# **BLOX ESBC** User Manual

#### Copyright

Copyright © 2016 blox.org All rights reserved.

No part of this publication may be copied, distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language without the prior written permission of blox.org. This document has been prepared for professionals and properly trained personnel, and the customer assumes full responsibility when using it.

#### **Proprietary Rights**

The information in this document is Confidential to blox.org and is legally privileged. The information and this document are intended solely for the addressee. Use of this document by anyone else for any other purpose is unauthorized. If you are not the intended recipient, any disclosure, copying, or distribution of this information is prohibited and unlawful.

#### Disclaimer

Information in this document is subject to change without notice and should not be construed as a commitment on the part of **blox.org.** And does not assume any responsibility or make any warranty against errors. It may appear in this document and disclaims any implied warranty of merchantability or fitness for a particular purpose.

#### About this manual

This manual describes the Blox Esbc product application and explains how to work and use it major features. It serves as a means to describe the user interface and how to use it to accomplish common tasks.

#### **Document Conventions**

In this manual, certain words are represented in different fonts, typefaces, sizes, and weights. This highlighting is systematic; different words are represented in the same style to indicate their inclusion in a specific category. Additionally, this document has different strategies to draw User attention to certain pieces of information. In order of how critical the information is to your system, these items are marked as a note, tip, important, caution, or warning.



- **Bold** indicates the name of the menu items, options, dialog boxes, windows and functions.
- The color <u>blue</u> with underline is used to indicate cross-references and hyperlinks.
- Numbered Paragraphs Numbered paragraphs are used to indicate tasks that need to be carried out. Text in paragraphs without numbering represents ordinary information.
- The Courier font indicates a command sequence, file type, URL, Folder/File name e.g. <u>www.blox.org</u>

#### Support Information:

Every effort has been made to ensure the accuracy of the document. If you have comments, questions, or ideas regarding the document contact online support: <u>support@blox.org</u>

## **Table of Contents**

About this Manual	3
Document Conventions	3
1. Freeblox (User Interface)	7
1.1 Accessing the Web GUI	7
1.2 Dashboard	8
1.3 Network Status	9
2. Network	10
2.1 Interfaces	10
2.1.1 Settings	10
2.1.2 Virtual IP	11
2.1.3 VLAN	13
2.2 Routes	14
2.3 Device Access	16
3. System	17
3.1 Time Settings	17
3.2 Logging	
3.3 Package upgrade	
3.4 Email Server settings	19
4. Media	21
4.1 Media Profile	21
4.2 T38 FAX Profiles	23
5.Signalling	25
5.1 SIP Domain	25
5.2 SIP Profile	25
5.3 SIP Headers	29
5.4 Trunk Configuration	
5.5 Roaming Users	
5.6 Least Cost Routing	

5.7 TLS Settings	37
5.7.1 Device Root CA	
5.7.2 Server Certificates	38
5.7.3 Client Certificates	38
5.8 General Settings	39
6. Presence	40
6.1. Subscribers	40
6.2. Events	41
7. Security	42
7.1 SIP	42
7.1.1 Attacks Detection	42
7.1.2 Protocol Compliance	47
7.1.3 Signature Update	47
7.2 Firewall	50
7.2.1 Firewall Config	50
7.2.2 Firewall Rate Limiting	52
7.2.3 Port forwarding	53
7.2.4 White list IP Addresses	54
7.2.5 Blacklist IP Addresses	54
7.2.6 Dynamic Blacklist IP Addresses	57
7.2.7 Geo IP Filters	59
7.3 VPN	60
7.3.1 IPSec VPN	60
8. Status	66
8.1 Profile Status	66
8.2 Trunk Status	66
8.3 Roaming User Status	66
8.4 Active calls	67
8.5 Logs	67

8.5.1 Signaling Logs	57
8.5.2 Media Logs	58
8.5.3 LCR Logs	68
8.5.4 System Logs	69
8.5.5 Security Logs	59
9. Reports	70
9.1 CDR Reports	70
10. Tools	71
10.1 Administration	71
10.2 Diagnostics	71
10.2.1 Run Diagnostics	71
10.2.2 Ping	72
10.2.3 Trace route	72
10.3 Trouble shooting	73
10.4 Logs Archive	73

# 1. Freeblox (User Interface)

Freeblox is the GUI designed for Blox ESBC & user can configure the features and the SBC administration.

Accessing the Web GUI of Blox Esbc (follow instruction as per Quick Installation Guide)

## 1.1 Accessing the Web GUI

Blox Esbc Web GUI can be accessed via Management Port, Please follow the quick installation guide for details.

The message will prompted the connection is untrusted, Click on Add Exception to continue the process. Once get the certificate, to confirm security Exception and proceed to access the GUI Login page.

The WebUI has been made accessible only via HTTPS. The recommended browser for accessing Blox Esbc WebUI is Mozilla Firefox.

On launching the Blox Esbc WebUI, the web application will prompt to enter the administrator credentials to login.



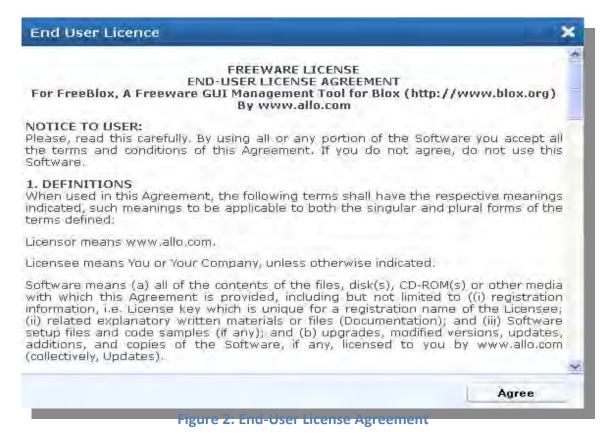
Figure 1: Login Page

#### **End User License**

In proprietary software, an end-user license or software license agreement is the contract between the licensor and purchaser, establishing the purchaser's right to use the software.

An End User License Agreement (EULA) is a legal contract between a software application author or publisher and the user of that application.

The user should be prompted to accept the Freeware license agreement and click "Agree button" to proceed further.



## 1.2 Dashboard

On the very first login, the WebGUI will provide you an overview of Blox Esbc configuration status.

BLOX					Welcom Firmiware vension : FreeB 06-October-16 1	
• Dashboard )	Dashboard 🥝					
Network	System Status	Sig Update Versio	0		Status	
<ul> <li>System</li> <li>Media</li> <li>Signalling</li> </ul>	Up-Time 1 day	FreeBlox Signature	es 1.0.00		<ul> <li>DPI Enabled</li> <li>Firewall Enabled</li> </ul>	bled
<ul> <li>Presence</li> <li>Security</li> </ul>	Memory Usage (Total Memory : 2005 MB) 17% Flash Usage (Flash Size : rootfs /dev/mmcblk0p2B)	Last 10 Alerts				-
I Status I Tools	116 116 CPU Usage	Time 10/06-10:47:20	27	Category 140	Message "(spp_sip) Maximum dialo "(spp_sip)	Src IP 192.168.0.183
	0%	10/06-10:47:44 10/06-10:48:08	27 27	140 140	(spp_sip) Maximum dialo "(spp_sip) Maximum dialo	192.168.0.18 192.168.0.18
	[Version encode]	10/06-10:48:32	27	140	"(spp_sip) Maximum dialo	192,168.0.18
	Network Info Refresh	10/06-10:48:56	27	140	"(spp_sip) Maximum dialo "(see sig)	192.168.0.18
	DEV MAC ADDR IP GATEWAY TYPE	10/06-10:49:20	27	140	"(spp_sip) Maximum dialo	192.168.0.18
	eth1 00:17:F7:00:43:02 10:10:10.1 Interface eth2 00:17:F7:00:43:03 192:168:10:148192:168:10:254Interface	10/06-10:49:44	27	140	"(spp_sip) Maximum dialo "(spp_sip)	192,168.0.18
	eth0 F4:4E:FD:38:7A:1110.1.1.1 Transcoding	10/06-10:50:08	27 27	140 140	Maximum dialo "(spp_sip) Maximum dialo	192.168.0.18
			12.2		"(son sin)	

#### Figure 3: Dashboard

The Right of the top panel shows the current time of device. Top panel also shows the firmware release version and has an icon which will refresh the page.

On the right side of the top panel, clicking on settings icon shows the menu which has Web Settings and Logout options.

Web Settings allows user to change the Old Password & Session Timeout values where as user name is Read-Only.

Clicking Logout will kill the session and redirects to the Login page.

System Status Panel shows Device up time, Memory Usage, Flash Usage & CPU Usage.

Sig Update Version Panel shows Blox Esbc Signature version and Release State.

Network Status Panel shows IP, LAN MAC, WAN MAC and Gateway of the device.

#### **1.3 Network Status**

Once the GUI is accessed user can configure the network configuration by following the below steps

1. After login user has to click on the refresh button in the network status in the Dashboard

2. Once the network status is refreshed it will display all the available interfaces in the board

3. Once the interfaces are displayed in the dashboard user can configure the WAN and LAN ip address of the Blox Esbc through Network--> Settings page

Dashboard	> Dashboard 🖉				
Network	System Status	Sig Update Versio	n	Status	
System Media Signalling	Up-Time 1 day Memory Usage (Total Memory : 2005 MB)	FreeBlox Signature	es 1.0.00	😑 DPI Enabled	
Presence		Last 10 Werts			
Status	Flash Usage (Flash Size ; rootfs /dev/mmcblk0p2B)	Time	ID Cate	ory Message	Src IP
Tools	CPU Usage	10/06-10:47:20	27 14	"(spp_sip) Maximum dialo	192.168.0.1
	0%	10/06-10:47:44	27 14	"Come sim)	400 400 0 4
	Network Status	10/06-10:48:08	27 144	Manage also 3	402 400 0 4
	Network status	10/06-10:48:32	27 14	Wana ata Y	192 169 0 1
	Network Info	10/06-10:48:56	27 144	Warner of a St	102 100 0 1
	DEV MAC ADDR IP GATEWAY TYPE	10/06-10:49:20	27 140	Plana da Y	192 169 0 4
	eth1 00:17:F7:00:83:02 10.10.10.1	10/06-10:49:44	27 140	Warner stars	102 100 0
	eth2 00:17:F7:00:A3:03 192:168:10.148192:168:10.254Interface eth0 F4:4E:FD:38:7A:1110.1.1.1 Transcoding	10/06-10:50:08	27 14	Warnen alle V	402 460 0 4
		10/06-10:50:32	27 144	Wanna ala b	192 169 0
		×+ ×		112 7 5	*** *** * *

**Figure 4: Network Status** 

Security Alert Summary Panel shows four links and on mouse over shows the details of Top 10 Signatures, Top 10 Categories, and Top Source & Top Destinations.

## 2. Network

This Network tab provides detailed information about Interfaces, settings, Routes and Device Access of the Blox Esbc.

In Blox Esbc mainly consists of 3 Ethernet interfaces such as internal, external and Transcoding interface.

User can configure the Virtual IP and VLAN for Blox Esbc.

## 2.1 Interfaces

An interface is a shared boundary across which two separate components of computer system exchange information. User can configure IP addresses for the networks.

## 2.1.1 Settings

Navigate through Network > Settings

A LAN interface deals with any type of SIP signaling which goes in and out of the Blox Esbc.

The signaling interfaces on the Blox Esbc are the physical Ethernet adapters.

It allows user to configure Host Name, IP Configuration in Static mode. IP Address/Mask, Gateway & DNS fields are editable only in Static IP mode. It also allows user to enable or disable SSH access to device.

User can save configurations by clicking on Save and can ignore saving the configurations by clicking on Cancel.

Edit Network	Interface Prof	file	×
Interface name Interface type	WANIFACE External Interface	1) + 11	
Device Id IP type	eth1 (00:17:F7:00:A	A2:81) •	
Ip address Netmask	61.X.X.X 255.255.255.0	<ul> <li>(i).</li> </ul>	
Gateway DNS Server	61.X.X.X 8.8.8.8	<ul> <li>(i)</li> <li>(ii)</li> </ul>	
NAT Settings	NO NAT T	IP Address	
		CAN	CEL

#### **Figure 5: Settings**

#### **Transcoding Settings**

If the Transcoding card is detected, user can configure the Transcoding Interface. It shows the interface type as Transcoding Interface. And also user can specify the IP address and Netmask.

Transcoding card is mandatory for SRTP and T38.

#### IP Troubleshooting:

In most installs, the network cards and IP settings will work straight out of the box. However, getting the network up the first time can be an exercise in frustration in some circumstances. Issues include;

- Network card compatibility
- Invalid networks settings (username, password, default gateway)
- Cable/DSL modems that cache network card hardware information

#### 2.1.2 Virtual IP

Navigate through Network > Interfaces> Virtual IP

A Virtual IP address (VIP or VIPA) is an IP address assigned to multiple applications residing on a single server, multiple domain names, or multiple servers, rather than being assigned to a specific single server or network interface card (NIC).

Dashboard	Virtual IP 🔮				
🗕 Network 💦 💊	Name -	Interface +	Address +	Netmask +	D
Interfaces		Consideration of the second			
<ul> <li>Settings</li> </ul>			No c	lata available.	
🗧 General					
<ul> <li>Virtual IP</li> </ul>					
VLAN					
Routes					
Device Access					
👂 System					
🔋 Media					
Signalling	0				
Presence	· · · · · · · · · · · · · · · · · · ·				
Security	Add New	Delete Selected			
Status		A THE OCCUPATION OF T			
🔰 Tools					

**Figure 6: Virtual IP** 

Click Add new, to create a Virtual IP.

Name	Internal VIP	. @	
Interfaces	LANIFACE T LA	N/10.10.10.1	
IP Address	10.2.2.1	19	
Netmask Description	255.255.255.0	10	
	interface		
	Interfaces IP Address Netmask	Interfaces LANFACE • ① LA IP Address 10.2.2.1 Netmask 255.255.2 Description Virtual ip addr	InterfacesLANIFACE • ILAN / 10.10.10.1IP Address10.2.2.1Netmask255.255.255.0DescriptionVirtual ip address with internal

**Figure 7: Create Virtual IP** 

#### **Create Virtual IP**

Name	Specify the name for the IP address for user's reference. The user can choose any name to recognize the Virtual IP.
Interfaces	Select the appropriate interfaces from the drop down list where the user desires to create a Virtual IP. Ex: For both External/Internal can be any interface which will be configured by the user (manually).This applies to VLAN as well.
IP Address	Enter the IP address for Virtual IP settings. E.g.: 10.2.2.1
Netmask	Enter the subnet mask address for Virtual IP settings. The default setting is 255.255.255.0
Description	Provide the description for the Virtual IP. (Optional)

## 2.1.3 VLAN

#### Navigate through Network > Interfaces> VLAN

A VLAN is a logically separate IP sub network. It allows multiple IP networks and subnets to exist on the same-switched network. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to change in network requirements and relocation of workstations and server nodes.

Network >	Tag ID 🔻	Interface 🗢	Description +	Options
nterfaces Settings Virtual IP	2	ethD		ZX
VLAN outes evice Access				
System				
Media Signalling				
Security				

Figure 8: VLAN

Click Add New, to create VLAN.

reate VLAN			X
Tag ID Interfaces		erface / 192.168.10.23:	L
IP Address	192.168.10.200	05	
Netmask Description	255.255.255.0	0	
		SAVE	NCEL

#### Figure 9: Create VLAN

Tag ID	User can specify unique Tag ID in the range of 1-4092. So that they can easily identified the multiple no of VLANs with Tag ID.
Interfaces	Select the appropriate interfaces from the drop down list where the user desires to create a VLAN. Vlan can be created for internal and external interfaces. Ex: if user wants to create the virtual IP in wan side select Eth0, WAN Interface-192.168.10.231 If the user wants to create the virtual IP in LAN side select Eth2,LAN Interface-10.0.0.1
IP Address	Enter the appropriate IP address for creating VLAN.
Netmask	Enter the subnet mask address for VLAN. The default setting is 255.255.255.0
Description	Provide the description for the VLAN. (Optional)

After clicking on 'save' button, followed by apply changes button in the top right corner of the panel.

#### 2.2 Routes

Navigate through **Network > Interfaces> Routes** 

Blox Esbc can also be used in conjunction with SIP trunks to provide call control and make routing/policy decisions on how calls are routed through the LAN/WAN.



**Figure 10: Routes** 

#### Click Add New, to create a route

Name	Route1	(Ø)
Destination	192.168.0.85	(0)
Netmask	255.255.255.0	(B).
Gateway	192.168.0.254	m.
Metric	10 00	
Interfaces	eth0 💌 🕑 Wan /	192.168.10.231
Description	Route outside	V

Figure 11: Create Route

Name	Specify the name for the Routes for user's reference. The user can choose any name to recognize the Routes.
Destination	User can specify the destination Address, to where it should be routed.
Netmask	Enter the subnet mask address for Routes. The default setting is 255.255.255.0
Gateway	User can specify the gateway IP address for particular network. E.g: 192.168.0.100- IP address, the gateway will be 192.168.0.254.
Metric	User can specify Metric value in the range of 0-31

Interfaces	Select the appropriate interfaces from the drop down list where the
	user desires to create a Route.
	Ex: if user wants to create the virtual IP in wan side select Eth0, WAN
	Interface-192.168.10.231
	If the user wants to create the virtual IP in LAN side select Eth2,LAN
	Interface-10.0.0.1
Description	Provide the description for the Routes. (Optional)

## **2.3 Device Access**

## Navigate through Network > Device Access

It allows user to create a rule for device access that allows access to the device anywhere.

Network )	Name -	IP Type 🕈	Address +	Comments +	Enabled	Options
iterfaces outes	DefaultAllAccess	ANY		Default rule that al		XX
vice Access						
System Media						
Signalling	-					
Security						
Status						
atatus						

Figure 12: Device Access

Click Add New, to create Device Access Rule.

Name	Default access
IP Туре	IP_BANGE
Address	Ū
Enable	☑ @.
Comments	Default rule that allows access to the device from anywhere
	Q.

Figure 13: Create Device Access Rule

Name	Specify the name for the Device Access for user's reference.
	The user can choose any name to recognize the Device
	Access.
ІР Туре	User can select the appropriate IP type from the drop down
	list. IP types are IP_Host, IP_Network, IP_Range, and
	MAC_ADDR.
Address	Specify IP Address/Netmask or IP range or MAC address.
Enable	It allows the user to either enable or disable Device access
	rule.
Comments	User can specify the comments in the length of 64 char's.

# 3. System

This System tab provides detailed information about Time Settings, Logging, Package Upgrade and Email Server Settings.

## 3.1 Time Settings

## Navigate through System > Time Settings

It allows user to configure Date / Time. It allows user to configure Date / Time. They can be either set manually (uses RTC) or automatically (through NTP). Default: NTP.

User can select the configuration type from the configuration type menu that allows selecting the time zones from the drop down menu.

For NTP configuration mode, add the NTP Server to the NTP list by clicking on Add button and can also delete the NTP Servers from the list by selecting and clicking on Delete button.

Clicking on Apply will apply the configurations and Cancel will ignore the configurations made.

Network	The second second second		
- System	Date / Time Settings	1	
Time Settings	Configuration Type	NTP 💌 🛈	
Logging	Date/Time	22 : 48 - 24	1 02 1 2015
Package Upgrade	Daternine	22 : 48 - 24	
E-mail Server Settings	Time Zone	Africa/Abidjan	V O
Media	NTP Server		Add
Signalling		3.in.pool.ntp.org	Delete
Security		4.in.pool.ntp.org	
Status			-
Tools			

Figure 14: Date/Time Settings

## 3.2 Logging

Navigate through System > Logging

It allows user to configure Remote Log Server settings.

The administrator can configure the Blox Esbc to send the security alerts generated on detecting the SIP based attacks, to the remote Syslog server.

The logging page will allow enable/disable the remote logging of security alerts and to which Syslog server the security alerts are to be forwarded.

Network	a second		10
= System 💦 🔉	Logging		10
Time Settings		Remote Logging:	
Logging		Syslog server	1
Package Upgrade		5) 510g 551 751	
E-mail Server Settings			
🕨 Media	Save	Cancel	
Signalling			
Security			
<ul> <li>Status</li> </ul>			
Tools			



## 3.3 Package upgrade

Navigate through System > Package Upgrade

It can upgrade by selecting a .tgz and .iso file from the system and clicking on Upgrade button which reboots the device on success.

Click upgrade, It displays the package name, which version of upgrade is installed in the package upgrade.

Dashboard	Package Upgrade 🕝			
Network				
System	Current Firmware Versio	on: SBC 0.9.0.00 beta	0	
ime Settings ogging	(Choose the filepath of the	new firmware)		
ackage Upgrade	Filename: Browse Not	file selected. (Need Reboot)		
-mail Server ettings				
Media	Upgrade			
Signalling	opgrade			
Security	Package Name =	Version Installed +	Platform 🗢	
Status	allo ministun client	0.9	x86 64	
Status				
	allo_mtslib	0.9	x86_64	
		0.9 0.9	x86_64 x86_64	
	allo_mtslib			
	allo_mtslib allo_mtsserver	0.9	x86_64	
	allo_mtslib allo_mtsserver allo_sbc_config	0.9 0.9	x86_64 x86_64	
Tools	allo_mtslib allo_mtsserver allo_sbc_config allo_sbc_miniupnpd	0.9 0.9	x86_64 x86_64 x86_64	

Figure 16: Package Upgrade

## **3.4 Email Server settings**

Navigate through System > Email Server Settings

All email accounts we host, regardless of the domain name, will use the following server settings.

Dashboard	E-mail Server 🔞			
Network	E-mail Notification Settin	ine in		
• System 🔉	Leman Rouncation Settin	na.		
Time Settings	Server IP / Port	192.168.0.200	C 65535	00
Logging				
Package Upgrade	Sender E-mail ID	admin@allo.com	1	57
E-mail Server Settings	Receiver E-mail ID	roger@allo.com		Œ
• Media	Authentication	Auth_login 🔽 💷		
<ul> <li>Signalling</li> </ul>	Username	admin	0	
Security	Password		0	
Status		N	-4	
Tools				

## Figure 17: Email Server Settings

Server IP /Port	User can specify the Email server IP address and Server port.
Sender Email ID	The user can extends the verification process to include
	professed responsible addresses. Eg: <u>admin@gmail.com</u>
Receiver Email ID	The user can specify the Receiver email id Eg:
	<u>roger@gmail.com</u>
Authentication	User can select authentication from the drop down list. If
	authentication is required by the End point.
Username	Username of endpoint (e.g.: Testing) will use to authenticate
	with the Email server settings.
Password	Enter the valid password and its authenticating Email server
	settings.

## 4. Media

This section will provide detailed information about Media profile.

## 4.1 Media Profile

#### Navigate through Media > Media Profile

A media profile deals with all forms of media which goes in and out of the Blox Esbc. Media Profile takes care of channeling of respective media.

Through media profile, user can configure the media port range as well as type of the media like Transcoding or general media.

The media profile deal with all Transcoding functions. Example: conversion from G.729 to G.722. Also it deals with all other functions related to media (RTP/SRTP). Media profiles are the actual DSPs that perform RTP streaming, trans-coding etc.

Network		Name -	External Interface 🕈	Internal Interface 🛎	Media Interface +	Description +	Opti	ions
System Media		genmed	ethO	eth2	eth2:1	profile for general	1	×
edia Profile		transmedia	ethO	eth2	eth1	profile for transcod		×
8 Fax Profiles	_							-
Signalling								
orgnaming								
Security								
Security								
and a starter								
Security Status								
Security Status								
Security Status		Add liew	Delete Selected					

Click Add New, to create Media Profile.

Media Settings	Franscoding Sett	ings		_
Jame	TRansmedia	( <u>D</u> )		
Description	Media profile with	transcoding1	(i)	
External Interface	WANIFACE		NAT	
Internal Interface	LANIFACE	¥ 🗇 ;10.10.10.1		
transcoding Interface	TRANSIFACE	+ 0 10.1.1.1		
RTP Port Start	17000			
RTP Port End	18000			
Media TOS	11 0			
4edia TOS	11			

## Figure 19: Media Settings

Name	Enter the name for the Media Profile for user's reference. The user can
	choose any name to recognize the Media profile.
Description	Provide the brief description for the Media profile.(Optional)
External Interface	User can select the particular WAN IP address prompting in the drop list,
	which has to be sent outside of SBC.
Internal Interface	User can select the particular LAN IP address prompting in the drop list,
	which has to be received to internal side of SBC.
Media Interface	It specifies the Kind of media to be selected here.
	User can select the particular Media interface prompting in the drop list
	which can be either Virtual IP or a Transcoding IP.
RTP Port Start	User can be specified the starting port range which the particular media
	profile starts.
	If you want to set up the port range out of which the RTP ports will be
	dynamically taken, specify the End port respectively, in this field.
RTP Port End	User can be specified the ending port range which the particular media
	profile starts.
	If you want to set up the port range out of which the RTP ports will be

	dynamically taken, specify the End port respectively, in this field.
Media TOS	User can specify the Media ToS value.

Media S	ettings	Transcoding Settings	
Codec	g729 g711u g711a	G > >> < <	
Enable Silence Suppressi	on 🗌		

#### **Transcoding Settings**

Our Transcoding cards are designed to handle complex codec translation, using dedicated DSP resources, which would otherwise be processed by host CPU in software. This card greatly reduces the MIPS or CPU consumption, so that it can be used for handling other tasks.

**Codec** - Our Transcoding card supports all the codecs: G722.2, AMR, GSM-EFR, GSM-FR, G.711, G.722, G.722 1C/Siren 14, G.723.1, G.726, G.729AB, T.38 FAX, iLBC

Voice signals from the PSTN come in the form of the G.711 codec, but the VoIP terminal equipment and networks can support a variety of different voice codecs, such as G.729. The VoIP infrastructure needs the capability to mediate between endpoints supporting different codecs.

User can desire to select the Codecs for Transcoding.

## 4.2 T38 FAX Profiles

#### Navigate through Media > T38 FAX Profiles

T38 is a protocol that describes how to send a fax over a computer data network. It is needed because fax data can not be sent over a computer data network in the same way as voice communications. T38 fax is converted to an image, sent to the other T38 fax device and then converted back to an analog fax signal.

le profile2 0 9600 testing 2 X	profile1 0 9600 test profile e profile2 0 9600 testing	Name -	Fax Version +	Max Bit Rate 🕈	Description *	Option
iter profile2 0. 9600 testing 🖉 🕻	e profile2 0 9600 testing		a second s	and the second sec	o adden priori	
ofiles		> profile1	0	9600	test profile	1 >
ofiles		profile?	0	9600	testing	1 X
						4
						(a) (a)
						<u>1</u>

#### Figure 21: T38 FAX Profiles

Click Add New, to create T38 FAX Profile.

Media Profile	transmedia 🕕	
Name	profile2	
Description	testing	0
T38 Fax Version	0	
T38 Max Bit Rate	9600 🤒 🖉	
T38 Fax Rate Management	transferredTCF 🛛 😵 🗐	
T38 Fax ECM Enable		
T38 Fax Udp EC	t38UDPRedundancy 😽 💿	

Figure 22: Create T38 Fax Profile

Media Profile	Enter the media profile name for create T38 FAX Profile.
Name	Descriptive name for the T38 FAX Profile for user's reference.
Description	Provide the description for the T38 FAX Profile. (Optional)
T38 Fax Version	It is an ITU recommendation for allowing transmission of fax
	over IP networks in real time. User can select the FAX Version
	from the dropdown list.
T38 Max Bit Rate	It specifies the maximum bit rate from the drop down list.
	E.g.9600
T38 Fax Rate Management	User can select the Fax Rate Management like transferred TCP,
	local TCF from the drop down list.
T38 Fax ECM Enable	User can either enable or disable the FAX ECM.
T38 Fax Udp EC	User can select any types like t38UDPFEC, t38UDPRedundancy
	from the drop down list.

# 5. Signaling

Signaling section allows a user to create SIP Domain, SIP Profile, Trunk Configuration, Roaming Users, Least Cost Routing, and TLS Settings.

## 5.1 SIP Domain

Navigate through Signaling > SIP Domain

The Domain-based routing for roaming users provides support for matching an outbound dial peer based on the domain name or IP address provided in the sip domain field.

Create SI	P Domain P	Profile			×
SIP Domain	example.org	(j)			
				SAVE	CANCEL

#### Figure 24: Create Sip Domain Profile

User can create domain names for both internal and external side and assign the domain names to corresponding sip profiles

## 5.2 SIP Profile

#### Navigate through **Signaling** > **SIP Profile**

A SIP Profile is an account built on the Blox Esbc which contains a set of SIP attributes that are associated to the Blox Esbc itself. The SIP profile is used as a configuration for how the external endpoints may connect to the Blox Esbc. You bind an IP address, port, and other SIP related parameters to a SIP profile.

It contains SIP UA configuration. Blox Esbc can be configured to behave as multiple UA each with a different configuration (and therefore a different set of IP: port pair each).

Name 🔻	Interface \$	SIP Port ÷	SIP Protocol +	Description +	Options
External profile	wan	8061	udp	External sip profile	/ ×
internal profile	lan	6060	udp	Internal sip profile	/ ×
lanprofile	lan	5060	udp	lan profile	× 🕺
wanprofile	wan	8060	udp	wan profile test	XX

Add New

Delete Selected

## **Figure 24: Sip Profile Results**

## Click Add New, to create SIP Profile.

Edit SIP Profile					×
Nan	ne	nternal profile	0		i.
Des	cription	nternal sip profile for	roaming user	(E)	
Inte	erfaces [	an 🔻 🛈 LAN / 10	0.10.10.1 NAT		
SIP	Protocol/Port	udp 🔻 💿 6060	0		
Rec	quired TLS	Verified	TLS		
Ser	ver Certs	None	* (1)		
SIP	TOS	( <u>3</u> )			
Sip	Domain	example.org	example.org	*	1
Allc	w (IP:PORT)		Add		*
		10.10.10.200.5060	Delete		
			-		
SIP	' Headers			1 1	
				SAVE	CANCEL
-					

Figure 25: Create Sip Profile

Name	Enter the name for the SIP Profile for user's reference. E.g.: Internal
	profile
Description	It provides the brief description for the profile name.(Optional)
Interfaces	User can select the respective network device name from the dropdown
	list for internal (LAN) and external (WAN) networks.
	Ex: if user wants to create the SIP profile in wan side select network
	device name WANIFACE in this case or the name specified while
	configuring the external interface
	If the user wants to create the SIP profile in LAN side select network
	device name LANIFACE in this case or the name specified while
	configuring the internal interface
SIP Protocol/Port	Blox Esbc SIP profile allows user to select multiple protocols (udp, tcp
	and tls) which can be available in dropdown protocol list. And Specify the
	SIP port in the range of 1-65535.
Required TLS	Turn on the strictest and strongest authentication possible. This
	parameter is used for incoming TLS connections where blox acts as a
	server. If disabled the verification process will succeed if the client does
	not provide a certificate, if enabled the verification process will only
	succeed if the client provides a certificate and this verifies correctly
	against the server's list of trusted CAs
Verified TLS	Turn on the strictest and strongest authentication possible. This
	parameter is used for incoming TLS connections where blox acts as a
	server. If disabled the blox will not request the client a client-certificate.
	This means that the client is not authenticated. If enabled blox sends a
	client-certificate request to the client.Verified TLS check box is enabled
	only if required TLS is checked
Server Certificates	If TLS SIP Protocol is enable, this server certificate is active. User can
	select the server certificates from the dropdown list.
SIP Domain	Select the appropriate domain name from the box, for the interface
	selected in the interfaces option
SIP TOS	The user can set the Type of Service (TOS) byte on outgoing IP packets
	for various protocols. The TOS byte is used by the network to provide

	some level of Quality of Service (QoS) even if the network is Congested
	with other traffic.
Allow (IP: PORT)	Creates a list of IP addresses along with port number to be allowed for a
	particular SIP profile.
	E.X.: 10.10.200:5060
	10.10.300:5060
	The above mentioned IP address is internal side of Blox Esbc. User can
	select the respective Internal (LAN)/ External (WAN) side IP: Port or user
	can mention 'any' if he wants to allow all the ip address and port
SIP Headers	Select the sip header manipulation rule required from the box

## 5.3 Sip Headers

#### Navigate through > Signaling > Sip Headers

Header manipulation is used when specific components within SIP messages need to be modified. SIP Header Manipulation provides the flexibility to add, remove, or modify any attribute in a SIP message on the Blox. The most common reason for doing this is to fix an incompatibility problem between two SIP endpoints. This could range from anything such as Softswitch/PSTN incompatibility or an issue between two different IP PBX platforms in a multi-site Enterprise where calls between them fail due to issues in the SIP messaging.

Name Description	Rule1 header fiel removal
List of Conditions	[]
Condition1 Action Pa	aram1 Param2 Options
Create/Edit Conditions	SAVE
Condition	None 🔹
Action	remove_hf
Param-1	User-Agent

Name	Enter the name for the Sip Header Manipulation for user's reference.	
Description	It provides the brief description for the sip header manipulation name.(Optional)	
Condition	Select the condition you wish to add in the SHM rule from the drop down list	
Action	User can assign the action to be performed for the condition selected from the drop down list	
Param	Header name to be removed	

## **5.4 Trunk Configuration**

#### Navigate through > Signaling > Trunk Configuration

SIP Trunks are used to connect Blox Esbc to a remote SIP Providers/User Agents. SIP Trunks can be used to communicate with SIP carriers or with IP-PBXs. It is the description of how the Blox Esbc will communicate with that endpoint. Example: IP address, port, etc.

SIP Trunks usually contains

- Remote Domain Information
- Remote authentication credentials
- Remote Registration information

SIP Trunks are bound to SIP Profiles. A single SIP Profile can be connected to multiple SIP Trunks

Babytel       198.38.7.11:5060       Trunk with       Image: Constraint of the second secon	Babytel       198.38.7.11:5060       Trunk with       Image: Constraint of the second secon	Name -	Server IP Port +	Description +	Option
Nano1         192.168.10.132:5060         Trunk with         Image: Constraint of the second	Nano1         192.168.10.132:5060         Trunk with         Image: Constraint of the state of the			a protection of a party of	
Image: Nano2         192.168.0.42:5060         Trunk with         Image: Nano2           Image: Trunk1         192.168.10.100:5060         First trun         Image: Nano2         Image: Nano2 <td>□         Nano2         192.168.0.42:5060         Trunk with         ∠         ×           ation         □         Trunk1         192.168.10.100:5060         First trun         ∠         ×</td> <td>🔲 Babytel</td> <td>198.38.7.11:5060</td> <td>Trunk with</td> <td>× ×</td>	□         Nano2         192.168.0.42:5060         Trunk with         ∠         ×           ation         □         Trunk1         192.168.10.100:5060         First trun         ∠         ×	🔲 Babytel	198.38.7.11:5060	Trunk with	× ×
tion 🗌 Trunk1 192.168.10.100:5060 First trun 🧭 🗶	ution 🗌 Trunk1 192.168.10.100:5060 <u>First trun</u> 🖉 🗶	> 🗋 Nano1	192.168.10.132:5060	Trunk with	🖉 🗙
ITUNKI 192.166-10.100:5060 <u>First trun</u>	ITUNKI 192.166-10.100:5060 <u>First trun</u>		192.168.0.42:5060	Trunk with	/ ×
ng 🗌 Trunk2 192.168.10.100:5060 Second tru 🖉 🔀	ng 🗌 Trunk2 192.168.10.100:5060 <u>Second tru</u> 🔏 🔀	on 🔲 Trunk1	192.168.10.100:5060	First trun	1 ×
		Trunk2	192.168.10.100:5060	Second tru	/ ×
		Add llow	Dolara Selected		
Add lleve Digitize Selected	Add llaw Deleta selected		TOTE S'OLORION		

## Figure 27: Trunk Configuration

Click Add New, to create Trunk Configuration.

Trunk Name	Babytel	8		
Description	trunk with babaytel		(1)	
Server	198.38.7.11:5060	(11)		
SIP Domain	sip.babytel.ca	(E)		
User	16046285242	0		
Password	*******	0		
SIP Registrar	198.38.7.11:5060	0		
Registrar Expire	360 ①			
Outbound Caller ID	16046285242	100		-

Figure 28: Create Trunk Configuration

Trunk Name	Trunk name of the user's choice to identify for particular
	PBX.
Description	Provide the description for the Trunk name. (Optional)
Server, SIP (Domain/ IP: PORT)	It expects an IP address along with port number to which the
	particular trunk needs to be registered.
	E.g.: 192.168.0.200: 5060
	Above example shows the IP address of provider/User agent
	with SIP port number.
User	The name of the user either provided by SIP provider or any
	extension of the PBX. E.g.: 99999
	Username of endpoint (E.g.: 99999) will use to authenticate

	with the Trunk Configuration.		
Password	Enter the Password and its authenticating Trunk		
	Configuration.		
SIP Registrar (IP: Port)	It expects an IP address along with port number where to g		
	registered. Eg. 192.168.0.200:5060		
	It specifies the SIP registrar in the format: IP Address and port		
	number of the PBX.		
Registrar Expire	SIP Trunk registration expiry timeout, Specify Registrar empire		
	in the range 360-3600.		
Outbound Caller ID	Configure the Caller ID Number that would be applied for		
	outbound calls over this trunk. E.g.:99999		
Outbound Proxy URI	IP address or hostname with port of the outbound proxy URI.		
	This ensures that all the SIP packets are sent via specified		
	proxy URI. Specify outbound proxy URI in the format IP		
	Address: Port		
User Agent	Specify the customized SIP User Agent used for SIP Method,		
	default Blox- <version>.</version>		
Internal SIP Profile	Internal (LAN) SIP Profile interfaces to the local PBX or IP end points.		
	User can select Internal SIP profile from the dropdown list.		
External SIP Profile	<b>External</b> SIP Profile interfaces to the ITSP or SIP trunk provider.		
	User can select External SIP profile from the dropdown list.		
Media Profile	In this filed, user can select the type of media like Transcoding		
	or general.		
	E.g.: general media- <b>10.2.2.1</b>		
	Transcoding media- 10.1.1.1		
Media Encryption (LAN)	The media encryption feature using secure RTP (SRTP) delivers		
	the ability to encrypt LAN Side media packets. SRTP is a		
	security profile for RTP that adds confidentiality, message		
	authentication, and replay protection to that protocol.		
Media Encryption (WAN)	The media encryption feature using secure RTP (SRTP) delivers		
	the ability to encrypt WAN Side media packets. SRTP is a		
	security profile for RTP that adds confidentiality, message		

	authentication, and replay protection to that protocol.
T38 Profile	Provide a T38 Profile which is already configured. The drop
136 FIOILIE	
	down menu will show the available T38 profiles.
Add Prefix	It's an optional field, in which user can add a number as a
	prefix for the particular trunk. Specify add prefix before the
	dialed number.
Strip Digits	It allows user to specify the number of digits that will be
	stripped from the dialed number.
	E.g.: 5- It will get stripped from the caller no.
Allow Inbound	It provides a checkbox that user can enable/disable the option
	allow inbound for trunk configuration.
Inbound URI	Provide an IP address with port number of respective internal
	(LAN) PBX.
	Ex. 10.10.10.200:5060
	Internal (LAN) PBX IP along with SIP port.
Max Inbound	The user can restrict the number of incoming calls, which can
	be coming through that particular trunk. Also user can select
	Max inbound to configure the trunks.
Allow Outbound	This field allows the user to either enable or disable outbound
	calls. User can make calls through that particular trunk.
Max Outbound	The user can restrict the number of outgoing calls, which can
	be making through that particular trunk.

## 5.5 Roaming Users

Navigate through > Signaling > Roaming Users

Roaming user is to create a profile for Internal (LAN) PBX such that user agents can register from the External network providing the details of roaming profiles.

Roaming user is a kind of user/extension which can register to the LAN side PBX by giving the Blox Esbc IP address and roaming port during registration

	Name 🔻	Force Expire +	Description +	Options
0	Roam2	3600	Roaming user with Na	/ X
C	Roamelastix	3600	Roaming user configu	🖉 🗙

Add New Delete Selected

## Figure28: Roaming Users Result

## Click Add New, to create Roaming user Profile.

Name	Roaming User
Description	Roaming user for PBX200
Internal SIP Profile	internal profile
External SIP Profile	External profile
	Sip Domains Destination URI example.org 10.10.200:5060
Media Profile	GeneralMedia 🔻
Media Encryption (LAN)	Nome (i)
Media Encryption (WAN)	None
T38 Profile	None (i)
IP Auth	
Force Expire	3600 (ē)
Max Inbound	100 (i)
Max Outbound	100 0
Presence	<b>I</b> 0
Presence Server	( <u>ī</u> )
Presence Domain	3
Enum	Ĩ.
Enum Type	ehum
Enum Suffix	e164.arpa
Enum Service	sip

Figure 29: Create Roaming User Profile

## Create Roaming User Profile

Name	Enter a name for the Roaming users for user's reference. The
	user can choose any name to recognize the Roaming User
	profile.
Description	Provide the description for Roaming profile.(Optional)
LAN SIP Profile	Expects internal (LAN) side IP which is placed behind the Blox
	Esbc. User can select the configured internal side SIP profile
	from the drop down list.
WAN SIP Profile	Expects External (WAN) side IP which is present in the
	external network. User can select the configured external
	side SIP profile from the drop down list.
SIP Domains/Destination URI	The domain name which user is selected in the external sip
	profile configuration will be displayed in the sip domains field
	The user has to can provide the URI of the destination for
	which calls has to be routed if reaches the corresponding
	domain name
Media Profile	In this filed user can select the type of media like Transcoding
	or general
	User can select the Media profile from the drop down list.
Media Encryption (LAN)	The media encryption feature using secure RTP (SRTP)
	delivers the ability to encrypt LAN Side media packets. SRTP
	is a security profile for RTP that adds confidentiality, message
	authentication, and replay protection to that protocol. This
	field is enabled only if the user is using transcoding media in
	the media profile
Media Encryption (WAN)	The media encryption feature using secure RTP (SRTP)
	delivers the ability to encrypt WAN Side media packets. SRTP
	is a security profile for RTP that adds confidentiality, message
	authentication, and replay protection to that protocol. This
	field is enabled only if the user is using transcoding media in
	the media profile

T38 Profile	Provide a T38 Profile which is already configured. The drop
	down menu will show the available T38 profiles.
IP Auth	User can check this option if need to enable ip authentication
	for roaming users, and configure the allowable ip:port in the
	allow (ip:port) field in the external sip profile configuration
Force Expire	Force a time period where the roaming user registration will
	be forced to expire. Specify force expire in the range of 1-
	3600.
Max Inbound	User can specify the max allowable roaming users in this field
	for inbound
Max Outbound	User can specify the max allowable roaming users in this field
	for outbound
Presence	User can check this option if he want to use the presence
	feature, blox will work as a presence client
Presence server	User can provide the presence server ip address in this field
	in the format IP address: Port.
Presence Domain	User can provide the presence server domain address in this
	field
Enum	User can check this option if he want to use the enum
	feature
Enum Type	Blox Esbc enum type allows user to select multiple
	enum(enum, isn and isn2) which can be available in
	dropdown list.
Enum suffix	User can specify the suffix for the enum in this field or can
	use the default value, default suffix will be e164.arpa
Enum service	User can specify the service which he wanted to use with
	enum, default is sip

# 5.6 Least Cost Routing

## Navigate through Signaling -> Least Cost Routing

Least cost routing uses the graphic user interface of the Blox Esbc to allow users to create routing rules. Least Cost Routing rules can be used to route calls based on route costs.

Name *	Description =	Options
LCRroute1	LCR route for ellast	× ×
9 >		
figuration		
Jsers		
t Routing as		
gs		

Figure 30: Least Cost Routing

Click Add New, to create LCR Rule.

Name	Least 1		
Description	LCR Rule for Elastix	(£)	
Prefix To Match	00	1	
LAN SIP Profile	-No Profile-	× 6	
Trunks Config		<u> </u>	3
		>	
		>>	
		<	
		11	

Figure 31: Create LCR Rule

Name	Enter the name of the Least Cost Routing for user's reference.
Description	Provide the description for the Least Call Routing.
Prefix to match	User can add any number as a prefix for the respective LCR rule. They can identify prefix to match in the range of (1-16) numbers only.
LAN SIP Profile	Provide the Internal (LAN) side SIP profile which has been createdfor LCR.Select respective SIP profile where the call need to get routed
Trunks Config	The user has to create an LCR similar for trunk configuration.By default it displays all the trunks configured in the Blox Esbc. Usercan select a particular trunk accordingly to their priority.The prefix has to be matched with configured prefix insidethe PBX for that particular selected trunk.

# **5.7 TLS Settings**

#### 5.7.1 Device Root CA

In this Section, user can upload a CA file and generate the same along with the Country name, Province Name, Organization name, Email address, Encryption strength and valid days etc.

To download Device root CA, user need to generate the certificate locally by using generate option.

Network		
System	Upload Generate Download Root CA	
Media		
- Signalling	Certificate:	*
SIP Profile	Data: Version: 3 (0x2)	
Trunk Configuration	Serial Number: 15610969937660150014	
Roaming Users	(0xd8a54e72a58900fe)	
Least Cost Routing	Signature Algorithm: shalWithRSAEncryption Issuer: CN=certificate, ST=karnataka,	
TLS Settings	C=in/emailAddress=sbc@allo.com, O=cem	
- Device Root CA	Validity	
Server Certs	Not Before: Feb 12 01:29:45 2015 GMT Not After : Mar 14 01:29:45 2015 GMT	
- Client Certs	Subject: CN=certificate, ST=karnataka,	
NAT Settings	C=in/emailAddress=sbc@allo.com, 0=cem	~
Security		
Status		
Tools		

Figure 32: Device Root CA

# 5.7.2 Server Certificates

In this section, user can upload the certificates with Passphrases.

Dashboard	Server Certificates 🔞	
Network		
System	Upload Generate	
Media		
Signalling 🔉	Certificates -	Options
IP Profile	and American	
runk Configuration	servercert	
oaming Users		
east Cost Routing		
LS Settings		
Device Root CA		
Server Certs		
Client Certs		
AT Settings		
Security		
Status		



# **5.7.3 Client Certificates**

It provides detailed information about the client certificates with viable options which are uploaded in Blox Esbc.

Dashboard	Client Certificates 🔞	0
Network	Connected Clinet Control of	
System	Generate Client Certificates	
🕨 Media	Certificates *	Options
= Signalling 💦	- Contract	
SIP Profile	yealink	
Trunk Configuration		
Roaming Users		
Least Cost Routing		
TLS Settings		
<ul> <li>Device Root CA</li> </ul>		
<ul> <li>Server Certs</li> </ul>		
<ul> <li>Client Certs</li> </ul>		
NAT Settings		
Security		
Status		
• Tools		

#### **Figure 34: Client Certificates**

Initially Device Root CA needs to be generated

After generating the Device Root CA, Server Certificates will get an option to generate the Server Certificates.

Similarly client certificates needs to be generated and saved locally. Client Certificate needs to be uploaded in the End user agent client (say IP Phones: yealink, snom)

# **5.8 General Settings**

#### **Global Settings**

In global settings user can specify the User-Agent name which he wants to sent in the message going out from the Blox Esbc

User can also specify the maximum number of cdr records to be store in the Blox Esbc

#### Nat Settings

NAT (Network Address Translation) translates the source IP address of a device on one network interface, usually the Internal, to a different IP address as it leaves another interface, usually the interface connected to the ISP and the Internet. This enables a single public address to represent a significantly larger number of private addresses.

Dashboard	General Settings 🎱				
Network	The second second second				
• System	Global Settings				- AN
🔹 Media		User Agent	Blox-Esbo	(1)	
- Signalling >	2	Maximum CDR Recor	d 10000		
SIP Domain	Ballan State				-
SIP Profile	NAT Settings				- 0
SIP Headers		Keepalive SIP Method	OPTIONS .		
Trunk Configuration					
Roaming Users		Keepalive Interval	30	_	
Least Cost Routing		Keepalive From-URI	sip: sbc@blox.org	( <u>i</u> )	
TLS Settings					
General Settings					
Presence	Save Cancel				
Security					
👂 Status					
Tools					



# 6.Presence

Presence also known as presence information, conveys the ability and willingness of a user to communicate across a set of devices. SIP is particularly well suited as a presence protocol. SIP location services already contain presence information, in the form of registrations.Furthermore, SIP networks are capable of routing requests from any user on the network to the server that holds the registration state for a user. The presence support is used fo Roaming user, this support will add SIP method SUBSCRIBE and NOTIFY

#### 6.1 Subscribers

## Navigate through Presence > subscribers

Configure the subscribe ers used for the presence feature

Create Subscribers	Profile		*
User name Operator Roaming User Profile	No Profile •		
		BÅVE	CANCEL

# Figure 36: Subscribers

User name	Enter the user name of the subscriber you wish to use
operator	Check the box if the user want to use the subscriber as operator
Roaming user Profile	Select rhe required roaming user profile which the subscriber want to use from the drop down box

#### 6.2 Events

Navigate through Presence > Events

Configure the events list for the subscriber

Create Ever	nts list Profile					x
From Username		0				*
Roaming User Profile	No Profile 🔻					
		_		*	-	
Subscribers List			00	1940	(E)	
			*	*	 -	
Events	france council	0		-		
	message-sum					
0 C De alvada	application/p	121				- 0
AC Packets	- P P M M M M M M M M					

#### Figure 37: Events

From Username	Enter the username for which user need to create the event
Roaming User Profile	Select the required roaming user profile which user want to use for this event from the drop down list
Subscribers List	Select the required subscribers from the available list to active list for this event
Events	Configure this field as "message-summary"
AC Packets	Use the default value for this field is application/pidf+Xml
Expire	Configure the expire time for the event

# 7. Security

# 7.1 SIP

## 7.1.1 Attacks Detection

## Navigate through Security > SIP > Attacks Detection

The SIP Attack Detection page allows to configure the SIP Deep packet Inspection rules categories. The administrator can enable/disable the inspection against particular category of rules, action to be taken on detecting attacks matching the rules in the categories. The possible actions that the Blox Esbc can execute are log the alert, block the packets containing the attack vector and blacklist the attacker IP for the given duration. The blocking duration of how long the attacker up needs to be blocked is also configure per category level.

The following table lists the SIP Deep packet Inspection rules categories supported in Blox Esbc and configuration parameters in each category.

Network	Category	Action	Blocking Duration (seconds)	Enabled	Options	
System	Sip Devices Scanning	Block	120		1	
Media	SIP Extensions Discovery	Block	120		1	
Signalling Security 3	Multiple Authentication Failures/Bruteforce password cracking Attempt	Log	1800		1	
Attacks	Ghost calls Attempt	Block	1800		1	
Detection	SIP Protocol Compliance	Log	none		1	
Protocol Compliance	Sip Dos Attacks	Block	1800		1	1
Signature Jpdate	Sip DDos Attacks	Block	1800		1	
Firewall /PN	TCP Syn Flood	Block	1800		1	
Status	TCP Flood	Block	1800		1	1
Tools	TCP Distributed Flood	Block	1800		1	

#### **Figure 36: SIP Attacks Detection**

Category	Description	User Configurable options
Reconnaissance Attacks	This can be considered as the first step of attacking any system or a network. In this a hacker tries to learn information about our network typically conducts a ping sweep of the target network to determine which IP addresses are alive. Then the intruder determines which services or ports are active on the live IP addresses. From this information, the intruder queries the ports to determine the type and version of the application and operating system running on the target host. The attacker often uses port scanning, for example, to discover any vulnerable ports. After a port scan, an attacker usually exploits known vulnerabilities of services associated with open ports that were detected.	-

SIP Devices Scanning	The intruder will scan the PBX ports to see what devices are connected to it. With that info, he can exploit 3rd party vulnerabilities. The Blox Esbc will not respond to his query.	_
SIP Extensions Discovery	The intruder will ask the PBX to divulge the range of the extension numbers. With that info, he can try different passwords to take control of these extensions. The Blox Esbc will not respond to that query.	Invalid SIP User Registration Attempts/Duration
Multiple Authentication Failures/Brute force password Attempt	The intruder will try to log in with different user names and passwords multiple times. Once he succeeds, he will have control of that extension. The Blox Esbc can block, log or blacklist the IP for a period of time if it exceeds the authorized number of trials/second.	Failed Authentication Attempts/Duration
Ghost calls Attempt	The intruder will generate calls to an extension and it will look like the calls come from that same extension. His goal is to crash the PBX resulting in disrupted communication. The Blox Esbc can block, log or blacklist the IP for a period of time if it exceeds the authorized number of trials/second.	No of Anonymous Invite Responses/Duration
SIP Protocol Compliance	This kind of attacks refers to use of some kind of automated tool like SIPP to generate false script where some of the most important fields of SIP headers and body can body can be modified in terms of their length like "From header length", "To Header length", "Contact length". It can also be useful in handling the correct use of Maximum Dialog within a session, SIP Ports and its Protocol.	_
SIP Anomaly Attacks	The SIP Deep packet inspection engine running the	-

		1
	STM appliance has been made to inspect the SIP	
	traffic with the SIP Security Compliance rules in built	
	into the SIP DPI engine.	
	The anomalies in the SIP Message headers can result	
	to various erroneous conditions, SIP parser failures &	
	malformed packets which will lead to SIP applications	
	vulnerable to attacks.	
	The Default parameters will be used by the SIP deep	
	packet engine for identifying the different protocol	
	anomaly conditions and take the action configured	
	by the administrator.	
	Configuring inappropriate values for these	
	parameters can result to the disruptive impact in the	
	VOIP deployment. Administrators with more in-depth	
	understanding with the SIP Protocol can choose to	
	tune these parameters for their specific deployment	
	needs. Otherwise, it is recommended to use the	
	default settings for these parameters.	
SIP Dos Attacks	Flooding attempts using various SIP messages.	No of SIP Request
		Messages/Duration
SIP DDos Attacks	Distributed flooding attempts using various SIP	No of SIP Response
	messages.	Messages/Duration
	Cross Site Scripting (also known as XSS or CSS) is one	
	of the most common application layer hacking	
	techniques.	
SIP Cross site	In general, cross-site scripting refers to that hacking	
scripting Attacks	technique that leverages vulnerabilities in the code	-
	of a web application allow an attacker to send	
	malicious content from an end-user and collect some	
	type of data from the victim.	

	The use of XSS might compromise private information, manipulate or steal cookies, create requests that can be mistaken for those of a valid user, or execute malicious code on the end-user systems. It can be used to steal data about "From Header", "To Header", and "Call -ID", "CONTACT "," Extension Password and other such confidential data.	
Buffer overflow Attacks	This refers to illegally trying to access the resources of the SIP device like its memory address for which it does not have the authenticate permissions leading to data corruption of this address along with its adjacent address.	-
3 <sup>rd</sup> Party Vendor Vulnerabilities	This attack refers to any malicious activities from 3 <sup>rd</sup> party like DIGIUM Asterisk channel driver DOS attempt and other such attack.	_
TCP Syn Flood	It's a kind of DOS attack in which a large number of <b>TCP SYN</b> packets are sent to the victim's device .Each of these packets will try to establish a new session, thus consuming the victim's device resources. Such attack is also called open half connection as these new sessions are not terminated and finally the legitimate users are barred from availing the Device resources.	No of TCP Syn Packet within specified duration
TCP Flood	This refers to flooding the device with general TCP packet on any port where legitimate users are barred from availing the Device resources after some interval of time.	No of TCP Packet within specified duration
TCP Distributed Flood	In a <b>TCP DDos</b> attack, the incoming <b>TCP traffic</b> flooding the victim originates from many different sources – potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack	No of TCP Packet within specified duration

UDP Flood	<ul> <li>simply by blocking a single IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.</li> <li>This refers to flooding the device with general UDP packet on any port where legitimate users are barred from availing the Device resources after some interval of time.</li> </ul>	No of UDP Packet within specified duration
UDP Distributed Flood	In a <b>UDP DDos</b> attack, the incoming <b>UDP traffic</b> <b>flooding</b> the victim originates from many different sources – potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.	No of UDP Packet within specified duration
Generic Attacks	<ul> <li>Some of the common attacks under this category are</li> <li>Bye Teardown, Registration Hijack, Registration</li> <li>Adder, and Registration Eraser.</li> <li>1) Bye Teardown attack disrupts a call that is in session between two users.</li> <li>2) Registration Hijack: The first step in hijacking a registration is to find register able addresses and it hijacks the already registered extension.</li> <li>3) Registration Adder: This tool attempts to bind another SIP address to the target, effectively making a phone call ring in two places (the legitimate user's desk phone and the attacker's phone).</li> <li>4) Registration Eraser: This tool will effectively cause a denial of service by sending a spoofed SIP REGISTER</li> </ul>	-

message to convince the	proxy that a phone/user is
unavailable.	

## 7.1.2 Protocol Compliance

#### Navigate through Security > SIP > Protocol Compliance

The SIP Deep packet inspection engine running the Blox Esbc appliance has been made to inspect the SIP traffic with the SIP Security Compliance rules in built into the SIP DPI engine. The anomalies in the SIP Message headers can result to various erroneous conditions, SIP parser failures & malformed packets which will lead to SIP applications vulnerable to attacks.

System	SIP Protocol Compl	SIP Methods					. 0			
Media	Max Sessions	4097	Max From length	256	SIP Methods	invite			invite	1
Signalling	intern and a state inte	©		0		cancel		>	cancel	
Security >	Max Dialogs per session	2048	Max To length	256		ack bye		23	ack bye	_
IP	36351011	(M)		00		register		<	register	
Attacks	Max URI length	256	Max Via length	1024		options		-	options	
Detection		( <u>u)</u>	4			refer	20	<<	refer	~
Protocol Compliance	Max Call ID length	80	Max Contact	1024		subscribe			subscribe	120
Signature		C.	length	123	-					
Jpdate	Max Request name	20	Max Content	2048						
irewall	length	(B)	length	0						
/PN		_		-						
Status										

**Figure 37: Protocol Compliance** 

The following parameters will be used by the SIP deep packet engine for identifying the different protocol anomaly conditions and take the action configured by the administrator.

Configuring inappropriate values for these parameters can result to the disruptive impact in the VOIP deployment. Administrators with more in-depth understanding with the SIP Protocol can choose to tune these parameters for their specific deployment needs. Otherwise it is recommended to use the default settings for these parameters.

#### Max\_sessions

A SIP session is the application level connection setup created between the SIP server and SIP client for exchanging the audio/video messages with each other.

The max\_sessions parameter defines the maximum number session that SIP deep packet inspection engine can keep track of. The default value has been set as 4096.

#### Max Dialogs per session

Max\_Dialogs\_per\_session specifies the maximum number of SIP messages transaction that can happen between the SIP server and client.

#### Methods

This parameter specifies on what methods to check for SIP messages.

Following are the SIP messages that SIP DPI Engine can identify: (1) invite, (2) cancel, (3) ack, (4) bye, (5) register, (6) options, (7) refer, (8) subscribe, (9) update (10) join (11) info (12) message (13) notify (14) prack.

#### Max\_uri\_len

The URI identifies the user or service to which SIP request is being addressed. Max\_uri\_len specifies the maximum Request URI field size. Default is set to 256. The allowed range for this option is 1 - 65535.

#### Max\_call\_id\_len

The Call-ID header field in SIP message acts as a unique identifier that relates to sequence of messages exchanged between SIP client and server. Max\_call\_id\_len specifies the maximum Call-ID field size. Default is set to 256. The allowed range for this option is 1 - 65535.

#### Max\_requestName\_len

Max\_requestName\_len specifies the maximum request name size that is part of the CSeq ID. Default is set to 20. The allowed range for this option is 1 - 65535

#### Max\_from\_len

The From header field indicates the identity of the initiator of the SIP request. Max\_from\_len specifies the maximum From field size. The allowed range for this option is 1 - 65535.

#### Max\_to\_len

The To header field specifies the desired recipient of the SIP request. Max\_to\_len specifies the maximum To field size. Default is set to 25

6. The allowed range for this option is 1 - 65535.

#### Max\_via\_len

The Via header field indicates the transport used for the SIP transaction & identifies the location where the SIP response is to be sent.

Max\_via\_len specifies the maximum via field size. Default is set to 1024. The allowed range for this option is 1 - 65535.

#### Max\_contact\_len

Identifier used to contact that specific instance of the SIP client/server for subsequent requests. Max\_contact\_len specifies the maximum Contact field size. Default is set to 256. The allowed range for this option is 1 - 65535.

#### Max\_content\_len

Max\_content\_len specifies the maximum content length of the message body. Default is set to 1024. The allowed range for this option is 1 - 65535.

## 6.1.3 Signature Update

#### Navigate through Security > SIP > Signature Update

It allows user to schedule the update by configuring the time schedule fields. Apply will cause signature to be updated according to the time scheduled by user.

The option "Update Signatures now" updates the signatures at that moment.

▶ Dashboard	Signature Update 🙆
Network	
System	Signature Update Settings
Media	Enable Update
Signalling	Time Schedule 2 00 AM 🗸 Daily 🗸 Sanday 1
🝷 Security 💦 🔉	
SIP	
<ul> <li>Attacks</li> <li>Detection</li> </ul>	Apply Cancel Update Signatures now
<ul> <li>Protocol</li> <li>Compliance</li> </ul>	
🤟 Signature 💋	
Firewall	
VPN	
🕨 Status	
Tools	

Figure 38: Signature Update

# 7.2 Firewall

# 7.2.1 Firewall Config

Navigate through Security > Firewall > Firewall Config

The firewall rules configuration will allow the administrator in configuring what traffic should be allowed to protected SIP PBX/Gateway network from untrusted wan zone, besides DPI enabled SIP traffic and RTP traffic.

The administrator needs to specify the source and destination networks and port numbers and protocol that will be used as the matching criteria in the filtering rule and action to be taken on matching the filtering rule.

The possible actions are to block the traffic and allow the traffic on matching the filtering rule. The rules precedence will be in the order in which the rules configured on firewall rules table. Shows the table with columns Name, Enabled, Src Type, Src Addr, Dst Type, Dst Addr, Protocol, Port and Action.

User can search the entries by entering the value in the Search box which appears on top right of the table.

Clicking on Add New opens a dialog with fields Name, Enabled, Src Type, Src Addr, Dst Type, Dst Addr, Protocol, Port and Action.

Single entry can be deleted by clicking on the delete button. Multiple entries can be deleted by selecting the check boxes which appears on left of each entry. Delete Selected will delete the entries which are selected.

User can sort (Ascending / Descending) the table entries by clicking on the particular column of the table for e.g. Name.

Entry can be edited by clicking on 🖍 button.

Entry can be deleted by clicking on 🔀 button.

<u> </u>		Name =	Src Type 🛎	Src Addr 🗢	Dst Type 🔹	Dst Addr 🔹	Protocol *	Port *	Action 🗢	Enabled	Opt	ions
		Dhcp Access	ANY		ANY		udp	67,68	Allow		1	×
ng		Dns Access	ANY		ANY		any	53	Allow		1	×
>		ICMP Access	ANY		ANY		icmp	0	Allow		1	x
		NTP Access	ANY		ANY		udp	123	Allow		1	×
all Config		SSH Access	ANY		ANY		tep	22	Allow		1	×
all Rate		Telnet Access	ANY		ANY		tep	23	Allow		1	×
orwarding ist IP s		Web Access	ANY		ANY		tcp	80,443,8080,8088	Allow		1	×
ist IP rs sses P Filters	Ĺ	i <mark>dd New</mark> D	elete Selected									



Click Add New, to create the firewall Rule.

Name	NTP Access
Enabled	(ī)
Src Type	ANY 💽 💿
Src Address	(3)
Dst Type	ANY 💽
Dst Address	(3)
Protocol	any 💌 😟
Port	)( <u>E</u>
Action	Allow 💉 🛈

# Figure 40: Create Firewall Rule

Name	Specify the name for the Firewall Rules for user's reference. The user
	can choose any name to recognize the Firewall Rules.
Frahlad	It allows the wear to either anable or disable Firewall Dulas
Enabled	It allows the user to either enable or disable Firewall Rules.
Src Type	User can select the appropriate Src type from the drop down list.
Sicilype	oser can select the appropriate sic type norm the alop down list.
Src Address	User can configure and apply the Firewall rule to particular Source
	6 11 / 1
	Address (Src Address). E.g.10.0.0.3
	· · · · ·
Dst Type	User can select the appropriate Dst type from the drop down list.
,	
Dst Address	User can configure and apply the Firewall rule to particular destination

	Address (Dst Address). E.g.:192.168.0.8
Protocol	Protocols specify interactions between the communicating entities. User can select the type of protocol whether it is TCP or UDP from the drop down list.
Port	User can configure and apply the Firewall rule to particular port number.E.g.:5060
Action	User can select the action either block or action from the drop down list.

Changes can be saved by clicking on '**Save'** button and can ignore the changes by clicking on Cancel button.

# 7.2.2 Firewall Rate Limiting

#### Navigate through Security > Firewall > Firewall Rate Limiting

Firewall Rate Limiting allows user to configure global firewall settings.

Dashboard	Firewall Rate Limiting		
Network	The second second second		
System	Firewall Rate Limiting		-00
Media	TCP Syn Flood Rate	1024	œ
<ul> <li>Signalling</li> </ul>	TCP Syn Flood Burst	128	0
<ul> <li>Security</li> </ul>	TCP Flood Rate	4096	0
SIP Firewall	TCP Flood Burst	96	(T)
<ul> <li>Firewall Config</li> </ul>	UDP Flood Rate	8192	œ
Firewall Rate	UDP Flood Burst	198	0
<ul> <li>Port Forwarding</li> </ul>		128	0.
<ul> <li>Whitelist IP</li> <li>Addresses</li> </ul>		1.000	
<ul> <li>Blacklist IP</li> <li>Addresses</li> </ul>	ICMP Flood Burst	64	0.
Dynamic     Blacklist IP			
Addresses	Save Cancel		
- Geo IP Filters			
VRN			
<ul> <li>Status</li> </ul>			
• Tools			

**Figure 41: Firewall Rate Limiting** 

# 7.2.3 Port forwarding

Navigate through Security > Firewall > Port forwarding

It is used to forward incoming connection requests to internal network hosts.

Network		Name +	Interface	Protocol	External Addre	Extornal	Port + Int	ornal Addros	s 🔹 Internal Port 🗧	Descrip	tion
System		Manne	milenace	1 1010201	- LATERNAL Addre	LATERINAL		ernal Addres			
Media		elastix	ethO	any	192.168.0.203	8443	10.10.10.2	200 844	3 <u>elastix g</u> u	ui 🖉	×
Signalling		elastix 1	ethO	any	192.168.0.203	8443	10.10.10.2	200 844	3 <u>elastix g</u> u	ui 🛛 🖉	×
ecurity											
0											
wall											
Firewall Config											
iting											
Firewall Rate iting Port Forwarding Whitelist IP											
iting Port Forwarding Whitelist IP dresses	Ą	id Hew	Dojete S	elected							
iting Port Forwarding Whitelist IP	A	dd Hew	Belete S	elected							
iting Port Forwarding Whitelist IP Iresses Blacklist IP Iresses Dynamic	A	<del>ld Hew</del>	Delete S	siected							
iting Port Forwarding Whitelist IP resses Blacklist IP resses Dynamic Kilist IP	A	dd llew	Dejete S/	elected							
iting Port Forwarding Whitelist IP Iresses Blacklist IP Iresses	A	<del>ld llow</del>	balete S	elected							
iting Port Forwarding Whitelist IP Iresses Blacklist IP Iresses Dynamic Kilist IP Iresses	A	dd Hew	bolete Sr	slected							

# Figure 42: Port Forwarding

Click Add New, to create port forwarding Rule.

Name	elastix 1	(C).	
Interfaces	eth0 👻 🖲		
Protocol	any 📝 🕕		
External Address	192.168.0.203	(3)	
External Port	8443		
Internal Address	10.10.10.200	(0)	
Internal Port	8443 0		
Description	elastix mi		( <u>1</u> )

# Figure 43: Create Port Forwarding Rule

Name	Specify the name for the Port forwarding for user's reference.
	The user can choose any name to recognize the Port
	forwarding.
Interfaces	Select the appropriate interfaces from the drop down list
	where the user desires to create Port forwarding.
	Ex: if user wants to create the virtual IP in wan side select Eth0,
	WAN Interface-192.168.10.231

Eth2,LAN Interface-10.0.0.1ProtocolProtocols specify interactions between the communicating entities. User can select the type of protocol whether it is TCP or UDP from the drop down list.External AddressThis address assigned to you by your Internet Service Provider and allows user to enter the external address. E.g.:192.168.x.x	Γ	
ProtocolProtocols specify interactions between the communicating entities. User can select the type of protocol whether it is TCP or UDP from the drop down list.External AddressThis address assigned to you by your Internet Service Provider and allows user to enter the external address. E.g.:192.168.x.xExternal PortThe port forwarding is used to identify your external address and detects open ports on your connection.Internal AddressThe internal IP address is assigned by your local network router that often begins with 192.168.x.x.Internal PortIt specifies the internal port that connects to the local area		If the user wants to create the virtual IP in LAN side select
entities. User can select the type of protocol whether it is TCP or UDP from the drop down list.External AddressThis address assigned to you by your Internet Service Provider and allows user to enter the external address. E.g.:192.168.x.xExternal PortThe port forwarding is used to identify your external address and detects open ports on your connection.Internal AddressThe internal IP address is assigned by your local network router that often begins with 192.168.x.x.Internal PortIt specifies the internal port that connects to the local area		Eth2,LAN Interface-10.0.0.1
or UDP from the drop down list.External AddressThis address assigned to you by your Internet Service Provider and allows user to enter the external address. E.g.:192.168.x.xExternal PortThe port forwarding is used to identify your external address and detects open ports on your connection.Internal AddressThe internal IP address is assigned by your local network router that often begins with 192.168.x.x.Internal PortIt allows user to find the IP addresses in their local network.Internal PortIt specifies the internal port that connects to the local area	Protocol	Protocols specify interactions between the communicating
External AddressThis address assigned to you by your Internet Service Provider and allows user to enter the external address. E.g.:192.168.x.xExternal PortThe port forwarding is used to identify your external address and detects open ports on your connection.Internal AddressThe internal IP address is assigned by your local network router that often begins with 192.168.x.x.Internal PortIt allows user to find the IP addresses in their local network.Internal PortIt specifies the internal port that connects to the local area		entities. User can select the type of protocol whether it is TCP
Internal PortThe port forwarding is used to identify your external address and detects open ports on your connection.Internal AddressThe internal IP address is assigned by your local network router that often begins with 192.168.x.x.Internal PortIt allows user to find the IP addresses in their local network.		or UDP from the drop down list.
External PortThe port forwarding is used to identify your external address and detects open ports on your connection.Internal AddressThe internal IP address is assigned by your local network router that often begins with 192.168.x.x.Internal PortIt specifies the internal port that connects to the local area	External Address	This address assigned to you by your Internet Service Provider
External PortThe port forwarding is used to identify your external address and detects open ports on your connection.Internal AddressThe internal IP address is assigned by your local network router that often begins with 192.168.x.x.Internal PortIt specifies the internal port that connects to the local area		and allows user to enter the external address.
and detects open ports on your connection.Internal AddressThe internal IP address is assigned by your local network router that often begins with 192.168.x.x.It allows user to find the IP addresses in their local network.Internal PortIt specifies the internal port that connects to the local area		E.g.:192.168.x.x
Internal AddressThe internal IP address is assigned by your local network router that often begins with 192.168.x.x. It allows user to find the IP addresses in their local network.Internal PortIt specifies the internal port that connects to the local area	External Port	The port forwarding is used to identify your external address
that often begins with 192.168.x.x.It allows user to find the IP addresses in their local network.Internal PortIt specifies the internal port that connects to the local area		and detects open ports on your connection.
It allows user to find the IP addresses in their local network.Internal PortIt specifies the internal port that connects to the local area	Internal Address	The internal IP address is assigned by your local network router
Internal Port It specifies the internal port that connects to the local area		that often begins with 192.168.x.x.
		It allows user to find the IP addresses in their local network.
network (LAN).	Internal Port	It specifies the internal port that connects to the local area
		network (LAN).
Description Provide the description for the Port Forwarding. (Optional)	Description	Provide the description for the Port Forwarding. (Optional)

# 7.2.4 White list IP Addresses

#### Navigate through Security > Firewall > White list IP Addresses

This page allows to configure the white listed IP addresses in the untrusted wan zone from which the access to communicate with the protected SIP network will be allowed by the Blox Esbc firewall.

It will also allows configuring whether the white rules take precedence over the blacklist rules (both static and dynamic) configured on the device at any instant.

White list Rules Precedes over Blacklist Rules can be saved by clicking on 'Save' button.

It shows the table with columns Name, IP Type, Address, Enabled and Comments.

User can search the entries by entering the value in the Search box which appears on top right of the table.

Clicking on Add New opens a dialog with fields Name, IP Type, Address, Enabled and Comments.

Single entry can be deleted by clicking on the delete button. Multiple entries can be deleted by selecting the check boxes which appears on left of each entry. Delete Selected will delete the entries which are selected.

User can sort (Ascending / Descending) the table entries by clicking on the particular column of the table for e.g. Name.

Entry can be edited by clicking on 🖉 button.

Entry can be deleted by clicking on 🔀 button.

Dashboard	Whitelist IP Addres	sses 🥨				
Network	Whitelist IP Rules Precedes over Blacklist IP Rules					
System	Name -	IP Type #	Address +	Comments +	Enabled	Options
Media	test1	IP HOST	192,168,10,66	Whitelist test 1		/ ×
Signalling	-			and an and an and		
Security >	test2	IP_HOST	192.168.10.86	whitelist test2		XX
SIP						
Firewall						
Firewall Config						
Firewall Rate						
Limiting						
Limiting Port Forwarding	g					
Limiting Port Forwardini Whitelist IP	g					
Limiting Port Forwardin Whitelist IP Addresses	g					
Limiting Port Forwarding		Alere Selectori				
Limiting Port Forwarding Whitelist IP Addresses Blacklist IP Addresses Dynamic		elete Selecteri				
.imiting Port Forwarding Addresses Addresses Addresses Addresses Jannamic Jacklist IP		ølete Selected				
.imiting Port.Forwarding Whitelist IP Addresses Blacklist IP Addresses Dynamic Jacklist IP Addresses		elete Selectori				
Jimiting Port, Forwarding Whitelist IP Addresses Diacklist IP Addresses Dynamic Nacklist IP Addresses Geo IP Filters		elete Selecteri				
Jimiting Port, Forwardinu Whitelist IP Addresses Dynamic Jacklist IP Addresses Geo IP Filters Geo IP Filters /PN		elete Selected				
Limiting Whitelist IP Addresses Blacklist IP Addresses Dynamic Blacklist IP Addresses		elete Selecteri				

**Figure 44: Whitelist IP Addresses** 

Click Add New, to create a Whitelist Rule.

Name	test2		
Ір Туре	IP_HOST 🛛 👻 🗵		
Address	192.168.10.86	(E)	
Enable	0		
Comments	whitelist test2		
			(T)
		SAVE	CAN

Figure 45: Create Whitelist Rule

Name	Specify the name for the White list Rules for user's reference. The user
	can choose any name to recognize the White list Rules.
ІР Туре	User can select the appropriate IP type from the drop down list. The
	various IP types are IP_Host, IP_Network, IP_Range, and MAC_ADDR.
Address	Specify IP Address/Netmask or IP range or MAC address.
Enable	It allows the user to either enable or disable White list Rules.
Comments	User can specify the comments in the length of 64 char's.

Changes can be saved by clicking on 'Save' button and can ignore the changes by clicking on Cancel button.

#### 7.2.5 Blacklist IP Addresses

#### Navigate through Security > Firewall > Blacklist IP Addresses

This page allows to configure the black listed IP addresses in the untrusted wan zone from which the access to communicate with the protected SIP network will be blocked by the Blox Esbc firewall.

Dashboard	Blacklist IP Addres	ses 🙆				
Network	Name -	IP Type 🕈	Address +	Comments +	Enabled	Options
System Media	Test2	IP_HOST	192.168.10.66	Blacklist test 1		/ x
Signalling	Testing	IP_HOST	192.168.10.66	Blacklist Testing	<b>V</b>	/ ×
Security 🦻						
P						
rewall						
Firewall Config Firewall Rate						
miting						
Port Forwarding						
Whitelist IP ddresses	Add New	A REAL PROPERTY.				
Blacklist IP ddresses	Add llew	elete Selected				
Dynamic						
acklist IP Idresses						
Geo IP Filters						
PN .						
Status						
Tools						

#### **Figure 46: Blacklist IP Addresses**

Click Add New, to create a Blacklist Rule.

Name	Testing	
ІР Туре	IP_HOST	
Address	192.168.10.66	
Enable	0	
Comments	Blacklist Testing	
		(3)

Figure 47: Create Blacklist Rule

It shows the table with columns Name, IP Type, Address, Enabled and Comments.

Clicking on Add New opens a dialog with fields Name, IP Type, Address, Enabled and Comments.

Single entry can be deleted by clicking on the delete button. Multiple entries can be deleted by selecting the checkboxes which appears on left of each entry. **Delete Selected** will delete the entries which are selected.

User can sort (Ascending / Descending) the table entries by clicking on the particular column of the table for e.g. Name.

Entry can be edited by clicking on 🖉 button.

Entry can be deleted by clicking on 🔀 button.

Changes can be saved by clicking on 'Save' button and can ignore the changes by clicking on Cancel button.

#### 7.2.6 Dynamic Blacklist IP Addresses

#### Navigate through Security > Firewall > Dynamic Blacklist IP Addresses

The dynamic blacklist addresses are the blocking rules added by the Blox Esbc SIP deep packet inspection engine to block the traffic from attacker IP addresses for the blocking duration configured in the rules category, on detecting the attack.

The dynamic blacklist addresses page will allow the administrator to see the dynamic blacklist addresses currently configured on the device at any instant. In case if the administrator wants to override and allow the traffic from particular blacklisted IP, he can delete the address from the dynamic blacklist addresses page.

Dashboard	Dynamic Blacklist IP Addresses	
Network	Address -	Options
System		
Media	192.168.10.66	×
Signalling		
- Security		
SIP		
Firewall		
🚽 Firewall Config		
<ul> <li>Firewall Rate</li> <li>Limiting</li> </ul>		
- Port Forwarding		
<ul> <li>Whitelist IP</li> <li>Addresses</li> </ul>	Delete Selecteri	
<ul> <li>Blacklist IP</li> <li>Addresses</li> </ul>	Delete Selected	
<ul> <li>Dynamic Blacklist IP Addresses</li> </ul>		
Geo IP Filters		
VPN		
Status		
Tools		

Figure 48: Dynamic Blacklist IP Addresses

It shows the table with columns Address and Options.

Single entry can be deleted by clicking on the delete button. Multiple entries can be deleted by selecting the check boxes which appears on left of each entry. "Delete Selected" will delete the entries which are selected.

User can sort (Ascending / Descending) the table entries by clicking on the particular column of the table for e.g. Name.

Entry can be deleted by clicking on 🔀 button.

#### 6.2.7 Geo IP Filters

Navigate through Security > Firewall > Geo IP Filters

The administrator can choose to block the traffic originating from the specific countries towards the protected SIP network, by configuring the GeoIP filter rules in Blox Esbc.

Clicking on Allow All Countries will allow all the countries and Block All Countries will block all the countries.

Clicking on Update Geo IP will download the latest database from website and replace the existing country database.

It shows the table with columns Country Name and Allowed.

User can search the entries by entering the value in the Search box which appears on top right of the table.

User can sort (Ascending / Descending) the table entries by clicking on the particular column of the table for e.g. Name.

Entry can be edited by clicking on 🖉 button.

Changes can be saved by clicking on 'Save' button and can ignore the changes by clicking on Cancel button.

<ul> <li>Network</li> <li>System</li> </ul>	Allow All Countries Block All Countries Update Geo IP		
Media	Country Name	Allowed	Options
Signalling	RUSSIAN FEDERATION		
• Security			
SIP	SYRIAN ARAB REPUBLIC		
Firewall	SUDAN		1
Firewall Config     Firewall Rate	NIGERIA		1
<ul> <li>Firewall Rate</li> <li>Limiting</li> <li>Port Forwarding</li> </ul>	KOREA, REPUBLIC OF		2
<ul> <li>Whitelist IP</li> <li>Addresses</li> </ul>	CHINA		1
<ul> <li>Blacklist IP</li> <li>Addresses</li> </ul>	UKRAINE		1
Dynamic Blacklist IP Addresses	ALGERIA		1
🔸 Geo IP Filters			
VPN			
Status			

**Figure 49: Geo IP Filters** 

# 7.3 VPN

A virtual private network (VPN) tunnel provides a secure communication channel either between two gateway VPN firewalls or a remote VPN client and gateway VPN firewall. As a result, the IP address at least one of the tunnel endpoints needs to be known in advance in order for the other tunnel endpoint to establish (or reestablish) the VPN tunnel.

# 7.3.1 IPSec VPN

Navigate through VPN > IPSec VPN

Enable     Disable     Save	Marcala Para and	for some of the same
Policy Name 🔻	Remote Gateway +	Enabled Option
ipsecvpn	192.168.0.81	2
>		
PN		

#### Figure 50: IFSEC VPIN

#### **Policy Settings**

IPSec has the following two modes of forwarding data across a network:

- Tunnel mode
- Transport mode

Each differs in its application as well as the amount of overhead added to the passenger packet. These modes are described in more detail in the next two sections.

#### **Tunnel Mode**

It works by encapsulating and protecting an entire IP packet. Because tunnel mode encapsulates or hides the IP header of the pre-encrypted packet, a new IP header is added so that the packet can be successfully forwarded. The encrypting devices themselves own the IP addresses used in this new header.

It can be configured with either or both IPSec protocols (ESP and AH). Tunnel mode results in additional packet expansion of approximately 20 bytes because of the new IP header.

Tunnel mode is widely considered more secure and flexible than transport mode. IPSec tunnel mode encrypts the source and destination IP addresses of the original packet, and hides that information from the unprotected network.

Policy Settings	IKE IPSec Advanced	
Enable		
Policy Name	Testing	
Mode	💿 Tunnel 🔘 Transport	
Policy Type	P2P O Road Warrior	
Local Gateway	192.168.0.103	
Local Network	0.0.0.0	
Remote Gateway	192.168.0.123	
Remote Network	0.0.0.0	
	SAVE	CANCEL

Enable	This allows the user to either enable or disable policy settings. If it's
	enabled, then this policy is deployed.
Policy Name	Enter the policy name for the IPSec VPN for user reference.
Mode	User can select different modes p2p / Road warrior depending on
	these 2, tunnels and transport can be selected.
Policy Type	User can select either p2p / Road warrior policy type.
Local gateway	It specifies the gateway IP of the device. E.g.: 192.168.x.x
Local network	Network behind the gateway need to be accessed. Eg:
	192.168.0.0/24
Remote gateway	Enter the Remote gateway IP. E.g.: 192.168.x.x
Remote network	It specifies Remote gateway to be accessed. Eg: 192.168.1.0/24
IKE	

To implement a VPN solution with encryption, periodic changing of session encryption keys is necessary. Failure to change these keys makes the VPN susceptible to brute force decryption attacks. IPSec solves the problem with the IKE protocol, which makes use of two other protocols to authenticate a crypto peer and to generate keys. IKE uses a mathematical algorithm called a Diffie-Hellman exchange to generate symmetrical session keys to be used by two crypto peers.

IKE also manages the negotiation of other security parameters such as the data to be protected, the strength of the keys, the hash methods used, and whether the packets are protected from anti-replay. ISAKMP normally uses UDP port 500 as both the source and destination port.

Create IPSec VPN	Rule
Policy Settings IK	E IPSec Advanced
IKE Exchange Mode Lifetime Encryption Algorithm Hash Algorithm Authentication method Preshared key DH Group	Main 5 in minutes 3DES MD5 PreSharedKey Show password 2
	SAVE CANCEL

#### Figure 52: IKE

IKE Exchange Mode	User can select two modes like Main or aggressive mode to be sustained.
Lifetime	It specifies time after the renegotiation of phase 1 happens
Encryption Algorithm	It can be used during phase 1 negotiation
Hash Algorithm	It is mainly used for authentication in phase 1.
Authentication Method	It allows a single method (PreSharedKey) to authenticate the IKE
	mode instance of all methods.
	The selected authentication allows user to configure the field.
Preshared Key	This secret key is mainly used for authentication.
DH Group	Key exchange protocol allows two parties without any initial shared
	sheet to create one securely.

#### IPSec

#### Transport: can use AH/ESP mode.

#### **AH (Authentication Header)**

The AH protocol (IP protocol 51) forms the other part of IPSec. It does not encrypt data in the usual sense, by hiding the data but it adds a tamper-evident seal to the data. It also protects the non-mutable fields in the IP header carrying the data, which includes the address fields of the IP header.

The AH protocol should not be used alone when there is a requirement for data confidentiality.

#### **ESP (Encapsulating Security Protocol)**

The ESP header (IP protocol 50) forms the core of the IPSec protocol. This protocol, in conjunction with an agreed-upon set of security Parameters or transform set, protects data by rendering it indecipherable. This protocol encrypts the data portion of the packet only and uses other protections (HMAC) for other protections (data integrity, anti-replay, and man-in-the-middle). Optionally, it can also provide for authentication of the protected data.

Rule	>		
IPSec	Advanced		
	ESP		
Î	in minutes		
5 💙			
AES128 AES192 AES256 Blowfish CAST128			
SHA1			
		SAVE	CANCEL
	IPSec AH • 5 3DES AES128 AES128 AES128 AES128 AES128 3DES MD5 SHA1	IPSec Advanced	IPSec Advanced     AH ESP     in minutes     5     3DES     AES128   AES128

Figure 53: IPSec Settings

Transport	User can use AH/ESP mode
Lifetime	It specifies the time, after the renegotiation of phase 2 happens.
PFS Group	Perfect Forward Secrecy of keys does not compromise keys.

Encryption Algorithm	It can be used during phase 2 negotiations. And allows user to
	select different algorithms from the dropdown list.
Authentication Algorithm	It is used for authentication in phase 2. It allows user to select
	anyone of the algorithms from the dropdown list.

# Advanced

Create IPSec VPN Rule								
IPSec Advanced								
on 🛩								
off 🔛								
20 in seconds								
30 in seconds								
	CANCEL							
	IPSec Advanced							

# Figure 54: Advanced

Enable compression	User can used deflate alg to compress traffic.
Nat Traversal	If the gate is noted then this option has to be on or force else select
	no.
Enable Dead Peer	User can enable keep alive signals for the connection.
Detection	
DPD Delay	It allows keep alive signals that are sent for this connection.
DPD Max fail	It specifies Max number of second keep alive signals that are sent
	for connection.

# 8. Status

# 8.1 Profile Status

Navigate through Status > Profile Status

Profile Status shows the configured SIP trunks, roaming users, least counting routing, along with the corresponding LAN profile, WAN profile and Media profile IP addresses and port numbers.

And also it shows the Log viewer settings, which allows user to refresh the page and edit the refresh time interval.

Dashboard	Profile Status 🙆					
Network	Log Viewer Settings		(1)			
System						
🖡 Media	300 Update Refre	sh Interval Refresh				
Signalling			_			
Security	SIP Trunk	Roaming User	LCR	LAN Profile	WAN Profile	Media Profile
• Status	Trunk1:192.168.10.100:5060	*	-	Lantrunk1:192.168.5.35:6060	wantrunk1:192.168.10.231:9010	genmed:10.0.0.2:45000-55000
Profile Status	Trunk2:192.168.10.100:5060	2	8	Lantrunk2:192.168.5.35:6030	Wantrunk2:192.168.10.231:8030	genmed:10.0.0.2:45000-55000
Trunk Status	Babytel:198.38.7.11:5060	-	8	Lanbabytel:192.168.5.35:6050	Wanbabytel:192.168.10.231:8050	genmed:10.0.0.2:45000-55000
Roaming User Status	Nano1:192.168.10.132:5060	-	-	Lannano:192.168.5.35:6080	Wannano:192.168.10.231:6090	genmed:10.0.0.2:45000-55000
Active Calls	Nano2:192.168.0.42:5060	2	2	Lannano2:192.168.5.35:7080	Wannano2:192.168.10.231:7090	genmed:10.0.0.2:45000-55000
Logs Reports	-	Roam1:192.168.5.61:5060	-	Lanroam1:192.168.5.35:6010	WanRoam1:192.168.10.231:8020	genmed:10.0.0.2:45000-55000
Tools	-		Least1	Lanler:192.168.5.35:7030		-

## Figure 55: Profile Status

# 8.2 Trunk Status

## Navigate through Status > Trunk Status

Trunk Status shows the current status of the configured trunks in the Blox Esbc. It contains user name, domain, registrar etc. And also it shows the Log viewer settings which allows user to refresh the page and edit the refresh time interval.

Network	Log Viewer Settings											
System												
Media		Update	Refresh Inter	val Refr	esh							
Signalling	_				-							
Security	State -	Username 🗧	Domain ±	Registrar 🗧	AOR \$	Last Reg Sent #	Reg Timeout :	User Agent :	Contact :	Recv =	Expd ¢	Socket a
Status 🔉	REGISTRAR	_ 6200		sip:192.16	sip:6200@1	Wed Feb 25	Wed Feb 25	FPBX-2.8.1	sip:6200@1	sip:192.16	2015-02-25	udp:192.1
Profile Status	REGISTERED	9999		sip:192.16	sip:9999@1	Wed Feb 25	Wed Feb 25	FPBX-2.8.1	sip:9999@1	sip:192.16	2015-02-25	udp:192.1
Trunk Status Roaming User Status	REGISTERED	4444		sip:192.16	sip:4444@1	Wed Feb 25	Wed Feb 25	FPBX-2.8.1	sip:4444@1	sip:192.16	2015-02-25	udp:192.1
Active Calls	REGISTERED	)		sip:192.16	sip:7300@1	VVed Feb 25	Wed Feb 25					
∟ogs	REGISTERED	)		sip:198.38	sip:160462	Wed Feb 25	Wed Feb 25					
Reports		1604628524						FPBX-2.8.1	sip:160462	sip:192.16	2015-02-25	udp:192.1

#### Figure 56: Trunk Status

# 8.3 Roaming User Status

#### Navigate through Status > Roaming User Status

It displays the current status of roaming users configured in Blox Esbc. It contains user name, domain, registrar etc. And also it shows the Log viewer settings which allows user to refresh the page and edit the refresh time interval.

Network System	Log Viewer Se	ttings	-	- 10					
Media	300	Update Re	fresh Interval Refresh	1					
Signalling Security	Username +	Domain +	User Agent ‡	Contact +	Received •	Expires \$	Last Modified #	Socket #	Attr =
Status 🔉	1010		Yealink SIP-T22P 7.72.0.30	sip:1010@192.168.10.69:5064	sip:192.16	2015-02-25	2015-02-25	udp:192.16	udp:192.16
rofile Status runk Status	1004		Yealink SIP-T22P 7.72.0.75	sip:1004@192.168.10.52:5062	sip:192.16	2015-02-25	2015-02-25	udp:192.16	udp:192.16
aming User Status tive Calls									
gs ports									

#### Figure 57: Roaming User Status

# 8.4 Active calls

## Navigate through Status > Active calls

It displays status of the live calls along with Dialing ID, Call ID, From URI, Caller contact, To URI, Callee Contact, start time, timeout and profiles etc.

And also it shows the Log viewer settings, which allows user to Update, refresh interval and refresh the page.

Network	Log Viewer Sett	ings 🕕			
System					
Media	300	Update Refresh Interval Refresh			
Signalling					
- orginaling					
Security	Dialling ID -	Call ID #	From URI \$	Caller Contact #	prosta a sec
Security Status Profile Status Trunk Status		Call ID € 32 6f3e5862140a4b8025a665a413dd06ff@192.16			Caller Sock
Security     Status     Profile Status Trunk Status Roaming User Status Active Calls					
Security     Status     Status     Profile Status     Trunk Status     Roaming User Status     Active Calls     Logs     Reports					

Figure 58: Active Calls

# 8.5 Logs

# 8.5.1 Signaling Logs

Navigate through Status> Logs> Signaling Logs

Signaling logs demonstrates complete logs of the SIP request methods received by the Blox Esbc. The Log viewer settings allows user to update refresh interval and Refresh the Log viewer settings.



#### Figure 59: Signaling Logs

# 8.5.2 Media Logs

#### Navigate through Status> Logs> Media Logs

It shows the log messages about the media which are sending and received by the Blox Esbc. The Log viewer settings allows user to update refresh interval and Refresh the Log viewer settings.

Network	Log Viewer Setting:	s (1)	
System	300 1	a deservation and the second	
Media	300	Update Refresh Interval Refresh	
Signalling Security	Date -	Log Msg +	
Status )	Feb 24 23:42:11	NAT-PMP Transcoding enabled without Transcoding DSP Address::	A
rofile Status	Feb 24 23:42:11	NAT-PMP Transcoding enabled without Transcoding DSP Address::	
runk Status oaming User Statu	Feb 24 23:42:11 Feb 24 23:42:11	NAT-PMP Transcoding enabled without Transcoding DSP Address::	
ctive Calls ogs	Feb 24 23:42.11 Feb 24 23:41:47	NAT-PMP Transcoding enabled without Transcoding DSP Address:: NAT-PMP Transcoding enabled without Transcoding DSP Address::	
Signalling Logs Media Logs	Feb 24 23:41:47	NAT-PMP Transcoding enabled without Transcoding DSP Address:	
LCR Logs	Feb 24 23:41:29	NAT-PMP Transcoding enabled without Transcoding DSP Address::	
System Logs Security Logs eports Tools	Feb 24 23:41:29	NAT-PMP Transcoding enabled without Transcoding DSP Address:	×

#### Figure 60: Media Logs

#### 8.5.3 LCR Logs

Navigate through Status> Logs> LCR Logs

It displays call logs which are made through Least Cost Routing. The Log viewer settings allows user to update refresh interval and Refresh the Log viewer settings.

<ul> <li>Network</li> <li>System</li> </ul>	Log Viewer Settings							
Media	300 L	pdate Refresh Interval Refresh						
Signalling Security	Date -	Log Msg ÷						
Status 🔉	Feb 25 01:47:16	Received 192.168.5.35.7080 Got REGISTER sip:7300@192.168.5.35 7080/sip	^					
rofile Status	Feb 25 01:47:16	REGISTER Unprocessed, Dropping SIP Method REGISTER received from sip.7300@192.168.5.35/7080 192.168.5.61 5060 to sip 192.168.5.35						
runk Status oaming User Status	Feb 25 01:47:13	Received 192.168.10.231:9010 Got OPTIONS sip:Unknown@192.168.10.100/sip 9999@192.168.10.231						
ctive Calls	Feb 25 01:47:13	Received 192.168.10.231:8030 Got OPTIONS sip:Unknown@192.168.10.100/sip 4444@192.168.10.231						
.ogs	Feb 25 01:47:12	Received 192.168.5.35:7080 Got REGISTER sip:7300@192.168.5.35 7080/sip						
Signalling Logs	Feb 25 01:47:12	REGISTER Unprocessed, Dropping SIP Method REGISTER received from sip.7300@192.168.5.35:7080 192.168.5.61 5060 to sip 192.168.5.35						
Media Logs LCR Logs	Feb 25 01:47:08	Received 192.168.5.35:7080 Got REGISTER sip:7300@192.168.5.35 7080/sip						
System Logs Security Logs Reports	Feb 25 01:47:08	REGISTER Unprocessed, Dropping SIP Method REGISTER received from sip:7300@192.168.5.35:7080 192.168.5.61 5060 to sip 192.168.5.35	~					

#### Figure 61: LCR Logs

#### 8.5.4 System Logs

Navigate through Status > Logs > System logs

System log shows all the log messages of Blox Esbc. The Log viewer settings allows user to update refresh interval and Refresh the Log viewer settings.

<ul> <li>Network</li> <li>System</li> </ul>	Log Viewer Settings		
Media	300 L	Jpdate Refresh Interval Refresh	
Signalling Security	Time +	Message +	1
Status 🔉	Feb 25 01:47:48	allosbc-0-9-0-beta(27793); Received 192.168.5.35:7080 Got REGISTER sip:7300@192.168.5.35 7080/sip	
Profile Status Frunk Status	Feb 25 01:47:48	allosbc-0-9-0-keta[27793]; REGISTER Unprocessed, Dropping SIP Method REGISTER received from sip:7300@192.168.5.35;7080 192.168.5.61 5060 to sip 192.168.5.35	
Roaming User Status	Feb 25 01:47:44	allosbc-0-9-0-beta[27795]: Received 192.168.5.35:7080 Got REGISTER sip:7300@192.168.5.35 7080/sip	
Active Calls .ogs	Feb 25 01:47:44	allosbc-0-9-0-beta[27795]: REGISTER Unprocessed, Dropping SIP Method REGISTER received from sip:7300@192.168.5.35 5060 to sip 192.168.5.35	
<ul> <li>Signalling Logs</li> <li>Media Logs</li> </ul>	Feb 25 01:47:40	allosbc-0-9-0-beta[27794]; Received 192:168:5:35:7080 Got REGISTER sip:7300@192:168:5:35 7080/sip	
<ul> <li>LCR Logs</li> <li>System Logs</li> </ul>	Feb 25 01:47:40	allosbc-0-9-0-beta[27794]; REGISTER Unprocessed, Dropping SIP Method REGISTER received from sip:7300@192.168.5.35,7080 192.168.5.61 5060 to sip 192.168.5.35	~
<ul> <li>Security Logs</li> <li>Reports</li> <li>Tools</li> </ul>			

#### Figure 62: System Logs

#### 8.5.5 Security Logs

Navigate through Status > Logs > Security logs

A security log provides a track security related information in Blox Esbc with Signature ID, Signature category and name. It also shows the Time stamp information, Source IP & Port, Destination IP & Port and type of protocol whether it is TCP or UDP.

The Log viewer settings allows user to update refresh interval and Refresh the Log viewer settings.

<ul> <li>Network</li> <li>System</li> <li>Media</li> </ul>	Log Viewer Se		lefresh Interv	val Refr	0 esh									
Signalling Security	Time +	ID ÷	Category	¢ Category	Name 🕈 Mes	sage 🕈	Src IP	÷	Src Port *	Dst IF	¢ ¢	Dst Port 4	Proto	col
Status > Profile Status Trunk Status Roaming User	12/04-16:23:55	5 70110001	7011	SIP Extensions Discovery	"Sig: SIP Extensions Identificatior Attempt"	192.168	1.5.61	5060	192.168.5	5.35	6060	UDP	Blacklist	
ctive Calls ogs Signalling Logs	12/04-16:23:55	5 70110001	7011	SIP Extensions Discovery	"Sig: SIP Extensions Identification Attempt"	192.168	1.5.61	5060	192.168.5	5.35	6030	UDP	Blacklist	
Media Logs LCR Logs System Logs Security Logs	12/04-16:23:51	70110001	7011	SIP Extensions	"Sig: SIP Extensions Identification	, 192.168	1.5.61	5060	192.168.5	5.35	6060	UDP	Blacklist	*

Figure 63: Security Logs

# 9. Reports

# 9.1 CDR Reports

Navigate through Status > Reports > CDR Reports

Call Detailed Reports (CDR) displays detailed information about the calls through Blox Esbc.

Dashboard	CDR	Reports 🕜										
Network	Log	viewer Settings			0							
System	-	and the set of the second of										
🕨 Media		300 Update R	efresh Interv	al Refre	sh							
Signalling	_							_				_
Security	10 ÷	Time #	Metho	od # Source	e 🛎 🤇 Cha	nnel ‡ Desti	nation 🗧	Dest Channel 👙	SIP Code #	SIP Reason	•	Duration +
Status 🔥	1587	23:42:11 2015-02-24	INVITE	sip:100@19	sip:192.16	sip:7300@1		487	Request Te	0	0	^
Profile Status	1586	23:41:29 2015-02-24	INVITE	sip:100@19	sip:192.16	sip:7300@1		487	Request Te	0	0	
Frunk Status	1585	23:32:30 2015-02-24	INVITE	sip:100@19	sip:192.16	sip:7300@1		487	Request Te	0	0	
Roaming User Status Active Calls	1584	23:16:55 2015-02-24	INVITE	sip:7300@1	sip:192.16	sip:100@19	sip:7300@	200	OK.	1	8	
Logs	1582	23:15:20 2015-02-24	INVITE	sip:7300@1	sip:192.16	sip:100@19	sip:7300@	200	OK	1	8	
Reports	1580	23:13:15 2015-02-24	INVITE	sip:7300@1	sip:192.16	sip:100@19	sip:7300@	200	OK.	1	23	
CDR Reports	1578	23:12:10 2015-02-24	INVITE	sip:7300@1	sip:192.16	sip:100@19	sip:7300@	1 200	OK.	1	8	
Tools	1576	23:02:56 2015-02-24	INVITE	sip:7300@1	sip:192.16	sip:100@19	sip:7300(a	200	OK	1	9	~

Figure 64: CDR Reports

# 10. Tools

# **10.1 Administration**

#### Navigate through Tools > Administration

User can do factory reset by clicking on Factory Reset button.

They restart Blox Esbc services by clicking on Restart STM Services button.

User can reboot device by clicking on Reboot button.

User can shutdown device by clicking on Shutdown button.

User can take back up of the configuration by clicking on Config Back-Up button.

Restoring the configuration can be done by selecting the configuration file from the system and clicking on the Config Restore button which reboots the machine on success.

Dashboard	Administration 🕜
Network	
System	Factory Reset
🖡 Media	(g) Restart STM Services
Signalling	
Security	(1) Reboot
<ul> <li>Status</li> </ul>	(1) Shutdown
• Tools >	
Administration	Config Back-up
Diagnostics	Select configuration file : Browse No file selected. Config Restore (Requires Reboot)
Troubleshooting	
Logs Archive	

Figure 65: Administration

# **10.2** Diagnostics

Navigate through Tools > Diagnostics > Run Diagnostics

# 10.2.1 Run Diagnostics

User can run diagnostics by clicking on Run Diagnostics button and result can be seen in the text region.

Diagnostics report can be downloaded by clicking on the Get Report button



#### Figure 66: Diagnostics

#### 10.2.2 Ping

Navigate through Tools > Diagnostics > Ping

User can ping a host by entering values for host IP / Domain Name and selecting the count from the list.

Ping button will send a ping request to the host and Reset button clears the entered values.

Ping result is shown in the text area which appears below the ping and reset buttons.



Figure 67: Ping Result

#### 10.2.3 Trace route

Navigate through Tools > Diagnostics > Traceroute

User can trace route a host by entering values for host IP / Domain Name, hop count and enabling the ICMP by clicking ICMP checkbox.

Traceroute button will send a trace route request to the host and Reset button clears the entered values.

Traceroute result is shown in the text area which appears below the ping and reset buttons.

Dashboard	Traceroute 🕝
Network	Host 192 168 10 231
System	
Media	Hop Count 3
Signalling	ICMP
Security	Traceroute Reset
Status	
Tools >	traceroute to 192.168.10.231 (192.168.10.231), 3 hops max, 60 byte packets 1 192.168.10.231 (192.168.10.231) 0.036 ms 0.007 ms 0.007 ms
dministration	
iagnostics	
Run Diagnostics	
Ping	
Traceroute	
roubleshooting	
logs Archive	

Figure 68: Trace Route Result

# **10.3 Trouble shooting**

## Navigate through Tools > Trouble Shooting

By Clicking on Enable DPI or Disable DPI button which enables or disables DPI.



**Figure 69: Trouble Shooting** 

# **10.4 Logs Archive**

#### Navigate through **Tools** > **Logs Archive**

After the device storage has reached its limit, logs are stored in USB storage device if one is connected. Logs archive summary is listed in the text area.





# Thank You