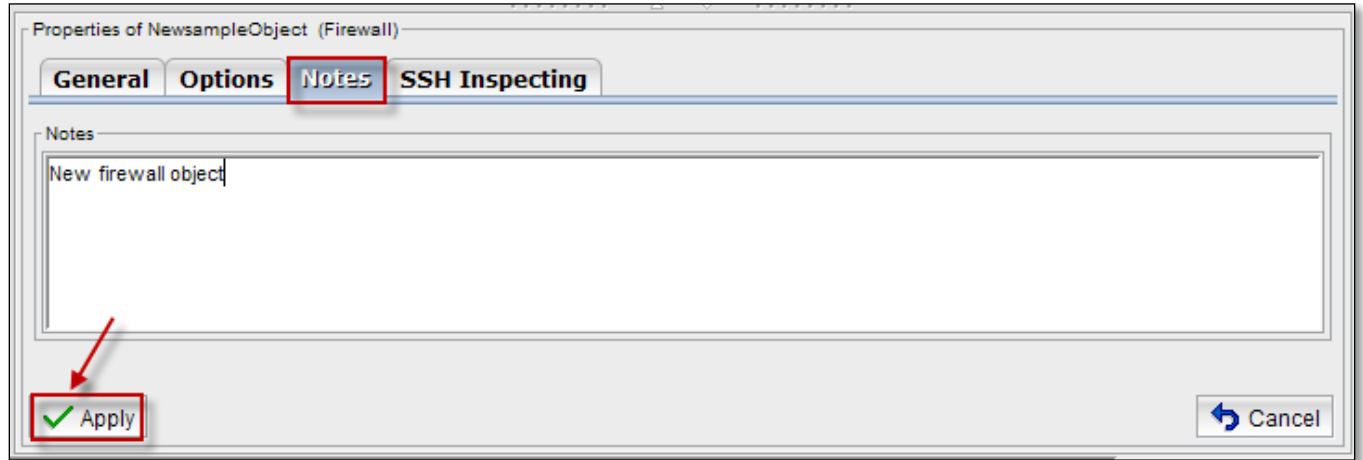
Under **General** tab, the name of the new firewall object is displayed



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.



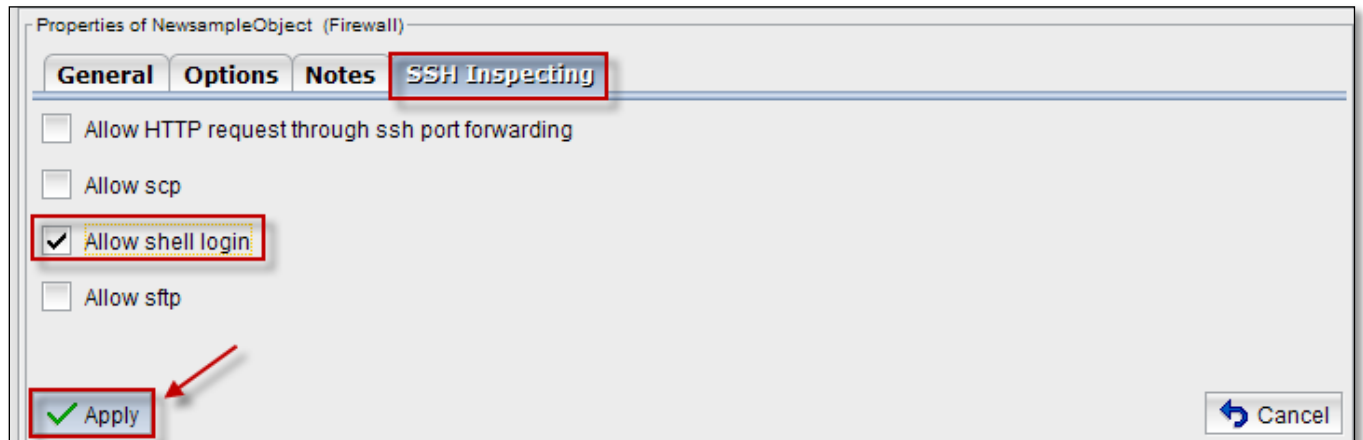
Under **Notes tab**, we can describe any points regarding new firewall Object and click on **Apply tab**.



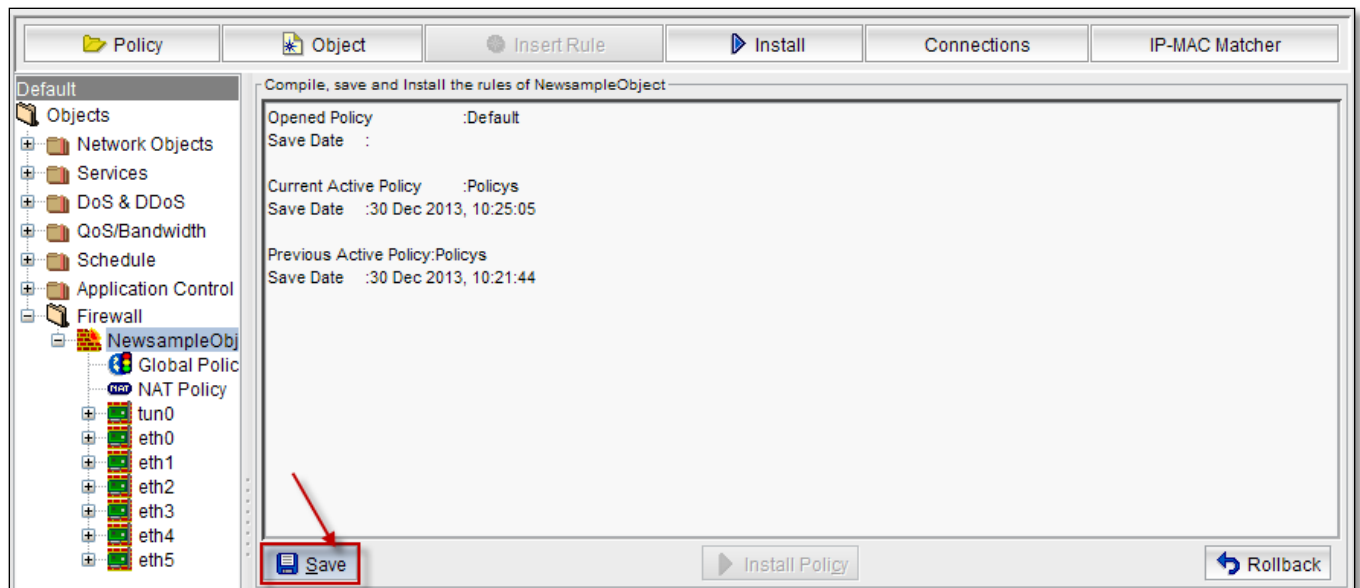
SSH inspecting

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.

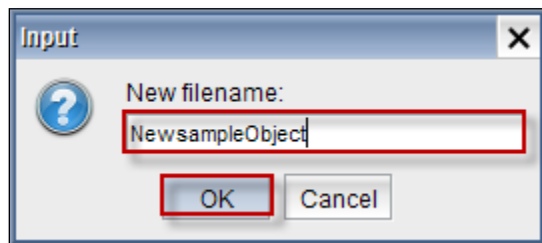
In **SSH Inspecting tab**, we can check mark options like **Allow HTTP request through ssh port forwarding**, **Allow scp**, **Allow shell login**, **Allow sftp** and click on **Apply tab** to apply them to the firewall object.



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



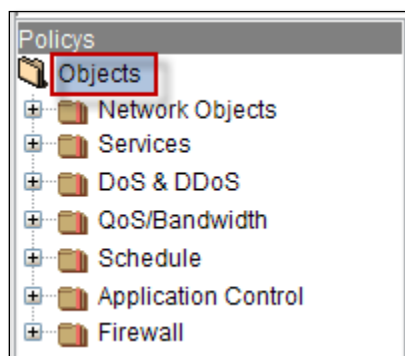
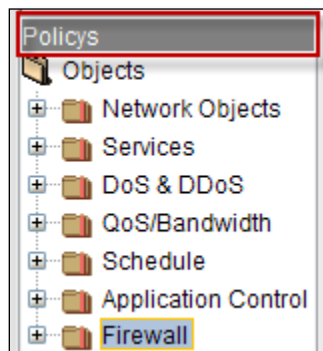
Objects

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 LOG 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**.

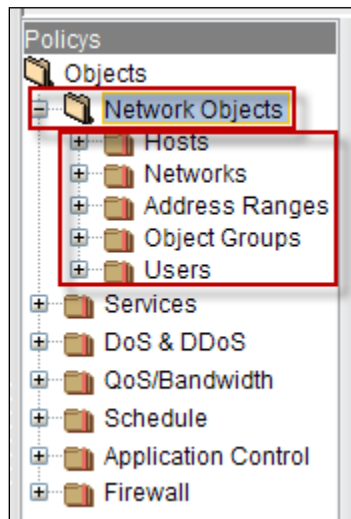


Network Objects

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.

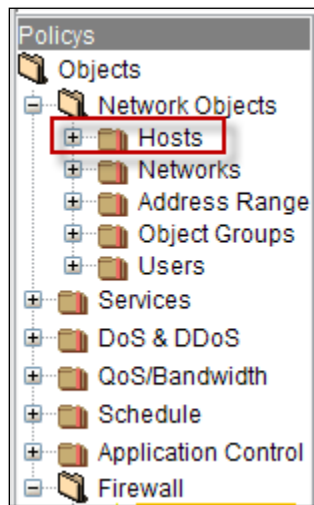
It consists of **Hosts**, **Networks**, **Address Ranges**, **Object Groups**, **Users**.



Brief Summary about each of the parameters in Network Objects:

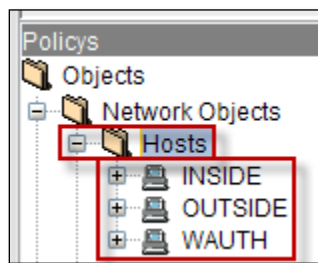
1	Hosts	It enables us to Add new Host
2	Networks	It enables us to Add new Networks
3	Address Ranges	It enables us to Create new Address Range
4	Objects Groups	It enables us to Add new Object Groups
5	Users	It enables us to Add new User Groups

Hosts

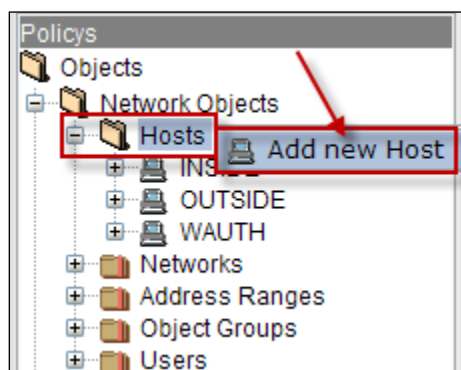


Expand Hosts, by default it consists of three Hosts.

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)

Make a new Host object

General Notes

Name
Newhost

Interface

Name interface1

IP: 10 . 0 . 0 . 1

MAC(optional): 00 : 00 : 00 : 00 : 00 : 00

+ Add Cancel X Delete

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.

Properties of Newhost (Host)

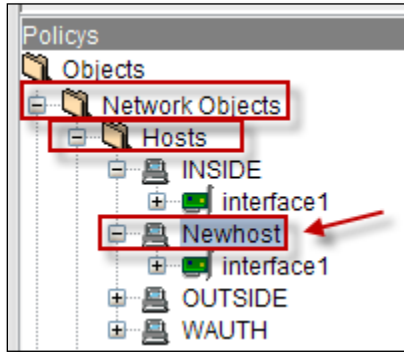
General Notes

Notes

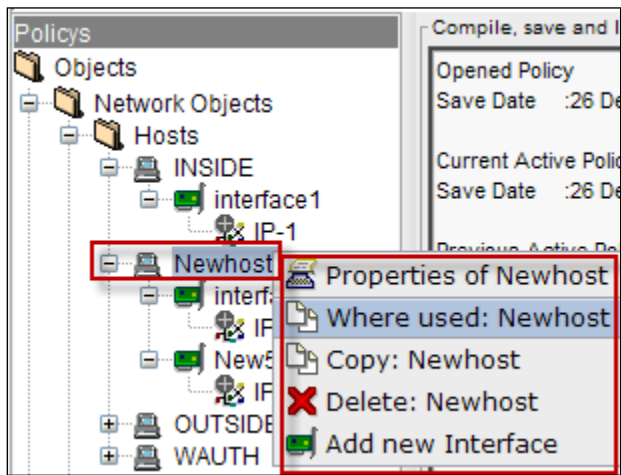
New Host is added to the Network objects
Interface of Newhost is 1
IP Address:10.0.0.1

✓ Apply Cancel X Delete

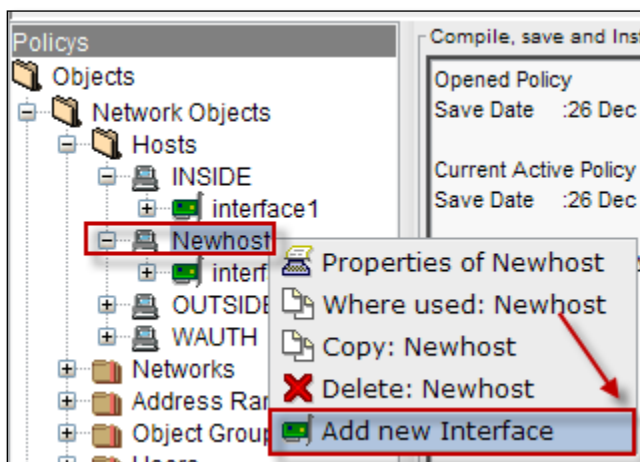
We can notice newly added Host under the Hosts list with selected type of the Interface.



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.



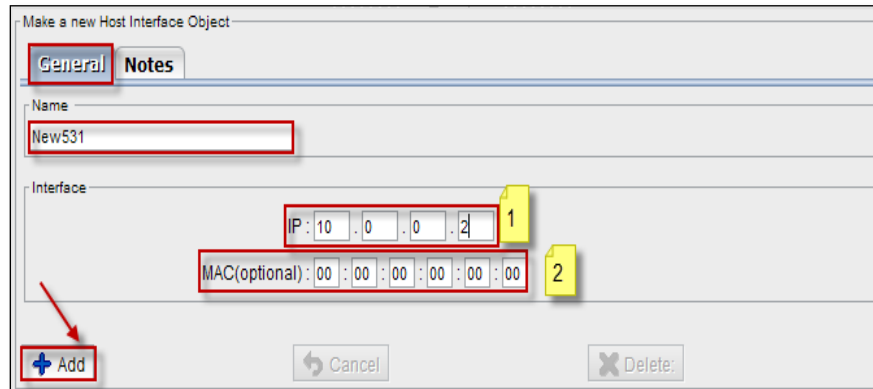
Below screen appears, Select **General** tab.

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:

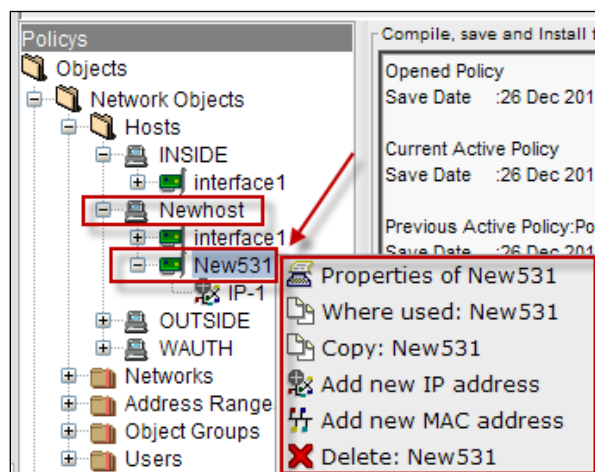
1	IP	Give the IP Address of the Interface
2	MAC(Optional)	Give the MAC Address (Optional)



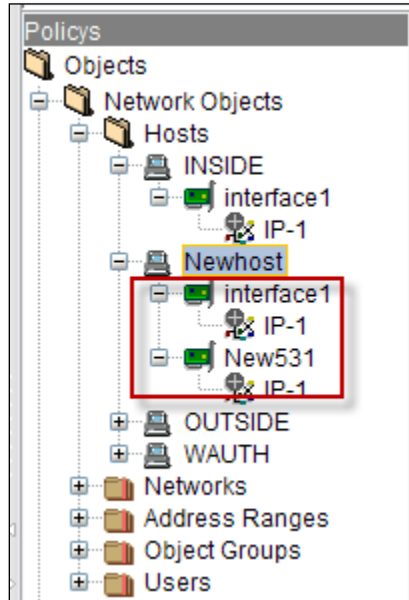
Click on **Add** tab.

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

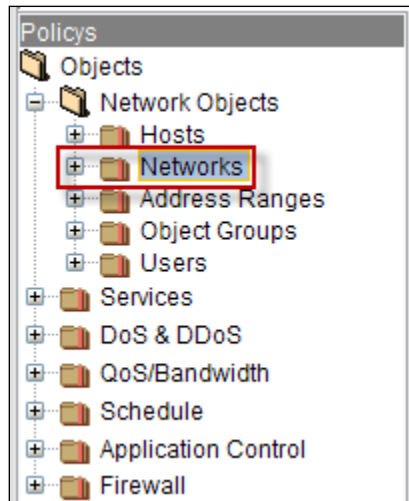
Right click on the Interface to perform actions like viewing **Properties** of the Interface, to find out where it is used, **copying** Interface, **Adding new IP address** to the Interface, **Adding new MAC address** to the Interface and **Deleting** Interface.



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

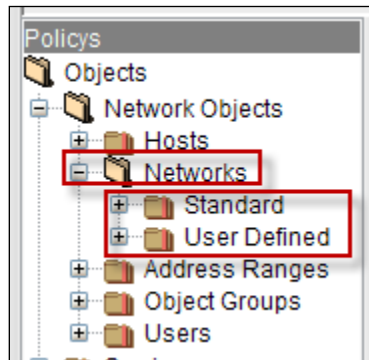


Networks

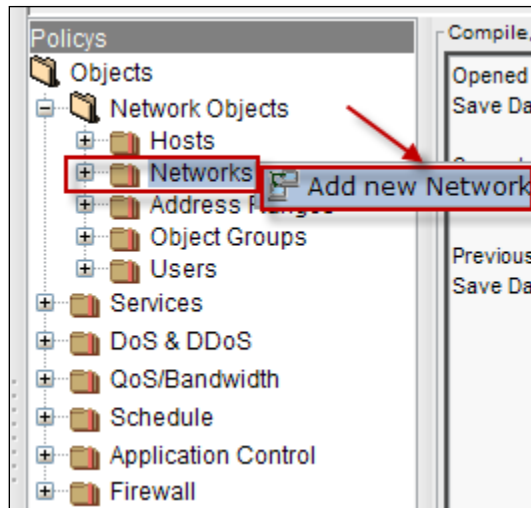


Expand Networks, by default it consists of two Network

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)

Make a new Network object

General Notes

Name
Newnetwork

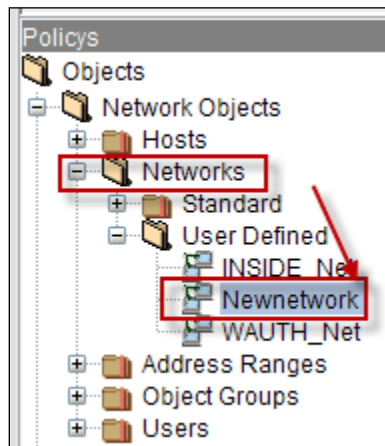
IP and Mask

IP	10	.	0	.	0	.	3
Mask	255	.	255	.	255	.	0

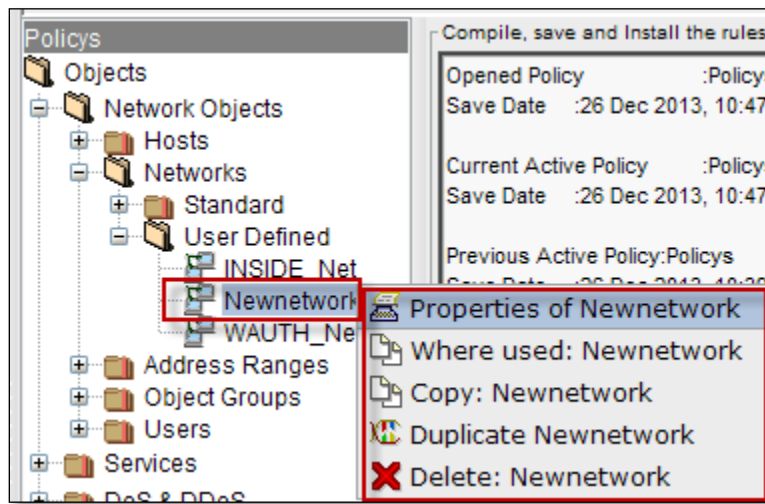
+ Add Cancel Duplicate Delete

Click on **Add** tab.

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



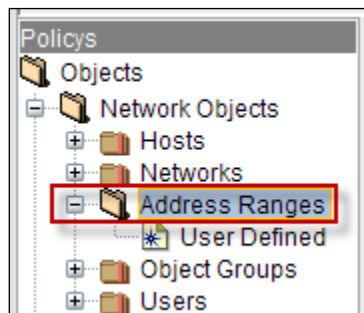
Right click on added Network, to perform actions like viewing **Properties** of the Network, to find out where it is used, **copying** Network, **Duplicating** Network and **Deleting** Network.



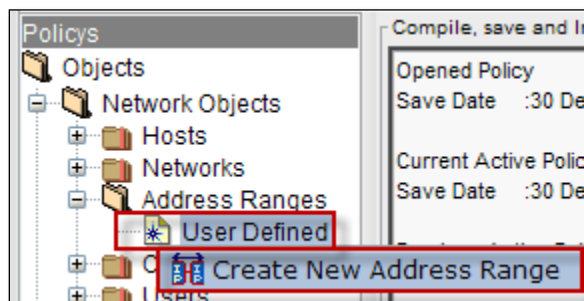
Address Ranges



Expand Address Ranges, User Defined is displayed



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



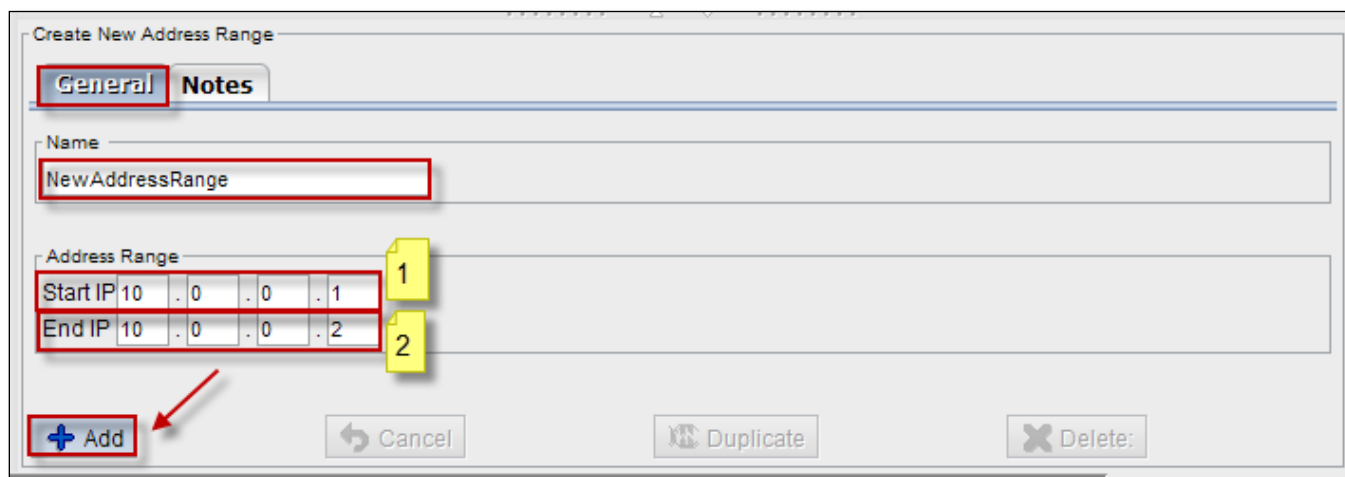
Below screen appears, Select **General** tab.

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:

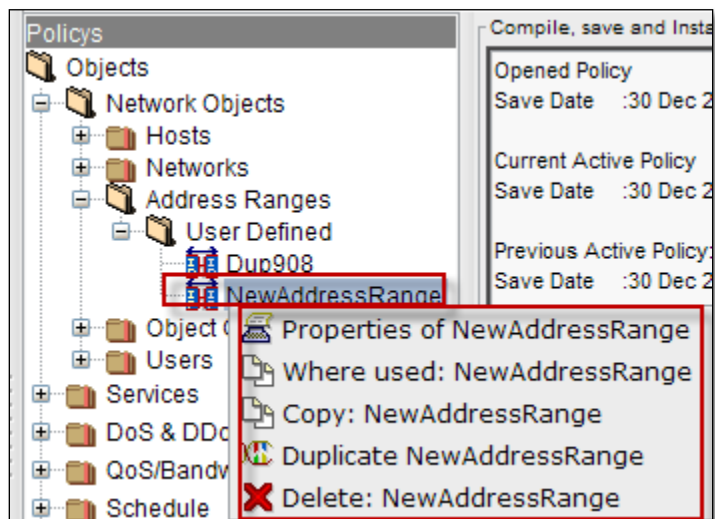
1	Start IP	Give the IP Address of the Interface
2	End IP	Give the MAC Address (Optional)



Click on **Add** tab.

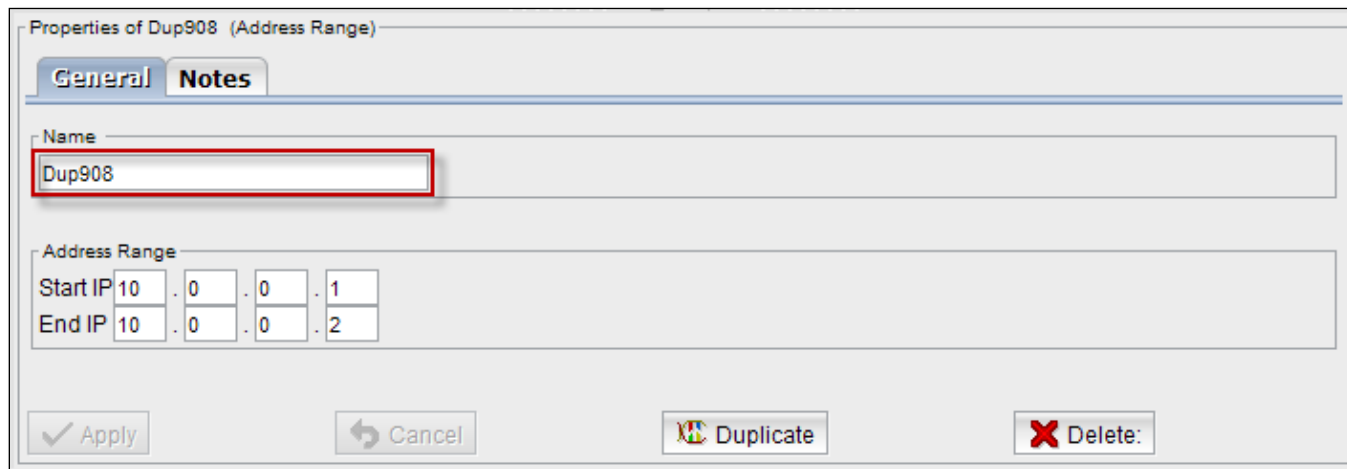
We can notice the new Address Range in the below screen.

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.

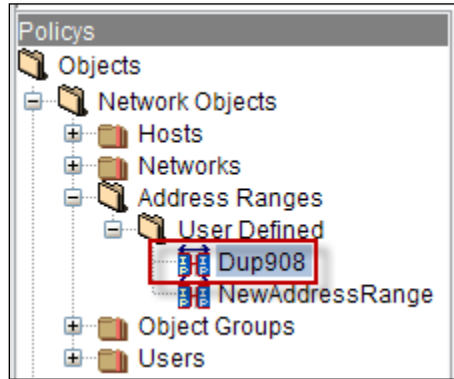


When we click on Duplicate **New Address Range**, below screen appears.

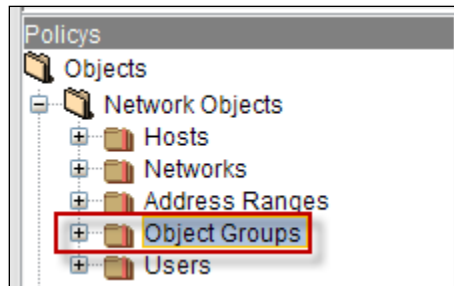
In which it displays **Name** of the Duplicate Address Range and **Address Range**.



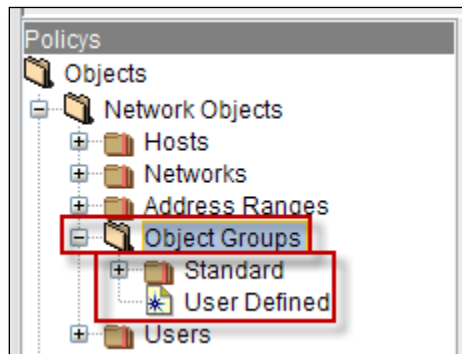
We can notice **Duplicate Address Range** under User Defined list.



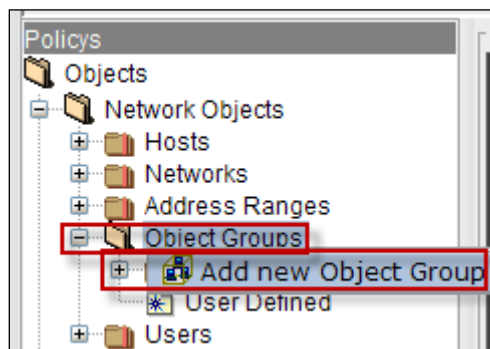
Object Groups



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



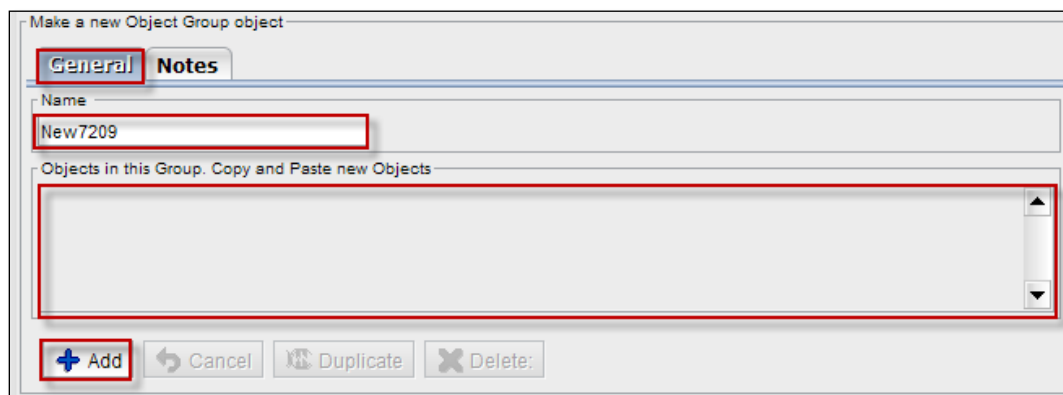
Right click on Object Groups, to add new object Group.



Below screen appears.

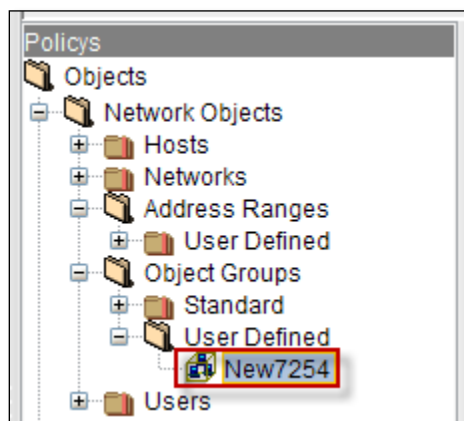
Select **General** tab, give the name of the new Object Group.

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

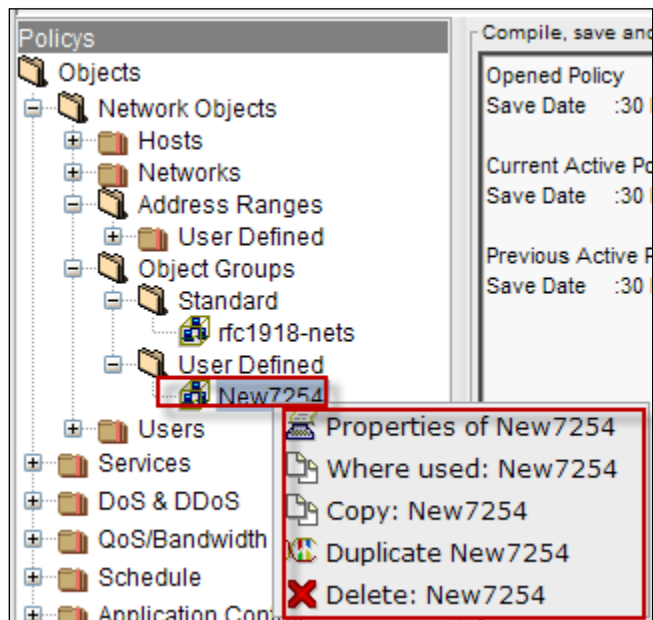


Click on **Add** tab.

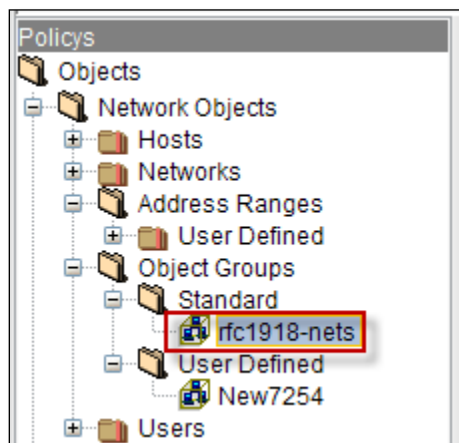
We can notice new **Object Group** in the **User Defined**.



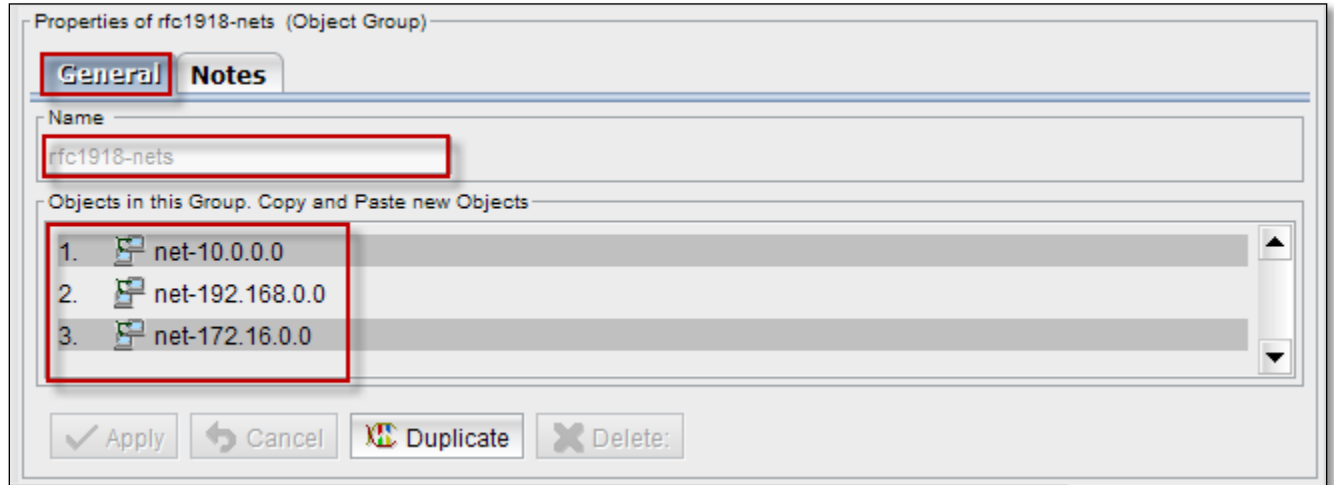
Right click on the **Object Group**, to perform actions like viewing **Properties** of the Object Group, to find out where it is used, **copying** Object Group, **Duplicating** Object Group and **Deleting** Object Group.



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

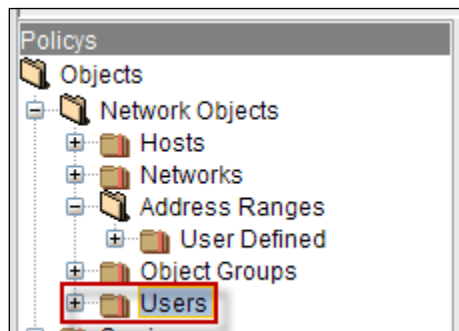


We can notice name of the **Object Group** and list of objects in the Group.

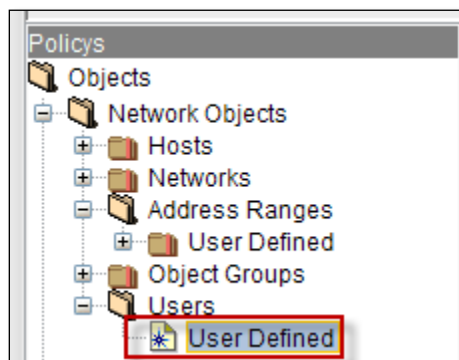


Users

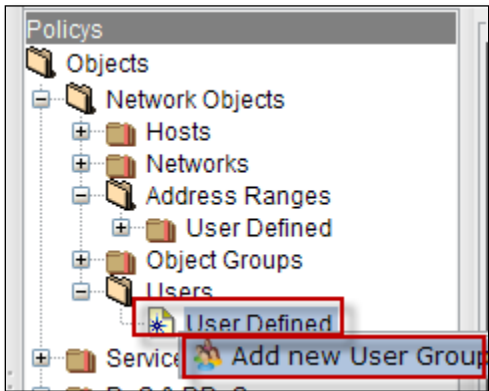
Expand **Users**.



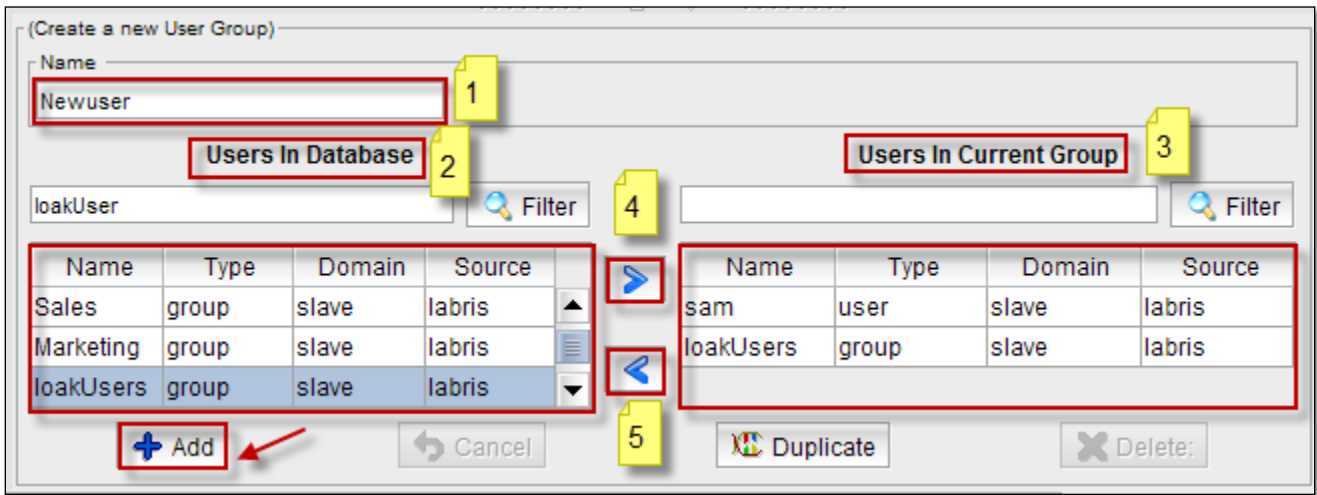
By default **User Defined** is displayed.





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



Below screen appears.

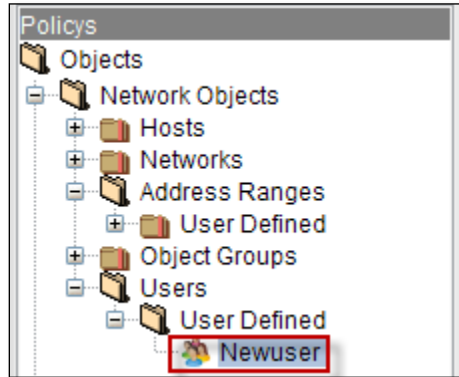


These are the inputs two add new **User Group**:

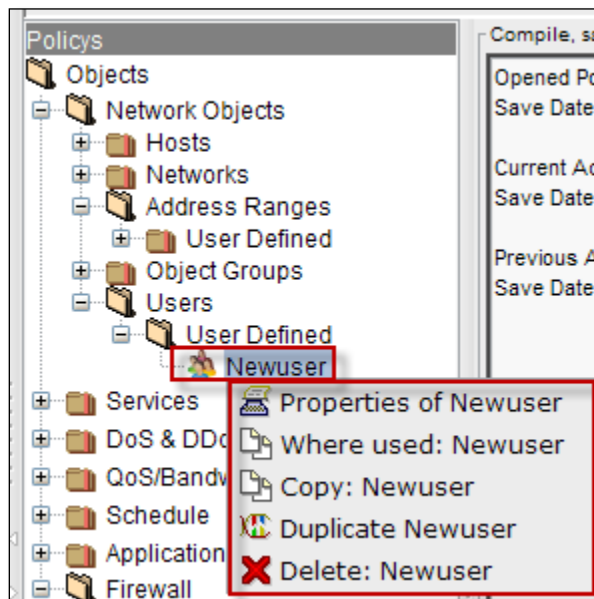
1	Name	Type Name of the new User Group
2	Users in Data base	Displays Users in Data base
3	Users in Current Group	Displays Users in Current Group
4		It enables to add Users from Database to Current Group
5		It enables to remove Users from Current Group

Click on **Add** tab.

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

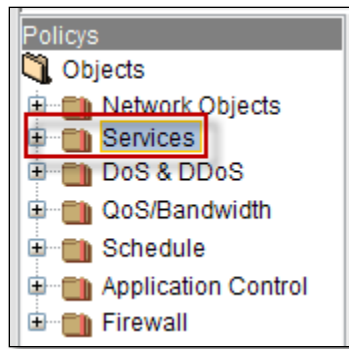


Right click on the User Group, to perform actions like viewing **Properties** of the User Group, to find out where it is used, **copying** User Group, **Duplicating** User Group and **Deleting** User Group.

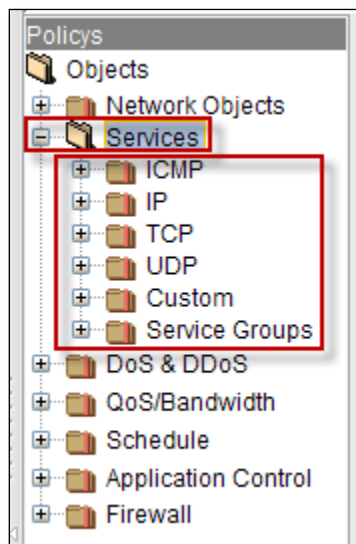


Services

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).

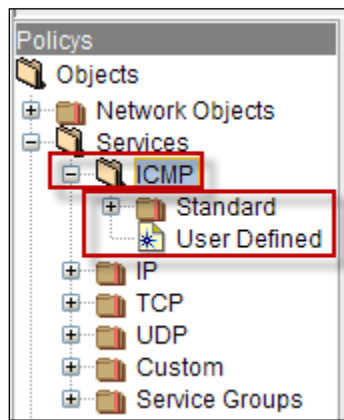


Expand **Services**, service Objects **ICMP**, **IP**, **TCP**, **UDP**, **Custom**, **Service Groups** are displayed

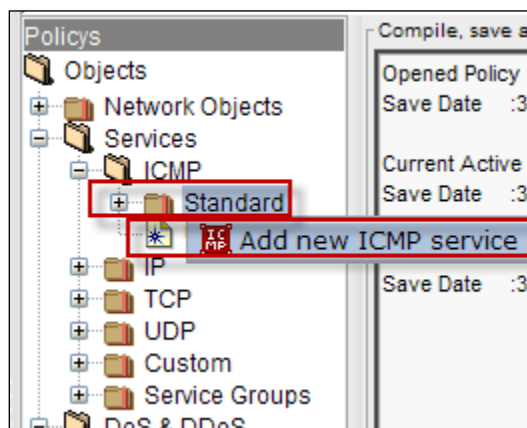


ICMP

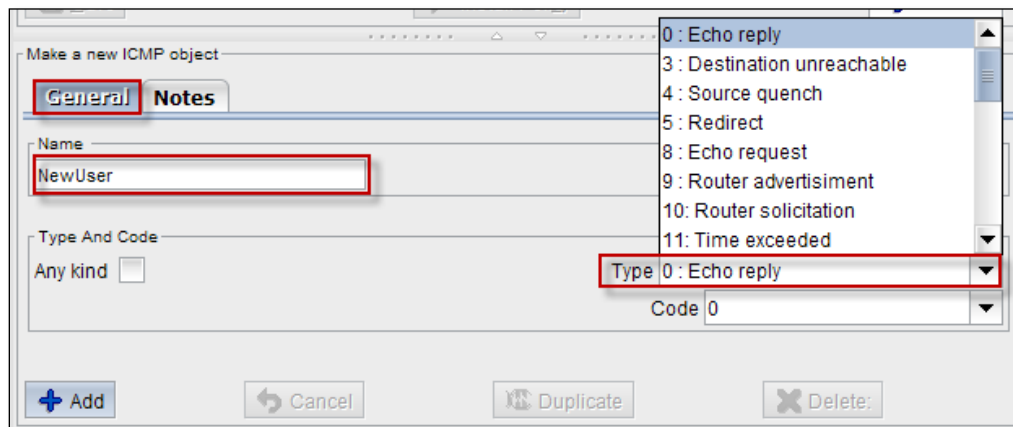
Expand **ICMP**, by default **Standard** and **User Defined**.



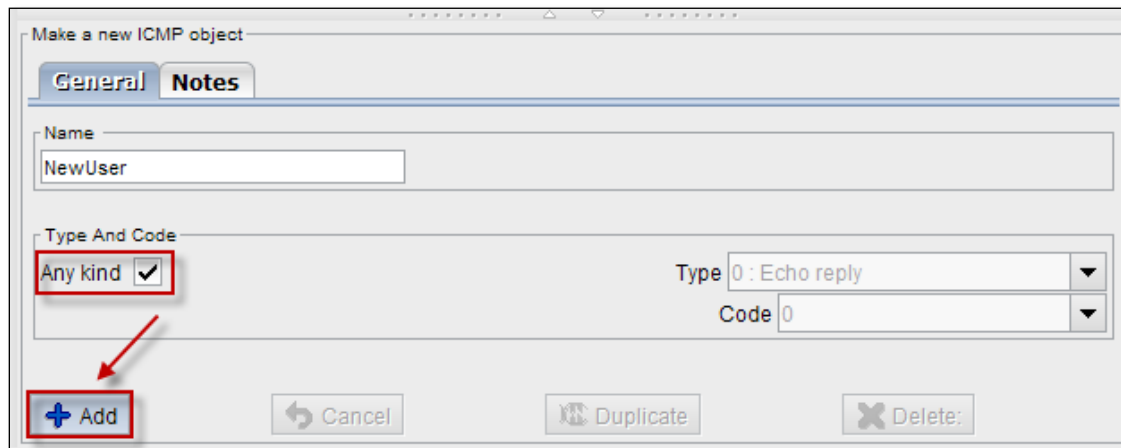
Right click on **Standard**, to add new **ICMP** service



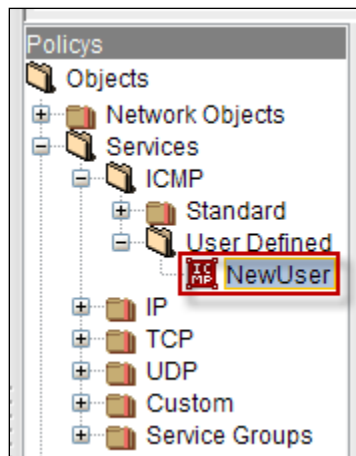
Select **General** tab, to give the name of the **ICMP** object and choose the type of object from the drop down list in the **Type** tab



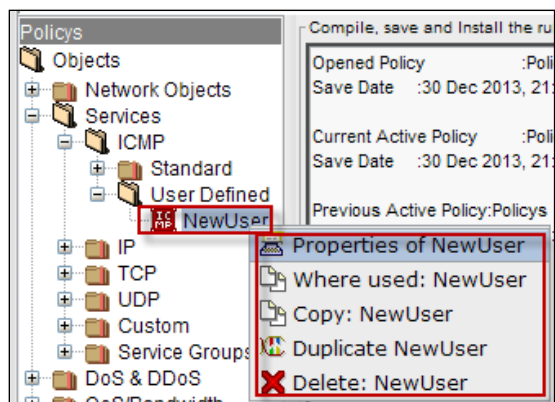
Enable **Any kind** option and click on **Add** tab



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

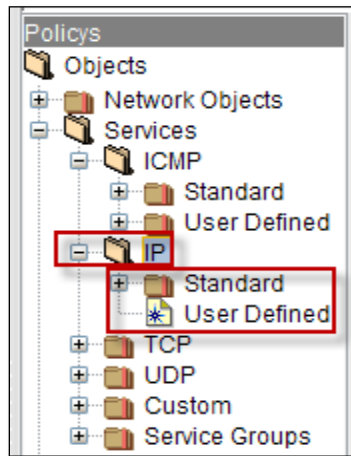


Right click on the new ICMP Service object, to perform actions like viewing **Properties** of the ICMP Service object, to find out where it is used, **copying** ICMP Service object, **Duplicating** and **Deleting** ICMP Service object.

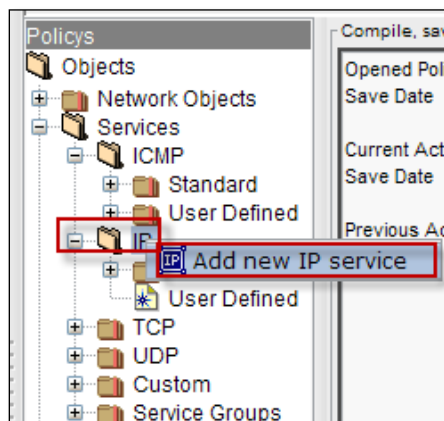


IP

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

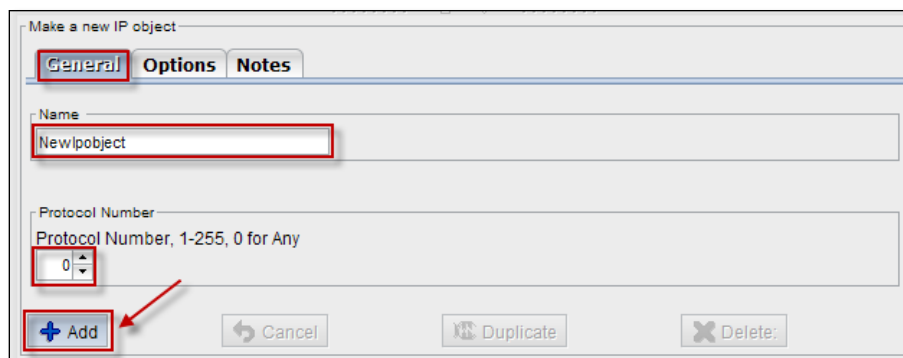


Right click on **IP**, to add new **IP** service

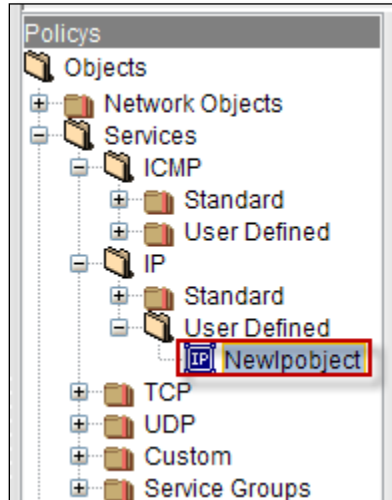


Select **General** tab, give the name of the **IP** object and choose Protocol Number.

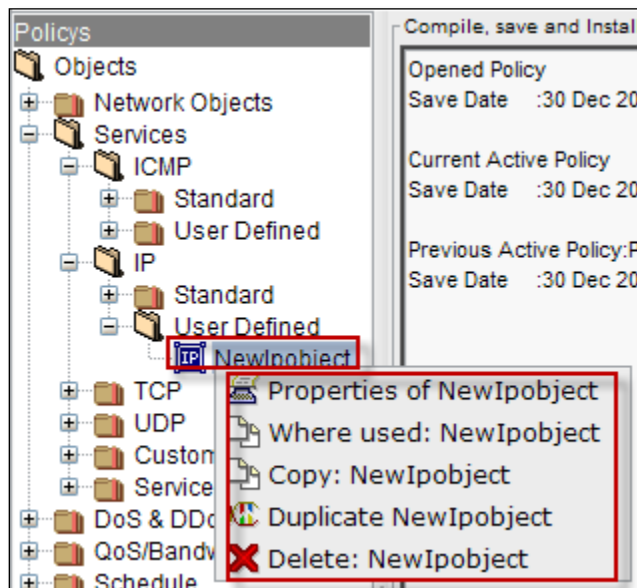
Click on **Add** tab.



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

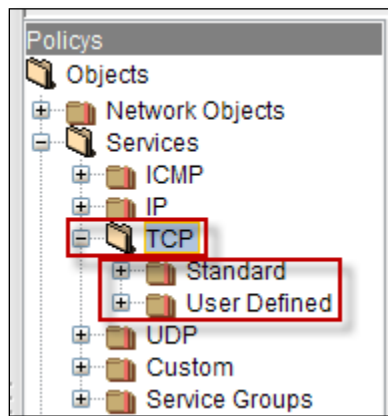


Right click on the new IP Service object, to perform actions like viewing **Properties** of the IP Service object, to find out where it is used, **copying** IP Service object, **Duplicating** and **Deleting** IP Service object.

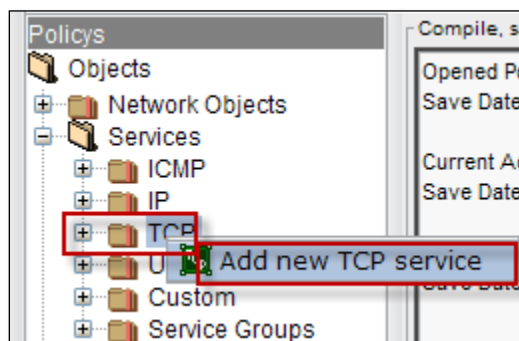


TCP

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

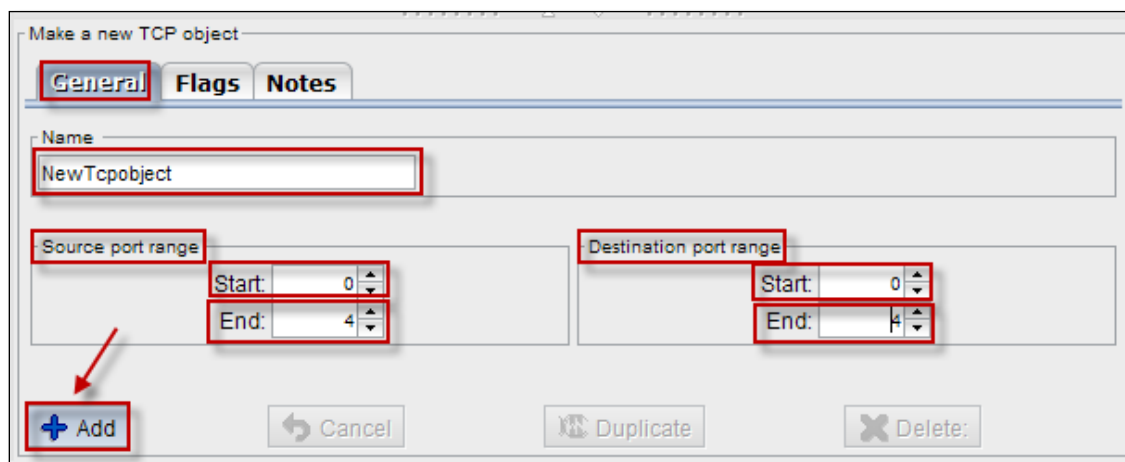


Right click on **TCP**, to add new **TCP** service.



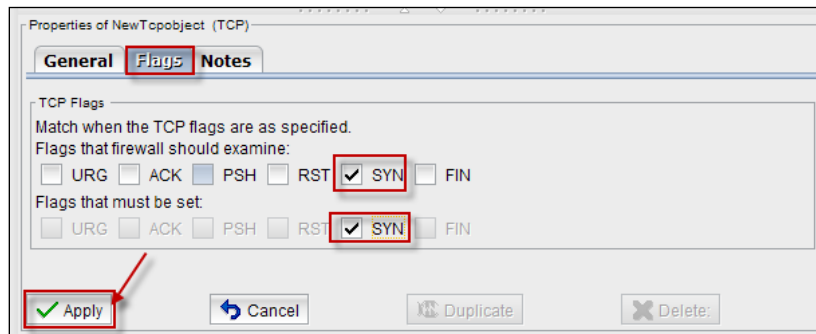
Select **General** tab, give the **Name** of the TCP object and choose **Source port range**, **Destination port range**.

Click on **Add** tab.

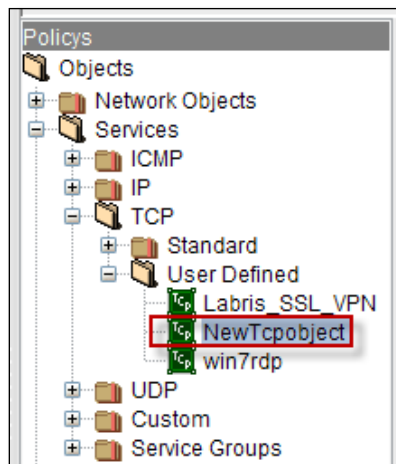


Select **Flags tab**, to enable Flags which need to be examined by the firewall.

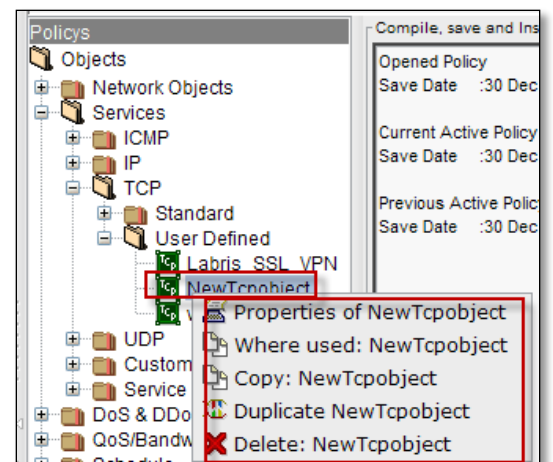
Click on **Apply tab**.



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

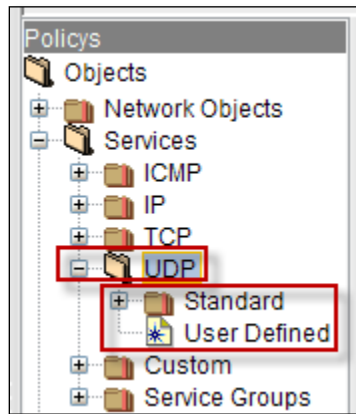


Right click on the new TCP Service object, to perform actions like viewing **Properties** of the TCP Service object, to find out where it is used, **copying** TCP Service object, **Duplicating** and **Deleting** TCP Service object.

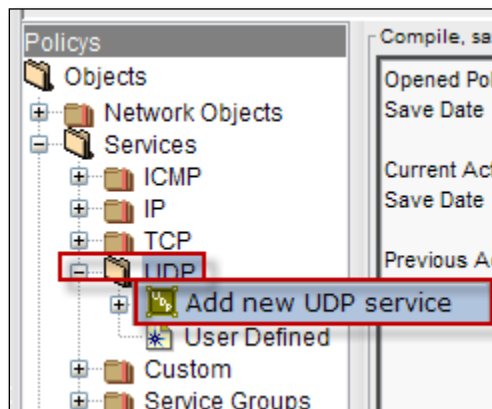


UDP

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

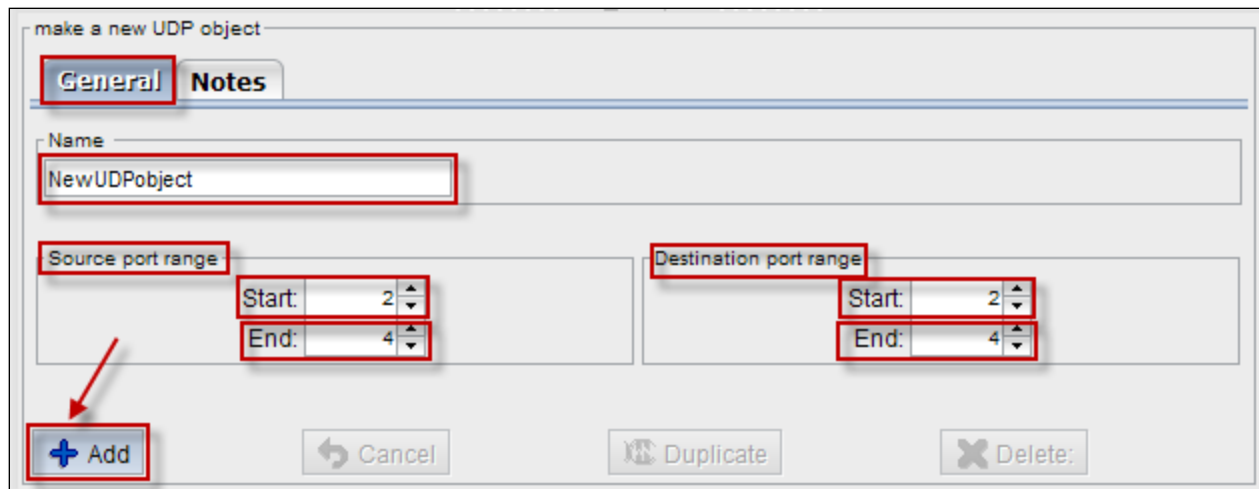


Right click on **UDP**, to add new **UDP** service.

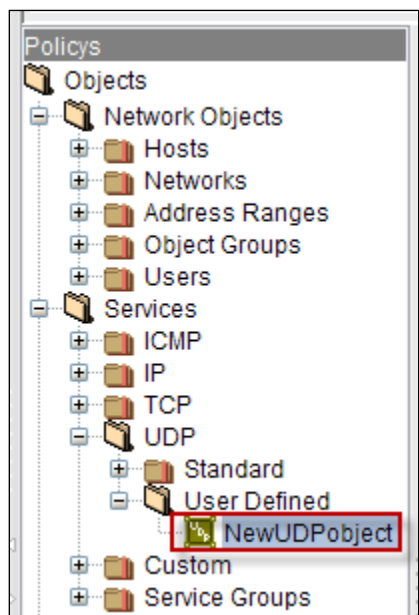


Select **General tab**, give the **Name** of the UDP object and choose **Source port range**, **Destination port range**.

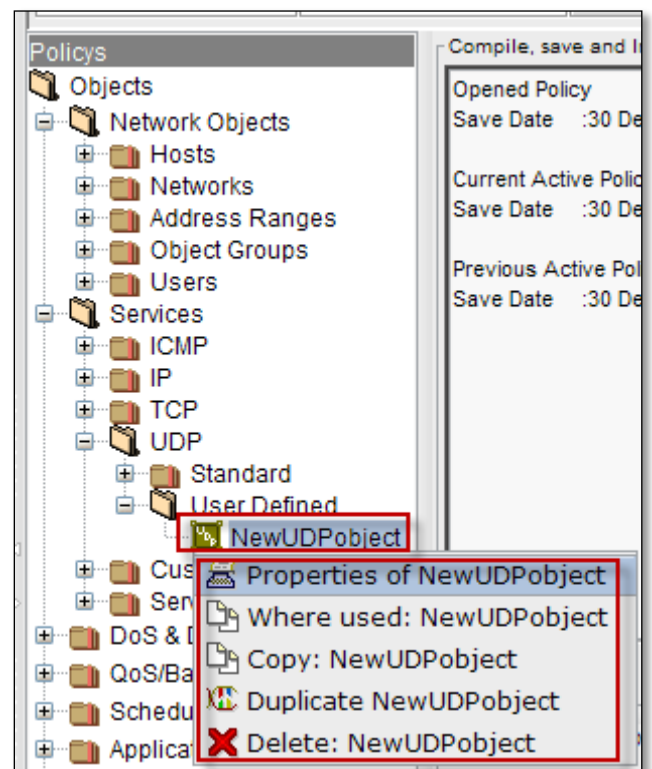
Click on **Add tab**.



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

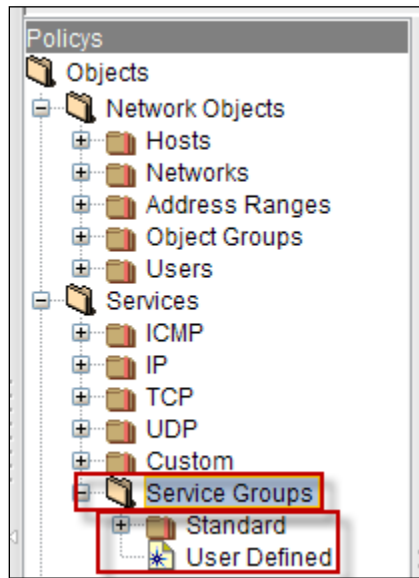


Right click on the new UDP Service object, to perform actions like viewing **Properties** of the UDP Service object, to find out where it is used, **copying** UDP Service object, **Duplicating** and **Deleting** UDP Service object.

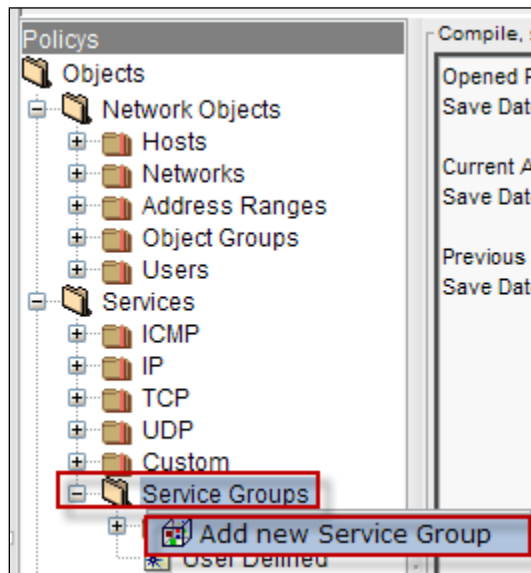


Service Groups

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



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

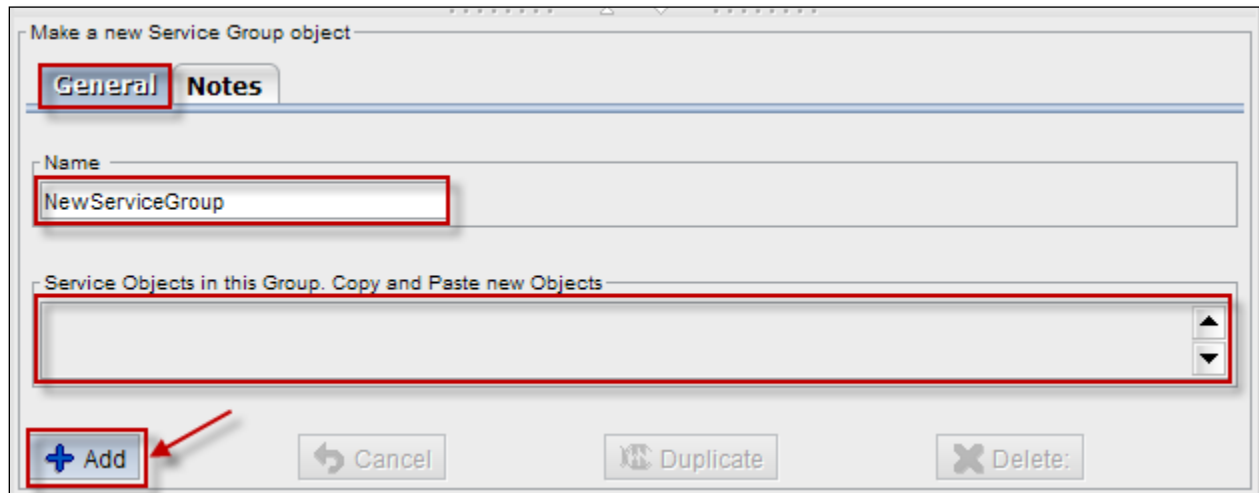


Below screen appears.

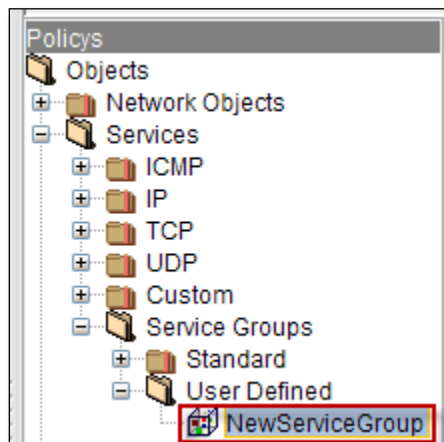
Select **General tab**, give the name of the new Service object Group.

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

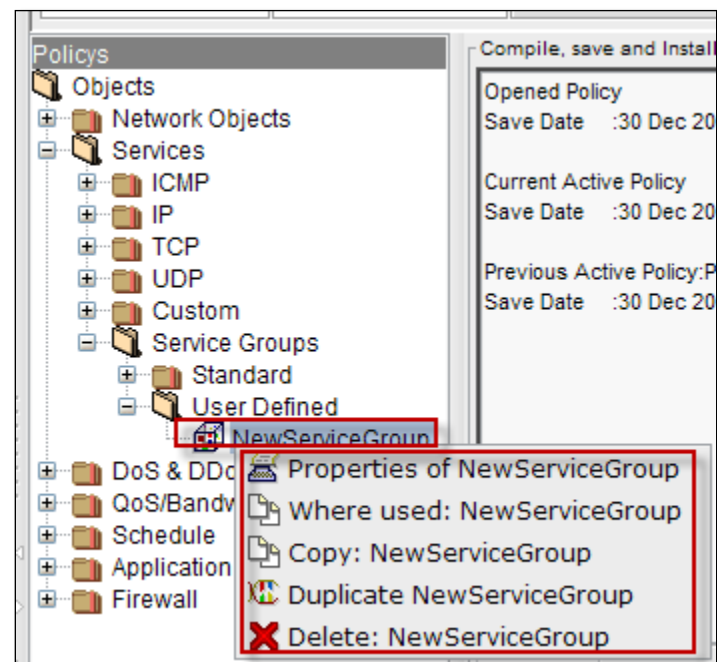
Click on **Add tab**.



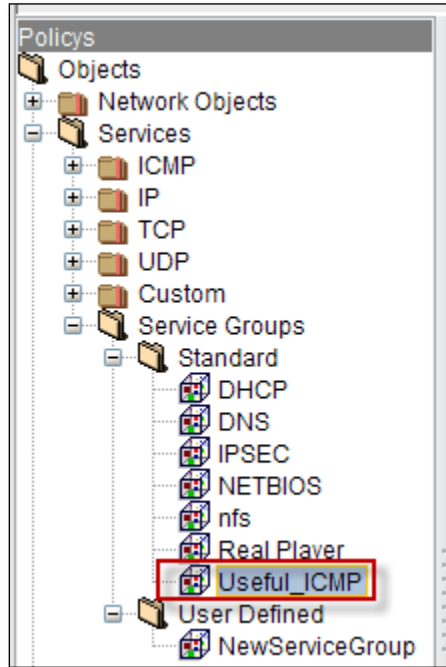
We can notice new **Service** Group under **User Defined**.



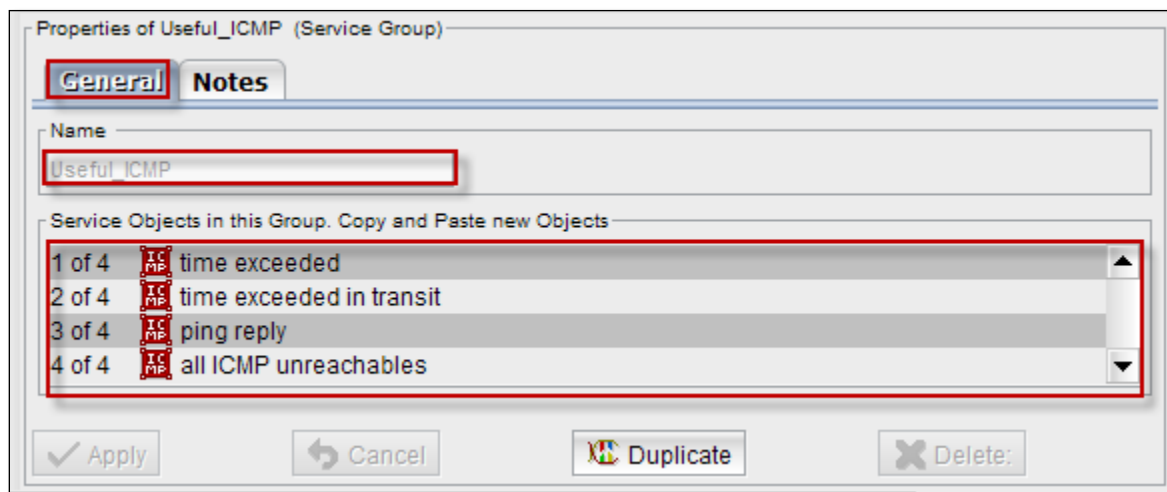
Right click on the new Service Group, to perform actions like viewing **Properties** of the New Service Group, to find out where it is used, **copying** New Service Group, **Duplicating** and **Deleting** New Service Group.



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.



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.

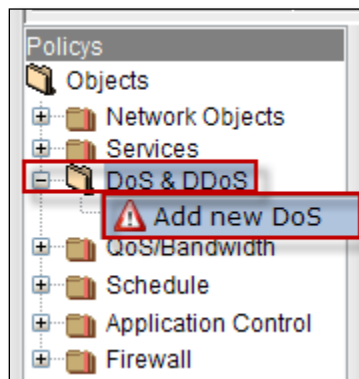
*Source - www.searchsecurity.com



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



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

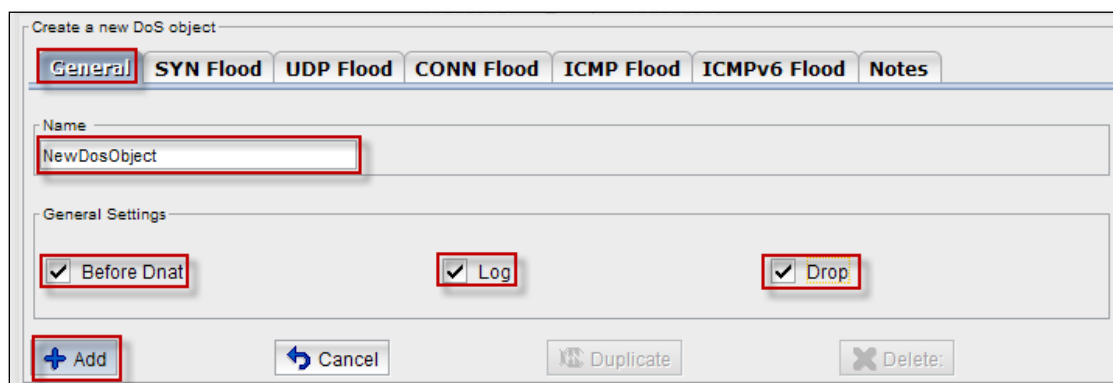


General

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' dialog box with the 'SYN Flood' tab selected. The 'SYN Flood Settings' section contains a list of checkboxes on the left and input fields for counts and bursts 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 699, Burst (1-10000) 800. At the bottom, there are buttons for '+ Add', 'Cancel', 'Duplicate', and 'Delete'.

Setting	Count	Burst (1-10000)
SYN Flood	1	400
Per Source	40	55
Per Destination	699	800
Total		

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' dialog box with the 'UDP Flood' tab selected. The 'UDP Flood Settings' section contains a list of checkboxes on the left and input fields for counts and bursts 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'.

Setting	Count	Burst (1-10000)
UDP Flood	30	60
Per Source	60	900
Per Destination	800	1000
Total		

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

☒ CONN Flood
☒ Per Source
☒ Per Destination
☒ Total

Count	50	Burst (1-10000)	599
Count	300	Burst (1-10000)	3000
Count	500	Burst (1-10000)	878

+ Add Cancel Duplicate 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

☒ ICMP Flood
☒ Per Source
☒ Per Destination
☒ Total

Count	70	Burst (1-10000)	299
Count	67	Burst (1-10000)	887
Count	200	Burst (1-10000)	300

+ Add Cancel Duplicate 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.

Create a new DoS object

General SYN Flood UDP Flood CONN Flood ICMP Flood **ICMPv6 Flood** Notes

ICMPv6 Flood Settings

<input checked="" type="checkbox"/> ICMPv6 Flood	Count	220	Burst (1-10000)	330
<input checked="" type="checkbox"/> Per Source	Count	380	Burst (1-10000)	4500
<input checked="" type="checkbox"/> Per Destination	Count	1	Burst (1-10000)	5
<input checked="" type="checkbox"/> Total				

Notes

In Notes column, we can write information regarding new DOS Object.

Create a new DoS object

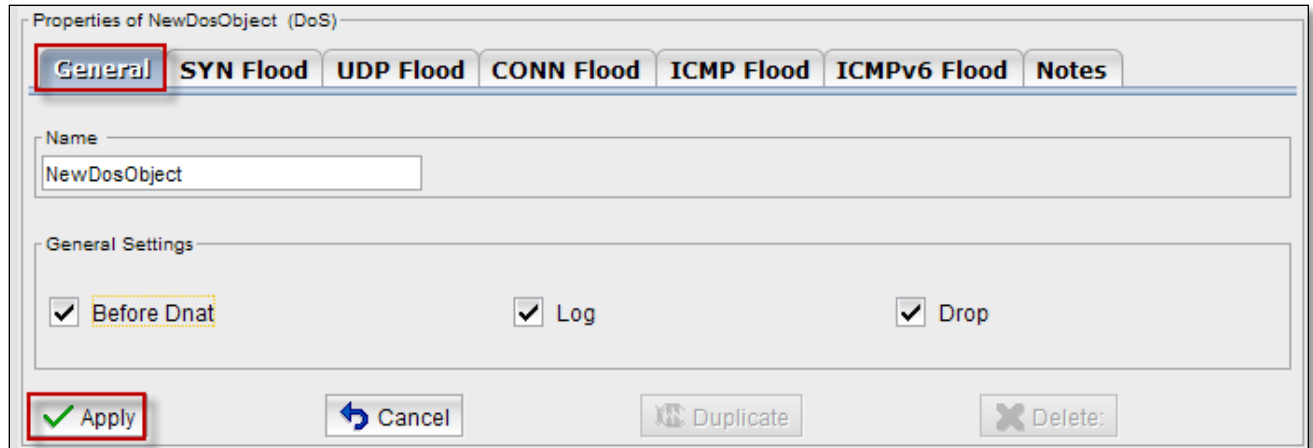
General SYN Flood UDP Flood CONN Flood ICMP Flood ICMPv6 Flood **Notes**

Notes

NewDosObject

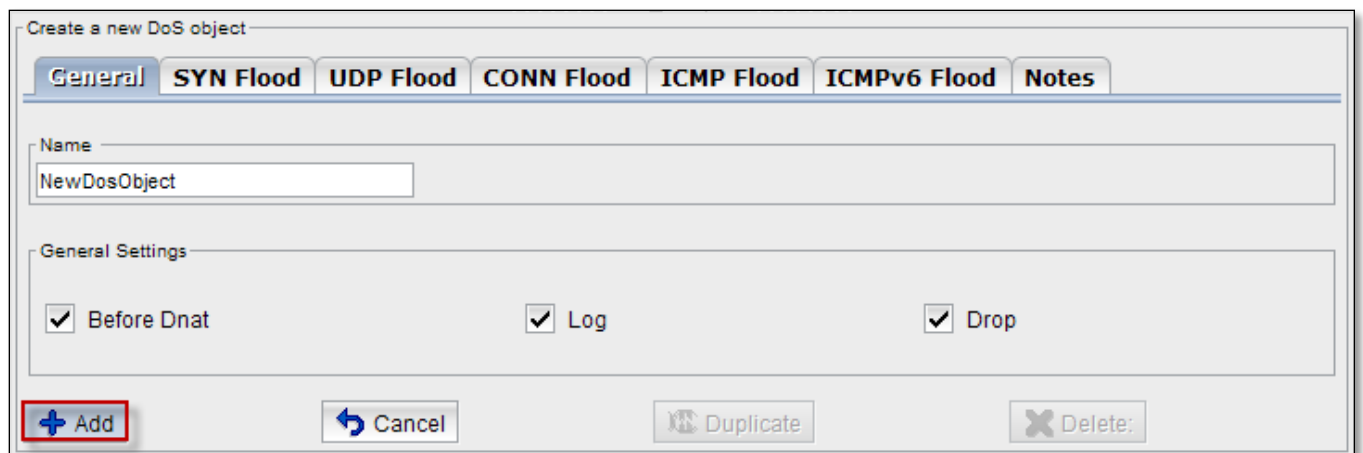
+ Add Cancel Duplicate Delete

After providing all the inputs to the New Dos Object, click on **Apply** tab.



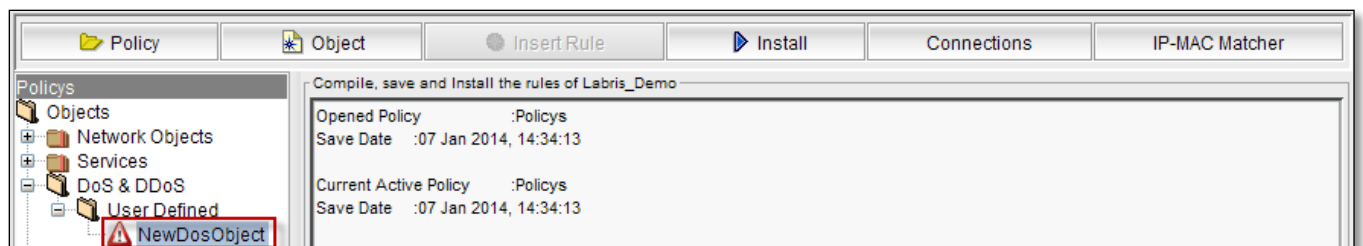
The image shows the 'Properties of NewDosObject (DoS)' dialog box. It has several tabs: 'General' (highlighted with a red box), 'SYN Flood', 'UDP Flood', 'CONN Flood', 'ICMP Flood', 'ICMPv6 Flood', and 'Notes'. The 'Name' field contains 'NewDosObject'. Under 'General Settings', there are three checked checkboxes: 'Before Dnat' (highlighted with a yellow box), 'Log', and 'Drop'. At the bottom, there are four buttons: 'Apply' (highlighted with a red box and a green checkmark icon), 'Cancel', 'Duplicate', and 'Delete'.

Click on **Add** tab.

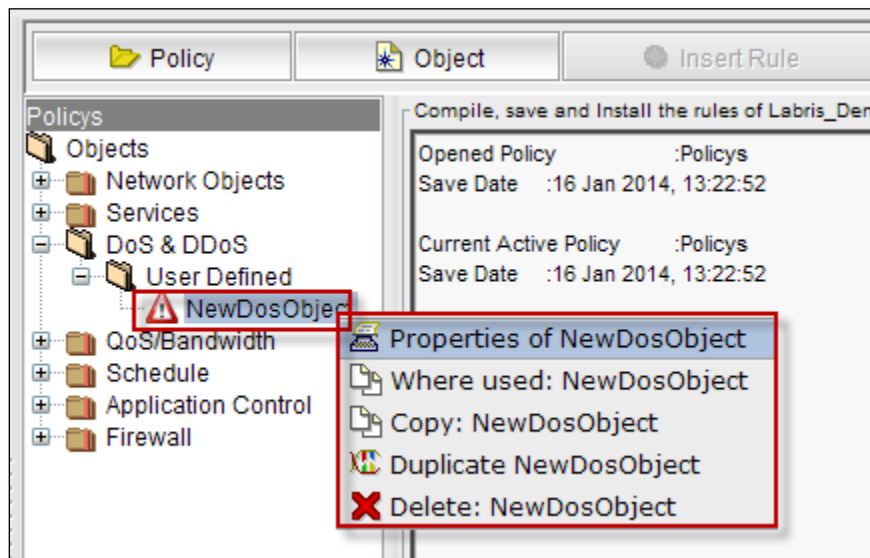


The image shows the 'Create a new DoS object' dialog box. It has the same tabs as the previous dialog: 'General' (highlighted with a red box), 'SYN Flood', 'UDP Flood', 'CONN Flood', 'ICMP Flood', 'ICMPv6 Flood', and 'Notes'. The 'Name' field contains 'NewDosObject'. Under 'General Settings', there are three checked checkboxes: 'Before Dnat', 'Log', and 'Drop'. At the bottom, there are four buttons: 'Add' (highlighted with a red box and a blue plus icon), 'Cancel', 'Duplicate', and 'Delete'.

In the below screen, we can notice New Dos Object under User Defined.

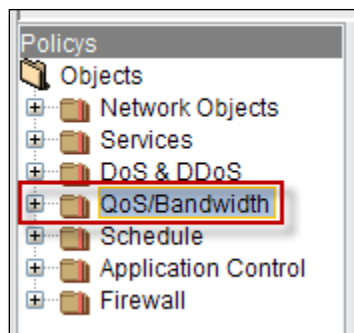


Right click on the New Dos object, to perform actions like viewing **Properties** of the Dos object, to find out where it is used, **copying** object, **Duplicating** and **Deleting** Dos object.

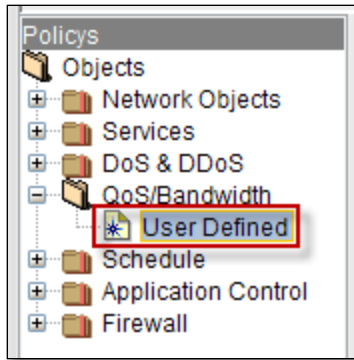


QoS/Bandwidth

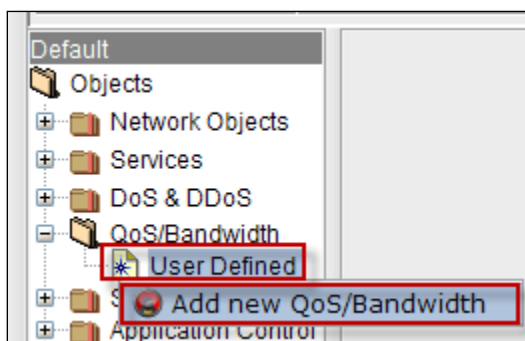
QoS (Quality of Service) plays a crucial role in ensuring high-quality performance to latency and bandwidth sensitive applications. Differential treatment of traffic based on rules are accepted and prioritized. Necessary protocols and performance of the network is effectively improved by QoS.



Expand QoS/Bandwidth, by default **User Defined** is displayed.



Right click on User Defined under QoS/Bandwidth, to add new QoS/Bandwidth.



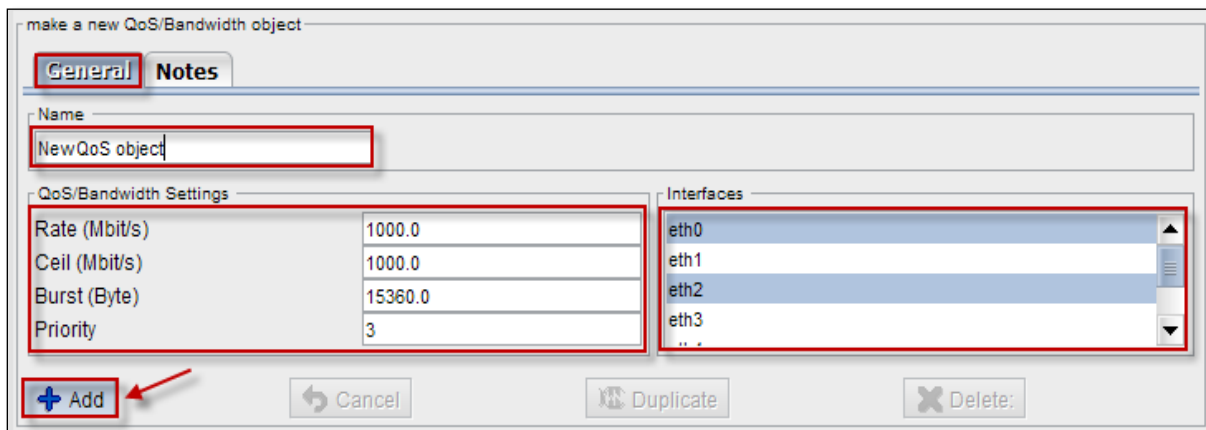
General

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**.

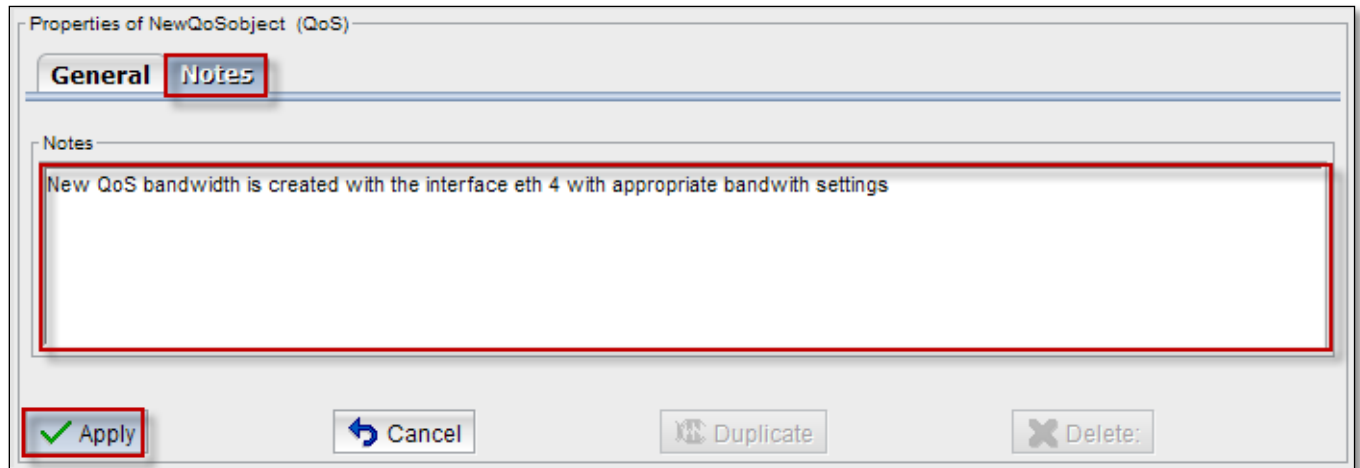
Choose Interface for the New QoS/Bandwidth object from the list of **Interfaces**.



Click on **Add tab**.

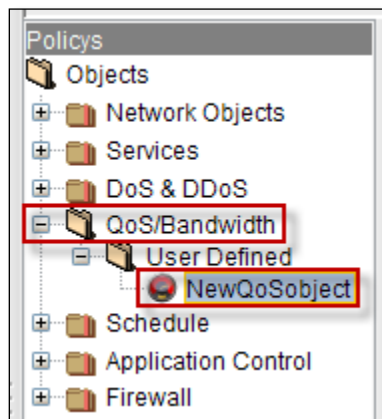
Notes

Select **Notes tab** to write notes regarding new object creation.

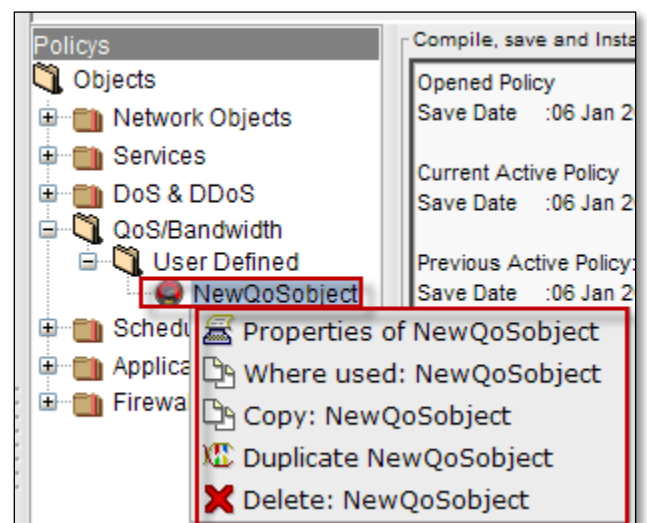


Click on **Apply tab**.

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.

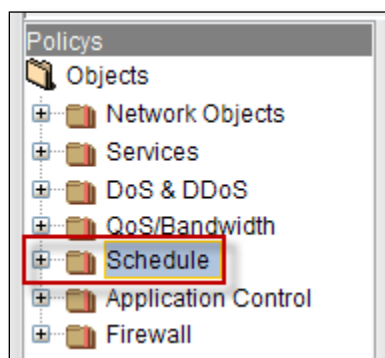


Schedule

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.

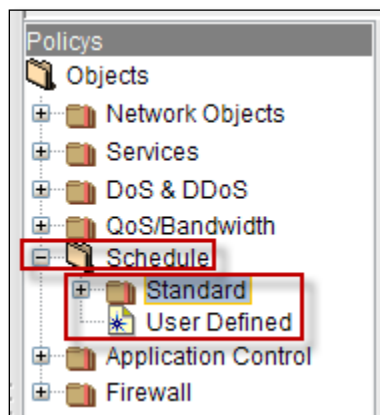
Firstly schedule should be created under Firewall and then apply a schedule to the rule or while creating a rule pick up appropriate defined schedule to the rule.

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.

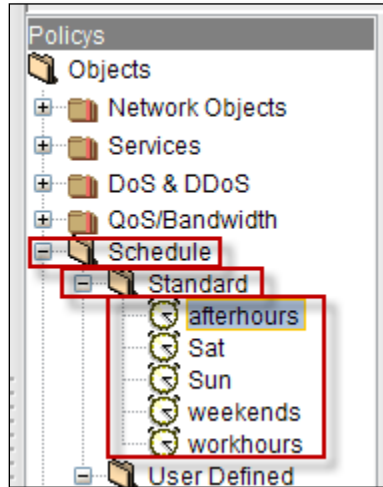


Standard

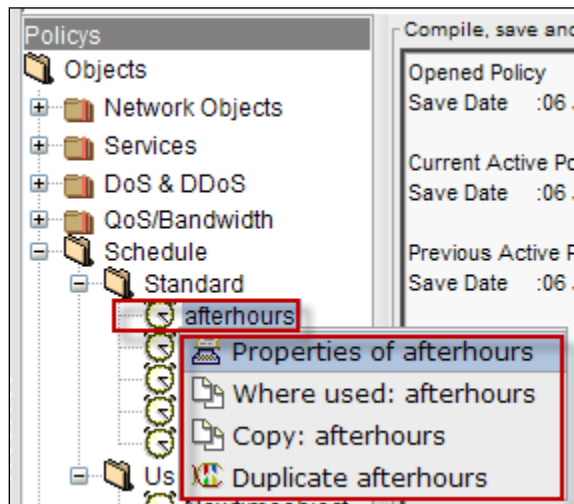
Expand schedule, **Standard** and **User Defined** is displayed.



Expand **standard**, by default some schedule objects are displayed under **Standard Schedule**.

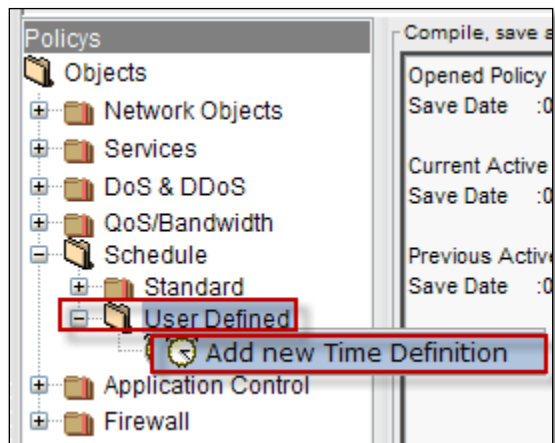


Right click on the schedule object, to perform actions like viewing **Properties** of the Schedule object, to find out where it is used, **copying** object, **Duplicating** and **Deleting** Schedule object.



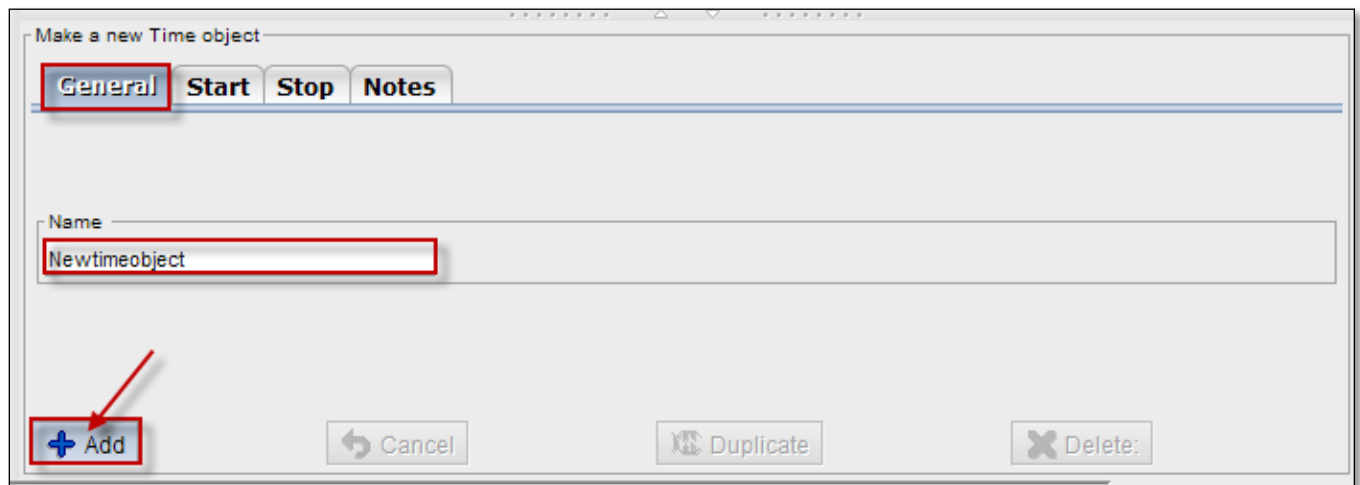
User Defined

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.


Properties of Newtimeobject (Time)

General **Start** Stop Notes

☒ Activate date 1

☒ Activate hour 2

☒ Activate day 3

Date: Jan 7, 2014 

Hour: 72 Minute: 20

Day of Week: Tuesday

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

Properties of Newtimeobject (Time)

General **Start** Stop Notes

☐ Activate date

☐ Activate hour

☐ Activate day

Date: Jan 7, 2014

Hour: 0 Minute: 20

Day of Week: Tuesday


Stop

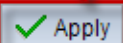
Schedule object stop time should be mentioned in this section, select **Stop** tab.

Properties of Newtimeobject (Time)

General Start **Stop** Notes

☒ Activate date 1
☐ Activate hour 2
☒ Activate day 3

Date: Jan 16, 2014  calender
Hour: 0 Minute: 0
Day of Week: Wednesday

 Apply Cancel Duplicate Delete

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

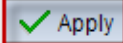
Select **Notes** tab, to write necessary information regarding time Object.

Properties of Newtimeobject (Time)

General Start Stop **Notes**

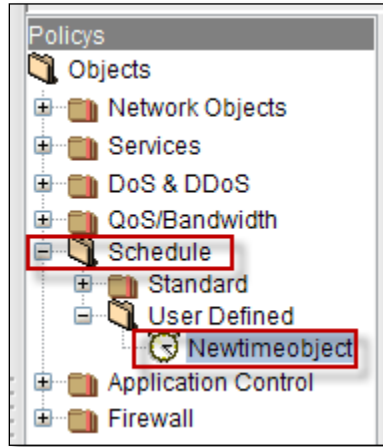
Notes

new time object is created with start time and stop time

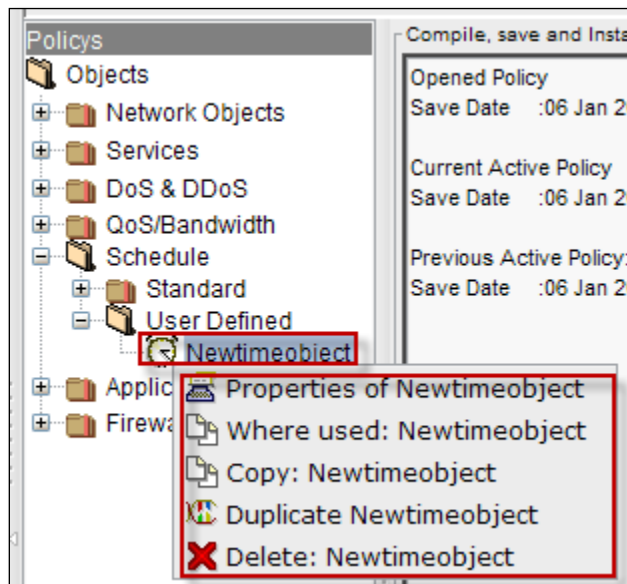
 Apply Cancel Duplicate Delete

Click on **Apply** tab.

We can notice new time Object in the below screen.

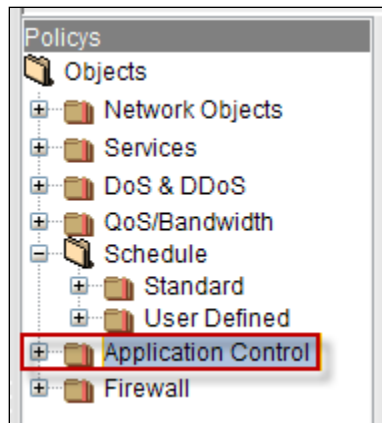


Right click on the schedule object, to perform actions like viewing **Properties** of the Schedule object, to find out where it is used, **copying** object, **Duplicating** and **Deleting** Schedule object.



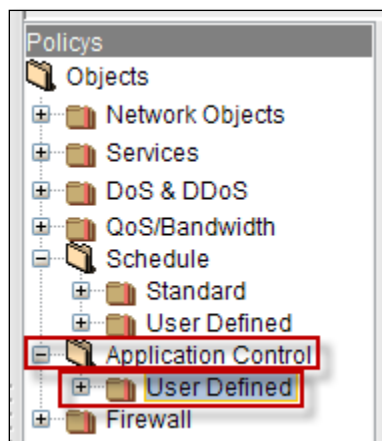
Application Control

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

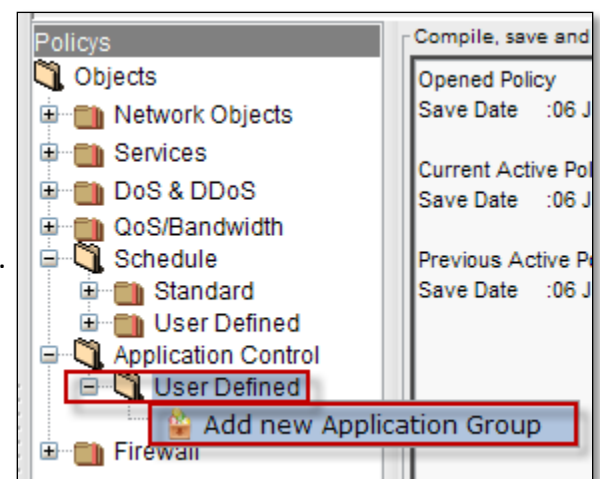


User Defined

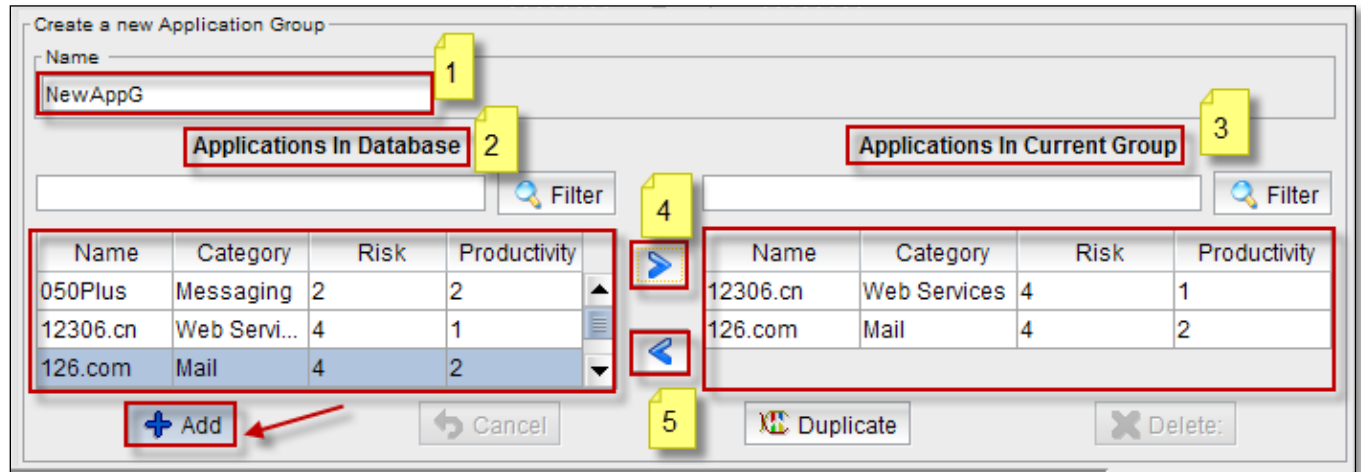
Expand Application Control, by default User Defined is displayed.





Right click on **User Defined** to add new Application Group.



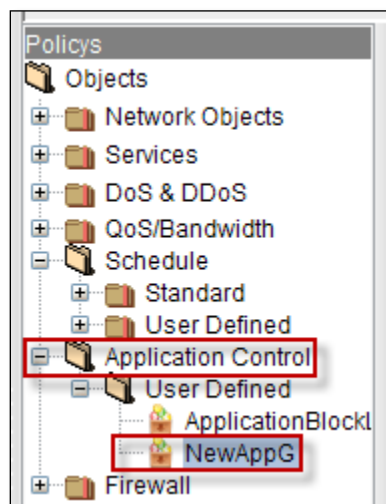
Creating new application group



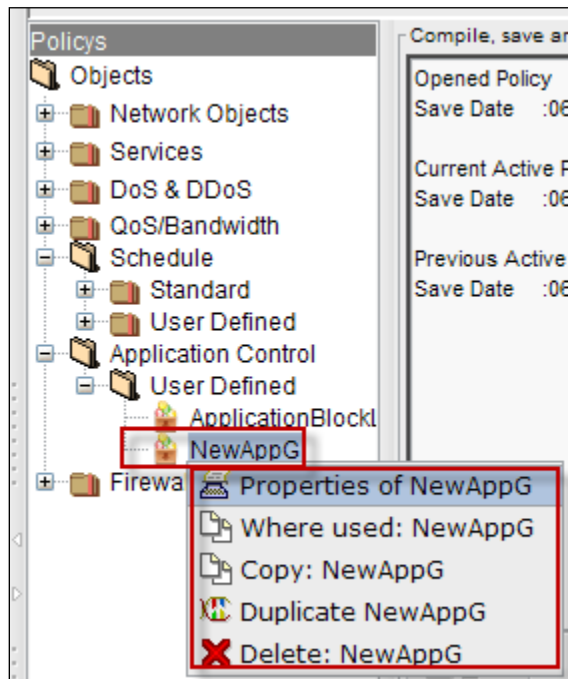
These are the inputs for new Application Group.

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.



Firewall

Firewall is a concept which blocks unwanted traffic and passes desirable traffic to and from both sides of the network.

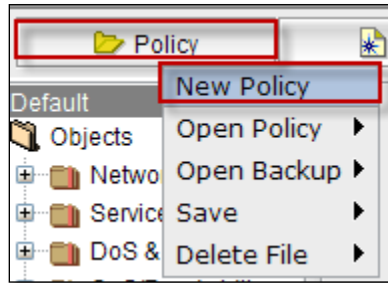
A firewall is a system (either software or hardware or both) that enforces an access control policy between two networks.

Example:

- Allows: http, mails etc
- Keeps out : Intruders ,Denial of services attacks, spam etc.

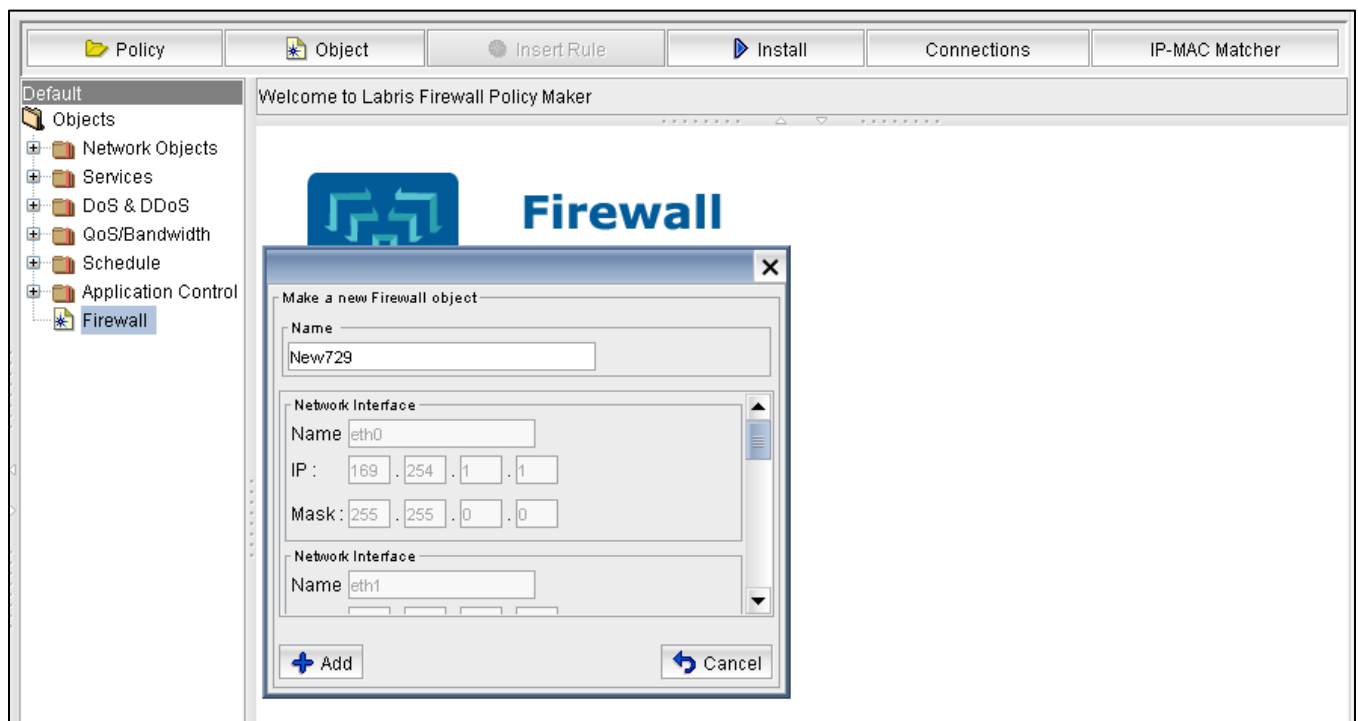
Labris Firewall Management

Install, Save (create a new policy object for first setup), Install Policy

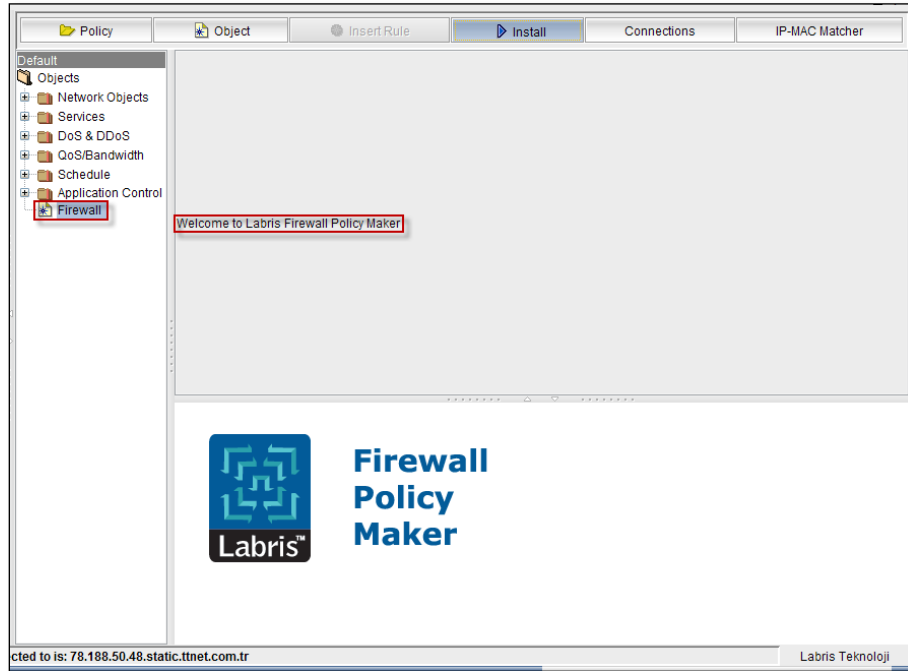


Creating new policy firewall object

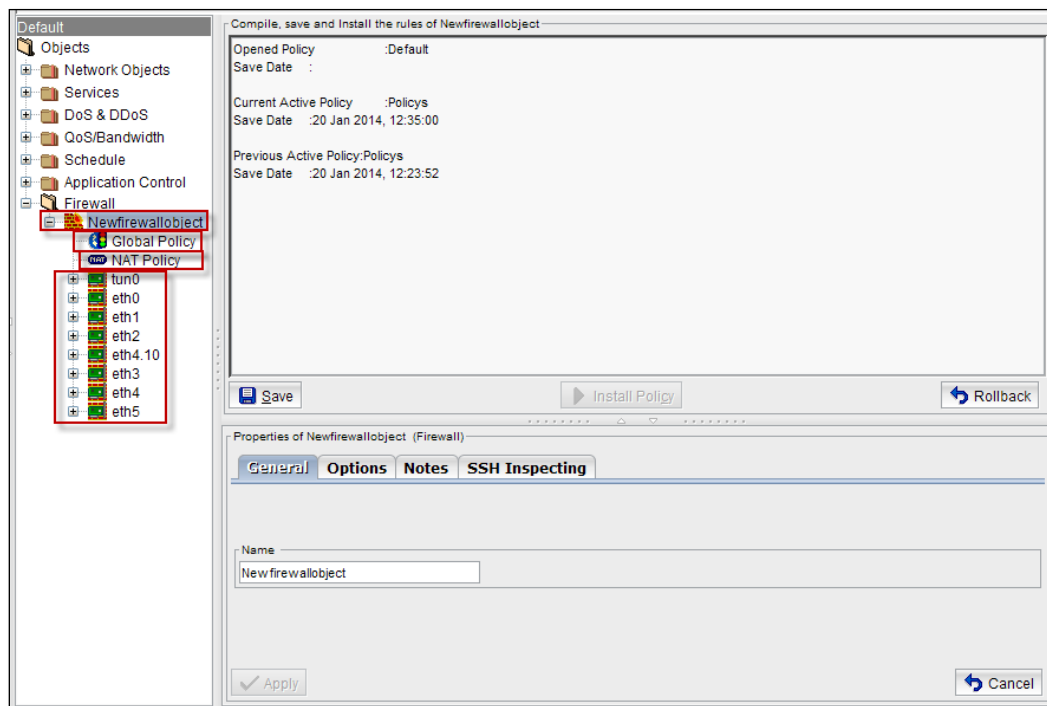
Give the **Name** of the Object in the Name tab, by default Network Interfaces have been selected for the new firewall object and click on **Add** tab.



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.

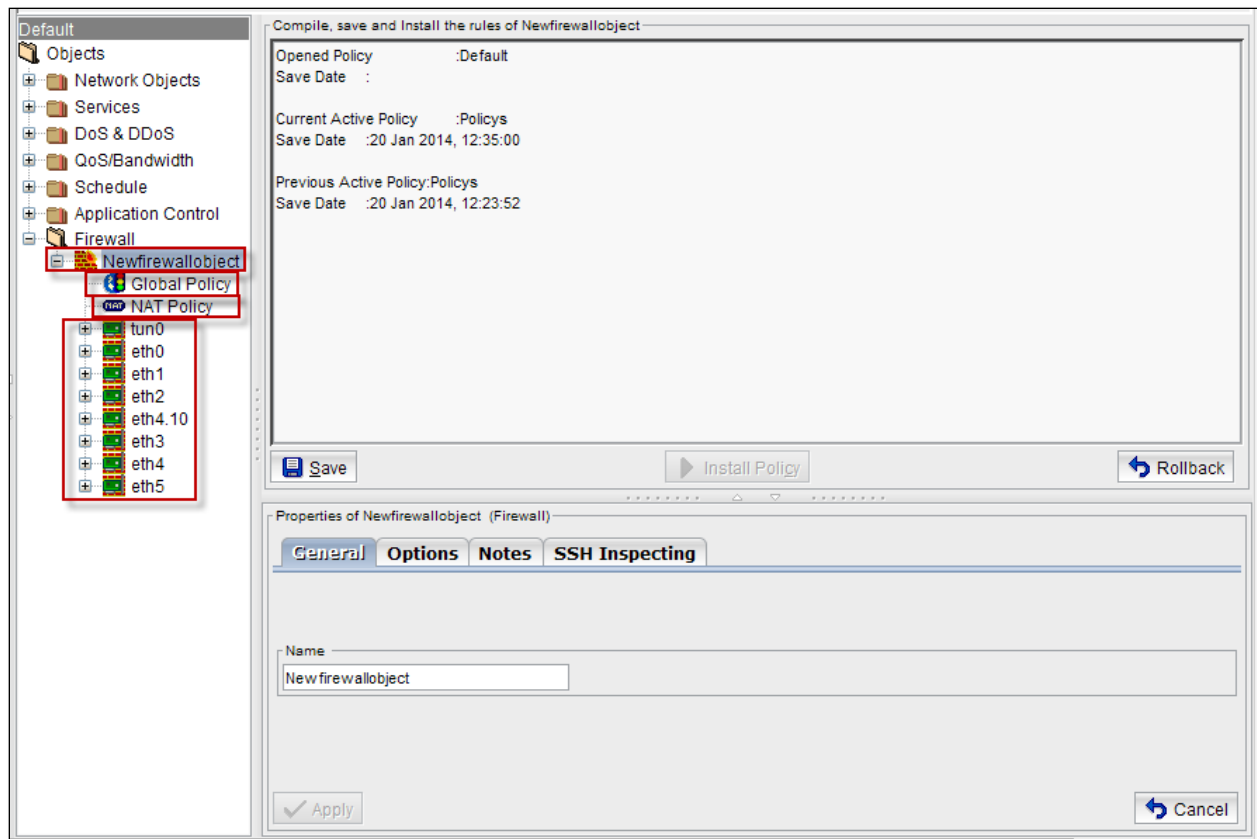
For example, a lot of the IP subnet address from internal network will route to outside network with single IP address.

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

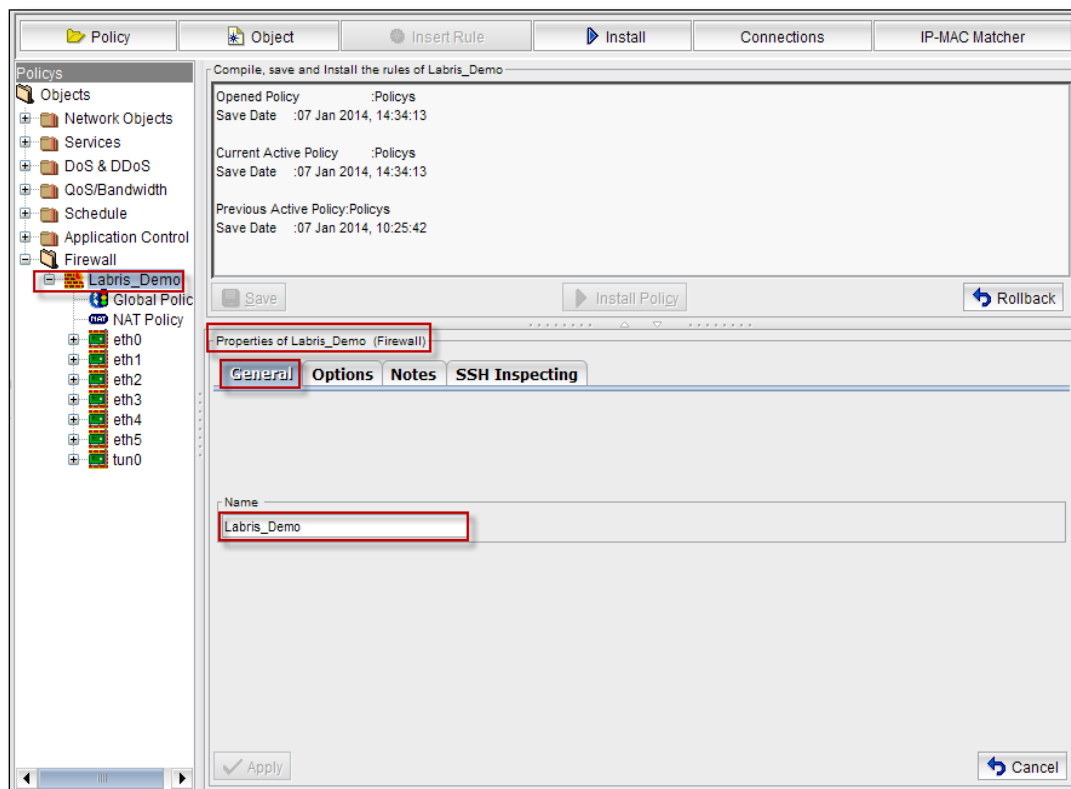
- **Interface** - Use this property to match which network port or data link packet is traversing such as "eth0" for Ethernet built-in.
- **Source MAC Address** - Use this property to specify an Ethernet Hardware Address that matches the source MAC (Media Access Control) address in the link layer frame 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.

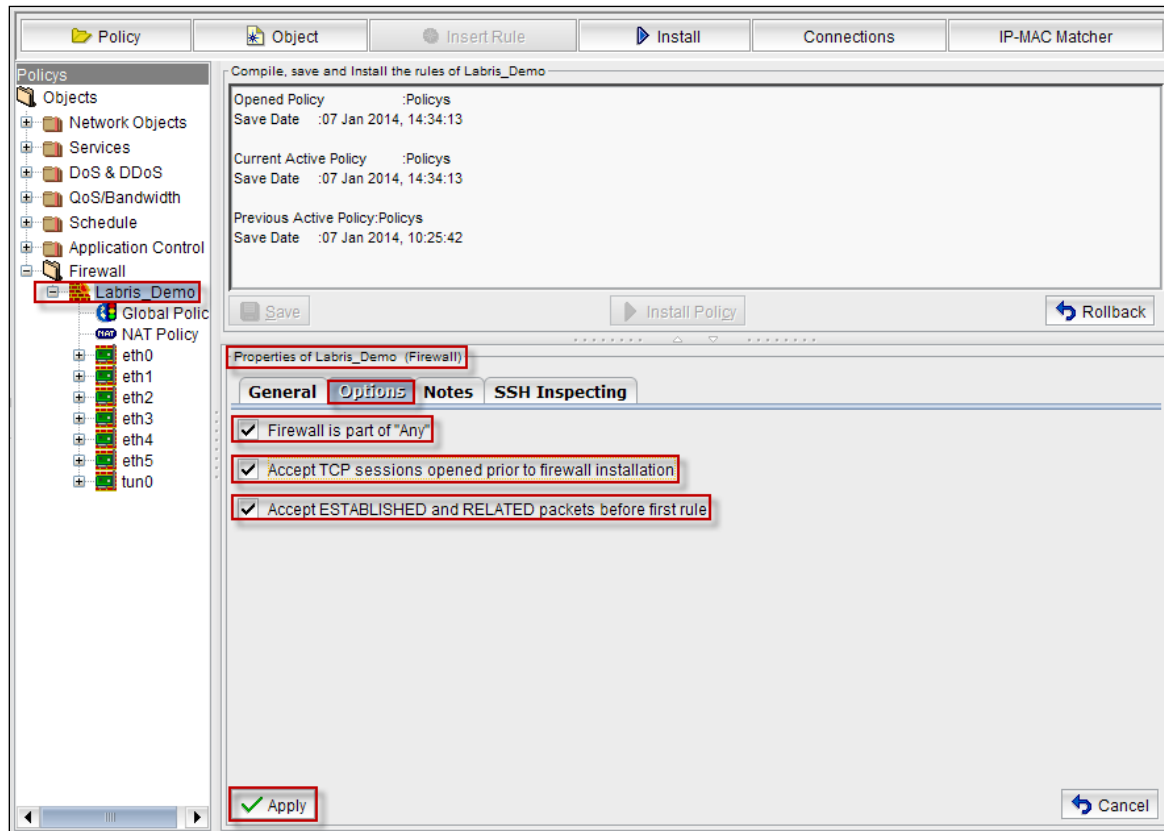
Select **General tab**to view details about Name of the Firewall object.

We can change name and click on Apply tab to change the name.



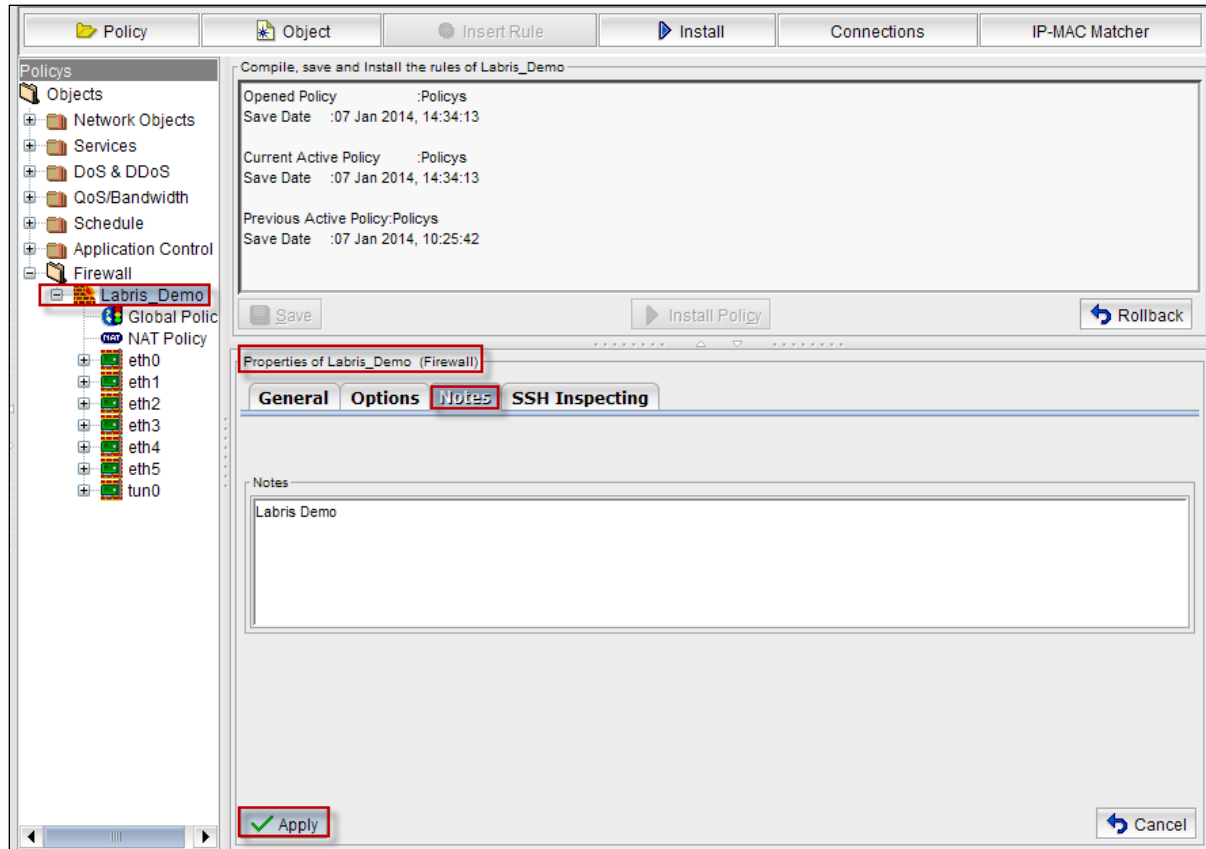
Select **Options** tab.

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.

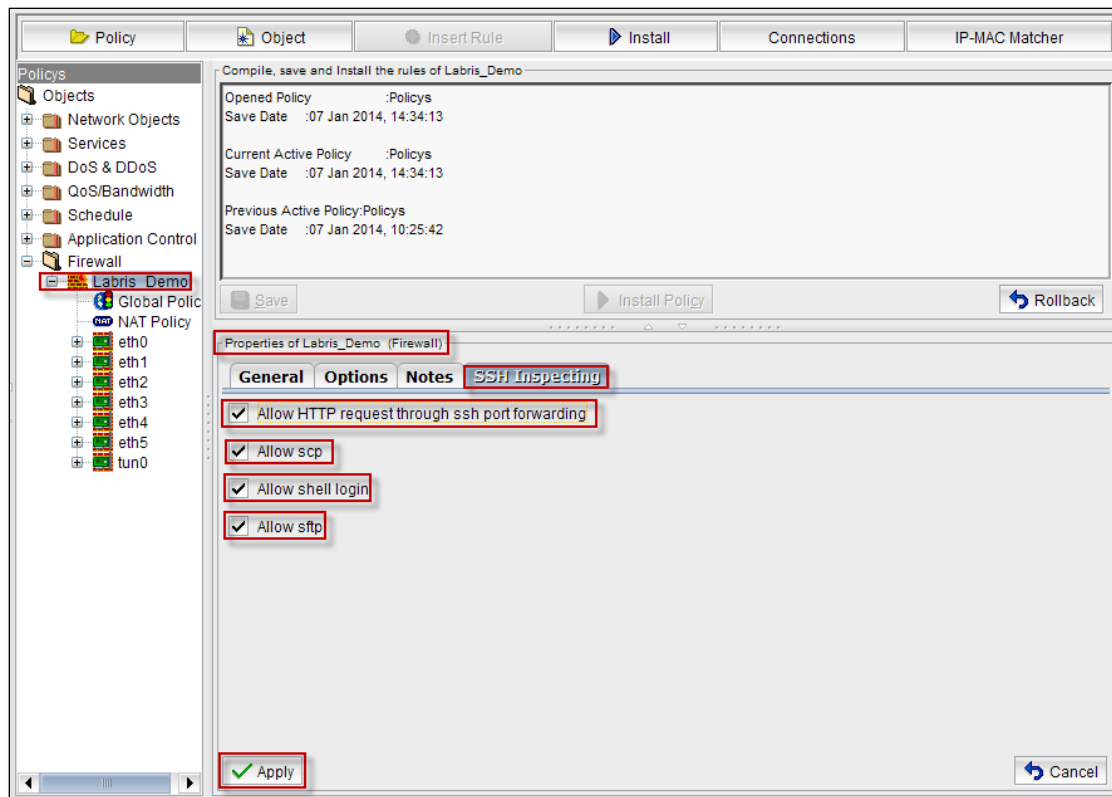
Select **Notes** tab to write information regarding firewall object (Optional).



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**.



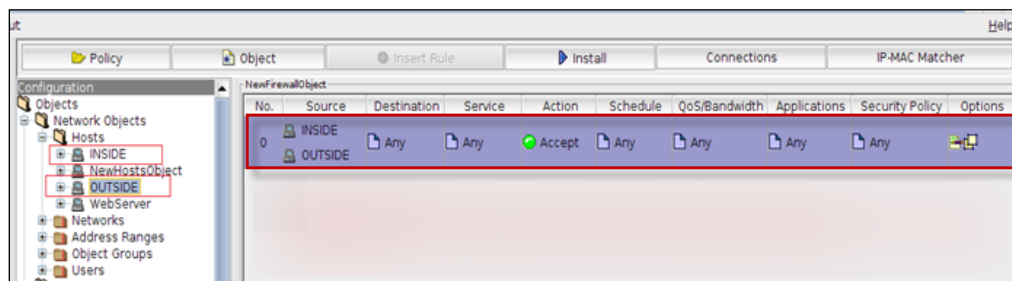
Click on **Apply** tab to apply changes

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

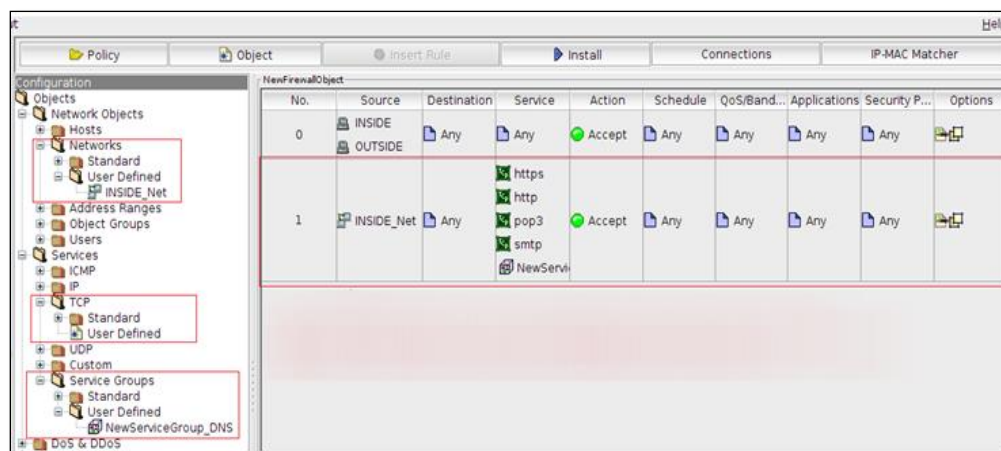


My global policy

In the above screen we can notice columns such as Source, Destination, Service, Action, Schedule, QoS/Bandwidth, Application, Security Policy, Options.

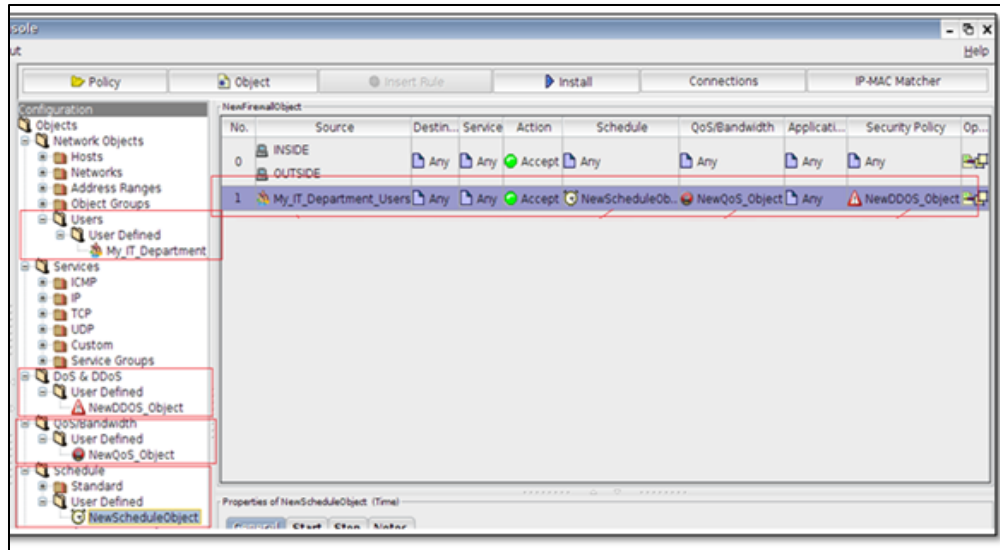
Application is allowed if the created Source with interfaces INSIDE & OUTSIDE is accessed, and when the Destination, Service, Schedule, QoS/Bandwidth, Application, Security Policy options are Selected as ANY. We can even drag-and-drop the desired objects created earlier, or copy and paste can be added with it.

Example 2: My network objects for policy.



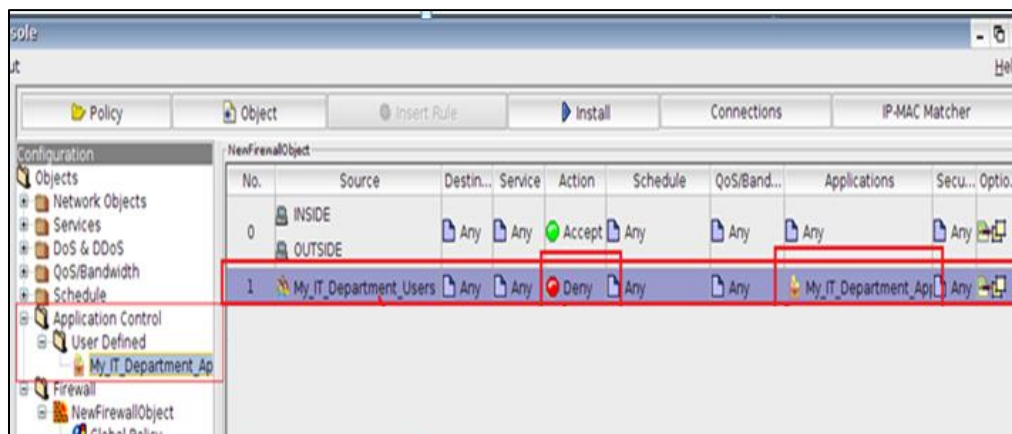
All of the destinations on the IP addresses of the source of the rule INSIDE_Net with access to only the specified services. This rule also holds at their outer radio marker internal IP addresses on the policy.

Example 3: How do we add a rule for users and My.applicaiton.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.

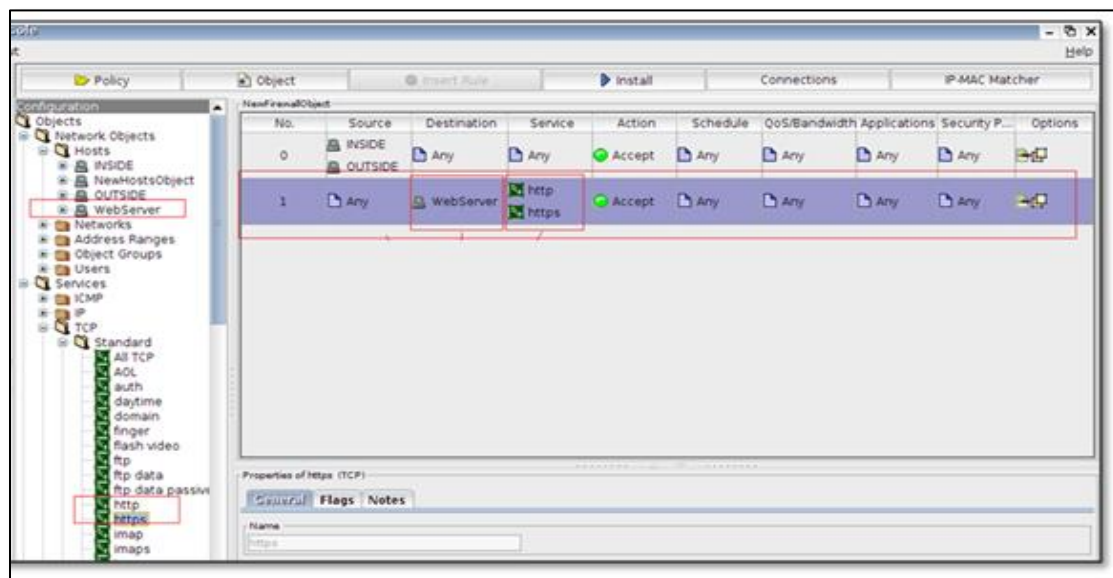
How to add an application control rule for users?



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).

Policy

Object

Insert Rule

Install

Connections

IP-MAC Matcher

Policy

Labris_Demo

Global Policy

NAT Policy

eth0

eth1

eth2


eth3

eth4

eth5

tun0

No.	Source	Destination	Service	Action	Schedule	QoS/Band...	Applicatio...	Security P...	Options
0	suleym...	win_for	Any	Accept	Any	Any	Any	Any	
1	INSIDE	OUTSI...	Any	Accept	Any	Any	Any	Any	
2	Any	kalilinux	8090	Accept	Any	Any	Any	Any	
3	INSIDE	Any	Any	Deny	Any	Any	Applicati	Any	
4	Any	w2k12	rdp	Accept	Any	Any	Any	Any	
	INSIDE	win7							



Firewall

Policy

Maker

ected to is: 78.188.50.48.static.ttnet.com.tr

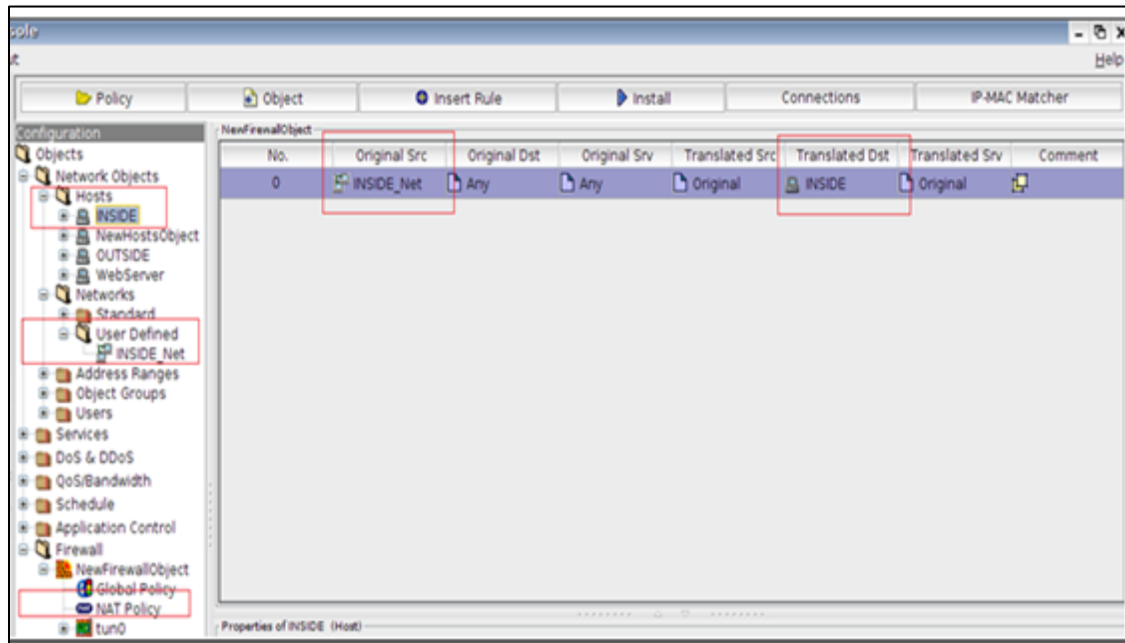
Labris Teknoloji

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.

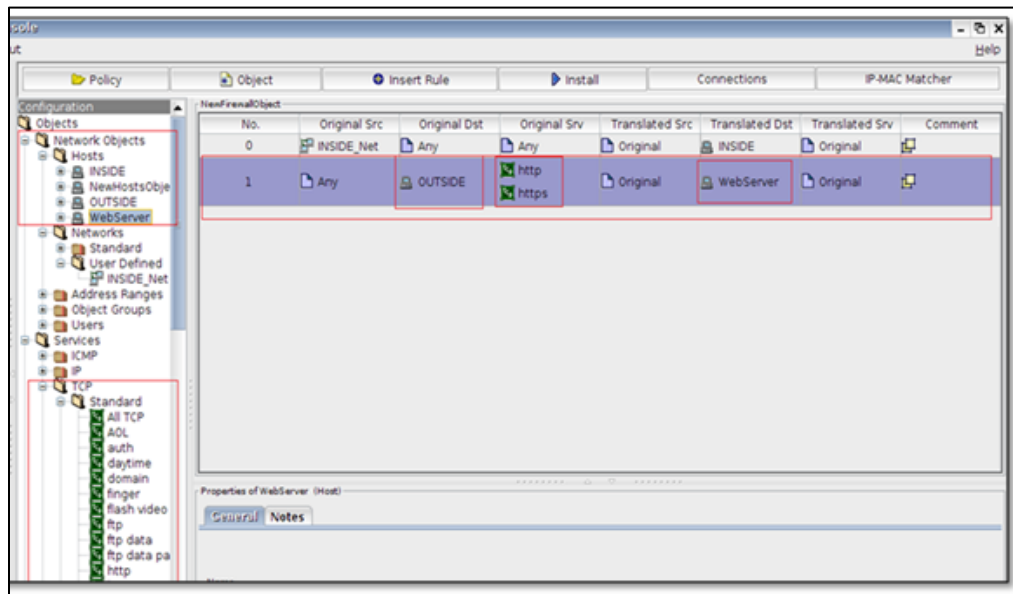
Example1: Internet NAT policy



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

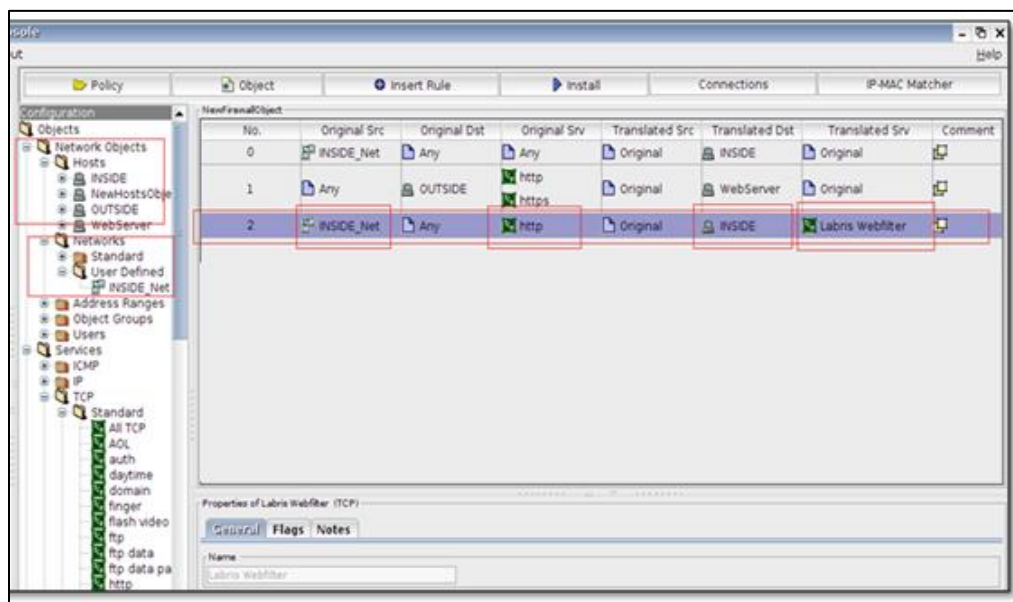
Example2: Web server access from Wide Area Network.



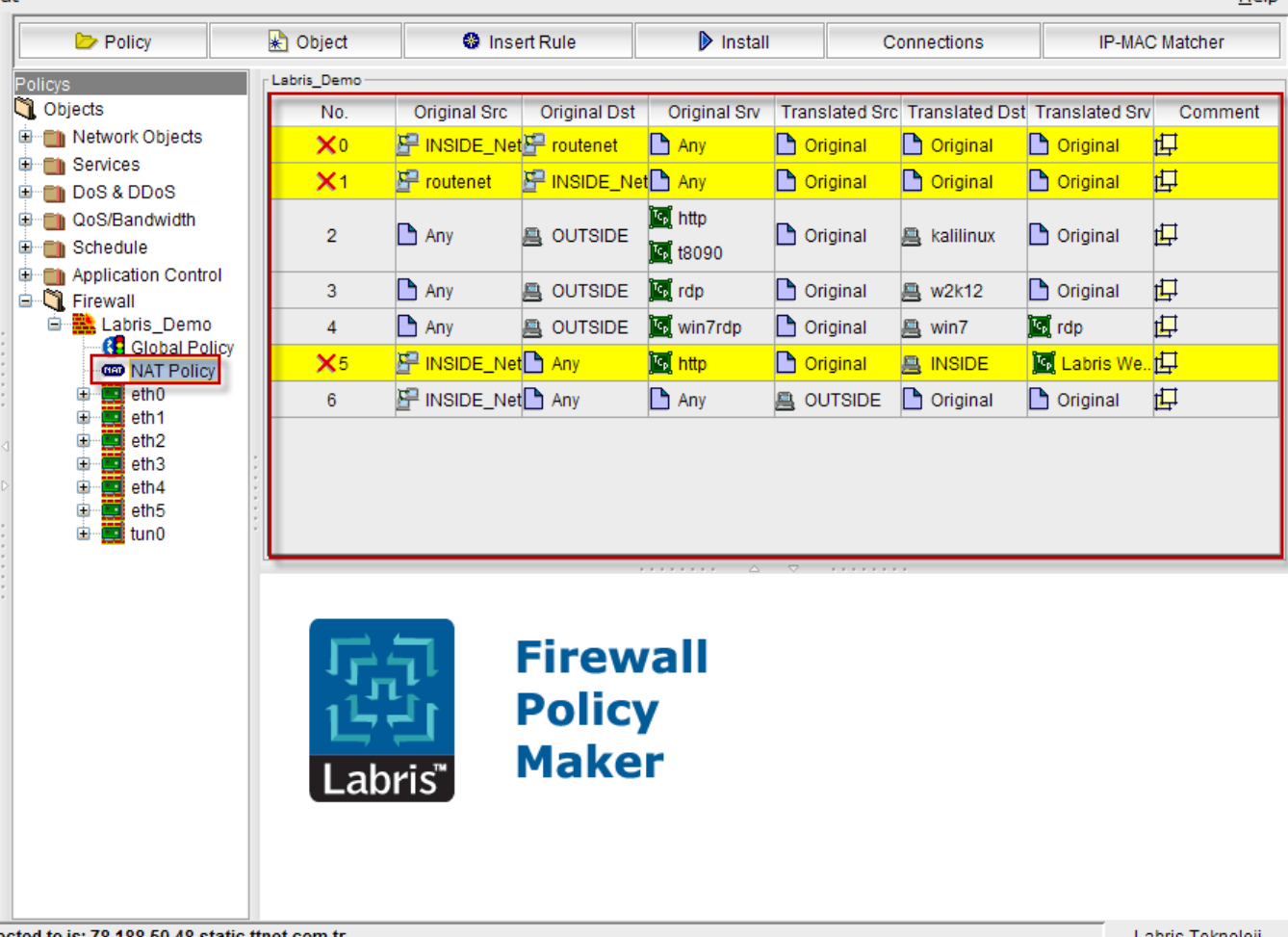
Any source outside web server "any" http and https access to the supplier global policy is written as (For **global policy** please refer to **ADD Next generation firewall** section) and later to the server on specific ports from outside should identify which requests inside.

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: Policy > Objects > NAT Policy. The main area shows a table of NAT rules for the 'Labris_Demo' policy. The table has columns: 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 or in error. Rule 5 is a NAT rule mapping 'INSIDE_Net' to 'Any' for 'http' service, translated to 'INSIDE' for 'Labris We..'. Below the table, the Labris logo and 'Firewall Policy Maker' text are visible. The status bar at the bottom shows the IP address '78.188.50.48.static.ttnet.com.tr' and the company name '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	

Labris™ Firewall Policy Maker

ected to is: 78.188.50.48.static.ttnet.com.tr

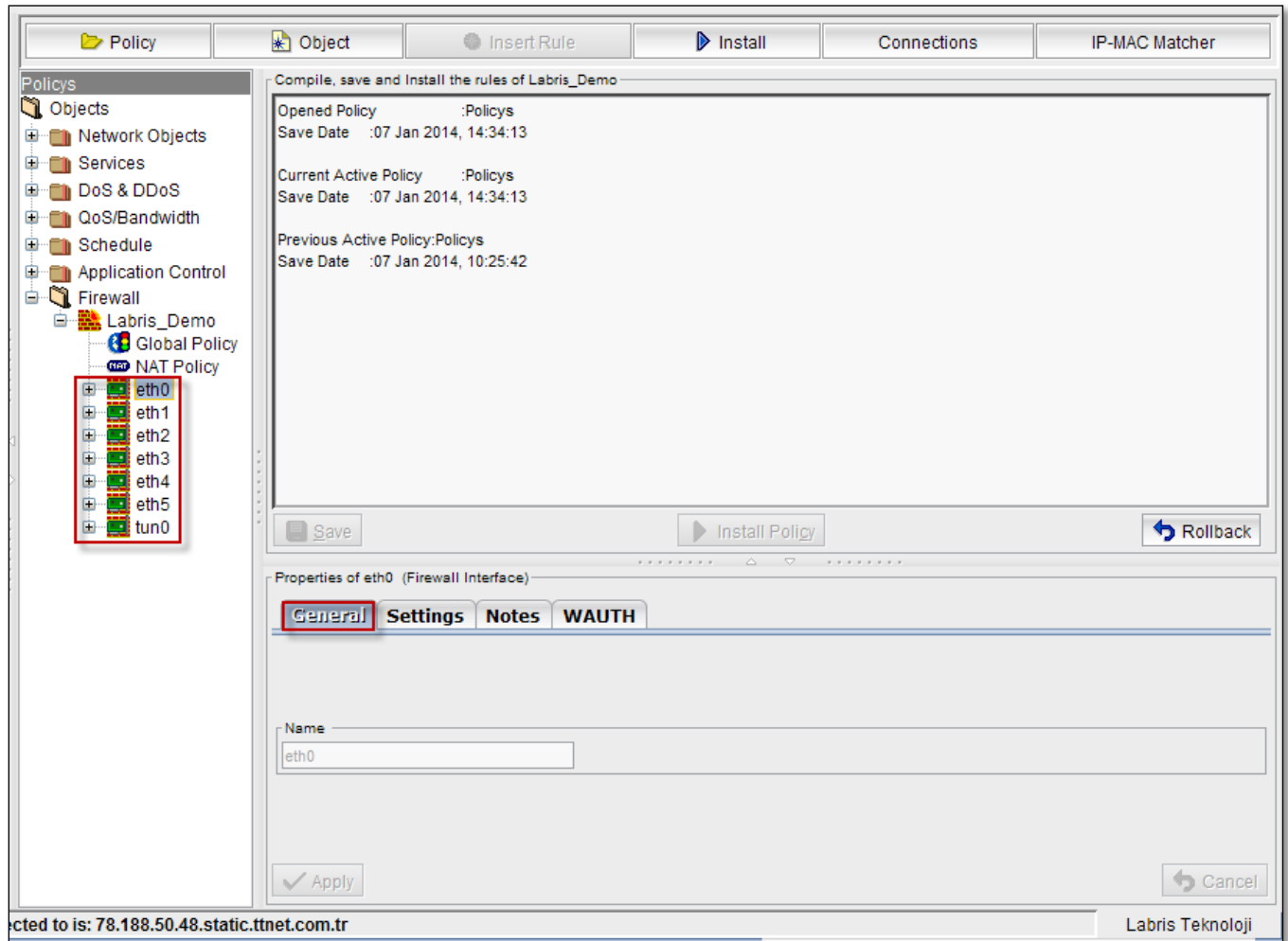
Labris Teknoloji

Interfaces

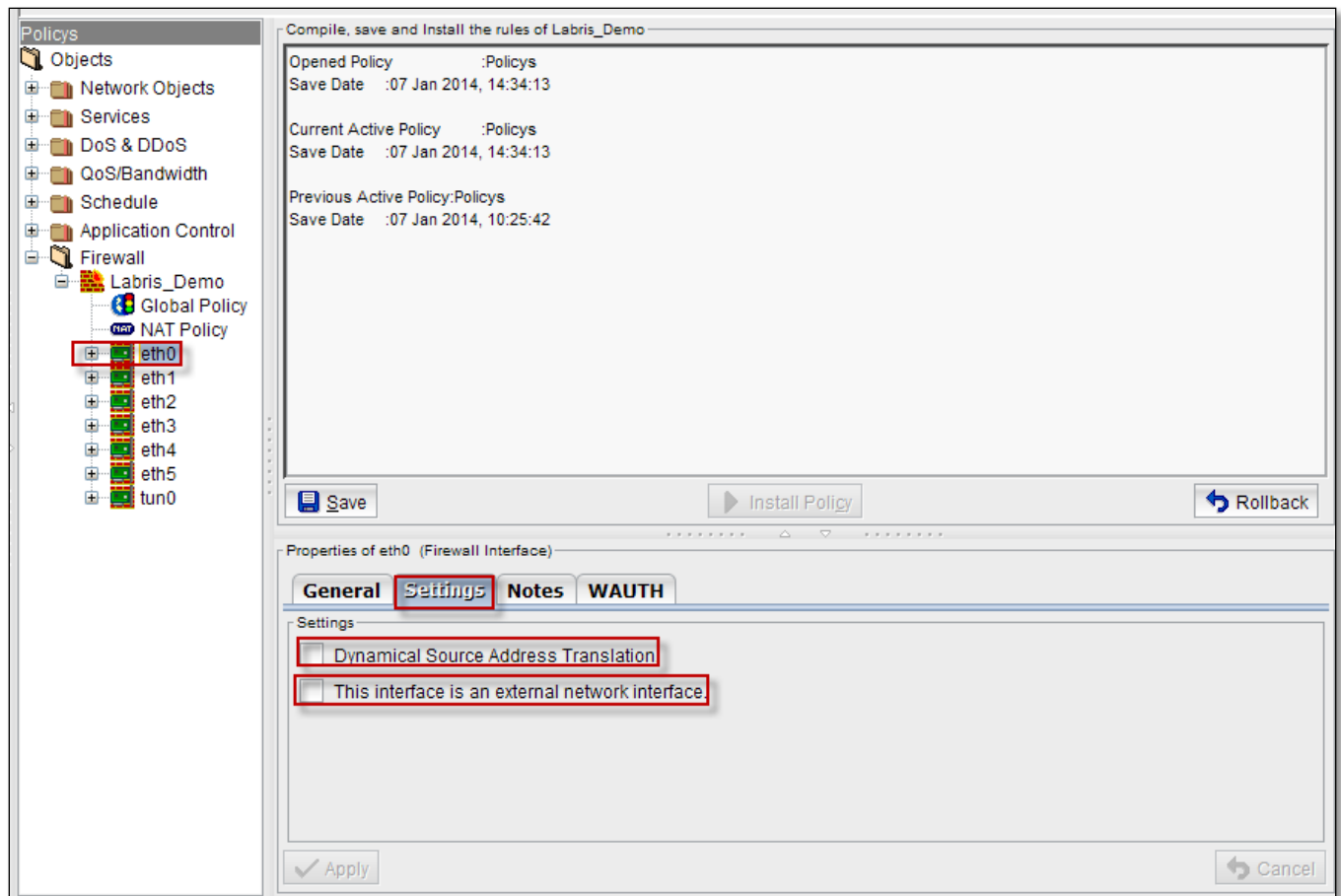
By default seven Interfaces are present in the firewall object.

They are **eth0**, **eth1**, **eth2**, **eth3**, **eth4**, **eth5**, **tun0**.

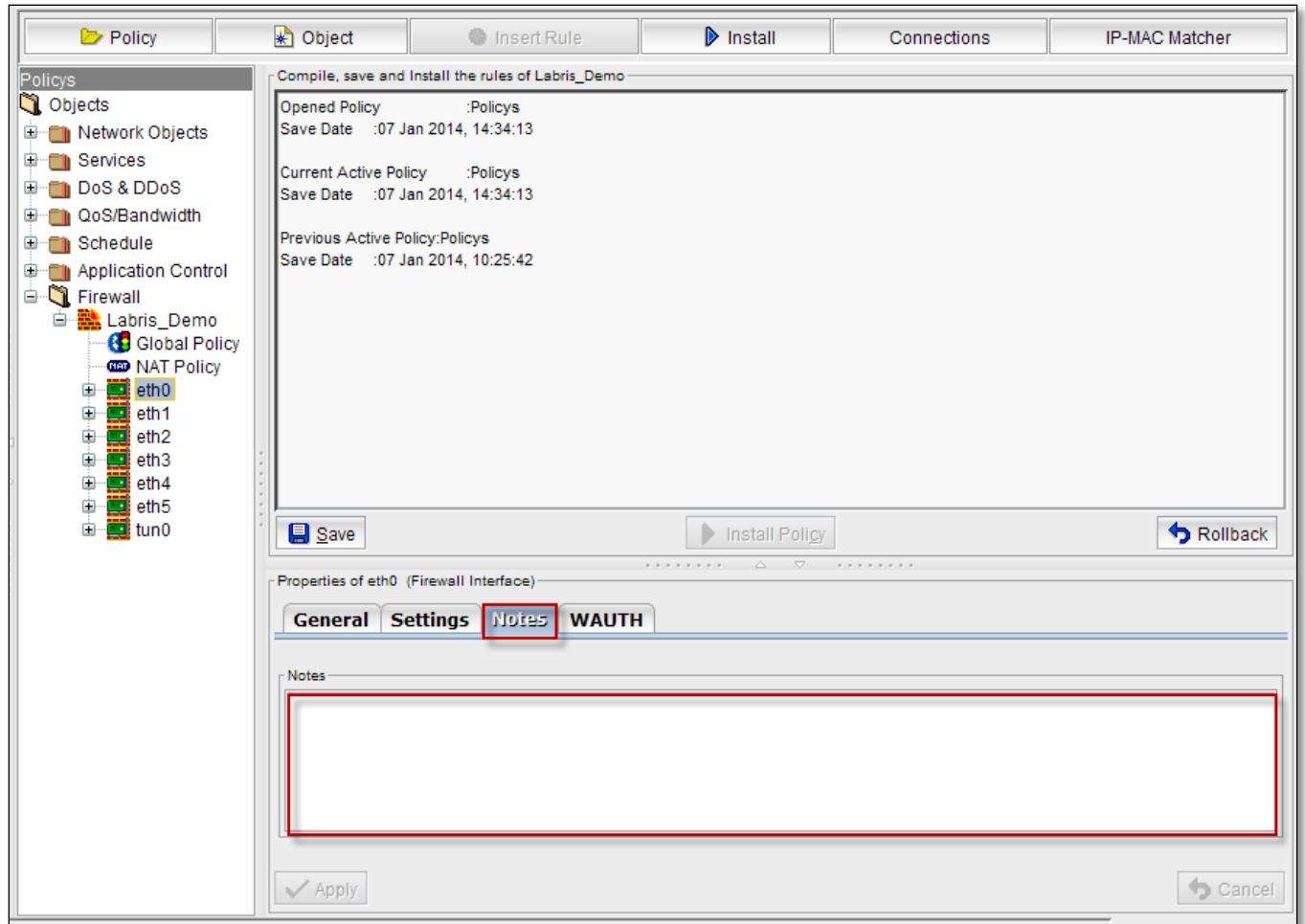
Select **General tab**, Name of the interface is displayed.



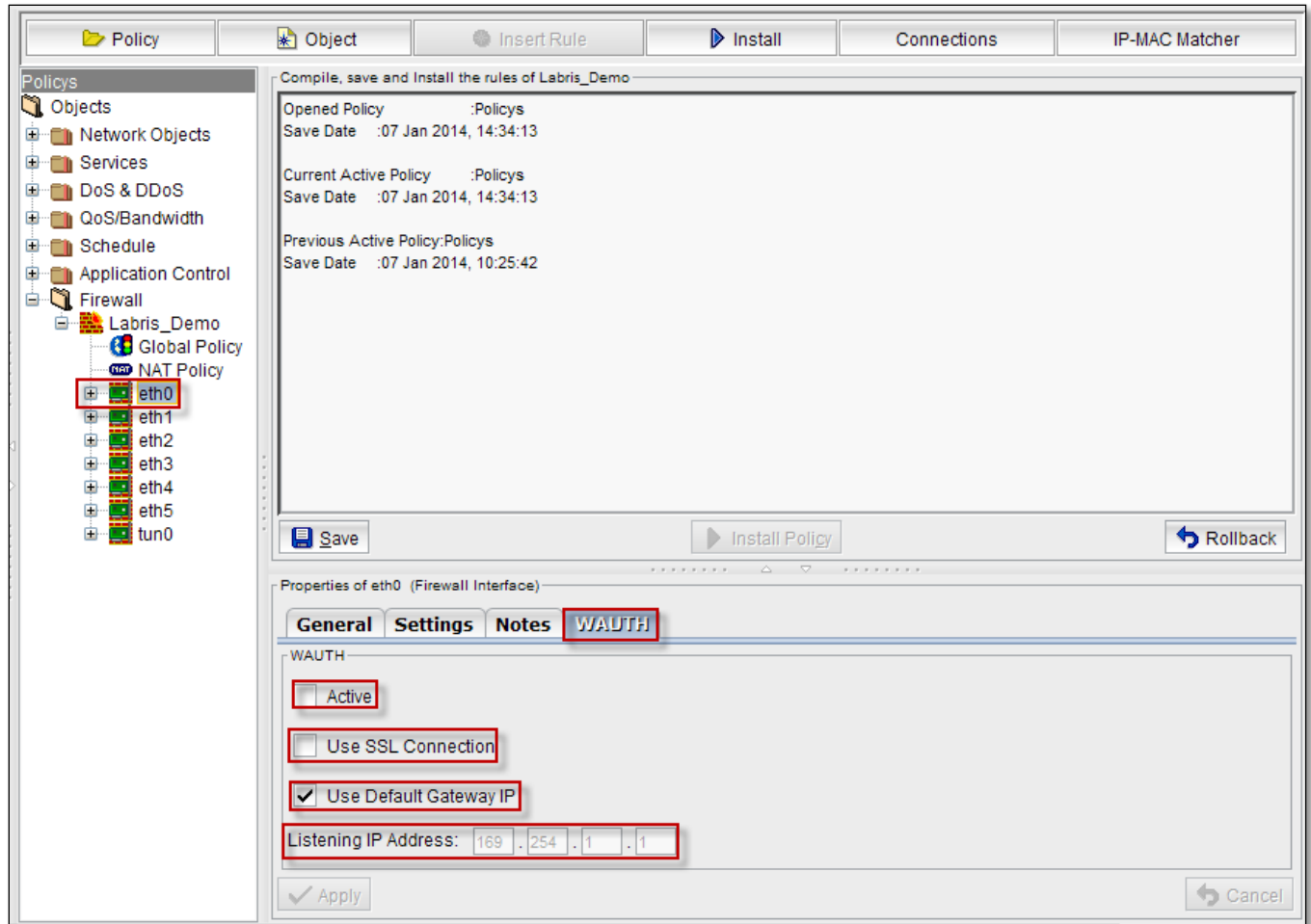
Select **Settings tab**, we can Enable or Disable **Dynamical source Address Translation**, This interface is an external network interface.



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).

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.

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.

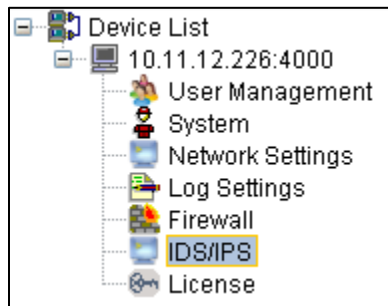
lfp DROP IN MNG IF	A management request connection which does not have management permission is blocked.
lfp DROP OUT MNG IF	Response to a management request connection which does not have management permission is blocked.
lfp DROP IN CONSOLE	Access to management ports is blocked.
lfp DROP OUT CONSOLE	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.

IDS/IPS

Right Click on the **IDS / IPS** tab and click on **Connect** to get connected to the IDS/IPS tab

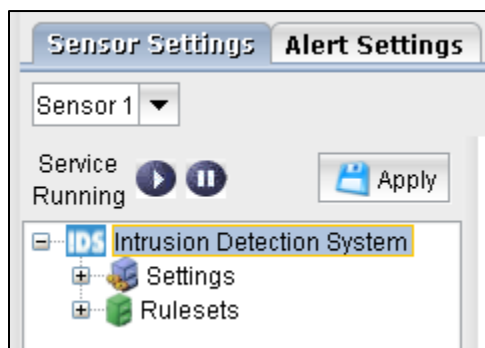


Sensor Settings

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



Settings

Network Settings

Under Intrusion Detection System we find options like **Settings > Network settings**

Sensor 1 configuration: listening all interfaces

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**.

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_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 \$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

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.

The screenshot shows the 'Sensor Settings' window for 'Sensor 1'. The 'Alert Settings' tab is active. On the left, the 'Intrusion Detection System' tree has 'Network Settings' highlighted. The main table lists variables and their values. The 'HOME_NET' variable is highlighted with a red box, showing a value of '10.1.1.0/24' and a status of 'Disabled'.

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

Below the table, the 'Variable Settings' section for 'HOME_NET' is shown, including its value and a detailed comment explaining how to configure it.

Changes are applied to the variables immediately. We can notice in the below screen.

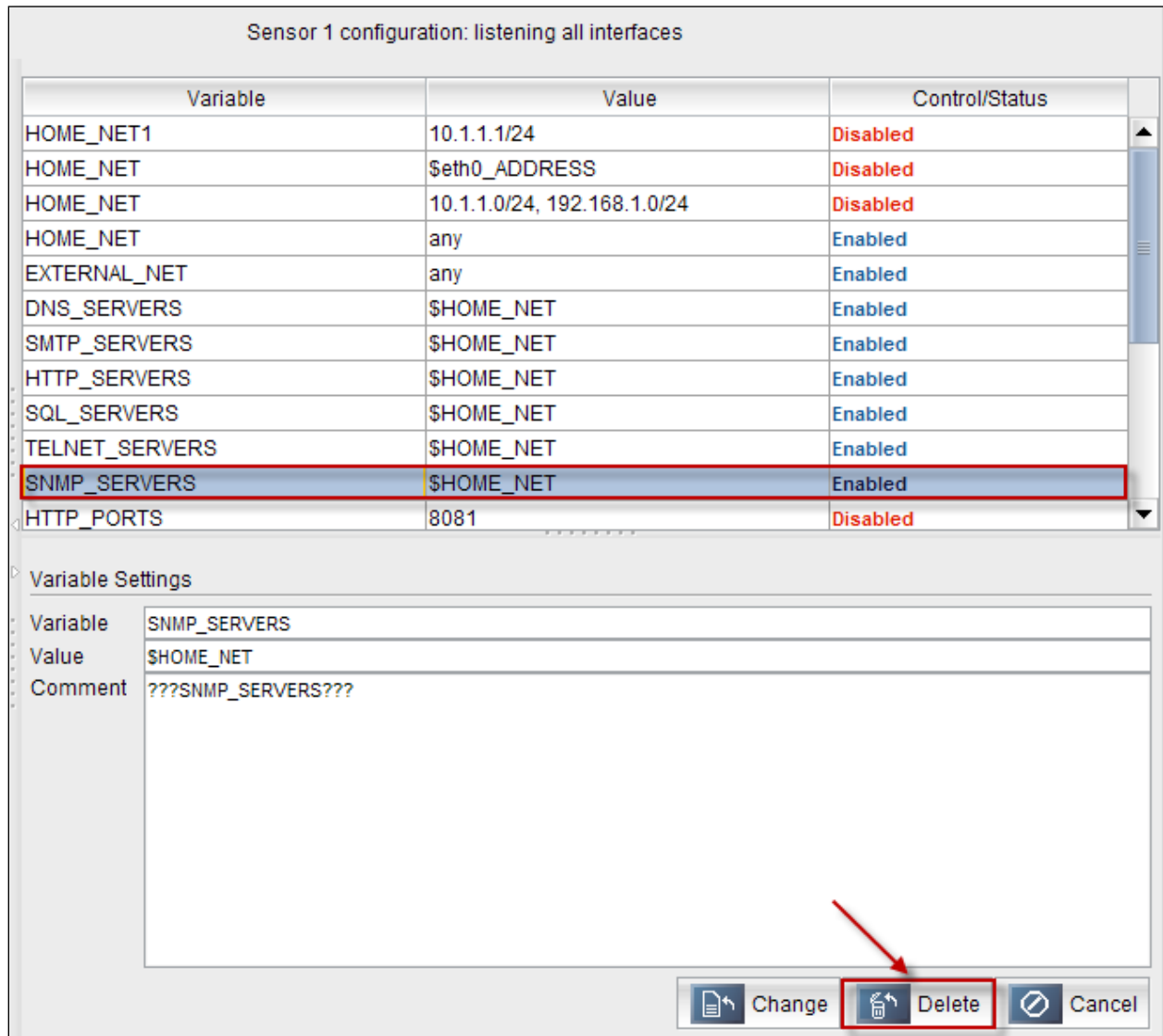
This screenshot shows the same 'Sensor Settings' window after the change. The 'HOME_NET' variable is now 'Enabled', as indicated by the green text in the 'Control/Status' column. The other variables and the 'Variable Settings' section remain the same.

Variable	Value	Control/Status
HOME_NET	10.1.1.0/24	Enabled
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

Deleting variable

Select one of the variables from the list right pane and click on **Delete**.

Selected variables are deleted from the list immediately.



Cancel

Click on **Cancel** tab to **revert back** to the same settings as before.

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
HTTP_PORTS	8081	Disabled
HTTP_PORTS	80	Enabled

Variable Settings

Variable: TELNET_SERVERS
Value: \$HOME_NET
Comment: List of telnet servers on your network.
This allows only look for attacks to systems that have a service up.
These configurations MUST follow the same configuration scheme as defined above for \$HOME_NET.

Change Delete **Cancel**

Labris Teknoloji

Click on **Apply** tab to **apply the modified settings** in Network settings tab

Sensor 1

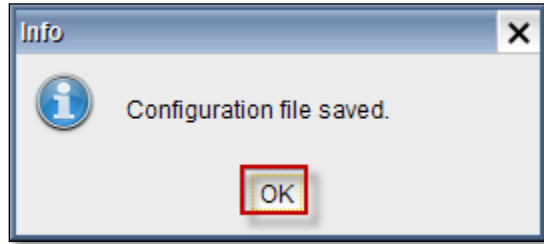
Service Running **Apply**

Intrusion Detection System
Settings
Network Settings
Interface
Rulesets

Sensor 1 configuration: listening all interfaces

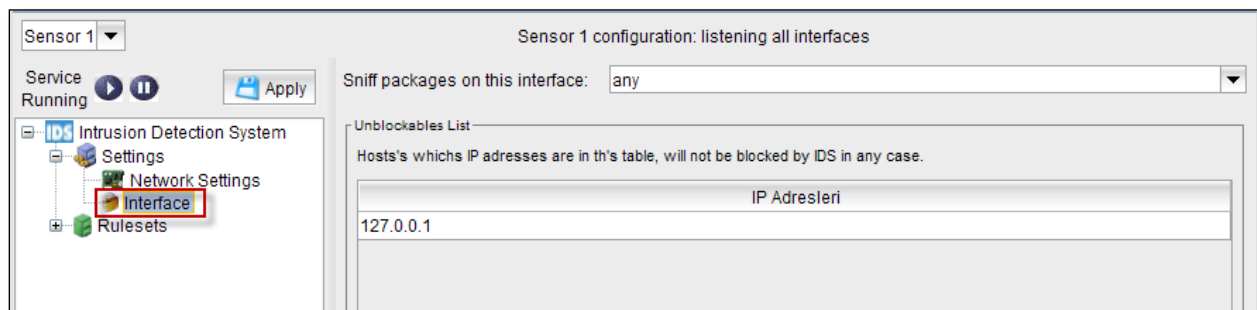
Variable	Value	Control/Status
HOME_NET1	10.1.1.1/24	Disabled
HOME_NET	\$eth0_ADDRESS	Disabled
HOME_NET	10.1.1.0/24, 192.168.1.0/24	Disabled
HOME_NET	any	Enabled
EXTERNAL_NET	any	Enabled
DNS_SERVERS	\$HOME_NET	Enabled
SMTP_SERVERS	\$HOME_NET	Enabled
HTTP_SERVERS	\$HOME_NET	Enabled
SQL_SERVERS	\$HOME_NET	Enabled
TELNET_SERVERS	\$HOME_NET	Enabled
SNMP_SERVERS	\$HOME_NET	Enabled
HTTP_PORTS	8081	Disabled

Click **Ok** to save the changes

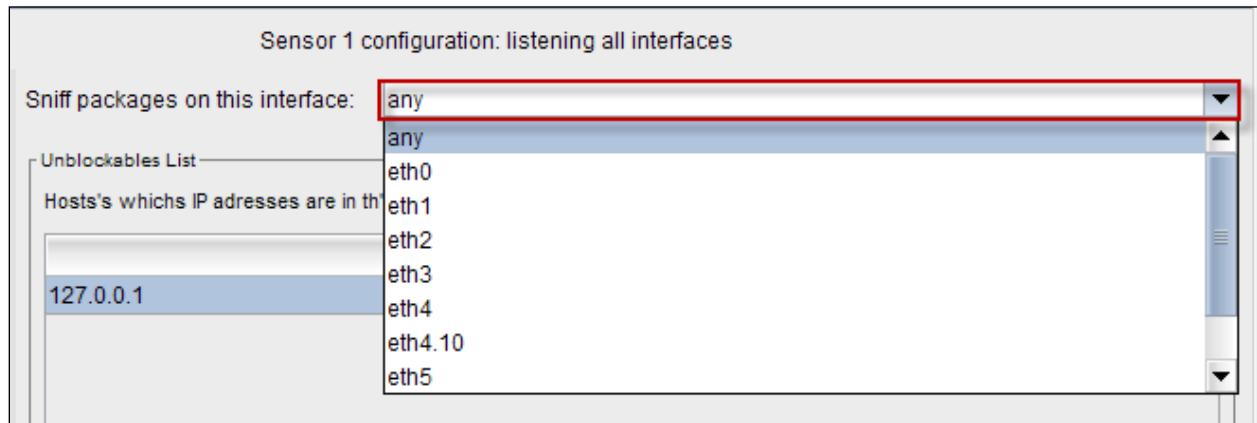


Interface

Select **Interface** tab from the left pane

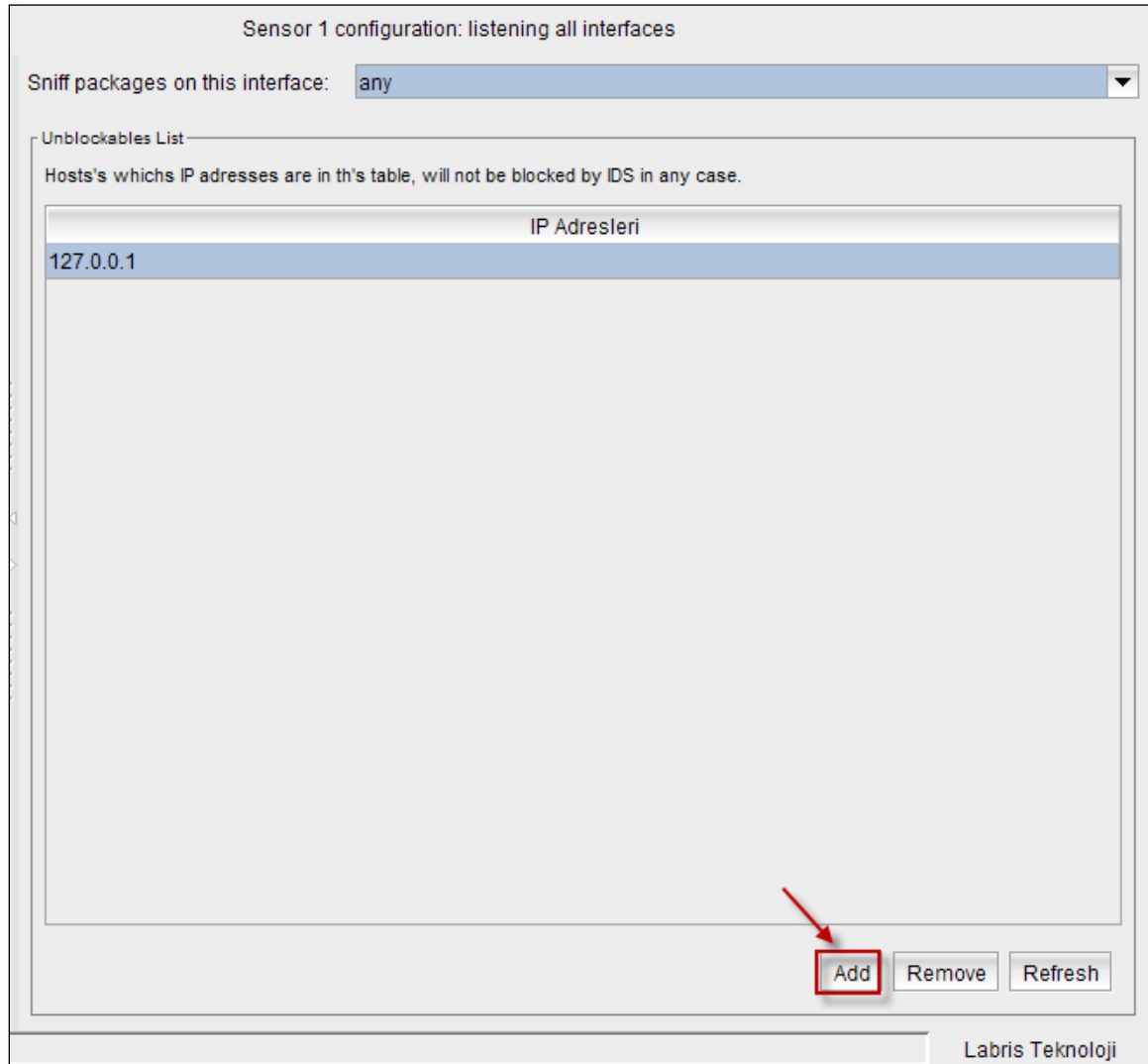


From the **drop down list** select any one of the required **Ethernet** type

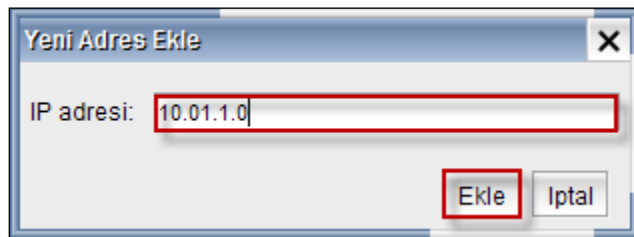


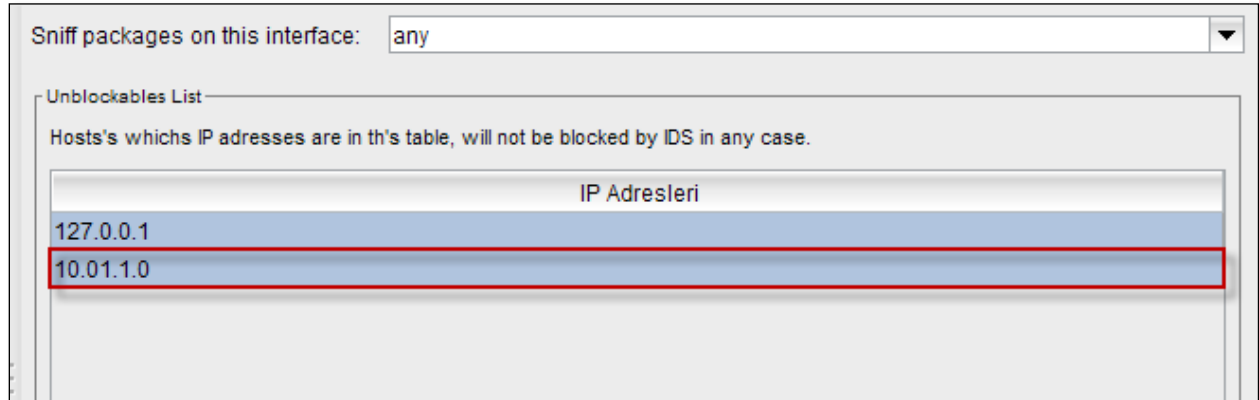
Adding IP

Click on **Add** tab to Add the new IP Address to the **unblockable list**



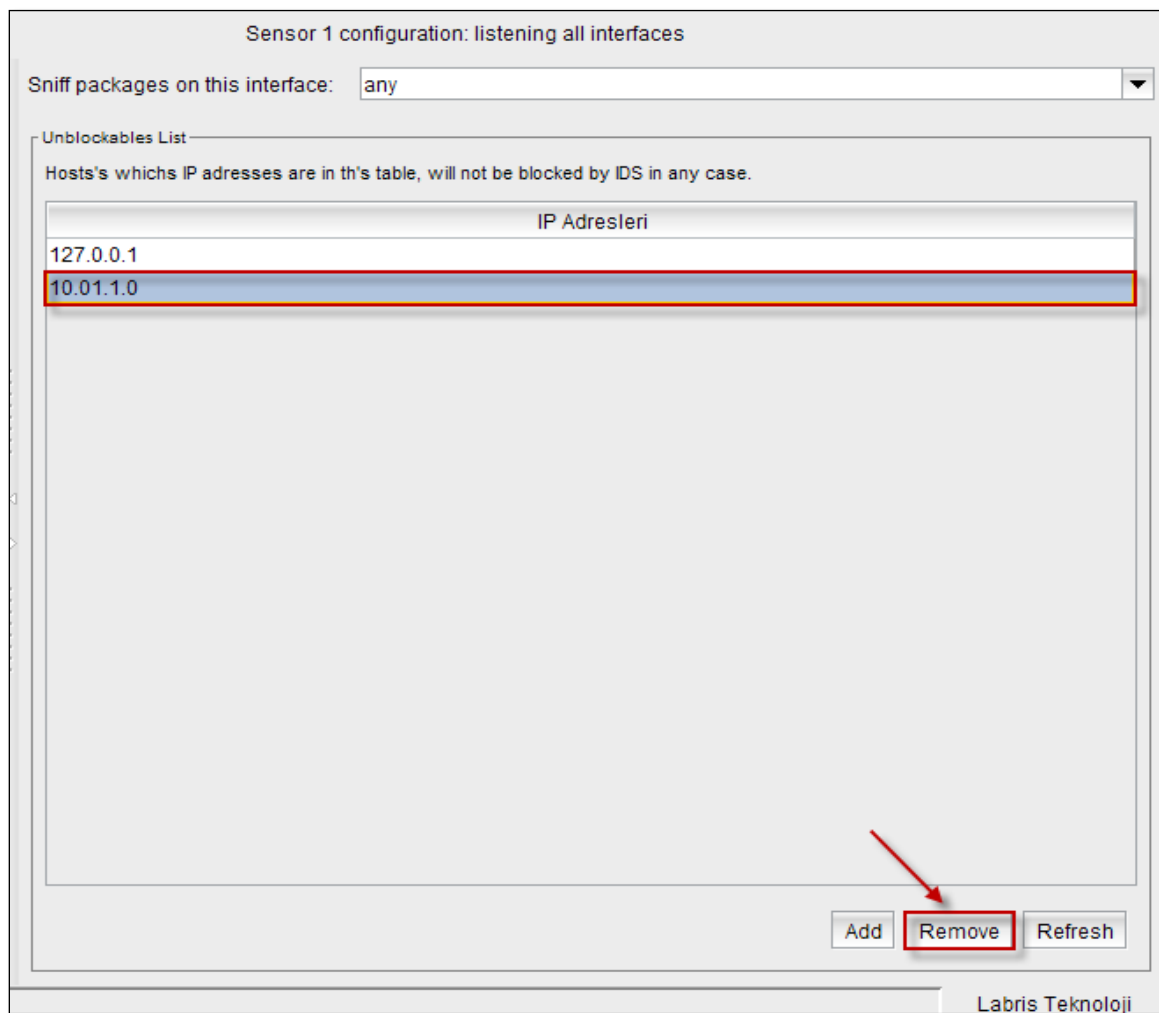
Enter the **IP Address** which you wanted to add to the list and click on **"EKLE"**





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.

Sensor 1 configuration: listening all interfaces

Sniff packages on this interface:

Unblockables List

Hosts's whichs IP addresses are in th's table, will not be blocked by IDS in any case.

IP Adresleri
127.0.0.1

Refresh

Click on **Refresh** Tab to refresh the entire tab.

Sniff packages on this interface:

Unblockables List

Hosts's whichs IP addresses are in th's table, will not be blocked by IDS in any case.

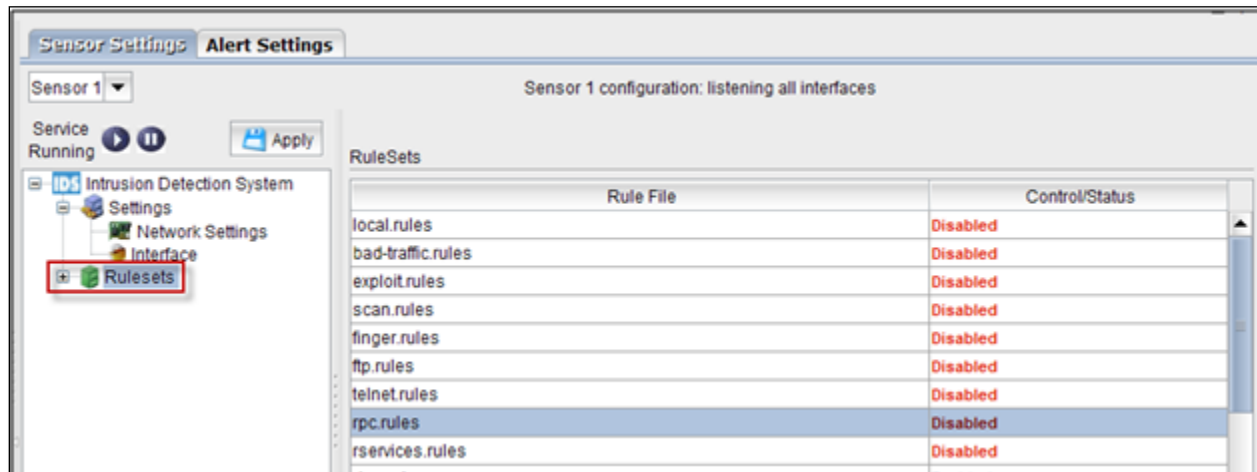
IP Adresleri
127.0.0.1

Add Remove Refresh

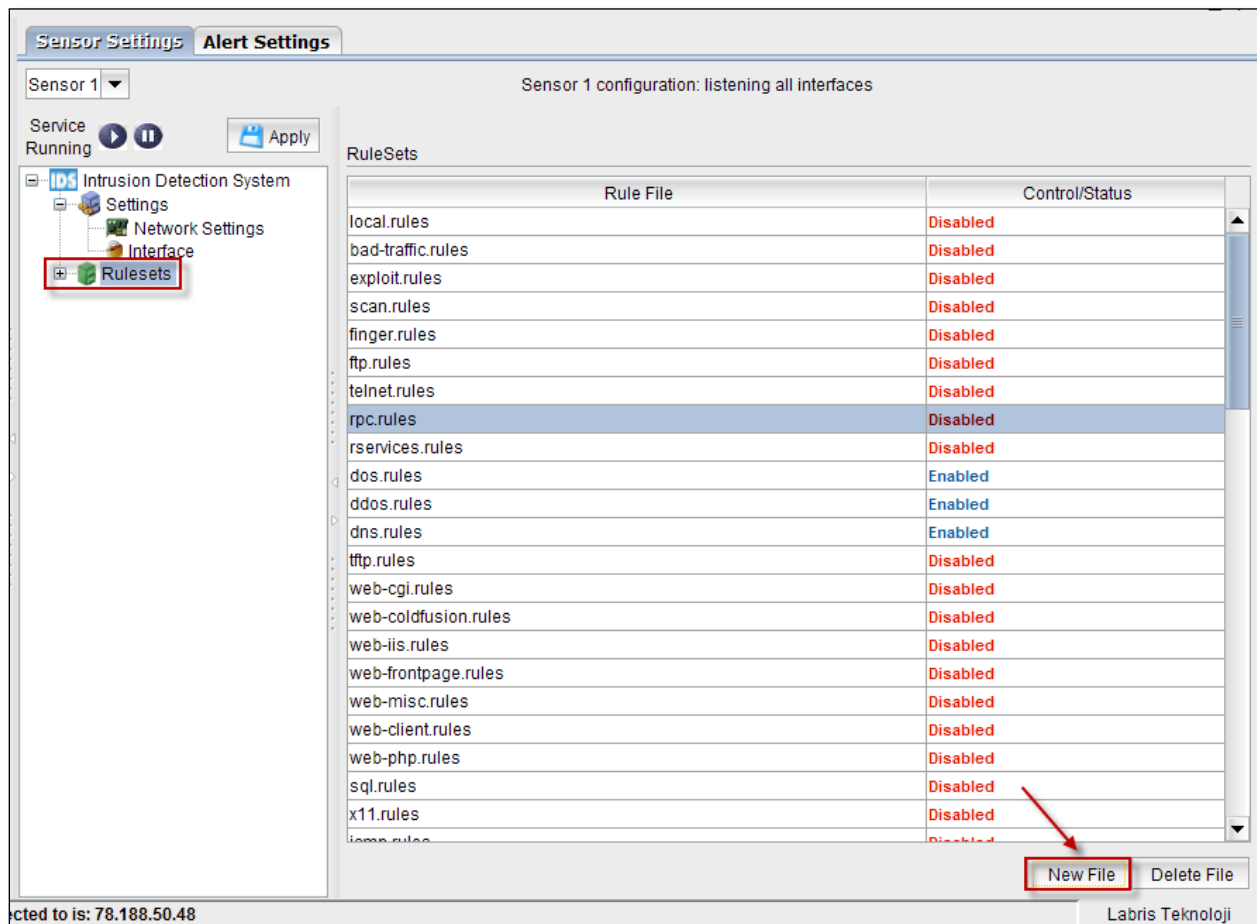
Labris Teknoloji

Rule sets

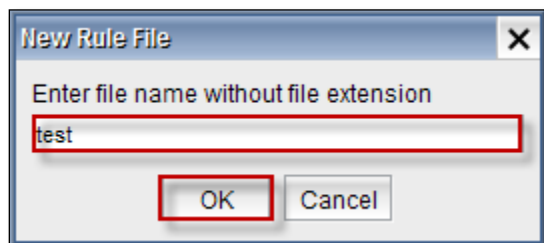
Select **Rulesets** tab from the left pane.



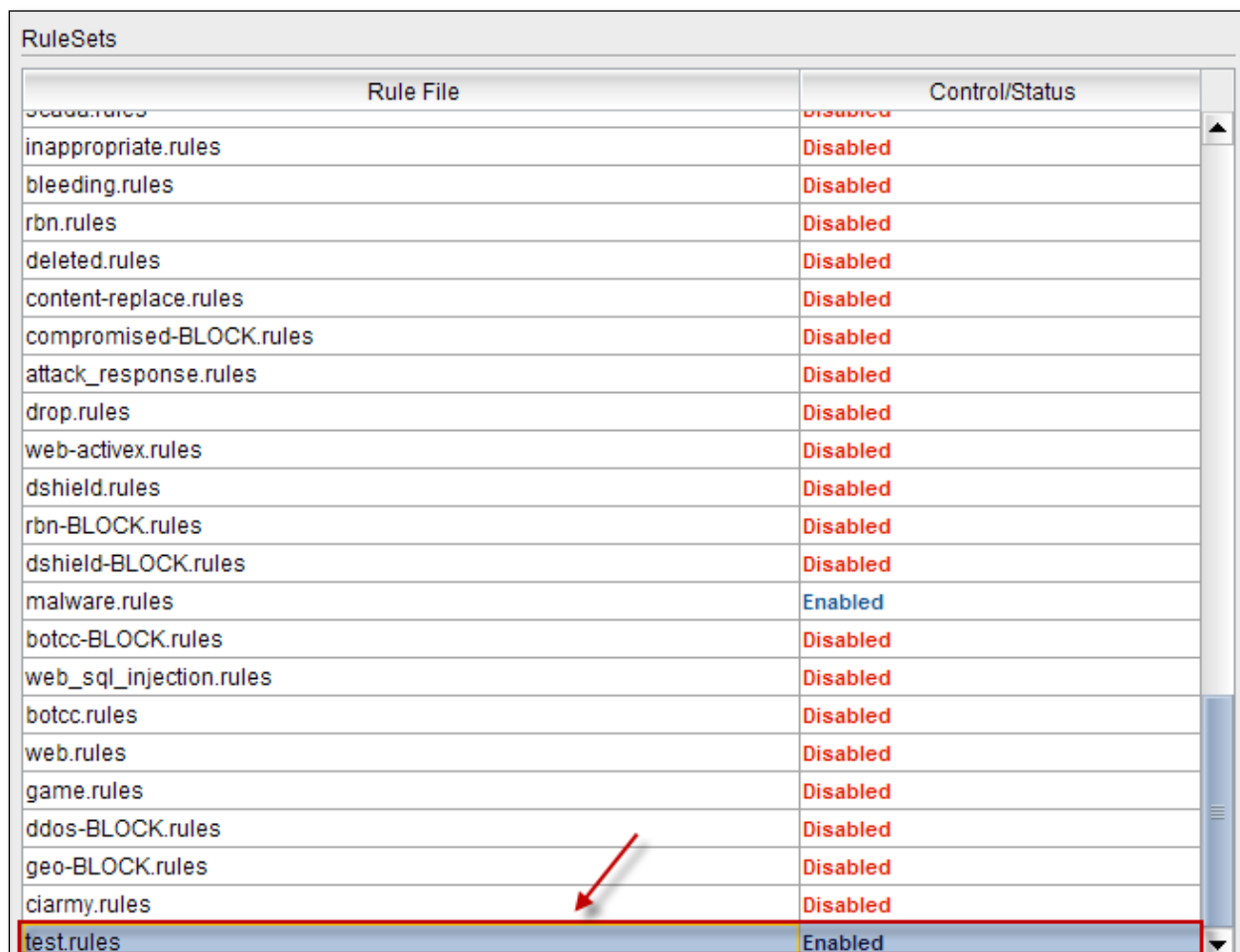
Click on **New File** to create a new rule file.



Give the **name** of the file without any extension and click **Ok**.

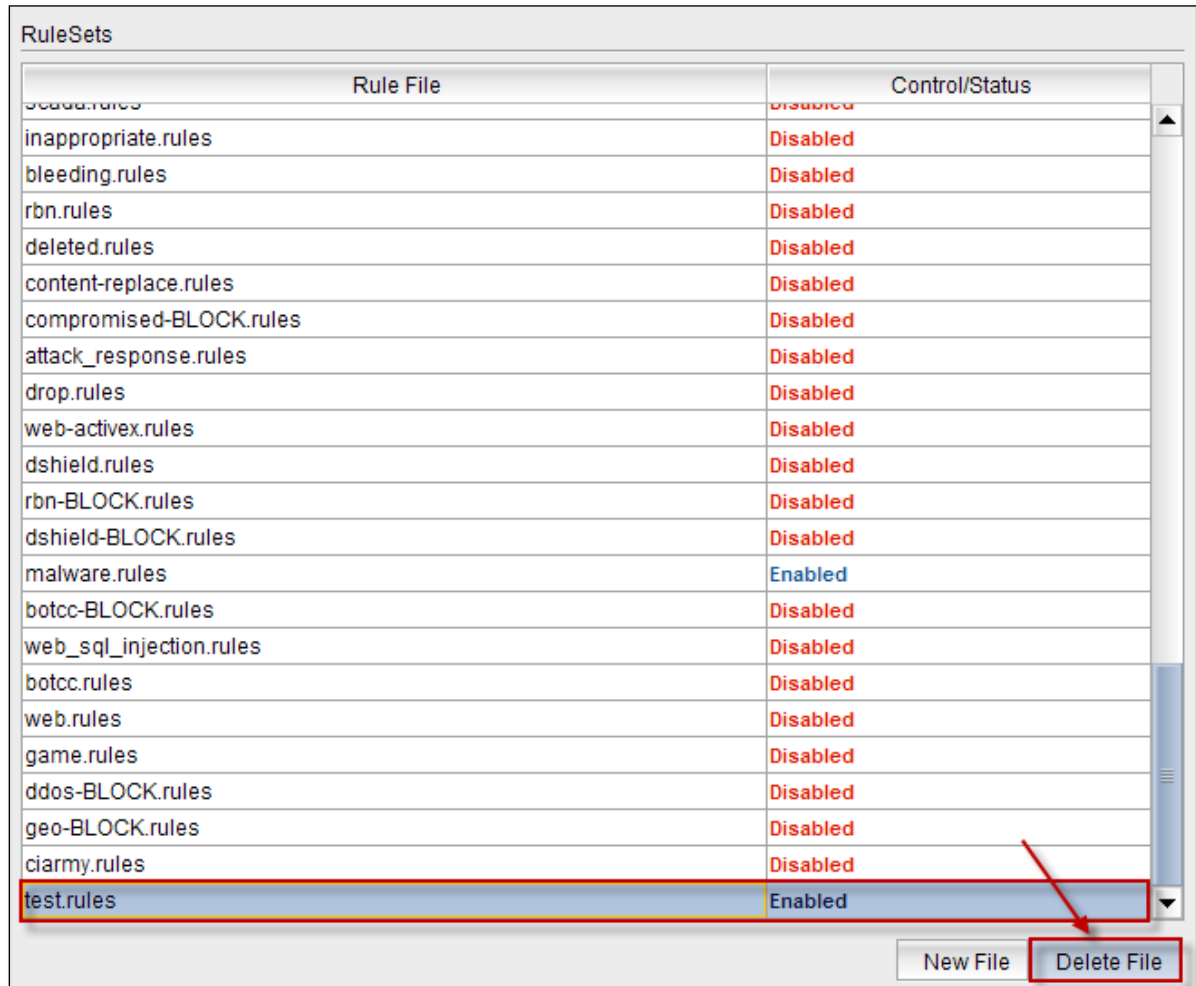


You can notice that the new file with the name **test** is **added** to the list.



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 form the list and click on **delete file** tab to remove the file form the list.

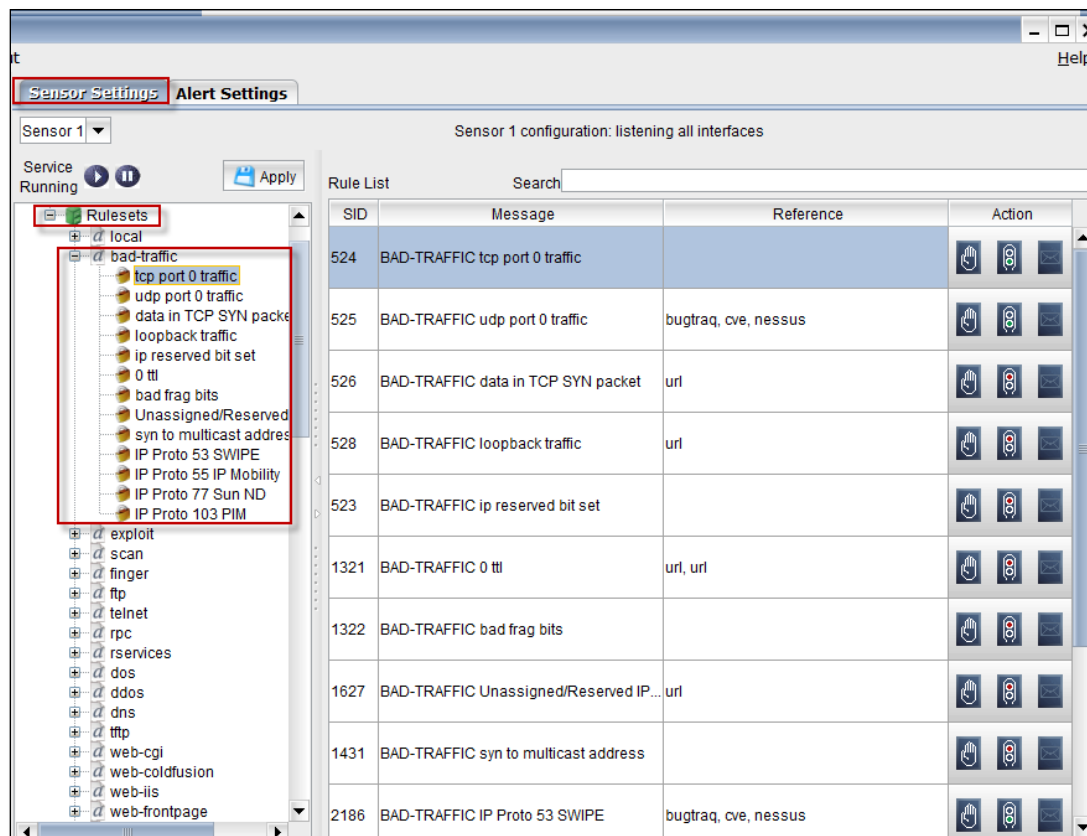


Rulesets List

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**.

Sensor Settings **Alert Settings**

Sensor 1 configuration: listening all interfaces

Service Running Apply

Rulesets

- local
 - bad-traffic
 - tcp port 0 traffic
 - udp port 0 traffic
 - data in TCP SYN packets**
 - loopback traffic
 - ip reserved bit set
 - 0 ttl
 - bad frag bits
 - Unassigned/Reserved
 - syn to multicast address
 - IP Proto 53 SWIPE
 - IP Proto 55 IP Mobility

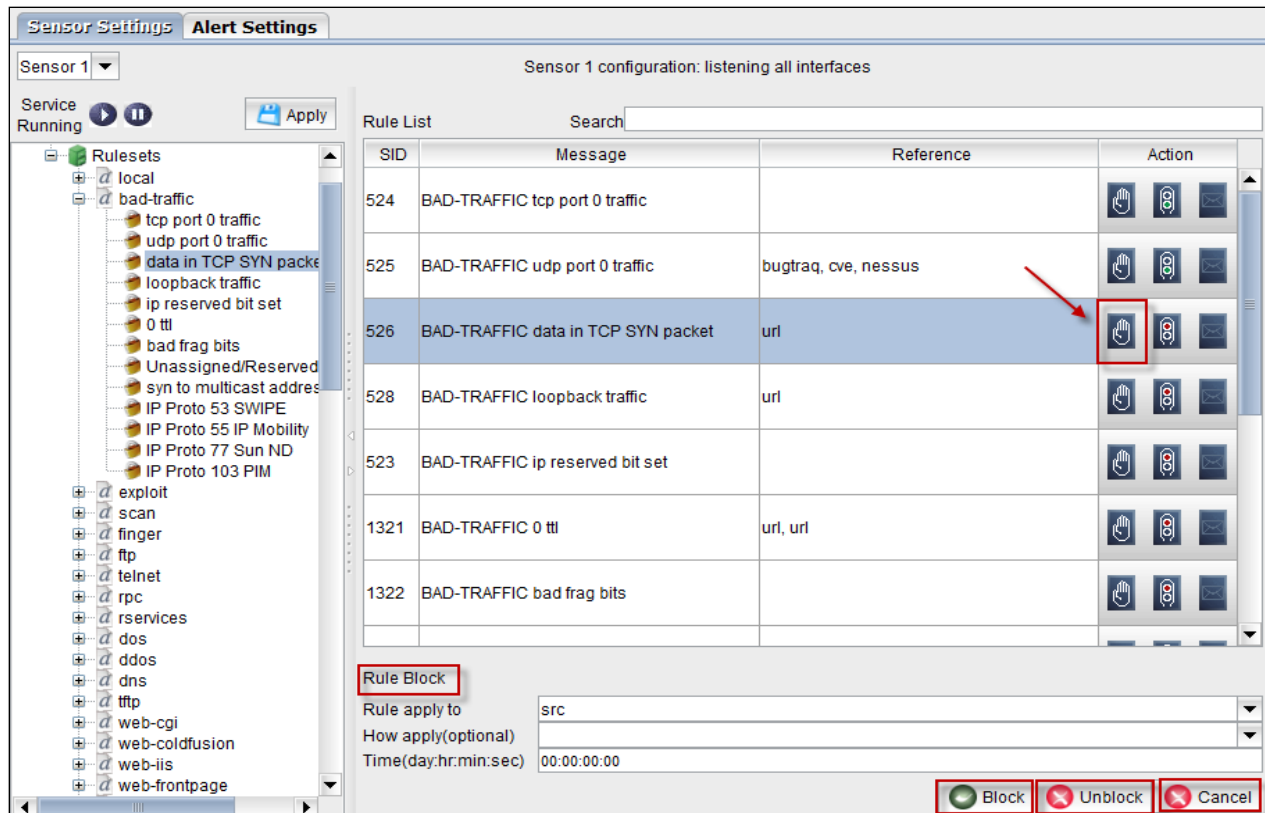
Rule List Search

SID	Message	Reference	Action
524	BAD-TRAFFIC tcp port 0 traffic		
525	BAD-TRAFFIC udp port 0 traffic	bugtraq, cve, nessus	
526	BAD-TRAFFIC data in TCP SYN packet	url	
528	BAD-TRAFFIC loopback traffic	url	

Click on



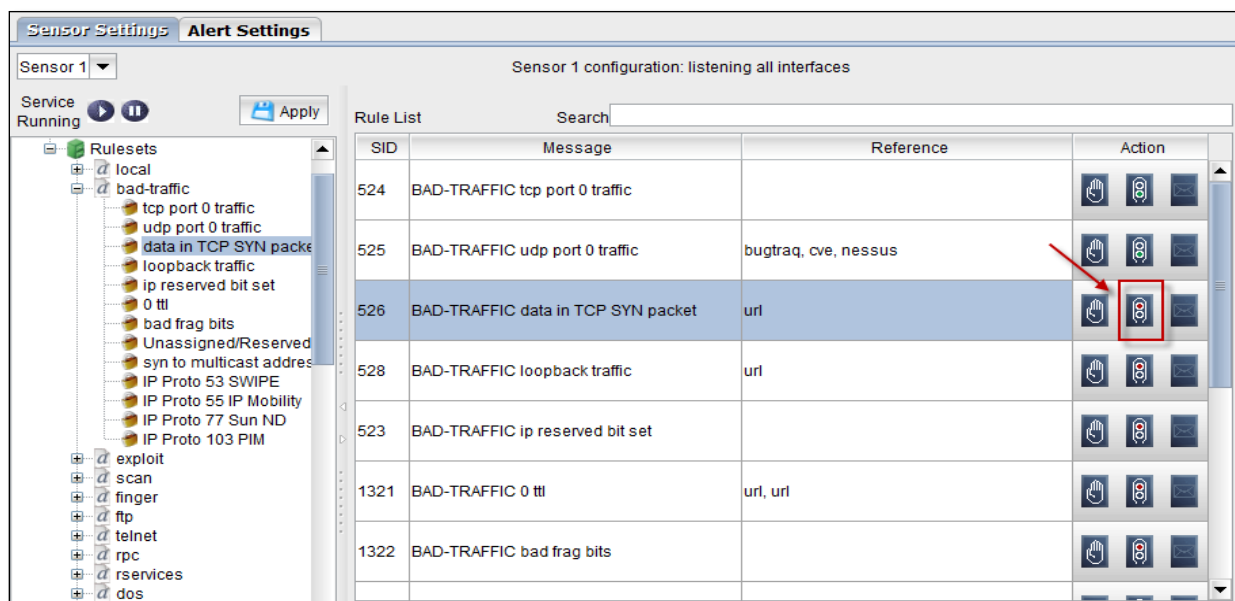
the icon from the Action Tab to **Block**, **UnBlock** or **cancel** the selected Rule.



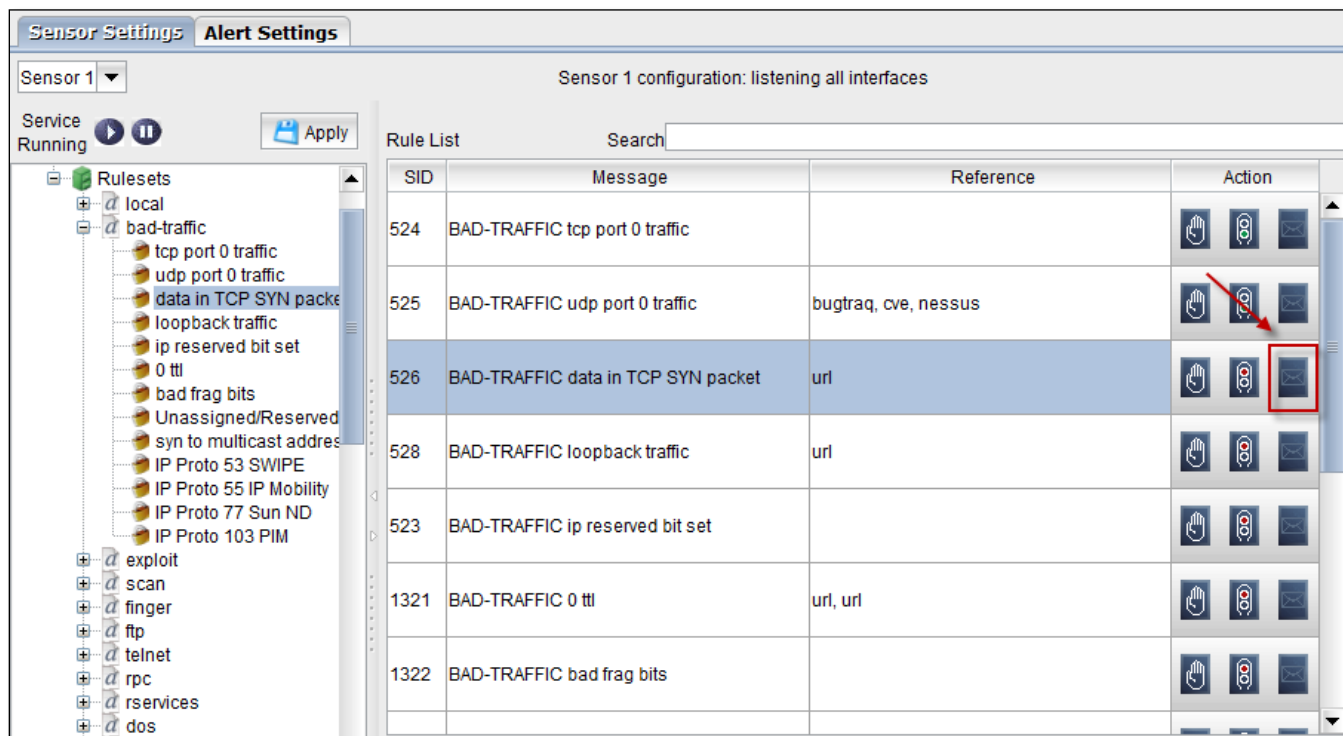
Click on the highlighted icon to **Start / Stop** the Rule.

Red Light – Stop

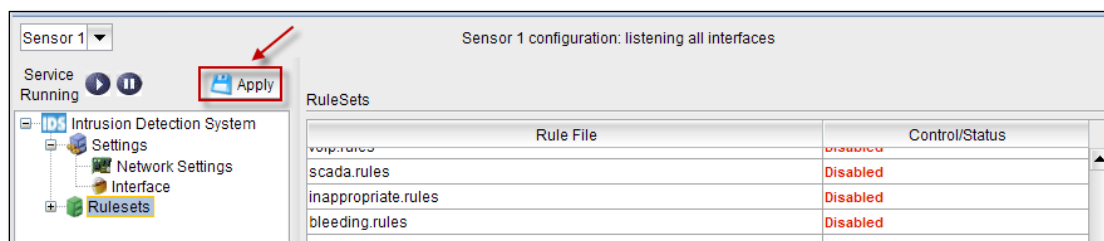
Green Light - Start



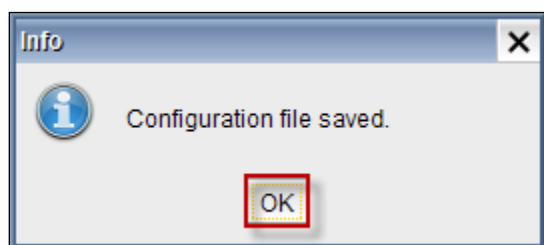
Click on the highlighted icon to redirect to the reference URL which is specified in the list.



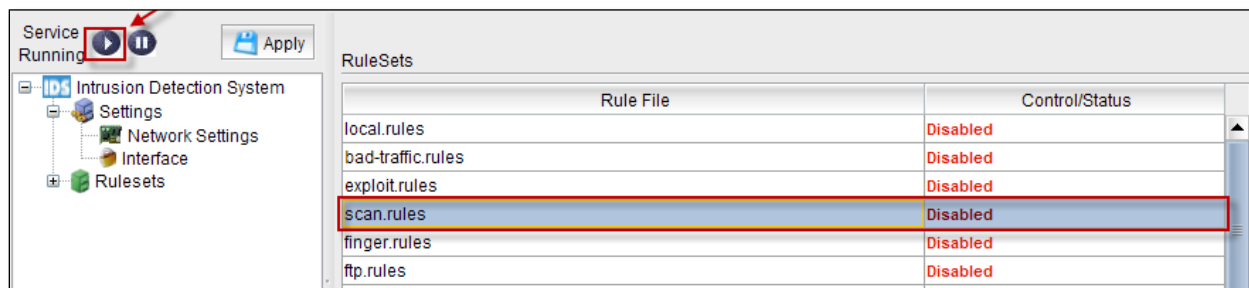
Click on **Apply** tab to **apply the modified settings** in Rulesets tab.



Click on **Ok** to save the changes.



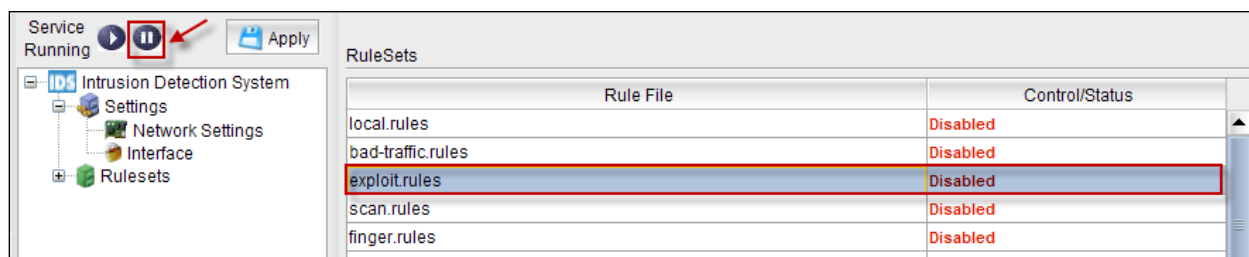
Click on the **Start** tab as shown in the screen to start the IDS Service for chosen sensor



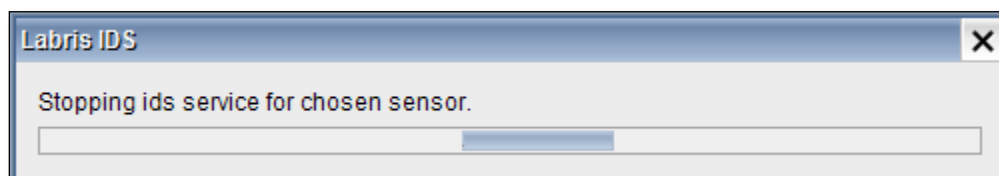
Below screen appears stating that Starting IDS service is in progress.



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.



Alert Settings

In the **Alert** tab we can find options like **Mail Alert Settings** ,**Report Mails** and **Alerts**.

Sensor SettingsAlert Settings

Mail Alert Settings

Sender mail address: The mail address that is used to post alerts by the ids mail alert service.
Administrator Mail: Alert mails will be sent to this address.
SMTP server: IP address of the SMTP server in the network.

Sender mail address

ids@labristeknoloji.com




Administrator mail address

admin@labristeknoloji.com

SMTP host

smtp.example.com

Mail Alert Service Status: Running



Report Mails

To: admin@labristeknoloji.com

Schedule: Every Day

00:00

Alerts

IDS alert duration on database (Day)

15

Save

Mail Alert Settings

Give the inputs in the below fields.

Mail Alert Settings

Sender mail address: The mail address that is used to post alerts by the ids mail alert service.
Administrator Mail: Alert mails will be sent to this address.
SMTP server: IP address of the SMTP server in the network.

Sender mail address

ids@labristeknoloji.com

1

Administrator mail address

admin@labristeknoloji.com




2

SMTP host

smtp.example.com

3

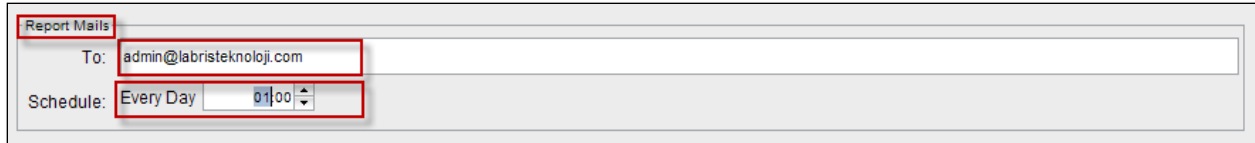
Mail Alert Service Status: Running



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.



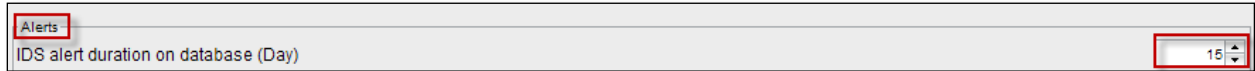
Report Mails

To: admin@labristeknoloji.com

Schedule: Every Day 01:00

Alerts

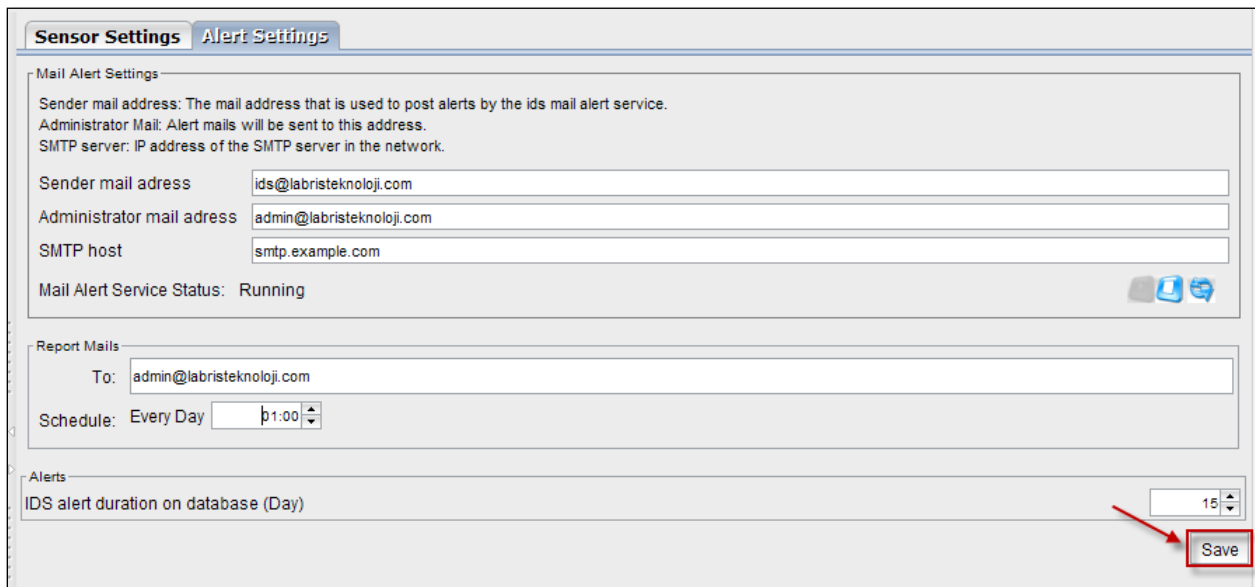
In the **Alerts** tab, we can change the **IDS Alert Duration** depending on the requirement.



Alerts

IDS alert duration on database (Day) 15

Click on **save** tab to save the modified settings



Sensor Settings **Alert Settings**

Mail Alert Settings

Sender mail address: The mail address that is used to post alerts by the ids mail alert service.
Administrator Mail: Alert mails will be sent to this address.
SMTP server: IP address of the SMTP server in the network.

Sender mail address: ids@labristeknoloji.com
Administrator mail address: admin@labristeknoloji.com
SMTP host: smtp.example.com

Mail Alert Service Status: Running

Report Mails

To: admin@labristeknoloji.com
Schedule: Every Day 01:00

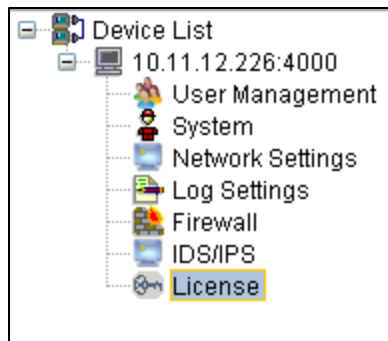
Alerts

IDS alert duration on database (Day) 15

Save

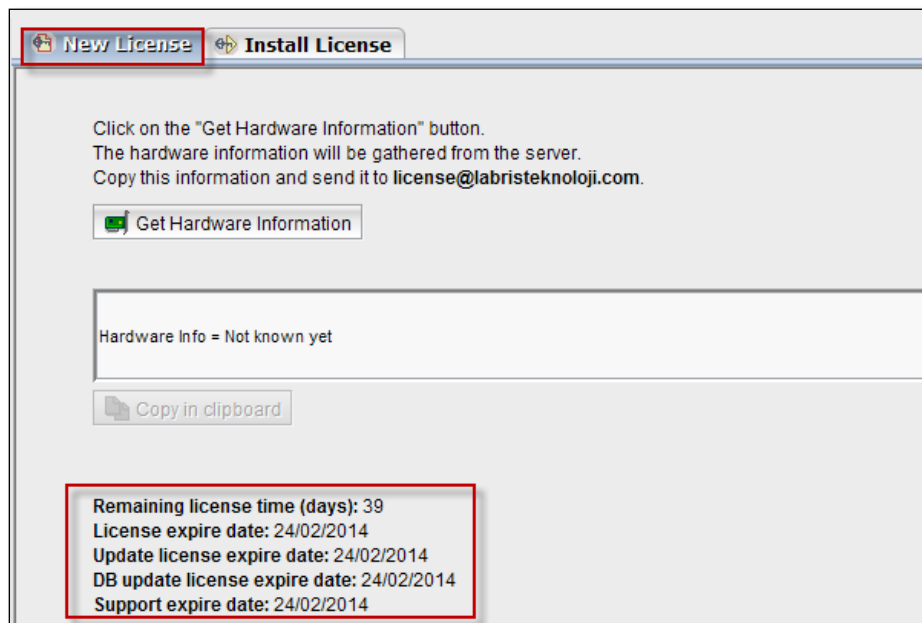
License

Right click on License and select **connect**.

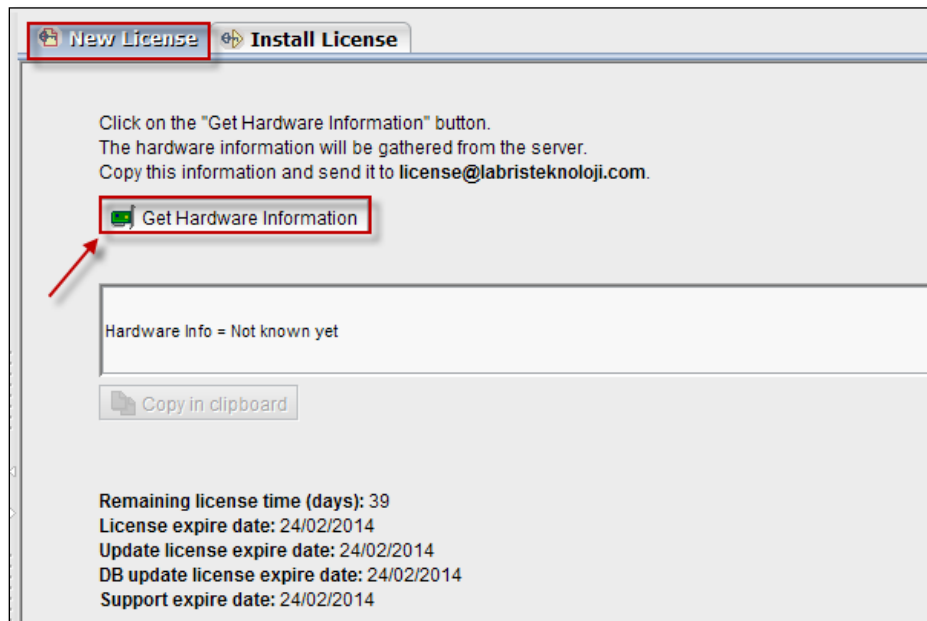


New License

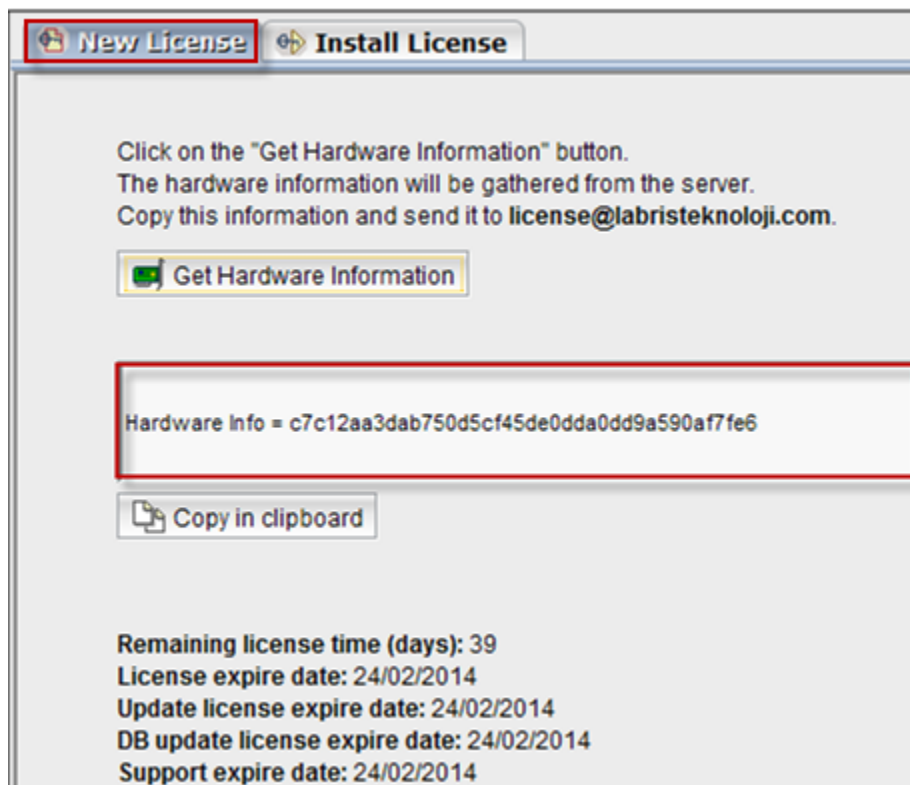
Click on **New License**, Information regarding License is being displayed.



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**.

New License Install License

Enter the file path and name or choose the file by clicking on "Open" file.
Then click on "Install" button to install the license file on the server.

File: Open File

Signature Open File

Send the file to the server

Note

For License file, please request from the service provider.

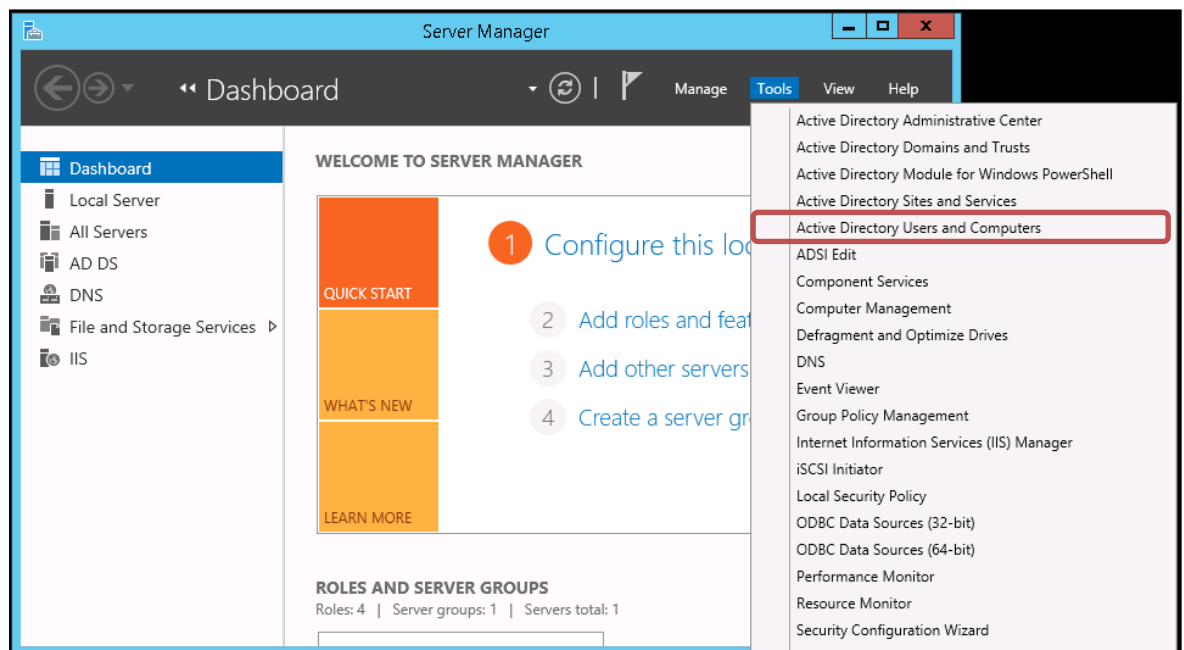
NTLM Authentication AD Configuration

Active Directory users can be used in areas such as URL Log, Wauth by integrating Labris products with Active Directory. Authorization can be made with the user name or rules can be written.

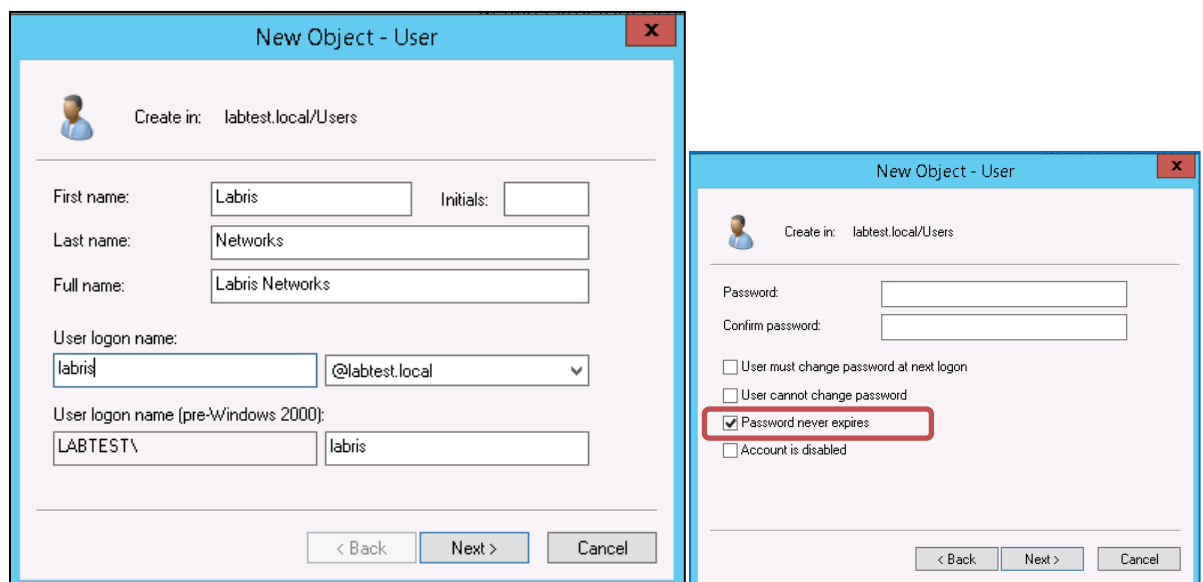
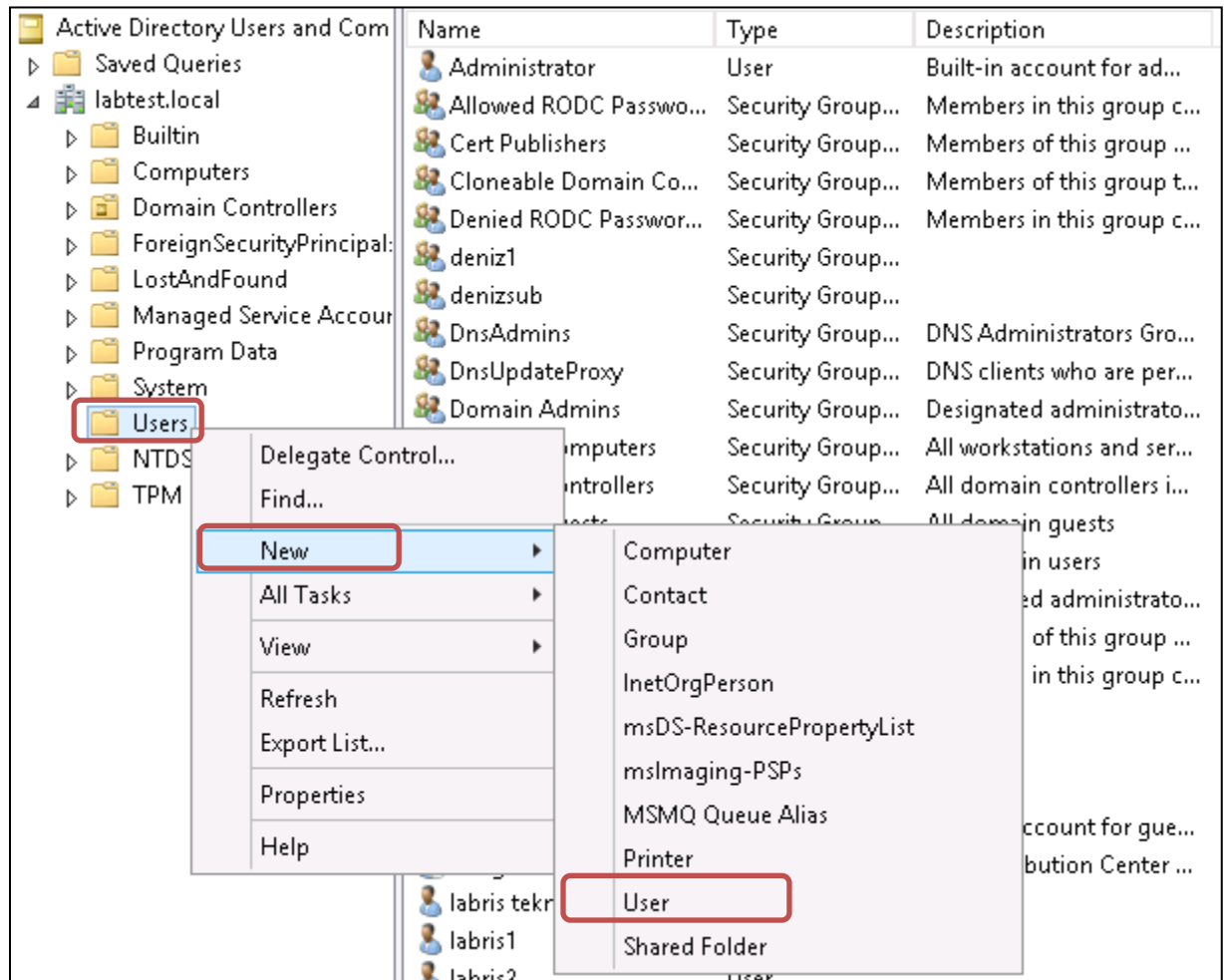
Active Directory Integration

Step 1: User and computer registration open on active directory for the integration of Labris.

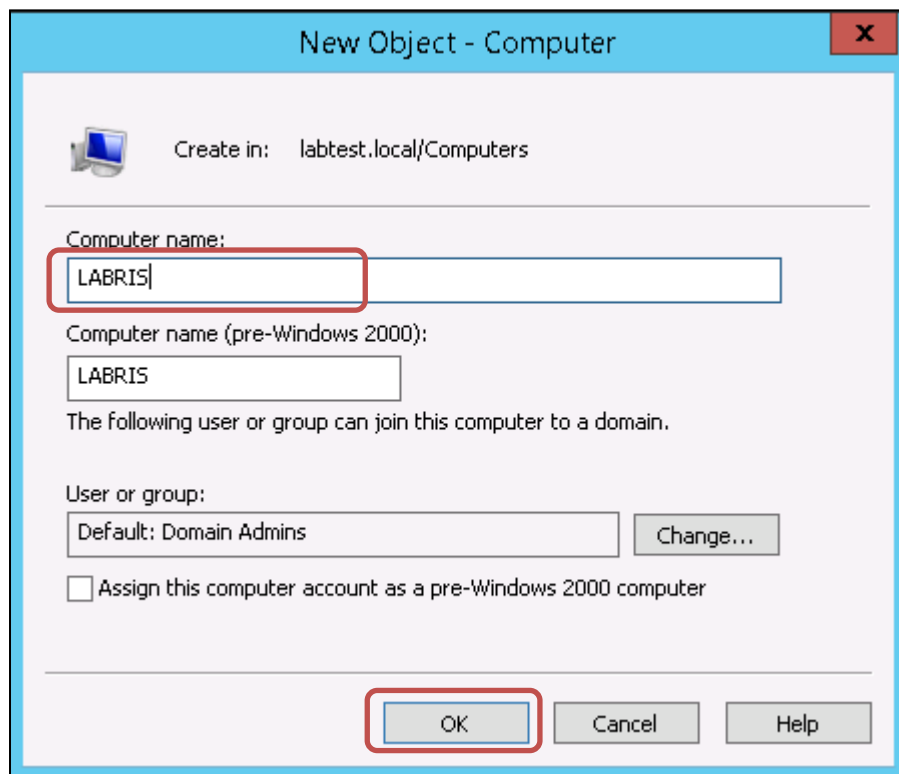
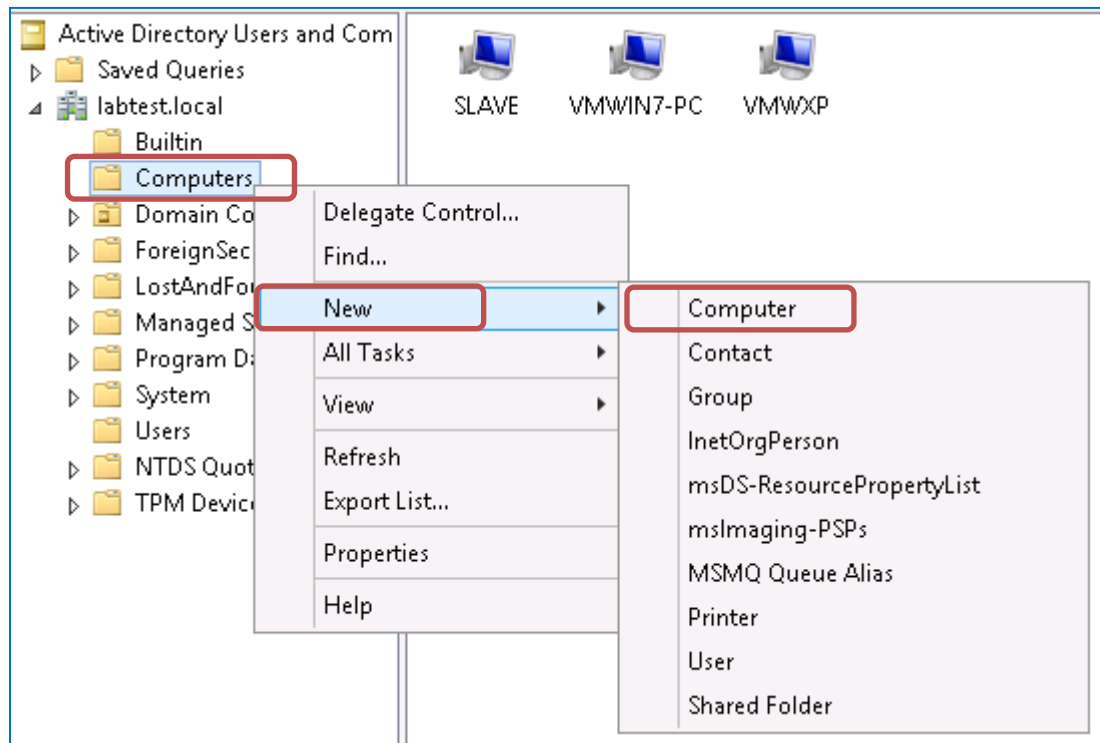
- a. It is entered **Active Directory Users and Computers** management window.



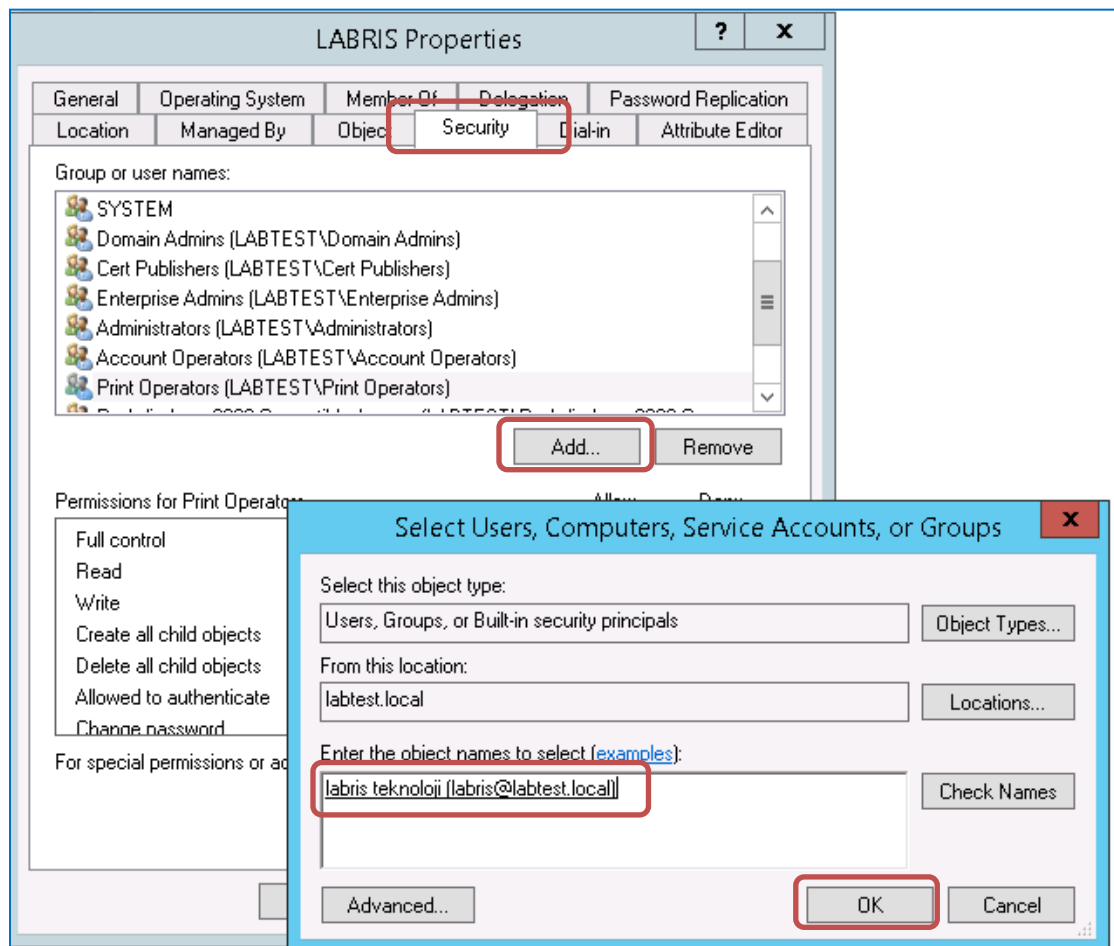
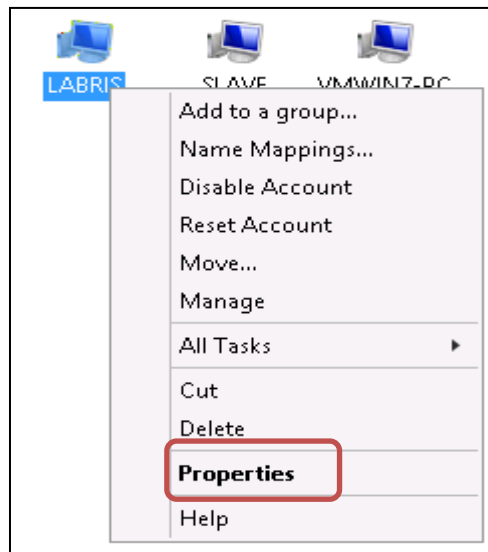
- b. A user is created with the name called as "Labris" under **users**.

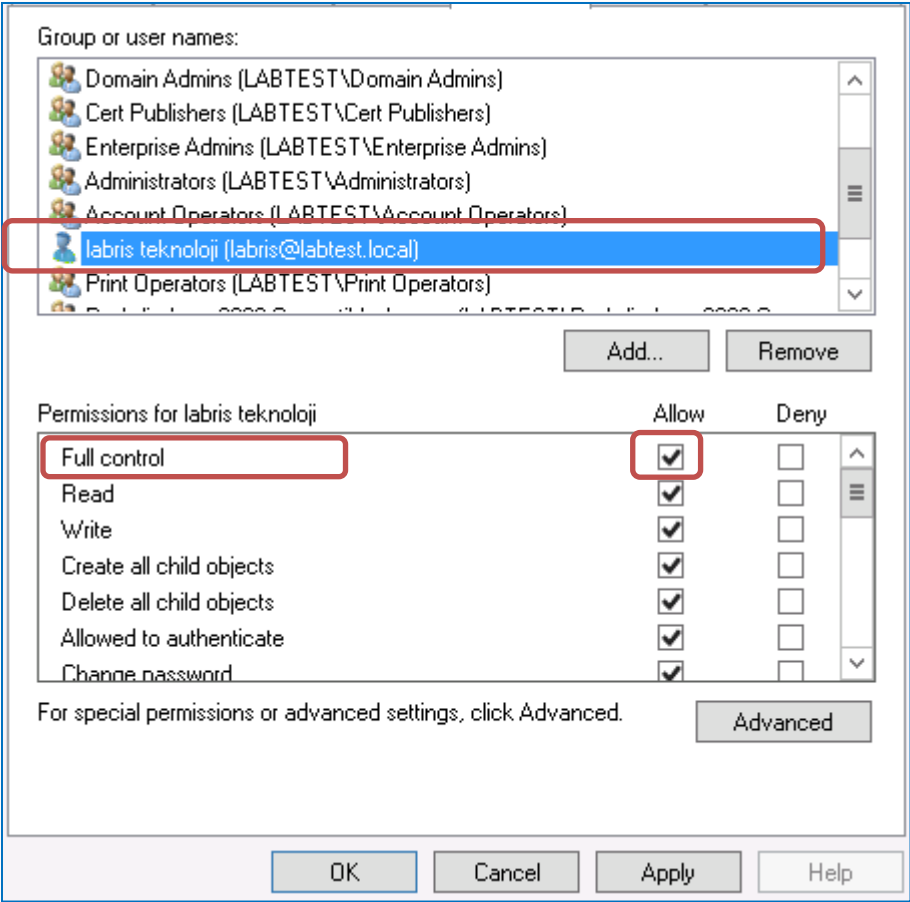


- c. Computer registration opens with Labris device name (hostname) under **computers**. You can view the computer name of Labris from **Labris management console> System> General Settings**.



- d. Full authority from the security field is given for **labris** user opened on defined **computer**. If you cannot see the security area, **View > Advanced Features** are selected.





Step 2: Labris Active Directory settings are made.

NTLM authentication information is entered by CLI.

webfilter-join-domain

Usage: webfilter-join-domain <realm> <dc-hostname> <dc> <ads> <user> <password> [workgroup]

Example:

webfilter-join-domain labtest.local w2k12.labtest.local 172.16.17.110 172.16.17.110 labris Asd12345 LABTEST

```
[root@logtest ~]# webfilter-join-domain labtest.local w2k12.labtest.local 172.16.17.110 172.16.17.110 labris Asd12345 LABTEST
Shutting down SMB services: [ OK ]

Shutting down Winbind services: [ OK ]
172.16.17.110
172.16.17.110
PING 172.16.17.110 (172.16.17.110) 56(84) bytes of data.
64 bytes from 172.16.17.110: icmp_seq=1 ttl=128 time=1.00 ms
64 bytes from 172.16.17.110: icmp_seq=2 ttl=128 time=0.000 ms

--- 172.16.17.110 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.000/0.500/1.000/0.500 ms
PING 172.16.17.110 (172.16.17.110) 56(84) bytes of data.
64 bytes from 172.16.17.110: icmp_seq=1 ttl=128 time=0.000 ms
64 bytes from 172.16.17.110: icmp_seq=2 ttl=128 time=0.000 ms

--- 172.16.17.110 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.000/0.000/0.000/0.000 ms
Connection to 172.16.17.110 389 port [tcp/ldap] succeeded!
return code: 0
[root@logtest ~]#
```

Return Code should be 0.

These are the inputs for the Active Directory Integration

No	Parameter	Value	Description
1	realm	labtest.local	Active Directory Domain name is written.
2	dc-hostname	w2k12.labtest.local	Domain name is written with the name of Active Directory server.
3	dc	172.16.17.110	Active Directory server's IP address is written.
4	adc	172.16.17.110	Active Directory server's IP address is written.
5	user	labris	Active Directory username.
6	password	Asd12345	Active Directory password.
7	workgroup	LABTEST	Active directory domain name is entered.

Integration can be checked with the following subjects.






wbinfo -t

net ads testjoin

```
[root@test1 ~]# wbinfo -t
checking the trust secret via RPC calls succeeded
[root@test1 ~]# net ads testjoin
Join is OK
```

Step 3: Active Directory users and groups are displayed on User Management module.

Refresh button is pressed after the integration and click **OK** in the warning appeared on the screen. As seen in the picture, it can be seen that Active Directory users are listed.

Users Groups WAUTH						
Select All <input type="checkbox"/>	 Delete	 Edit	 Add	<input type="text"/>		 Filter
	User Name	Name Surname	Source	Domain	Global	Note
<input type="checkbox"/>	test	test	labris	slave	<input type="checkbox"/>	
<input type="checkbox"/>	labris4		ad	labtest.local	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	krbtgt		ad	labtest.local	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	labris6		ad	labtest.local	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	labris2		ad	labtest.local	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	labris	Labris Networks	labris	slave	<input type="checkbox"/>	
<input type="checkbox"/>	labris3		ad	labtest.local	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	aaa		ad	labtest.local	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	guest		ad	labtest.local	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	lanris1		ad	labtest.local	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	administrator		ad	labtest.local	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	logtest1		ad	labtest.local	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	suleyman		ad	labtest.local	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	labris5		ad	labtest.local	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	labris		ad	labtest.local	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	logtest		ad	labtest.local	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	bbb		ad	labtest.local	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	12345678901	admin	labris	slave	<input type="checkbox"/>	
						 Refresh

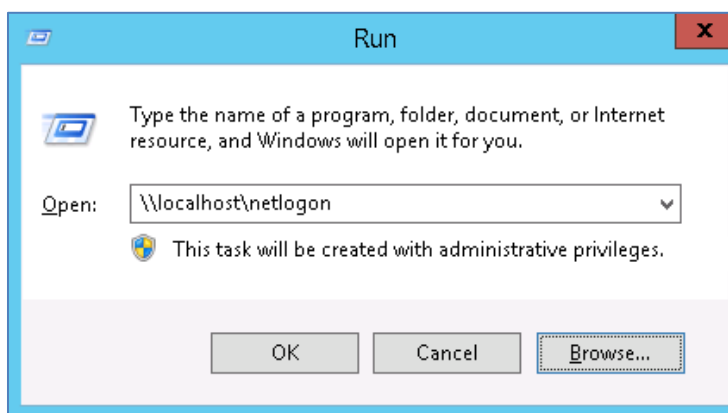
Windows Labris Logon Tracer

Windows Logon Tracer is the software for monitoring and informing logon status of AD users. User names will be shown in Labris logs thanks to Logon Tracer.

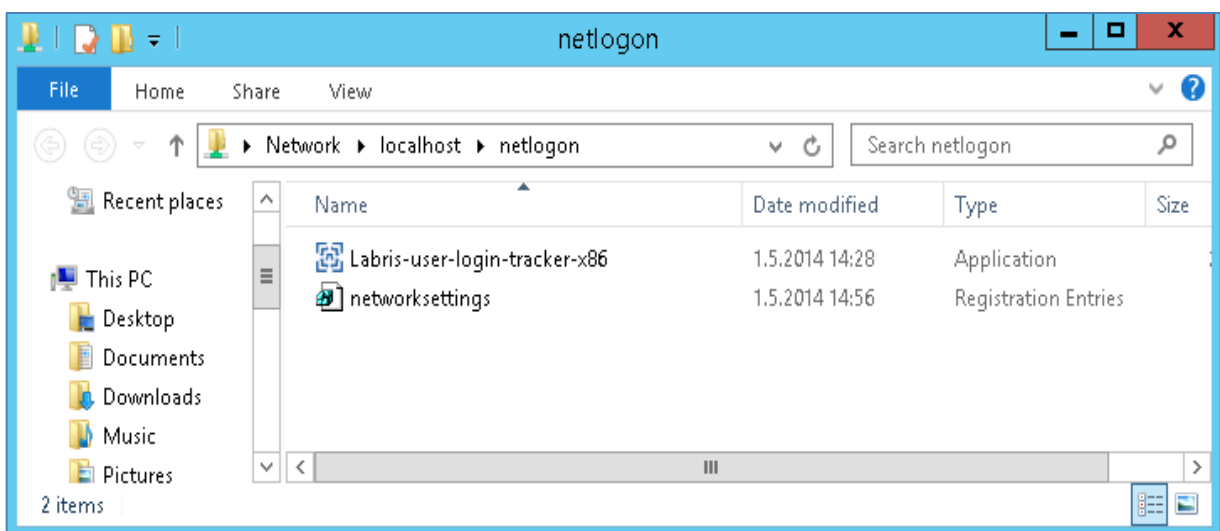
Logon Script Configuration

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.

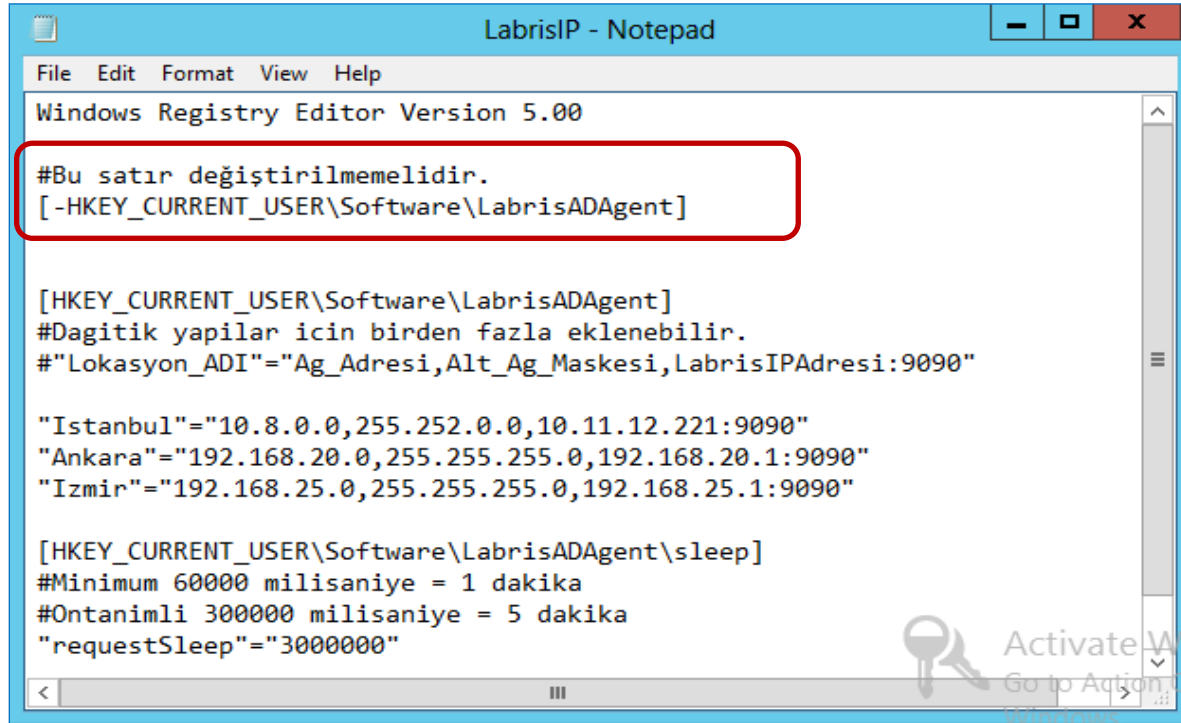


b. Network settings registry file is edited for the network settings.

Right button + edit are clicked on **network settings** 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.

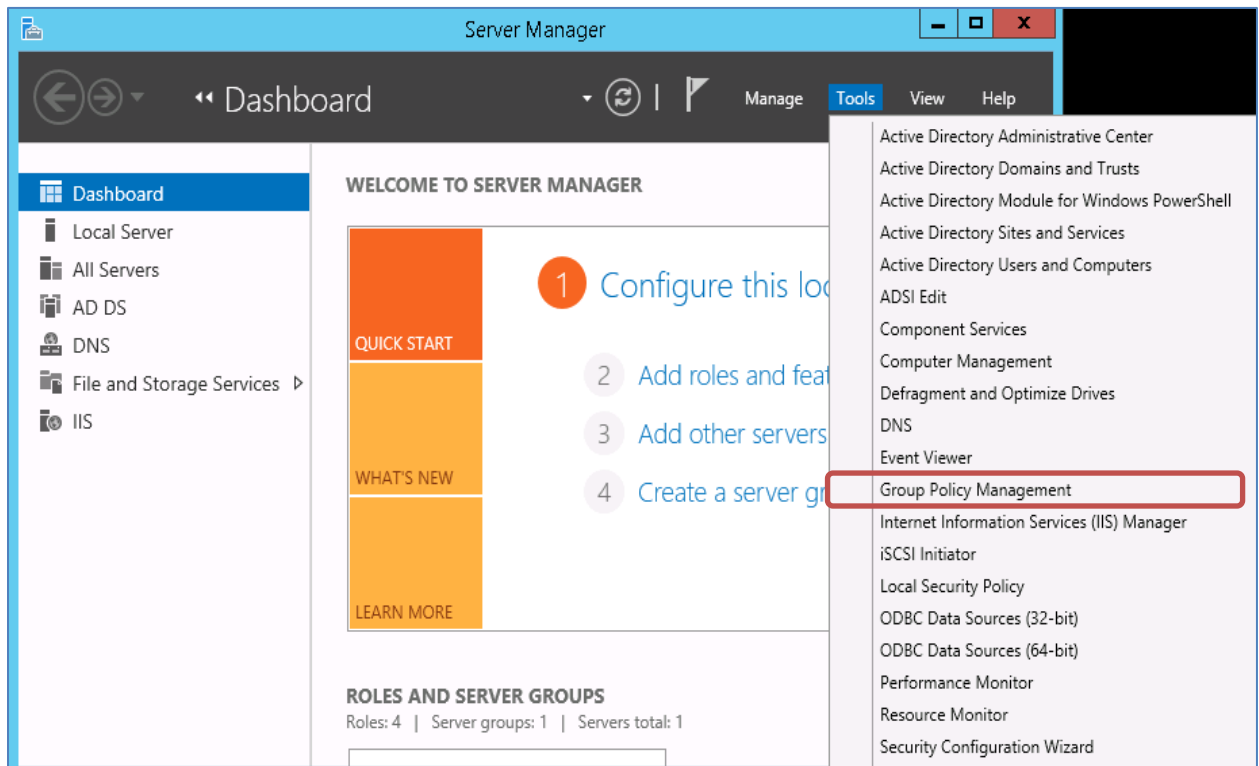


Parameter Description

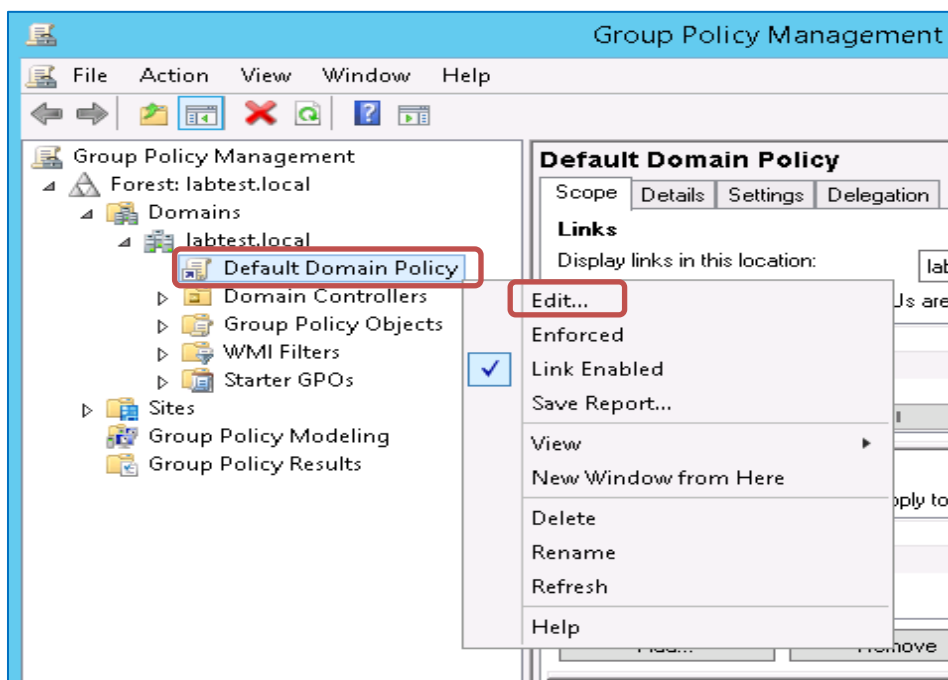
No	Parameter	Value	Description
1	Location Name	Istanbul	The location name to be made network identification.
2	Network Address	192.168.20.0	Network address of the Labris device location is written.
3	Subnet Mask	255.255.255.0	The subnet mask belongs to network address specified is defined.
4	Labris IP 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.

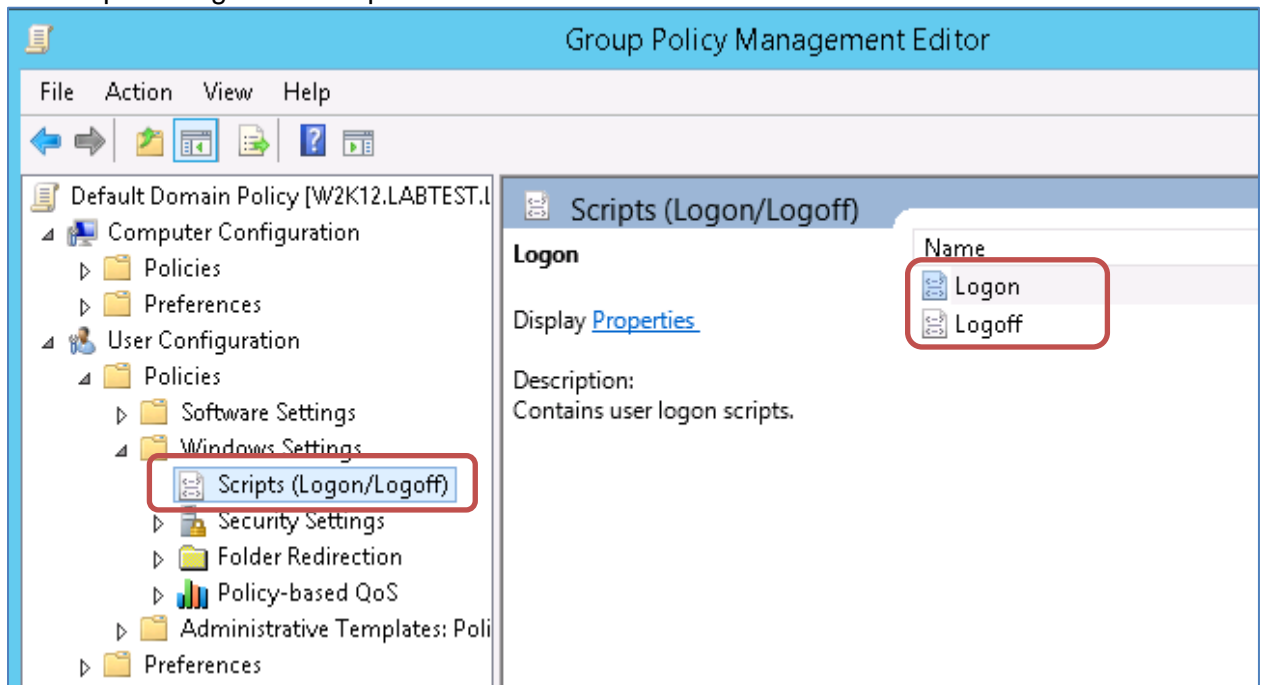
It is entered in the **Group Policy Management** window.



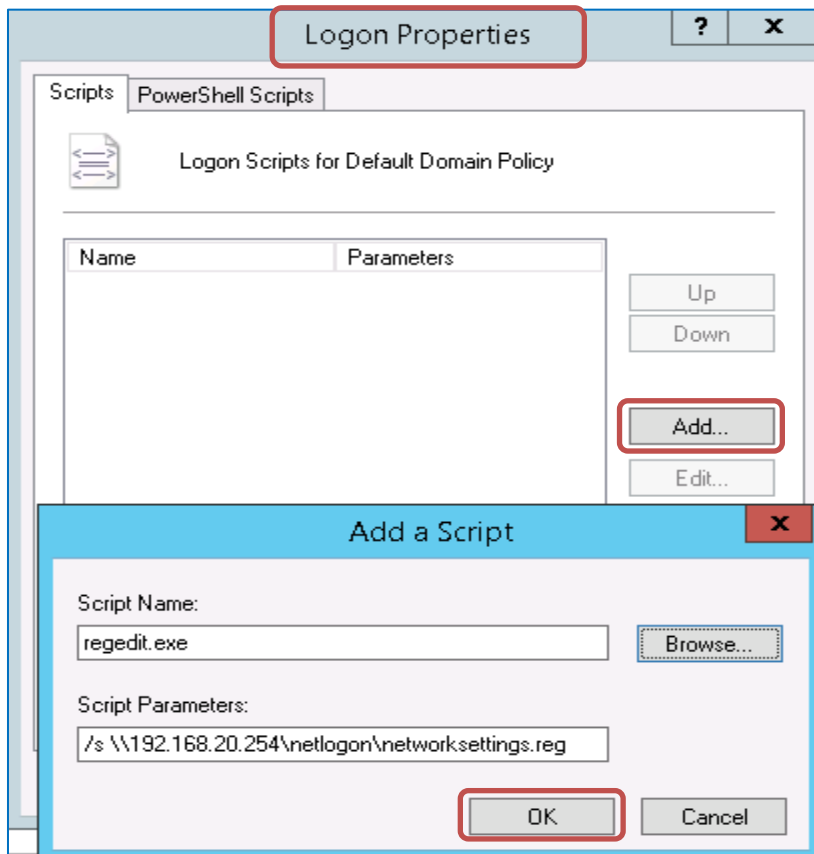
Default Domain Policy is set. If desired, settings can also be made here by creating a different group policy.



Script Settings section opens.



- e. **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

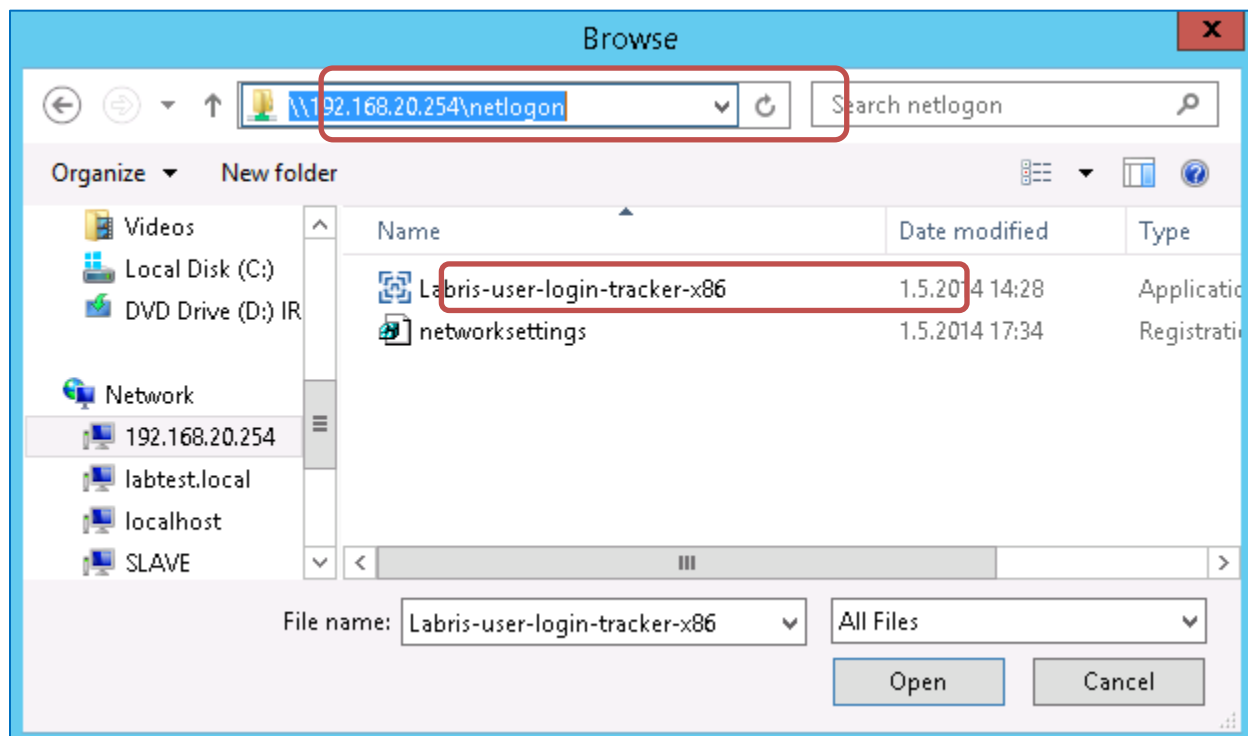
No	Parameter	Value	Description
1	Script name	regedit.exe	Registry editing tool in which will run registry file that we set.
2	Script Parameters 1	/s	It will not be displayed while applying registry record in user computers.
3	Script Parameters 2	\\192.168.20.254\netlogon\networksettings.reg	The path of networksettings.reg file is displayed, which we copied to netlogon directory of active directory server.

Labris User login 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.

Add a Script

Script Name:

\\192.168.20.254\netlogon\Labris-user-login-tracker-x86.exe

Browse...

Script Parameters:

logon \\192.168.20.254\netlogon\networksettings.reg

OK

Cancel

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.

Logon Properties

Scripts

PowerShell Scripts

Logon Scripts for Default Domain Policy

Name

Parameters

regedit.exe

/s \\192.168.20.254\n...

\\192.168.20.254\netlo...

logon \\192.168.20.25...

Up

Down

Add...

Edit...

Remove

To view the script files stored in this Group Policy Object, press the button below.

Show Files...

OK

Cancel

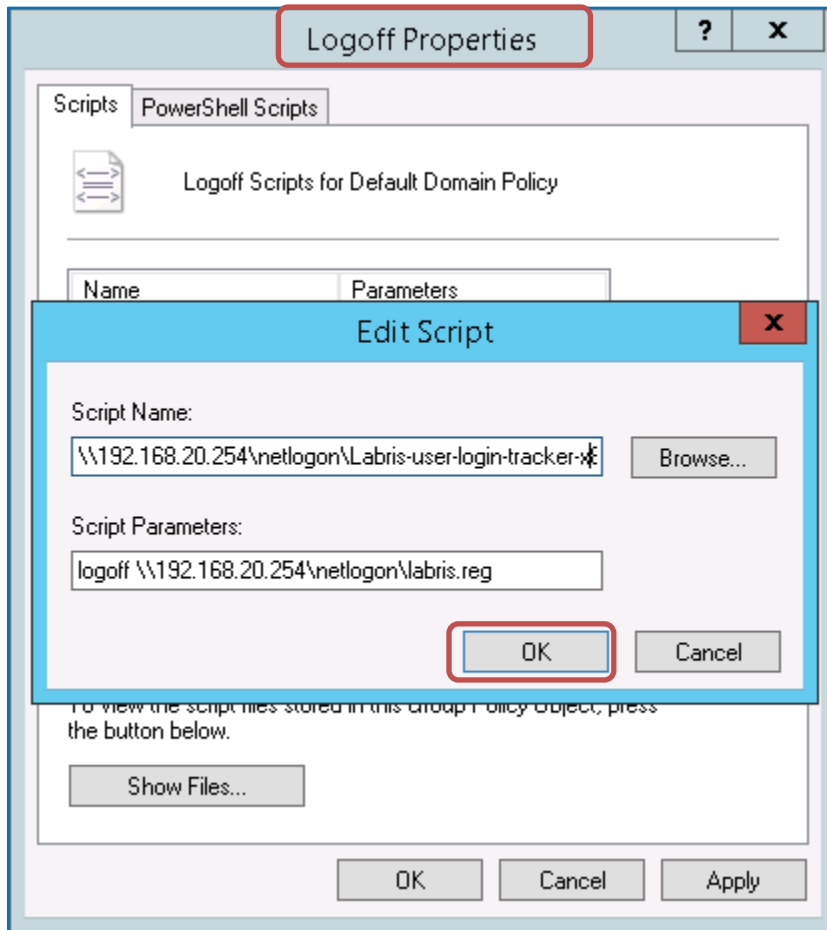
Apply

342

Labris Networks

Logoff settings are clicked and then Add is clicked.

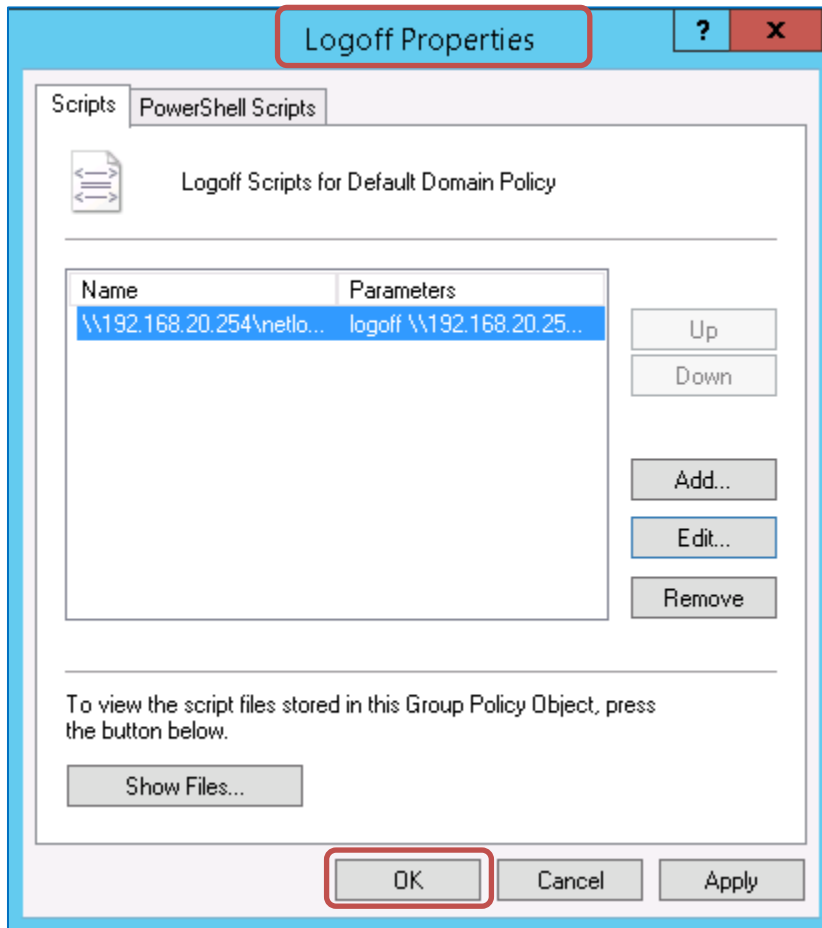
As in the setting of logon, **Labris-user-login-tracker-x86.exe** is selected and script parameters are written.



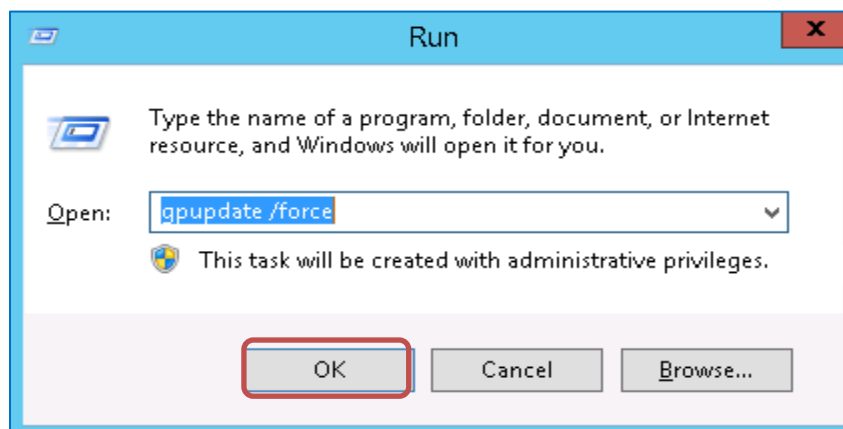
Parameter Description

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.

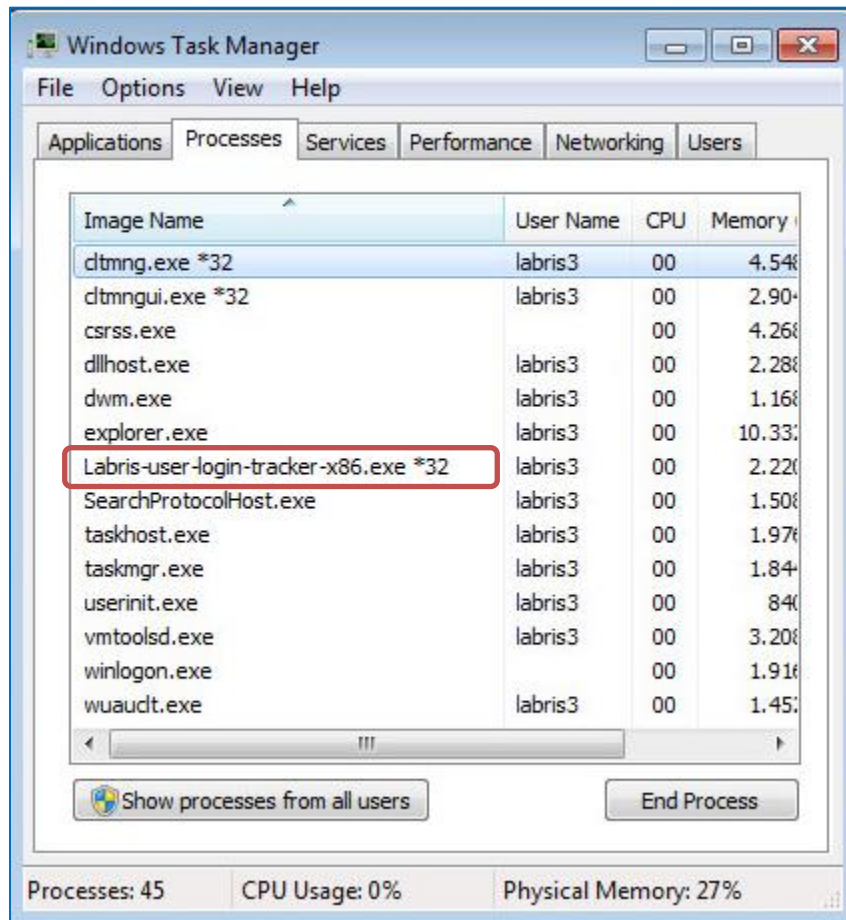


- f. Group Policy settings are applied.
For the changes to be valid, Group Policy settings will be updated for all users.
Run opens by using "**Windows + R**" keys.
The settings are applied by giving **gpupdate / force** command to this area.



- g. 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.



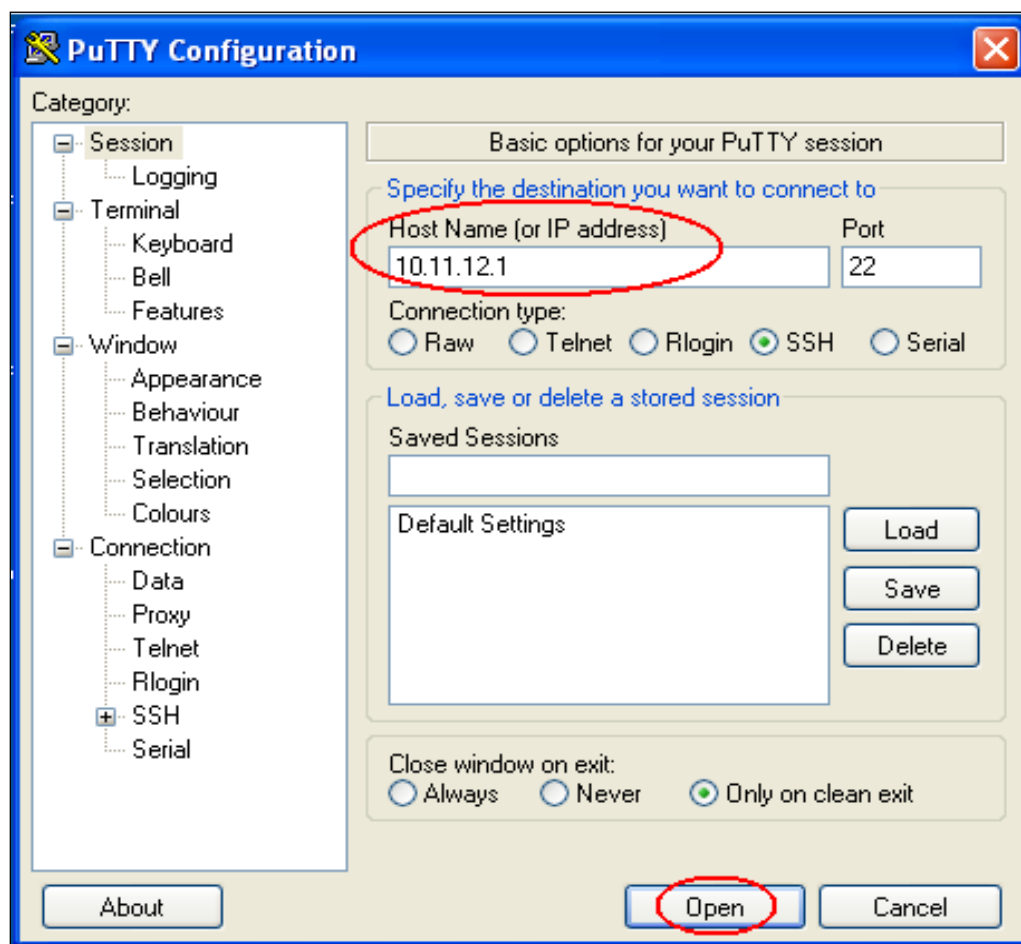
To provide control over Labris;

"**labrisdb_user_manager.py -getall-ip**" command is written on the command line and it is seen that the IP addresses of users came.

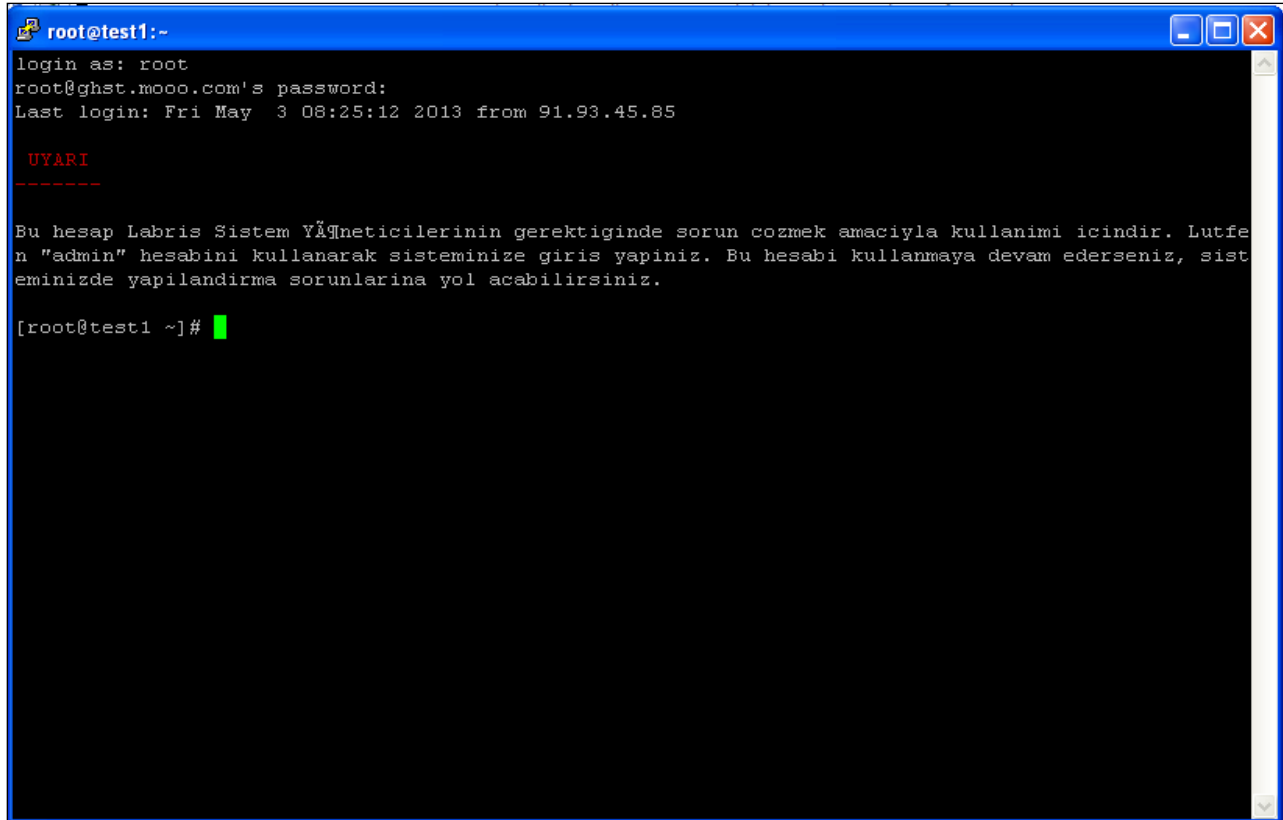
CLI Access

You can download the console access software (Putty) from [here](#).

Type your Labris IP address in the 'Hostname' field and click 'Open'.



If you are connecting for the first time, you'll see a certificate error. You may safely accept the certificate in this case. Type in your username (root) and password to connect.



```
root@test1:~  
login as: root  
root@ghst.mooo.com's password:  
Last login: Fri May 3 08:25:12 2013 from 91.93.45.85  
  
UYARI  
-----  
  
Bu hesap Labris Sistem Yöneticilerinin gerektiğinde sorun cozmek amacıyla kullanımı içindir. Lütfen "admin" hesabını kullanarak sisteminize giriş yapınız. Bu hesabı kullanmaya devam ederseniz, sisteminizde yapılandırma sorunlarına yol açabilirsiniz.  
  
[root@test1 ~]#
```



Nothing will be shown in the screen while you're typing.
Please go on and press <enter>.

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
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTM	Unified Threat Management
WAN	Wide Area Network
WAUTH	Wireless Authentication



Labris
NETWORKS