



# Cyberoam User Guide

**Version 10**

Document version 1.0 – 10.6.6.042 - 24/11/2017

## Important Notice

Cyberoam Technologies Pvt. Ltd. has supplied this Information believing it to be accurate and reliable at the time of printing, but is presented without warranty of any kind, expressed or implied. Users must take full responsibility for their application of any products. Cyberoam Technologies Pvt. Ltd. assumes no responsibility for any errors that may appear in this document. Cyberoam Technologies Pvt. Ltd. reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

## USER'S LICENSE

Use of this product and document is subject to acceptance of the terms and conditions of Cyberoam End User License Agreement (EULA) and Warranty Policy for Cyberoam UTM Appliances.

You will find the copy of the EULA at <http://www.cyberoam.com/documents/EULA.html> and the Warranty Policy for Cyberoam UTM Appliances at <http://kb.cyberoam.com>.

## RESTRICTED RIGHTS

Copyright 1999 - 2015 Cyberoam Technologies Pvt. Ltd. All rights reserved. Cyberoam, Cyberoam logo are trademark of Cyberoam Technologies Pvt. Ltd.

## Corporate Headquarters

Cyberoam House,  
Saigulshan Complex, Opp. Sanskruti,  
Beside White House, Panchwati Cross Road,  
Ahmedabad - 380006, GUJARAT, INDIA.  
Tel: +91-79-66216666  
Fax: +91-79-26407640 Website: [www.cyberoam.com](http://www.cyberoam.com)

## Content

<b>Preface</b> .....	<b>6</b>
<b>Introduction</b> .....	<b>10</b>
Administrative Interfaces .....	11
Web Admin Console .....	11
Command Line Interface (CLI) Console .....	11
Cyberoam Central Console (CCC) .....	12
Web Admin Console .....	13
Web Admin Language .....	13
Supported Browsers .....	14
Login procedure .....	15
Log out procedure .....	16
Menus and Pages.....	17
Page .....	19
Icon bar .....	20
List Navigation Controls .....	21
Tool Tips .....	21
Status Bar .....	21
Common Operations.....	22
<b>Getting Started</b> .....	<b>24</b>
Dashboard .....	26
Alert Messages Doclet .....	26
Appliance Information Doclet .....	27
System Usage Doclet .....	27
System Status Doclet .....	28
Recent Web Viruses Detected Doclet .....	28
Recent Mail Viruses Detected Doclet .....	29
Gateway Status Doclet .....	29
Recent Malware Alerts Doclet .....	30
License Information Doclet .....	31
Recent FTP Viruses Detected Doclet.....	31
Recent IPS Alerts Doclet .....	31
Today Usage Summary Doclet .....	32
DoS Attack Status Doclet.....	32
Web Traffic Analysis Doclet .....	33
HA Details Doclet .....	33
<b>System</b> .....	<b>35</b>
Administration .....	35
Settings .....	36
Appliance Access .....	40
Administrator Profiles.....	42
Profile Parameters .....	43
Access Denied Page .....	44
Password .....	45
Central Management .....	46
API.....	49
Configuration .....	51
Time .....	51
Notification .....	53
Messages.....	57
Configuring Web Proxy Settings .....	66
Enabling and Configuring Parent Proxy.....	67
Configuring Captive portal .....	68
Theme.....	72
Maintenance .....	73
Backup & Restore.....	73

Firmware .....	76
Licensing .....	78
Services .....	81
Updates.....	83
Import Export.....	85
<b>SNMP .....</b>	<b>87</b>
SNMP terms.....	87
Agent Configuration.....	88
Community.....	89
V3 User.....	91
<b>Certificate .....</b>	<b>92</b>
Certificate.....	93
Certificate Authority .....	99
Certificate Authority Parameters .....	101
Certificate Revocation List (CRL).....	104
Adding a new CRL.....	105
<b>Diagnostics .....</b>	<b>106</b>
Tools .....	106
System Graph .....	110
Packet Capture.....	118
Connection List.....	125
Consolidated Troubleshoot Report (CTR) .....	128
<b>Objects.....</b>	<b>129</b>
Hosts .....	130
IP Host .....	130
IP Host Group.....	134
MAC Host.....	136
FQDN Host.....	138
FQDN Host Group .....	140
Country Host .....	142
Country Host Group.....	145
Services.....	147
Services .....	147
Service Group .....	150
Schedule.....	152
Schedule.....	152
File Type.....	154
<b>Network.....</b>	<b>156</b>
Interface.....	156
Interface .....	157
VLAN .....	169
Link Aggregation Group.....	175
IP Tunnel.....	179
Zone.....	182
Wireless WAN.....	186
Status.....	187
Settings.....	188
Gateway .....	193
Gateway.....	194
Static Route .....	204
Unicast.....	204
Multicast.....	206
Source Route .....	209
Dynamic Route .....	211
RIP.....	212
OSPF .....	217
BGP .....	224
PIM-SM.....	226
Routing Information .....	227
DNS.....	240



DNS Host Entry .....	243
Address Assignment for IPv6 Devices .....	245
Router Advertisement .....	246
DHCP .....	251
DHCP Server .....	252
DHCP Lease .....	257
DHCP Relay .....	258
ARP-NDP .....	260
Neighbors .....	261
Dynamic DNS .....	266
<b>Identity .....</b>	<b>269</b>
Authentication .....	270
Authentication Server .....	271
Configuring External Authentication Server .....	273
1. Configuring Active Directory Server Settings .....	273
2. Configure LDAP Authentication Settings .....	285
3. Configure RADIUS Server Settings .....	289
4. Configure TACACS+ Server Settings .....	292
Firewall .....	294
Configuring Authentication for VPN Traffic .....	300
Configuring Authentication for Admin Traffic .....	302
User Groups .....	303
Users .....	310
Users .....	311
Clientless Users .....	321
Guest Users .....	327
General Settings .....	327
Manage Guest Users .....	331
SMS Gateway .....	342
Policy .....	346
Access Time Policy .....	347
Surfing Quota Policy .....	350
Data Transfer Policy .....	353
Live Users .....	357
Live Users .....	357
<b>Firewall .....</b>	<b>365</b>
IPv6 .....	366
IPv6 Features supported in CyberoamOS .....	366
Default Firewall Rules .....	368
Rule .....	370
IPv4 Firewall Rule .....	370
Manage Firewall Rule List .....	373
IPv4 Firewall Rule Parameters .....	376
IPv6 Firewall Rules .....	387
Manage Firewall Rule List .....	389
IPv6 Firewall Rule Parameters .....	392
Virtual Host .....	400
NAT Policy .....	409
Spoof Prevention .....	411
Configuring Spoof Prevention Settings .....	411
Trusted MAC .....	413
DoS .....	416
Settings .....	418
Bypass Rules .....	421
<b>Web Filter .....</b>	<b>424</b>
Settings .....	424
Web Category .....	427
Search URL .....	431
URL Group .....	432

---

Web Filter Policy .....	434
ICAP .....	440
Server .....	440
Policy .....	441
<b>Application Filter.....</b>	<b>444</b>
Application List.....	444
Application Filter Category .....	446
Application Filter Policy .....	448
<b>IM.....</b>	<b>454</b>
IM Contact .....	454
IM Contact Group .....	456
IM Rules .....	458
Login .....	459
Conversation .....	461
File Transfer .....	464
Webcam.....	466
Content Filter .....	467
<b>QoS .....</b>	<b>469</b>
Settings.....	470
QoS Policy.....	472
<b>Logs &amp; Reports.....</b>	<b>479</b>
Configuration .....	480
Syslog Servers .....	481
Log Settings .....	484
Netflow .....	487
Log Viewer.....	488
4-Eye Authentication .....	495
Settings.....	496
De-Anonymize.....	497

# Preface

Welcome to Cyberoam's - User Guide.

Cyberoam Unified Threat Management Appliances offer identity-based comprehensive security to organizations against blended threats - worms, viruses, malware, data loss, identity theft; threats over applications viz. Instant Messengers; threats over secure protocols viz. HTTPS; and more. They also offer wireless security (WLAN) and 3G wireless broadband and analog modem support can be used as either Active or Backup WAN connection for business continuity.

Cyberoam integrates features like stateful inspection firewall, VPN, Gateway Anti-Virus and Anti-Spyware, Gateway Anti-Spam, Intrusion Prevention System, Content & Application Filtering, Data Leakage Prevention, IM Management and Control, Layer 7 visibility, Bandwidth Management, Multiple Link Management, Comprehensive Reporting over a single platform.

Cyberoam has enhanced security by adding an 8th layer (User Identity) to the protocol stack. Advanced inspection provides L8 user-identity and L7 application detail in classifying traffic, enabling Administrators to apply access and bandwidth policies far beyond the controls that traditional UTMs support. It thus offers security to organizations across layer 2 - layer 8, without compromising productivity and connectivity.

Cyberoam UTM Appliances accelerate unified security by enabling single-point control of all its security features through a Web 2.0-based GUI. An extensible architecture and an 'IPv6 Ready' Gold logo provide Cyberoam the readiness to deliver on future security requirements.

Cyberoam provides increased LAN security by providing separate port for connecting to the publicly accessible servers like Web server, Mail server, FTP server etc. hosted in DMZ which are visible the external world and still have firewall protection.

**Note**

- Default Web Admin Console username is 'admin' and password is 'admin'
- Cyberoam recommends that you change the default password immediately after installation to avoid unauthorized access.

# About this Guide

This Guide provides information regarding the administration, maintenance, and customization of Cyberoam and helps you manage and customize Cyberoam to meet your organization's various requirements including creating groups and users and assigning policies to control web as well as application access.

## Guide Organization

The Cyberoam User Guide organization is structured into the thirteen parts that follow the Cyberoam Web Admin Console structure. Within these parts, individual topics correspond to security Appliance management interface layout.

This Guide is organized into thirteen parts:

### Part I – Introduction

This part covers various features of Web 2.0 based graphical interface.

### Part II – Getting started

This part covers how to start using Cyberoam after deployment.

### Part III Basics

This part covers basic building blocks in Cyberoam.

### Part IV System

This part covers a various security Appliance controls for managing system status information, registering and managing the Cyberoam security Appliance and its subscription licenses through registration portal, managing firmware versions, defining profiles for role based access, scheduling backups and restoring, various and using included diagnostics tools for troubleshooting.

### Part V Objects

This part covers various Objects which are the logical building blocks for configuring various policies and rules, which include:

- host – IP, network and MAC Addresses. They are used in defining firewall rules, virtual host, NAT policy, IPSec, L2TP and VPN policies
- services which represent specific protocol and port combination for example, DNS service for TCP protocol on 53 port. Access to services are allowed or denied through firewall rules.
- schedule to control when the firewall rule, Access time policy, Web filter policy, Application filter policy, or QoS policy will be in effect for example, All Days, Work Hours
- file types – defining web filter policy, SMTP scanning rules
- certificates – VPN policies

**Part VI Network**

This part covers configuring the Cyberoam Appliance for your network. It includes configuring Cyberoam interfaces and DNS settings, adding VLAN sub interfaces and custom zones, configuring DHCP. It also covers configuration of the 3G wireless WAN interface on the Cyberoam Appliances that support the feature.

**Part VII Identity**

This part covers how to configure user level authentication and manage users and user groups.

**Part VIII Firewall**

This part covers tools for managing how the Cyberoam Appliance handles traffic through the firewall.

**Part IX Web Filter**

This part covers how to configure and manage Web filtering in Cyberoam through categories and policies.

**Part X Application Filter**

This part covers how to configure and manage application filtering in Cyberoam through categories and policies.

**Part XI IM**

This part covers how to configure and manage restrictions on instant messaging services provided by the Yahoo and MSN messengers.

**Part XII QoS**

This part covers how to configure and manage bandwidth through QoS policy that allocates and limits the maximum bandwidth usage of the user and controls web and network traffic.

**Part XIII Logs & Reports**

This part covers managing logging and reporting feature. Cyberoam provides extensive logging capabilities for traffic, system and network protection functions. Detailed log information and reports provide historical as well as current analysis of network activity to help identify security issues and reduce network abuse.

## Technical Support

You may direct all questions, comments, or requests concerning the software you purchased, your registration status, or similar issues to Customer care/service department at the following address:

Corporate Office  
Cyberoam House,  
Saigulshan Complex, Opp. Sanskruti,  
Beside White House, Panchwati Cross Road,  
Ahmedabad - 380006, GUJARAT, INDIA.  
Tel: +91-79-66216666  
Fax: +91-79-26407640: [www.cyberoam.com](http://www.cyberoam.com)

Cyberoam contact:

Technical support (Corporate Office): +91-79-66065777

Email: [support@cyberoam.com](mailto:support@cyberoam.com)

Web site: [www.cyberoam.com](http://www.cyberoam.com)

Visit [www.cyberoam.com](http://www.cyberoam.com) for the regional and latest contact information.

# Introduction

The Appliances use Layer 8 technology to help organizations maintain a state of readiness against today's blended threats and offer real-time protection.

Unified Threat Management Appliances offer identity-based comprehensive security to organizations against blended threats - worms, viruses, malware, data loss, identity theft; threats over applications viz. Instant Messengers; threats over secure protocols viz. HTTPS; and more. They also offer wireless security (WLAN) and 3G wireless broadband. Analog modem support can be used as either Active or Backup WAN connection for business continuity.

The Appliance integrates features like stateful inspection firewall, VPN, Gateway Anti-Virus and Anti-Spyware, Gateway Anti-Spam, Intrusion Prevention System, Content & Application Filtering, Data Leakage Prevention, IM Management and Control, Layer 7 visibility, Web Application Firewall, Bandwidth Management, Multiple Link Management and Comprehensive Reporting over a single platform.

The Appliance has enhanced security by adding an 8th layer (User Identity) to the protocol stack. Advanced inspection provides L8 user-identity and L7 application detail in classifying traffic, enabling Administrators to apply access and bandwidth policies far beyond the controls that traditional UTMs support. It thus offers security to organizations across layer 2 - layer 8, without compromising productivity and connectivity.

The Appliance accelerates unified security by enabling single-point control of all its security features through a Web 2.0-based GUI. An extensible architecture and an 'IPv6 Ready' Gold logo provide Appliance the readiness to deliver on future security requirements.

The Appliances provides increased LAN security by providing separate port for connecting to the publicly accessible servers like Web server, Mail server, FTP server etc. hosted in DMZ which are visible the external world and still have firewall protection.

## Layer 8 Security:

The Appliance's features are built around its patent pending Layer 8 technology. The Layer 8 technology implements the human layer of networking by allowing organizations control traffic based on users instead of mere IP Addresses. Layer 8 technology keeps organizations a step ahead of conventional security solutions by providing full business flexibility and security in any environment including WI-FI and DHCP.

### Note

- All the screen shots in the Cyberoam User Guides are taken from NG series of Appliances. The feature and functionalities however remains unchanged across all Cyberoam Appliances.

## Administrative Interfaces

Appliance can be accessed and administered through:

- Web Admin Console
- Command Line Interface Console
- Cyberoam Central Console

**Administrative Access** An administrator can connect and access the Appliance through HTTP, HTTPS, telnet, or SSH services. Depending on the Administrator login account profile used for access, an administrator can access number of Administrative Interfaces and Web Admin Console configuration pages.

Appliance is shipped with two administrator accounts and four administrator profiles.

Administrator Type	Login Credentials	Console Access	Privileges
Super Administrator	admin/admin	Web Admin Console CLI console	Full privileges for both the consoles. It provides read-write permission for all the configuration performed through either of the consoles.
Default	cyberoam/cyber	Web Admin console only	Full privileges. It provides read-write permission for all the configuration pages of Web Admin console.

### Note

- We recommend that you change the password of both the users immediately on deployment.

## Web Admin Console

Web Admin Console is a web-based application that an Administrator can use to configure, monitor, and manage the Appliance.

You can connect to and access Web Admin Console of the Appliance using HTTP or a HTTPS connection from any management computer using web browser:

- HTTP login: `http://<LAN IP Address of the Appliance>`
- HTTPS login: `https://<LAN IP Address of the Appliance>`

For more details, refer section [Web Admin Console](#).

## Command Line Interface (CLI) Console

Appliance CLI console provides a collection of tools to administer, monitor and control certain Appliance component. The Appliance can be accessed remotely using the following connections:

- Remote login Utility – TELNET login



To access Appliance from command prompt using remote login utility – Telnet, use command **TELNET <LAN IP Address of the Appliance>**. Use default “admin”.

#### SSH Client (Serial Console)

SSH client securely connects to the Appliance and performs command-line operations. CLI console of the Appliance can be accessed via any of the SSH client using LAN IP Address of the Appliance and providing Administrator credentials for authentication.

#### Note

**Start SSH client and create new Connection with the following parameters:**

**Host – <LAN IP Address of the Appliance>**

**Username – admin**

**Password – admin**

Use CLI console for troubleshooting and diagnose network problems in details. For more details, refer version specific Console Guide available on <http://docs.cyberoam.com/>.

## Cyberoam Central Console (CCC)

Distributed Cyberoam Appliances can be centrally managed using a single Cyberoam Central Console (CCC) Appliance, enabling high levels of security for Managed Security Service Provider (MSSPs) and large enterprises. To monitor and manage Cyberoam using CCC Appliance you must:

Configure CCC Appliance in Cyberoam

Integrate Cyberoam Appliance with CCC using: Auto Discovery or Manually

Once you have added the Appliances and organized them into groups, you can configure single Appliance or groups of Appliances.

For more information, please refer CCC Administrator Guide.

## Web Admin Console

CyberoamOS uses a Web 2.0 based easy-to-use graphical interface termed as Web Admin Console to configure and manage the Appliance.

You can access the Appliance for HTTP and HTTPS web browser-based administration from any of the interfaces. Appliance when connected and powered up for the first time, it will have a following default Web Admin Console Access configuration for HTTP and HTTPS services.

Services	Interface/Zones	Default Port
HTTP	LAN, WAN	TCP Port 80
HTTPS	WAN	TCP Port 443

The administrator can update the default ports for HTTP and HTTPS services from **System > Administration > Settings**.

## Web Admin Language

The Web Admin Console supports multiple languages, but by default appears in English. To cater to its non-English customers, apart from English, Chinese-Simplified, Chinese-Traditional, Hindi, Japanese and French languages are also supported. Administrator can choose the preferred GUI language at the time of logging on.

Listed elements of Web Admin Console will be displayed in the configured language:

- Dashboard Doclet contents
- Navigation menu
- Screen elements including field & button labels and tips
- Error messages

## Supported Browsers

You can connect to the Web Admin Console of the Appliance using HTTP or a secure HTTPS connection from any management computer using one of the following web browsers:

Browser	Supported Version
Microsoft Internet Explorer	Version 8+
Mozilla Firefox	Version 3+
Google Chrome	All versions
Safari	5.1.2(7534.52.7)+
Opera	15.0.1147.141+

The minimum screen resolution for the management computer is 1024 X 768 and 32-bit true xx-color.

The Administrator can also specify the description for firewall rule, various policies, services and various custom categories in any of the supported languages.

All the configuration done using Web Admin Console takes effect immediately. To assist you in configuring the Appliance, the Appliance includes a detailed context-sensitive online help.

## Login procedure

The log on procedure authenticates the user and creates a session with the Appliance until the user logs-off.

To get to the login window, open the browser and type the LAN IP Address of Cyberoam in the browser's URL box. A dialog box appears prompting you to enter username and password.

Screen – Login Screen


Screen Element	Description
<b>Username</b>	Enter user login name.  If you are logging on for the first time after installation, use the default username.
<b>Password</b>	Specify user account password.  Dots are the placeholders in the password field.  If you are logging on for the first time after installation with the default username, use the default password.
<b>Language</b>	Select the language. The available options are Chinese-Simplified, Chinese-Traditional, English, French, and Hindi.  Default – English
<b>Log on to</b>	To administer Cyberoam, select 'Web Admin Console'  To view logs and reports, select "Reports".  To login into your account, select "My Account".
<b>Login button</b>	Click to log on the Web Admin Console.

Screen – Login screen elements

The Dashboard appears as soon as you log on to the Web Admin Console. It provides a quick and fast overview of all the important parameters of your Appliance.

## Log out procedure

To avoid un-authorized users from accessing Cyberoam, log off after you have finished working. This will end the session and exit from Cyberoam.

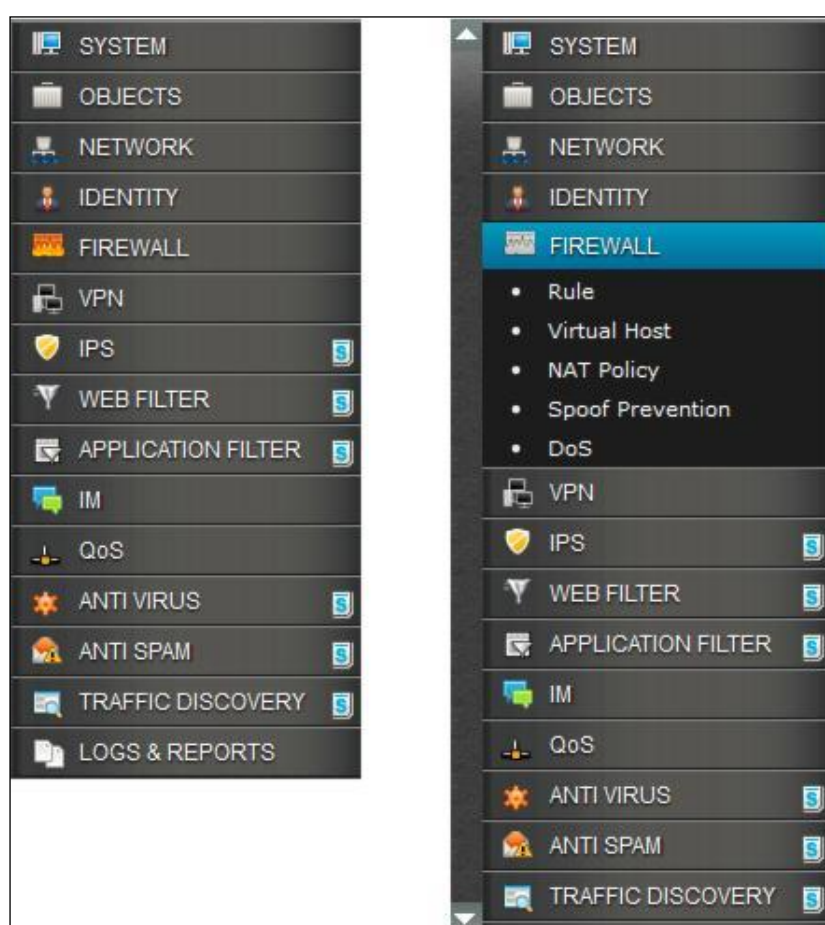
To log off from the Appliance, click the  button located at the top right of any of the Web Admin Console pages.

## Menus and Pages

The Navigation bar on the leftmost side provides access to various configuration pages. This menu consists of sub-menus and tabs. On clicking the menu item in the navigation bar, related management functions are displayed as submenu items in the navigation bar itself. On clicking submenu item, all the associated tabs are displayed as the horizontal menu bar on the top of the page. To view a page associated with the tab, click the required tab.

The left navigation bar expands and contracts dynamically when clicked on without navigating to a submenu. When you click on a top-level heading in the left navigation bar, it automatically expands that heading and contracts the heading for the page you are currently on, but it does not navigate away from the current page. To navigate to a new page, first click on the heading, and then click on the submenu you want navigate to.

On hovering the cursor upon the up-scroll icon ▲ or the down-scroll icon ▼, automatically scrolls the navigation bar up or down respectively.



The navigation menu includes following modules:

- System – System administration and configuration, firmware maintenance, backup - restore
- Objects – Configuration of various policies for hosts, services, schedules and file type
- Networks – Network specific configuration viz., Interface speed, MTU and MSS settings, Gateway, DDNS
- Identity – Configuration and management of User and user groups
- Firewall – Firewall Rule Management

- VPN – VPN and SSL VPN access configuration
- IPS – IPS policies and signature
- Web Filter – Web filtering categories and policies configuration
- Application Filter – Application filtering categories and policies configuration
- WAF – Web Application Filtering policies configuration. Available in all the models except CR15iNG and CR15wiNG.
- IM – IM controls
- QoS – Policy management viz., surfing quota, QoS, access time, data transfer
- Anti Virus – Antivirus filtering policies configuration
- Anti Spam – Anti Spam filtering policies configuration
- Traffic Discovery – Traffic monitoring
- Logs & Reports – Logs and reports configuration

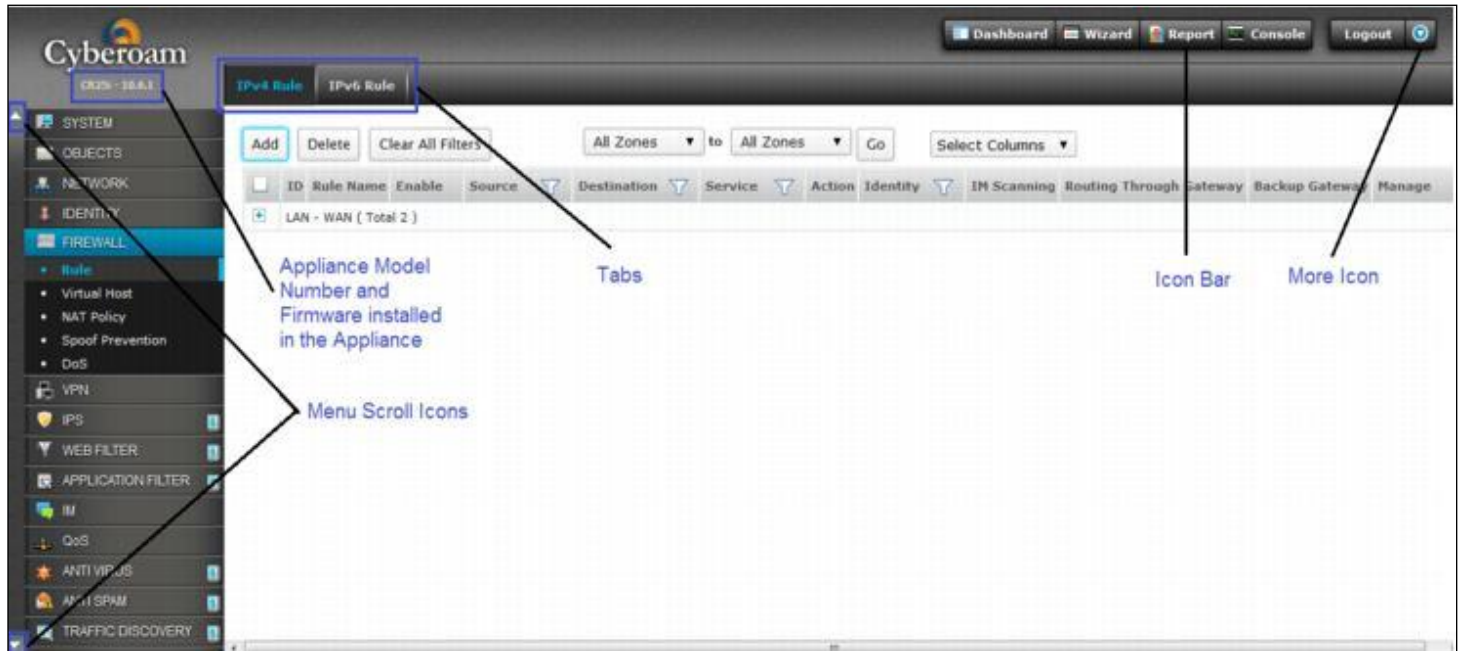
**Note**

- Use F1 key for page-specific help.
- Use F10 key to return to Dashboard.

Each section in this guide shows the menu path to the configuration page. For example, to reach the **Zone** page, choose the **Network** menu, then choose **Interface** sub-menu from the navigation bar, and then choose **Zone** tab. Guide mentions this path as **Network > Interface > Zone**.

## Page

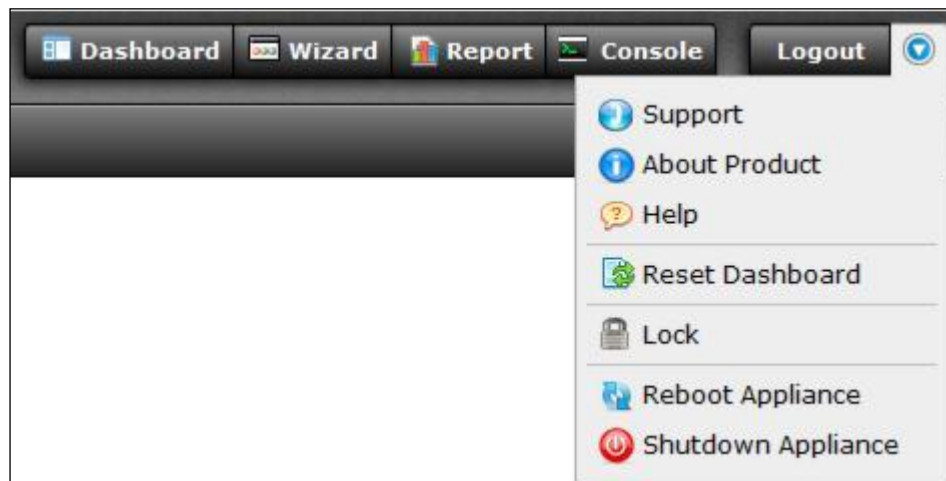
A typical page looks as shown in the below given image:



Screen – Page



## Icon bar



The Icon bar on the upper rightmost corner of every page provides access to several commonly used functions like:

**Dashboard** – Click to view the Dashboard

**Wizard** – Opens a Network Configuration Wizard for a step-by-step configuration of the network parameters like IP Address, subnet mask and default gateway for your Appliance.


**Report** – Opens a Reports page for viewing various usage reports. Integrated Logging and Reporting solution - iView, to offer wide spectrum of 1000+ unique user identity-based reporting across applications and protocols and provide in-depth network visibility to help organizations take corrective and preventive measures.



This feature is not available for CR15xxx series of Appliances.

**Console** – Provides immediate access to CLI by initiating a telnet connection with CLI without closing Web Admin console.

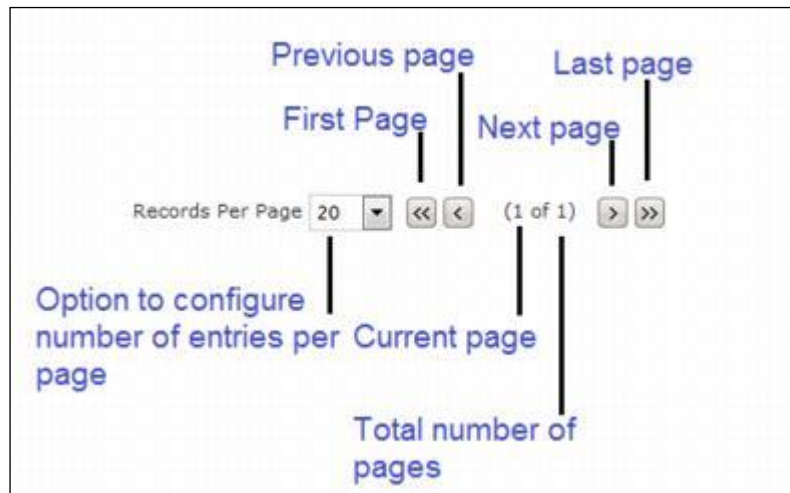
**Logout** – Click to log off from the Web Admin Console.

**More Options**  – Provides options for further assistance. The available options are as follows:


- **Support** – Opens the customer login page for creating a Technical Support Ticket. It is fast, easy and puts your case right into the Technical Support queue.
- **About Product** – Opens the Appliance registration information page.
- **Help** – Opens the context – sensitive help page.
- **Reset Dashboard** – Resets the Dashboard to factory default settings.
- **Lock** – Locks the Web Admin Console. Web Admin Console is automatically locked if the Appliance is in inactive state for more than 3 minutes. To unlock the Web Admin Console you need to re-login. By default, Lock functionality is disabled. Enable Admin Session Lock from **System > Administration > Settings**.
- **Reboot Appliance** – Reboots the Appliance.
- **Shutdown Appliance** – Shut downs the Appliance .

## List Navigation Controls

The Web Admin Console pages display information in the form of lists that are spread across the multiple pages. Page Navigation Control Bar on the upper right top corner of the list provides navigation buttons for moving through the list of pages with a large number of entries. It also includes an option to specify the number entries/records displayed per page.



## Tool Tips

To view the additional configuration information use tool tip. Tool tip is provided for many configurable fields. Move the pointer over the icon  to view the brief configuration summary.

## Status Bar

The Status bar at the bottom of the page displays the action status.

Status : ✓ Country Host 'Sydney\_Office' has been added successfully.

Status : ✗ User could not be registered. User or User group with the same name already exists, choose a different name.


## Common Operations



### Adding an Entity

You can add a new entity like policy, group, user, rule, or host by clicking the Add button available on most of the configuration pages. Clicking this button either opens a new page or a pop-up window.



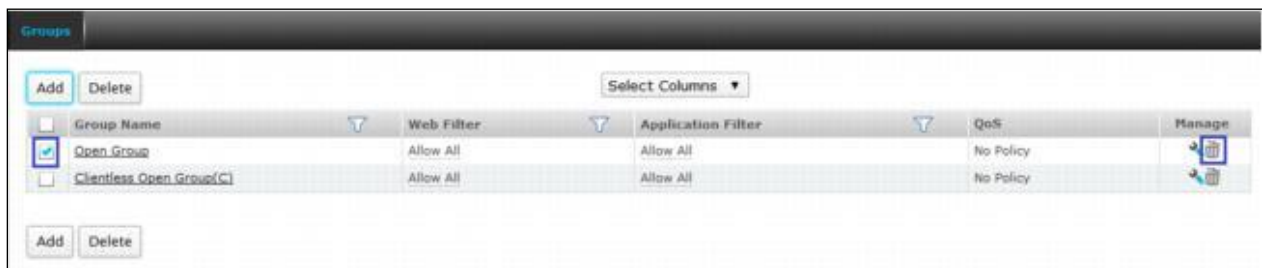
### Editing an Entity

All the editable entities are hyperlinked. You can edit any entity by clicking either the hyperlink or the Edit icon  under the Manage column.

<input type="checkbox"/>	Interface Name	Interface Type	Status	Zone Name	MAC Address	MSS	MTU	Interface Speed	Manage
<input type="checkbox"/>	PortA	Physical	Unplugged	LAN	00:0D:15:32:46:63	1460	1500	Auto-negotiated	
<input type="checkbox"/>	PortB	Physical	Connected, 1000 Mbps - Full Duplex	WAN	00:0D:15:32:46:64	1460	1500	Auto-negotiated	


### Deleting an Entity

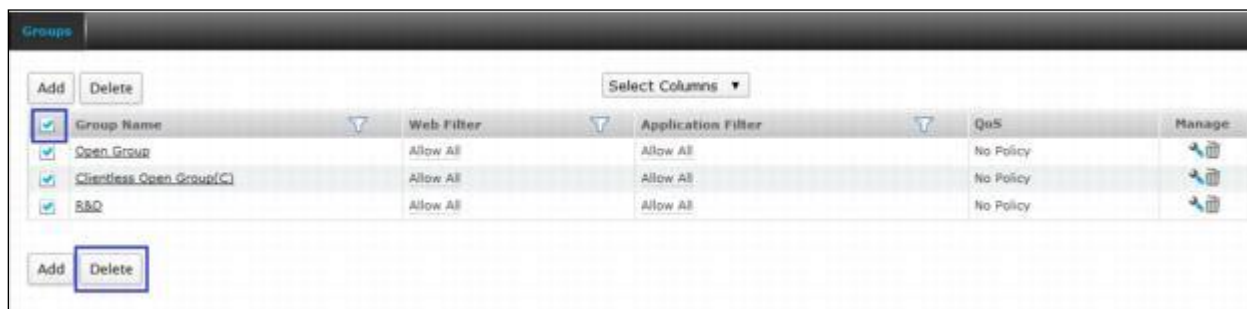
You can delete an entity by selecting the checkbox and clicking the Delete button or Delete icon.



To delete multiple entities, select  individual entity and click the Delete button.





To delete all the entities, select  in the heading column and click the Delete button.





## Sorting Lists

To organize a list spread over multiple pages, sort the list in ascending or descending order of a column attribute. You can sort a list by clicking a column heading.

- Ascending Order icon  in a column heading indicates that the list is sorted in ascending order of the column attribute.
- Descending Order icon  in a column heading indicates that the list is sorted descending order of the column attribute.

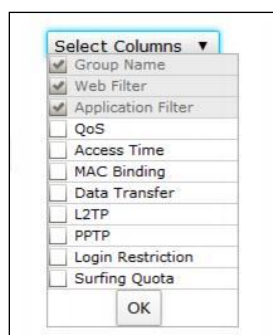
## Filtering Lists

To search specific information within the long list spread over multiple pages, filter the lists. Filtering criteria vary depending on a column data and can be a number or an IP address or part of an address, or any text string combination.

To create filter, click the Filter  icon in a column heading. When a filter is applied to a column, the Filter icon changes to .

## Configuring Column Settings

By default on every page all columnar information is displayed but on certain pages where a large number of columnar information is available, all the columns cannot be displayed. It is also possible that some content may not be of use to everyone. Using column settings, you can configure to display only those numbers of columns which are important to you.



To configure column settings, click Select Column Settings and select the checkbox against the columns you want to display and clear the checkbox against the columns which you do not want to display. All the default columns are greyed and not selectable.

# Getting Started

Once you have deployed and configured Cyberoam in your network and registered the copy of your Cyberoam, you can start using the Cyberoam.

## 1. Start monitoring

Once you have deployed the Appliance successfully you can start monitoring user activities in your Network. Depending on the Web and Application Filter Policy configured at the time of installation, certain categories will be blocked or allowed for LAN to WAN traffic with or without authentication.

## 2. View Reports

Monitor your Network activities using Reports.

To view Reports, log on to iView by clicking Reports on the topmost button bar from the Web Admin Console and log on with the default username 'admin' and password 'admin'.

- View user surfing trends from **Web Usage > Top Web User report**
- View your organization's Category wise surfing trends from **Web Usage > Top Categories report**
- View mail usage from **Mail Usage > Top Mail Senders** and Mail Receivers report

## 3. Configure for Username based monitoring

As user activity is monitored and logged based on IP address, all the reports generated are also IP address based. To monitor and log user activities based on User names, you have to configure Appliance for integrating user information and authentication process.

Integration will identify access request based on Usernames and generate reports based on them.

- If your Network uses Active Directory Services and users are already created in ADS, configure your Appliance to communicate your ADS.
- If your Network uses RADIUS, configure for your Appliance to communicate with RADIUS.
- If your Network uses LDAP, configure for your Appliance to communicate with LDAP.
- If your Network uses NTLM, configure your Appliance to communicate with NTLM.

## 4. Customize

You can create additional policies to meet your organization's requirement.

You can:

Control user based per zone traffic by creating firewall rule. Refer to Firewall for more details.

Control individual user surfing time by defining Surfing quota policy. Refer to Surfing Quota policy for more details.

Schedule Internet access for individual users by defining Access time policy. Refer to Access time policy for more details.

Control web access by defining Web and Application Filter Policies. Refer to Web and Application Filter Policy for more details.





Allocate and restrict the bandwidth usage by defining QoS policy. Refer to QoS policy for more details.

Limit total as well as individual upload and/or download data transfer by defining data transfer policy. (Refer Data transfer policy for more details.)

## Dashboard

The Appliance dashboard appears as soon as you log on to the Web Admin Console.

The Dashboard provides a quick and bird's eye view of all the important parameters of your Appliance that require special attention such as password, access to critical security services, system resources usage, IPS alerts, notifications of subscription expirations and many more. Dashboard uses Doclets to display this information.

Dashboard page is completely customizable and the administrator can reposition doclets by dragging and dropping or close the doclet by clicking  icon that are pertinent to the user and requires special attention for managing your Appliance on the top and the information used less often moved to the bottom. Administrator can even reset doclets position to default by selecting Reset Dashboard option  from More Options dropdown button . You can also refresh the doclets by clicking  icon.

## Alert Messages Doclet

Alert Message doclet allows the administrator to monitor and track system events of the Appliance. Each alert message displays the date and time that the event occurred.

Alert Message doclet displays following alerts:

The default password for the user "admin" has not been changed. We highly recommend you to change the password. – This alert is displayed when default password for the super administrator is not changed.

On-Appliance reporting is currently OFF. No reports are being generated. Use CLI command "set on-Appliance-report on" to start on-Appliance reporting. – This alert is displayed when Appliance reporting is disabled. By default, Appliance reporting is enabled.

The default Web Admin Console password has not been changed.

HTTPS, SSH based management is allowed from the WAN. This is not a secure configuration. We recommend using a good password.

HTTP, Telnet based management is allowed from the WAN. This is not a secure configuration. We recommend using a good password.

Your Appliance is not registered.

The modules expired.

Apart from preventing spyware from entering and infecting your network, the Appliance can also detect any unwanted applications and Spyware infected hosts that are already there in the network that is, network infected before Appliance was deployed and provides alert on Dashboard.

Color coding and symbolic representations are used for easier identification of alert messages.

The color coding is as under:


- Green: Indicates less severe notifications.
- Red: Indicates severe and security related notifications.
- Blue: Indicates firmware download notifications.

The icons used are as under:





: Indicates password related notifications.

: Indicates security related advice.

: Indicates Alert messages.

: Indicates firmware download notifications.

**Alert Messages**

-  Monday New firmware is available. Please read [release notes](#). [Download](#) new firmware. release firmware hash is #f2490ad5cb408a98900fd44c28aefc62
-  Monday The default password for the user "admin" has not been changed. We highly recommend you to change the password. [Click Here](#) to change password.
-  Monday Your Appliance is not registered.
-  2013-Nov For security reasons, the default CA certificate used in HTTPS scanning in your appliance has been replaced with a unique CA certificate. For uninterrupted secure browsing over HTTPS, you may need to re-import the same in the browser. For more information, [Click Here](#) [More Alerts](#)

## Appliance Information Doclet

The Appliance Information doclet provides Appliance information. Doclet provides:

- Model number of the Appliance which is deployed for example, CR35iNG and its Appliance key,
- Base firmware version, for example 10.6.1 and build number which is installed,
- Version number of various subscription modules - IPS Signature, Anti Virus, Webcat Signature, and Application Signatures used by the Appliance to categorize and control traffic or detect and block virus.

<b>Appliance Information</b>	
Appliance Key	C12012446556-KDE6H7
Model Number	CR35iNG
Firmware Version	10.6.2 <a href="#">[Check for Upgrades]</a>
Firmware Build	369
IPS Signature Version	3.12.8
Anti Virus Version	3.50,1,5.08
Webcat Signature Version	0.0.0.206
Application Signatures	4.12.8

## System Usage Doclet

The System Usage doclet displays graphs pertaining to CPU and memory usage. A period-wise graph is displayed providing information of the last two hours of CPU and Memory Usage.

### CPU Info graphs

CPU Info graphs allow the Administrator to monitor the CPU usage by the Users and System components. Last two hour CPU Usage - Graph shows past two hour's CPU usage in percentage.

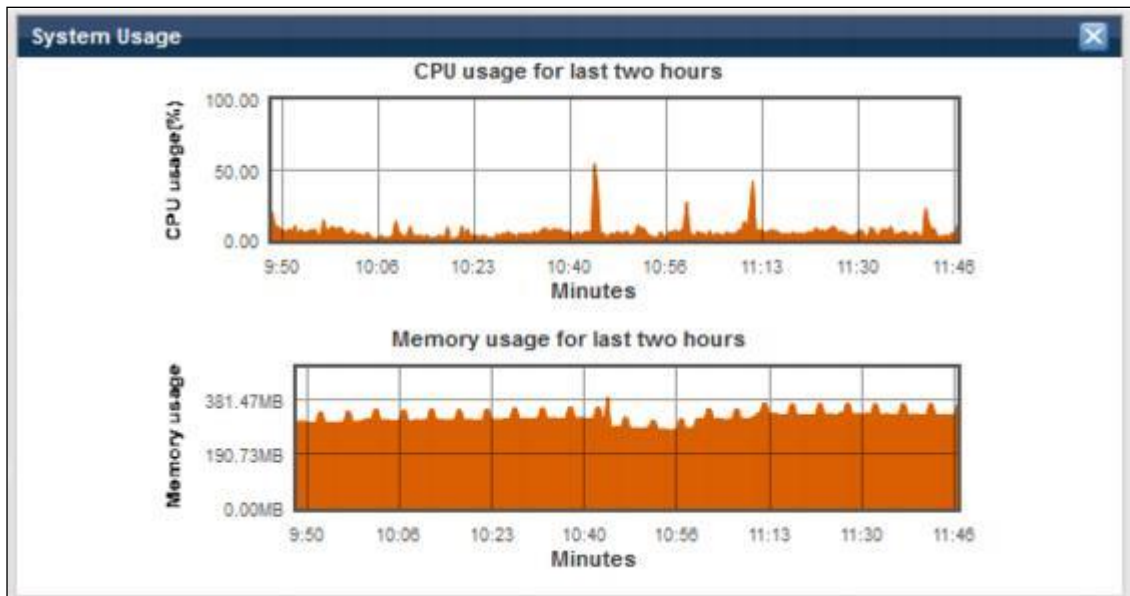


## Memory Info graphs

Memory Info graphs allow the Administrator to monitor the memory usage in MB.

Last two hours Memory Usage - Graph shows past two hour's memory usage in MB.

To view more graphs, go to **System > Diagnostics > System Graphs**. You can view Period wise Utilities graphs.



## System Status Doclet

System Status doclet provides general system information such as current system date and time, number of days since the Appliance is up and running, and the total number of currently connected users.

You can change the system time from CLI Console from System Settings menu though we do not recommend changing time as this affects all the logs and reports. Refer Cyberoam Console Guide for more information.

System Status	
System Time	Tue 26 Nov 2013 13:59:00
Up Time	4 days, 2 hours, 27 minutes
Live Connected Users	121

## Recent Web Viruses Detected Doclet

The Web Viruses Detected doclet provides web virus information.

Doclet provides:

- The date and time at which the web virus is detected. The date is displayed in format – Day DD:MM:YYYY. The time is displayed in format HH:MM:SS.

- The name of the user during whose activity the web virus was detected.
- The name of the domain in which the web virus is detected.
- The name of the detected web virus.

## Recent Mail Viruses Detected Doclet

The Recent Mail Viruses detected doclet provides information about the mail virus detected by the Appliance.




Doclet provides:





- The time and date when the Appliance detected virus. The date and time is displayed in the format Day DD:MM:YYYY HH:MM:SS.
- The name of the protocol via which the virus infected Email is received.
- The Email address of the recipient who has received the virus infected Email.
- The subject of the virus infected Email that is received.
- The name of the virus detected by the Appliance.

Recent Mail Viruses detected				
Time	Protocol	Recipient	Subject	Name
Fri 02 Nov 2012 12:29:18	IMAP4	reg@gct.com	Re: Payment has been made.	TR/ATRAPS .Gen

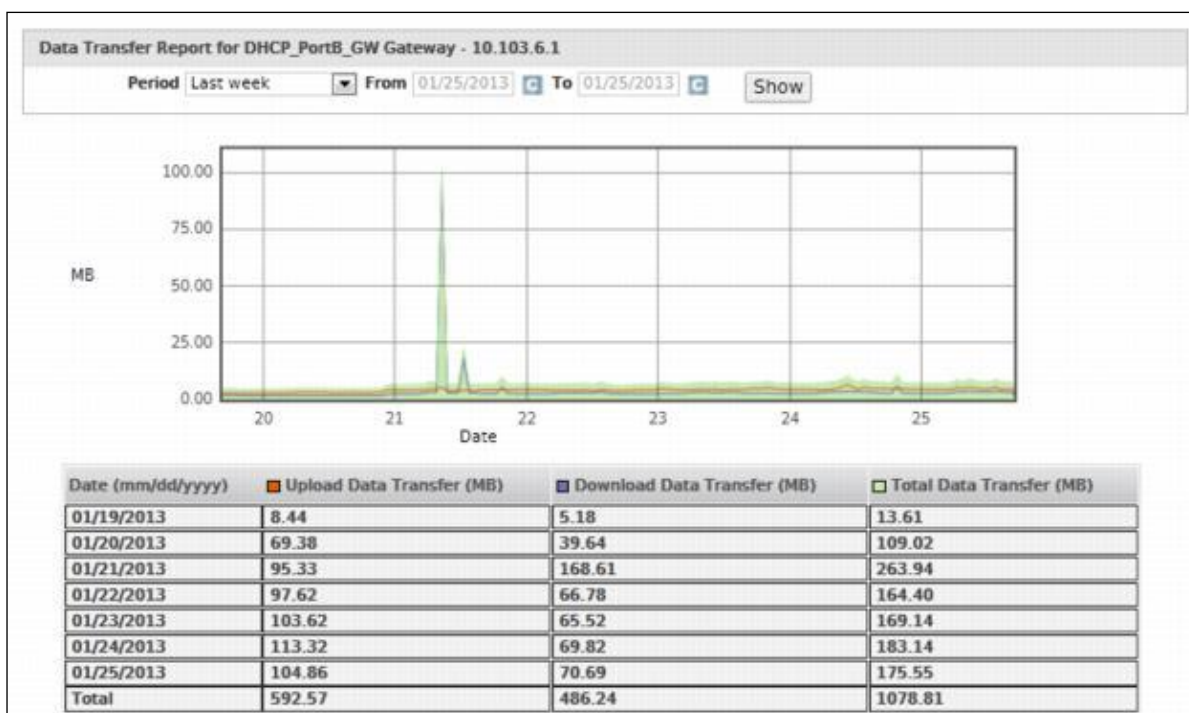
## Gateway Status Doclet

The Gateway Status Doclet provides information about the Gateway. Doclet provides:

- The name of the gateway. Click the Graph icon  against the Gateway to view data transfer via the particular gateway.
- The IP Address (IPv4/IPv6) of the gateway.
- The status of Gateway whether is reachable or not that is – Active  or Deactive 

Gateway Status		
Gateway Name	Gateway IP Address	Status
DHCP_PortB_GW 	128.0.0.1	
10.202.63.254 	10.202.63.254	

- View Data Transfer Graph.



User can select the period from the available options for the Report of Data Transfer through the Gateway.

#### Available Options:

Last Week  
Last Month  
Custom

Graph displays the upload, download and total data transfer through Gateway.

X-axis – Date (depending on the period selected)

Y-axis – KB /MB/GB used.

#### Legends

Orange Color – Upload Data Transfer (MB)  
Purple Color – Download Data Transfer (MB)  
Green Color – Total Data Transfer (MB)

#### Note

- When the selected period is “Custom”, then the user can select to view data of maximum last six (06) months. At a time maximum of thirty (30) days data will be displayed.

## Recent Malware Alerts Doclet

The Malware Alerts doclet provides spyware information. Doclet provides:

The date and time at which the spyware is detected. The date is displayed in format – Day DD:MM:YYYY.  
The time is displayed in format HH:MM:SS.

- The source IP Addresses and destination IP address from where the spyware originated and is destined to, respectively.
- The name of the signature using which the spyware got detected.
- The severity level of the spyware viz., critical, major, moderate, minor, warning.
- The action taken on the detected spyware as per the configured policy viz., allow packet, drop packet, drop session, reset, and bypass session.
- The Signature Identification Number to which the spyware matched.

## License Information Doclet

License Information doclet provides the information about the subscription modules. Doclet provides:

- The Appliance registration information. If the Appliance is registered, the Email Address used for Appliance registration is displayed. If the Appliance is not registered, click the underlined link against Appliance Not Registered, to navigate to System > Maintenance > Licensing for further information.
- Subscription status of the modules available for subscription.

The status of the subscription module can be one of the following:

Status	Meaning
Expires on Day DD MM YYYY	Subscription expiry date
Unsubscribed	Module is not subscribed
Subscription Expired	Subscription has expired



License Information	
Registered Email ID	akka@ic.ma
Subscriptions	
Web and Application Filter	Expires On Fri 23 May 2014
Intrusion Prevention System (IPS)	Expires On Fri 23 May 2014
Gateway Anti Virus	Expires On Fri 23 May 2014
Gateway Anti Spam	Expires On Fri 23 May 2014
8 x 5 Support	Expires On Fri 23 May 2014
24 x 7 Support	Unsubscribed
WAF	Expires On Wed 01 Jan 2014

## Recent FTP Viruses Detected Doclet

The FTP Viruses Detected doclet provides web virus information. Doclet provides:

- The date and time at which the FTP virus is detected. The date is displayed in format – Day DD:MM:YYYY. The time is displayed in format HH:MM:SS.
- The name of the user during whose file transfer activity the FTP virus was detected.
- The name of the domain in which the FTP virus is detected.
- The name of the detected FTP virus.

## Recent IPS Alerts Doclet

The IPS Alert doclet provides traffic information identified for malicious activity on the network. Doclet provides:

- The date and time at which the malicious traffic is detected. The date is displayed in format – Day DD:MM:YYYY. The time is displayed in format HH:MM:SS.
- The source and destination IP address from where the malicious traffic originated and is destined to, respectively.
- The name of the signature using which the malicious traffic got detected.
- The severity level of the malicious traffic.
- The action taken on the detected malicious traffic as per the configured policy.

Recent IPS Alerts				
Time	Src/Dst	Signature Name	Severity	Action
Thu 26 Dec 2013 11:33:12	63.250.204.25/192.168.4.33 (N/A)	Apache HTTP Server mod_rpaf x-forwarded-for Denial of Service	Major	Detect

## Today Usage Summary Doclet

The Today Usage Summary doclet provides Internet usage information and search statistics for the current day. Doclet provides:

- Total HTTP hits
- The total number of search queries made using google and yahoo search engines. Clicking any search engine opens respective search engine report, providing search details like search date and time, name of the user, IP address through which the search request was placed, and the search string. The Appliance also provides similar report for other search engines like Bing, Wikipedia, Rediff, and eBay and can be viewed from **Logs & Reports > View Reports > Reports > Search Engine**.

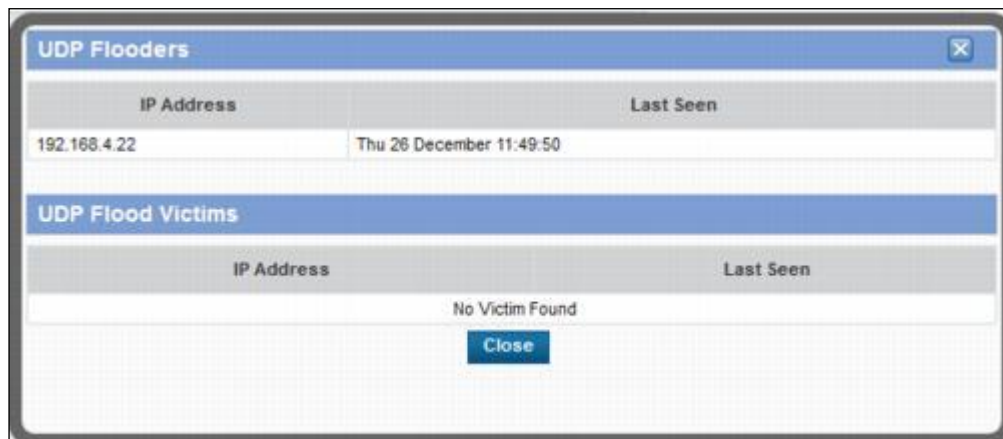
Today Usage Summary		
HTTP Hits	26755	
Search Engine Queries	Google : 44	Yahoo : 0

## DoS Attack Status Doclet

The DoS Attack Status Doclet provides information about DoS Attacks. Doclet provides:

1. Attack type. Click on the hyperlink to view real time updates on flooding. It displays details of the Source IP Addresses (Flooders) used for flooding and the targeted IP Addresses (Flood Victims). Also, it displays the date and time at which the flooding is detected.
2. Displays whether Source/Destination packet control is applied or not.
3. Number of packets dropped in case Source/Destination packet control is applied.

DoS Attack Status				
Attack Type	Source		Destination	
	Applied	Traffic Dropped	Applied	Traffic Dropped
<a href="#">SYN Flood</a>	Yes	0	No	0
<a href="#">UDP Flood</a>	Yes	19544	No	0
<a href="#">TCP Flood</a>	No	0	No	0
<a href="#">ICMP Flood</a>	Yes	0	No	0



## Web Traffic Analysis Doclet

The Web Traffic Analysis doclet provides web traffic information.

The web traffic is by default classified into four categories: Productive, Non-Working, Neutral, and Unhealthy. Traffic is classified under category - N/A, if it does not fall in any of the default categories. Different colors represent different categories. Doclet provides:

- **Distribution by Hits** – Graph displays total traffic hits per category. Clicking the hyperlink will open the detailed report.
- **Distribution by Data Transfer** – Graph displays total data transferred per category.



## HA Details Doclet

The HA Details doclet not available in models CR15i, CR25ia, CR15wi, CR25wi, CR35wi, CR15iNG.

The Doclet provides HA configuration mode, Primary and Auxiliary Appliance key, Dedicated link port, Monitored Interface list and current connections.

Screen Element	Description
<b>HA Configuration Mode</b>	Displays the HA Configuration mode for cluster. HA can be configured in one of the following two modes: Active-Active and Active-Passive.
<b>Appliance Key</b>	Displays Appliance key only after HA is configured.
<b>Peer Appliance Key</b>	Displays peer's Appliance Key.

	<p>In case of Primary Appliance, it displays the Auxiliary Appliance Key.</p> <p>In case of Auxiliary Appliance, it displays the Primary Appliance Key.</p>
<b>Dedicated HA Link Port</b>	Displays the HA link port that is configured on Primary Appliance and to be used HA link port on Auxiliary Appliance
<b>Monitored Interface List</b>	<p>Displays the Appliance port to be monitored.</p> <p>Both the Appliances will monitor their own ports and if any of the monitored port goes down, Appliance will leave the cluster and failover will occur.</p>
<b>Connection</b>	Displays connections served by Primary and Auxiliary Appliance.

HA Details	
HA Configuration Mode	Active-Active
Appliance Key	C069800033-JU22FF [Primary]
Peer Appliance Key	C016700564-U5QDVF [Auxiliary]
Dedicated HA Link Port	PortF
Monitored Interface List	PortA,PortC,PortE
Connection	1058 / 613



# System

System allows configuration and administration of Cyberoam Appliance for secure and remote management as well as administrative privilege that you can assign to admin users. It also provides the basic system settings and language settings for the Web Admin Console. Configuration of several non-network features, such as SNMP, custom messages, portal setting and themes can be done through System.

## Administration

Administration page provides an option to configure general settings for your Appliance. Various ports and login security can be configured using this submenu. The Administrator can also restrict administrative access to various local services available from the zone. Administrator can create profile(s) to be assigned to the admin users for configuring and managing the Appliance. You can administer port numbers, remote login security, local login security and local ACL services from Administration submenu.



## Settings

Use the Settings page to make modifications in the general port settings and Web Admin Login parameters. Make changes to the login parameters for restricting the local and remote users based on the time.

To manage the administration settings, go to **System > Administration > Settings**.

**Web Admin Settings**

HTTP Port\*

HTTPS Port\*

Certificate\*  (The above selected certificate will also be used for My Account.)

---

**SSL VPN Settings**

SSL VPN Port\*

Certificate\*

Per User Certificate Encryption  Enabled

Receive Passphrase via\*  Client Bundle  On-screen Link  Email

Default language for SSL VPN Web Portal

---

**Login Security (Remote Admins)**

Lock Admin Session After  Minutes Of Inactivity

Logout Admin Session After  Minutes Of Inactivity

Block Admin Login

After  unsuccessful attempts from same IP in  Seconds (1-120)

Block login access for  Minutes (1-60)

---

**Administrator Password Complexity Settings**

Enable Password Complexity Check

Minimum Password length should be of  characters

Include atleast 1 each Upper and Lower case alphabetic characters

Include atleast 1 numeric character

Include atleast 1 special character like '@', '\$', '!', etc

( Note: Password must not be a User Name )

---

**Login Disclaimer Settings**

Enable Login Disclaimer

[Click Here](#) to modify the Disclaimer Message ( System-> Configuration-> Messages )

[Click Here](#) to Preview the Disclaimer Message

---

**Language Settings**

Default Configuration Language

**Screen – Manage Administration Settings**

## Parameters

Screen Element	Description
<b>Web Admin Settings</b>	
<b>HTTP Port</b>	Provide the port number to configure HTTP Port.

	Default – 80
<b>HTTPS Port</b>	Provide the port number to configure HTTPS Port for Secured Web Admin Console access.  Default – 443
<b>Certificate</b>	Certificate to be used by User MyAccount and Captive Portal.
<b>SSL VPN Settings</b>	
<b>SSL VPN Port</b>	Provide the port number to configure SSL VPN Port.  Default – 8443
<b>Certificate</b>	Default Certificate that will be used by SSL VPN. After configuring Tunnel Access if you want to configure Certificate from a different CA, change SSL Server Certificate from <b>VPN &gt; SSL &gt; Tunnel Access page</b> .
<b>Per User Certificate Encryption</b>	Selecting this option will allow the user to have user specific certificate encryption.
<b>Receive Passphrase via</b>	Select a mode to receive a passphrase from the available options:  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• <b>Client Bundle</b></li> <li>• <b>On-screen Link</b></li> <li>• <b>Email</b></li> </ul> Default – By default, the passphrase is received is Client Bundle.
<b>Default Language for SSL VPN Web Portal</b>	Select a default language to be used for SSL VPN Web Portal from the available options:  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• <b>English</b></li> <li>• <b>Hindi</b></li> <li>• <b>Chinese – Traditional</b></li> <li>• <b>Chinese – Simplified</b></li> <li>• <b>French</b></li> <li>• <b>Japanese</b></li> </ul>
<b>Login Security (Remote Admins)</b>	
To prevent the unauthorized access to the Web Admin Console and CLI, configure Admin Session Lock, Admin Session Logout time and Block Admin Login to block the access after number of failed login attempts.  Configure inactive time in minutes after which the Appliance will be locked automatically. This configuration will be applicable to following Cyberoam components:	

- Web Admin Console
- Telnet Console
- IPSec Connection Wizard
- Network Wizard
- Group Import Wizard

Configure inactive time in minutes after which the administrator will be logged out automatically. By default, admin session logout time is 30 minutes.

#### Note

- Admin Session Logout time value must be greater than the Lock Admin Session time.

Block Admin Login – Enable to block login to the Web Admin Console and CLI if allowed failed login attempts exceeds.

Configure number of allowed failed login attempts from the same IP Address within the time limit.

Specify number of minutes for which the administrator will not be allowed to login i.e. if allowed failed login attempts exceeds, the administrator account will locked for the configured minutes.

#### Administrator Password Complexity Settings

Password Complexity can be configured to ensure that administrators are using secure passwords.

Enable Password Complexity Settings to enforce following constraints:

- Minimum Password length. Configure minimum characters required in the password. By default, the Minimum Password length is eight (8) characters.
- Require minimum one Upper and lower case alphabet
- Require minimum one number i.e. 0 - 9
- Require at least one special character e.g. @, \$, %
- Password cannot be same as username.

All the enabled constraints are applied to administrator user password.

#### Login Disclaimer Settings

The Login Disclaimer allows setting a written message that administrators must read and agree prior to logging on to the Web Admin Console and CLI for Appliance administration. If a disclaimer is set, it must be accepted before administrator can login.

Default disclaimer can be customized as per the requirement from the Messages page (**System > Configuration > Messages**). One can also review the customized message before setting.

#### Language Settings

##### Default Configuration Language

Select a default configuration language. On changing the language Appliance reboots, removes all the customizations, and displays all the default configurations in the selected language.

**Available Options:**

	<ul style="list-style-type: none"><li>• English</li><li>• Hindi</li><li>• Chinese – Traditional</li><li>• Chinese – Simplified</li><li>• French</li><li>• Japanese</li></ul> <p>Please make sure to take the backup as the entire custom configuration will be lost. Appliance restores the backup in the same language in which it is taken.</p>
--	---

**Table – Administration Settings screen elements**

## Appliance Access

Appliance Access allows limiting the Administrative access of the following Appliance services from various default as well as custom zones – LAN, WAN, DMZ, and VPN:

- Admin Services – HTTP, HTTPS, Telnet, SSH
- Authentication Services – Windows/Linux Client, Captive portal, NTLM, Radius SSO
- Network Services – DNS, Ping/Ping6
- Other Services – Web Proxy, SSL VPN, Wireless Protection

To manage the access to devices, go to **System > Administration > Appliance Access**.

Zone	Admin Services				Authentication Services				Network Services		Other Services		
	HTTP	HTTPS	Telnet	SSH	Windows/Linux Client	NTLM	Captive Portal	Radius SSO	Ping/Ping6	DNS	Wireless Protection	SSL VPN	Web Proxy
LAN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DMZ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
VPN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WiFi	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Screen – Appliance Access Settings

### Default Access Control Configuration

When the Appliance is connected and powered up for the first time, it will have a default Access configuration.

**Admin Services** – HTTP (TCP port 80), HTTPS (TCP port 443), Telnet (TCP port 23) and SSH (TCP port 22) services will be enabled for administrative functions in LAN zone. HTTP (TCP port 80), HTTPS (TCP port 443) and SSH (TCP port 22) services will be enabled for administrative functions in WAN zone. HTTP (TCP port 80) services will be enabled for administrative functions in DMZ zone.

**Authentication Services** – Windows/Linux Client (UDP port 6060), Captive portal Authentication (TCP port 8090) and Radius SSO will be enabled for User Authentication Services in LAN zone. User Authentication Services are not required for any of the Administrative functions but required to apply user based internet surfing, bandwidth, and data transfer restrictions.

**Network Services** – Ping/Ping6 and DNS services will be enabled for LAN zone.

**Other Services** – Web Proxy service will be enabled for LAN zone. SSL VPN (TCP port 8443) service will be enabled for LAN, WAN and DMZ zone.

### Updating Default Access Control Configuration

Use access control to limit the access to the Appliance for administrative purposes from the specific authenticated/trusted networks only.

**Admin Services** – Enable/disable access to the Appliance using following service from the specified zone: HTTP, HTTPS, Telnet and SSH.

**Authentication Services** – Enable/disable following service from the specified zone: Windows/Linux Client, Captive portal, NTLM, Radius SSO.

Note: The SMBv2 protocol is introduced in Windows Vista and Windows Server 2008, hence NTLM compatibility will not be applicable for Windows Server 2003 and earlier versions.

**Network Services** – Enable/disable following service from the specified zone: DNS, Ping/Ping6

**Other Services** – Enable/disable following service from specified zone: Web Proxy, SSL VPN, Wireless Protection.

## Administrator Profiles

Role-based administration capabilities are provided to offer greater granular access control and flexibility.

It allows an organization to separate super administrator's capabilities and assign through Profiles. Profiles are a function of an organization's security needs and can be set up for special-purpose administrators in areas such as firewall administration, network administration, and logs administration. Profiles allow granting permissions to individual administrators depending on their role or job need in organization.

The profile separates Appliance features into access control categories for which you can enable none, read only, or read-write access.

For ease of use, by default the Appliance provides 5 profiles:

- **Administrator** – super administrator with full privileges
- **Audit Admin** – read-write privileges for Logs & Reports – Configuration, Report Access and De-Anonymization only
- **Crypto Admin** – read-write privileges for Certificate configuration only
- **HAPProfile** – read-only privileges. If HA is configured, any user accessing Web Admin Console of Auxiliary Appliance will have privileges as defined in HAPProfile.
- **Security Admin** – read-write privileges for all features except Profiles, Password, Certificates, WAF Alerts, Traffic Discovery and Log & Reports - Configuration, Log Viewer, Report Access

An Administrator with full privileges can create other custom administrators and assign them restricted/full privileges. A custom administrator so created, has restricted privileges and can only update their Email Address and password.








### Note

- You cannot delete the default profiles.
- You cannot delete the profile assigned to administrator.

## Manage Profiles

To manage default and custom profiles, go to **System > Administration > Profile**.


The Profiles list shows the default and custom profiles you have created and enables you to add, edit, and delete profiles.

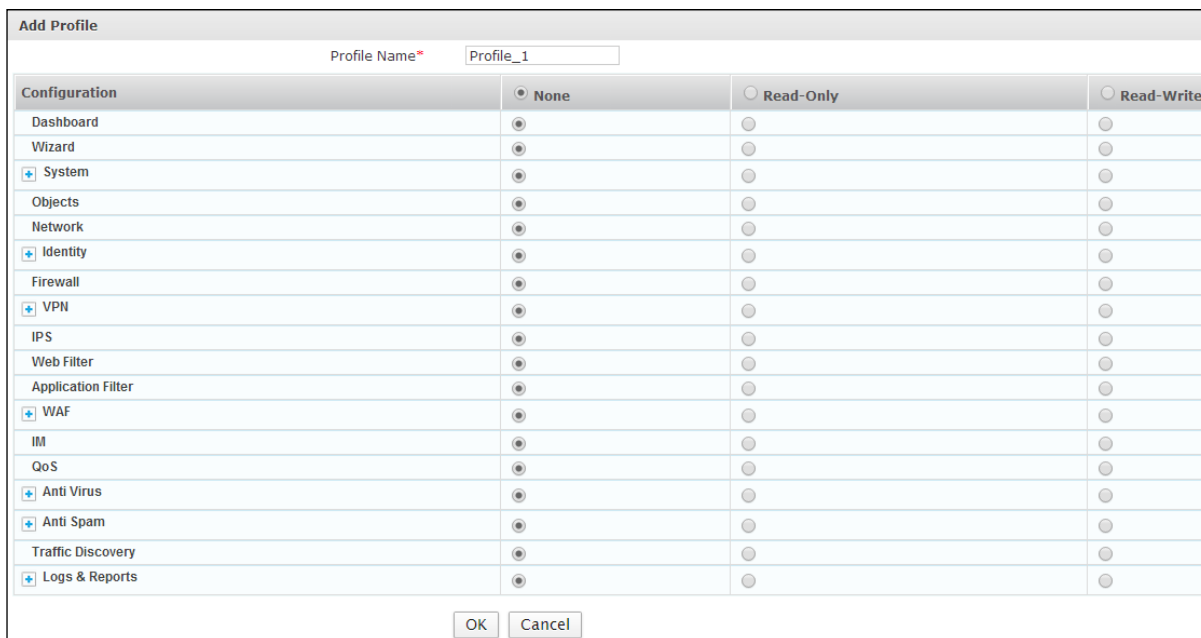
Add		Delete	
<input type="checkbox"/>	Profile	Manage	
<input type="checkbox"/>	<a href="#">Administrator</a>		
<input type="checkbox"/>	<a href="#">Audit Admin</a>		
<input type="checkbox"/>	<a href="#">Crypto Admin</a>		
<input type="checkbox"/>	<a href="#">HAPProfile</a>		
<input type="checkbox"/>	<a href="#">Security Admin</a>		
<input type="checkbox"/>	<a href="#">Zone Security</a>	 	

Add Delete

Screen – Manage Profile

## Profile Parameters

To add or edit profiles, go to **System > Administration > Profile**. Click Add Button to add a new profile. To update the details, click on the Profile or Edit icon  in the Manage column against the profile to be modified.



Configuration	<input checked="" type="radio"/> None	<input type="radio"/> Read-Only	<input type="radio"/> Read-Write
Dashboard	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Wizard	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ System	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Objects	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Network	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ Identity	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Firewall	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ VPN	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
IPS	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Web Filter	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Application Filter	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ WAF	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
IM	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
QoS	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ Anti Virus	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ Anti Spam	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Traffic Discovery	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ Logs & Reports	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Screen – Add Profile


Screen Element	Description
<b>Add Profile</b>	
<b>Profile Name</b>	Specify a name to identify the profile.
<b>Configuration</b>	<p>Click on the access level you want to provide to a profile. There are three levels of access each of the created profile can have.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>None</b> – No access to any page</li> <li>• <b>Read-Only</b> – View the pages</li> <li>• <b>Read-Write</b> – Modify the details</li> </ul> <p>Access levels can be set for individual menus as well. You can either set a common access level for all the menus or individually select the access level for each of the menu. Click  icon against a menu to view the items under that menu.</p> <p>For example, if you set access level as Read-Only against the Web Filter, the profile user would only be able to view the Web Filter menu but would not be able to make any modifications. To make modifications, Read-Write option is to be used.</p>

Table – Add Profile screen elements



## **Access Denied Page**

The Appliance provides role-based administration capabilities and privileges are assigned to the Administrator through Profiles. Administrator can have read only, read-write or no access privilege for the pages of Web Admin Console.

Access denied page is displayed when the Administrator tries to access a page or perform the operation, which is not allowed to them.

## Password

The Appliance is shipped with one global super admin with the credentials – username & password as “admin”. Both the consoles – Web Admin Console and CLI, can be accessed with the same credentials. This administrator is always authenticated locally that means by the Appliance itself.

### Note

- It is strongly recommended to change the password for this username immediately after deployment.

To change password, go to **System > Administration > Password**.

The screenshot shows a web interface titled "Default Admin Password Settings". It contains the following elements:

- User Name:** A text field containing the value "admin".
- Current Password \*:** An empty text input field.
- New Password \*:** A text input field containing the placeholder text "Password".
- Confirm Password:** A text input field containing the placeholder text "Confirm Password".
- Buttons:** Two buttons are located at the bottom: "Apply" and "Reset To Default".

Screen – Change Password

### Parameters

Screen Element	Description
<b>Default Admin Password Settings</b>	
<b>User Name</b>	The Default Admin User Name is – admin.
<b>Current Password</b>	Provide the current admin password.
<b>New Password</b>	Password - Specify new admin password.
	Confirm Password - Confirm the specified new admin password.
<b>Reset to Default</b>	Click to reset the password to factory default password.

Table – Change Password screen elements

## Central Management

Apart from managing and monitoring the Appliance directly, it can also be done through Cyberoam Central Management if deployed within your organization.

To enable Appliance management through CCC, go to **System > Administration > Central Management**.

**Central Management Settings**

**Enable Central Management**

IPAddress / Domain \*

**Appliance Management**

**Communication Details**

Heartbeat Protocol  Syslog (Recommended)  HTTP (Send Keep-Alive Heartbeat request from appliance to Central Management)

Secure Communication  Enable

Heartbeat Port \*

**Configuration Synchronization**

Synchronization Mode  Central Management will push configuration changes to the Appliance ⓘ  
 Appliance will fetch configuration changes from Central Management

Connection Protocol  HTTPS  HTTP

Port

**Signature Distribution**

Signature Distribution Port \*

Screen – Central Management

### Parameters

Screen Element	Description
<b>Central Management Settings</b>	
<b>Enable Central Management</b>	Enable to manage the Appliance through Central Management.
<b>IP Address / Domain</b>	Specify the IP Address/Domain for Central Management.
<b>Port</b>	Specify the value to the Port over which the information will be sent.
<b>Appliance Management</b>	Enable to configure and communicate with the Appliance through Central Management.
Communication Details	
<b>Heartbeat Protocol</b>	Select Heartbeat Protocol from the available options.  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• Syslog</li> <li>• HTTP</li> </ul>

	<p>Selected Heartbeat Protocol specifies how the information will be provided.</p> <p>Syslog is the default Heartbeat Protocol.</p>
<b>Secure Communication</b>	<p>Enable this option to secure the Connection between the Appliance and Central Management Server.</p>
<b>Heartbeat Port</b>	<p>Specify the Heartbeat Port.</p> <p>Central Management receives heartbeat information on the specified port.</p> <p>By default, the Heartbeat Port are:</p> <ul style="list-style-type: none"> <li>• Syslog – 514</li> <li>• HTTP – 80</li> </ul> <p>The Appliance will send information at specific intervals to Central Management. The Central Management will analyze the information received from the Appliance periodically and send necessary alerts.</p> <p>For details about Alerts, refer to Central Management Guide.</p> <p>Enabling the “Secure Communication” option will set the default Heartbeat Port values to</p> <ul style="list-style-type: none"> <li>• Syslog – 6514</li> <li>• HTTP – 443</li> </ul>
<b>Configuration Synchronization</b>	
<b>Synchronization Mode</b>	<p>Specify the method to be used for sending configuration updates:</p> <p>Available Options:</p> <ul style="list-style-type: none"> <li>• <b>Central Management will push configuration changes to the Appliance</b> – Select if the Appliance is directly connected to the Internet. In this case the Central Management keeps on passing updates to the Appliance if any configurations are updates. Communication will be done on port 80.</li> <li>• <b>Appliance will fetch configuration changes from Central Management</b> – Select if the Appliance is behind NAT device. In this case the Appliance keeps on asking for updates to the Central Management.</li> </ul>

<b>Connection Protocol</b>	Select the protocol through which the updates are sent from the available options:  Available Options: <ul style="list-style-type: none"><li>• HTTP</li><li>• HTTPS</li></ul>
<b>Port</b>	Displays the port number for the protocol selected.
<b>Signature Distribution</b>	Enable if you want to automatically update AV, IPS and Application Signatures from the Central Management Console.
<b>Signature Distribution Port</b>	Configure port on which appliance and Central Management Console communicates.  Default - 80

**Table – Central Management screen elements**

## API

Application Programming Interface (API) is an interface which allows third party applications to communicate with Cyberoam. This page allows the Administrator to log on and log off users.

The screenshot shows a web interface with two main sections. The top section is titled 'API Configuration' and contains a checkbox labeled 'Enabled'. Below it is a search bar with the text 'Search/Add' and an 'Add' button. Underneath the search bar is a list area labeled 'IP Address' which currently shows 'No Record'. An 'Apply' button is located below the IP address list. The bottom section is titled 'API Explorer' and contains a large text area labeled 'Request XML String\*' with a 'Parse and Apply' button at the bottom right.

Screen – API Configuration

## Parameters

Screen Element	Description
<b>API Configuration</b>	
<b>API Configuration</b>	Enable to allow only authorized third-party Solution Providers like ISP, System Integrators to use API for log on and log off process.  Default - Disable
<b>IP Address</b>	Add the IP Addresses allowed to place the XML log on and log off requests.  You will be able to add IP Address only if API Configuration is enabled.
<b>API Explorer</b>	
<b>Request XML String</b>	Specify the XML content containing the configurations to enable user log on or log off.
<b>Parse and Apply</b>	Click to parse the XML Content and apply the configurations.

Table – API screen elements

For all the requests, XML response will be displayed in a pop-up window.

**Sample XML Request Code:**

```
<Request><LiveUserLogin><UserName>cyberoam</UserName><Password>cyber</Password><IPAdress>10.21.18.15</IPAddress><MacAddress>00:0C:29:2D:D3:AC</MacAddress></LiveUserLogin></Request>
```

```
<Request><LiveUserLogout><Admin><UserName>admin</UserName><Password>admin</Password></Admin><UserName>cyberoam</UserName><IPAddress>10.21.18.15</IPAddress></LiveUserLogout></Request>
```

**For versions prior to 10.6.1 MR-1**

```
<Request><LiveUserLogout><UserName>cyberoam</UserName><IPAddress>10.21.18.15</IPAddress></LiveUserLogout></Request>
```

Please use the below link to use API:

<https://<Cyberoam IP>/corporate/APIController?reqxml=<Add the XML request here>>

For example:

[https://<Cyberoam](https://<Cyberoam IP>/corporate/APIController?reqxml=<Request><LiveUserLogin><UserName>cyberoam</UserName><Password>cyber</Password><IPAddress>10.21.18.15</IPAddress><MacAddress>00:0C:29:2D:D3:AC</MacAddress></LiveUserLogin></Request>)

[IP>/corporate/APIController?reqxml=<Request><LiveUserLogin><UserName>cyberoam</UserName><Password>cyber</Password><IPAddress>10.21.18.15</IPAddress><MacAddress>00:0C:29:2D:D3:AC</MacAddress></LiveUserLogin></Request>](https://<Cyberoam IP>/corporate/APIController?reqxml=<Request><LiveUserLogin><UserName>cyberoam</UserName><Password>cyber</Password><IPAddress>10.21.18.15</IPAddress><MacAddress>00:0C:29:2D:D3:AC</MacAddress></LiveUserLogin></Request>)

**Note**

- When the user logs on using API, the client type of all users will display “API Client” on the Live Users page.

## Configuration

The Configuration page allows basic configuration of the Appliance including GUI localization, mail server, customized messages, web & parent proxy settings, themes and outlook for the Captive portal.

### Time

Appliance current date and time can be set according to the Appliance's internal clock or synchronized with an NTP server. Appliance clock can be tuned to show the right time using global Time servers so that logs show the precise time and Appliance internal activities can also happen at a precise time.

To configure time settings, go to **System > Configuration > Time**.

Current Time **2013-01-05 18:22:56**

Time Zone **Asia/Kolkata**

Set Date & Time

Date

Time  HH  MM  SS

Sync with NTP Server

Use pre-defined

Use Custom

(Enter NTP Server IP Address/Domain)

No Record
-----------

Sync Status

Screen – Time Settings



## Parameters

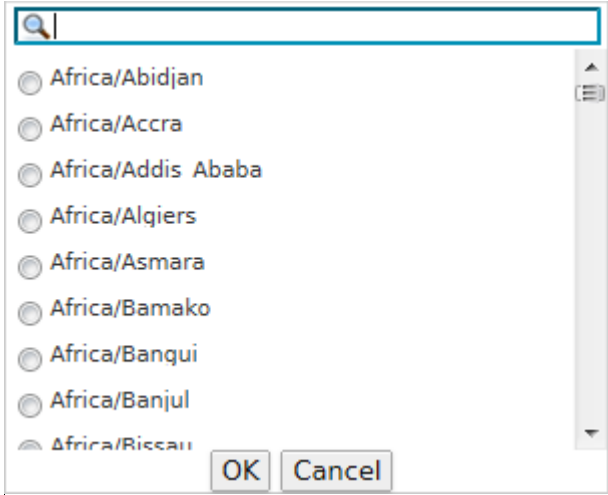

Screen Element	Description
<b>Current Time</b>	Displays the current system time.
<b>Time Zone</b>	<p>Select time zone according to the geographical region in which the Appliance is deployed.</p> 
<b>Set Date &amp; Time</b>	Select to configure the date and time for Appliance's clock.
<b>Date</b>	Specify the date by clicking Calendar  icon.
<b>Time</b>	Specify the time in HH:MM:SS format.
<b>Sync with NTP server</b>	<p>Select to synchronize the Appliance time automatically with an NTP server.</p> <p>NTP stands for Network Time Protocol, and it is an Internet standard protocol used to synchronize the clocks of Appliance to time reference.</p>
<b>Use pre-defined</b>	Select to use the pre-defined NTP servers – asia.pool.ntp.org & in.pool.ntp.org.
<b>Use Custom</b>	<p>Specify the NTP server IP Address or domain name to synchronize time with it. If custom NTP server is defined, time is synchronized with custom server and not with pre-defined servers.</p> <p>Appliances use NTP Version 3 (RFC 1305). One can configure up to 10 NTP servers. At the time of synchronization, it queries each configured NTP server sequentially. When the query to the first server is not successful, Appliance queries second server and so on until it gets a valid reply from one of the NTP servers configured.</p>
<b>Sync Status</b>	Click 'Sync Now' button to synchronize the Cyberoam clock with the NTP Server.

Table – Time Setting screen elements

## Notification

Configure a Mail Server IP Address, Port and Email Address for the Appliance to send and receive alert Emails.

To configure mail server settings, go to **System > Configuration > Notification**.

**Mail Server Settings**

Mail Server IPv4 Address / FQDN\* - Port\*  -  Default - 25

Authentication Required

Username

Password \*\*\*\*\*

Connection Security\*  ▼

Certificate  ▼

---

**Email Settings**

From Email Address\*

Send Notifications to Email Address\*

---

**Email Notification**

IPSec Tunnel UP/Down  Enable

Screen – Mail Server Notification

## Parameters

Screen Element	Description
<b>Mail Server Settings</b>	
<b>Mail Server IPv4 Address/FQDN - Port</b>	Specify the Mail Server IP Address or FQDN and Port number.  Default – 25 if Connection Security is configured as STARTTLS Default – 465 if Connection Security is configured as SSL/TLS
<b>Authentication Required</b>	Enable to authenticate user before sending an Email.  Specify user credentials.
<b>User Name</b>	Specify the User Name, which uniquely identifies user and will be used for login.
<b>Password</b>	Specify the password.

<b>Connection Security</b>	<p>Select Connection Security mode, to be used for establishing a secured connection between SMTP Client and the SMTP Server for SMTP Mail Notification.</p> <p>Available Options:</p> <ul style="list-style-type: none"> <li>• <b>None</b> – Select if your SMTP Server does not support TLS (Transport Layer Security) or a secured connection between SMTP Client and the SMTP Server is not required. If selected, a normal TCP connection is established, without any security.</li> <li>• <b>STARTTLS</b> – SMTP Client establishes a TCP connection with the SMTP Server to learn about the TLS capabilities of the server. If the SMTP Server supports STARTTLS, the connection is upgraded to TLS. If the SMTP Server does not support STARTTLS, the SMTP Client continues to use the normal TCP connection.</li> <li>• <b>SSL/TLS</b> – SMTP Client establishes a TLS connection with the SMTP Server. In case the SMTP Server does not support TLS, no connection is made between the SMTP Client and the SMTP Server.</li> </ul> <p>Default – None</p>
<b>Certificate</b>	<p>Select a Certificate, to be used for authentication by SMTP Client and the SMTP Server.</p> <p>Default - ApplianceCertificate</p>
<b>Email Settings</b>	
<b>From Email Address</b>	Specify the Email Addresses from which the notification is to be mailed.
<b>Send Notifications to Email Address</b>	Specify the Email Address to which the notification is to be mailed.
<b>Email Notification</b>	

<p><b>IPSec Tunnel UP/Down</b></p>	<p>Check to enable receiving of Email notification, if the IPSec VPN tunnel connectivity is lost.</p> <p>Email alerts are sent to Administrator on the configured Email Address. All the IPSec tunnels follow the single central configuration done.</p> <p>An Email is sent only for Host to Host and Site to Site tunnel connections; if it flaps due to one of the following reasons:</p> <ul style="list-style-type: none"> <li>• A peer is found dead (DPD)</li> <li>• Failed to re-establish connection after Dead Peer Detection (DPD)</li> <li>• IPSec Security Association (SA) is expired and is required to be re-established.</li> <li>• IPSec Tunnel comes up without administrator intervention after losing the connectivity</li> </ul> <p>Email shall contain following basic information:</p> <ul style="list-style-type: none"> <li>• IPSec Connection name</li> <li>• IP Addresses of both participating hosts/network</li> <li>• Current state of the IPSec Tunnel connection, viz, Up or Down</li> <li>• Exact Time when the IPSec Tunnel connection was lost</li> <li>• Reason for lost of IPSec Tunnel connection</li> <li>• Appliance Model Number</li> <li>• Firmware version and build number</li> <li>• Appliance Key (if registered)</li> <li>• Appliance LAN IP Address</li> <li>• HA configuration – Primary/Auxiliary (if configured)</li> </ul> <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• An Email is sent for each subnet pair in case of Site to Site connections, having multiple local/remote networks.</li> <li>• An Email sent with respect to IPSec Tunnel coming; do not have any reason mentioned within.</li> <li>• Description of IPSec Tunnel connection is included in the Email, only if the information for same is provided by the Administrator.</li> </ul> </div>
<p><b>Test Mail</b></p>	<p>Click to validate the Sender's and Receiver's Email Address. The Appliance does so by sending a test mail that follows the Sender – Receiver path thereby verifying its validity.</p> <ul style="list-style-type: none"> <li>• From – Email Address of the sender.</li> <li>• To – Email Address of the receiver.</li> <li>• Subject – Subject starting the purpose of the Email.</li> <li>• Body – Message to be sent via Email.</li> </ul>

	<p>Click "Send" button to send the Email.</p> <p>An error message is automatically generated in case the test Email is unsent. The following screen shows the message that is displayed at the bottom left of the console in case such an event occurs.</p> <p>This event is logged as Notice in the <b>Reports &gt; Event</b> section of Cyberoam iView Reports.</p>
--	---

**Table – Mail Server Notification screen elements**

**Status :**  **Failed to connect to the Mail Server. For more information please check**

**Screen – Predefined Authentication Messages**

**Note**





- Mail Server configuration changes automatically when changed from the Network Configuration Wizard and vice versa.

## Messages

























The Messages page allows the Administrator to send messages to the various users. Messages help Administrator to notify users about problems as well as Administrative alerts in areas such as access, user sessions, incorrect password, and successful log on and log off etc.

Messages, up to 256 characters can be sent to a single user or multiple users simultaneously, whenever an event occurs.

To customize the default messages, go to **System > Configuration > Messages**. You can:

- Edit – Click Edit icon  to edit the default message and create a customized message to be displayed to the user.
- Save – Click Save icon  to save the edited message or Cancel icon  to ignore the changes.
- Reset – Click Reset icon  to reset the edited message to the default message.

## Predefined Authentication Messages

Message Key	Message	Manage
<b>Authentication</b>		
User account blocked (AD Policy)	Login failed. Your AD Server account is locked.	
User account disabled (AD Policy)	Login failed. Your account on AD Server is disabled.	
User account expired (AD Policy)	Login failed. Your account on AD Server has expired.	
Clientless User Login Not Allowed	Clientless user is not required to login	
Data Transfer Exhausted	Your data transfer has been exceeded, Please contact the administrator	
Deactive User	You have been deactivated by the Administrator	
Delete User	You have been disconnected.	
Disconnect User	You have been disconnected by Admin.	
Guest User Validity Expired	User validity expired.	
Login not allowed at this time (AD Policy)	Login failed. You are not permitted by AD Server to login at this time.	
Invalid Machine	You are not allowed to login from this machine	
Login not allowed at this workstation (AD Policy)	Login failed. You are not permitted by AD Server to login at this workstation.	
Someone else is logged in from same IP Address	Someone else is logged in from same IP Address	
Logged Off Successful Message	You have successfully logged off	
Logged On Successful Message	You have successfully logged in	
Max Login Limit	You have reached Maximum Login Limit.	
Not Authenticate	The system could not log you on. Make sure your password is correct	
Not Currently Allowed	You are not allowed to login at this time	
User password expired (AD Policy)	Login failed. Your password on AD Server has expired.	
User needs to reset the password (AD Policy)	Login failed. You must reset your AD Server password.	
Logged Off Due To Session Time Out	Your session has timed out. Please log in again.	
Surfing Time Exhausted	You have used up your allotted surfing time, so you have been disconnected from the Internet.	
Surfing Time Expired	Surfing time expired, Please contact the administrator.	
Logout Notification	You will be logged off automatically after sometime. If you wish to continue browsing tap this notification.	
<b>SMTP</b>		
<b>IM</b>		
<b>Administration</b>		
<b>SMS Customization</b>		

Screen – Predefined Authentication Messages

Messages	Description/Reason
<b>Authentication</b>	
<b>User account blocked (AD Policy)</b>	Login failed. Your AD Server account is locked.
<b>User account disabled (AD Policy)</b>	Login failed. Your account on AD Server is disabled.
<b>User account expired (AD Policy)</b>	Login failed. Your account on AD Server has expired.
<b>Clientless User Login Not Allowed</b>	Clientless user is not required to login.
<b>Data Transfer Exhausted</b>	Your data transfer has been exceeded. Please contact the Administrator.
<b>Deactive User</b>	You have been deactivated by the Administrator.
<b>Delete User</b>	You have been disconnected.
<b>Disconnect User</b>	You have been disconnected by Admin.
<b>Guest User Validity Expired</b>	Guest User validity has expired.
<b>Login not allowed at this time (AD Policy)</b>	Login failed. You are not permitted by AD Server to login at this time.
<b>Invalid Machine</b>	Message is sent if User tries to login from the IP Address not assigned to him/her.
<b>Login not allowed at this workstation (AD Policy)</b>	Login failed. You are not permitted by AD Server to login at this workstation.
<b>Someone else is logged in from same IP Address</b>	Message is sent if someone else has already logged with the same IP Address.
<b>Logged Off Successful Message</b>	Message is sent when User logs off successfully.
<b>Logged On Successful Message</b>	Message is sent when User logs on successfully.
<b>Max Login Limit</b>	Message is sent if User has reached the maximum login limit.
<b>Not Authenticate</b>	Message is sent if User name or password is incorrect..
<b>Not Currently Allowed</b>	Message is sent if User is not permitted to access at this time  Access Time policy applied to the User account defines the allowed access time and not allowed access at any other time.
<b>User password expired (AD Policy)</b>	Login failed. Your password on AD Server has expired.



<b>User needs to reset the Password (AD Policy)</b>	Login failed. You must reset your AD Server password.
<b>Logged Off Due To Session Time Out</b>	Message is sent when session has timed out and user is logged of automatically.
<b>Surfing Time Exhausted</b>	<p>Message is sent when User is disconnected because his/her allotted surfing time is exhausted</p> <p>The surfing time duration is the time in hours the User is allowed Internet access that is defined in Surfing time policy. If hours are exhausted, User is not allowed to access.</p>
<b>Surfing Time Expired</b>	Administrator has temporarily deactivated the User and will not be able to log on because User surfing time policy has expired.
<b>Logout Notification</b>	You will be logged off automatically after sometime. If you wish to continue browsing tap this notification.

**Table – Predefined Authentication Message screen elements**

## Predefined SMTP Messages

Message Key	Message	Manage
+ Authentication		
- SMTP		
CTIPD Rejection	Cyberoam Anti Spam has blocked this email because the sender's IP Address is blacklisted.	^ v
CTIPD Temporary Rejection	Cyberoam Anti Spam has blocked this email because the sender's IP Address is temporarily blacklisted.	^ v
Probable Spam Rejection	Cyberoam Anti Spam Engine has identified this email as a bulk email. Ref-id:%REFID%	^ v
Probable Virus Outbreak Rejection	Cyberoam outbreak detection engine has rejected this mail because it seems to be a Virus outbreak.	^ v
Spam Rejection	Cyberoam Anti Spam Engine has identified this email as a spam. Ref-id:%REFID%	^ v
Virus Outbreak Rejection	Cyberoam outbreak detection engine has rejected this mail because it has identified it as a Virus outbreak.	^ v
Email Domain Rejection	Cyberoam Anti Spam has blocked this email because the sender domain has been blocked by the administrator.	^ v
Spam Mail Rejection	Cyberoam Anti Spam has blocked this email because the sender has been blocked by the administrator.	^ v
Mail Header Rejection	Cyberoam Anti Spam has blocked this email because it contains a restricted mime header.	^ v
Mail/Virus Rejection	Cyberoam Anti Virus Engine has rejected this mail because it contains the virus %VIRUSNAME%.	^ v
IP Address Rejection	Cyberoam Anti Spam has blocked this email because the sender IP has been blocked by the administrator.	^ v
Oversized Mail Rejection	Cyberoam Anti Spam has blocked this email because the message size exceeds the maximum allowed size.	^ v
Undersized Mail Rejection	Cyberoam Anti Spam has blocked this email because the message size is less than the allowed size.	^ v
Delivery Notification (to Sender)	Your mail has been sent successfully.	^ v
Attachment Infection	Cyberoam Anti Virus Engine has rejected this mail because it is suspected to have the virus %VIRUSNAME%.	^ v
RBL Rejection	Cyberoam Anti Spam has blocked this email because the sender IP Address is blacklisted.	^ v
Suspected Infection	Cyberoam Anti Virus Engine has rejected this mail because it is suspected to have the virus %VIRUSNAME%.	^ v
+ IM		
+ Administration		
+ SMS Customization		

Screen – Predefined SMTP Messages

Messages	Description/Reason
<b>SMTP</b>	
<b>CTIPD Rejection</b>	Message will be sent when the mail is blocked as sender's IP Address is blacklisted.
<b>CTIPD Temporary Rejection</b>	Message will be sent when the mail is blocked as sender's IP Address is blacklisted temporarily.

<b>Probable Spam Rejection</b>	Message will be sent when mail is suspected as probable spam mail and is rejected.
<b>Probable Virus Outbreak Rejection</b>	Message will be sent when outbreak detection engine rejects mail because it seems to be a Probable Virus outbreak.
<b>Spam Rejection</b>	Message will be sent when spam mail is rejected.
<b>Virus Outbreak Rejection</b>	Message will be sent when outbreak detection engine rejects mail because it is identified as a Virus outbreak.
<b>Email Domain Rejection</b>	Message will be sent when Administrator has blocked the mail sender domain.
<b>Spam Mail Rejection</b>	Message will be sent when Administrator has blocked the mail sender.
<b>Mail Header Rejection</b>	Message will be sent when mail is rejected as it contains a restricted mime header.
<b>Mail/Virus Rejection</b>	Message will be sent when virus infected mail is rejected.
<b>IP Address Rejection</b>	Message will be sent when Administrator has blocked the mail sender IP.
<b>Oversized Mail Rejection</b>	Message will be sent when mail is rejected because message size exceeds the maximum allowed size.
<b>Undersized Mail Rejection</b>	Message will be sent when mail is rejected because the message size is less than the allowed size.
<b>Delivery Notification (to Sender)</b>	Message will be sent to the mail sender when mail is successfully delivered to the receiver.
<b>Attachment Infection</b>	Message will be sent when mail is rejected due to virus infected attachment.
<b>RBL Rejection</b>	Message will be sent when the IP Address from which mail is send is blacklisted.
<b>Suspected Infection</b>	Message will be sent when mail is suspected as virus infected mail and is rejected.

Table – Predefined SMTP Message screen element

## Predefined IM Messages

Message Key	Message	Manage
<input checked="" type="checkbox"/> Authentication		
<input checked="" type="checkbox"/> SMTP		
<input checked="" type="checkbox"/> IM		
File Transfer Block Notification (to sender)	You are not allowed to transfer files to this contact	
Message Block Notification (to sender)	You are not allowed to communicate with this contact	
Privacy Notification To Non-Suspect (on the first message sent from either side)	Cyberoam is monitoring your conversation with this contact	
Privacy Notification To Suspect (After user has logged in)	Cyberoam is monitoring your conversation	
Virus Scan Notification (to sender)	File transferred by you found to be virus infected	( 16:50 , 3:38 )
Webcam Block Notification (to Inviter)	You are not allowed to view/invite for webcam	

Screen – Predefined IM Messages

Messages	Description/Reason
<b>IM</b>	
<b>File Transfer Block Notification (to sender)</b>	Message will be sent when the Administrator has blocked transfer files with this contact.
<b>Message Block Notification (to sender)</b>	Message will be sent when the Administrator has blocked communication with this contact.
<b>Privacy Notification to Non-Suspect (on the first message sent from either side)</b>	Message will be sent once the IM session starts to inform user that their conversation is being monitored with this contact.
<b>Privacy Notification to Suspect (After user has logged in)</b>	Message will be sent as soon as the user logs on to IM to inform users that their conversation is being monitored.
<b>Virus Scan Notification (to sender)</b>	Message will be sent when the file transferred is virus infected.
<b>Webcam Block Notification (to Inviter)</b>	Message will be sent when Administrator has blocked webcam usage.

Table – Predefined IM Message screen element

## Administration Messages

Message Key	Message	Manage
Administration	<p><b>A C C E S S W A R N I N G</b></p> <p>This is a private computer system. Unauthorized access or use is prohibited and only authorized users are permitted. Use of this system constitutes consent to monitoring at all times and user should have no expectation of privacy.</p>	
SMS Customization		

Screen –Administration Message

Messages	Description/Reason
<b>Administration</b>	
<b>Disclaimer Message</b>	<p><b>A C C E S S W A R N I N G</b></p> <p>This is a private computer system. Unauthorized access or use is prohibited and only authorized users are permitted.</p> <p>Use of this system constitutes consent to monitoring at all times and user should have no expectation of privacy.</p> <p>Unauthorized access or violations of security regulations is unlawful and hence if monitoring reveals either of it, appropriate disciplinary action will be taken against the employees violating security regulations or making unauthorized use of this system.</p>

Table – Predefined Administration Message screen elements

## Predefined SMS Customization Messages



Message Key	Message	Manage
+ Authentication		
+ SMTP		
+ IM		
+ Administration		
- SMS Customization		
Default SMS Text	Your Username is "{username}" and Password is "{password}". Your account validity is up to "{expiredate}". We highly recommend you to	

Screen – Predefined SMS Customization Message

Messages	Description/Reason
<b>SMS Customization</b>	
<b>Default SMS Text</b>	Your Username is "{username}" and Password is "{password}". Your account validity is up to "{expiredate}". We highly recommend you to change your password.

Table – Predefined SMS Customization Message screen elements

## Customizing the Default Messages

Click the Edit icon  against the message to be customized, update the message and click the Save icon  to save the edited message.

## Resetting the Customized Messages

Click the Reset icon  against the message to reset it to the default message.

## Configuring Web Proxy Settings

The Appliance can also act as a Web Proxy Server. To use your Appliance as a Web Proxy Server, configure the Appliance's LAN IP Address as a proxy server IP Address in the browser setting and enable access to Web Proxy services from the Appliance Access section.

### Note

- Web Proxy enforces Web and Application Filter policy and Anti Virus policy as configured in User and Firewall Rule.
- IPS policy is applicable on the traffic between proxy and WAN, but not between user and proxy.
- QoS policy is not applicable on the direct proxy traffic.

To configure Web Proxy settings, go to **System > Configuration > Web Proxy**.

The screenshot displays the Web Proxy configuration interface. At the top, the 'Web Proxy Port' is set to 3128. Below this, the 'Trusted Ports' section features a search and add input field, an 'Add' button, and a scrollable list of ports. The list includes 21, 70, 80, 88, 210, 443, 563, and 1025-65535. Each port entry has a small 'X' icon for deletion. An 'Apply' button is located at the bottom of the list.

Screen – Web Proxy Settings

### Parameters


Screen Element	Description
<b>Web Proxy Port (Applicable only when the Appliance is configured as Web Proxy)</b>	Specify the Port number which is to be used for Web Proxy.  Default – 3128
<b>Trusted Ports</b>	Appliance allows the access to those sites which are hosted on standard ports, only if deployed as Web Proxy. To allow access to the sites hosted on the non-standard ports, you have to define non-standard ports as trusted ports.  Click Add button to add the HTTP trusted ports and Cancel icon  to delete the trusted ports.

Table – Web Proxy Settings screen elements

## Enabling and Configuring Parent Proxy

Parent Proxy is essential when it is required that the Internet access is to be routed through a government-approved proxy server. In this situation, it is necessary that the security Appliance routes the user access request through that government-approved proxy server. The Appliance may be deployed as Parent Proxy either within (LAN) or outside (WAN) the network.

Enable Parent Proxy when the web traffic is blocked by the upstream Gateway. When enabled all the HTTP requests will be sent to web parent proxy server via Appliance.

To configure Parent Proxy settings, go to **System > Configuration > Parent Proxy**. Specify IP Address or FQDN, Port, Username and Password, if Parent Proxy is enabled.

**IPv4 Parent Proxy**

Parent Proxy  Enable

Domain Name/IPv4 Address \*

Port \*

Username

Password

---

**IPv6 Parent Proxy**

Parent Proxy  Enable

Domain Name/IPv6 Address\*

Port \*

Username

Password

**Screen – Parent Proxy Settings**

### Parameters

Screen Element	Description
<b>IPv4 Parent Proxy</b>	
<b>Parent Proxy</b>	Click to enable the Parent Proxy if the web traffic is blocked by the upstream Gateway.



	If enabled, the Appliance forwards all the HTTP requests to parent proxy server.
<b>Domain Name/IPv4 Address</b>	Specify the Domain Name or IPv4 Address for the Parent Proxy.
<b>Port</b>	Specify the Port number, which is to be used for Parent Proxy.  Default – 3128
<b>Username &amp; Password</b>	Specify the Username & Password for authentication.
<b>IPv6 Parent Proxy</b>	
<b>Parent Proxy</b>	Click to enable the Parent Proxy if the web traffic is blocked by the upstream Gateway.  If enabled, the Appliance forwards all the HTTP requests to parent proxy server.
<b>Domain Name/IPv6 Address</b>	Specify the Domain Name or IPv6 Address for the Parent Proxy.
<b>Port</b>	Specify the Port number, which is to be used for Parent Proxy.  Default – 3128
<b>Username &amp; Password</b>	Specify the Username & Password for authentication.

Table – Parent Proxy Setting screen elements

## Configuring Captive portal

Appliance provides flexibility to customize the Captive portal Login page. This page can include your organization name and logo.

To customize the Captive portal page, go to **System > Configuration > Captive portal**.

Appliance also supports customized page in languages other than English.

**General Settings**

Logo  Default  Custom  No file selected. Size 125x70 pixels

Logo URL\*

Page Title\*

Login Page Header  HTML Input

Login Page Footer  HTML Input

Username Caption\*  HTML Input

Password Caption\*  HTML Input

Login Button Caption\*

Logout Button Caption\*

My Account Link Caption\*

---

**Color Scheme**

Background Color   Header, Footer Font Color

Page Title Background Color   Page Title Font Color

Caption Font Color

---

**Custom HTML Template**

Use Custom HTML Template

HTML Text 

```

margin-bottom:15px;
}
div#__loginbox a{
margin-bottom:15px;
}
</style>
</head>
<body >
<center>

<div>
<h3>{company_logo}</h3>
<h2>Captive Portal</h2>
<div id="__loginbox"></div>
</div>
</center>

```

Screen – Captive Portal Settings

Parameters

Screen Element	Description
<b>General Settings</b>	
<b>Logo</b>	To upload the custom logo, specify Image file name to be uploaded else click “Default”.  Use Browse to browse and select the complete path.  The image size should not exceed 125 X 70 pixels.
<b>Logo URL</b>	Provide a URL to be redirected to on clicking the Logo.  Default - <a href="http://www.cyberoam.com">http://www.cyberoam.com</a> .
<b>Page Title</b>	Provide a page title.

	Default - Cyberoam User Portal
<b>Login Page Header</b>	Provide the text to be displayed as header on the Captive Portal login page.
<b>Login Page Footer</b>	Provide text to be displayed as footer on the Captive Portal login page.
<b>User Name Caption</b>	Provide label for the user name textbox to be displayed on the Captive Portal login page.  Default - User Name
<b>Password Caption</b>	Provide label for the password textbox to be displayed on the Captive Portal login page.  Default - Password
<b>Login Button Caption</b>	Provide label for the login button to be displayed on the Captive Portal login page.  Default – Login
<b>Logout Button Caption</b>	Provide label for the logout button to be displayed on the Captive Portal login page.  Default - Logout
<b>My Account Link Caption</b>	Provide a text to be displayed for My Account login page link. By clicking the link, user will be directed to the My Account login page.  Default - Click here for User My Account
<b>Color Scheme</b>	
Customize the color scheme of the Captive portal if required. Specify the color code or click the square box to pick the color.	
<b>Custom HTML Template</b>	
<b>Use Custom HTML Template</b>	Enable to fully customize captive portal using custom HTML code.
<b>HTML Text</b>	Provide HTML code to render captive portal according to your requirement. Dynamic contents like banners from external web servers, customizable “Message of the day” box and so on can be integrated in the HTML code.  By default, sample HTML will be displayed.  <b>Note</b> <ul style="list-style-type: none"> <li>It is essential to have one HTML div element in the HTML text. Cyberoam’s Login box will be placed in this div element.</li> </ul>
<b>Preview Button</b>	Click to view the custom settings before saving the changes.

---

<b>Reset to Default Button</b>	Click to revert to the default settings.
--------------------------------	--

**Table – Captive Portal Setting screen elements**

## Theme

Theme page provides a quick way to switch between predefined themes for Web Admin Console. Each theme comes with its own custom skin, which provides the color scheme and font style for entire Web Admin Console i.e. navigation frame, tabs and buttons.

To change the theme, go to **System > Configuration > Theme**.

## Maintenance

Maintenance facilitates handling the backup and restore, firmware versions, licensing, services and update. The Administrator can take manual backup and alternately, automatic backup can be scheduled on regular intervals.

Backup stored on the system can be restored anytime from Backup & Restore page.

The Administrator can upload a new firmware image, boot from firmware or reset to the configuration to factory defaults. Firmware image can be downloaded from the relevant sites. Maximum of two firmware images are available simultaneously.

- [Backup & Restore](#)
- [Firmware](#)
- [Licensing](#)
- [Services](#)
- [Update Definitions](#)
- [Import Export](#)

## Backup & Restore

Backup is the essential part of data protection. No matter how well your system is treated, no matter how much it is taken care of, you cannot guarantee that your data is safe, if it exists only at one place.

Backups are necessary in order to recover data from the loss due to the disk failure, accidental deletion or file corruption. There are many ways of taking backup and just as many types of media to use as well.

Backup consists of all the policies and all other user related information.

Appliance facilitates to take back-up only of the system data, either through scheduled automatic backup or using a manual backup.

Once the backup is taken, the file for restoring the backup must be uploaded.

### Note

- Restoring data older than the current data results to the loss of current data.

To backup and restore data, go to **System > Maintenance > Backup & Restore**, You can:

- [Backup & Restore](#)
- [Schedule Backup](#)

Backup	
Backup Mode	<input checked="" type="radio"/> Local <input type="radio"/> FTP <input type="radio"/> Email
Backup Prefix	<input type="text"/>
Backup Frequency	<input checked="" type="radio"/> Never <input type="radio"/> Daily <input type="radio"/> Weekly <input type="radio"/> Monthly
	<input type="button" value="Apply"/> <input type="button" value="Backup Now"/> <span style="margin-left: 20px;">Last backup taken on Thu 18 Sep 2014 16:34:31</span> <input type="button" value="Download Now"/>
Backup Restore	
Restore Configuration	<input type="button" value="Browse..."/> No file selected.
	<input type="button" value="Upload and Restore"/>

Screen – Backup and Restore

Screen Element	Description
<b>Backup</b>	
<b>Backup Mode</b>	Select how and to whom backup files should be sent.  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• <b>Local</b> – Backup is taken and stored on the Appliance itself.</li> <li>• <b>FTP</b> – configure FTP server IP Address (IPv4/IPv6) and login credentials.</li> <li>• <b>Email</b> – configure Email ID on which backup is to be mailed.</li> </ul>
<b>Backup Prefix</b>	Specify backup file name (prefix). The backup file name format is as follows: <ul style="list-style-type: none"> <li>• <b>With Prefix:</b> &lt;Prefix&gt;_Backup_&lt;Appliance Key&gt;_&lt;timestamp&gt;</li> <li>• For example:               <ul style="list-style-type: none"> <li>• Dallas_Backup_ABCDEY190_26Nov2014_12.09.24</li> <li>• NY_Backup_ABCDEY190_26Nov2014_12.09.24</li> </ul> </li> <li>• <b>Without Prefix(Default):</b> Backup_&lt;Appliance Key&gt;_&lt;timestamp&gt;</li> <li>• For example:               <ul style="list-style-type: none"> <li>• Backup_ABCDEY190_26Nov2014_12.09.24</li> <li>•</li> </ul> </li> </ul> If prefix is not provided, the default format is used for backup file.
<b>Backup Frequency</b>	Select the system data backup frequency.  We recommend to schedule the backup on a regular basis. To determine the backup frequency, consider how much information is added or modified regularly.


	<p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Never</b> – Backup will not be taken at all.</li> <li>• <b>Daily</b> –Backup will be taken every day.</li> <li>• <b>Weekly</b> –Backup will be taken every week.</li> <li>• <b>Monthly</b> –Backup will be taken every month.</li> </ul> <p><b>Schedule</b></p> <p>Specify the day/date and time for Daily, Weekly and Monthly backup.</p>
<b>Backup Now</b>	Click to take the backup of system data till date.
<b>Download Now</b>	Click to download the latest backup that is available for uploading.
<b>Backup Restore</b>	
<b>Restore Configuration</b>	<p>To restore the configuration, specify configuration to be uploaded.</p> <p>Use Browse button to select the complete path.</p>

**Table – Backup and Restore screen elements**



## Firmware

**System > Maintenance > Firmware** page displays the list of available firmware versions downloaded. A Maximum of two firmware versions are available simultaneously and one of the two firmware versions is active i.e. the firmware is deployed.

**Upload firmware**  – The Administrator can upload a new firmware. Click to specify the location of the firmware image or browse to locate the file. You can simply upload the image or upload and boot from the image. The uploaded firmware can only be active after the next reboot. The existing firmware then will be removed and the new firmware will be available.

In case of Upload & Boot, firmware image is uploaded and upgraded to the new version, closes all sessions, restarts, and displays the login page. This process may take few minutes since the entire configuration is also migrated in this process.


**Boot from firmware**  – Option to boot from the downloaded image and activate the respective firmware.

**Boot with factory default configuration**  – Appliance is rebooted and loads default configuration.

### Note

- Entire existing configuration will be lost, if this option is selected.

**Active**  - Active icon against a firmware suggests that the Appliance is using that firmware.

Version	Active	Manage
10.04.5 build 007		  
10.6.1 RC-2		 

Screen – Manage Firmware

At the time of uploading new firmware, error “New Firmware could not be uploaded” might occur due to one of the following reasons:

**Wrong upgrade file** - You are trying to upload wrong upgrade file i.e. trying to upload version 9.x upgrade on version X Appliances. Download the upgrade file specific to your Appliance model and version from <https://customer.cyberoam.com>.

**Incorrect firmware image** - You are trying to upload an incorrect firmware image for your Appliance model. All the firmware's are model-specific firmware and are not inter-changeable. Hence, firmware of one model is not applicable on another model. For example, an error is displayed, if Appliance model CR25ia is upgraded with firmware for model CR50ia.

**Incompatible firmware** - You are trying to upload incompatible firmware. For compatibility issues, refer the Compatibility Annotations section in Release Notes of the version before trying to upload.

**Mismatch in Registration information** - Registration information of the Appliance and Customer My Account are not matching.

**Changes in Appliance Hardware** - Appliance Hardware configuration is not the standard hardware configuration. Contact support for assistance.

**Image with incorrect MD5 checksum** – There are chances that the firmware you have downloaded has got corrupted during the downloading process. Download it again and compute MD5 checksum of the

downloaded firmware. Compare computed checksum with the checksum published on the <http://download.cyberoam.com/checksum>. In case of mismatch, download the file again.

## Licensing

Appliance consists of two (2) types of modules:

- **Basic module** – Firewall, VPN, SSL VPN, Bandwidth Management, Multi Link Manager and Reports.
- **Subscription modules** – Web and Application Filter, IPS, Gateway Anti Virus, Gateway Anti Spam, 8 x 5 Support, 24 x 7 Support, WAF and Outbound Spam Protection. All the appliance models may not support subscription modules. Please refer to [Subscription Matrix](#) for details.

Basic Module is pre-registered with the Appliance for the indefinite time period usage while Subscription Modules are to be subscribed before use.


You can [subscribe](#) to any of the subscription modules:

- without key for free 15-days trial subscription
- with key

On deployment, Appliance is considered to be unregistered and all the modules as unsubscribed. You need to register the Appliance if you want to

- Avail 8 X 5 support
- Subscribe to any of the subscription modules
- Subscribe for free trial of any of the subscription modules
- Register for 24 X 7 support

Select **System > Maintenance > Licensing** to view the Appliance registration details and various modules' subscription details. The various status of the Appliance is described below:

- Registered – Appliance is registered
- Unregistered – Appliance is not registered
- Subscribed -- Module is subscribed
- Unsubscribed – Module is not subscribed. Subscription icon  against the module in the navigation menu indicates that the module is not subscribed. Click the subscription icon to navigate to the Licensing page and follow the screen steps to subscribe. Alternately, browse to <http://customer.cyberoam.com> to subscribe the module.
- Trial – Trial subscription
- Expired – Subscription expired

To manage the licensing options, go to **System > Maintenance > Licensing**. You can:

- [View Appliance Registration Details](#)
- [Manage Module Subscription Online](#)
- [View Module Subscription Details](#)
- Synchronize – Click 'Synchronize' button, once the Appliance or modules are registered online. The details of Appliance and subscription modules are automatically synchronized with Customer My Account and the updated details are displayed on the Licensing Page.

Appliance Registration Details		
Model	CR35iNG (C127900005-868DBB)	
Company Name	Cyberoam	
Contact Person	Joseph Vaz Ph: 959959959	
Registered Email Address	joseph.vaz@cyberoam.com	
Manage Module Subscription Online		
Synchronize Licenses with Customer My Account	<input type="button" value="Synchronize"/>	
To register appliance, update or renew modules go to <a href="http://customer.cyberoam.com/">http://customer.cyberoam.com/</a>		
To subscribe for Trial version of modules go to <a href="http://customer.cyberoam.com/">http://customer.cyberoam.com/</a>		
Module Subscription Details		
Module	Status	Expiration Date
Web and Application Filter	Trial	Tue 31 Dec 2013
IPS	Trial	Tue 31 Dec 2013
Gateway Anti Virus	Trial	Tue 31 Dec 2013
Gateway Anti Spam	Trial	Tue 31 Dec 2013
8 x 5 Support	Expired	-
24 x 7 Support	Unsubscribed	-
WAF	Trial	Tue 31 Dec 2013
Outbound Spam Protection	Subscribed	Tue 31 Dec 2013

### Screen – Licensing

#### Viewing the Appliance Registration Details

Screen Element	Description
<b>Appliance Registration Details</b>	
<b>Model</b>	Displays Appliance Model number which is registered and its Appliance key e.g. CR35iNG (C127900005-868DBB)
<b>Licensed Users (if applicable)</b>	Number of user licenses purchased
<b>Company Name</b>	Name of the company under which the Appliance is registered
<b>Contact Person</b>	Name of the contact person in the company
<b>Registered Email Address</b>	Email Address used for Appliance registration.

Table – Licensing screen elements

#### Manage Module Subscription Online

If the Appliance is not registered, browse to <http://customer.cyberoam.com> to register.

To register the Appliance, you need to create a Customer Account. You can create customer account and register the Appliance in a single step. Once the Appliance is registered, subscribe other modules for the trial or with license keys.

You can subscribe to following modules:

- Web and Application Filter
- IPS
- Gateway Anti Virus
- Gateway Anti-spam
- 8 X 5 Support
- 24 X 7 Support
- WAF
- Outbound Spam Protection

Once the Appliance is registered or subscribed for any module, if the details are not synchronized, Web Admin console do display the updated subscription details.

### Viewing the details of Module Subscription

Screen Element	Description
<b>Module Subscription Details</b>	
<b>Module</b>	Module that can be subscribed.
<b>Status</b>	Status of the module – Registered, Unregistered, Subscribed, Unsubscribed, Trial, Expired.
<b>Expiration Date</b>	Module subscription expiry date.

**Table – Module Subscription screen elements**

## Services

You can view the current status and manage all the configured services:

- Anti Spam
- Anti Spam Center Connectivity
- Anti Virus
- Authentication
- DNS Server
- IPS
- Web Proxy
- WAF – Available in all the models except CR15iNG and CR15wiNG
- DHCP Server
- DHCPv6 Server
- Router Advertisement Service

To manage various services, go to **System > Maintenance > Services**.

Services	Status	Manage
Anti Spam Anti Spam Center Connectivity	Running Connected	Stop
Anti Virus	Running	Stop
Authentication	Running	Restart
DNS Server	Running	Stop
IPS	Running	Stop
Web Proxy	Running	Restart
DHCP Server	Running	Stop
DHCPv6 Server	Stopped	Start
Router Advertisement Service	Stopped	Start

Screen – Manage Services

### Parameters

- **Services** - Name of the configured service.
- **Status** - Current status of the service
- **Manage** - Click to start or stop or restart the respective service.

### Action table

Button	Usage
Start	Start the service whose status is 'Stopped'.
Stop	Stop the service whose status is 'Started'.
Restart	Restart service: Only for Authentication Service and Web Proxy Service.

**Status table**

<b>Status</b>	<b>Description</b>
<b>No Web Server configured</b>	No Web Server is configured. If web server is not configured, Start button will be disabled.
<b>Connected</b>	When Internet connectivity is available for the Gateway.
<b>Running</b>	Service has successfully started.
<b>Disconnect</b>	When Internet connectivity unavailable for the Gateway.
<b>Stopped</b>	When a service is stopped.

## Updates

The Updates page allows the administrator to configure automatic updates for Anti Virus definitions, IPS Signatures and Web category database. Definitions can be updated from Central Server or CCC. Alternately, these definitions can also be updated manually from this page itself.

To enable automatic updates, go to **System > Maintenance > Updates** and click against the required checkbox followed by Apply.

Updates Status					
Module	Version	Last Update Status	Last Update Mode	Auto Update	Update Now
Anti Virus Definition	7.11.149.250	Successfully on Fri 16 May 2014 15:08:42	Automatic	<input checked="" type="checkbox"/>	<input type="button" value="Update Now"/>
IPS Signatures	3.11.65	Upgrade not Available on Fri 16 May 2014 00:35:01	Automatic	<input checked="" type="checkbox"/>	<input type="button" value="Update Now"/>
Application Signatures	4.11.65	Upgrade not Available on Fri 16 May 2014 00:35:01	Automatic	<input checked="" type="checkbox"/>	<input type="button" value="Update Now"/>

Manual Signature Updates	
Upload File	<input type="button" value="Choose File"/> No file chosen
<input type="button" value="Upload"/>	

Over-the-air Hotfix and Product Improvement Program	
<input checked="" type="checkbox"/> Allow Over-the-air Hotfix	
<input checked="" type="checkbox"/> Participate in the Product Improvement Program	<p>We, at Cyberoam, know that the best products are the ones our customers can use to their fullest potential and satisfy their requirements. Cyberoam continuously strives to understand and anticipate customer needs in order to deliver world-class products.</p> <p>In order to achieve this goal, Cyberoam has implemented this program to continuously improve the product. This program is designed solely to benefit our customers.</p> <p>Through this program, we seek user participation to allow us to collect the appliance hardware, configuration, and usage statistics periodically in the encrypted form.</p> <p>Participation in the program is voluntary, and the end results are product improvements to better meet the needs of our customers.</p> <p>Click <a href="#">here</a> to view details of the program.</p>
<input type="button" value="Apply"/>	

### Screen – Manage Updates

#### Manual Updates Parameters

Screen Element	Description
<b>Updates Status</b>	
<b>Module</b>	Module name whose definitions can be updated.
<b>Version</b>	Version number of the Module
<b>Last Update Status</b>	Status along with date of the last update: Successful or Failure
<b>Last Update Mode</b>	Mode of the Last update: Automatic or Manual
<b>Auto Update</b>	To update module definitions automatically, select “Auto Update” as “ON”.
<b>Update Now Button</b>	Click ‘Update Now’ button to update the module definitions.
<b>Manual Signature Updates</b>	
<b>Upload File</b>	To update signature manually, browse and upload the file.
<b>Over-the-air Hotfix and Product Improvement Program</b>	
<b>Allow Over-the-air Hotfix</b>	<p>Hotfixes are applied automatically if available. Disable if you do not want to apply hotfix.</p> <p>Default - Enable</p>



<b>Participate in the Product Improvement Program</b>	<p>Cyberoam has designed and implemented Product Improvement Program to benefit its customers and to continuously improve the product. Through this program, we seek user participation to allow us to collect the appliance hardware, configuration, and usage statistics periodically in the encrypted form.</p> <p>Participation in the program is voluntary and disable this option if you do not want to participate.</p> <p>Click <a href="#">here</a> to view details of the program.</p> <p>Default - Enable</p>
---	--

**Table – Manage Updates screen elements**

## Import Export

Cyberoam provides backup-restore feature which allows to create a copy of the appliance configuration and restore it on same or other compatible appliance. However, the contents within the backup file are encrypted and hence cannot be updated before restoring it on the appliance.

Import Export page allows administrator to export appliance configuration to a text file and import configuration from a text file to appliance. The contents of the text file are in human readable XML format and hence the contents could be updated offline. Administrator can export configuration to a text file and import it on another compatible appliance after updating the configurations. Administrators can also choose to export all/few of the appliance configurations.

This feature will be useful when importing configuration settings on large number of appliances.

Screen – Import Export

### Import Export Parameters

Screen Element	Description
<b>Import</b>	
<b>Import File</b>	Use Browse button to select the complete path of the tar file to be imported.
<b>Import Type</b>	Select import type.  Available options: <ul style="list-style-type: none"> <li>• Preserve existing configuration – Existing configuration of the Appliance will be preserved and new configurations will also be imported.</li> <li>• Overwrite existing configuration – Existing entity configuration on the appliance will be overwritten with the entity configuration in the imported tar file.</li> </ul>
<b>Import</b>	Click to import the configuration on the appliance.
<b>Export</b>	

<b>Export full configuration</b>	Select to export all the entities configuration to a text file.
<b>Export selective configuration</b>	<p>Select to export only selected entities configuration. Entities can be selected from the drop-down menu.</p> <p>Dependent entities for the selected entity will also be exported.</p> <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>While exporting configuration for FQDN Host/IP Host/Country Host, their groups will not be exported even though "Include dependent entity" is selected. To export both IP Hosts and IP Host Group, one can export IP Host Group or select to export both IP Host and IP Host Group.</li> </ul> </div> <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>While exporting configuration for SSL VPN Policy/L2TP Configuration/PPTP Configuration, users and users groups added will not be exported even though "Include dependent entity" is selected. To export both configuration and its members, one can export users or select to export both SSL VPN Policy/L2TP Configuration/PPTP Configuration and Users.</li> </ul> </div>
<b>Export</b>	Click to export the configuration.

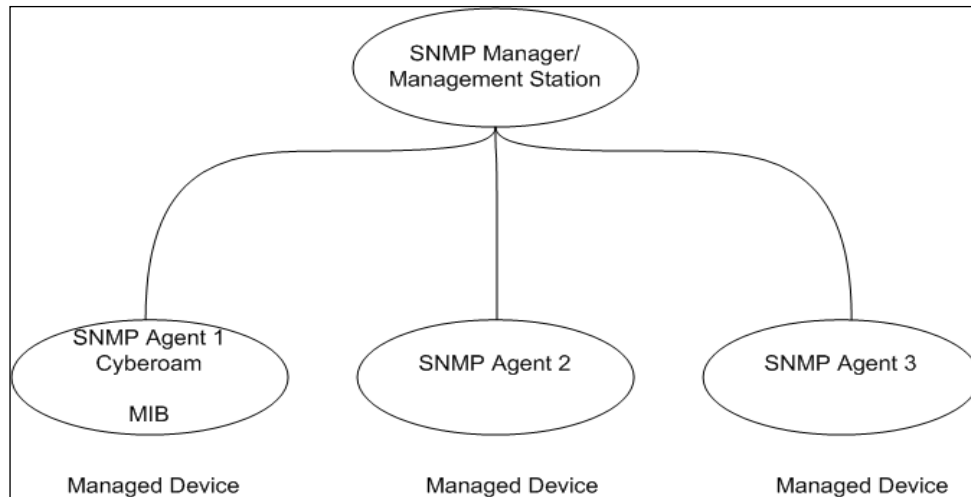
**Table – Import Export screen elements**

**Note**

- While exporting/importing configuration is in process, one cannot perform backup/restore operations.
- The export and import files are of .tar extension. Example: API-1421656341945133.tar
- Configuration exported from appliance with higher firmware versions cannot be imported on lower versions.
- The destination Cyberoam appliance on which configuration is to be imported must have the same or greater number of ports than the source appliance from which configuration is exported.

## SNMP

Simple Network Management Protocol (SNMP) is used as the transport protocol for network management. Network management consists of a station or manager communicating with network elements such as hosts, routers, servers, or printers. The agent is the software on the network element (host, router, printer) that runs the network management software. In other words, the agent is a network element. The agent will store information in a Management Information Base (MIB). Management software will poll the various network elements/agents and get the information stored in them. The manager uses UDP port 161 to send requests to the agent and the agent uses UDP port 162 to send replies or messages to the manager. The manager can ask for data from the agent or set variable values in the agent. Agents can reply and report events.



SNMP collects information two ways, if SNMP agent is installed on the devices:

- The SNMP Management Station/Manager will poll the network devices/agents
- Network devices/agents will send trap/alert to SNMP management station/Manager.

### SNMP terms

- **Trap** – An alert that is sent to a management station by agents.
- **Agent** – A program at devices that can be set to watch for some event and send a trap message to a management station if that event occurs
- **SNMP community** – An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities.

Use SNMP to configure agent, community and the SNMPv3 users. Appliance supports SNMPv1 & SNMPv2c protocols. Agent configuration page is used to configure agent name, agent port and the contact person for the program. The community page is used for adding, managing and deleting the communities for protocols SNMPv1 and SNMPv2c. Use SNMPv3 user page to add, manage and delete v3 users. Apart from IPv4 Addresses, SNMP now supports IPv6 Addresses also.

## Agent Configuration

Use Agent configuration page to configure SNMP agents. The configuration details include name, description, location, contact person, agent port and manager port.

To configure agents, go to **System > SNMP > Agent Configuration**.

Screen – Agent Configuration

### Parameters

Screen Element	Description
Enable SNMP Agent	Select to enable SNMP Agent.
Name	Specify a name to identify the agent.
Description	Agent Description
Location	Specify the physical location at which the Appliance is deployed.
Contact Person	Specify the contact information for the person responsible for the maintenance of above specified Appliance.
Agent Port	Specify the port which the Appliance should use to send traps.  Default - 161
Manager Port	Remote SNMP Management station/Manager uses this port to connect to the Appliance.  Default - 161

Table – Agent Configuration screen elements

## Community

Community is a group of SNMP Managers and an SNMP Agent may belong to one or more than one community. An Agent does not respond to requests from a management station(s) that does not belong its communities.

Each Community can support SNMPv1, SNMPv2c or both. The Appliance sends traps to all the communities. You must specify a trap version for each community.

This page provides a list of all the communities added and you can sort the list based on community name. The page also provides the option to add a new community, update the parameters of the existing community, or delete the community.

## Manage Communities

To configure communities, go to **System > SNMP > Community**.


		Protocol Version		Trap			
<input type="checkbox"/>	Name ▲	Source	v1	v2c	v1	v2c	Manage
<input type="checkbox"/>	<u>test</u>	10.101.1.1	Yes	No	No	No	

Screen – Manage Communities

Screen Element	Description
<b>Name</b>	Name of the community.
<b>Source</b>	IP Address of the SNMP Manager that can use the settings in the SNMP community to monitor the Appliance.
<b>Protocol Version</b>	Configured SNMP protocol version support v1 or v2c.
<b>Trap</b>	Configured trap support- v1 or v2c. Traps will be sent to the SNMP Managers who support the specified versions only.

Table – Manage Communities screen elements

## Adding a new SNMP Community

To add or edit a community, go to **System > SNMP > Community** and click the Add button . To update the details, click on the Community or Edit icon  in the Manage column against the community you want to modify.



The screenshot shows a dialog box titled "Add Community" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Name \***: A text input field.
- Description**: A text area with a vertical scrollbar.
- IP Address \***: A text input field.
- Protocol Version \***: Two radio button options,  v1 and  v2c.
- Trap Support**: Two radio button options,  v1 and  v2c.
- At the bottom, there are two buttons: **OK** and **Cancel**.

Screen – Add Community

## Parameters

Screen Element	Description
<b>Name</b>	Enter the name to identify the community.
<b>Description</b>	Enter the community description.
<b>IP Address</b>	Specify IP Address (IPv4/IPv6 Address) of the SNMP Manager that can use the settings in the SNMP community to monitor the Appliance.
<b>Protocol Version</b>	Enable the required SNMP protocol version support.  SNMP v1 and v2c compliant SNMP managers have read-only access to Appliance system information and can receive Appliance traps.
<b>Trap Support</b>	Enable the required version for trap support.  Traps will be sent to the SNMP Managers who support the specified versions only.

Table – Add Community screen elements

## V3 User

SNMP version 3 has the capability of using authentication. Only the authenticated user can request the information.

This page displays the list of all the v3 users. The page provides the option to add a new v3 user, update the password of the user, or delete the user.

### Manage v3 Users

To manage v3 users, go to **System > SNMP > v3 User**.

<input type="checkbox"/>	User Name	Manage
<input type="checkbox"/>	Test	

Screen – Manage v3 Users

Screen Element	Description
User Name	User name of the v3 user.

Table – Manage v3 Users screen elements

### Adding a new V3 User

To add or edit a v3 user, go to **System > SNMP > v3 User**. Click the Add button to add a new v3 user.

To update the details, click on the v3 user or Edit icon in the Manage column against the v3 user you want to modify.

**Add V3 User** [X]

Name \*

Password \*

Confirm Password

OK Cancel

Screen – Add v3 User

### Parameters

Screen Element	Description
Name	Specify a name to identify the v3 user.
Password	Provide a password for authentication.
	Confirm the password for authentication.

Table – Add v3 User screen elements



## Certificate

A digital certificate is a document that guarantees the identity of a person or entity and is issued by the Certificate Authority (CA). Certificates are generated by the third party trusted CA. They create certificates by signing public keys and identify the information of the communicating parties with their own private keys. This way it is possible to verify that a public key really belongs to the communicating party only and not been forged by someone with malicious intentions.

A certificate signed by a Certificate Authority (CA) identifies the owner of a public key. Each communicating party may be required to present its own certificate signed by a CA verifying the ownership of the corresponding private key. Additionally, the communicating parties need to have a copy of the CA's public key. In case private key is lost or stolen or the information is changed, CA is responsible for revoking the certificate. CA also maintains the list of valid and revoked certificates.

To use Certificates for authentication, you must have valid CA and a certificate. You need to upload CA if you are using external CA. You also require to upload the certificate. You can generate a self signed certificate if you want to use it as CA.

You can also use Appliance to act as a certificate authority and sign its own certificates. This eliminates the need of having your own certificate authority. If you are using Appliance as CA, you have to generate a self-signed certificate, which can be used in various VPN policies.

- [Certificate](#)
- [Certificate Authority](#)
- [CRL](#)

## Certificate

Certificate page allows you to generate self-signed certificate, upload certificate or generate certificate signing request (CSR). This page also facilitates you to manage certificates, which involve updating and regenerating, revoking, downloading and deleting certificates.

You can use Appliance to act as a certificate authority and sign its own certificates. This eliminates the need of having your own certificate authority.

If Appliance is used as CA, you have to generate a self-signed certificate, which can be used in various VPN policies.

If you are using a third party CA, you have to submit a request to CA for issuing a certificate. Once CA issues a certificate, you have to upload to use it in VPN policy.

## Manage Certificates

To manage certificates, go to **System > Certificate > Certificate**.


- Revoke – Click to revoke self-signed certificate if lost, stolen or updated.
- Download – Click to download the self-signed certificate or CSR.

<input type="checkbox"/>	Name	Valid From	Valid Upto	Authority	Type	Manage
<input type="checkbox"/>	ApplianceCertificate	2012-11-01	2036-12-31	✓	Upload	
<input type="checkbox"/>	<a href="#">Client_Certificate</a>	2013-01-03	2013-01-04	✓	Self Signed	
<input type="checkbox"/>	<a href="#">Server_Certificate</a>	2013-01-03	2013-01-04	✓	Self Signed	

Screen – Manage Certificate

## View the list of Certificates

Screen Element	Description
<b>Name</b>	Name of the Certificate
<b>Valid From</b>	Valid activation date for the certificate
<b>Valid Up To</b>	Certificate expiry date
<b>Authority</b>	Certificate Authority if applicable. ✓ - If the Certificate Authority is available. ✗ - If the Certificate Authority is not available
<b>Type</b>	Certificate Type – self-signed or certificate signing request (CSR) or Upload (third party certificate)
<b>Download Icon</b>	Click Download Icon  to download Certificate. Only self signed certificate and certificate signing request can be downloaded.

<p><b>Revoke Icon</b></p>	<p>Click Revoke Icon  to revoke self-signed certificate if lost, stolen or updated.</p> <p>Revoked certificate is automatically added to the Certificate Revocation List (CRL). You can download revoked certificate and circulate if required.</p>
---------------------------	--

**Table – Manage Certificate screen element**

## Adding a new Certificate

To add or edit certificates, go to **System > Certificate > Certificate**. Click Add Button to add a new certificate or Edit Icon to modify the details of the certificate.

Action \*  Upload Certificate  Generate Self Signed Certificate  Generate Certificate Signing Request (CSR)

Name \*

Certificate File Format \*  ▼

Certificate \*   File should be in PEM (.pem) format.

Private Key \*   File should be in .key format.

Passphrase \*

Confirm Passphrase

**Screen – Add Certificate (Upload Certificate)**

Action \*  Upload Certificate  Generate Self Signed Certificate  Generate Certificate Signing Request (CSR)

Name \*

Valid From \*  C

Valid Upto \*  C

Key length \*  ▼

Key Encryption  Enable

Certificate ID \*  ▼

**Identification Attributes**

Country Name \*  ▼

State \*

Locality Name \*  (eg. city name)

Organization Name \*  (eg. company name)

Organization Unit Name \*  (eg. department name)

Common Name \*  (eg. server's hostname)

Email Address \*


**Screen – Add Certificate (Generate Self Signed Certificate)**

Action *	<input type="radio"/> Upload Certificate	<input type="radio"/> Generate Self Signed Certificate	<input checked="" type="radio"/> Generate Certificate Signing Request (CSR)
Name *	<input type="text"/>		
Valid Upto *	<input type="text" value="2013-01-09"/>	<input type="button" value="C"/>	
Key length *	<input type="text" value="512"/>	<input type="button" value="v"/>	
Encryption	<input type="checkbox"/> Enable		
Certificate ID *	<input type="text" value="DNS"/>	<input type="button" value="v"/>	<input type="text"/>
<b>Identification Attributes</b>			
Country Name *	<input type="text" value="Andorra"/>	<input type="button" value="v"/>	
State *	<input type="text"/>		
Locality Name *	<input type="text"/>	(eg. city name)	
Organization Name *	<input type="text"/>	(eg. company name)	
Organization Unit Name *	<input type="text"/>	(eg. department name)	
Common Name *	<input type="text"/>	(eg. server's hostname)	
Email Address *	<input type="text"/>		
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			

Screen – Add Certificate (Generate Certificate Signing Request (CSR))

## Parameters

Screen Element	Description
<b>Action</b>	Select an action from the available options:  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• Upload Certificate</li> <li>• Generate Self Signed Certificate</li> <li>• Generate Certificate Signing Request</li> </ul>
<b>Upload Certificate</b>	
<b>Name</b>	Specify a name to identify the Certificate.
<b>Certificate File Format</b>	Select the format of Certificate file from the available options.  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• <b>PEM (.pem):</b> Privacy Enhanced Mail (PEM) is a Base64 encoded DER certificate. It is used for encoding the certificate in ASCII code. The certificate and private key are stored in separate files.</li> <li>• <b>DER (.der):</b> Distinguished Encoding Rules (DER) is a binary form of ASCII PEM format certificate used on Java platform. The certificate and private key are stored in separate files.</li> <li>• <b>CER (.cer):</b> Canonical Encoding Rules (CER) is a binary format for encoding certificates. It contains information about the owner of certificate, its public and private keys.</li> <li>• <b>PKCS7 (.p7b):</b> Public Key Cryptography Standards (PKCS) is a format for encoding the certificate in ASCII code. It contains only certificates and not the private key.</li> <li>• <b>PKCS12 (.pfx or .p12):</b> Public Key Cryptography Standards (PKCS12) is a binary format for encoding certificates. It</li> </ul>

	stores a private key with a public key certificate. It is used on Windows platform.
<b>Certificate</b>	Specify the certificate to be uploaded. Use Browse to select the complete path.
<b>Private Key</b>	Specify private key for the certificate. Use Browse to select the complete path.
<b>Passphrase</b>	Specify and re-confirm a passphrase for a certificate used for authentication. Passphrase must be at least 4 characters long.
<b>Generate Self Signed Certificate (Option available only after configuring Error! Reference source not found.)</b>	
<b>Name</b>	Specify a name to identify the certificate.
<b>Valid From and Valid Up To</b>	Specify certificate validity period using Calendar  . Validity period is the certificate life i.e. period up to which the certificate will be considered as valid.  Default – 1 day
<b>Key Length</b>	Select key length. Key length is the number of bits used to construct the key.  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• 512</li> <li>• 1024</li> <li>• 1536</li> <li>• 2048</li> <li>• 4096</li> </ul> <p>Generally the larger the key, lesser is the chance that it will be compromised but requires more time to encrypt and decrypt data than smaller keys.</p> <p>Default – 512</p>
<b>Key Encryption</b>	Click to enable key encryption.
<b>Passphrase</b>	Password for a Certificate used for authentication. Password must be at least 8 characters long. This option is enabled only if the Key Encryption option is selected.
<b>Confirm Passphrase</b>	Re-enter password for confirmation.
<b>Certificate ID</b>	Specify certificate ID. You can specify any one of the following:  Available Options: <ul style="list-style-type: none"> <li>• <b>DNSIP Address (IPv4/IPv6 Address)</b></li> <li>• <b>Email Address</b></li> <li>• <b>DER ASN1 DN(X.509) (Applicable when Authentication Type is Digital Certificate)</b></li> </ul>

	Once the certificate is created, you need to download and send this certificate to the remote peer with whom the connection is to be established.
<b>Identification Attributes</b>	
<b>Country Name</b>	Select the country.
<b>State</b>	Specify the state within the country.
<b>Locality Name</b>	Specify the name of the locality.
<b>Organization Name</b>	Specify the organization name, which will use this certificate and domain name. This domain will be certified to use the Certificate.  Use unique Domain name only.
<b>Organization Unit Name</b>	Specify the department/unit name, which will use this certificate and domain name. This domain will be certified to use the Certificate.  Use unique Domain name only.
<b>Common Name</b>	Specify the common name.  A common name comprises of host + domain name or is a fully qualified domain name that is used to resolve to SSL VPN interface. It must be same as that of the Web address to be accessed when connecting to a secured site.
<b>Email Address</b>	Specify the Email Address of the contact person for communication.
<b>Generate Certificate Signing Request (CSR)</b>	
<b>Name</b>	Name to identify the certificate.
<b>Valid Up To</b>	Specify certificate validity period using Calendar. Validity period is the certificate life i.e. period up to which the certificate will be considered as valid. Minimum validity period is one day.
<b>Key Length</b>	Select key length. Key length is the number of bits used to construct the key.  Generally the larger the key, the less chance that it will be compromised but requires more time to encrypt and decrypt data than smaller keys.
<b>Encryption</b>	Click to enable the key encryption.
<b>Passphrase</b>	Passphrase for a Certificate used for authentication. Passphrase must be at least 4 characters long. This option is available only if the Encryption option is checked.
<b>Confirm Passphrase</b>	Re-enter passphrase for confirmation
<b>Certificate ID</b>	Specify certificate ID. You can specify any one of the following:  Available Options: <ul style="list-style-type: none"> <li>• DNSIP Address (IPv4/IPv6 Address)</li> </ul>


	<ul style="list-style-type: none"> <li>Email Address</li> <li>DER ASN1 DN(X.509) (Applicable when Authentication Type is Digital Certificate)</li> </ul>
<b>Identification Attributes</b>	
<b>Country Name</b>	<p>Select the Country for which the Certificate will be used.</p> <p>Generally, this would be the name of the country where Appliance is deployed.</p>
<b>State</b>	<p>Select the State for which the Certificate will be used.</p> <p>Generally, this would be the name of the state where Appliance is deployed.</p>
<b>Locality Name</b>	<p>Select the Locality for which the Certificate will be used.</p> <p>Generally, this would be the name of the Locality where Appliance is deployed.</p>
<b>Organization Name</b>	<p>Specify your organization name, which will use this certificate and domain name. This domain will be certified to use the Certificate.</p> <p>Use unique Domain names only.</p>
<b>Organization Unit Name</b>	<p>Specify your department/unit name, which will use this certificate and domain name. This domain will be certified to use the Certificate.</p> <p>Use unique Domain names only.</p>
<b>Common Name</b>	Specify Common Name.
<b>Email Address</b>	Specify Email Address.

Table – Add Certificate screen elements

## Downloading the Certificate

Under the Manage column, click the Download Icon  against the certificate you want to download. Only self signed certificate and certificate signing request can be downloaded. Certificate is downloaded as a .tar.gz file.

## Revoking the Certificate

Under the Manage column, click the Revoke Icon  to revoke self-signed certificate if lost, stolen or updated. Revoked certificate is automatically added to the Certificate Revocation List (CRL). You can download revoked certificate and circulate if required.

## Certificate Authority

The Appliance provides a facility to generate a local certificate authority as well as import certificates, signed by commercial providers, such as VeriSign.

A certificate signed by a Certificate Authority (CA) identifies the owner of a public key. Each communicating party may be required to present its own certificate signed by a CA verifying the ownership of the corresponding private key. Additionally, the communicating parties need to have a copy of the CA's public key. In case private key is lost or stolen or the information is changed, CA is responsible for revoking the certificate. CA also maintains the list of valid and revoked certificates.

After your CA has issued a certificate or have local certificate, you can upload it for use in VPN.

You can use default CA and can modify and re-generate it as per your requirement if you are not using any external CA. Using this CA, you can generate self-signed certificate and use it in VPN policy.

Using Third Party CA involves uploading:

- CA and root certificate
- Certificate
- CRL (Certificate Revocation List)

If the remote peer is using certificate issued by the following third party CA, you are not required to upload CA:


- VeriSign
- Entrust
- Microsoft

### Note

- Default CA is regenerated automatically when it is updated.

The page displays list of all the certificate authority and you can filter list based on certificate authority name. The page also provides option to download, regenerate CA, update the parameters of the existing CA, or delete the CA.

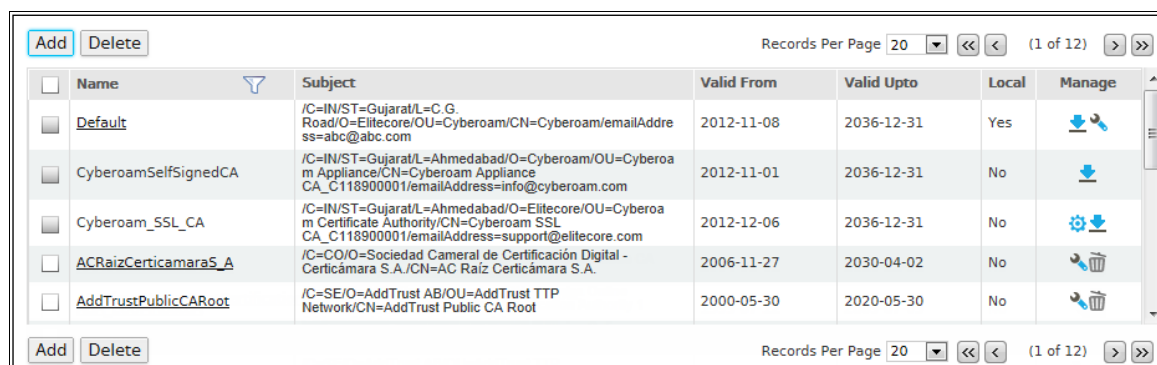
To manage Certificate Authorities, go to **System > Certificate > Certificate Authority**.

- [Download](#) – Click the Edit icon  in the Manage column against the Default Certificate Authority to modify the certificate authority. Once modified, click Download button to download the certificate Authority.



## Manage Certificate Authorities

To manage Certificate Authorities, go to **System > Certificate > Certificate Authority**.



Name	Subject	Valid From	Valid Upto	Local	Manage
Default	/C=IN/ST=Gujarat/L=C.G. Road/O=Elitecore/OU=Cyberoam/CN=Cyberoam/emailAddress=abc@abc.com	2012-11-08	2036-12-31	Yes	
CyberoamSelfSignedCA	/C=IN/ST=Gujarat/L=Ahmedabad/O=Cyberoam/OU=Cyberoam Appliance/CN=Cyberoam Appliance CA_C118900001/emailAddress=info@cyberoam.com	2012-11-01	2036-12-31	No	
Cyberoam_SSL_CA	/C=IN/ST=Gujarat/L=Ahmedabad/O=Elitecore/OU=Cyberoam Certificate Authority/CN=Cyberoam SSL CA_C118900001/emailAddress=support@elitecore.com	2012-12-06	2036-12-31	No	
ACRaizCerticamaraS_A	/C=CO/O=Sociedad Cameral de Certificación Digital - Certicámara S.A./CN=AC Raiz Certicámara S.A.	2006-11-27	2030-04-02	No	
AddTrustPublicCARoot	/C=SE/O=AddTrust AB/OU=AddTrust TTP Network/CN=AddTrust Public CA Root	2000-05-30	2020-05-30	No	

Screen – Manage Certificate Authority

## View the list of Certificate Authorities

Screen Element	Description
Name	Name of the Certificate Authority
Subject	Certificate Subject
Valid From and Valid Up To	Certificate validity date i.e. activation and expiry date.
Local	Whether CA is local or third party
Regenerate Certificate Authority Icon	Click to regenerate Certificate Authority.

Table – Manage Certificate Authority screen elements

### Note

- Default CA cannot be deleted.

## Download Certificate Authority

If you are using a local CA, you need to download CA and forward to the remote peer. Go to **System > Certificate > Certificate Authority** and click Default. It displays the details of the default CA. Click download icon to download the zip file.


## Regenerating Certificate Authority

Under the Manage column, click the regenerate icon .

### Note

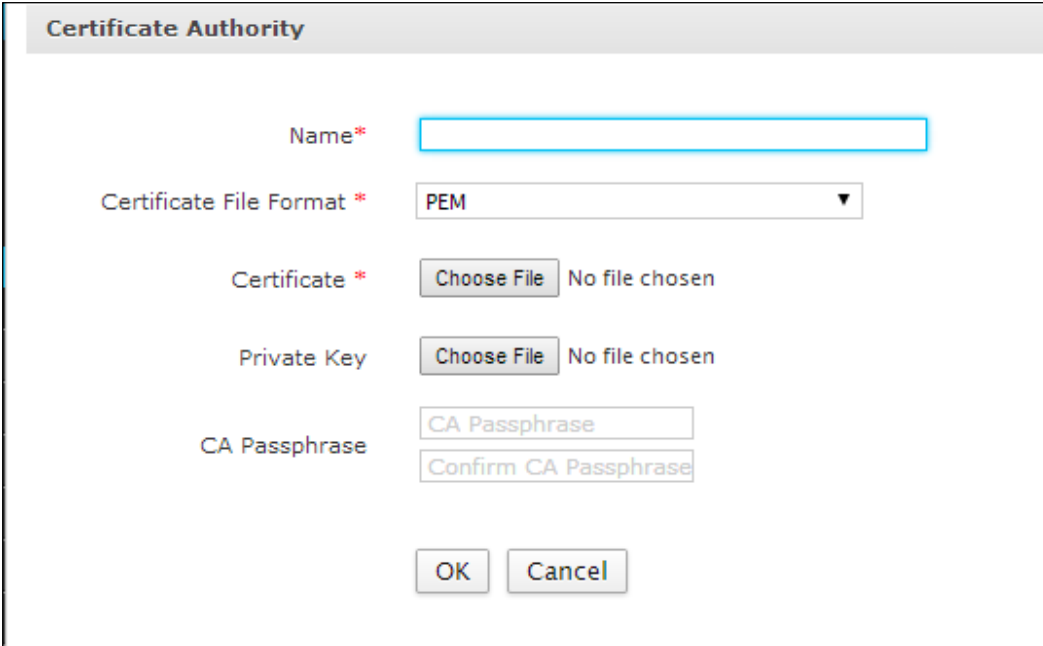
- Default CA is regenerated automatically when it is updated

## Certificate Authority Parameters

To add or edit certificate authority, go to **System > Certificate > Certificate Authority**. Click the Add button to add a new certificate authority. To update the details, click on the certificate authority or Edit icon  in the Manage column against the certificate authority you want to modify. To update and regenerate the default certificate, click on the default certificate.

- [CA Parameters](#)
- [Default CA Parameters](#)

### CA Parameters



Screen – Add Certificate Authority

Screen Element	Description
<b>Certificate Authority</b>	
<b>Name</b>	Specify a name to identify the Certificate Authority.
<b>Certificate File Format</b>	<p>Select format of the root certificate to be uploaded.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>PEM</b> (Privacy Enhanced Mail): A format encoding the certificate in ASCII code. The certificate, request, and private key are stored in separate files.</li> <li>• <b>DER</b>: A binary format for encoding certificates. The certificate, request, and private key are stored in separate files.</li> </ul>

<b>Certificate</b>	Specify full path from where the certificate is to be uploaded. Alternately, use Browse button to select the path.
<b>Private Key</b>	Specify full path from where the Private Key is to be uploaded. Alternately, use Browse button to select the path.
<b>CA Passphrase</b>	CA Passphrase for authentication. Passphrase must be at least 4 characters long.  Confirm CA passphrase for authentication.

Table – Add Certificate Authority screen elements

### Default CA Parameters

To edit default certificate authority, go to **System > Certificate > Certificate Authority**. Click on the **Default** certificate to update and regenerate the default certificate.

Screen – Default Certificate Authority

Screen Element	Description
<b>Certificate Authority</b>	
<b>Name</b>	Default. This name cannot be changed
<b>Country Name</b>	Specify the name of the country where Appliance is installed.
<b>State</b>	Specify the name of the state where Appliance is installed.
<b>Locality Name</b>	Specify the name of the locality where Appliance is installed.
<b>Organization Name</b>	Specify the organization name, which will use this certificate and domain name. This domain will be certified to use the Certificate.  Use unique Domain name only.

<b>Organization Unit Name</b>	Specify the department/unit name, which will use this certificate and domain name. This domain will be certified to use the Certificate.  Use unique Domain name only.
<b>Common Name</b>	Specify the common name.  A common name comprises of host + domain name or is a fully qualified domain name that is used to resolve to SSL VPN interface. It must be same as that of the Web address to be accessed when connecting to a secured site.
<b>Email Address</b>	Specify the Email Address of the contact person for communication.
<b>CA Passphrase</b>	Specify Passphrase for a Certificate Authority. Passphrase must be at least 4 characters long.  Re-enter passphrase for confirmation.  Click "Change CA Passphrase" to modify the passphrase.

**Table – Default Certificate Authority screen elements**

### Download Certificate Authority

If you are using local CA, you need to download CA and forward to the remote peer. Go to **System > Certificate > Certificate Authority** and click Default. It will display details of the default CA. Click Download to download the zip file.

## Certificate Revocation List (CRL)

CA maintains the list of valid and revoked certificates.

Certificate Revocation List (CRL) page is a way to check the validity of an existing certificate. Certificates which are stolen, lost or updated are revoked by CA and CA publishes such revoked certificates in Revocation list. VPN connection cannot be established using revoked certificates, hence it is necessary to update the CRL at regular intervals.

The page displays the list of available CRLs. It also provides option to add a new CRL, download the CRL, edit, and delete the existing CRL.

- [Download](#) – Click Download to download CRL.

### Manage Certificate Revocation List

To manage CRL, go to **System > Certificate > CRL**.

<input type="checkbox"/>	Name	Local	Manage
<input checked="" type="checkbox"/>	Default	Yes	<a href="#">Download</a>

Screen – Manage Certificate Revocation List (CRL)

Screen Element	Description
<b>Name</b>	Name of the Certificate Revocation list.
<b>Local</b>	Whether CA is local or third party.

Table – Manage Certificate Revocation List (CRL) screen elements

## Adding a new CRL

If you are using an External Certificate Authority, you need to upload the CRL obtained from that External Certificate Authority.

To add or edit CRL, go to **System > Certificate > CRL**. Click Add Button to add a new CRL or Edit Icon to modify the details of the CRL.

Screen – Add Certificate Revocation List (CRL)

### Parameters

Screen Element	Description
<b>Certificate Revocation List</b>	
<b>Name</b>	Name to identify the CRL.
<b>CRL File</b>	Specify CRL file to be uploaded. Use Browse to select the complete path.

Table – Add Certificate Revocation List (CRL) screen element

### Download CRL

Once CA is generated, default CRL is generated with name Default.tar.gz. Once you revoke the certificate, the details of the revoked certificate are added to the default file and regenerated. You can download and distribute if required.

Select **System > Certificate > CRL** and to view the list of CRLs.

Click “Download” link against the CRL name to be downloaded. It downloads the zip file, unzip the file to check the details.

## Diagnostics

Diagnostic page allows checking of the health of your Appliance in a single shot. Information can be used for troubleshooting and diagnosing problems found in your Appliance.

It is like a periodic health check up that helps to identify the impending Appliance related problems. After identifying the problem, appropriate actions can be taken to solve the problems and keep the Appliance running smoothly and efficiently.

- [Tools](#)
- [System Graphs](#)
- [Packet Capture](#)
- [Connection List](#)
- [Consolidated Troubleshoot Report](#) (CTR)

## Tools

Using Tools, one can view the statistics to diagnose the connectivity problem, network problem and test network communication. It assists in troubleshooting issues such as hangs, packet loss, connectivity, discrepancies in the network.

Go to **System > Diagnostics > Tools** to view the various statistics.

- [Ping](#)
- [Trace Route](#)
- [Name lookup](#)
- [Route lookup](#)

## Ping

Ping is a most common network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.

Ping sends ICMP echo request/replies to test connectivity to other hosts. Use standard ICMP ping to confirm that the server is responding. Ping confirms that the server can respond to an ICMP ping request.

Use Ping diagnostically to

- Ensure that a host computer you are trying to reach is actually operating or address is reachable or not
- Check how long it takes to get a response back
- Get the IP Address from the domain name
- Check for packet loss

Screen – Tools - Ping

Screen Element	Description
<b>IP Address/Host Name</b>	Specify the IP Address (IPv4/IPv6) or fully qualified domain name to be pinged.  It determines network connection between Appliance and host on the network. The output shows if the response was received, packets transmitted and received, packet loss if any and the round-trip time. If a host is not responding, ping displays 100% packet loss.
<b>Interface</b>	Select the Interface through which the ICMP echo requests are to be sent.  Available Options: <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> </ul>
<b>Interface</b>	Select the Interface through which the ICMP echo requests are to be sent.
<b>Size</b>	Specify the Ping packet size.  Default – 32 bytes Size Range – 1 to 65507

Table – Tools - Ping



## Trace Route

Trace Route is a useful tool to determine if a packet or communications stream is being stopped at the Appliance, or is lost on the Internet by tracing the path taken by a packet from the source system to the destination system, over the Internet.

Use trace Route to

- find any discrepancies in the network or the ISP network within milliseconds.
- trace the path taken by a packet from the source system to the destination system, over the Internet.

**Screen – Tools – Trace Route**

Screen Element	Description
<b>IP Address/Host Name</b>	Specify the IP Address (IPv4/IPv6) or fully qualified domain name.  It determines network connection between Appliance and host on the network. The output shows all the routers through which data packets pass on way to the destination system from the source system, maximum hops and Total time taken by the packet to return measured in milliseconds.
<b>Interface</b>	Select the Interface through which the requests are to be sent.  Available Options: <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> </ul>
<b>Interface</b>	<ul style="list-style-type: none"> <li>• Select the interface (Port) through which the requests are to be sent.</li> </ul>
<b>Size</b>	Specify the Ping packet size (in bytes).

**Table – Tools – Trace Route**

## Name lookup

Name lookup is used to query the Domain Name Service for information about domain names and IP Addresses. It sends a domain name query packet to a configured domain name system (DNS) server. If a domain name is entered, one gets back an IP Address to which it corresponds, and if an IP Address is entered, then one gets back the domain name to which it corresponds. In other words, it reaches out over the Internet to do a DNS lookup from an authorized name server, and displays the information in the user understandable format. Also one can view all the available DNS Servers configured in Appliance by selecting option “Name Lookup”. Selecting this option will also provide information about the time taken to connect to each of the DNS server. Based on the least time, one can prioritize the DNS server.

Screen – Tools – Name Lookup

Screen Element	Description
IP Address/Host Name	Specify IP Address (IPv4/IPv6) or fully qualified domain name that needs to be resolved.
DNS Server IP	Select the DNS server to which the query is to be sent.

Table – Tools – Name Lookup

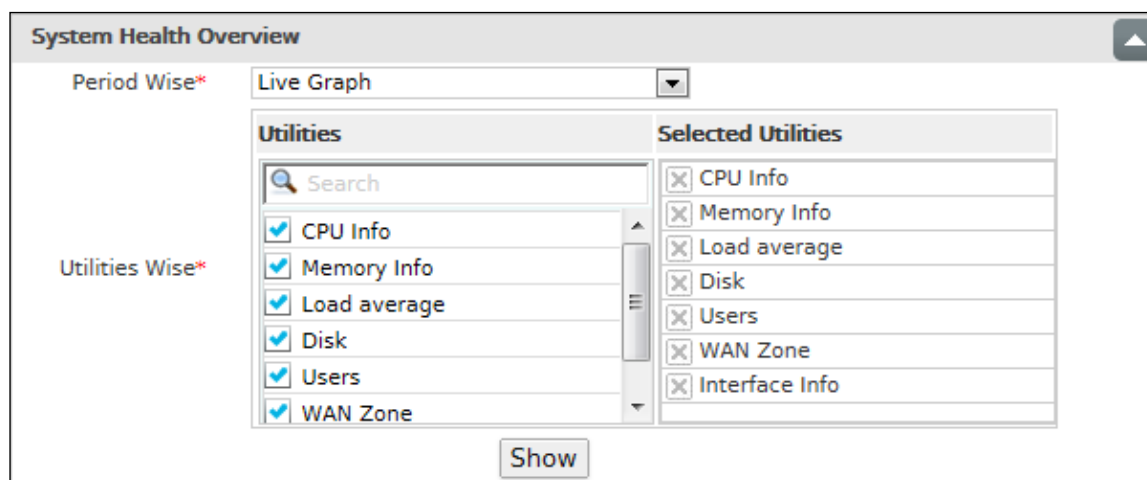
## Route lookup

If you have routable networks and wish to search through which Interface, the Appliance routes the traffic then lookup the route for the IP Address (IPv4/IPv6).

Screen – Tools – Route Lookup

## System Graph

Use System Graph to view Graphs pertaining to System related activities for different time intervals.



Screen – System Health Overview

Period wise graph will display following graphs for the selected period: Live Graph, CPU usage Info, Memory usage Info, Load Average and Interface usage Info. These graphs are same as displayed in Utility wise graphs. They are regrouped based on the time interval.

To view graphs, go to **System > Diagnostics > System Graphs**. You can view Period wise Utilities graphs.

Utility wise graph will display following graphs for the selected time period i.e. Live Graph (last two hours), Last 24 hours, Last 48 hours, Last Week, Last Month, Last Year:

- CPU usage Info
- Memory usage Info
- Load Average
- Disk usage
- Number of Live Users
- Data transfer through WAN Zone
- Interface usage Info

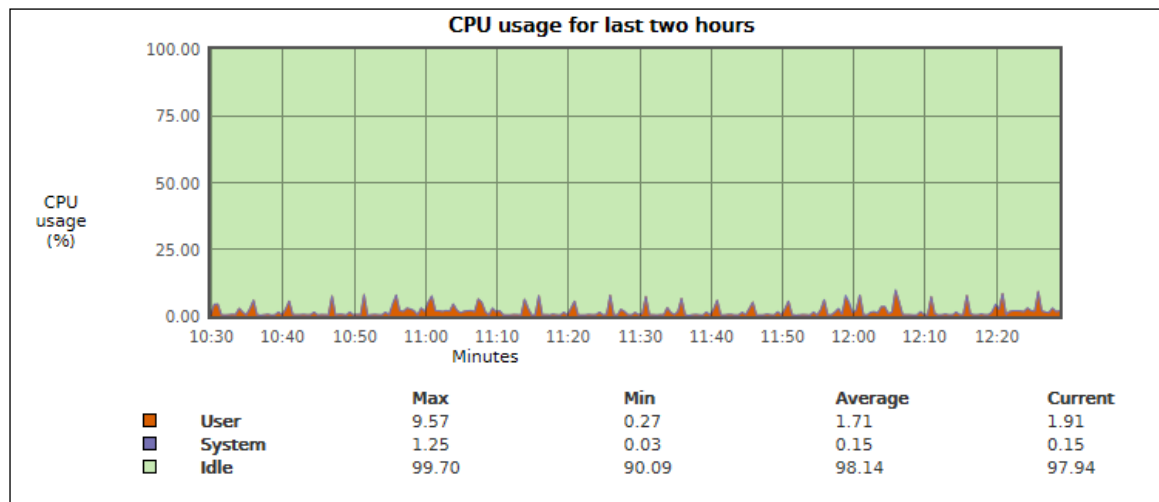
### Live Graphs

Live graphs allow Administrator to monitor the usage of resources of the last two hours. Graph displays the percentage wise CPU and Memory usage. It also displays load average and traffic statistics on each interface.

### CPU Info graphs

CPU Info graphs allow Administrator to monitor the CPU usage by the Users and System components. Graphs display percentage wise minimum, maximum, average and current CPU usage by User and System and CPU Idle time.

Last two hour CPU Usage – Below graph shows past two hour's CPU usage in percentage.



**Screen – Last two hours CPU usage**

X-axis – Minutes/ Hours/Days/Months (depending on the period selected)

Y-axis – CPU usage (%)

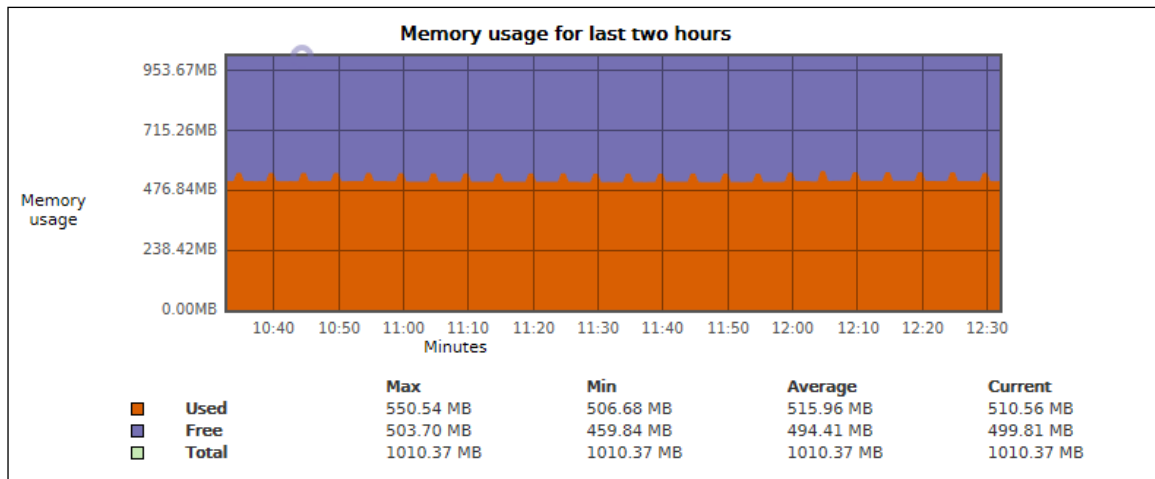
### Legends

- Orange Color – CPU used by User
- Purple Color – CPU used by System
- Green Color – CPU Idle time

### Memory Info graphs

Memory Info graphs allow Administrator to monitor the memory usage in percentage. Graphs displays the memory used, free memory and total memory available.

Last two hours Memory Usage – Below graph shows past two hour's memory usage in percentage. Graphs displays the memory used, free memory and total memory available.



Screen – Last two hours Memory usage

X-axis – Minutes/ Hours/Days/Months (depending on the period selected)

Y-axis – Memory used (MB)

**Legends**

Orange Color – Memory used

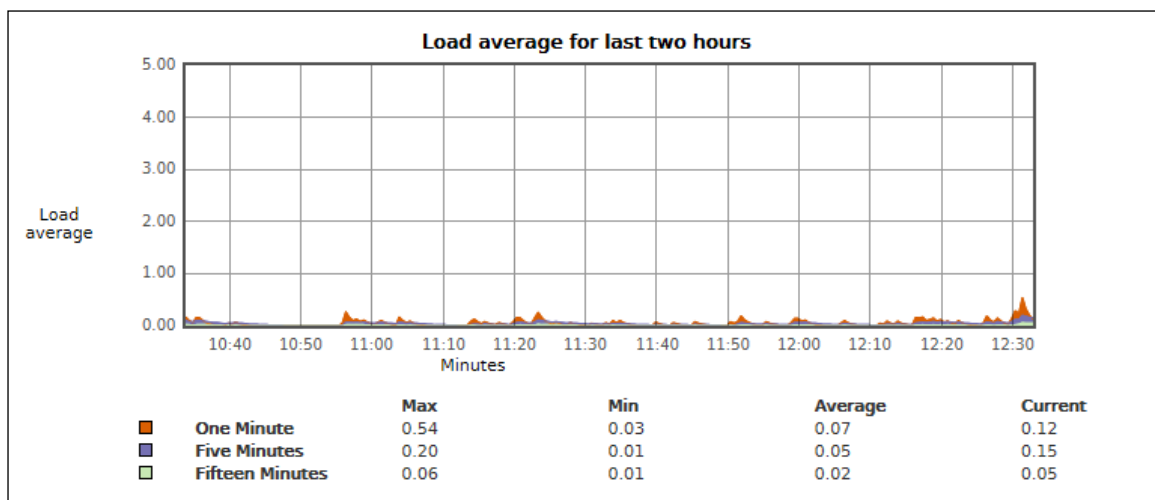
Purple Color – Free Memory

Green Color – Total Memory

**Load Average graphs**

Load Average graphs allow Administrator to monitor the load on the System. Graphs display the minimum, maximum, average and current load on the System at the interval of one minute, five minute, and fifteen minutes.

Last two hour Load Average - Below graph shows past two hour's average load on the system.



Screen – Last two hours Load Average usage

X-axis – Minutes/ Hours/Days/Months (depending on the period selected)  
 Y-axis – Load Average (%)

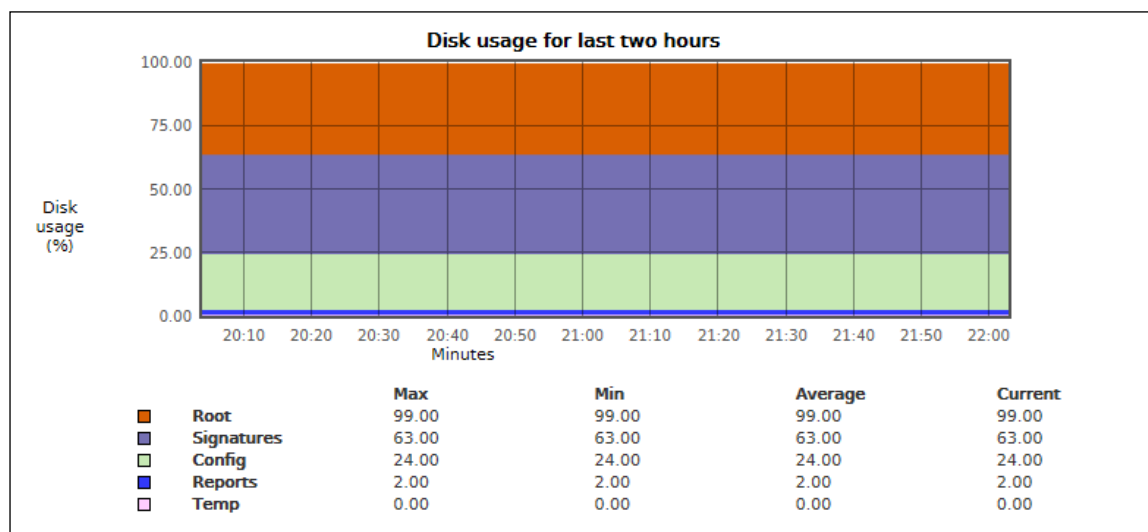
**Legends**

- Orange Color – One minute
- Purple Color – Five minutes
- Green Color – Fifteen minutes

**Disk Usage graphs**

Disk Usage graphs allow the Administrator to monitor the disk usage by various components viz., root file, signatures, configurations, reports and temporary files. Graphs display the minimum, maximum, average and current disk usage.

Last two hours Disk Usage – Below graphs displays the minimum, maximum, average and currently used disk space in percentage by various components in last two hours.



**Screen – Last two hours Disk Usage**

X-axis – Minutes/ Hours/Days/Months (depending on the period selected)  
 Y-axis – Disk usage (%)

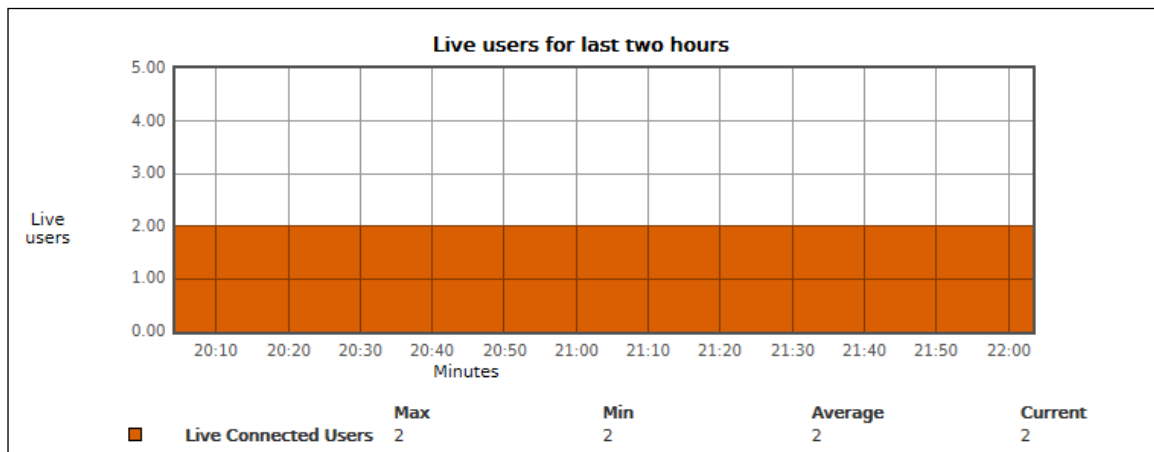
**Legends**

- Orange Color – Disk space used by Root
- Purple – Disk space used by Signatures
- Green Color – Disk space used by Config files
- Blue Color – Disk space used by Reports
- Pink Color – Disk space used by Temp

## Live Users Graph

Live Users graphs allow the Administrator to monitor the number of live user for the selected time duration.

Last two hours Live Users – Below graphs displays number of users (live) connected to the Internet. In addition, shows minimum, maximum and average no. of users connected during the selected graph period. This will help in knowing the peak hour of the day.



Screen – Last two hours Live Users

X-axis – Minutes/ Hours/Days/Months (depending on the period selected)

Y-axis – Number of Live Users

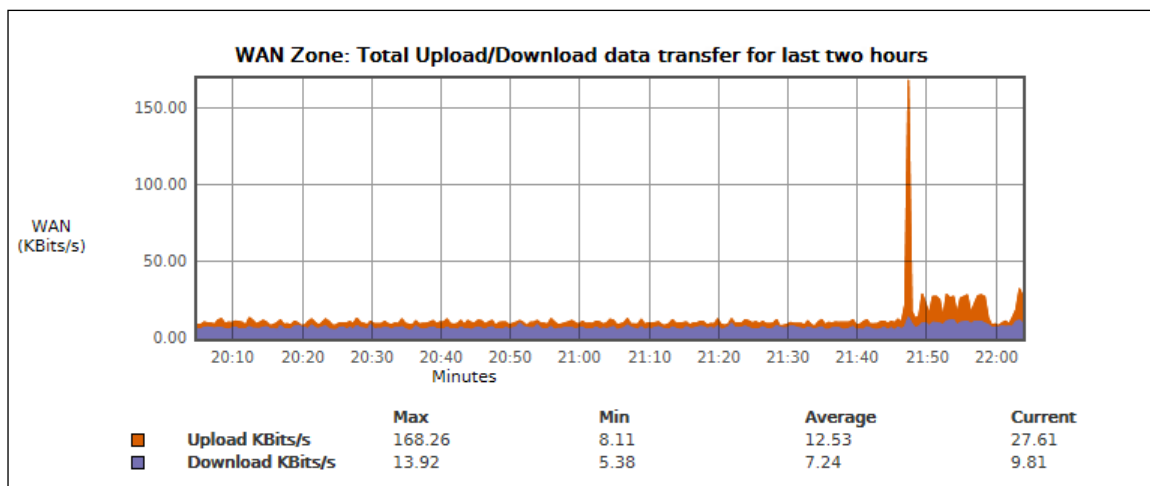
## Legends

Orange Color – Number of Live Users

## Data transfer Graphs for WAN zone

Data transfer graphs for WAN zone segregated in to three (3) graphs providing the various information about data transfer via WAN zone.

Last two hours Data Transfer through WAN Zone – Below graphs displays combined graph of Upload and Download data transfer. Colors differentiate upload and download data traffic. In addition, shows the minimum, maximum and average data transfer for upload and download individually.



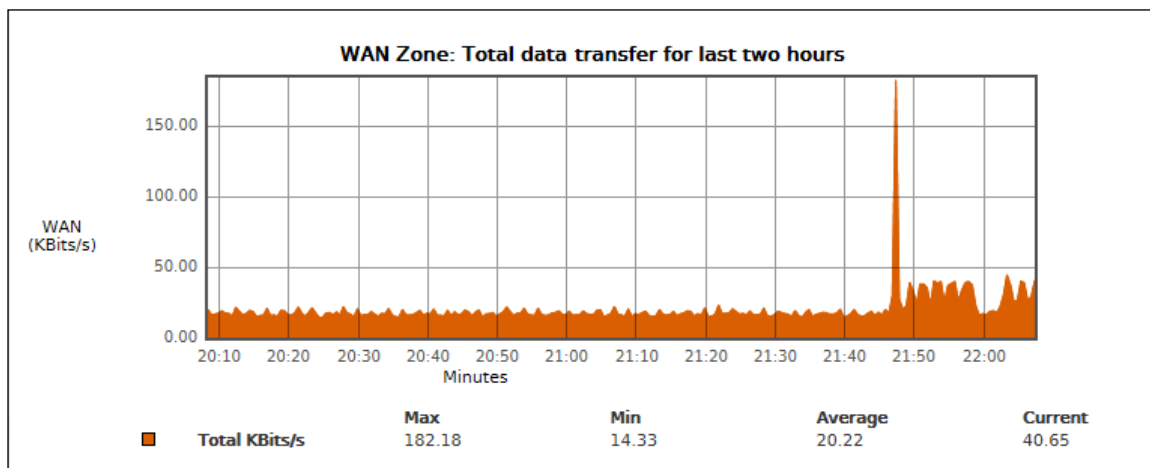
Screen – Last two hours Upload/Download Data Transfer

X axis – Minutes/ Hours/Days/Months (depending on the period selected)  
 Y-axis – Upload + Download in KBits/Second

**Legends**

- Orange Color - Upload traffic
- Purple Color – Download traffic

Last two hours Total Data Transfer through WAN Zone – Below graphs displays total data transfer during the last two hours. In addition, shows minimum, maximum and average data transfer.



Screen – Last two hours Total Data Transfer

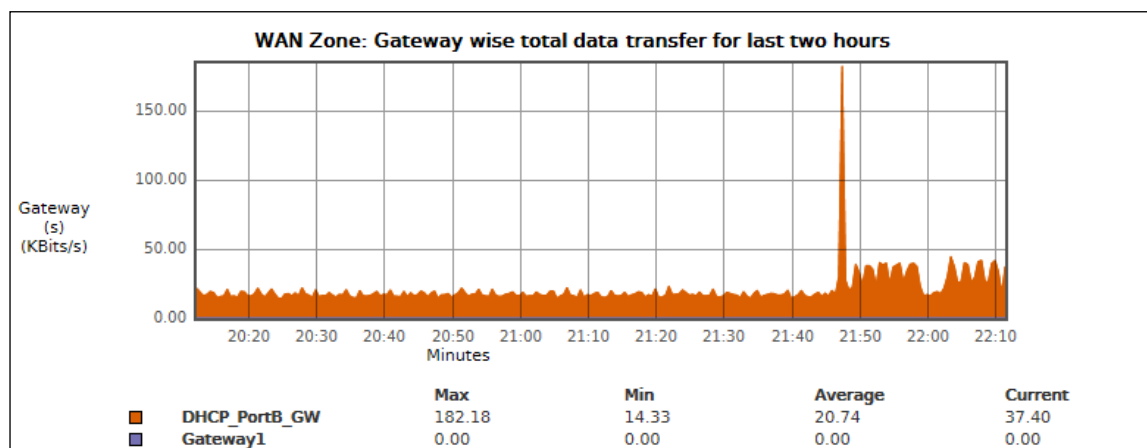
X axis – Minutes/ Hours/Days/Months (depending on the period selected)  
 Y-axis – Total data transfer in KBits/Second



## Legends

Orange Color – Total KBits/Second

Last two hours Gateway wise Total Data Transfer through WAN Zone – Gateway wise total data transfer for last two hours through WAN Zone - Graph displays total data transferred through all the configured gateways during last two hours. In addition, shows minimum, maximum and average data transfer.



**Screen – Last two hours Gateway wise Total Data Transfer**

X axis – Minutes/ Hours/Days/Months (depending on the period selected)

Y-axis – Gateway wise data transferred in KBits/Second

## Legends

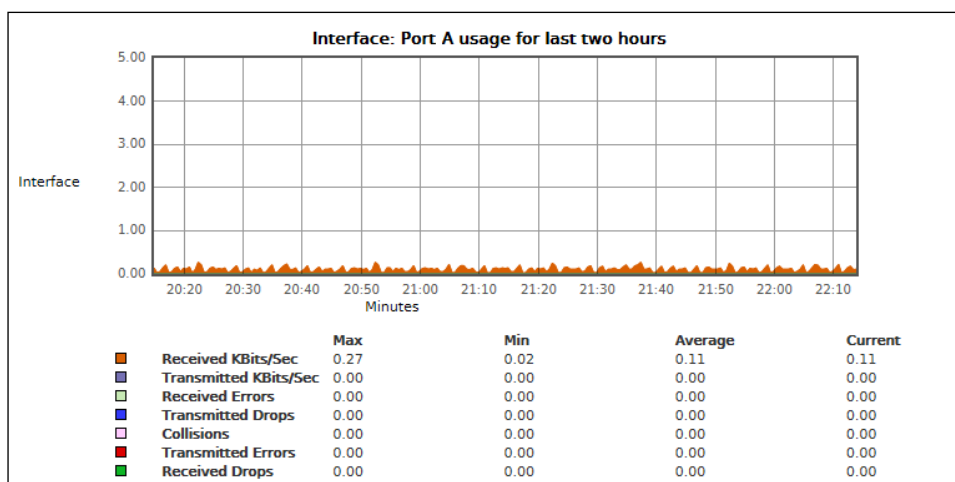
Orange Color – Default Gateway

Purple Color – Second Gateway (if configured)

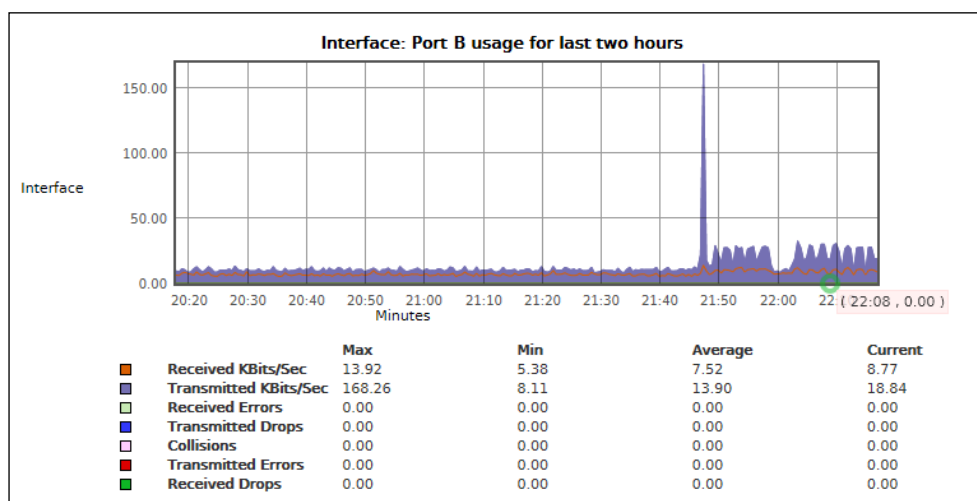
## Interface Info graphs

Interface Info graph displays following traffic statistics for all the Interfaces - physical interfaces, VLAN interfaces, Wireless LAN and WAN interfaces:

- Bits received and transmitted through Interface
- Errors occurred while transmitting and receiving packets through the Interface
- Packets dropped while transmitting and receiving packets through the Interface
- Collisions occurred while transmitting and receiving packets through the Interface



Screen – Last two hours Port A Interface Usage



Screen – Last two hours Port B Interface Usage

X-axis – Minutes/ Hours/Days/Months (depending on the period selected)

Y-axis – KBits/Sec

### Legends

- Orange Color – Bits Received (Kbits/Sec)
- Purple Color – Bits Transmitted (Kbits/Sec)
- Light Green Color – Received Errors
- Blue Color – Bits Transmitted but Dropped
- Pink Color – Collisions
- Red Color – Transmitted Errors
- Dark Green – Bits Received but Dropped

### Note

- Today and yesterday graphs are plotted at an average of five (5) minutes.
- Weekly Graph is plotted at an average of fifteen (15) minutes.
- Monthly Graph is plotted at an average of six (6) hours.
- Yearly Graph is plotted at an average of one (1) day.

## Packet Capture

Packet capture displays packets details on the specified interface. It will provide connection details and details of the packets processed by each module packets e.g. firewall, IPS along with information like firewall rule number, user, Web and Application Filter policy number etc. This will help administrators to troubleshoot errant Firewall Rules.



To capture information about packets, go to **System > Diagnostics > Packet Capture**. You can:

- [Configure Capture Filter](#) – Click the Configure Button to configure filter settings for capturing the packets.
- [View](#) – Click on the packet to view the packet information.
- [Display Filter](#) – Click the “Display Filter” Button to specify the filter conditions for the packets.
- Clear – Click the Clear Button to clear the details of the packets captured.

### View the list of Captured Packets

The screenshot displays the Packet Capture interface. At the top, it shows 'Trace on, Buffer Size 2048 KB, Buffer used 29 KB' and 'Capture Filter : -'. Below this is a table of captured packets with columns: Time, In Interface, Out Interface, Ether Type, Source IP, Destination IP, Packet Type, Ports[src,dst], Rule ID, Status, and Reason. The table contains several rows of data, including UDP, ARP, and TCP packets. Below the table are buttons for 'Configure', 'Display Filter', 'Stop', 'Refresh', and 'Clear'. The bottom section shows 'Packet Information' for a selected packet, including Ethernet Header, IP Header, and Hex & ASCII Detail.

Screen – Packet Capture

Screen Element	Description
<b>Packet Capture</b>	
<b>Packet Capture</b>	Displays following capturing configuration:  Trace On  - packet capturing is on  Trace Off  - packet capturing is off.

	<p>Buffer Size : 2048 KB</p> <p>Buffer used : 0 - 2048 KB</p> <p>Captured packets fill the buffer up to a size of 2048 KB. While the packet capturing is on, if the buffer used exceeds the stipulated buffer size, packet capturing stops automatically. In such a case, you would have to manually clear the buffer for further use.</p> <p>Capture Filter – There are various filter conditions for capturing the packets. The BPF String is used for filtering the packet capture.</p> <p>For example, Capture Filter - host 192.168.1.2 and port 137</p>
<b>Captured Packet</b>	
<b>Configure Button</b>	<p>Capture filter can be configured through following parameters:</p> <ul style="list-style-type: none"> <li>• Number of Bytes to Capture (per packet)</li> <li>• Wrap Capture Buffer Once Full</li> <li>• Enter BPF String</li> </ul> <p>Refer to <a href="#">Configure Capture Filter</a> for more details.</p>
<b>Display Filter Button</b>	<p>Log can be filtered as per the following criteria: Interface Name, Ether Type, Packet Type, Source IP, Source Port, Destination IP, Destination Port.</p> <p>Refer to <a href="#">Display Filter</a> for more details.</p>
<b>Start/Stop Button</b>	Start/Stop packet capturing
<b>Refresh Button</b>	Refresh the list of packets captured
<b>Clear Button</b>	Clear Button is to clear the buffer
<b>Time</b>	Packet capture time
<b>In Interface</b>	Interface from which packet is coming
<b>Out Interface</b>	Interface to which packet is sent
<b>Ether Type</b>	<p>Ether Type – IPv4 or IPv6 or ARP</p> <p>Ether Type is a field in an Ethernet frame. It is used to indicate the protocol encapsulated in the Ethernet frame.</p>
<b>Source IP</b>	Source IP Address (IPv4/IPv6) of the packet
<b>Destination IP</b>	Destination IP Address (IPv4/IPv6) of the packet
<b>Packet Type</b>	Type of Packet – ARP Request or UDP
<b>Ports [src, dst]</b>	Source and Destination ports

<b>Rule ID</b>	Firewall Rule ID
<b>Status</b>	<p>Displays the status of the packet. The various status are as described below:</p> <ul style="list-style-type: none"> <li>• <b>Incoming</b> – Packets received on on WAN or LAN interface.</li> <li>• <b>Forwarded</b> – Packet forwarded to Out Interface</li> <li>• <b>Consumed</b> – Packets designated for or used by the Appliance</li> <li>• <b>Generated</b> – Packets generated by the Appliance</li> <li>• <b>Violation</b> – In case of any policy violation, Appliance will drop the packet and show the status “Violation”</li> </ul>
<b>Reason</b>	Reason for packet being dropped, if it is dropped.
<b>Connection Status</b>	Displays state of connection.
<b>Served By</b>	
<b>Web Filter ID</b>	Web Filter policy ID applied on the connection traffic.
<b>Connection Flags</b>	System Flags
<b>Application ID</b>	Application ID applied on the connection traffic.
<b>Application Category ID</b>	Application category ID applied on the connection traffic.
<b>Connection ID</b>	Unique ID assigned to a connection.
<b>Gateway ID</b>	Gateway ID through which the connection traffic is routed.
<b>SSL VPN Policy ID</b>	SSL VPN policy ID applied on the connection traffic.
<b>Bandwidth Policy ID</b>	Bandwidth policy ID applied on the connection traffic.
<b>User Group</b>	User Group membership.
<b>IPS Policy ID</b>	IPS policy ID applied on the connection traffic.
<b>Application Filter ID</b>	Application filter policy ID applied on the connection traffic.
<b>Web Category ID</b>	Web category ID applied on the connection traffic.
<b>Master Connection ID</b>	Master connection ID of current connection.
<b>User Name</b>	Name of the user establishing connection.
<b>Packet Information</b>	
<b>Packet Information</b>	Packet Information including header details and entities including firewall rules & policies.
<b>Hex &amp; ASCII Detail</b>	
<b>Hex &amp; ASCII Detail</b>	Packet Information in Hex & ASCII values.

Table – Packet Capture screen elements

## Configuring Capture Filter

Capture Filter page allows configuration of number of bytes to be captured per packet.

Screen – Configure Capture Filter

Screen Element	Description
<b>Number of Bytes to Capture (per packet)</b>	Specify the number of bytes to be captured per packet.
<b>Wrap Capture Buffer Once Full</b>	Click to Enable 'Wrap Capture Buffer Once Full' checkbox to continue capturing the packets even after the buffer is full.  When the checkbox is enabled, the packet capturing starts again from the beginning of the buffer.
<b>Enter BPF String</b>	Specify BPF string  BPF (Berkeley Packet Filter) sits between link-level driver and the user space. BPF is protocol independent and use a filter-before-buffering approach. It includes a machine abstraction to make the filtering efficient. For example, host 192.168.1.2 and port 137.  Refer to <a href="#">BPF String Parameters</a> for filtering specific packets.

Table – Configure Capture Filter screen elements

## BPF String Parameters

How to check packets of the	Example
<b>specific host</b>	host 10.10.10.1
<b>specific source host</b>	src host 10.10.10.1
<b>specific destination host</b>	dst host 10.10.10.1
<b>specific network</b>	net 10.10.10.0

---

<b>specific source network</b>	src net 10.10.10.0
<b>specific destination network</b>	dst net 10.10.10.0
<b>specific port</b>	Port 20 or port 21
<b>specific source port</b>	src port 21
<b>specific destination port</b>	dst port 21
<b>specific host for the particular port</b>	host 10.10.10.1 and port 21
<b>the specific host for all the ports except SSH</b>	host 10.10.10.1 and port not 22
<b>specific protocol</b>	proto ICMP, proto UDP , proto TCP or proto ARP

## Display Filter

Display Filter page restricts the packet capturing to specific type of packets only. There are other filtering conditions such as the type of interface, ether type, source IP address & destination IP address.

Screen – Configure Display Filter

Screen Element	Description
<b>Interface Name</b>	Select the physical interface from the list for filtering packets log.
<b>Ether Type</b>	Select the Ethernet Type: IPv4 or IPv6 or ARP,  EtherType is a field in an Ethernet frame. It is used to indicate the protocol encapsulated in the Ethernet frame.
<b>Packet Type</b>	Select the packet type used from the list for filtering packets.
<b>Source IP</b>	Specify Source IP Address (IPv4/IPv6).
<b>Source Port</b>	Specify Source Port number.
<b>Destination IP</b>	Specify Destination IP Address (IPv4/IPv6).
<b>Destination Port</b>	Specify Destination Port number.



<b>Reason</b>	<p>Select the reason to display filter from the available options.</p> <p>Available Options:</p> <ul style="list-style-type: none"> <li>• Firewall</li> <li>• Local_ACL</li> <li>• DOS_ATTACK</li> <li>• INVALID_TRAFFIC</li> <li>• INVALID_FRAGMENTED_TRAFFIC</li> <li>• ICMP_REDIRECT</li> <li>• SOURCE_ROUTED_PACKET</li> <li>• FRAGMENTED_TRAFFIC</li> <li>• APPLICATION_FILTER</li> <li>• USER_IDENTITY</li> <li>• IPS</li> <li>• FOREIGN_HOST</li> <li>• IPMAC_FILTER</li> <li>• IP_SPOOF</li> <li>• ARP_POISONING</li> <li>• SSL_VPN_ACL_VIOLATION</li> <li>• Virtual_Host</li> <li>• ICMP Error Message</li> </ul>
<b>Status</b>	<p>Select status of the filter from available options.</p> <p>Available Options:</p> <ul style="list-style-type: none"> <li>• Allowed</li> <li>• Violation</li> <li>• Consumed</li> <li>• Generated</li> <li>• Incoming</li> <li>• Forwarded</li> </ul>
<b>Rule ID</b>	Specify ID for the Rule.
<b>User</b>	Select user from the list of users created before.
<b>Connection ID</b>	Specify connection ID.
<b>Clear</b>	Click to clear the details of filter.

**Table – Configure Display Filter screen elements**

## Connection List

Connection list provides current or live connection snapshot of your Appliance in the list form. Apart from the connection details, it also provides information like Firewall Rule ID, User ID, Connection ID per connection. It is also possible to filter the connections list as per the requirement and delete the connection.

The Administrator can set the Refresh Interval to automatically refresh the list at the configured time interval or manually refresh the list by clicking the Refresh button. To filter the connection list click the Display Filter button and specify the parameters.

To view connection list, go to **System > Diagnostics > Connection List**. You can:

- Set refresh interval
- [Display Filter](#) – Click the “Display Filter” Button to specify the filter connection based on the various parameters.

Time	Connection ID	In Interface	Out Interface	Source IP	Destination IP	Protocol	Source Port	Destination Port	Master Connection	Manage
19:37:44	3128424128	PortB	-	10.202.22.8	10.202.22.2	TCP	59734	80	0	
18:38:58	3128422688	-	PortB	10.202.22.2	180.179.170.220	TCP	48440	80	0	
19:37:22	3128425568	-	PortB	10.202.22.2	10.201.4.51	UDP	43651	53	0	
19:37:22	3128423840	-	PortB	10.202.22.2	10.201.4.51	UDP	41236	53	0	
19:37:38	3128424416	-	PortB	10.202.22.2	10.202.63.254	ICMP	8	0	0	

Screen – Connection List

## Live Connections Details

Screen Element	Description
<b>Connection List</b>	
<b>Refresh Interval</b>	Select the time interval after which the connection list will be refreshed.  Choose the time or click Refresh button to refresh the list.
<b>Display Filter Button</b>	Connections can be filtered as per the following criteria: Interface, Source IP Address and Port, Destination IP Address and Port, Protocol, Firewall rule ID and Username.  Refer to <a href="#">Display Filter</a> for more details.
<b>Select Columns</b>	<a href="#">Customize Columns</a> to be displayed. Click the ‘Select Column’ to customize the columns to be displayed. By default, Time, Connection Status, In Interface, Out Interface, Source IP, Destination IP, Protocol, Source Port, Destination Port, Rule ID, Username and Flag columns are selected and visible. You can select other column to be displayed.
<b>Time</b>	Connection time
<b>In Interface</b>	Interface used by incoming connection

<b>Out Interface</b>	Interface used by outgoing connection
<b>Source IP</b>	Source IP Address of the connection
<b>Destination IP</b>	Destination IP Address of the connection
<b>Protocol</b>	Connection protocol e.g. TCP, UDP
<b>Source Port</b>	Source port of the connection
<b>Destination Port</b>	Destination port of the connection
<b>Rule ID</b>	Firewall Rule ID that allows the session
<b>User Name</b>	Name of the user establishing connection
<b>Flags</b>	System flag
<b>Connection ID</b>	Unique ID of a connection
<b>Master Connection ID</b>	Master connection ID of current connection
<b>User Group</b>	User Group membership
<b>Web Filter ID</b>	Web filter policy ID applied on the connection traffic
<b>Application Filter ID</b>	Application filter policy ID applied on the connection traffic
<b>IPS Policy ID</b>	IPS policy ID applied on the connection traffic
<b>QoS Policy ID</b>	QoS policy ID applied on the connection traffic
<b>SSLVPN Policy ID</b>	SSL VPN policy ID applied on the connection traffic
<b>Gateway ID</b>	Gateway ID through which the connection traffic is routed
<b>Web Category ID</b>	Web category ID applied on the connection traffic
<b>Application ID</b>	Application ID applied on the connection traffic
<b>Application Category ID</b>	Application category ID applied on the connection traffic
<b>Connection served by</b>	Appliance serving the connection
<b>Translated Source</b>	Translated source IP Address for outgoing traffic.
<b>Translation Destination</b>	Translated Destination IP Address for outgoing traffic
<b>Rx Bytes</b>	The amount of data in bytes received this session
<b>Tx Bytes</b>	The amount of data in bytes sent this session
<b>Rx Packets</b>	Number of packets received in this session
<b>Tx Packets</b>	Number of packets received in this session
<b>Connection Status</b>	Displays the status of the connection.
<b>Connection State</b>	Displays the state of the connection.
<b>Expiry (second)</b>	Connection will expire in displayed seconds if idle
<b>Delete Button</b>	Stops the connection

Table – Connection List screen elements

## Configuring Connection Filter Parameters

To filter the connection list click the Display Filter button and specify the parameters.

Screen – Configure Connection Filter

Screen Element	Description
<b>In Interface</b>	Interface used by incoming connection.
<b>Out Interface</b>	Interface used by outgoing connection.
<b>User</b>	Name of the user establishing connection.
<b>Network Protocol</b>	Select the network protocol used to establish connection.  Available Options: <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> </ul>
<b>Source IP</b>	IP Address (IPv4/IPv6) from which connection is established.
<b>Destination IP</b>	IP Address (IPv4/IPv6) on which connection is established.
<b>Protocol</b>	Protocol used to establish connection.
<b>Source Port</b>	Source port of the connection.
<b>Destination Port</b>	Destination port for the connection.
<b>Rule ID</b>	Firewall Rule ID.
<b>Clear</b>	Click to clear the details of connection filter.

Table – Configure Connection Filter screen elements

## Consolidated Troubleshoot Report (CTR)

To help Support team to debug the system problems, troubleshooting report can be generated which consists of the system's current status file and log files. File contains details like list of all the processes currently running on system, resource usage etc. in the encrypted form.

The Administrator has to generate and mail the saved file at [support@cyberoam.com](mailto:support@cyberoam.com) for diagnosing and troubleshooting the issue. File will be generated with the name: CTR\_<APPKEY>\_\_<MM\_DD\_YY >\_<HH\_MM\_SS>

where

APPKEY is the Appliance key of the Appliance for which the report is generated

MM\_DD\_YY is the date (month date year) on which the report is generated

HH\_MM\_SS is the time (hour minute second) at which the report is generated

By default, debug mode is off for all the subsystems. Before generating Log file, enable debug mode by executing following command at CLI command prompt:

```
console > diagnostics subsystems <subsystem name> debug on
```

### Note

- Debug mode cannot be enabled, if you want to generate only the system snapshot.

Screen – Cyberoam Troubleshoot Report

Screen Element	Description
<b>Consolidated Troubleshooting Report</b>	
<b>Generate CTR for</b>	Enable the option(s) for which CTR should be generated.  Available Options: <ul style="list-style-type: none"> <li>• <b>System Snapshot</b> – Generates snapshots to display the issues in the system.</li> <li>• <b>Log Files</b> – Generates log files.</li> </ul>
<b>Reason</b>	Specify the reason for generating CTR.

Table – Cyberoam Troubleshoot Report screen elements

# Objects

Objects are the logical building blocks of various policies and rules, which include:

- Host – IP, network and MAC Addresses. They are used in defining the Firewall Rules, Virtual Host, NAT policy, IPSec, L2TP and VPN policies.
- Services – Represents specific protocol and port combination for example, DNS service for TCP on port 53. Access to services are allowed or denied through Firewall Rules.
- Schedule – Controls when the Firewall Rule, Access Time policy, Web Filter policy, Application Filter policy, or QoS policy is applicable for example, All Days, Work Hours.
- File Types – Defining Web Filter policy, SMTP Scanning Rules

Appliance supports four types of hosts:

- IP Host
- MAC Host
- FQDN Host
- Country Host
  
- [Hosts](#)
- [Services](#)
- [Schedule](#)
- [File Type](#)

## Hosts

An IP host is a logical building block used in defining Firewall Rules, Virtual Host and NAT policy. By default, the numbers of hosts equal to the number of ports in the Appliance, are already created.

Object – IP/MAC Host represents various types of addresses, including IP Addresses, networks and Ethernet MAC Addresses.

To apply common policies to multiple IP hosts, group IP hosts in an IP Host Group.

- [IP Host](#)
- [IP Host Group](#)
- [MAC Host](#)
- [FQDN Host](#)
- [FQDN Host Group](#)
- [Country Host](#)
- [Country Host Group](#)
- 

### IP Host

Hosts allow the entities to be defined once and be re-used in multiple referential instances throughout the configuration. For example, an Internal Mail Server with an IP Address as 192.168.1.15. Rather than repeated use of the IP Address while constructing Firewall Rules or NAT Policies, it allows to create a single entity called Internal Mail Server as a Host name with an IP Address as 192.168.1.15. This host, Internal Mail Server can then be easily selected in any configuration screen that uses Hosts as a defining criterion.

By using hosts instead of numerical addresses, you only need to make changes at a single location, rather than in each configuration where the IP Address appears.

Using Hosts, reduces the error of entering incorrect IP Addresses, makes it easier to change addresses and increases readability.

To configure IP Host, go to **Objects > Hosts > IP Host**.

The IP Host page displays the list of all the dynamic hosts which are automatically added on creation of VPN Remote access connections (IPSec and SSL) and the default hosts that are automatically created for remote access connection - ##ALL\_RW, ##WWAN1, ##ALL\_IPSEC\_RW and ##ALL\_SSLVPN\_RW along the manually added hosts. The page also provides option to add a new host, update the existing host, or delete a host.

#### Note

- System hosts cannot be updated or deleted.
- Dynamic hosts which are automatically added on creation of VPN Remote access connections cannot be updated or deleted.
- Default hosts that are created for remote access connection - ##ALL\_RW, ##WWAN1, ##ALL\_IPSEC\_RW and ##ALL\_SSLVPN\_RW cannot be updated or deleted.

## Manage the list of IP Hosts

To manage IP hosts, go to **Objects > Hosts > IP Host**.

<input type="checkbox"/>	Name	Type	Address Detail	IP Family	Manage
<input type="checkbox"/>	##ALL_IPSEC_RW	System Host	NA	IPv4	
<input type="checkbox"/>	##ALL_RW	System Host	NA	IPv4	
<input type="checkbox"/>	##ALL_SSLVPN_RW	System Host	NA	IPv4	
<input type="checkbox"/>	#PortA	System Host	172.16.16.222/255.255.255.255	IPv4	
<input type="checkbox"/>	#PortB	System Host	NA	IPv4	
<input type="checkbox"/>	#PortC	System Host	10.202.22.10/255.255.255.255	IPv4	
<input type="checkbox"/>	#PortD	System Host	NA	IPv4	
<input type="checkbox"/>	#WLAN1	System Host	10.10.13.1/255.255.255.255	IPv4	

**Screen – Manage IP Host**


Screen Element	Description
<b>Name</b>	Displays the name of the IP Host.
<b>IP Family</b>	Displays the type of IP Family.
<b>Type</b>	Type of IP Hosts – Single or range of IP, Network, and list of assorted IP Addresses.
<b>Address Detail</b>	Configured IP Addresses for the host.

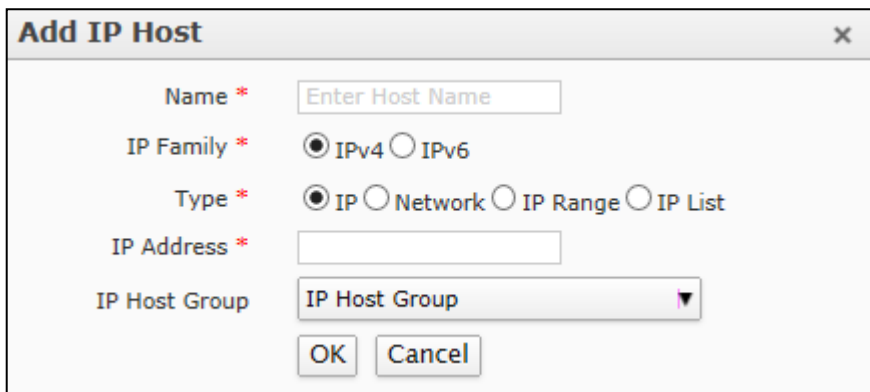
**Table – Manage IP Host screen elements**

List also displays dynamic hosts which are automatically added on creation of VPN Remote access connections (IPSec and SSL) and the default hosts that are automatically created for remote access connection - ##ALL\_RW, ##WWAN1, ##ALL\_IPSEC\_RW and ##ALL\_SSLVPN\_RW.



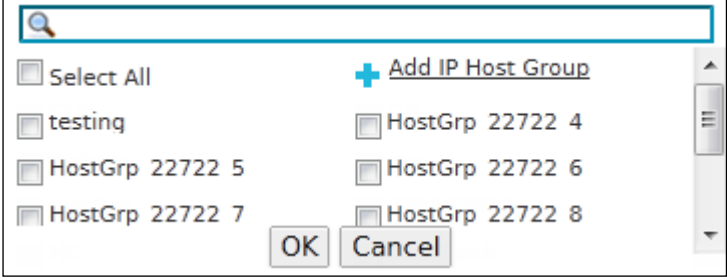
## Add an IP Host

To add or edit an IP host, go to **Objects > Hosts > IP Host**. Click the Add button to add a new host. To update the details, click on the host or Edit icon  in the Manage column against the host to be modified.



Screen – Add IP Host

Screen Element	Description
<b>Name</b>	Specify a name to identify the IP Host.
<b>IP Family</b>	Select the type of IP Family from the options available.  Available Options: <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> </ul>
<b>Type</b>	Select the type of host.  <b>Available options:</b> <ul style="list-style-type: none"> <li>• Single IP Address</li> <li>• Network IP Address with subnet</li> <li>• IP Range</li> <li>• <b>IP list</b> to add assorted IP Addresses. Use comma to specify assorted multiple IP Addresses. Create IP list to configure single Firewall Rule for multiple IP Address which are not in a range.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Only Class B IP Addresses can be added in IP list. IP Addresses can be added or removed from IP list.</li> </ul> </div>
<b>IP Address</b>	Specify IP Address based on the Host Type selected.
<b>IP Host Group</b>	Select host group i.e. host group membership. Single host can be member of multiple host groups.



You can also add a host group from Add Host page itself.

**Note**

- IP Host Group is not available for IP List type.

Table – Add IP Host screen elements

## IP Host Group

Host group is a grouping of hosts. Firewall Rule can be created for the individual host or host groups.

The IP Host Group page displays the list of all the host groups. The page also provides an option to add a new host group, update the parameters of the existing host group, add members to the existing host group, or delete a host group.

### Note

- Dynamic host groups that are automatically added on creation of VPN Remote Access Connections cannot be updated or deleted.

### Manage IP Host Groups list

To configure host groups, go **Objects > Hosts > IP Host Group**.


Name	Description	IP Family	Manage
Test		IPv4	 

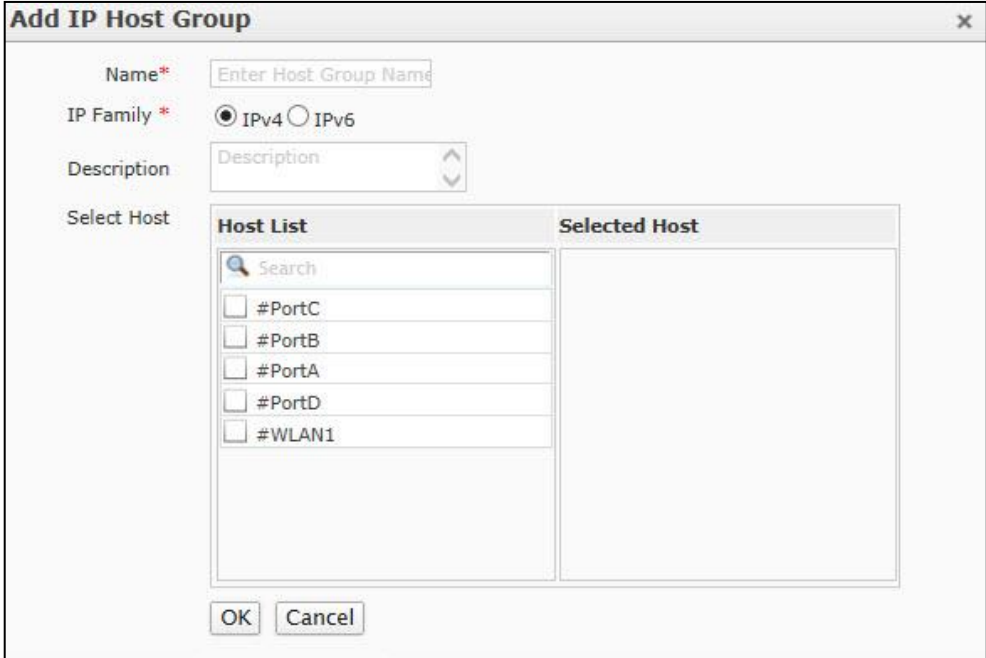
Screen – Manage IP Host Group

Screen Element	Description
Name	Name of the IP Host Group.
IP Family	Displays the type of IP Family.
Description	Description of the Host Group.

Table – Manage IP Host Group screen elements

## IP Host Group Parameters

To add or edit a host group, go to **Objects > Hosts > IP Host Group**. Click the Add button to add a new host group. To update the details, click on the host group or Edit icon  in the Manage column against the host group to be modified.



Screen – Add IP Host Group

Screen Element	Description
<b>Name</b>	Specify a name to identify the IP Host group.
<b>IP Family</b>	Select the type of IP Family from the options available.  Available Options: <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> </ul>
<b>Description</b>	Describe the IP Host Group.
<b>Select Host</b>	'Host' List displays all the hosts including default hosts.  Click the checkbox to select the hosts. All the selected hosts are moved to 'Selected host' list.  Single host can be a member of multiple host groups.  A group with IPv4 and IPv6 hosts cannot be created.

Table – Add IP Host Group screen elements

## MAC Host

Appliance allows creating a host based on MAC Address. One can create a MAC Host of either a single MAC Address or multiple MAC Addresses.

MAC Hosts allow entities to be defined once and be re-used in multiple referential instances throughout the configuration. For example, test has a MAC Address as 00:16:76:49:33:CE or 00-16-76-49-33-CE. Rather than remembering the MAC Address of the intended machine while applying policies, you can simply provide its MAC Host name.

By using MAC hosts, you only need to make changes in a single location, rather than in each configuration where the MAC Address appears.

Using MAC Hosts reduces the error of entering incorrect MAC Addresses, makes it easier to change addresses, and increases readability.

The MAC Host page displays the list of all the available MAC host. The page also provides option to add a new MAC host, update the existing host, or delete a host.

### View the list of MAC Hosts

To view list of MAC Host, go to **Objects > Hosts > MAC Host**.

<input type="checkbox"/>	Name	Type	Address Detail	Manage
<input type="checkbox"/>	mac2	Address	00:16:76:49:33:CF	
<input type="checkbox"/>	mac19	Address	00:16:76:49:33:C2	
<input type="checkbox"/>	mac18	Address	00:16:76:49:33:90	
<input type="checkbox"/>	MAC_22939_11	Address	11:22:33:44:55:66	
<input type="checkbox"/>	MAC_22939_28	Address	11:22:33:44:55:66	

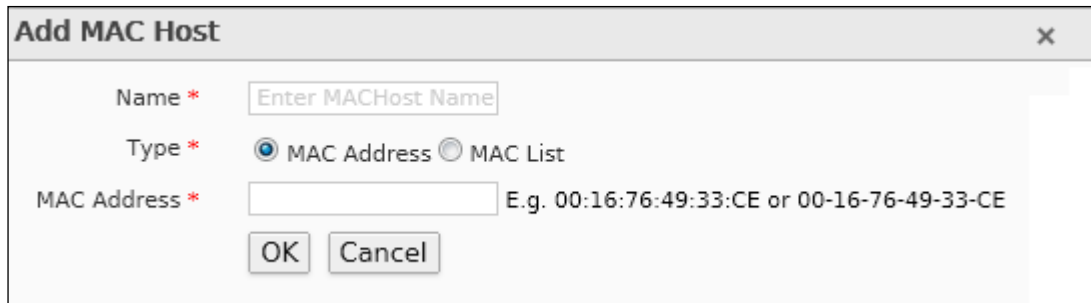
Screen – Manage MAC Host

Screen Element	Description
<b>Name</b>	Displays the name of the MAC Host.
<b>Type</b>	Displays the Type of MAC Hosts – single or multiple.
<b>Address Detail</b>	Displays the configured MAC Addresses.

Table – Manage MAC Host screen elements

## MAC Host Parameters

To add or edit a MAC host, go to **Objects > Hosts > MAC Host**. Click the Add button to add a new host. To update the details, click on the host or Edit icon  in the Manage column against the host to be modify.



**Add MAC Host** [Close]

Name \*

Type \*  MAC Address  MAC List

MAC Address \*  E.g. 00:16:76:49:33:CE or 00-16-76-49-33-CE

Screen – Add MAC Host

Screen Element	Description
<b>Name</b>	Specify a name to identify the MAC Host.
<b>Type</b>	Select the MAC Host Type.  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• <b>MAC Address</b> – Single MAC Address</li> <li>• <b>MAC list</b> – Multiple MAC Addresses</li> </ul>
<b>MAC Address</b>	Specify MAC Address based on the Host Type selected in the form of 00:16:76:49:33:CE or 00-16-76-49-33-CE  Use comma to configure multiple addresses.

Table – Add MAC Host screen elements

## FQDN Host

Hosts allow entities to be defined once and be re-used in multiple referential instances throughout the configuration. For example, [www.example.com](http://www.example.com) has an IP Address as 192.168.1.15. Rather than remembering the IP Address of the intended website while accessing it, you can simply provide [www.example.com](http://www.example.com) in the browser. The FQDN [www.example.com](http://www.example.com) will now be mapped to its respective IP Address, and the intended webpage opens.

The FQDN Host page displays the list of all the available FQDN host. The page also provides option to add a new FQDN host, update the existing host, or delete a host.

To configure FQDN Host, go to **Objects > Hosts > FQDN Host**.

### Note

- System hosts cannot be updated or deleted.
- Dynamic hosts which are automatically added on creation of VPN Remote access connections cannot be updated or deleted.
- Default hosts that are created for remote access connection - ##ALL\_RW, ##WWAN1, ##ALL\_IPSEC\_RW and ##ALL\_SSLVPN\_RW cannot be updated or deleted.

## Manage FQDN Hosts list

To manage MAC hosts, go to **Objects > Hosts > FQDN Host**.

Name	FQDN	Manage
FQDNHost_23046_1	miloufifonours.skyblog.fr	[Wrench] [Trash]
FQDNHost_23046_10	nycdrummond.superforum.fr	[Wrench] [Trash]
FQDNHost_23046_11	oriane974.blogone.fr	[Wrench] [Trash]
FQDNHost_23046_12	montagnes-d.logitest.fr	[Wrench] [Trash]
FQDNHost_23046_13	nrj-music-tour-a.aftel.fr	[Wrench] [Trash]


Screen – Manage FQDN Host

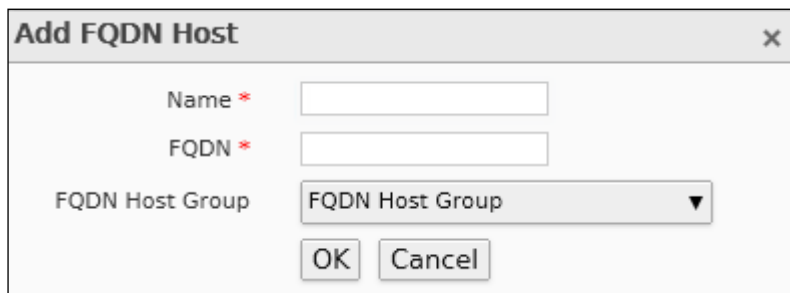
Screen Element	Description
Name	Displays the name of the FQDN Host.
FQDN	Displays the configured FQDN addresses for the host.

Table – Manage FQDN Host screen elements

List also displays dynamic hosts which are automatically added on creation of VPN Remote access connections (IPSec and SSL) and the default hosts that are automatically created for remote access connection - ##ALL\_RW, ##WWAN1, ##ALL\_IPSEC\_RW and ##ALL\_SSLVPN\_RW.

## Adding an FQDN Host

To add or edit a FQDN host, go to **Objects > Hosts > FQDN Host**. Click the Add button to add a new host. To update the details, click on the host or Edit icon  in the Manage column against the host to be modified.



Screen – AddFQDN Host

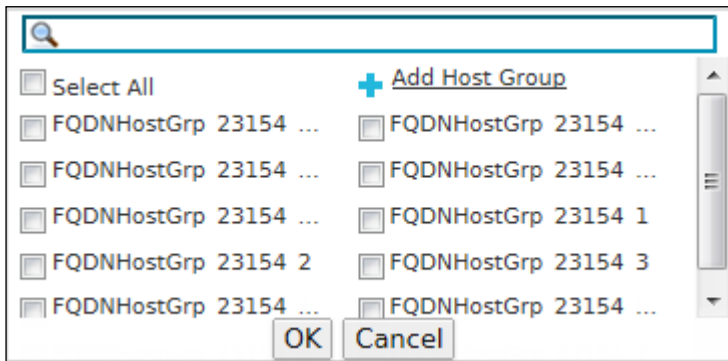
Screen Element	Description
<b>Name</b>	Specify a name to identify the FQDN Host.
<b>FQDN</b>	Specify the FQDN Address based on the Host Type selected.
<b>FQDN Host Group</b>	<p>Select host group i.e. host group membership. Single host can be a member of multiple host groups.</p>  <p>You can also add a host group from Add Host page itself or from <b>Objects &gt; Hosts &gt; FQDN Host Group</b> page..</p>

Table – Add FQDN Host screen elements



## FQDN Host Group

FQDN Host Group is a grouping of FQDN hosts. Firewall Rule can be created for the individual FQDN host or host group to block or unblock access to any website.

The FQDN Host page displays the list of all the available FQDN host. The page also provides an option to add a new FQDN host group, update the parameters of the existing host group, add members to the existing host group, or delete a group.

To configure host groups, go to **Objects > Hosts > FQDN Host Group**.

### Note

- Dynamic host groups which are automatically added on creation of VPN Remote Access connections cannot be updated or deleted.

## Manage FQDN Host Group list

To manage FQDN hosts group, go to **Objects > Hosts > FQDN Host Group**.

<input type="checkbox"/>	Name	Description	Manage
<input type="checkbox"/>	<a href="#">FQDNHostGrp_23154_1</a>		
<input type="checkbox"/>	<a href="#">FQDNHostGrp_23154_10</a>		
<input type="checkbox"/>	<a href="#">FQDNHostGrp_23154_11</a>		
<input type="checkbox"/>	<a href="#">FQDNHostGrp_23154_12</a>		
<input type="checkbox"/>	<a href="#">FQDNHostGrp_23154_13</a>		
<input type="checkbox"/>	<a href="#">FQDNHostGrp_23154_14</a>		

Screen – Manage FQDN Host Group

Screen Element	Description
Name	Displays the name of the FQDN Host Group.
Description	Displays the description of the FQDN Host Group.

Table – Manage FQDN Host Group screen elements

## Adding a FQDN Host Group

To add or edit a FQDN host group, go to **Objects > Hosts > FQDN Host Group**. Click the Add button to add a new host. To update the details, click on the host or Edit icon in the Manage column against the host group to be modified.

Screen – Add FQDN Host Group

Screen Element	Description
<b>Name</b>	Specify a name to identify the FQDN Host group.
<b>Description</b>	FQDN Host Group description.
<b>Select Host</b>	<p>“Host” List displays all the hosts including default hosts.</p> <p>Click the checkbox to select the hosts. All the selected hosts are moved to “Selected host” list.</p> <p>Single host can be a member of multiple host groups.</p>

Table – Add FQDN Host Group screen elements

## Country Host

Country Based Host is required to allow/block the traffic from/to a particular country. Hosts allow entities to be defined once and be re-used in multiple referential instances throughout the configuration. For example, you want to deny incoming traffic from country “X”. You can select the country “X” and select the option to block the traffic coming from “X”.

To configure Country Host, go to **Objects > Hosts > Country Host**.

### Note

- System hosts cannot be updated or deleted.
- Dynamic hosts which are automatically added on creation of VPN Remote access connections cannot be updated or deleted.
- Default hosts that are created for remote access connection - ##ALL\_RW, ##WWAN1, ##ALL\_IPSEC\_RW and ##ALL\_SSLVPN\_RW cannot be updated or deleted.

## Manage Country Host List

To manage Country hosts, go to **Objects > Hosts > Country Host**.

<input type="checkbox"/>	Name	Country	Manage
<input type="checkbox"/>	Macedonia	Macedonia	
<input type="checkbox"/>	Lithuania	Lithuania	
<input type="checkbox"/>	Norway	Norway	
<input type="checkbox"/>	Jersey	Jersey	
<input type="checkbox"/>	Central African Republic	Central African Republic	
<input type="checkbox"/>	United Arab Emirates	United Arab Emirates	


Screen – Manage Country Host

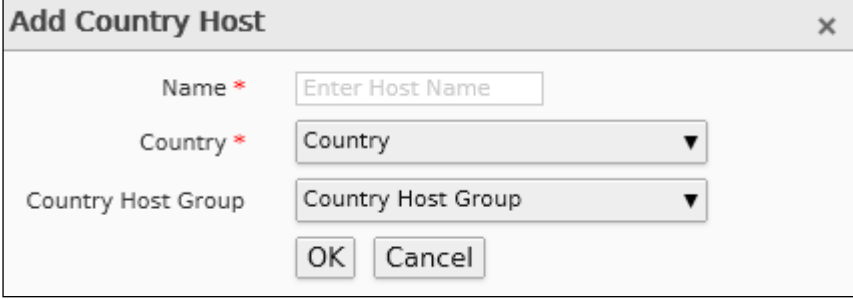
Screen Element	Description
Name	Displays the name of the Country Host.
Country	Displays the configured Country.

Table – Manage Country Host screen elements

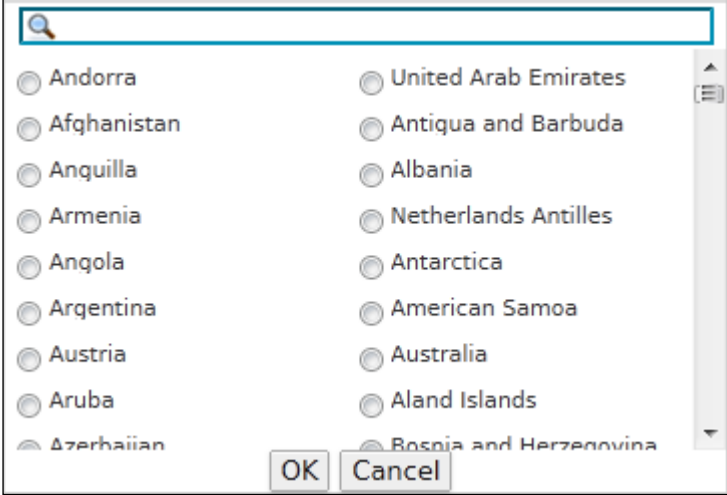
List also displays dynamic hosts which are automatically added on creation of VPN Remote access connections (IPSec and SSL) and the default hosts that are automatically created for remote access connection - ##ALL\_RW, ##WWAN1, ##ALL\_IPSEC\_RW and ##ALL\_SSLVPN\_RW.

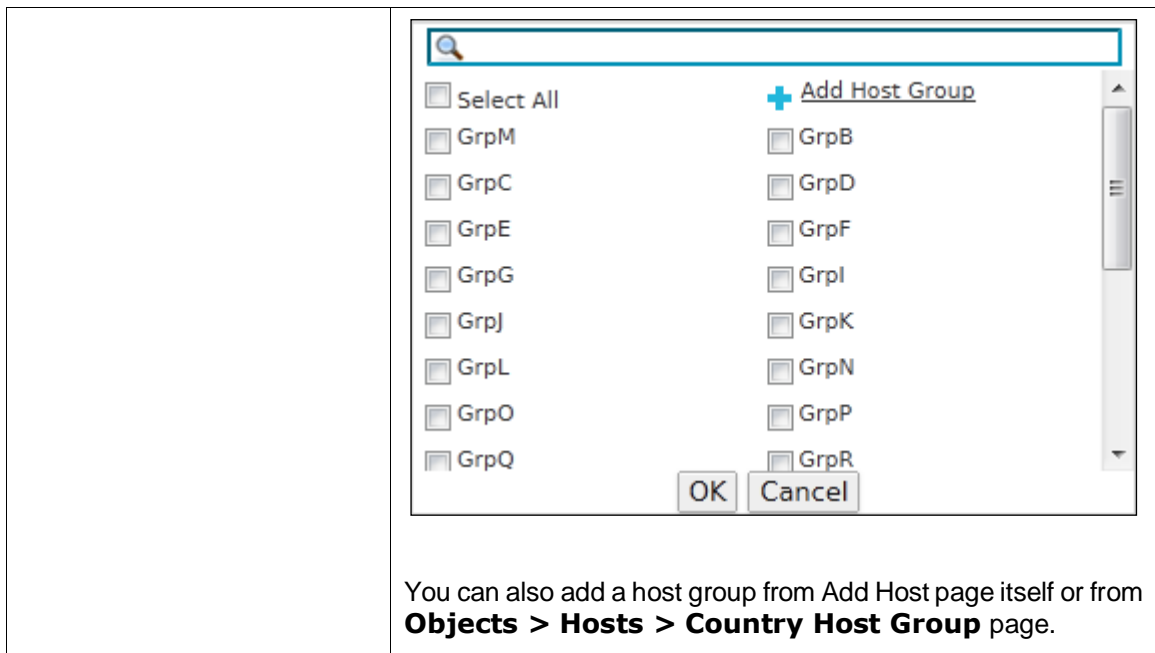
## Adding a Country Host

To add or edit a Country host, go to **Objects > Hosts > Country Host**. Click the Add button to add a new host. To update the details, click on the host or Edit icon  in the Manage column against the host to be modified.



Screen – Add Country Host

Screen Element	Description
<b>Name</b>	Specify a name to identify the Country Host.
<b>Country</b>	Select the Country. 
<b>Country Host Group</b>	Select host group i.e. host group membership. Single host can be member of multiple host groups.



**Table – Add Country Host screen elements**

## Country Host Group

Country Host Group is a grouping of Country Hosts. Multiple countries can be selected to block or allow incoming traffic by using Country Host Group. Firewall Rule can be created for an individual Country Host or Country Host Groups.

The Country Host Group page displays the list of all the available Country host groups. The page also provides option to add a new host group, update the parameters of the existing host group, add members to the existing host group, or delete a group.

### Note

- Dynamic host groups which are automatically added on creation of VPN Remote Access connections cannot be updated or deleted.

## Manage Country Host Group list

To manage Country host group, go to **Objects > Hosts > Country Host Group**.


<input type="checkbox"/>	Name	Description	Manage
<input type="checkbox"/>	<u>Group</u>		
<input type="checkbox"/>	<u>GrpB</u>	CountryHostGRP	
<input type="checkbox"/>	<u>GrpC</u>	CountryHostGRP	
<input type="checkbox"/>	<u>GrpD</u>	CountryHostGRP	
<input type="checkbox"/>	<u>GrpE</u>	CountryHostGRP	
<input type="checkbox"/>	<u>GrpF</u>	CountryHostGRP	
<input type="checkbox"/>	<u>GrpG</u>	CountryHostGRP	
<input type="checkbox"/>	<u>GrpH</u>	CountryHostGRP	
<input type="checkbox"/>	<u>GrpI</u>	CountryHostGRP	

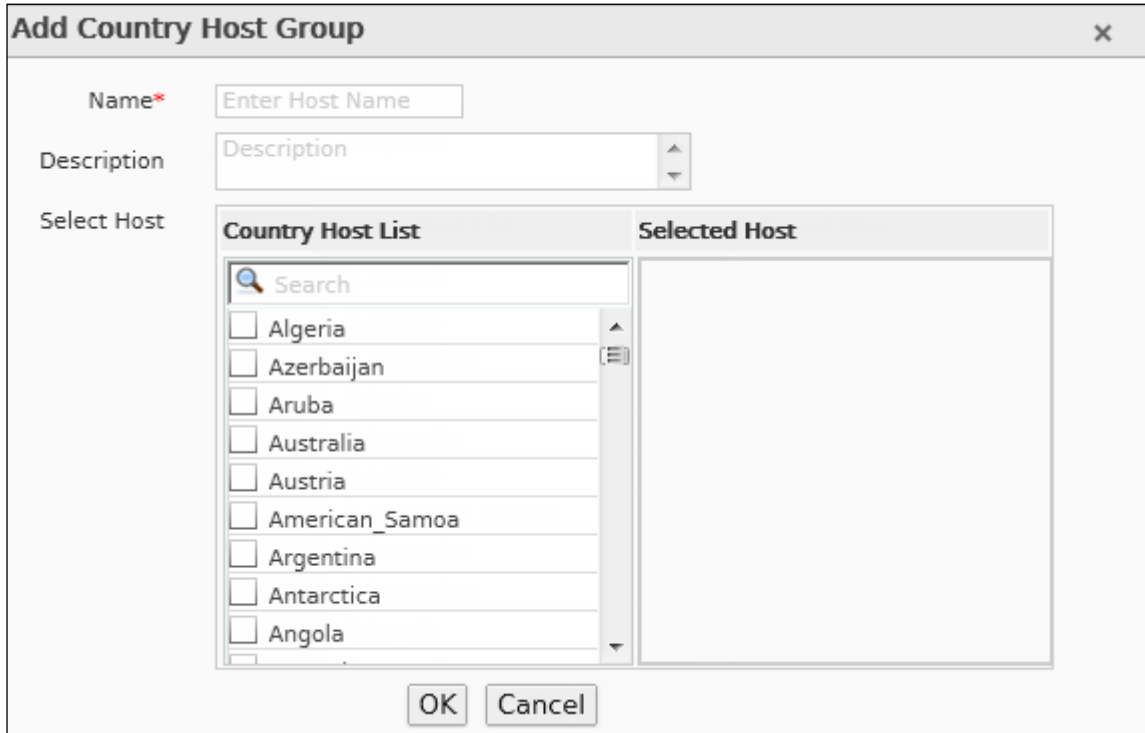
Screen – Manage Country Host Group

Screen Element	Description
<b>Name</b>	Displays the name of the Country Host Group.
<b>Description</b>	Displays the description of the Country Host Group.

Table – Manage Country Host Group screen elements

## Adding a Country Host Group Parameter

To add or edit a Country Host Group, go to **Objects > Hosts > Country Host Group**. Click the Add button to add a new host. To update the details, click on the host or Edit icon  in the Manage column against the host group to be modified.



Screen – Add Country Host Group

Screen Element	Description
<b>Name</b>	Specify a name to identify the Country Host group.
<b>Description</b>	Country Host Group description.
<b>Select Host</b>	<p>The “Host” List displays all the hosts including default hosts.</p> <p>Click the checkbox to select the hosts. All the selected hosts are moved to the 'Selected host' list.</p> <p>Single host can be a member of multiple host groups.</p>

Table – Add Country Host Group screen elements

## Services

Services represent types of Internet data transmitted via particular protocols or applications. It allows identifying the traffic based on the attributes of a given protocol.

Protect your network by configuring Firewall Rules to

- block services for specific zone
- limit some or all users from accessing certain services
- allow only specific user to communicate using specific service

Appliance is shipped with several default services and allows creating:

- Custom service definitions
- Firewall Rule for custom service definitions
- [Services](#)
- [Service Group](#)

## Services

Services are definitions of certain types of network traffic and combine information about a protocol such as TCP, ICMP or UDP as well as protocol-related options such as port numbers. You can use services to determine the types of traffic allowed or denied by the firewall.

Certain well-known traffic types have been predefined in services. These predefined services are defaults, and cannot be updated or deleted. If you require service definitions that are different from the predefined services, you can add them as custom services.

The Services page displays the list of all the default and custom services. The page also provides an option to add a new service, update the parameters of the existing service, or delete a service.

### Note

- Service used by a Firewall Rule cannot be deleted.
- Default Service can neither be updated nor deleted.



## Manage Service List

To manage services, go to **Objects > Services > Services**.


Name	Protocol	Details	Manage
Service_26103_1	TCP/UDP	TCP (1) / (2)	
Service_26103_10	TCP/UDP	TCP (10) / (11)	
Service_26103_11	TCP/UDP	TCP (11) / (12)	
Service_26103_12	TCP/UDP	TCP (12) / (13)	
Service_26103_13	TCP/UDP	TCP (13) / (14)	

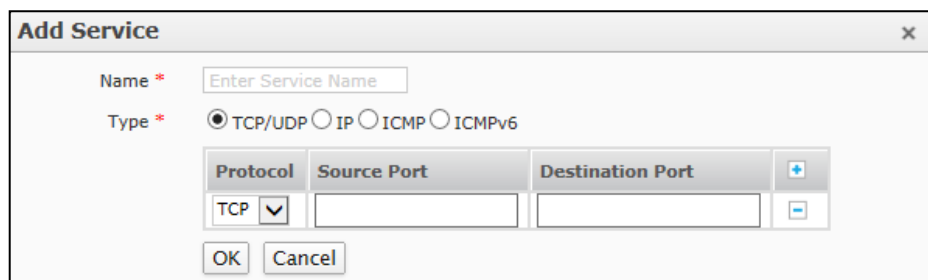
**Screen – Manage Service**

Screen Element	Description
<b>Name</b>	Displays the name of the Service.
<b>Protocol</b>	Displays the protocol used for the service.
<b>Details</b>	Details of the ports, protocol number or ICMP type and code based on the protocol selected.

**Table – Manage Service screen elements**

## Service Parameters

To add or edit a service, go to **Objects > Services > Services**. Click the Add button to add a new service. To update the details, click on the service or Edit icon  in the Manage column against the service you want to modify.



Screen – Add Services



Screen Element	Description
<b>Name</b>	Specify a name to identify the Service.
<b>Type</b>	<p>Select a protocol for the service.</p> <p><b>Available options:</b></p> <ul style="list-style-type: none"> <li>• <b>TCP/UPD</b> – Enter Source and Destination port. You can enter multiple ports for the same service.</li> <li>• <b>IP</b> – Select Protocol Number for the service. You can select multiple ports for the same service.</li> <li>• <b>ICMP</b> – Select ICMP Type and Code. You can enter multiple types and codes for the same service.</li> <li>• <b>ICMPv6</b> – Select ICMPv6 Type and Code. You can enter multiple types and codes for the same service.</li> </ul> <p>Use Add icon  and Remove icon  to add and delete the parameters respectively.</p>

Table – Add Services screen elements

## Service Group

Service Group is a grouping of services. Custom and default services can be grouped in a single group.

Use to configure Firewall Rules to:

- block group of services for specific zone
- limit some or all users from accessing group of services
- allow only specific user to communicate using group of service

To make it easier to add Firewall Rules, create groups of services and then add one firewall to allow or block access for all the services in the group. A service group can contain default services as well as custom services in any combination. A service can be member of multiple groups i.e. service can be included in multiple service groups.

The Service Group page displays the list of all default and custom groups. The page also provides options to add a new group, update the parameters of the existing group, add members to the existing group, or delete a group.

### Note











- Service Groups used by a Firewall Rule cannot be deleted.
- Default Service Groups can neither be updated nor deleted.

To manage Service Groups, go to **Objects > Services > Service Group**.

### Note

- Default Service Groups cannot be deleted.
- If a service group is assigned to Firewall Rule, it cannot be deleted.

## Manage Service Group list


<input type="checkbox"/>	Name	Description	Manage
<input checked="" type="checkbox"/>	PPTP_GROUP	TCP (1:65535) / (1723), IP Protocol No 47 (GRE)	
<input type="checkbox"/>	<a href="#">ServiceGrp_26211_1</a>		 
<input type="checkbox"/>	<a href="#">ServiceGrp_26211_14</a>		 
<input type="checkbox"/>	<a href="#">ServiceGrp_26211_15</a>		 
<input type="checkbox"/>	<a href="#">ServiceGrp_26211_16</a>		 
<input type="checkbox"/>	<a href="#">ServiceGrp_26211_17</a>		 

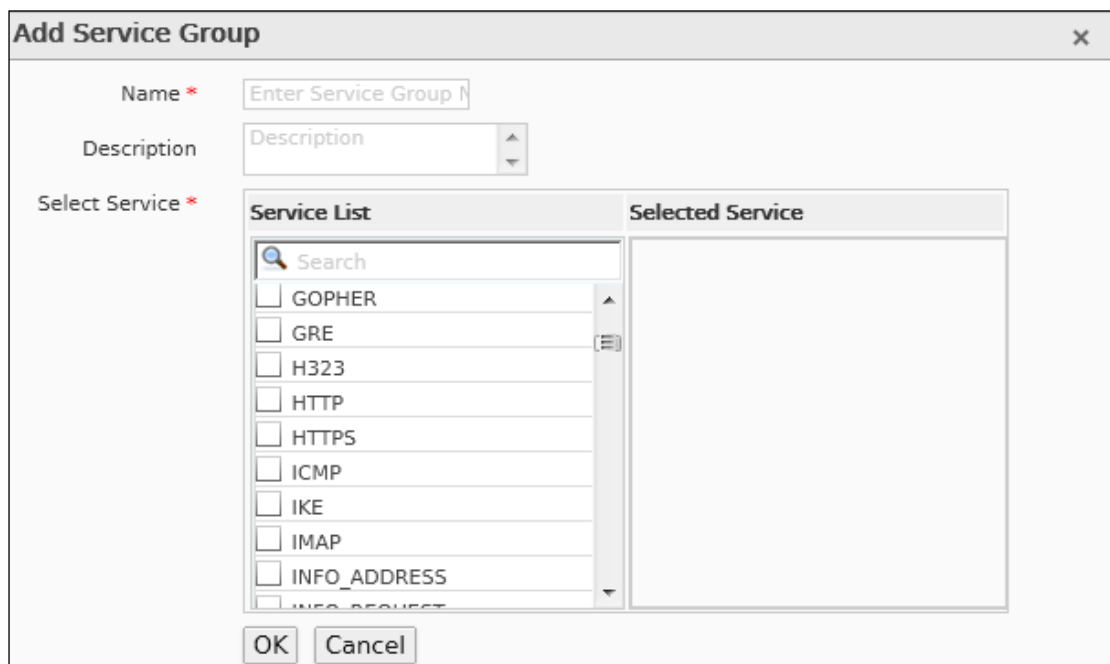
Screen – Manage Service Group

Screen Element	Description
Name	Displays the name of the Service Group.
Description	Description of the Service Group.

Table – Manage Service Group screen elements

### Service Group Parameters

To add or edit a service group, go to **Objects > Services > Service Group**. Click the Add button to add a new service group. To update the details, click on the service group or Edit icon  in the Manage column against the service group to be modified.



Screen – Add Services Group

Screen Element	Description
<b>Name</b>	Specify a name to identify the Service Group.
<b>Description</b>	Service Group Description.
<b>Select Service</b>	<p>“Service List” displays all the services including default services.</p> <p>Click the checkbox to select the service. All the selected services are moved to the “Selected Service” list.</p> <p>Single service can be member of multiple groups.</p> <p>You can also search for a particular service from the list.</p>

Table – Add Services Group screen elements

## Schedule

Schedule defines a time schedule for applying Firewall Rule or Web & Application Filter policy i.e. used to control when Firewall Rules or Internet Access policies are active or inactive.

Schedule also defines the system triggered scan for Rogue AP Scan.

Types of Schedules:

- **Recurring** – use to create policies that are effective only at specified times of the day or on specified days of the week.
- **One** – time - use to create Firewall Rules that are effective once for the period of time specified in the schedule. One time schedule can be implemented through firewall only.
- [Schedule](#)

## Schedule

The Appliance is shipped with following pre-defined schedules which can be applied to Firewall Rules and various policies: Work hours (5 Day week), Work hours (6 Day week), All Time on Weekdays, All Time on Weekends, All Time on Sunday, All Days 10:00 to 19:00. You can also create new schedule and modify the existing schedules.

The Schedule page displays the list of all the predefined and custom schedules. The page also provides options to add a new schedule, update the parameters of the existing schedule, or delete a schedule.


To manage Schedules, go to **Objects > Schedule > Schedule**.

### Note

- If a Schedule is used by Firewall Rule or any policies, it cannot be deleted.

## Manage Schedules

To manage schedules, go to **Objects > Schedule > Schedule**.

<input type="checkbox"/>	Name	Type	Description	Manage
<input type="checkbox"/>	<a href="#">Schedule12</a>	One Time		 
<input type="checkbox"/>	<a href="#">All Days 10:00 to 19:00</a>	Recurring	All Days 10:00 to 19:00	 
<input type="checkbox"/>	<a href="#">All Time on Sunday</a>	Recurring	All Time on Sunday	 
<input type="checkbox"/>	<a href="#">All Time on Weekdays</a>	Recurring	All Time on Weekdays Mon - Fri	 
<input type="checkbox"/>	<a href="#">All Time on Weekends</a>	Recurring	All Time on Weekends	 
<input type="checkbox"/>	<a href="#">Schedule_26318_11</a>	Recurring		 
<input type="checkbox"/>	<a href="#">Schedule_26318_12</a>	Recurring		 

Screen – Manage Schedule

Screen Element	Description
Name	Displays the name of the Schedule.
Type	Displays the Type of Schedule – Recurring or One Time
Description	Description of the Schedule.

Table – Manage Schedule screen elements

## Schedule Parameters

Screen – Add Schedule

Screen Element	Description
Name	Name to identify the Schedule.
Description	Specify Schedule Description.
Type	<p>Select “Schedule Type”.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Recurring</b> – Use to create access time policies that are effective only at specified times of the day or on specified days of the week.</li> <li>• <b>One Time</b> – Use to create Firewall Rules that are effective once for the period of time specified in the schedule. It cannot be applied to any of the policies but can be implemented through Firewall Rule only.</li> <li>• <b>Start &amp; End Date</b> - Specify Start and Stop date. This is applicable for the one time schedule only.</li> </ul> <p>Also, select the days of the week and specify time for the schedule to be active. Stop time cannot be greater than start time.</p>

Table – Add Schedule screen elements

## File Type

File Type is a grouping of file extensions or MIME headers. The Appliance allows filtering Internet content based on file extension and MIME headers. For example, you can restrict access to particular types of files from sites within an otherwise-permitted category.

When both Extension & MIME header are configured, both will be matched separately. If a file does not match any extension or header, it is passed. Access decision is based on the action configured for the extension.

Depending on the organization requirement, allow or deny access to the file types with the help of policies by groups, individual user, time of day, and many other criteria.

For convenience, the Appliance is shipped with several default File Types categories. You can use these or even create a new File Type category to suit your needs.

Custom file type is given priority over default category while allowing/restricting the access and is implemented through Web Filter policy.

The File Type Category page displays the list of all the predefined and custom file type categories. The page also provides options to add a new category, update the parameters of the existing category, or delete a category.

### Note

- Category included in Web Filter Policy cannot be deleted.
- Default Categories cannot be edited or deleted.

## Manage File Type Categories

To manage file type categories, go to **Objects > File Type > File Type**.


Add		Delete			
Name	File Extensions	MIME Headers	Description	Manage	
<input checked="" type="checkbox"/> Audio Files	gsm, sd2, qcp, kar, smf, midi, mid, ulw, snd, aifc, aif, aiff, m3uri, m3u, wav, rm, ram, mp3, wmv	audio/x-gsm, audio/vnd.qcelp, audio/x-midi, application/x-midi, audio/midi, audio/x-mid, x-music/x-midi, audio/basic, audio/x-adpcm, audio/aiff, audio/x-aiff, audio/x-mpeurl, audio/wav, audio/x-wav, application/vnd.rn-realmedia, audio/x-au, audio/x-pn-realaudio, audio/mpeg3, audio/x-mpeg-3, audio/x-ms-wmv	Audio Files  The Backup Files category includes individual file backups and files related to backup software. Individual backup files are often generated automatically by software programs. Backup software files include incremental backups and full system backups.		
<input checked="" type="checkbox"/> Backup Files	asd, bak, bkp, bup, dba, dbk, fbw, gho, nba, old, ori, sqb, tlg, tmp				
<input checked="" type="checkbox"/> Compressed Files	7z, alz, deb, gz, pkg, pup, rar, rpm, sea, sfx, sit, sitx, tar, gz, tgz, war, zip, zipx	application/x-7z-compressed, application/x-alz, application/x-deb, application/x-gzip, application/x-newton-compatible-pkg, application/x-rar-compressed, application/sea, application/x-sea, application/x-sit, application/x-stuffit, application/gnutar, application/x-compressed, application/x-zip-compressed, application/zip, multipart/x-zip	Compressed files use file compression in order to save disk space. Compressed archive formats can also be used to compress multiple files into a single archive.		
<input checked="" type="checkbox"/> Configuration Files	cfg, clg, dbb, ini, keychain, prf, pfx, psl, rdf, reg, thmx, vmx, wfc	application/pics-rules, application/vnd.ms-officetheme	Configuration files store settings for the operating system and applications. These files are not meant to be opened by the user, but are modified by the corresponding application when the program preferences are changed. Configuration files may also be called preference files or settings files.		
<input type="checkbox"/> Cyberoam	avi, dat, fic, flv, m15, m1a, m1u, m75, mls, mov, mp2, mpeg, mpg, mpm, qt, rm, smi, smil, sml, swf, vfw, wmv	Video/fic, application/smil, application/vnd.rn-realmedia, application/x-shockwave-flash, application/x-simile, application/x-troff-msvideo, video/avi, video/flv, video/flv, video/mpeg, video/msvideo, video/quicktime, video/x-flv, video/x-mpeg, video/x-mpeg2a, video/x-msvideo			
<input checked="" type="checkbox"/> Database Files	accdb, db, dsn, mdb, mdf, pdb, sql, sqlite	application/msaccess, application/x-msaccess, application/vnd.msaccess, application/vnd.ms-access, application/mdb, application/x-mdb, chemical/x-pdb	Database files store data in a structured format, organized into tables and fields. Individual entries within a database are called records. Databases are commonly		

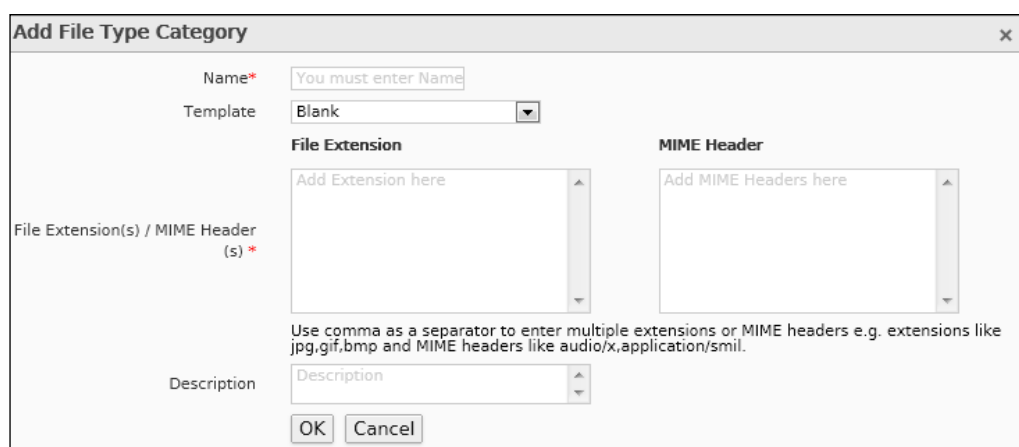
Screen – Manage File Type Category

Screen Element	Description
<b>Name</b>	Displays the name of the File Type Category.
<b>File Extensions</b>	Displays the File types included in Category.
<b>MIME Headers</b>	MIME header included in Category.
<b>Description</b>	Description of the File Type Category.

Table – Manage File Type Category screen elements

## File Type Category Parameters

To add or edit a file type category, go to **Objects > File Type**. Click the Add button to add a new file type category. To update the details, click on the file type category or Edit icon  in the Manage column against the file type category to be modified.



Screen – Add File Type Category

Screen Element	Description
<b>Name</b>	Specify a name to identify the File Type Category.
<b>Template</b>	Select a template if you want to create a new category based on an existing category and want to inherit all the file extensions and MIME header from the existing category.
<b>File Extension(s)/MIME Header(s)</b>	<p>Enter the file extensions and MIME header to be included in the category. Multiple extensions and MIME headers can be entered using comma e.g. bmp, jpeg</p> <p>At the end of the MIME header, wildcard * can be added to include all-inclusive pattern. For example, if MIME header is configured in the format audio/*, than all the files with MIME Type - audio will be considered.</p> <p>Appendix C lists the default file type categories.</p>
<b>Description</b>	Describe the File Type Category.

Table – Add File Type Category screen elements



# Network

Network establishes how your Appliance connects, interacts with your network, and allows configuring of network specific settings.

This menu covers how to configure the Appliance to operate in your network. Basic network settings include configuring your Appliance interface and DNS settings. More advanced configuration includes adding Virtual LAN sub-interfaces and custom zones to the network configuration. It also describes how to use DHCP to provide convenient automatic network configuration for your clients. It provides steps on how to backup and restore your system configuration.

- [Interface](#)
- [Wireless WAN](#)
- [Gateway](#)
- [Static Route](#)
- [DNS](#)
- [DHCP](#)
- [ARP](#)
- [Dynamic DNS](#)

## Interface

The Appliance is shipped with a number of physical interfaces/ports and the number of interfaces depends on the Appliance model. The physical interfaces can be configured as:

- **Alias** – Alias allows binding multiple IP Addresses onto a single physical interface. It is another name for the interface that will easily distinguish this interface from another interface.
- **Bridge Pair** – Bridge pair enables to configure transparent subnet gatewaying.
- **LAG** – Link Aggregation Group (LAG) is a method by which multiple network connections can be combined into a single connection. It is also known as trunking, NIC teaming, NIC bonding and Ether Channel. LAG is mostly used for handling LAN traffic.
- **VLAN** – Virtual LAN is a broadcast domain configured on switch on a port-by-port basis.
- **WLAN** – Wireless Local Area Network (WLAN) is used to associate devices through wireless distribution method and connection to the Internet is provided through an access point.
- **WWAN** – Wireless WAN is wide area network (WAN) for data that is typically provided by the cellular carriers to transmit a wireless signal over a range of several miles to a mobile device.
- **TAP** - Test Access Point (TAP) interface enables to deploy Cyberoam in Discover Mode. This mode enables Cyberoam to monitor all network traffic without making any changes in the existing network schema. Discover Mode could be configured through Command Line Interface (CLI).

### Pre-requisites for Discover Mode:

1. All relevant modules (IPS, Web & Application Filter, Anti Virus and Anti Spam) should be subscribed.
2. Cyberoam must be connected to the Internet for Web classification, IPS updates and SAR generation on cloud.
3. Cyberoam must be integrated with External Authentication servers like Active Directory, RADIUS, LDAP etc. to get users specific data in the Security Assessment Report (SAR). SAR provides visibility into potential risks prevailing within the corporate network like application and web risks, risky users and intrusion risks.

A Zone is a logical grouping of ports/interfaces and each port is a member of a zone.


#### Note

- If PPPoE is configured, WAN port is displayed as the PPPoE interface.

- [Interface](#)
- [IP Tunnel](#)
- [Zone](#)


## Interface

The Interface page displays a list of physical interfaces, aliases, virtual sub-interfaces, bridge-pair interfaces, interfaces configured as LAG, interfaces configured for wireless LAN, interfaces configured for wireless WAN and interfaces configured as TAP.

If the virtual sub-interface is configured for the physical interface, it is also displayed beneath the physical interface. Virtual sub-interface configuration can be updated or deleted. Click the Toggle Drill Down  icon to view the alias and virtual sub-interfaces defined for the said physical interface.


If a Wireless Network is configured with “Separate Zone” for Client Traffic mode under Wireless Protection > Wireless Networks, a virtual interface of type “Wireless Protection” is automatically created with the configured IP Address and Zone of the Wireless network on this page. The interface would be created with the name provided for the Wireless Network. To use the interface, you need to configure DHCP Server for the interface so that the wireless clients can connect to the appliance. The interface will be automatically deleted once the Wireless Network is deleted.

To manage interfaces, go to **Network > Interface > Interface**. You can:

- [Update Physical Interface/Port details](#) – Only Default Physical interface can be updated. Click the Interface Name or Edit icon  in the Manage column against the IP Address and netmask of physical interface to be modified.
- [Update Wireless WAN Connection](#) – Wireless WAN is the default interface along with other physical interfaces, if the device is supported by your Appliance.

#### Note

- Updating Interface also removes all its dependent configurations including:
- Interface Zone Binding, DNS, Gateway, Interface Based Hosts, VLAN Interfaces, Dynamic DNS
- Stops the DHCP Server to update the details and one need to restart manually
- Disconnects all tunnels and updates all the VPN Policies, Tunnels need to be manually reconnected.

- Toggle Drill Down icon – Click the  icon to view the alias and virtual sub-interfaces defined for the said physical interface.

#### Note

- A virtual sub-interface cannot be deleted, if virtual sub-interface is member of any zone or a firewall rule is defined for the virtual sub-interface.

- Deleting Interface also removes all its dependent configurations including: Interface Zone Binding, DHCP Server or Relay, Interface Based Firewall Rule, ARP – Static and Proxy, Virtual Hosts, Virtual Host based Firewall Rules, Interface based Hosts and References from Host Groups, Unicast and Multicast Routes.
- When deployed in Discover Mode, Cyberoam functions ONLY in a listening mode and, hence, none of the security policies will be applied.

## Manage Interfaces - Physical, Aliases & Virtual Sub-interfaces

To manage interfaces, go to **Network > Interface > Interface**.

<input type="button" value="Add Bridge"/> <input type="button" value="Add Alias"/> <input type="button" value="Add VLAN"/> <input type="button" value="Add LAG"/> <input type="button" value="Delete"/>												
	<input type="checkbox"/>	Interface Name	Interface Type	Status	IP Address		Zone Name	MAC Address	MSS	MTU	Interface Speed	Manage
					IP	Type						
	<input type="checkbox"/>	PortA	Physical	Connected, 1000 Mbps - Full Duplex	172.16.16.16/255.255.255.0	Static	LAN	00:0D:48:32:C5:63	1460	1500	Auto-negotiated	
	<input type="checkbox"/>	PortB	Physical	Connected, 1000 Mbps - Full Duplex	10.202.22.4/255.255.192.0	Static	WAN	00:0D:48:32:C5:64	1460	1500	Auto-negotiated	
	<input type="checkbox"/>	PortC	Physical	Unplugged	10.10.1.1/255.255.255.0	Static	DMZ	00:0D:48:32:C5:65	1460	1500	Auto-negotiated	
	<input type="checkbox"/>	PortD	Physical (TAP)	Unplugged	N/A	N/A	Discover	00:0D:48:32:C5:66	1460	1500	Auto-negotiated	
	<input type="checkbox"/>	PortE	Physical	Unplugged	1.1.1.1/255.255.255.0	Static	LAN	00:0D:48:32:C5:67	1460	1500	Auto-negotiated	
	<input type="checkbox"/>	PortF	Physical (TAP)	Unplugged	N/A	N/A	Discover	00:0D:48:32:C5:68	1460	1500	Auto-negotiated	

### Screen – Manage Interface

Screen Element	Description
<b>Interface Name</b>	<p>Displays the Interface name in case of Physical Interface, Port name and for Wireless WAN connection, WWAN name.</p> <p>If Alias or VLAN is added for the Interface, it is displayed beneath the physical interface. Click  to view the Alias or VLAN details.</p>
<b>Interface Type</b>	<p>Displays interface type.</p> <ul style="list-style-type: none"> <li>• TAP is displayed for the interfaces configured in Discover mode.</li> </ul>
<b>Status (Only when Appliance is deployed in Gateway mode)</b>	<p>Interface connection status –</p> <ul style="list-style-type: none"> <li>• Connected</li> <li>• Unplugged</li> <li>• Disabled</li> </ul>
<b>IP Address - IP</b>	<p>When appliance is deployed in Gateway mode, IP Address and the Netmask is displayed.</p> <p>When Appliance is deployed in Bridge mode, IP Address and Netmask is displayed for the bridge pair and not for the individual member interfaces.</p>

<b>IP Address – Type</b> (Only when Appliance is deployed in Gateway mode)	IP Address type <ul style="list-style-type: none"> <li>• Static</li> <li>• PPPoE</li> <li>• DHCP</li> <li>• Wireless Modem</li> </ul>
<b>Zone Name</b> (Only when the Appliance is deployed in Gateway mode)	Type of Zone to which the interface or sub-interface is bound to.
<b>MAC Address</b>	MAC Address selected.
<b>MSS</b>	Maximum Segment size specified
<b>MTU</b>	Configured Maximum Transmission Unit
<b>Interface Speed</b> (Only when the Appliance is deployed in Gateway mode)	Configured Interface Speed.

#### Screen – Manage Interface screen elements

#### Note

- Not all the operations are supported when Cyberoam is deployed in Bridge mode.
- Interface Manage page will display Zone Name as 'Discover' for interfaces configured in Discover Mode.
- TAP interface cannot be updated or deleted.
- Only unbound Physical Interfaces can be configured in Discover mode.

## Edit Physical Interface

(Only when the Appliance is deployed in Gateway mode)

Go to **Network > Interface > Interface**. Click the hyperlink of the physical interface whose settings need to be updated.

**General Settings**

Physical Interface: PortA

Network Zone: LAN

IPv4 Configuration

IP Assignment:  Static  PPPoE  DHCP

IPv4 / Netmask: 172.16.16.16 / 24 (255.255.255.0)

**Gateway Detail**

Gateway Name:

IP Address:

IPv6 Configuration

IP Assignment:  Static  DHCP

IPv6 / Prefix:  / 64

**Gateway Detail**

Gateway Name:

IP Address:

**Advanced Settings**

Interface Speed: Auto Negotiation

MTU: 1500 (1280 - 1500)

Override MSS: 1460 (536 - 1460)

Use Default MAC Address: 00:0D:48:32:C5:63

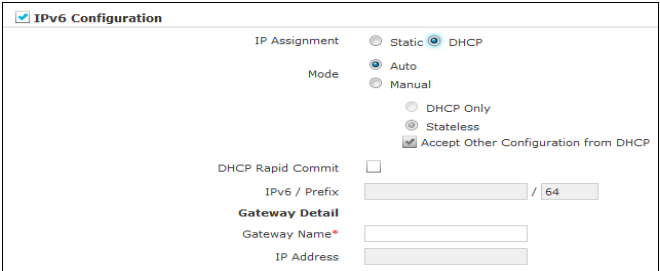
Override Default MAC Address:

Screen – Edit Physical Interface

Screen Element	Description
<b>General Settings</b>	
<b>Physical Interface</b>	Physical Interface for example, Port A, Port B
<b>Network Zone (Only when Appliance is deployed in Gateway mode)</b>	<p>Select Zone to which Interface belongs.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• None</li> <li>• LAN</li> <li>• WAN</li> <li>• DMZ</li> </ul> <p>To unbind, select “None”.</p>
<b>IPv4 Configuration</b>	
<b>IP Assignment</b>	Select IP Assignment type.

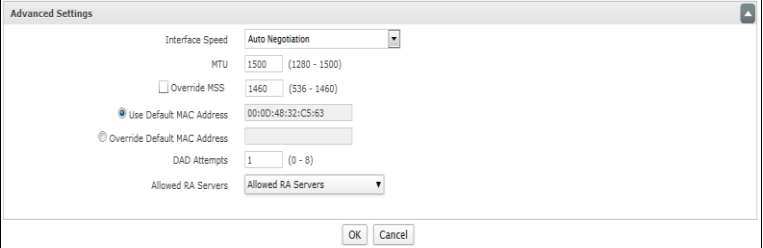
	<p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Static</b> – Static IP Addresses are available for all the zones.</li> <li>• <b>PPPoE</b> – PPPoE is available only for WAN Zone. If PPPoE is configured, WAN port is displayed as the PPPoE Interface.</li> <li>• <b>DHCP</b> – DHCP is available only for WAN Zone.</li> </ul>
<p><b>IPv4 / Netmask</b></p>	<p>Specify IPv4 Address and Network Subnet mask.</p>
<p><b>Gateway Detail (Only when Network Zone is “WAN”)</b></p>	<ul style="list-style-type: none"> <li>• <b>For “Static” IP assignment</b> – Specify the Gateway Name and IP Address through which the traffic is to be routed.</li> <li>• <b>For “PPPoE” IP assignment</b> – Specify the Gateway Name, IP Address, PPPoE account Username and Password, Service Name, LCP Echo Interval, LCP failure attempts.</li> </ul> <div data-bbox="651 730 1390 1149" style="border: 1px solid black; padding: 5px;"> <p><input checked="" type="checkbox"/> IPv4 Configuration</p> <p>IP Assignment <input type="radio"/> Static <input checked="" type="radio"/> PPPoE <input type="radio"/> DHCP</p> <p>IPv4 / Netmask* <input type="text"/> / <input type="text" value="/24 (255.255.255.0)"/> <input type="button" value="v"/></p> <p>Preferred IP <input type="text"/></p> <p><b>Gateway Detail</b></p> <p>Gateway Name* <input type="text"/></p> <p>IP Address <input type="text"/></p> <p>Username* <input type="text"/></p> <p>Password* <input type="password" value="Password"/></p> <p>Confirm Password <input type="password"/></p> <p>Access Concentrator/Service Name <input type="text"/> / <input type="text"/></p> <p><input checked="" type="checkbox"/> LCP Echo Interval Send LCP echo request every <input type="text" value="20"/> seconds (5-180,Default:20)</p> <p><input checked="" type="checkbox"/> LCP Failure Wait for LCP echo reply for <input type="text" value="3"/> attempts (Default:3)</p> <p><input type="checkbox"/> Schedule Time For Reconnect <input type="text" value="All Days of week"/> <input type="text" value="00"/> <input type="text" value="00"/> HH <input type="text" value="00"/> <input type="text" value="00"/> MM</p> </div> <p>Appliance initiates only those sessions with Access Concentrator, which can provide the specified service.</p> <ul style="list-style-type: none"> <li>• Preferred IP Many Internet Service Providers assign a fixed IP Address for the PPPoE connection. The Administrator is allowed to bind a static IP Address for a PPPoE.</li> <li>• LCP Echo Interval It is time to wait before sending echo request to check whether the link is alive or not.  Default – 20 Seconds.</li> <li>• LCP failure Appliance will wait for the LCP echo request response for the LCP Echo interval defined after every attempt. It declare PPPoE link as closed if it does not receive response after defined number of attempts.</li> </ul>

	<p>Default Attempts Allowed – 3</p> <ul style="list-style-type: none"> <li>• Schedule Time For Reconnect</li> </ul> <p>The assigned IP Address, dynamic or static (preferred), for a PPPoE connection may have a stipulated validity. Once the validity is over the PPPoE connection is terminated and reconnected.</p> <p>In order to avoid the reconnection during the working hours, the Administrator can enable the PPPoE reconnection schedule. An Administrator can choose to schedule the PPPoE reconnection on daily or weekly basis on the configured time (HH:MM).</p> <p>Default - Disable</p> <p>Default schedule when enabled – All days of week at 00:00 hours.</p> <ul style="list-style-type: none"> <li>• <b>For “DHCP” IP assignment</b> – Specify the Gateway Name and IP Address through which the traffic is to be routed.</li> </ul> <div data-bbox="663 976 1374 1245" style="border: 1px solid black; padding: 5px;"> <p><input checked="" type="checkbox"/> IPv4 Configuration</p> <p>IP Assignment    <input type="radio"/> Static <input type="radio"/> PPPoE <input checked="" type="radio"/> DHCP</p> <p>IPv4 / Netmask*    <input type="text"/> / <input type="text" value="/24 (255.255.255.0)"/> <input type="button" value="v"/></p> <p><b>Gateway Detail</b></p> <p>Gateway Name*    <input type="text"/></p> <p>IP Address    <input type="text"/></p> </div>
<b>IPv6 Configuration</b>	
<b>IP Assignment</b>	<p>Select IP Assignment type.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Static</b> – Static IP Addresses are available for all the zones.</li> <li>• <b>DHCP</b> – DHCP is available only for WAN Zone.</li> </ul>
<b>Mode</b>	<p>Select DHCP mode.</p> <p>Administrator can select to configure IPv6 address through Stateful (DHCPv6) or StateLess address assignment methods depending on the Managed (M) Address Configuration and Other (O) Configuration flags advertised in the Router Advertisement (RA) message.</p> <p>Available options:</p> <ul style="list-style-type: none"> <li>• Auto - If selected, IPv6 address will be configured based on the Router Advertisement packet through Stateless Address Auto-Configuration (SLAAC).</li> <li>• Manual - Administrator can select to configure IPv6 address either through SLAAC or DHCPv6.</li> </ul>

	<p><b>DHCP Only</b> – In this manual mode, client will configure IPv6 Address and other configuration parameters using DHCPv6 Server. Gateway details should be manually specified.</p> <p><b>Stateless</b> – In this manual mode, client will configure IPv6 Address based on advertised RA message through SLAAC.</p> <p><b>Accept Other Configuration from DHCP (Only for Stateless Manual mode)</b> – Select to configure other parameters using DHCPv6 Server. By default, it is enabled.</p> 
<p><b>DHCP Rapid Commit</b></p>	<p>If enabled, the interface will be configured using a 2-message exchange (Solicit and Reply) rather than the 4-message exchange (Solicit, Advertise, Request, and Reply). It enables quicker client configuration.</p> <p>Rapid commit should also be enabled on the DHCPv6 server.</p>
<p><b>IPv6 / Prefix (Only for Static IP Assignment)</b></p>	<p>Specify IPv6 Address and the Prefix.</p>
<p><b>Gateway Detail (Only when Network Zone is “WAN”)</b></p>	<ul style="list-style-type: none"> <li>• For <b>“Static” IP assignment</b> - Specify the Gateway Name and IPv6 Address through which the traffic is to be routed.</li> <li>• For <b>“DHCP” IP assignment</b> - Specify the Gateway Name, if “Stateless” manual mode is selected. For “DHCP only” manual mode, specify Gateway name and IPv6 Address.</li> </ul>
<b>Advanced Settings</b>	
<p><b>Interface Speed</b></p>	<p>Select Interface speed for synchronization.</p> <p>Speed mismatch between Appliance and 3<sup>rd</sup> party routers and switches can result into errors or collisions on interface, no connection or traffic latency, slow performance.</p> <p><b>Depending on the model deployed following options will be available:</b></p> <ul style="list-style-type: none"> <li>• Auto Negotiate</li> <li>• 10 Mbps - Full duplex</li> <li>• 10 Mbps - Half duplex</li> <li>• 100 Mbps - Full duplex</li> <li>• 100 Mbps - Half duplex</li> </ul>



	<ul style="list-style-type: none"> <li>• 1000 Mbps - Full duplex</li> <li>• 1000 Mbps - Half duplex</li> </ul> <p>Default – Auto Negotiate</p>
<b>MTU</b>	<p>Specify MTU value (Maximum Transmission Unit)</p> <p>MTU is the largest physical packet size, in bytes, that a network can transmit. This parameter becomes an issue when networks are interconnected and the networks have different MTU sizes. Any packets larger than the MTU value are divided (fragmented) into smaller packets before being sent.</p> <p>Default – 1500</p> <p>Acceptable Range – 576 to 1500</p>
<b>Override MSS</b>	<p>Click to override default MSS.</p> <p>MSS defines the amount of data that can be transmitted in a single TCP packet.</p> <p>Default – 1460</p> <p>Acceptable Range – 536 to 1460</p> <p>For PPPoE</p> <p>Default – 1452</p> <p>Acceptable Range – 528 to 1452</p>
<b>Use Default MAC Address</b> (Not available for alias, VLAN, virtual interfaces, PPPoE, serial modem interface, dedicated HA link, Wireless LAN, Wireless WAN and bridge interface)	<p>Click to use the default MAC Address for the Interface.</p> <p>If High Availability is configured, Virtual MAC Address will be the default MAC Address.</p>
<b>Override Default MAC Address</b> (Not available for alias, VLAN, virtual interfaces, PPPoE, serial modem interface, dedicated HA link, Wireless LAN, Wireless WAN and bridge interface)	<p>Click to override the default MAC Address for the Interface and enter the new MAC Address.</p> <p>On factory reset, it will be set to the default MAC Address.</p>

<p><b>DAD Attempts</b></p>	<p>Specify number of neighbour solicitation messages that are sent during Duplicate Address Detection (DAD) process.</p> <p>DAD is a process through which a node determines that the address it uses is not in use by another node.</p> <p>Acceptable Range - 0 to 8</p> <p>Default – 1</p>  <p>The screenshot shows the 'Advanced Settings' dialog box with the following fields: Interface Speed (Auto Negotiation), MTU (1500), Override MSS (1460), Use Default MAC Address (00:00:48:32:C5:63), Override Default MAC Address, DAD Attempts (1), and Allowed RA Servers (Allowed RA Servers). The DAD Attempts field is highlighted with a red box.</p>
<p><b>Allowed RA Servers</b></p>	<p>Select Router Advertisement Servers. RA client interface will accept or process RA packets only from the specified RA Servers.</p>

**Table – Edit Physical Interface screen elements**


**Note**

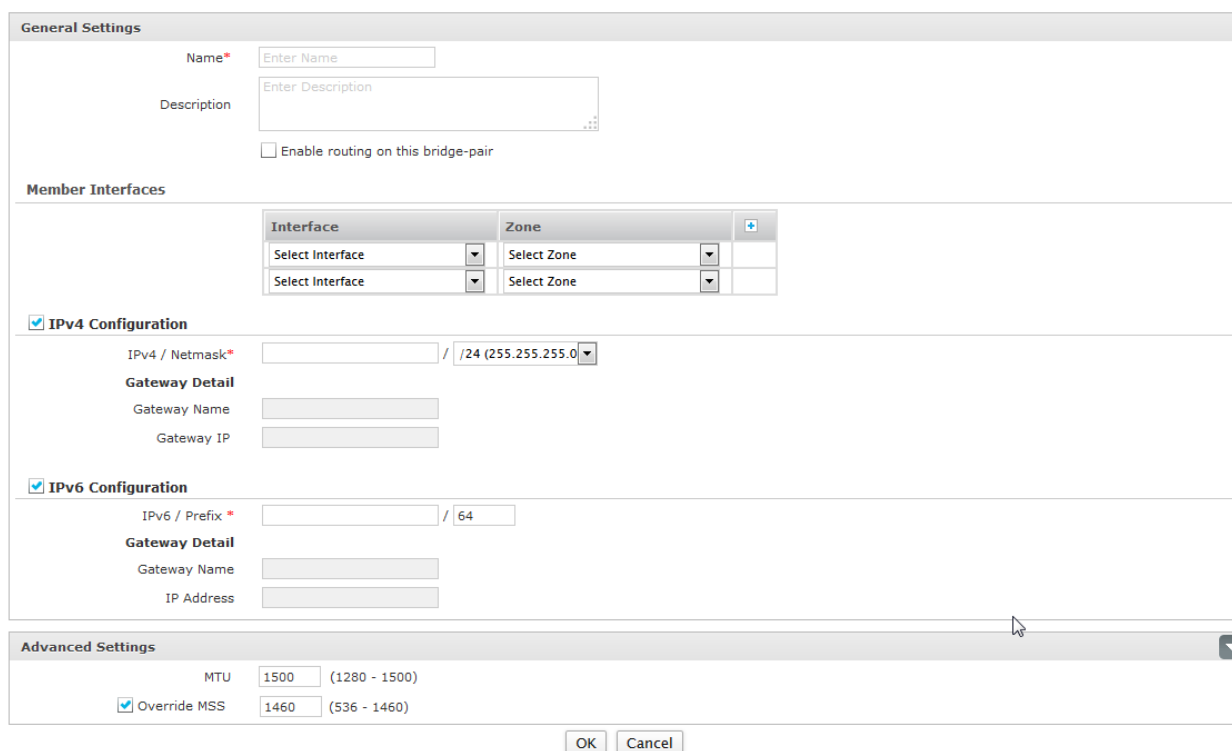
- PPPoE Interface is assigned a new dynamic IP Address for each new PPP session
- IP Address in Firewall Rules automatically changes when the new IP Address is leased
- If multiple gateways are defined then IP Address in the failover condition automatically changes when the new IP Address is leased.
- As IP Address to PPPoE interface is assigned dynamically, it cannot be viewed or changed from Network Configuration option of CLI Console.

## Bridge – Pair Parameters

(When Appliance is deployed as Bridge Mode / L2 Bridge Mode)

This feature is not supported in Cyberoam Virtual Security Appliances when deployed in Microsoft Hyper-V Hypervisors only.

To add or edit, go to **Network > Interface > Interface** and click Add Bridge – Pair. To update the details, click on the name of Bridge – Pair or Edit icon  in the Manage column against the Bridge – Pair you want to modify.



**General Settings**

Name\*

Description

Enable routing on this bridge-pair

**Member Interfaces**

Interface	Zone	
Select Interface	Select Zone	
Select Interface	Select Zone	

**IPv4 Configuration**

IPv4 / Netmask\*  /

**Gateway Detail**

Gateway Name

Gateway IP

**IPv6 Configuration**

IPv6 / Prefix \*  /

**Gateway Detail**

Gateway Name

IP Address

**Advanced Settings**

MTU  (1280 - 1500)

Override MSS  (536 - 1460)

OK Cancel

Screen – Add Bridge - Pair Interface

Screen Element	Description
<b>General Settings</b>	
<b>Name</b>	Provide a name to Identify the Bridge – Pair.
<b>Description</b>	Provide description for Bridge – Pair description.
<b>Enable routing on this bridge-pair</b>	Click to enable routing on this bridge-pair.
<b>Member Interfaces</b>	
<b>Interface</b>	Select the first physical interface for the bridge pair. For example, Port A, Port B.
<b>Zone</b>	Select zone to which the Interface 1 belongs.
<b>IPv4 Configuration</b>	

<b>IPv4/Netmask</b>	Specify IPv4 Address and the network subnet mask.
<b>Gateway Detail</b>	
<b>Gateway Name</b>	Specify a name to identify the Gateway.
<b>Gateway IP</b>	Specify IPv4 Address for the Gateway.
<b>IPv6 Configuration</b>	
<b>IPv6 / Prefix</b>	Specify IPv6 Address and the prefix.
<b>Gateway Detail</b>	
<b>Gateway Name</b>	Specify a name to identify the Gateway.
<b>IP Address</b>	Specify IPv6 Address for the Gateway.
<b>Advanced Settings</b>	
<b>MTU</b>	<p>Specify MTU value (Maximum Transmission Unit)</p> <p>MTU is the largest physical packet size, in bytes, that a network can transmit. This parameter becomes an issue when networks are interconnected and the networks have different MTU sizes. Any packets larger than the MTU value are divided (fragmented) into smaller packets before being sent.</p> <p>Default – 1500 Acceptable Range – 576 to 1500</p>
<b>Override MSS</b>	<p>Click to override default MSS.</p> <p>MSS defines the amount of data that can be transmitted in a single TCP packet.</p> <p>Default – 1460 Acceptable Range – 536 to 1460</p>


Table – Add Bridge - Pair Interface screen elements

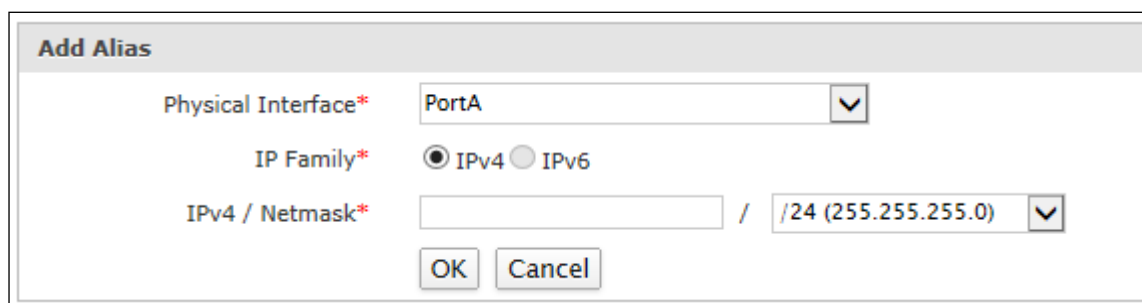
**Note**

- Multiport bridge can be configured. All interfaces of Cyberoam can be configured as member interfaces for a bridge-pair.
- A single WAN interface is supported in a multiport bridge-pair.
- Single interface cannot be part of multiple bridge.

## Alias Parameters

Alias allows binding multiple IP Addresses onto a single physical interface. It is another name for the interface that easily distinguishes this interface from other interfaces.

To add or edit an alias, go to **Network > Interface > Interface**. Click the Add button to add a new alias. To update the details, click on the alias name or Edit icon  in the Manage column against the alias you want to modify.



Screen – Add Alias

Screen Element	Description
<b>Add Alias</b>	
<b>Physical Interface</b>	Select Physical Interface for which Alias is to be bounded.  <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>Alias can be added for the Virtual Sub-Interface and WLAN interface.</li> </ul> </div>
<b>IP Family</b>	Select the IP Family for Alias.  <b>Available options:</b> <ul style="list-style-type: none"> <li>IPv4</li> <li>IPv6</li> </ul>
<b>IPv4/Netmask (For IPv4 Family)</b>	Specify IPv4 Address and select the network subnet mask.
<b>IPv6/Prefix</b>	Specify IPv6 Address and the prefix.  Default – 64

## VLAN

A LAN is a local area network and is defined as all devices in the same broadcast domain. Routers stop broadcasts while switches just forward them.

VLAN is a virtual LAN. In technical terms, VLAN is a broadcast domain configured on switch on a port-by-port basis. Normally, it is a router that creates the broadcast domain but with VLANs, a switch can create the broadcast domain.

VLAN allow you to segment your switched network so that broadcast domains are smaller, leaving more bandwidth for your end nodes. Devices that are in one VLAN can communicate with each other but cannot communicate with the devices in another VLAN. The communication among devices on a VLAN is independent of the physical network.

For devices on different VLANs to communicate, a layer 3 device (usually a router) must be used.

A VLAN segregates devices by adding 802.1Q VLAN tags to all of the packets sent and received by the devices in the VLAN. VLAN ID/tags are 4-byte frame extensions that contain a VLAN identifier as well as other information.

### Advantages

- Increased Port density
- Logical segmentation of Network irrespective of physical placement
- Granular security on heterogeneous LANs
- Improved Network throughput as VLAN confines broadcast domain

### Appliance and VLAN support

The Appliance supports VLANs for constructing VLAN trunks between an IEEE 802.1Q-compliant switch or router and your Appliances. Normally, the Appliance internal interface connects to a VLAN trunk on an internal switch, and the external interface connects to an upstream Internet router. Appliance can then apply different policies for traffic on each VLAN that connects to the internal interface.

In a typical VLAN configuration, 802.1Q-compliant VLAN layer-2 switches or layer-3 routers add VLAN IDs to packets. Layer-2 switches can handle packets passing between devices in the same VLAN. A layer-3 device such as router or layer-3 switch must handle packets passing between devices in different VLANs.

Appliance functions as a layer-3 device to control the flow of packets between VLANs. Appliance can also remove VLAN IDs/tags from incoming VLAN packets and forward untagged packets to other networks, such as the Internet.

VLAN support on the Appliance is achieved by means of virtual interface, which are logical interfaces nested beneath a physical interface/port. Every unique VLAN ID requires its own virtual interface. You add virtual interfaces to the Appliance's internal interface that have VLAN IDs that match the VLAN IDs of packets in the VLAN trunk. Appliance then directs packets with VLAN IDs to interfaces with matching VLAN IDs. You can define virtual interfaces on all the interfaces except the external interface i.e. interface for the WAN zone. Appliance adds VLAN IDs to packets leaving a VLAN interface or removes VLAN IDs from incoming packets and adds a different VLAN IDs to outgoing packets.

Virtual interface has most of the capabilities and characteristics of a physical interface, including zone membership, security services, routing, access rule controls, virus, and spam scanning.

Using VLANs, a single Appliance can provide security services and control connections between multiple domains. Traffic from each domain is given a different VLAN ID. Appliance can recognize VLAN IDs and apply security policies to secure network between domains. Appliance can also apply authentication, various policies, and firewall rule features on the network traffic.

## VLAN Interface Parameters

To add or edit VLAN interfaces, go to **Network > Interface > Interface**. Click the Add VLAN Button to add a new VLAN interface or the Edit Icon to modify the details of an existing VLAN interface.

Screen – Add VLAN Interface

## Parameters

Screen Element	Description
<b>ADD VLAN</b>	
<b>Physical Interface</b>	Select parent Interface for the virtual sub-interface. Virtual sub-interface will be the member of the selected physical Interface/Port.

<b>Zone</b>	<p>Select a Zone to assign to the virtual sub-interface. Virtual sub-interface will be the member of the selected zone. It can be the member of LAN, DMZ, WAN or custom zone.</p> <p>Virtual sub-interface created will remain unused until it is included in a zone.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>Zone membership can be defined at the time of defining virtual sub-interface or later whenever required.</li> <li>One can also create a custom zone for Virtual sub-interface and Virtual sub-interface can be the member of this custom zone.</li> </ul> </div>
<b>VLAN ID</b>	<p>Specify the VLAN ID. The interface VLAN ID can be any number between 2 and 4094. The VLAN ID of each Virtual sub-interface must match the VLAN ID of the packet. If the IDs do not match, the virtual sub-interface will not receive the VLAN tagged traffic.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>Virtual sub-interfaces added to the same physical interface cannot have the same VLAN ID. However, you can add virtual sub-interfaces with the same VLAN ID to different physical interface.</li> </ul> </div>
<b>IPv4 Configuration</b>	
<b>IP Assignment</b>	<p>Select IP Assignment type.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li><b>Static</b> – Static IP Addresses are available for all the zones.</li> <li><b>PPPOE</b> – PPPOE is available only for WAN Zone. If PPPoE is configured, the WAN port will be displayed as the PPPoE Interface.</li> <li><b>DHCP</b> – DHCP is available only for WAN Zone.</li> </ul>
<b>IPv4/Netmask</b>	<p>Specify the IPv4 Address for the interface and select the Network subnet mask.</p>
<b>Gateway Detail (Only when Network Zone is “WAN”)</b>	<ul style="list-style-type: none"> <li><b>For “Static” IP assignment</b> – Specify the Gateway Name and IP Address through which the traffic is to be routed.</li> <li><b>For “PPPoE” IP assignment</b> – Specify the Gateway Name, IP Address, PPPoE account Username and Password, Service Name, LCP Echo Interval, LCP failure attempts.</li> </ul>



<input checked="" type="checkbox"/> IPv4 Configuration	
IP Assignment	<input type="radio"/> Static <input checked="" type="radio"/> PPPoE <input type="radio"/> DHCP
IPv4 / Netmask*	<input type="text"/> / <input type="text" value="/24 (255.255.255.0)"/> <input type="button" value="v"/>
Preferred IP	<input type="text"/>
<b>Gateway Detail</b>	
Gateway Name*	<input type="text"/>
IP Address	<input type="text"/>
Username*	<input type="text"/>
Password*	<input type="password" value="Password"/> <input type="password" value="Confirm Password"/>
Access Concentrator/Service Name	<input type="text"/>
<input checked="" type="checkbox"/> LCP Echo Interval	Send LCP echo request every <input type="text" value="20"/> seconds (5-180,Default:20)
<input checked="" type="checkbox"/> LCP Failure	Wait for LCP echo reply for <input type="text" value="3"/> attempts (Default:3)
<input type="checkbox"/> Schedule Time For Reconnect	<input type="text" value="All Days of week"/> <input type="text" value="00"/> HH <input type="text" value="00"/> MM

The Appliance initiates only those sessions with Access Concentrator, which can provide the specified service.

### Preferred IP

Many Internet Service Providers assign a fixed IP Address for the PPPoE connection. The Administrator is allowed to bind a static IP Address for a PPPoE.

### LCP Echo Interval

It is time to wait before sending echo request to check whether the link is alive or not.

Default – 20 Seconds.

### LCP failure

The Appliance will wait for the LCP echo request response for the LCP Echo interval defined after every attempt. It declare PPPoE link as closed if it does not receive response after defined number of attempts.

Default Attempts Allowed – 3.

### Schedule Time For Reconnect

The assigned IP Address, dynamic or static (preferred), for a PPPoE connection may have a stipulated validity. Once the validity is over the PPPoE connection is terminated and reconnected.

In order to avoid the reconnection during the working hours, the Administrator can enable the PPPoE reconnection schedule. An Administrator can choose to schedule the PPPoE reconnection on daily or weekly basis on the configured time (HH:MM).

Default - Disable

	<p>Default schedule when enabled – All days of week at 00:00.</p> <ul style="list-style-type: none"> <li>• <b>For “DHCP” IP assignment</b> – Specify the Gateway Name and IP Address through which the traffic is to be routed.</li> </ul> <div data-bbox="655 443 1407 725" style="border: 1px solid black; padding: 5px;"> <p><input checked="" type="checkbox"/> <b>IPv4 Configuration</b></p> <p>IP Assignment    <input type="radio"/> Static <input type="radio"/> PPPoE <input checked="" type="radio"/> DHCP</p> <p>IPv4 / Netmask*    <input type="text"/> / <input type="text" value="/24 (255.255.255.0)"/> ▼</p> <p><b>Gateway Detail</b></p> <p>Gateway Name*    <input type="text"/></p> <p>IP Address    <input type="text"/></p> </div>
<b>IPv6 Configuration (Only for those interfaces which are assigned IPv6 Address)</b>	
<b>IP Assignment</b>	<p>Select IP Assignment type.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Static</b> – Static IP Addresses are available for all the zones.</li> <li>• <b>DHCP</b> – DHCP is available only for WAN Zone.</li> </ul>
<b>Mode</b>	<p>Select DHCP mode.</p> <p>Administrator can select to configure IPv6 address through Stateful (DHCPv6) or Stateless address assignment methods depending on the Managed (M) Address Configuration and Other (O) Configuration flags advertised in the Router Advertisement (RA) message.</p> <p><b>Available options:</b></p> <ul style="list-style-type: none"> <li>• <b>Auto</b> - If selected, IPv6 address will be configured based on the Router Advertisement packet through Stateless Address Auto-Configuration (SLAAC).</li> <li>• <b>Manual</b> - Administrator can select to configure IPv6 address either through SLAAC or DHCPv6.</li> </ul> <p>DHCP Only – In this manual mode, client will configure IPv6 Address and other configuration parameters using DHCPv6 Server. Gateway details should be manually specified.</p> <p>Stateless – In this manual mode, client will configure IPv6 Address based on advertised RA message through SLAAC.</p> <p>Accept Other Configuration from DHCP (Only for Stateless Manual mode) – Select to configure other parameters using DHCPv6 Server. By default, it is enabled.</p>

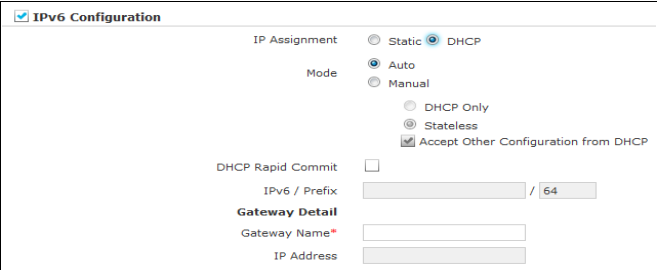
	
<b>DHCP Rapid Commit</b>	<p>If enabled, the interface will be configured using a 2-message exchange (Solicit and Reply) rather than the 4-message exchange (Solicit, Advertise, Request, and Reply). It enables quicker client configuration.</p> <p>Rapid commit should also be enabled on the DHCPv6 server.</p>
<b>IPv6/Prefix (Only for Static IP Assignment)</b>	Specify IPv6 Address and the prefix.
<b>Gateway Detail (Only when Network Zone is “WAN”)</b>	<ul style="list-style-type: none"> <li>• <b>For “Static” IP assignment</b> - Specify the Gateway Name and IPv6 Address through which the traffic is to be routed.</li> <li>• <b>For “DHCP” IP assignment</b> - Specify the Gateway Name, if “Stateless” manual mode is selected. For “DHCP only” manual mode, specify Gateway name and IPv6 Address.</li> </ul>
<b>Advanced Settings</b>	
<b>DAD Attempts</b>	<p>Specify number of neighbour solicitation messages that are sent during Duplicate Address Detection (DAD) process.</p> <p>DAD is a process through which a node determines that the address it uses is not in use by another node.</p> <p>Acceptable Range - 0 to 8</p> <p>Default – 1</p>
<b>Allowed RA Servers</b>	Select Router Advertisement Servers. RA client interface will accept or process RA packets only from the specified RA Servers.

Table – Add VLAN Interface screen elements

If custom zone is created for Virtual sub-interface, two default firewall rules for the zone are automatically created depending on zone type of the custom zone. For example, if the zone type for the virtual sub-interface is LAN, 2 default firewall rules under Virtual sub-interface to WAN zone are automatically created based on the default LAN to WAN zone firewall rules.

## Link Aggregation Group

Link Aggregation Group (LAG) is a method by which multiple network connections can be combined into a single connection. It is also known as trunking, NIC teaming, NIC bonding and Ether Channel. LAG is mostly used for handling LAN traffic.

### LACP

Link Aggregation Control Protocol (LACP) is a part of IEEE specification that groups two or more physical links into a single logical link. LACP must be enabled at both ends of the link to be functional.

Appliance supports LAG to combine multiple physical links into a single logical link so that bandwidth can be increased and automatic failover is available.

LAG supports two modes:

- **Active- Backup** – Provides automatic link failover facility. In this a single slave (member of LAG) remains active. If the active slave fails then other slave in the LAG becomes the active slave
- **LACP (802.3ad)** – This mode provides load balancing and automatic failover. In this mode all the links are used for forwarding the traffic.

#### Note

- Both the switches must support LACP.
- The member interface in LAG must have same properties.

### Advantages

- Unbound physical interfaces are supported.
- Only static physical interfaces are supported.
- PPPoE, 3G, 4G, WWAN, WLAN and Transport mode are not supported in LAG.

## Add LAG Interface

LAG interface cannot be added from CLI. Only its properties can be configured or edited from CLI.

Screen – Add LAG Interface

### Parameters

Screen Element	Description
<b>Global Settings</b>	
<b>Interface Name</b>	Enter a name for LAG interface.
<b>Member Interface</b>	<p>“Port List” displays all the unbounded ports.</p> <p>Click the checkbox to select the port. All the selected ports are moved to “Selected Port” list.</p> <ul style="list-style-type: none"> <li>At least 2 member ports are required for creating a LAG interface.</li> </ul>

	<ul style="list-style-type: none"> <li>Maximum 4 ports can be configured on a single LAG interface.</li> </ul>
<b>Mode</b>	<p>Select mode of LAG.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li><b>Active-Backup</b> – Select Active-Backup mode to provide fault tolerance only.</li> <li><b>802.3ad (LACP)</b> – Select 802.3ad (LACP) mode to load balance the traffic and provide fault tolerance.</li> </ul>
<b>Network Zone</b>	<p>Select network zone for the interface.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>LAN</li> <li>DMZ</li> <li>WAN</li> </ul>
<b>IPv4 Configuration</b>	
<b>IP Assignment</b>	<p>Select the IP Assignment scheme for interface from the options available:</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>Static</li> <li>DHCP</li> </ul> <p>Default – Static</p>
<b>IPv4 Address</b>	Specify IPv4 Address.
<b>Netmask</b>	Select the network subnet mask for the interface.
Gateway Detail	
<b>Gateway Name (Only for WAN Zone)</b>	Provide Gateway Name.
<b>IPv4 Address (Only for WAN Zone)</b>	Provide Gateway IPv4 Address.
<b>IPv6 Configuration</b>	
<b>IPv6 / Prefix</b>	Specify IPv6 Address and the prefix.
Gateway Detail	
<b>Gateway Name (Only for WAN Zone)</b>	Provide Gateway Name.
<b>IPv6 Address (Only for WAN Zone)</b>	Provide Gateway IPv6 Address.
<b>Advanced Settings</b>	
<b>Interface Speed</b>	Select Interface speed for synchronization.

	<p>Speed mismatch between the Appliance and 3<sup>rd</sup> party routers and switches can result into errors or collisions on interface, no connections or traffic latency, slow performance.</p> <p><b>Depending on the model deployed following options will be available:</b></p> <ul style="list-style-type: none"> <li>• Auto Negotiate</li> <li>• 100 Mbps - Full duplex</li> <li>• 100 Mbps - Half duplex</li> <li>• 10 Mbps - Full duplex</li> <li>• 10 Mbps – Half Duplex</li> </ul> <p>Default - Auto Negotiate</p>
<b>MTU</b>	<p>Specify MTU value (Maximum Transmission Unit).</p> <p>MTU is the largest physical packet size, in bytes, that a network can transmit. This parameter becomes an issue when networks are interconnected and the networks have different MTU sizes. Any packets larger than the MTU value are divided (fragmented) into smaller packets before being sent.</p> <p>Default - 1500 Acceptable Range - 576 to 1500</p>
<b>Override MSS</b>	<p>Click to override default MSS.</p> <p>MSS defines the amount of data that can be transmitted in a single TCP packet.</p> <p>Default - 1460 Acceptable Range - 536 to 1460</p>
<b>Xmit Hash Policy(Available only if LACP (802.3ad) mode is selected)</b>	<p>Select the Xmit hash Policy to be used for member interfaces from the options available:</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Layer2</b> – Select to generate the hash value using hardware MAC Addresses.</li> <li>• <b>Layer2+3</b> – Select to generate the hash value using a combination of Layer 2 (MAC Address) and Layer 3 (IP Address) protocol information.</li> <li>• <b>Layer3+4</b> – Select to generate the hash value using Transport layer protocol information.</li> </ul>
<b>Primary Interface (Available only if</b>	<p>Select an interface to be a primary interface. This interface remains active while it is available.</p>

<b>Active-Backup mode is selected)</b>	The interfaces included in the member interface are available in this list.
<b>Use Default MAC Address</b>	Click to use the default MAC Address for the Interface.  By default, the first port that is included in the member port becomes the default MAC Address.
<b>Override Default MAC Address</b>	Click to override the default MAC Address for the Interface and enter the new MAC Address.  On factory reset, it will be set to the default MAC Address.

Table – Add LAG Interface screen elements

## IP Tunnel

An IP Tunnel is an Internet Protocol network communications path between two networks. It is used to encapsulate one network protocol as carrier for another network protocol. It is often used by two separate networks having a router with different network address for communication. The Appliance supports IPv6 Tunnelling. Hence, IPv6 packets can be encapsulated in IPv4 headers using IP Tunnel.

This page provides a list of all the configured IP tunnels and the administrator can manage IP tunnels from this page.

To manage zones, go to **Network > Interface > IP Tunnel**

<input type="button" value="Add"/> <input type="button" value="Delete"/>		Records Per Page 20 <input type="button" value="⏪"/> <input type="button" value="⏩"/> (1 of 1) <input type="button" value="⏴"/> <input type="button" value="⏵"/>					
<input type="checkbox"/>	Tunnel Name	Tunnel Type	Zone	Local End Point	Remote End Point	Other Configurations	Manage
<input type="checkbox"/>	Test	6in4	WAN	1.1.1.1	10.1.1.1	TTL = 10 TOS = 10	
<input type="button" value="Add"/> <input type="button" value="Delete"/>		Records Per Page 20 <input type="button" value="⏪"/> <input type="button" value="⏩"/> (1 of 1) <input type="button" value="⏴"/> <input type="button" value="⏵"/>					

Screen – Manage Zones

Screen Element	Description
<b>Tunnel Name</b>	Displays the name of the Tunnel.
<b>Tunnel Type</b>	Type of IP Tunnel selected – 6in4 or 6to4 or 6rd or 4in6.
<b>Zone</b>	Type of Zone selected – LAN or DMZ or WAN.
<b>Local End Point</b>	Displays the IP Address of the Local End Point of the Tunnel.
<b>Remote End Point</b>	Displays the IP Address of the Remote End Point of the Tunnel.
<b>Other configurations</b>	Displays Time to Live (TTL) and Type Of Service (TOS) configuration.

Table – Manage IP Tunnel screen elements



## Adding an IP Tunnel

**IP Tunnel Settings**

Tunnel Name\*

Tunnel Type\*  ▼

Zone\*  ▼

Local End Point\*  ⓘ

Remote End Point\*  ⓘ

▼ **Advanced Settings**

TTL  (0 - 255)

TOS  (0 - 99)

Screen – IP Tunnel

Screen Element	Description
<b>Tunnel Name</b>	Specify a unique name to identify the tunnel.
<b>Tunnel Type</b>	<p>Select the type of tunnel from the options available.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>6in4</b> – Select to allow communication between two IPv6 endpoints across IPv4 network.</li> <li>• <b>6to4</b> – Select to allow communication between two IPv6 endpoints across IPv4 network.</li> <li>• <b>6rd</b> – Select to allow communication between two IPv6 endpoints across IPv4 network.</li> <li>• <b>4in6</b> – Select to allow communication between two IPv4 endpoints across IPv6 network.</li> </ul>
<b>Zone</b>	<p>Select the zone to create the tunnel for, from the options available.</p> <p>The tunnel will cater to the traffic of selected zone.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>LAN</b></li> <li>• <b>DMZ</b></li> <li>• <b>WAN</b></li> </ul>
<b>Local End Point</b>	<p>Specify IP Address of the Local End Point of the tunnel.</p> <p>Specify IPv4 Address for 6to4, 6in4 and 6rd tunnels.</p> <p>Specify IPv6 Address for 4in6 tunnel.</p>

<b>Remote End Point</b>	Specify IP Address of the Remote End Point of the tunnel.  Specify IPv4 Address for 6in4 tunnel. Specify IPv6 Address for 4in6 tunnel.
<b>Advanced Settings</b>	
<b>TTL</b>	Specify the Time To Live (TTL) life time of data.  The attribute Time to live (TTL) defines a limit on number of attempts to transmit an IP packet before discarding it.  Default - 0 Acceptable Range - 0 to 255
<b>TOS</b>	Specify the Type Of Service (TOS) of data.  The attribute Type Of Service (TOS) provides the value for an IP packet depending on which the service is provided. The service mainly defines the packet priority, type of route (latency, throughput, or reliable service)  Default - 0 Acceptable Range - 0 to 99

Table – IP Tunnel screen elements

## Zone

A Zone is a logical grouping of ports/physical interfaces and/or virtual sub-interfaces if defined.

Zones provide a flexible layer of security for the firewall. With the zone-based security, the administrator can group similar ports and apply the same policies to them, instead of having to write the same policy for each interface.

### Default Zone Types

LAN – Depending on the Appliance in use and network design, one can group one to six physical ports in this zone. Group multiple interfaces with different network subnets to manage them as a single entity. Group all the LAN networks under this zone.

By default the traffic to and from this zone is blocked and hence the highest secured zone. However, traffic between ports belonging to the same zone will be allowed.

DMZ (DeMilitarized Zone) – This zone is normally used for publicly accessible servers. Depending on the Appliance in use and network design, one can group multiple physical ports in this zone.

WAN – This zone is used for Internet services. It can also be referred to as Internet zone.

VPN – This zone is used for simplifying secure, remote connectivity. It is the only zone that does not have an assigned physical port/interface. Whenever the VPN connection is established, port/interface used by the connection is automatically added to this zone and on disconnection; port is automatically removed from the zone. Like all other default zones, scanning and access policies can be applied on the traffic for this zone.

Local – Entire set of physical ports available on your Appliance including their configured aliases are grouped in LOCAL zone. In other words, IP Addresses assigned to all the ports fall under the LOCAL zone.

## Manage Zone list

To manage zones, go to **Network > Interface > Zone**.

Add		Delete		Records Per Page 20			<input type="button" value="&lt;&lt;"/> <input type="button" value="&lt;"/> (1 of 1) <input type="button" value="&gt;"/> <input type="button" value="&gt;&gt;"/>	
<input type="checkbox"/>	Name	Members	Type	Device Access	Description	Manage		
<input type="checkbox"/>	LAN	PortA	LAN	Windows/Linux Client , Web Proxy, SSL VPN, Ping/Ping6, HTTP, HTTPS, Telnet, SSH, DNS, Captive Portal, Radius SSO				
<input type="checkbox"/>	WAN	PortB	WAN	SSL VPN, HTTP, HTTPS				
<input type="checkbox"/>	DMZ	PortC	DMZ	SSL VPN, HTTP				
<input type="checkbox"/>	LOCAL		LOCAL					
<input type="checkbox"/>	VPN		VPN					

Records Per Page 20




 (1 of 1)

**Screen – Manage Zones**

Screen Element	Description
<b>Name</b>	Displays the name of the Zone.
<b>Members</b>	Displays the physical interface bounded to the zone.
<b>Type</b>	Displays the Type of Zone selected – LAN or DMZ.
<b>Device Access</b>	Displays the name of device access activated under a zone.
<b>Description</b>	Displays the Zone description.

**Table – Manage Zones screen elements**

## Zone Parameters

To add or edit zones, go to **Network > Interface > Zone**. Click Add Button to add a new zone. To update the details, click on the zone or Edit icon  in the Manage column against the zone you want to modify.

**Add Zone**

Name \*

Type \*  LAN  DMZ

Members None

Description

Appliance Access

Admin Services

HTTP  HTTPS  TELNET  SSH

Authentication Services

Windows/Linux Client  Captive Portal  NTLM  Radius SSO

Network Services

DNS  Ping/Ping6

Other Services

Web Proxy  SSL VPN

Screen – Add Zones

Screen Element	Description
<b>Name</b>	Specify a name to identify the zone
<b>Type</b>	<p>Select the type of Zone from the available options.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>LAN</b> – Depending on the Appliance in use and network design, one can group one to six physical ports in this zone. Group multiple interfaces with different network subnets to manage them as a single entity. Group all the LAN networks under this zone.</li> </ul> <p>By default the traffic to and from this zone is blocked and hence the highest secured zone. However, traffic between ports belonging to the same zone will be allowed.</p> <ul style="list-style-type: none"> <li>• <b>DMZ (DeMilitarized Zone)</b> - This zone is normally used for publicly accessible servers. Depending on the Appliance in use and network design, one can group one to five physical ports in this zone.</li> </ul> <p><b>Note</b></p>

	<ul style="list-style-type: none"> <li>By default, entire traffic will be blocked except LAN to Local zone service likes Administration, Authentication, and Network.</li> </ul>
<b>Member Ports</b>	<p>'Member Ports' List displays all the ports that have been assigned to the selected Zone</p> <p>Click the checkbox to select the ports. All the selected ports are moved to 'Selected port' list.</p>
<b>Description</b>	Provide the description for the zone.
<b>Appliance Access</b>	<p>Appliance access defines the type of administrative access permitted on zone.</p> <p><b>Admin Services</b> – Enable Administrative Services that should be allowed through Zone</p> <ul style="list-style-type: none"> <li><b>HTTP</b> – Allow HTTP connection to the Web Admin console through this zone</li> <li><b>HTTPS</b> – Allow secure HTTPS connection to the Web Admin console through this zone</li> <li><b>Telnet</b> – Allow Telnet connection to CLI through this zone</li> <li><b>SSH</b> – Allow SSH connection to CLI through this zone</li> </ul> <p><b>Authentication Services</b> – Enable Authentication Services that should be allowed through Zone</p> <ul style="list-style-type: none"> <li>Windows/Linux Clients</li> <li>Captive Portal</li> <li>NTLM</li> <li>Radius SSO</li> </ul> <p><b>Network Services</b> – Enable Network Services that should be allowed through Zone</p> <ul style="list-style-type: none"> <li>DNS – Allow this zone to respond to DNS requests</li> <li>PING – Allow this zone to respond to pings</li> </ul> <p><b>Other Services</b> – Enable other Services that should be allowed through Zone</p> <ul style="list-style-type: none"> <li>Web Proxy</li> <li>SSL VPN - SSL VPN service is not available for Cyberoam CR15i models.</li> </ul>

Table – Add Zones screen elements

**Note**

- If DMZ uses Private IP Address, use NATing to make them publicly accessible.
- One cannot add zone if the Appliance is deployed as Bridge.

- Local and VPN zone cannot be updated or deleted.

## Wireless WAN

**This feature is not supported in Cyberoam Virtual Security Appliances.**

Wireless WAN is wide area network (WAN) for data that is typically provided by the cellular carriers to transmit a wireless signal over a range of several miles to a mobile device. WWAN connectivity allows a user with a laptop and a WWAN support to use the web, or connect to a VPN from anywhere within the regional boundaries of the cellular service.

They are popularly known as "wireless broadband".

To configure WWAN:

4. Enable WWAN from CLI with command: `cyberoam wwan enable`
  5. Re-login to Web Admin console
  6. Configure WWAN Initialization string and gateway from **Network > Wireless WAN > Settings** page
- Once WWAN is enabled from CLI, an interface named WWAN1 is created and it is the member of the WAN zone.
  - As WWAN interface is a member of WAN zone:
    1. All the services enabled for the WAN zone from the Appliance Access page are automatically applicable on WWAN1 connection too.
    2. All the firewall rules applied on WAN zone will be applied on WWAN interface
  - A default host named ##WWAN1 is created and firewall rule and VPN policies can be created for the default host.
  - WWAN1 gateway is added as Backup gateway
  - When the Wireless WAN is disabled from CLI, Wireless WAN menu, default host ##WWAN1 and WWAN gateway options will be removed from Web Admin Console.

### Note

- Wireless WAN is not supported in Bridge Mode.
  - DHCP Server configuration is not supported for WWAN interface.
  - If backup of an Appliance is taken on, which WWAN is enabled and restored on an Appliance where it is not enabled, WWAN configuration would still be visible.
- 
- [Status](#)
  - [Settings](#)

## Status

The page displays the status of the Wireless WAN connection. Along with details of the WWAN connection, the page also provides the facility to connect and disconnect the WWAN connection.

### View Connection Status

To view and manage WWAN connection, go to **Network > Wireless WAN > Status**.

Status	
Status	Connected <input type="button" value="Disconnect"/>
Modem Name	HUAWEI Mobile E1731
IP Address	106.214.0.226
Gateway IP	106.214.0.225
Bytes Uploaded	4946 Bytes
Bytes Downloaded	4430 Bytes
Time Duration	00:18:36

**Screen – WWAN Status**

Screen Element	Description
<b>Connect/Disconnect Button</b>	Click the button to connect or disconnect the WWAN connection. This process may take some time.
<b>Status</b>	Status of the Connection. Status messages can be of following types.  Possible Status: <ul style="list-style-type: none"> <li>• Modem not supported</li> <li>• No Modem plugged-in</li> <li>• Connecting...</li> <li>• Reconnecting</li> <li>• Connected</li> <li>• Disconnected</li> </ul>
<b>Modem Name</b>	Name of the Modem.
<b>IP Address</b>	IP Address assigned to the device.
<b>Gateway IP</b>	IP Address assigned as the gateway.
<b>Bytes Uploaded</b>	Number of Bytes uploaded (in KB).
<b>Bytes Downloaded</b>	Number of Bytes downloaded (in KB).
<b>Time Duration</b>	Time period since WWAN is connected.  Format: HH:MM::SS

**Table – WWAN Status screen elements**



## Settings

The page allows configuration of Wireless WAN connection.

### Configure WWAN Connection

To configure WWAN connection, go to **Network > Wireless WAN > Settings**.

General Settings	
Interface Name	<input type="text" value="WWAN1"/>
IP Assignment*	<input type="radio"/> Dial-up (PPP) <input checked="" type="radio"/> Network Adapter (DHCP) <input type="button" value="Show Recommended Configuration"/>
Connect*	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
Reconnect Tries*	<input type="text" value="Always"/>
User Name	<input type="text"/>
Password	<input type="text" value="Password"/>
SIM Card PIN Code	<input type="text" value="SIM Card PIN Code"/>
APN	<input type="text" value="airtelgprs.com"/>
DHCP Connect Command	<input type="text"/>
DHCP Disconnect Command	<input type="text"/>
Initialization String	<input type="text" value="Initialization String"/> <input type="button" value="+"/> <input type="button" value="-"/>
Gateway Settings	
Gateway Name*	<input type="text" value="WWAN1_GW"/>
Gateway IP	<input type="text" value="106.214.0.225"/>
Gateway Type*	<input type="radio"/> Active <input checked="" type="radio"/> Backup
Activate this Gateway	If <input type="text" value="ANY"/> Gateway fails
Action on Activation	<input checked="" type="radio"/> Inherit weight of the failed active gateway <input type="radio"/> Use pre-configured weight * <input type="text"/>
Other Settings	
MTU *	<input type="text" value="1500"/>
MSS *	<input type="text" value="1460"/>
MAC Address	<input checked="" type="radio"/> Use Default MAC Address <input type="radio"/> Override Default MAC Address <input type="text"/>
<input type="button" value="Apply"/>	

Screen – WWAN Settings

Screen Element	Description
<b>General Settings</b>	
<b>Interface Name</b>	Specify a name of the interface
<b>IP Assignment</b>	Select the IP Assignment method from the available options:  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• Dialup (PPP)</li> <li>• Network Adapter (DHCP)</li> </ul>
	Click to view the modem details and the recommended configuration.

<b>Show Recommended Configuration Button</b>	<p>The Information section shows following details:</p> <ul style="list-style-type: none"> <li>• Modem Name</li> <li>• Vendor ID</li> <li>• Product ID</li> <li>• SIM PIN Enabled – Yes/No</li> </ul> <p>The Configuration section provides following information:</p>	
	Field Name	Possible Values
	<b>Available IP Assignment Methods</b>	Dialup (PPP) Network Adapter (DHCP) Dialup (PPP) & Network Adapter (DHCP)
	<b>Modem Port</b>	Not Available Serial n (n= 0, 1, ...9)
	<b>Secondary Modem Ports</b>	Not Available Serial n (n = 0, 1, ...9)  It displays next promising modem port. This port must be utilized as “Modem Port”, if the recommended modem port fails to function.
	<b>APN</b>	Not Available <name>
	<b>DHCP Connect Command</b>	Not Required Required but not available <AT command>
	<b>DHCP Disconnect Command</b>	Not Required Required but not available <AT command>
	<p>Click “Load Recommended Configuration” button to load recommended configuration in the “Settings” page and use the same.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Clicking “Load Recommended Configuration” button flushes out previous configuration if any exist and replace it with the recommended configurations.</li> <li>• Values of “Secondary Modem Ports” will not be loaded on “Settings” page on clicking “Load Recommended Configuration” button.</li> </ul> </div>	

<p><b>Connect</b></p>	<p>Types of Dialing of WWAN connection.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Auto Dial &amp; Active Gateway</b> – When auto-dial is configured and gateway is added as Active. Appliance automatically connects to the ISP and this gateway takes part in Load balancing as per the weight configurations.</li> <li>• <b>Manual Dial &amp; Active Gateway</b> – When manual dial is configured and gateway is added as Active, Appliance does not automatically connect to ISP. Administrator needs to initiate dial action.</li> <li>• <b>Auto Dial &amp; Backup Gateway</b> – When auto-dial is configured and gateway is added as backup, on the event of failover, Appliance auto-dials to the ISP and all the traffic passes through that Wireless WAN link.</li> <li>• <b>Manual Dial &amp; Backup Gateway</b> – When Manual Dial is configured and gateway is added as backup, on event of failover, Appliance does not automatically connect the ISP. The Admin needs to go to the Web Console and perform the "Connect" action. Only then, traffic passes through Wireless WAN interface.</li> </ul>
<p><b>Reconnect Tries</b></p>	<p>Select the number attempts allowed to reconnect from the available options.</p> <p><b>Available options:</b></p> <ul style="list-style-type: none"> <li>• Always</li> <li>• 1</li> <li>• 2</li> <li>• 3</li> </ul> <p>Default – Always</p> <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• In case of DHCP, 'Always' is the only available option.</li> </ul> </div>
<p><b>Modem Port (Only for Dialup (PPP))</b></p>	<p>Serial interface on which modem will establish connection</p> <p>Available Options:</p> <ul style="list-style-type: none"> <li>• Serial 0 to 9</li> </ul> <p>In case incorrect serial interface is configured, one needs plug-out the modem or reboot the Appliance.</p>
<p><b>Phone Number (Only for Dialup (PPP))</b></p>	<p>Specify Phone number for connection.</p>
<p><b>User Name</b></p>	<p>Specify a Username for the connection.</p>
<p><b>Password</b></p>	<p>Specify a Password.</p>

<b>SIM Card PIN Code</b>	<p>PIN code to unlock PIN-enabled SIM card.</p> <p>Many operators lock their SIM card to prevent the use of other operator's SIM cards. These kinds of modems can be unlocked with the PIN code for connecting.</p>
<b>APN</b>	<p>Specify Access Point Name.</p> <p>Access Point Name (APN) is a configurable network identifier, used by the Appliance to identify the packet data network (PDN) / GSM carrier with which the user wants to communicate.</p>
<b>DHCP Connect Command (Only for Network Adapter (DHCP))</b>	Specify a DHCP command to connect to the Wireless WAN.
<b>DHCP Disconnect Command (Only for Network Adapter (DHCP))</b>	Specify a DHCP command to disconnect from the Wireless WAN.
<b>Initialization String</b>	Specify initialization string for the specific wireless modem. There can be more than one string and in such case, strings should be entered in proper order.
<b>Gateway Settings</b>	
<b>Gateway Name</b>	Specify a name to identify the Gateway.
<b>Gateway IP Address</b>	Specify IP Address of the Gateway.
<b>Gateway Type</b>	Specify Type of Gateway: Active or Backup.
<b>Weight</b>	<p>Depending on the weight, gateway for load balancing is selected. Appliance distributes traffic across links in proportion to the ratio of weights assigned to individual link.</p> <p>This weight determines how much traffic will pass through a particular link relative to the other link.</p> <p>When more than two gateways are configured and one gateway goes down, the traffic is switched over to the available gateways according to the ratio of the weights assigned to the available gateways.</p>
<b>Activate This Gateway (Only if option "Backup" Gateway Type is selected)</b>	<p>Select Gateway Activation Condition</p> <p>Dropdown will list all the configured gateways. Backup gateway will take over and traffic will be routed through the backup gateway only when the selected gateway fails.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>If &lt;Gateway Name&gt; Gateway Fails</b> – Backup gateway will take over and traffic will be routed through the backup gateway only when the &lt;Gateway Name&gt; gateway fails.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>If Any Gateway Fails</b> – Backup gateway will take over and traffic will be routed through backup gateway when any of the active gateways fail.</li> <li>• <b>If ALL the Gateways Fail</b> – Backup gateway will take over and traffic will be routed through backup gateway when all the configured active gateways fail.</li> </ul>
<b>Action on Activation (Only if option “Backup” Gateway Type is selected)</b>	<p>Configure weight for the backup gateway. Appliance distributes traffic across links in proportion to the ratio of weights assigned to individual link. This weight determines how much traffic will pass through a particular link relative to the other link.</p> <p>Select “Inherit weight of the failed active gateway” if you want Backup gateway to inherit the parent gateway’s (Active gateway) weight or select “User pre-configured weight” and specify weight.</p>
<b>Other Settings</b>	
<b>MTU</b>	<p>Specify MTU value (Maximum Transmission Unit)</p> <p>MTU is the largest physical packet size, in bytes, that a network can transmit. This parameter becomes an issue when networks are interconnected and the networks have different MTU sizes. Any packets larger than the MTU value are divided (fragmented) into smaller packets before being sent.</p> <p>Default – 1500. Acceptable Range – 576 to 1500</p>
<b>MSS</b>	<p>MSS defines the amount of data that can be transmitted in a single TCP packet.</p> <p>Default – 1460 MSS Input range – 536 to 1460</p>
<b>MAC Address (Only for Network Adapter (DHCP))</b>	<p>Select a method from the available options to provide MAC Address for the Modem:</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• Use Default MAC Address</li> <li>• Override Default MAC Address – On selection of this option, provide the MAC Address.</li> </ul>

Table – WWAN Settings screen elements

## Gateway

A Gateway is used to route traffic between networks. In case of failure of the gateway, the entire network traffic is dropped and communication with the outside network(s) is not possible.

By default, Appliance supports only one gateway. However, to cope with gateway failure problems, the Appliance provides an option to configure multiple gateways. But simply adding one more gateway is not an end to the problem. Optimal utilization of all the gateways is also necessary. The Appliance Multi Link Manger provides link failure protection by detecting the dead gateway and switching over to the active link and also provides a mechanism to balance traffic between various links.

At the time of deployment, you configured the IP Address for a default gateway through Network Configuration Wizard. You can change this configuration any time and configure additional gateways. You can use Multi Link Manger to configure multiple gateways for load balancing and failover.

By default, all the gateways defined through Network Configuration Wizard will be defined as “Active” gateway.

### Gateway Name

Name of the Gateway assigned at the time of installation.

### Gateway IP Address

IP Address of the Gateway assigned at the time of installation.

### Ethernet Port

Gateway/WAN port

### Gateway Type

Active – By default, traffic is routed through Active gateway.

Backup – Routes the traffic only when active gateway fails.

### Weight

Weight assigned to the Gateway and used for load balancing. Weight determines how much traffic will pass through a particular link relative to the other link. Administrators can set weight and define how the traffic should be directed to providers to best utilize their bandwidth investments.

## Gateway

The Appliance provides a powerful solution for routing and managing traffic across multiple Internet connections. Designed to provide business continuity to an organization of any size, Multilink Manager optimizes the use of multiple Internet links, such as T1s, T3s, DSL and cable connections from one or multiple Internet service providers. Capable of automatic failover in the event of link failure, it helps to assure that your network is always connected to the Internet.

It also gives you an option to configure multiple WAN interfaces to allow connecting your Appliance to more than one Internet Service Provider (ISP).

When you configure multiple external interfaces, you have even have an option to control which interface an outgoing packet uses.

## Load Balancing

Load balancing is a mechanism that enables balancing traffic between various links. It distributes traffic among various links, optimizing utilization of all the links to accelerate performance and cut operating costs. The Appliance employs weighted round robin algorithm for load balancing to enable maximum utilization of capacities across the various links.

Using link load balancing provides organizations a way to achieve:

- Traffic distribution that does not overburden any link
- Automatic ISP failover
- Improved User performance because of no downtime
- Increased bandwidth scalability

To achieve outbound traffic load balancing between multiple links:

- configure links in active-active setup i.e. define gateways as Active
- Assign appropriate weight to each gateway. Traffic is distributed across the links in proportion to the ratio of weights assigned to individual link.

## How it works

Load balancing is determined by the load metric also known as weight. Each link is assigned a relative weight and the Appliance distributes traffic across links in proportion to the ratio of weights assigned to individual link. This weight determines how much traffic will pass through a particular link relative to the other link.

Administrator can set weight and define how the traffic should be directed to providers to best utilize their bandwidth investments. Weight can be selected based on:

- Link capacity (for links with different bandwidth)
- Link/Bandwidth cost (for links with varying cost)

Weighted load balancing feature enables Network Managers to optimize network traffic and balance the load between multiple links/interfaces.

## Gateway failover



Gateway failover provides link failure protection so that when one link goes down; the traffic is switched over to the active link. This safeguard helps provide uninterrupted, continuous Internet connectivity to users. The transition is seamless and transparent to the end user with no disruption in service without any downtime.

To achieve WAN failover between multiple links:

- Configure links in Active-Backup setup
- define Active gateway/interface
- define Backup gateway/interface – traffic through this link is routed only when active interface is down
- define failover rule

In the event of Internet link failure, the Multilink Manager automatically sends traffic to available Internet connections without administrator intervention. If more than one link is configured as backup link, traffic is distributed among the links in the ratio of the weights assigned to them. On fail over, Backup Gateway can inherit the parent gateway's (Active Gateway) weight or can be configured.



### Gateway Failback










During a link failure, the Appliance regularly checks the health of a given connection, assuring fast reconnection when Internet service is restored. When the connection is restored and gateway is up again, without the Administrator's intervention, traffic is again routed through the Active gateway. In other words, backup gateway fails back on Active gateway. The page also displays status as Active  or Deactive  of the each gateway and failover rule in case multiple gateways are configured. You can change the gateway parameters, change gateway status, add or remove the failover rule, and view the data transfer done through the gateway.

For Backup gateway, weight is NA while for Active gateway, the configured weight is displayed.




### Manage Gateway list

To manage gateways, go to **Network > Gateway**.

- [Failover Rules](#) – Click the Edit icon  in the Manage column against the Gateway. Edit Gateway page is displayed through which you can configure Failover rules.
- [View Data Transfer](#) – Click the graph icon  in the Manage column against the Gateway to view data transfer.

IPv4 Gateway								
Name	IP Address	Interface	Type	Activate on Failure of	Weight	NAT Policy	Status	Manage
GW_10.202.6...	10.202.63.254	PortC - 10.202.22.10/255.255.192.0	Active	N/A	1	MASQ		 
PPPoE Test	128.0.0.1		Active	N/A	1	MASQ		 
Test	128.0.0.1		Active	N/A	1	MASQ		 









IPv6 Gateway								
Name	IP Address	Interface	Type	Activate on Failure of	Weight	NAT Policy	Status	Manage
PPPoE Test2	22::24	PortB - 22::22/64	Active	N/A	1	MASQ		 

Gateway Failover Timeout Configuration	
Gateway Failover Timeout	<input type="text" value="60"/> seconds (1-3600)
<input type="button" value="Apply"/>	

Screen – Manage Gateway



Screen Element	Description
<b>IPv4 Gateway</b>	
<b>Name</b>	Name of the Gateway.
<b>IP Address</b>	IPv4 Address of Gateway.
<b>Interface</b>	IPv4 Address and Netmask of the Interface.
<b>Type</b>	Type of Gateway – Active or Backup
<b>Activate on Failure of</b>	Activation condition, if Gateway is configured as Backup Gateway.
<b>Weight</b>	Weight assigned to the Gateway.  For Active gateway, weight which is configured will be displayed.  For Backup gateway, zero will be displayed when inactive
<b>Status</b>	Status of Gateway – Active  or Deactive 
<b>NAT Policy</b>	NAT policy assigned to the Gateway.
<b>Edit Icon</b>	Click  to Edit the Gateway
<b>Data Transfer</b>	Click  to view graph of data transfer.
<b>IPv6 Gateway</b>	
<b>Name</b>	Name of the Gateway.
<b>IP Address</b>	IPv6 Address of Gateway.
<b>Interface</b>	IPv6 Address and Prefix of the Interface.
<b>Type</b>	Type of Gateway – Active or Backup
<b>Activate on Failure of</b>	Activation condition, if Gateway is configured as Backup Gateway.
<b>Weight</b>	Weight assigned to the Gateway.  For Active gateway, weight which is configured will be displayed.  For Backup gateway, zero will be displayed when inactive
<b>NAT Policy</b>	NAT policy assigned to the Gateway.
<b>Status</b>	Status of Gateway – Active  or Deactive 
<b>Edit Icon</b>	Click  to Edit the Gateway
<b>Data Transfer</b>	Click  to view graph of data transfer.
<b>Gateway Failover Timeout Configuration</b>	
<b>Gateway Failover Timeout</b>	Configure the Gateway Failover timeout in seconds.

	<p>This is the time period for which Appliance waits before the Gateway Failover occurs.</p> <p>Default – 60 seconds</p> <p>Gateway Failover Timeout Input Range: 1 - 3600 seconds.</p>
--	---

Table – Manage Gateway screen elements

## Updating Gateway Configurations

To edit gateway details, go to **Network > Gateway > Gateway**. Click Edit Icon  against the gateway to modify the details of the gateway.

**Gateway Detail**


Name\*

IP Address\*

Interface\*

Type\*  Active  Backup

Weight\*

Default NAT Policy\*  

Screen – Edit Gateway (Active Gateway)

**Gateway Detail**


Name\*

IP Address\*

Interface\*

Type\*  Active  Backup

Weight\*

Default NAT Policy\*  

**Backup Gateway Details**

Activate this Gateway\*  If   Active gateway fails

Manually

Action on Activation\*  Inherit weight of the failed active gateway

Use pre-configured weight

Screen – Edit Gateway (Backup Gateway)

Screen Element	Description
Gateway Detail	
<b>Name</b>	Specify a name to identify the Gateway.
<b>IP Address</b>	Specify IP Address assigned to the Gateway.
<b>Interface</b>	Displays the IP Address and Netmask of the Interface.
<b>Type</b>	<p>Specify Gateway Type.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Active</b> – Default gateway(s). Traffic will route through active gateway(s). If there exists more than one active gateway then the traffic will be load balanced between these gateways depending upon their weight.</li> <li>• <b>Backup</b> – A gateway that can be used in an active/passive setup, where traffic is routed through Backup gateway only when Active gateway is down.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• This option is only available when two or more Gateways are configured.</li> </ul> </div>
<b>Weight</b>	<p>Depending on the weight, gateway is selected for the load balancing. Appliance distributes traffic across links in proportion to the ratio of weights assigned to individual link.</p> <p>This weight determines how much traffic will pass through a particular link relative to the other link.</p> <p>Gateways can be assigned weights from 1 to 100.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• When more than two gateways are configured and one gateway goes down, the traffic is switched over to the available gateways according to the ratio of the weights assigned to the available gateways.</li> </ul> </div>
<b>Backup Gateway (Only when Type is Backup)</b>	
<b>Activate This Gateway</b>	<p>Select Gateway Activation Condition: Automatically or Manually</p> <p><b>Automatic failover</b></p> <p>From the dropdown list specify when the backup gateway should take over from active Gateway. This takeover process will not require administrator's intervention.</p>

	<p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Specific Gateway</b> – Dropdown will list all the configured gateways. Backup gateway will take over and traffic will be routed through the backup gateway only when the selected gateway fails.</li> <li>• <b>ANY</b> – Backup gateway will take over and traffic will be routed through backup gateway when any of the active gateway fails</li> <li>• <b>ALL</b> – Backup gateway will take over and traffic will be routed through backup gateway when all the configured active gateways fail</li> </ul> <p><b>Manual failover</b> If you select “Manually”, Administrator will have to manually change the gateway if the active gateway fails.</p>
<b>Action on Activation</b>	<p>Configure weight for the backup gateway. Appliance distributes traffic across links in proportion to the ratio of weights assigned to individual link. This weight determines how much traffic will pass through a particular link relative to the other link.</p> <p>Inherit weight of the failed active gateway - backup gateway to inherit the parent gateway's (Active gateway) weight</p> <p>User pre-configured weight - Specify weight for the backup gateway.</p>

Table – Edit Gateway screen elements

## Configure Gateway Failover Rules

The transition from dead link to active link is based on the failover rule defined for the link. Failover rule specifies:

- how to check whether the link is active or dead
- what action to take when link is not active

Failover rule has the form:

IF

Condition 1

AND/OR

Condition 2

then

Action

Depending on the outcome of the condition, traffic is shifted to any other available/backup gateway.

Ping rule gets automatically created for every gateway. The Appliance periodically sends the ping request to check the health of the link and if it does not respond within the specified time, traffic is automatically sent through another available link. Selection of the gateway and how much traffic is to be routed through each gateway depends on number of configured active and backup gateways.

To configure Failover Rules, go to **Network > Gateway > Gateway**. Click the Edit Icon  in the Manage column against the Gateway.



Screen - Configure Gateway Failover




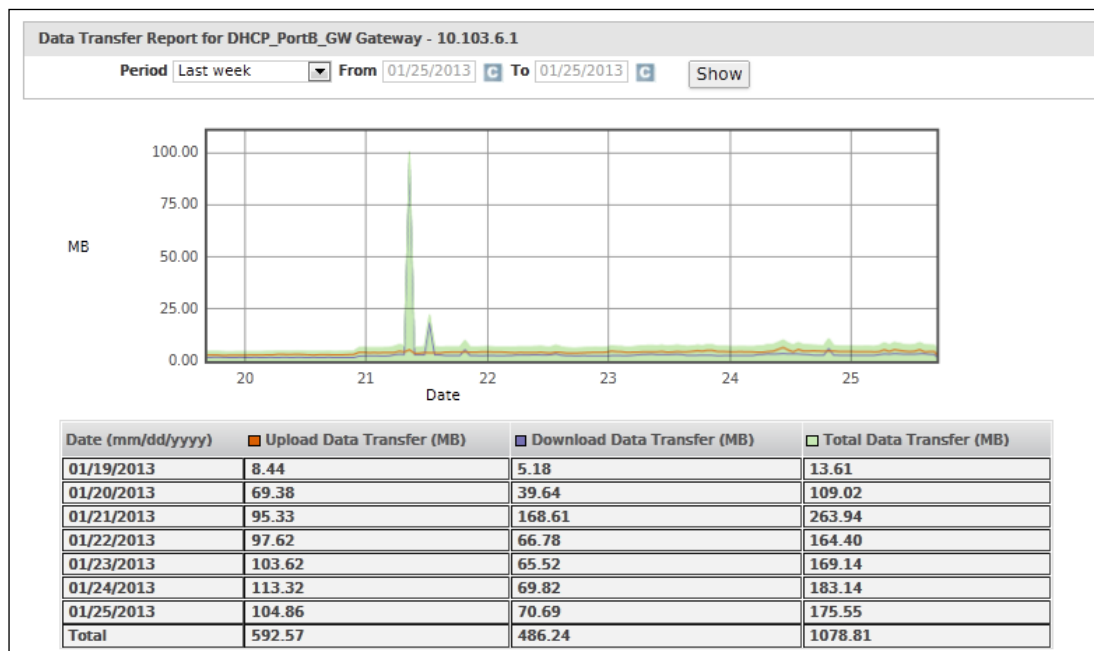
Screen – Add Gateway Failover Rule

Screen Element	Description
<b>IF Then Condition</b>	<p>Specify communication Protocol as TCP or PING (ICMP). Select the protocol depending on the service to be tested on the host.</p> <p>Specify port number for communication in case of TCP communication.</p> <p><b>IP Address</b> IP Address must be represented by the computer or Network device which is permanently running or most reliable.</p> <p>Condition AND - all the conditions must be satisfied OR - at least one condition must be satisfied</p> <p>A request is sent to an IP Address. If IP Address does not respond to the request, Appliance considers the IP Address as unreachable.</p>

**Table – Configure Gateway Failover screen elements**

## Viewing Data Transfer Activity through a Gateway

To configure failover rules, go to **Network > Gateway > Gateway**. Click the Data Transfer icon  in the Manage column against the Gateway to view the total data transferred through the gateway in the graphical as well as tabular format.



Screen – View Data Transfer

Screen Element	Description
<b>Data Transfer Report for Default Gateway -</b>	
<b>Period</b>	<p>Select the period from the available options for the Report of Data Transfer through the Gateway.</p> <p>Available Options:</p> <ul style="list-style-type: none"> <li>• Last Week</li> <li>• Last Month</li> <li>• Custom</li> </ul> <p>Graph displays the upload, download and total data transfer through Gateway.</p> <p>X-axis – Date (depending on the period selected)</p> <p>Y-axis – KB /MB/GB used.</p> <p>Legends</p> <p>Orange Color – Upload Data Transfer (MB)</p> <p>Purple – Download Data Transfer (MB)</p>

	<p>Green Color – Total Data Transfer (MB)</p> <div data-bbox="699 271 1390 427"><p><b>Note</b></p><ul style="list-style-type: none"><li>• When the selected period is “Custom”, then the user can select to view data of maximum last six (06) months. At a time, maximum of thirty (30) days data will be displayed.</li></ul></div>
--	---

**Table – View Data Transfer screen elements**



## Static Route

A route provides the Appliance with the information it needs to forward a packet to a particular destination. A static route causes packets to be forwarded to a destination other than the configured default gateway.



By specifying through which interface the packet will leave and to which device the packet should be routed, static routes control the traffic exiting the Appliance.

- [Unicast](#)
- [Multicast](#)
- [Source Route](#)



### Unicast

The Unicast page displays list of all the configured IPv4 and IPv6 unicast routes. You can filter the list based on IP address, gateway, interface, or distance. The page also provides option to update the route configuration, and delete the route.

To manage unicast routes, go to **Network > Static Route > Unicast**.

IPv4 Unicast Route						
<input type="checkbox"/>	<b>IP/Netmask</b>	<b>Gateway</b>	<b>Interface</b>	<b>Distance</b>	<b>Manage</b>	
<input type="checkbox"/>	192.168.101.0 / 255.255.255.0		PortB	0	 	


IPv6 Unicast Route						
<input type="checkbox"/>	<b>IP/Netmask</b>	<b>Gateway</b>	<b>Interface</b>	<b>Distance</b>	<b>Manage</b>	
<input type="checkbox"/>	32::32 / 64		PortB	1	 	

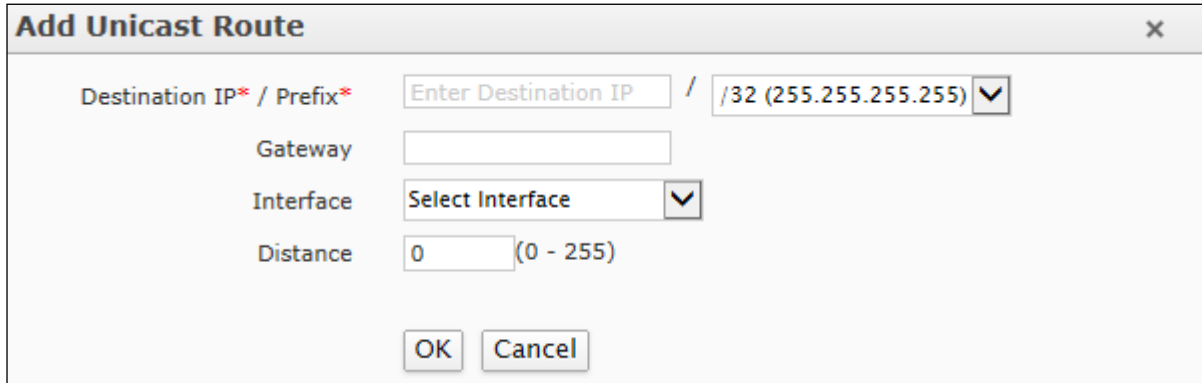
Screen – Manage Unicast Route

Screen Element	Description
<b>Unicast Route (IPv4/IPv6)</b>	
<b>IP/Netmask/Prefix</b>	Destination Network IP Address (IPv4/IPv6) and the Subnet Mask/Prefix.
<b>Gateway</b>	Destination Gateway IP Address.
<b>Interface</b>	Interface selected.
<b>Distance</b>	Distance between the source and the destination.

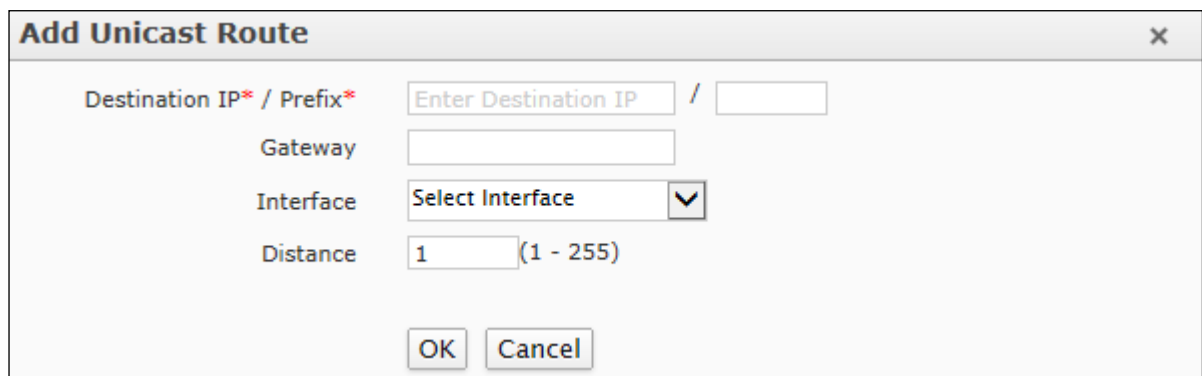
Table – Manage Unicast Route screen elements

## Unicast Route Parameters

To add or edit a unicast route, go to **Network > Static Route > Unicast**. Click the Add button to add a new unicast route. To update the details, click on the unicast route or Edit icon  in the Manage column against the unicast route you want to modify.



Screen – Add IPv4 Unicast Route



Screen – Add IPv6 Unicast Route

Screen Element	Description
<b>Destination IP</b>	Specify Destination IP Address.
<b>Netmask (IPv4)</b>	Specify Subnet Mask.
<b>Prefix (IPv6)</b>	Specify Prefix.
<b>Gateway</b>	Specify Gateway IP Address.
<b>Interface</b>	Select Interface from the list including Physical Interfaces, Virtual Sub-interfaces and Aliases.
<b>Distance</b>	Specify Distance for routing. Range of value is from 0 to 255.

Table – Add Unicast Route screen elements

## Multicast

Configure and manage multicast routes from this page.

### IP Multicast

Internet Protocol (IP) multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of recipients and homes. IP Multicast delivers source traffic to multiple receivers without adding any additional burden on the source or the receivers.

Applications like videoconferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news use IP multicasting.

If IP multicast is not used, the source is required to send more than one copy of a packet or individual copy to each receiver. In such case, high-bandwidth applications like Video or Stock, in which data is to be sent more frequently and simultaneously, use a large portion of the available bandwidth. In these applications, the only efficient way of sending information to more than one receiver simultaneously is by using IP Multicast.

### Multicast Group

Multicast is based on the concept of a group. An arbitrary group of receivers expresses an interest in receiving a particular data stream. This group does not have any physical or geographical boundaries—the hosts can be located anywhere on the Internet. Hosts that are interested in receiving data flowing to a particular group must join the group. Hosts must be a member of the group to receive the data stream.

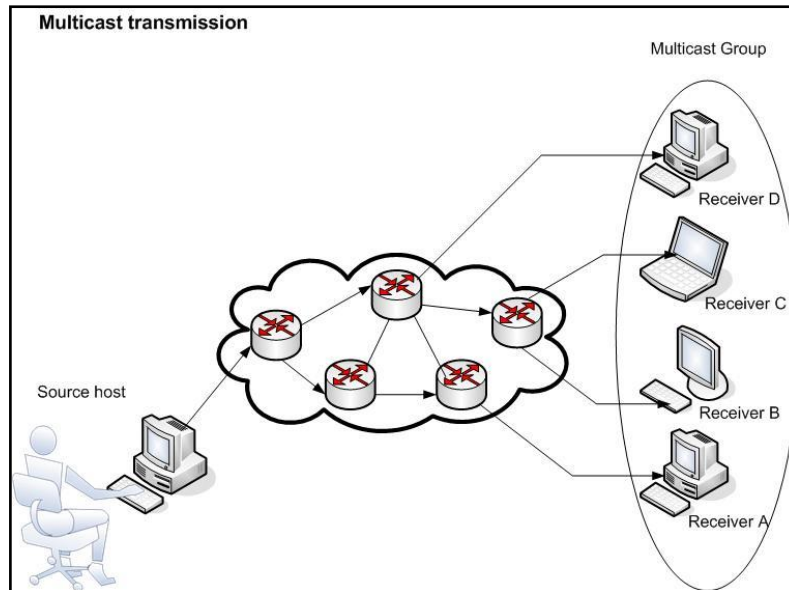
### IP Multicast Addresses

Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive traffic sent to this group.

### IP Class D Addresses

The Internet Assigned Numbers Authority (IANA) controls the assignment of IP multicast addresses. Multicast addresses fall in Class D address space ranging from 224.0.0.0 to 239.255.255.255.

This address range is only for the group address or destination address of IP multicast traffic. The source address for multicast datagram's is always the unicast source address.



### Multicast forwarding

With multicast forwarding, a router forwards multicast traffic to networks where other multicast devices are listening. Multicast forwarding prevents the forwarding of multicast traffic to networks where there are no nodes listening.

For multicast forwarding to work across inter-networks, nodes and routers must be multicast-capable.

A multicast-capable node must be able to:

- Send and receive multicast packets.
- Register the multicast addresses being listened to by the node with local routers, so that multicast packets can be forwarded to the network of the node.

IP multicasting applications that send multicast traffic must construct IP packets with the appropriate IP multicast address as the destination IP Address. IP multicasting applications that receive multicast traffic must inform the TCP/IP protocol that they are listening for all traffic to a specified IP multicast address.

### Manage Multicast Route list

To manage multicast routes, go to **Network > Static Route > Multicast**.

**Multicast Forwarding Setting**

Enable Multicast Forwarding Apply

**Manage Multicast Route**

Add Delete

Source IP	Multicast IP	Source Interface	Destination Interface	Manage
<input type="checkbox"/> 10.10.1.1	230.1.0.1	PortC	IPSec Connection	


Add Delete

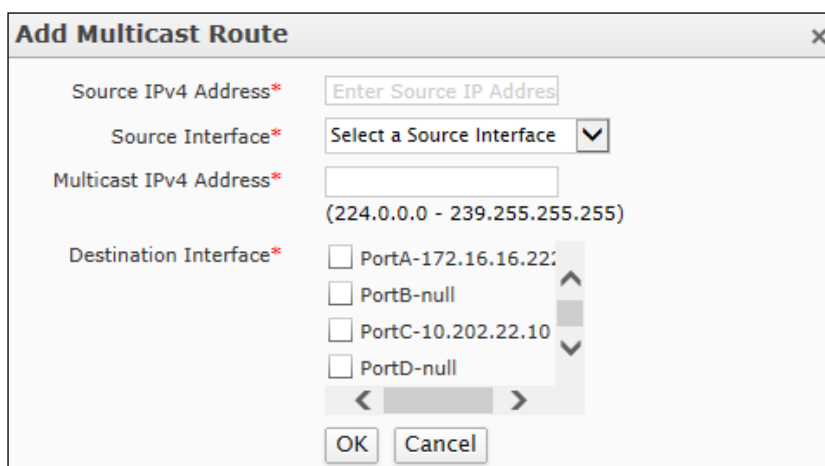
Screen – Manage Multicast Route

Screen Element	Description
<b>Multicast Forwarding Setting</b>	
<b>Enable Multicast Forwarding</b>	Click to enable multicast forwarding.  By default, Multicast Forwarding is disabled.
<b>Manage Multicast Route</b>	
<b>Source IP</b>	Source IP Address.
<b>Multicast IP</b>	Range of IP Address selected for Multicast route.
<b>Source Interface</b>	Source Interface selected.
<b>Destination Interface</b>	Destination Interface selected.

Table – Manage Multicast Route screen elements

### Multicast Route Parameters

To add or edit a multicast route, go to **Network > Static Route > Multicast**. Click the Add button to add a new multicast route. To update the details, click on the multicast route or Edit icon  in the Manage column against the multicast route you want to modify.



Screen – Add Multicast Route

Screen Element	Description
<b>Source IPv4 Address</b>	Specify Source IPv4 Address.
<b>Source Interface</b>	Select Source Interface from the list.
<b>Multicast IPv4 Address</b>	Specify range of Multicast IPv4 Address. For example, (224.0.2.0 - 239.255.255.255)
<b>Destination Interface</b>	Select Destination Interface from the list. You can select more than one destination interface.  Click the checkbox against the interface.

Table – Add Multicast Route screen elements

## Source Route

A route provides the Appliance with the information it needs to forward a packet to a particular destination. Source Routing is the technique by which the sender can explicitly mention the route through which the packet travels.

The page displays list of all the IPv4 and IPv6 source routes. The page provides an option to add, update and delete the existing routes.

To manage source routes, go to **Network > Static Route > Source Route**.


The screenshot displays two panels for managing source routes. The top panel is for IPv4 Source Route, and the bottom panel is for IPv6 Source Route. Each panel includes 'Add' and 'Delete' buttons and a table with columns for 'Network', 'Gateway', and 'Manage'. Both tables currently show 'No Records Found.'

Screen – Manage Source Routes

Screen Element	Description
Network	Network IP Address and the Subnet mask.
Gateway	Gateway IP Address.

Table – Manage Source Routes screen elements

## Parameters

To add or edit an explicit source route for packets, go to **Network > Static Route > Source Route**. Click the Add button to add a new source route. To update the details, click on the source route or Edit icon  in the Manage column against the source route you want to modify.

The screenshot shows a dialog box titled 'Add Explicit Source Route'. It contains two main input fields: 'Gateway\*' with a dropdown menu showing 'PortB\_GW', and 'Network Id\* / Prefix\*' with a text input field and a dropdown menu showing '/32 (255.255.255.255)'. There are 'OK' and 'Cancel' buttons at the bottom.

Screen – Add Source Route

---

Screen Element	Description
<b>Gateway</b>	Select the Gateway from the list.
<b>Network ID/Prefix</b>	Specify Network ID/Prefix (In case of IPv6 Addresses)
<b>Netmask</b>	Specify Subnet Mask.

**Table – Add Source Route screen elements**

## Dynamic Route

A route provides the Appliance with the information it needs to forward a packet to a particular destination. A dynamic route causes the Appliance to get the packet information at run time using dynamic routing protocols like RIP, OSPF, and BGP.

- [RIP](#)
- [OSPF](#)
- [BGP](#)
- [PIM-SM](#)
- [Routing Information](#)



## RIP

To configure RIP routes, go to **Network > Dynamic Route > RIP**.

Routing Information Protocol (RIP) is a widely used routing protocol that uses hop count to determine the best route to a destination.

RIP avoids routing loops from continuing indefinitely by limiting the number of hops permitted between the source and destination. The maximum number of hops supported is 15. Hence, if the hop count becomes 16, it is known as an infinite distance and is considered as unreachable.

With the help of RIP protocol, the Appliance sends the routing update messages at regular intervals to the next router. When the next router receives the changes, it updates them in the routing table and also increases the metric value for the path by 1. The sender of the message is considered as the next hop. The Appliance maintains only the route with the least metric value to a destination.

**Global Configuration**

Default Metric  (1 - 16)

Administrative Distance  (1 - 255)

RIP Version  Send V2 & Recieve both  V1  V2

**Timers**

Update  (5 - 2147483647)

Timeout  (5 - 2147483647)

Garbage  (5 - 2147483647)

Default Information Originate  on

Redistribute Connected  Enable Metric  (0 - 16)

Redistribute Static  Enable Metric  (0 - 16)

Redistribute OSPF  Enable Metric  (0 - 16)

Redistribute BGP  Enable Metric  (0 - 16)

**Networks**

Network	Netmask	Manage
10.10.10.1	255.255.255.255	

**Override Interface Configuration**

Interface	Manage
PortB	

Screen – Dynamic Route RIP

Screen Element	Description
<b>Global Configuration</b>	
<b>Default Metric</b>	<p>Specify the default metric value to be used for redistributed routes.</p> <p>Metric is a property that contains a value used by a routing protocol to decide a particular route to be taken.</p> <p>Default - 1 Acceptable Range - 1 - 16</p>
<b>Administrative Distance</b>	<p>Specify the administrative distance.</p> <p>Default - 120 Acceptable Range - 1 – 255</p>
<b>RIP Version</b>	<p>Select the RIP version to be used for sending and receiving the updates.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Send V2 &amp; Receive both</b></li> <li>• <b>V1</b></li> <li>• <b>V2</b></li> </ul>
<b>Timers</b>	
<b>Update</b>	<p>Specify the time interval in seconds between two periodic routing updates.</p> <p>Default - 30 seconds Acceptable Range (seconds) - 5 to 2147483647</p>
<b>Timeout</b>	<p>Specify the timeout time in seconds after which the route becomes invalid.</p> <p>Default - 180 seconds Acceptable Range (seconds) - 5 to 2147483647</p>
<b>Garbage</b>	<p>Specify the garbage time.</p> <p>Default - 120 seconds Acceptable Range (seconds) - 5 to 2147483647</p>
<b>Default Information Originate</b>	<p>Enable to control the distribution of default route.</p> <p>Default - Disabled</p>
<b>Redistribute Connected</b>	<p>Click to enable the redistribution of connected routes into RIP routing table.</p>

	Specify metric for redistributed connected routes.  Acceptable Range - 0 to 16
<b>Redistribute Static</b>	Click to enable the redistribution of static routes into RIP routing table.  Specify metric for redistributed static routes.  Acceptable Range - 0 to 16
<b>Redistribute OSPF</b>	Click to enable the redistribution of OSPF routes into RIP routing table.  Specify metric for redistributed OSPF routes.  Acceptable Range - 0 to 16
<b>Redistribute BGP</b>	Click to enable the redistribution of BGP routes into RIP routing table.  Specify metric for redistributed BGP routes.  Acceptable Range - 0 to 16
Network	
<b>Add</b>	Click to add an RIP network.
<b>Network</b>	Displays the IP Address of the Network.
<b>Netmask</b>	Displays the netmask of the Network.
<b>Edit</b>	Edit the Network.
<b>Delete</b>	Delete the Network
Override Interface Configuration	
<b>Select Interface</b>	Click to select an Interface.
<b>Interface</b>	Displays the configured interface.

Table – Dynamic Route RIP screen elements

### Adding RIP Networks

Click Add button under Networks to specify IPv4 Address network and subnet mask. You can also add, update, or delete the networks from this page.

Screen – Add RIP Network

## Overriding Global Interface Configuration

Click Select Interface button under Override Interface Configuration to override the Interface configuration. You can also add, update, or delete the Interface-specific configuration from this page.

Screen – Override Interface Configuration

Screen Element	Description
<b>Interface</b>	Select the interface for which you want to override the default configuration.
<b>RIP Version</b>	
<b>Send</b>	Select the RIP version to be used for sending the routing updates.  The RIP version can be V1 or v2 or v1 and v2 both. This overrides the version selected in the Global Configuration settings.  Default - V2
<b>Receive</b>	Select the RIP version to be used for receiving the routing updates.  The RIP version can be V1 or V2 or V1 and V2 both. This overrides the version selected in the Global Configuration settings.  By default, it receives both V1 and V2
<b>Split Horizon</b>	Enable to prevent the routing loops.

	Default - Disable
<b>Poisoned Reverse</b>	<p>Enable to prevent the Appliance from sending packets through the route that has become invalid.</p> <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• This option is available only after enabling “Split Horizon”.</li> </ul> </div> <p>Default – Disable</p>
<b>Authentication</b>	<p>Click to enable authentication of RIP packets.</p> <p>Provide password to authenticate the RIP packets.</p>
<b>Passive Mode</b>	<p>Enable to prevent the interface from sending RIP advertisements.</p> <p>Default - Disable</p>

**Table – Override Interface Configuration screen elements**

## OSPF

To configure OSPF routes, go to **Network > Dynamic Route > OSPF**.

Open Shortest Path First (OSPF) is an interior gateway protocol that multicasts the routing information to all the hosts within a single network. It sends routing information to all the routers in the network by calculating the shortest path to each router on the basis of the structure built up by each router.

OSPF allows sets of networks to be grouped together into what is known as areas. Area is a logical division of a network. Each area maintains a separate database whose information may be summarized by the connecting router. Hence, the topology of an area is not known to outside world. There are three types of areas:

### Backbone Area

Backbone area also known as area 0, distributes information between non-backbone areas. All other areas in the network are connected to it and the routing between areas takes place using routers which are connected to the backbone area as well as to their respective areas.

### Stub Area

A stub area is an area that do not receive route advertisements external to the Autonomous System (AS), which is a collection of networks under a common network operator that share same routing policy.

### NSSA

A Not-so-stubby-area (NSSA) is a type of stub area that can import AS external routes in a limited amount.

### Area Border Router

An Area Border Router (ABR) is a router that connects areas to the backbone network and maintains separate routing information for each area that it is connected to. It has interfaces in more than one area with at least one interface in backbone area.

**Global Configuration**

Router ID  (e.g. 12.34.5.66)

**▼ Advanced Settings**

Default Metric  (0 - 16777214)

ABR Type

Auto cost reference bandwidth (Mbits/s)  (1 - 4294967)

Default Information Originate  Never  Regular  Always

Metric  (0 - 16777214) Metric Type

Redistribute Connected  Enable

Metric  (0 - 16777214) Metric Type

Redistribute Static  Enable

Metric  (0 - 16777214) Metric Type

Redistribute RIP  Enable

Metric  (0 - 16777214) Metric Type

Redistribute BGP  Enable

Metric  (0 - 16777214) Metric Type

---

**Areas**

Area	Type	Authentication	Area Cost	Virtual Links	Manage
12.34.5.66	Normal	Text		-	

---

**Networks**

Network	Netmask	Area	Manage
192.168.10.10	255.255.255.255	12.34.5.66	

---

**Override Interface Configuration**

Interface	Manage
PortB	

**Screen – Dynamic Routing OSPF**

Screen Element	Description
<b>Global Configuration</b>	
<b>Router ID</b>	Specify a unique router ID. Example: 12.34.5.66.
<b>Advanced Settings</b>	
<b>Default Metric</b>	Specify the default metric value to be used for redistributed routes.  Metric is a property that contains a value used by a routing protocol to decide whether a particular route should be taken or not.  Default - 1

	Acceptable Range - 1 to 16777214
<b>ABR Type</b>	<p>Select the type of Area Border Router (ABR).</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Standard:</b></li> <li>• <b>CISCO</b></li> <li>• <b>IBM</b></li> <li>• <b>Shortcut</b></li> </ul>
<b>Auto Cost Reference Bandwidth (Mbits/s)</b>	<p>Specify cost reference to calculate the OSPF interface cost based on bandwidth.</p> <p>Default - 100Mbits/s</p> <p>Acceptable Range - 1 to 4294967</p>
<b>Default Information Originate</b>	<p>Select an option to control the distribution of default route.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Never</b></li> <li>• <b>Regular</b> – On selecting regular provide the metric and select the metric type.</li> <li>• <b>Always</b> – On selecting regular provide the metric and select the metric type.</li> </ul> <p>Default - Never</p>
<b>Redistribute Connected</b>	<p>Click to enable the redistribution of connected routes into OSPF routing table.</p> <p>Specify metric and metric type for redistributing connected routes.</p> <p>Acceptable Range - 0 to 16777214</p> <p>Metric Type - External Type 1 or External Type 2.</p>
<b>Redistribute Static</b>	<p>Click to enable the redistribution of static routes into OSPF routing table.</p> <p>Specify metric and metric type for redistributing static routes.</p> <p>Acceptable Range - 0 to 16777214</p> <p>Metric Type - External Type 1 or External Type 2.</p>
<b>Redistribute RIP</b>	<p>Click to enable the redistribution of OSPF routes into OSPF routing table.</p> <p>Specify metric and metric type for redistributing RIP routes.</p>



	Acceptable Range - 0 to 16777214 Metric Type - External Type 1 or External Type 2.
<b>Redistribute BGP</b>	Click to enable the redistribution of BGP routes into OSPF routing table.  Specify metric and metric type for redistributing BGP routes.  Acceptable Range - 0 to 16777214 Metric Type - External Type 1 or External Type 2.
<b>Areas</b>	
<b>Add</b>	Click to add an OSPF Area.
<b>Area</b>	Displays the IP Address of the Area.
<b>Type</b>	Displays the type of OSPF Area – Normal or Stub or Stub No-Summary or NSSA or NSSA No-Summary.
<b>Authentication</b>	Displays the type of authentication – Text or MD5.
<b>Area Cost</b>	Displays the area cost
<b>Virtual Links</b>	Displays the virtual link for an area
<b>Edit</b>	Edit the area.
<b>Delete</b>	Delete the area.
<b>Network</b>	
<b>Add</b>	Click to add an OSPF network.
<b>Network</b>	Displays the IP Address of the Network.
<b>Netmask</b>	Displays the netmask of the Network.
<b>Area</b>	Displays the IP Address of the Network.
<b>Edit Icon</b>	Edit the Network.
<b>Delete</b>	Delete the Network
<b>Override Interface Configuration</b>	
<b>Select Interface</b>	Click to select an Interface.
<b>Interface</b>	Displays the configured interface.
<b>Edit Icon</b>	Edit the Interface.
<b>Delete Icon</b>	Delete the Interface.

Table – Dynamic Routing OSPF screen elements

## Adding OSPF Areas

Click Add button under Areas to add, update, or delete areas.

Screen – Adding OSPF Areas



Screen Element	Description
<b>Area</b>	Specify IP Address for the area.
<b>Type</b>	Select the type of OSPF area.  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• Normal</li> <li>• Stub</li> <li>• Stub No-Summary</li> <li>• NSSA</li> <li>• NSSA No-Summary</li> </ul>
<b>Virtual Link (Available only if Normal area type is selected)</b>	Specify a virtual link for an area that does not have a physical connection to connect to the backbone area.  Use Add icon  and Remove icon  to add and remove the Virtual Links.
<b>Authentication</b>	Select the type of authentication from the options available.  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• Text</li> <li>• MD5</li> </ul>
<b>Area Cost</b>	Specify the area cost.  Acceptable Range - 0 to 16777215

Table – Adding OSPF Areas screen elements

## Adding OSPF Networks

Click Add button under Networks to specify IPv4 Address network and subnet mask. You can also add, update, or delete the networks from this page.

Screen – Adding OSPF Network

## Overriding Global Interface Configuration

Click Select Interface button under Override Interface Configuration to override the Interface configuration. You can also add, update, or delete the Interface-specific configuration from this page.

Screen – Overriding Global Interface Configuration

Screen Element	Description
Interface	Select the interface to be configured for OSPF.
Hello Interval	Specify the time interval after which the interface sends hello packet to the neighbor router.  Default - 10 seconds Acceptable Range (seconds) - 1 to 65535

<b>Dead Interval</b>	<p>Specify the time interval after which the interface is declared as dead.</p> <p>Default - 40 seconds</p> <p>Acceptable Range (seconds) - 1 to 65535</p>
<b>Retransmit Interval</b>	<p>Specify the time interval for retransmitting the link state advertisements (LSA) to the interface's neighbor.</p> <p>Default - 5 seconds</p> <p>Acceptable Range (seconds) - 3 to 65535</p>
<b>Transmit Delay</b>	<p>Specify the time in seconds needed to transmit a link state update packet to the interface.</p> <p>Default - 1 second</p> <p>Acceptable Range (seconds) - 1 to 65535</p>
<b>Interface Cost</b>	<p>Specify Interface Cost.</p> <p>Interface Cost can be provided either automatically by selecting "Auto" or providing interface cost manually.</p> <p>Acceptable Range (seconds) - 1 to 65535</p>
<b>Authentication</b>	<p>Select the type of authentication for authenticating the OSPF packets.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Text</b> – If text is selected provide a password for authentication.</li> <li>• <b>MD5</b> – If MD5 is selected provide Key ID and Key. Key ID can be from 0 to 255.</li> </ul>
<b>Router Priority</b>	<p>Specify priority for a router.</p> <p>Default - 1</p> <p>Acceptable Range - 0 to 255</p>

**Table – Overriding Global Interface Configuration screen elements**

## BGP

To configure BGP routes, go to **Network > Dynamic Route > BGP**.

Border Gateway Protocol (BGP) is a path vector protocol that contains path information, enabling the routers to share routing information so that loop-free routes can be created. This protocol is generally used by ISPs.

BGP selects a single path from the multiple advertisements received from multiple sources for the same route. When the path is selected, BGP puts it in the IP routing table and passes the path to its neighbor.

**Global Configuration**

Router ID  (e.g. 12.34.5.66)

Local As\*  (1 - 4294967295)

**Neighbors**

Neighbor	Remote As	Manage
192.168.10.10	4	

**Networks**

Network	Netmask	Manage
192.168.10.12	255.255.255.255	

Screen – Dynamic Routing BGP

Screen Element	Description
<b>Global Configuration</b>	
<b>Router ID</b>	Specify router ID for BGP. Example: 12.34.5.66.
<b>Local As</b>	Specify Local Autonomous System (AS) number.  Acceptable Range - 1 to 4294967295
<b>Neighbors</b>	
<b>Add</b>	Click to add a BGP neighbor.
<b>Neighbor</b>	Displays the IP Address of the Neighbor.

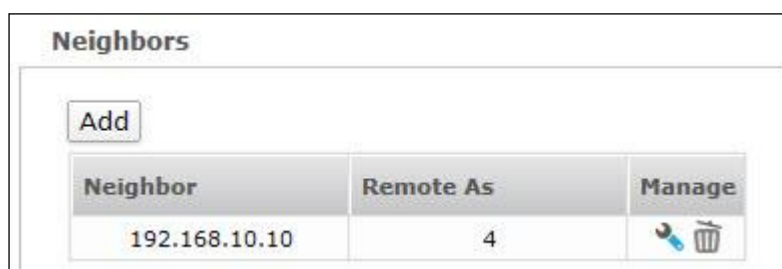
<b>Remote AS</b>	Displays Remote AS number of the Neighbor.
<b>Networks</b>	
<b>Add</b>	Click to add a BGP network.
<b>Network</b>	Displays the IP Address of the Network.
<b>Netmask</b>	Displays the Netmask.

Table – Dynamic Routing BGP screen elements

## Neighbors

Neighbors are the routers between which a TCP connection is established.

Click Add button under Neighbors to specify IPv4 Address of the neighbor router and AS number – remote-as. You can also add, update, or delete the neighbors from this page.



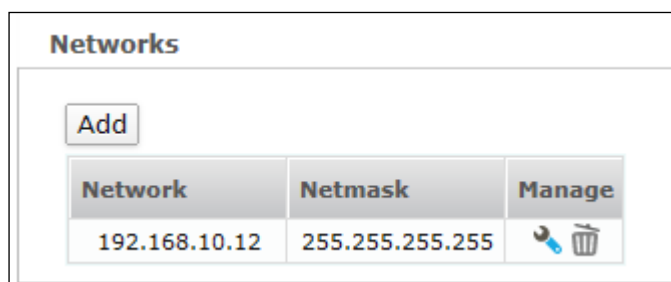
Screen – BGP Neighbors

Screen Element	Description
<b>IPv4 Address</b>	Specify IPv4 Address of the neighbor router.
<b>Remote AS</b>	Specify the remote AS number of neighbor.  Acceptable Range - 1 to 4294967295

Table – BGP Neighbors screen elements

## Networks

Click Add button under Networks to specify IPv4 Address network and subnet mask. You can also add, update, or delete the networks from this page.



Screen – BGP Networks

## PIM-SM

To configure PIM, go to **Network > Dynamic Route > PIM-SM**.

Protocol Independent Multicast (PIM) is a protocol for routing IP packets efficiently to multicast groups that may span throughout the internet. PIM provides dynamic multicast support on the appliance. With dynamic multicast support, a host can join/leave a multicast group dynamically and there is no need to manually add/delete multicast routing entries on the appliance.

Screen – Dynamic Routing PIM-SM

Screen Element	Description
<b>PIM-SM Configuration</b>	
<b>Enable PIM</b>	Enable PIM to provide dynamic multicast support on the appliance.
<b>PIM Enabled Interface</b>	Select the physical interfaces on which PIM service needs to be enabled.  To enable PIM, at least one interface has to be selected.  Note: <ul style="list-style-type: none"> <li>• Only IPv4 bound interfaces can be selected.</li> <li>• Alias, PPPoE and WWAN interfaces are not supported.</li> </ul>
<b>RP Settings</b>	Enable to configure Static or Candidate RP.  <b>Available Options:</b>

	<ul style="list-style-type: none"> <li>• Static RP</li> <li>• Candidate RP</li> </ul>
<b>Static RP</b>	
<b>RP IP</b>	<p>Specify a unicast IP Address for Static RP. RPs can be added or deleted.</p> <p>Maximum eight RP IP Addresses and maximum eight Multicast Group Addresses per RP are allowed.</p>
<b>Multicast Group List</b>	<p>Specify Multicast Group IP address or Network Address separated by comma that will be served by given RP.</p> <p>Use * in Multicast Group List to serve all the Multicast Groups by the defined RP.</p>
<b>Candidate RP</b>	
<b>Candidate RP IP</b>	Select interface IP that will be used as RP IP, if the router is selected as candidate RP.
<b>Multicast Group List</b>	<p>Specify Multicast Group IP address or Network Address separated by comma that will be served by given RP.</p> <p>Maximum eight Multicast Group IP/Network Addresses are allowed.</p> <p>Use * in Multicast Group List to serve all the Multicast Groups by the selected RP.</p>
<b>Candidate RP Priority</b>	<p>Specify the priority of the PIM router in RP election process.</p> <p>Default – 1</p> <p>Acceptable Range – 1 to 255</p>
<b>Timer</b>	<p>Specify time in seconds after which at every specified time, RP candidate messages are generated.</p> <p>Default – 60 seconds</p> <p>Acceptable Range (seconds) – 30 to 180</p>

Table – Dynamic Routing PIM screen elements

**Note**

- Cyberoam supports PIM version2 and PIM-SM mode with Rendezvous Point (RP) selection method as BSR (Bootstrap Router)

**Routing Information**

The Administrator can view various information and status of any dynamic routes configured using RIP, OSPF, and BGP protocols. This overview of the dynamic route information will be useful for further configurations and/or debugging.



## RIP

### Routes

Displays the entire routing configuration information and the routing table for an interface configured using RIP protocol.

Routes			
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP, K - Kernel route			
Sub-codes:			
(n) - normal, (s) - static, (d) - default, (r) - redistribute,			
(i) - interface			
Network	Next Hop	Metric From	Tag Time
Status			

- **Codes and Sub-codes:** Shows how the destination routing information is obtained.
- **Codes:** R – RIP, C – connected, S – Static, O – OSPF, B – BGP, K – Kernel route
- **Sub-codes:** (n) – normal, (s) – static, (d) – default, (r) – redistribute, (i) – interface
- **Network:** It is the IP Address and subnet mask of the destination.
- **Next Hop:** It is an IP Address of the next hop routing device.
- **Metric:** It is the number of routing devices (hop count) a packet must pass through to reach the final destination.
- **From:** Indicates the router (router IP Address) from which the metric is calculated to reach the destination. **If it is directly connected it will show “self”.**
- **Tag:** Indicates the method used for distinguishing between internal routes (learned by RIP) and external routes learned from External Gateway Protocol (ERP) protocols.
- **“0” indicates no tag attached to the route.**
- **Time:** Indicates the elapsed time after which the routing entry will be flushed from RIP table.

### Status

Displays the RIP routing protocol process parameters and statistics.

```

Routes
-----
Status
-----
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 8 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive any version
    Interface      Send Recv  Key-chain
  Routing for Networks:
    10.10.10.1/32
  Routing Information Sources:
    Gateway        BadPackets BadRoutes  Distance Last Update
  Distance: (default is 120)

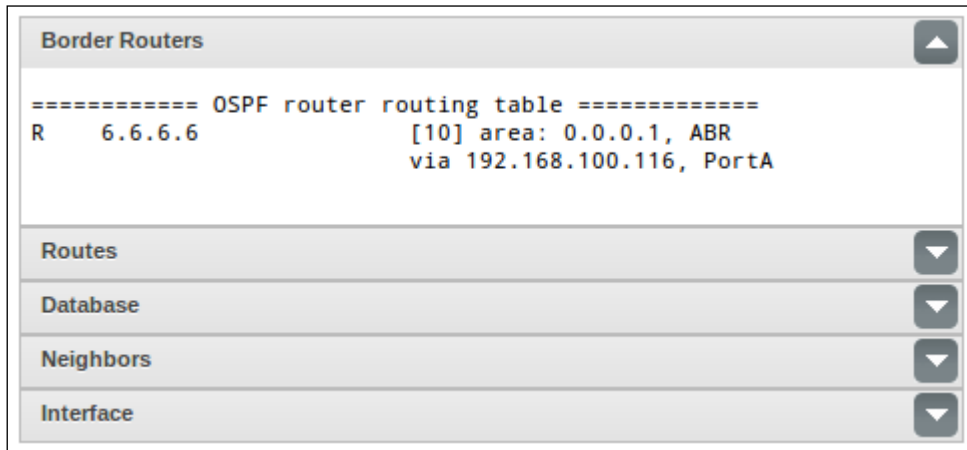
```

- **Routing Protocol is "rip"**: Indicates the routing protocol used.
- **Sending Updates**: Indicates the time between sending updates.
- **Next due**: Specifies when the next update is due to be sent.
- **Timeout after**: Indicates the timeout interval for RIP route after which it is declared invalid and removed from the routing table until the garbage-collect time expires.
- **Garbage collect**: Indicates the time period during which the route metric is set to 16. If no updates are received for the route before the expiry of garbage-collect timer, a route with metric 16 is deleted from the routing table.
- **Outgoing update**: Indicates whether the outgoing filtering list has been set.
- **Incoming update**: Indicates whether the incoming filtering list has been set.
- **Default redistribution metric**: Metric of routes that are redistributed from other routes
- **Redistribution**: Indicates the information about redistributed of other protocols.
- **Default version control**: Indicates the version of RIP packet that are sent and received.
- **Interface**: Shows a RIP-enabled routing interface
- **send**: Displays the version of RIP packets sent out to routing interface. The version is one of the following: **RIP1 or RIP2**
- **recv**: Displays the version of RIP packets accepted on routing interface. The version is one of the following: **RIP1, RIP2, Both**
- **key-chain**: Displayed the authentication key-chain name for the interface, if it is configured.
- **Routing for Network**: Indicates the networks for which the routing process is currently injecting routes.
- **Routing Information Sources**: Indicates the routing sources used to build the routing table. For each source, the following information is displayed.
- **Gateway**: It is an IP Address of the next hop routing device.
- **Bad Packets**: Indicates the number of bad packets received by router.
- **Bad Routes**: Indicates the number of invalid routes from the router.
- **Distance Last Update**: Indicates the time when the administrative distance was last updated.
- **Distance**: Indicates the administrative distance. The distance displayed by default is 120.

## OSPF

### Border Routers

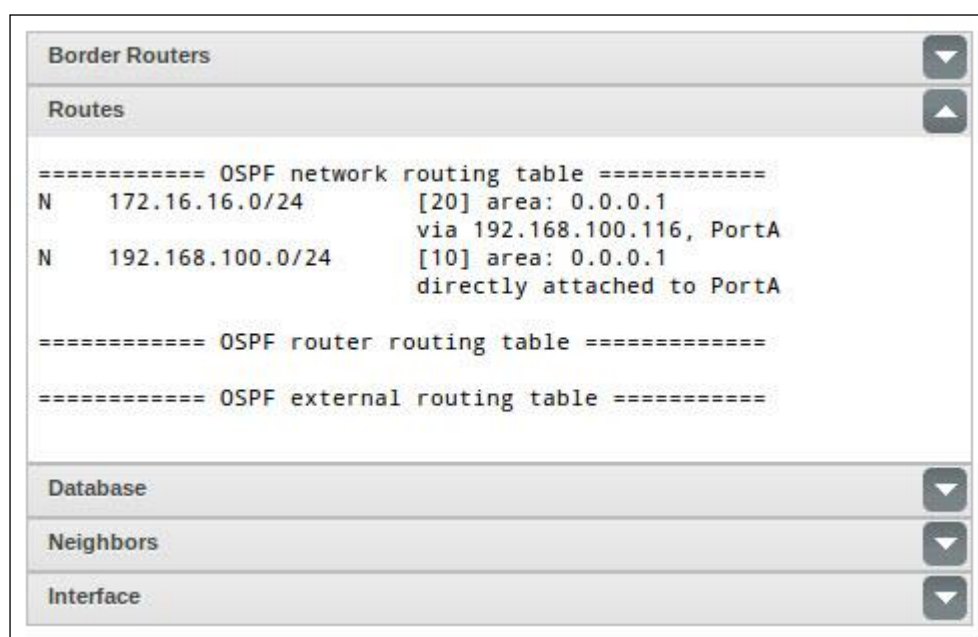
Displays the information about the internal OSPF routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR).



- **R:** Indicates that the information is provided for route to a particular border router.
- **Network IP Address:** Indicates the Router ID of the destination
- **Metric:** It is the cost to reach the final destination.
- **Area:** Indicates the Area Identifier of the outgoing interface.
- **Next Hop:** It is the management IP Address of the next hop routing device.
- **Outgoing Interface:** Indicates the name and IP Address of the outgoing interface to reach the destination.

### Routes

Displays the information about the internal OSPF routing table entries



- **N:** Indicates that the information is provided for a network.
- **Network IP Address:** Indicates the Router ID of the destination.
- **Metric:** It is the cost to reach the final destination.
- **Area:** Indicates the Area Identifier of the outgoing interface.
- **Next Hop:** It is the management IP Address of the next hop routing device.
- **Directly attached:** Indicates a network is directly connected to the interface.
- **Outgoing Interface:** Indicates the name and IP Address of the outgoing interface to reach the destination.

## Database

“Database” shows the list of information related to the OSPF database summary for a specific router. Each link-state database includes link-state an advertisement from throughout the areas to which router is attached.

Border Routers						
Routes						
Database						
OSPF Router with ID (15.15.15.1)						
Router Link States (Area 0.0.0.1)						
Link ID	ADV Router	Age	Seq#	CkSum	Link count	
6.6.6.6	6.6.6.6	75	0x80000006	0x05a9	2	
15.15.15.1	15.15.15.1	79	0x80000003	0xa2ce	1	
Net Link States (Area 0.0.0.1)						
Link ID	ADV Router	Age	Seq#	CkSum		
192.168.100.111	15.15.15.1	79	0x80000001	0x5652		
Router Link States (Area 0.0.0.2)						
Link ID	ADV Router	Age	Seq#	CkSum	Link count	
15.15.15.1	15.15.15.1	30	0x80000001	0x516e	1	
Neighbors						
Interface						

- **Link ID:** Indicates the ID of the link-state advertisement using which a router learns the route. In other words, while a link-state advertisement describes a router, the link-state ID router's OSPF router ID. It can be Networks IP Address or An address generated using the link-state ID
- **ADV Router:** Indicates the advertising Router ID of the destination.
- **Age:** Indicates the time, in seconds, since the LSA was generated.
- **Seq#:** Link state sequence number (detects old or duplicate link-state advertisements)

- **CkSum:** Fletcher checksum of the complete content of the link-state advertisement.
- **Link count:** Number of interfaces detected for router.
- **Net Link States:** It gives information about network LSA originated by DR (Designated Router)
- **Router Link States:** It gives information about router LSA originated by every router
- **Summary Net Link States:** Indicates the information about Summary LSA originated by ABR's

## Neighbors

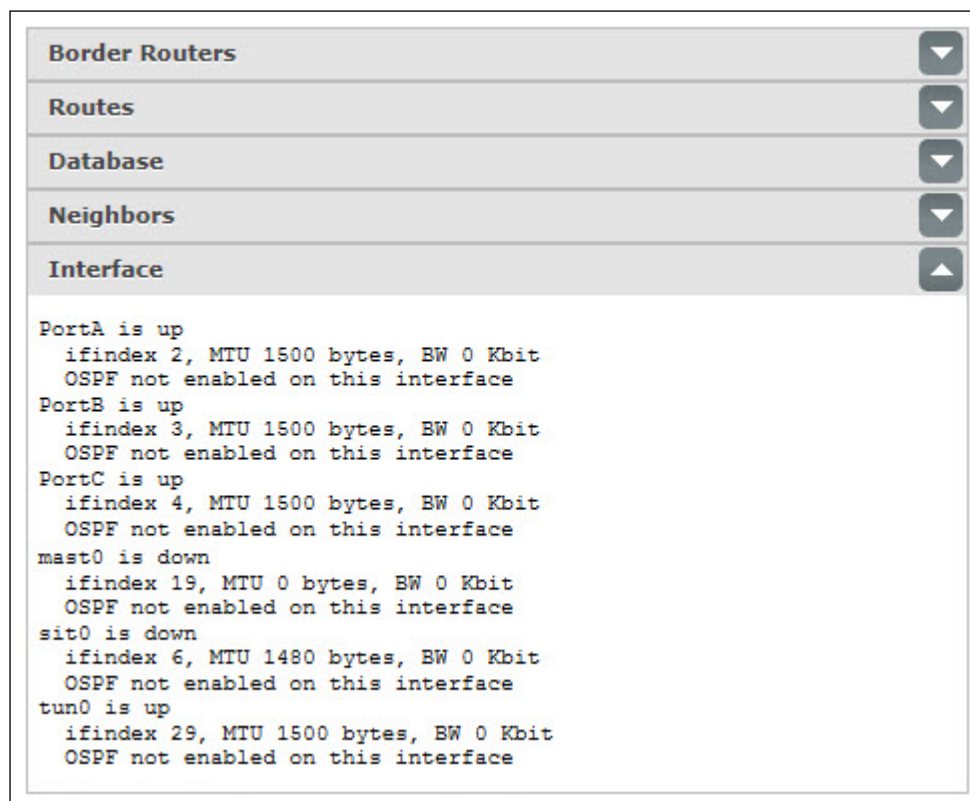
It provides neighbor information based on peer-interface relation.

Border Routers									
Routes									
Database									
Neighbors									
Neighbor ID	Pri	State	Dead Time	Address	Interface	RXmtL	RqstL	DBsmL	
6.6.6.6	1	Full/Backup	31.650s	192.168.100.116	PortA:192.168.100.111	0	0	0	
Interface									

- **Neighbor ID:** Indicates the neighbor router's ID.
- **Pri:** Indicates the router priority assigned to that neighbor.
- **State:** Displays the conversation between router and neighbor, since the neighbor was created. It can have one of the following values:
  - **Down:** Indicates the initial state of a neighbor conversation, that is, there has been no recent information received from the neighbor.
  - **Attempt:** It is valid only for neighbors attached to non-broadcast networks. It indicates that there has been no recent information received from the neighbor.
  - **Init:** Indicates a hello packet though has been received recently from a neighbor, the adjacency is not two-way that is, a bi-directional communication has not yet been established with neighbor.
  - **2-Way:** Indicates that a bi-directional communication is established between the routers and the neighbor has included the router ID in its hello message. The DR and BDR are elected from the set of neighbors in 2-Way state or higher.
  - **ExStart:** Indicates that the two routers are going to synchronize and determine which router will be Master and which the slave.
  - **Exchange:** Indicates that the two routers are describing their respective link-state database by sending database description packets.
  - **Loading:** Indicates that a link-state request packets are sent to the neighbor, requesting for more advertisement that have been discovered but are not yet received in Exchange state.
  - **Full:** Indicates both the routers have accomplished the exchange of all the relevant advertisements and can now appear in router-link and neighbor-link advertisements.
  - **Backup –** Indicates that the neighbor is backup designated router
- **Dead time:** The wait time in seconds to receive a Hello message from OSPF neighbor before assuming the neighbor is dead.
- **Address:** The IP Address of the router's interface with the neighbor.
- **Interface:** Indicates the IP Address of neighbor Interface
- **RXmtL:** Indicates that the link-state retransmit count.
- **RqstL:** Indicates that the link-state request count.
- **DBsmL:** Indicates that the link-state summary count.

## Interface

Displays OSPF interface information.



- **Interface Value:** Indicates the status of the physical interface, that is, whether the interface is up or down.
- **IfIndex:** Indicates the value of interface index (IfIndex). IfIndex is an identification unique number associated with an interface.
- **MTU:** Indicates the Maximum Transmission Unit (MTU) value of the interface. MTU is the largest physical packet size, in bytes, that a network can transmit. This parameter becomes an issue when networks are interconnected and the networks have different MTU sizes. Any packets larger than the MTU value are divided (fragmented) into smaller packets before being sent
- **BW:** Indicates the bandwidth of the Interface.
- **Internet Address:** Displays the IP Address of the Interface.
- **Network Type/IP Address:** Indicates the type of the network along with the IP Address.
- **Area:** Indicates the IP Address of the Area Identifier.
- **MTU mismatch detection:** Indicates whether the MTU Mismatch detection is enabled or disabled. If it is enabled, it would match the MTU of both the interfaces participating in Neighbor-ship establishment.
- **Router ID:** Indicates the identification number of the OSPF Router selected at the start of OSPF process. **The Router ID is unique within the OSPF Domain and does not change unless OSPF restarts or is manually modified.**
- **Network Type:** Indicates the type of Network to which the OSPF interface is connected. A network can be one of the following types:
- **Point-to-point:** A point-to-point network can connect only two routers.



- **Point-to-Multipoint (non-broadcast):** A point-to-multipoint network connects one router to several other routers.
- **Broadcast:** Indicates a network that supports broadcast. In broadcast network a single packet sent (broadcasted) by a router is received by all the routers within the network.
- **Non Broadcast Multiple Access (NBMA) - Indicates** that the network does not have capability to broadcast or multicast. It is used to accurate model X.25 and frame-relay environment in multiple-access network.
- **Cost:** Displays the OSPF metric. It is calculated using formula:  

$$108 / \text{Bandwidth (in bits per seconds [bps])}$$
 where  
 108 - Reference Bandwidth  
 Bandwidth – bandwidth of the interface in bps
- **Transmit delay:** Indicates time the time in seconds for which the OSPF router waits before flooding a link-state advertisement (LSA) over the link. The link state age is incremented by this value, before transmitting an LSA. Default - 1 second.
- **State:** Indicates current state of the specified interface. The state can be one of the following:
  - **DR:** The router is a designated router (DR) on the network.
  - **BDR:** The router is backup designated router (BDR) on the network.
  - **DROTHER:** The router is neither a DR nor a BDR on the network and it establishes adjacencies only with the DR and the BDR.
  - **Waiting:** The interface router is in waiting to announce the state of the link as DR. The wait time is determined by the wait time. This state is normal in case of non broadcast multi access network.
  - **Point-to-Point:** The interface in point-to-point state is fully functional and it starts exchanging hello packets with all its neighbors.
  - **Point-to-Multipoint:** Indicates the interface to be point-to multipoint for ODPF.
- **Priority:** Indicates the priority of the interface router. It assists in electing the DR and BDR on the network to which the interface is connected. A router with priority value 0 can never be a DR/BDR. Default - 1.
- **Designated Router ID:** Indicates the DR router ID for the respective network.
- **Backup Designated Router ID:** Indicates the BDR router ID for the respective network.
- **Saved Network-LSA sequence number:** Indicates the networks link-state sequence number. It is used to calculate shortest path first (SPF).
- **Multicast group membership:** Indicates the multicast group for which the router is a member.
- **Timer intervals configured:** Displays the value of following OSPF Timers:
  - **Hello:** Time interval in seconds that a router sends a hello packet.
  - **Dead:** Indicates the wait time in seconds before declaring a neighbor dead.
  - **Wait:** Displays the time interval that results the interface to exit out of the wait period and elect the DR on the network.
  - **Retransmit:** Displays the wait time before re-transmitting a Database Description (DBD) packet if it has not been acknowledged earlier.
  - **Hello Due In -** Specifies when the next Hello packet is due to be sent.
- **Neighbor Count:** Indicates the total number of discovered neighbors on the interface.
- **Adjacent neighbor count:** Indicates the total number of adjacent neighbors that are fully adjacent to the interface.

## BGP

### Neighbors

Displays the information about the TCP and BGP peers' connections and number of routes advertised/neighbor to/from that peer.

```

Neighbors
-----
BGP neighbor is 192.168.10.10, remote AS 4, local AS 5, external link
BGP version 4, remote router ID 0.0.0.0
BGP state = Active
Last read 01:39:21, hold time is 180, keepalive interval is 60 seconds
Message statistics:
  Inq depth is 0
  Outq depth is 0

          Sent      Rcvd
Opens:           0         0
Notifications:  0         0
Updates:         0         0
Keepalives:     0         0
Route Refresh:  0         0
Capability:     0         0
Total:           0         0

Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
Community attribute sent to this neighbor(both)
0 accepted prefixes

Connections established 0; dropped 0
Last reset never
Next connect timer due in 44 seconds
Read thread: off Write thread: off
  
```

Routes

Summary

- **BGP Neighbor:** Indicates IP Address of the BGP neighbor
- **Remote AS:** Indicates the AS number of the neighbor router.
- **Local AS:** Indicates the value of the configured Local Autonomous Systems (AS).
- **Internal/External Link:** Displays “internal links” for internal BGP (iBGP) neighbors and “external link” for external BGP (eBGP).
- **BGP Version:** Indicates BGP version used for communication with remote router.
- **Remote Router ID:** Indicates router ID (IP Address) of the neighbor router.
- **BGP State:** Indicates the Finite State Machine (FSM) stage. It describes what action should be taken by the BGP routing engine and when for session negotiation.
- **Last Read:** Displays the time, since BGP router the last received a message from neighbor. The time is displayed in HH:MM:SS format.
- **Hold Time:** Displays the time in seconds, until which the BGP will maintain the session with the neighbor without receiving any message from it.
- **Keepalive Interval:** Displays the time interval in seconds specifying how often BGP router sends the keep-alive message to the neighbor.
- **Message Statistics:** Indicates the statistics organized by message type.



- **InQ:** Indicates the number of messages that are in queue, pending to be processed from the neighbor.
- **OutQ:** Indicates the number of messages that are in queue, pending to be sent to the neighbor
- **Sent:** Indicates the number of messages sent to the neighbor.
- **Received:** Indicates the number of messages received from the neighbor.
- **Opens:** Indicates the total number of open messages sent and received.
- **Notifications:** Indicates the total number of error notification messages sent and received.
- **Updates:** Indicates the total number of update messages sent and received.
- **Keepalives:** Indicates the total number of keep-alive messages sent and received.
- **Route Refresh:** Indicates the total number of route refresh messages sent and received.
- **Capability:** Indicates the total number of BGP capabilities advertised and received from the neighbor.
- **Total:** Indicates the total number messages sent and received.
- **Minimum Time between advertisement runs:** Displays the time in seconds between the sent advertisements.
- **For Address Family:** Indicates the IP Address family.
- **Community attribute sent to this neighbor:** Indicates the numerical value of BGP community. This numerical value is assigned to a specific prefix and advertised to neighbor, based on which it decides the whether to filter or modify attributes.
- **Accepted Prefix:** Indicates the number of accepted prefixes that can participate in a BGP peer session.
- **Connections established:** Indicates the number of times a TCP and a BGP connection has been established successfully.
- **Dropped:** Indicates the number of times valid session failed or been taken down.
- **Last reset:** Displays the time since the previously established session with neighbor ended.
- **Local host and Local port:** Displays the IP Address and port number of local BGP router.
- **Foreign host and Foreign port:** Displays the IP Address of Neighbor and BGP destination port number.
- **Next hop:** It is the management IP Address of the next hop routing device.
- **Next connect timer due in:** Specifies when the next hello packet is due to be sent to the BGP neighbor.
- **Read Thread:** Indicates if the Read Thread is ON or Off.
- **Write Thread:** Indicates if the Write Thread is ON or Off.

## Routes

Displays the entire routing configuration information and the routing table for an interface configured using BGP protocol.

```

Neighbors
Routes
BGP table version is 0, local router ID is 12.34.5.66
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
+> 192.168.10.12/32 0.0.0.0             0         32768 i

Total number of prefixes 1

Summary

```

- **BGP Table Version:** Indicates the table version number. The version number is updated with any change in the BGP table.
- **Local Router ID:** Indicates the IP Address of the router.
- **Status codes and Origin codes:** Shows how the destination routing information is obtained.
- **Status codes:** A Status code indicates the status of the table entry and is displayed at the beginning of each line in the table. Status code value can be one of the following: s – suppressed, d –damped, h – history, \* – valid, > – best, i – internal, r – Routing Information Base (RIB)-failure, S – Stale, R – Removed
- **Origin codes:** An Origin code indicates the origin of the entry and is displayed at the end of each line in the table. Origin code value can be one of the following: i – Interior Gateway Protocol (IGP), e – Exterior Gateway Protocol (EGP), ? – incomplete/path not clear.
- **Network:** It is the IP Address and subnet mask of the destination.
- **Next Hop:** It is the management IP Address of the next hop routing device. 0.0.0.0 indicates the router has non-BGP routes to the network.
- **Metric:** It is the value of inter autonomous system metric.
- **LocPrf:** Indicates Local preference value.
- Local Preference is one of the methods to change the path taken by one Autonomous System (AS) to reach to another AS.
- Local Preference value indicates to AS about the path that has local preference, and one with the highest preference being preferred.
- **Weight:** Indicates the route weight as set via autonomous system filters. If there exist more than one path to a particular IP Address, then a path with highest weight is selected.
- **Path:** Indicates the Autonomous system path to the destination network.
- **Total number of prefixes:** Indicates the total number of prefixes/networks.

## Summary

Displays the status of all the BGP connections details like, path, prefixes and attributes information about all the connections to BGP neighbors.

Neighbors									
Routes									
Summary									
BGP router identifier 12.34.5.66, local AS number 5									
RIB entries 1, using 64 bytes of memory									
Peers 1, using 2484 bytes of memory									
Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
192.168.10.10	4	4	0	0	0	0	0	never	Active
Total number of neighbors 1									

- **BGP Router Identifier:** Router ID of the BGP Router
- **Local AS Number:** Indicates the local Autonomous System number to which this router belongs.
- **RIB entries:** Indicates the number of routing information entries in RIB
- **Memory:** Indicates the memory used by RIB entry(ies)
- **Peer:** Indicates the number of neighbor with which the connection is established.
- **Memory:** Indicates the memory used by neighbor entries.
- **Neighbor:** Indicates the IP Address of the neighbor.
- **V:** Indicates BGP version number provided to the neighbor.
- Local Preference is one of the methods to change the path taken by one Autonomous System (AS) to reach to another AS.
- Local Preference value indicates to AS about the path that has local preference, and one with the highest preference being preferred.
- **AS:** Indicates autonomous system number.
- **MsgRcvd:** Indicates the number of messages received from the neighbor.
- **MsgSent:** Indicates the number of messages sent to the neighbor.
- **TblVer:** Indicates the last version of the BGP database that was sent to the neighbor.
- **InQ:** Indicates the number of messages that are in queue, pending to be processed from the neighbor.
- **OutQ:** Indicates the number of messages that are in queue, pending to be sent to the neighbor.
- **Up/Down:** Indicates the total time of a BGP session to remain in Established state, or the current status of BGP session, if it is not in established state.
- **State/PfxRcd:** Indicates the state of the neighbor and the number of prefixes received.
- **Total number of neighbors:** Indicates the total number of neighbors.
- 

## PIM

### Interface Table

Displays all the PIM enabled interfaces and the neighbor information of each interface.

**Multicasting Routing Table**

Displays the information of the multicast groups joined. The information includes the source address, multicast group address, the incoming interface from which packets are accepted, list of outgoing interfaces to which packets are sent, PIM timers, flag bits etc.

**RP SET**

Displays RP set information which is a collection of group-to-RP mappings. This information is used to determine the RP for a multicast group and is maintained by a PIM router.

## DNS

The Domain Name System (DNS) is a system that provides a method for identifying hosts on the Internet using alphanumeric names called fully qualified domain names (FQDNs) instead of using difficult to remember numeric IP Addresses. In other words, it translates domain names to IP Addresses and vice versa.

The DNS server is configured at the time of installation. You can add additional IP addresses of the DNS servers to which the Appliance can connect for name resolution. If multiple DNS are defined, they are queried in the order as they are entered.

To configure DNS, go to **Network > DNS > DNS**.

**DNS List**

**IPv4**

Obtain DNS from DHCP

Obtain DNS from PPPoE

Static DNS

DNS 1

DNS 2

DNS 3

**IPv6**

Obtain DNS from DHCP

Static DNS

DNS 1

DNS 2

DNS 3

**DNS Query Configuration**

Choose server based on incoming requests record type

Choose IPv6 DNS server over IPv4

Choose IPv4 DNS server over IPv6

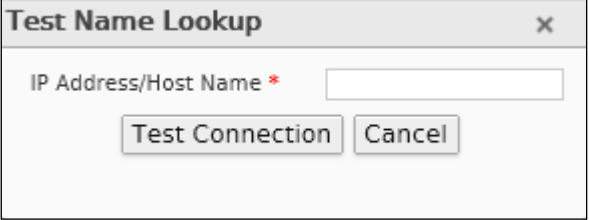
Choose IPv6 if request originator address is IPv6, else IPv4

Screen – Configure DNS

### Parameters

Screen Element	Description
DNS List	
IPv4	

<b>Obtain DNS from DHCP</b>	<p>Click “Obtain DNS from DHCP” to override the Appliance DNS with the DNS address received from DHCP server.</p> <p>Option is available if enabled from Network Configuration Wizard or if a DHCP interface is configured.</p>
<b>Obtain DNS from PPPoE</b>	<p>Click “Obtain DNS from PPPoE” to override the Appliance DNS with the DNS address received from PPPoE server.</p> <p>Option is available if enabled from Network Configuration Wizard or if a DHCP interface is configured.</p>
<b>Static DNS</b>	<p>Select to provide static IPv4 DNS server address.</p> <p>A maximum three static DNS IPv4 Addresses can be provided.</p>
<b>IPv6</b>	
<b>Obtain DNS from DHCP</b>	<p>Click to override the appliance DNS with the DNS address received from DHCPv6 server.</p> <p>Option is available if enabled from Network Configuration Wizard or if a DHCP interface is configured.</p>
<b>Static DNS</b>	<p>Provide static IPv6 address of DNS server.</p> <p>A maximum three static DNS IPv6 addresses can be provided.</p>
<b>DNS Query Configuration</b>	
<b>Choose server based on incoming requests record type</b>	<p>Select to choose the DNS server to be used for resolving the domain name on the basis of the incoming requests record type. Incoming request can be of A or AAAA.</p>
<b>Choose IPv6 DNS server over IPv4</b>	<p>Select to first choose IPv6 DNS server for resolving the DNS and then IPv4 DNS Server.</p> <p>If both IPv6 and IPv4 DNS servers are configured, then it first selects IPv6 DNS server for all requests followed by IPv4 DNS server.</p>
<b>Choose IPv4 DNS server over IPv6</b>	<p>Select to first choose IPv4 DNS server for resolving the DNS and then IPv6 DNS Server.</p> <p>If both IPv6 and IPv4 DNS servers are configured, then it first selects IPv4 DNS server for all requests followed by IPv6 DNS server.</p>
<b>Choose IPv6 if request originator address is IPv6, else IPv4</b>	<p>Select to choose IPv6 DNS server if request is received from IPv6 or choose IPv4 DNS server, if request is received from IPv4.</p>
<b>Apply</b>	<p>Click to apply the configured settings.</p>

<b>Test Name Lookup</b>	<p>Click and provide IP Address or host name for testing the connectivity with the DNS server.</p> 
-------------------------	---

**Table – Configure DNS screen elements**

## DNS Host Entry

The DNS Host Entry page displays the list of all the configured host entries. You can filter list based on Host/Domain name. The page provides the option to add, update, or delete the entries.

To manage DNS Host Entry, go to **Network > DNS > DNS Host Entry**.

Host/Domain Name	IP Address	TTL	Weight	Publish on WAN	Reverse DNS Lookup	Manage
<input type="checkbox"/> Test	1.1.1.1	60	1	No	Off	

Screen – Manage DNS Host Entries

Screen Element	Description
<b>Host/Domain Name</b>	Name of the Host/Domain.
<b>IP Address</b>	<p><b>IP Address</b> – Displays the IP Address of Host/Domain.</p> <p><b>TTL (Time To Live)(Seconds)</b> – Time until which the Host/Domain is valid for the DNS client.</p> <p><b>Weight</b> – Displays the weight for load balancing the traffic.</p> <p><b>Publish on WAN</b> – Displays whether the DNS Host Entry is published on WAN – Yes or No.</p>
<b>Reverse DNS Lookup</b>	Displays if Reverse DNS Lookup is enabled for Host/Domain.

Table – Manage DNS Host Entries

## Adding a DNS Host Entry

To add or edit a DNS Host Entry, go to Network > DNS > DNS Host Entry. Click the Add button to add a DNS Host Entry. To update the details, click on the DNS Host Entry or Edit icon in the Manage column against the DNS Host Entry you want to modify.

Screen – Add DNS Host Entry screen elements



Screen Element	Description
<b>Host/Domain Name</b>	Enter a Fully Qualified Domain Name (FQDN) for Host/Domain.
Address	
<b>Entry Type</b>	Select DNS Host Entry type. <ul style="list-style-type: none"> <li>• Available Options:</li> <li>• Manual – Manually enter the IP address for the host</li> <li>• Interface IP – Configure Interface as host</li> <li>•</li> </ul> Maximum Entries Per Host- 8
<b>IP Address</b>	Specify the IP Address of Host/Domain or select an Interface IP depending on the option selected for Entry Type.
<b>Time To Live (Seconds)</b>	Specify TTL in seconds.  Default - 60 Seconds
<b>Weight</b>	Specify weight for load balancing the traffic. distributes traffic across the links in proportion to the ratio of weights assigned to individual link.  This weight determines how much traffic will pass through a particular link relative to the other link.  Default - 1
<b>Publish on WAN</b>	Enable to publish DNS Host Entry on WAN.  Default - Disabled
<b>Reverse DNS Lookup</b>	Enable to allow reverse DNS lookup.  If there are multiple hosts resolving to same IP Address than Reverse DNS Lookup can be configured only for one of the multiple IP Address.

Table – Add DNS Host Entry screen elements

**Note**

- Only A and PTR type of DNS records are supported i.e. host/domain's IP Address and reverse lookup.
- Address (A) record - points a hostname to an IP Address and returns a 32-bit IPv4 address.
- AAAA record - points a hostname to an IP Address and returns a 128-bit IPv6 address.
- Pointer records (PTR) - are just the reverse of A records and are used for reverse lookups. It maps IP Address to a hostname.
- Maximum number of DNS entries allowed is 1024.
- If the Appliance interface is used as a DNS in client system then, a query is sent to configured DNS servers prior to querying the ROOT servers.

## Address Assignment for IPv6 Devices

IPv6 Clients are assigned IP Address through:

### **DHCP for IPv6**

Similar to IPv4, IPv6 can also use DHCP to assign IP Addresses to any clients. Cyberoam can be configured to be a stateful DHCP server. DHCP server is responsible for assigning the IP Address to the client and for keeping a record of all clients and the IPv6 Address assigned to them.

### **Stateless Address Auto-Configuration (SLAAC)**

The IPv6 protocol supports address auto configuration for stateless addresses. IPv6 devices automatically create unique link-local addresses for IPv6 enabled interfaces and clients use Router Advertisement messages to automatically configure their own IP Address.

## Router Advertisement

The Appliance acting as a router has the ability to participate in Stateless Auto Configuration (SLAAC) and by default provides IPv6 Address and a default gateway to the client.

When the Appliance interface is connected to a network and enabled, the host may send out an ICMPv6 (type 135) Router Solicitation (RS) message that requests Cyberoam to immediately generate Router Advertisement (RA) instead of their next scheduled time. On receiving the RS message, the Appliance immediately sends an ICMPv6 (type 134) Router Advertisement (RA) message announcing about its availability. Router Advertisements includes the information about which method to be used for address assignment, prefixes that are utilized for on-link determination and/or address configuration, hop limit value, several flag status, etc. The critical parameters can be administered centrally and could be automatically propagated to all hosts on the network. The Appliance advertises information about various interfaces and the Internet parameters either periodically or in response to RS message, informing all the nodes on the network about any modification in addressing information. Thus Router Advertisement (along with prefix flags) allows simple stateless auto configuration and guides a host about generating an address using auto-configuration.



### Configuring Router Advertisement Settings for an Interface

Screen – Router Advertisement Settings

Screen Element	Description
<b>Interface</b>	Select an interface for router advertisement.  All IPv6 enabled physical interfaces, LAG, VLAN and Bridge interfaces can be selected.
<b>Description</b>	Provide description for the interface to be selected for router advertisement.
<b>Min Advertisement Interval</b>	Specify the minimum time interval in seconds between two consecutive unsolicited router advertisement messages sent to the clients.  Acceptable Range (Seconds) - 3 to 1350 Default - 198 seconds

	<p>If the Maximum Advertisement Interval is 9 seconds or above, then the Minimum Advertisement Interval must be:</p> $0.75 * \text{Maximum Advertisement Interval}$
<b>Max Advertisement Interval</b>	<p>Specify the maximum time interval in seconds between two consecutive unsolicited router advertisement messages sent to the clients.</p> <p>Acceptable Range (Seconds) - 4 to 1800</p> <p>Default - 600 seconds</p>
<b>Managed Flag</b>	<p>Select to set the Manage Flag. When this flag is set, IPv6 addresses are obtained from DHCPv6 server.</p> <p>The option must be selected only if a DHCPv6 Server is available.</p> <p>By default, this flag is not selected.</p>
<b>Other Flag</b>	<p>Select to set the Other Flag. When this flag is set, DHCPv6 client obtains other network parameters like DNS server, Domain Name, NIS, NISP, SIP, SNTP, BCMS servers from DHCPv6 server.</p> <p>The option must be selected if a DHCPv6 Server is available.</p>
<b>Default Gateway</b>	<p>Select to use Cyberoam as default gateway for communication with client</p> <p>Life Time – Specify the time in seconds for Router Advertisement to be used as a default gateway at client end.</p> <p>The value specified should be between the value specified for “Max Advertisement Interval” and 9000 seconds.</p> <p>Default - 1800 seconds</p>
<b>Prefix Advertisement Configuration</b>	<p>Prefix Advertisement includes zero or more prefix options containing information that the default gateway advertises. This information is used by stateless address auto configuration to auto-generate a global IPv6 Address.</p> <p>Prefix Advertisement has its own list of attributes:</p> <p>Prefix / 64 - Provide first 64 bits of the IPv6 Address.</p>

	<p>The interface uses this prefix information from the Router Advertisement message to determine last 64 bits (interface identifier) of its 128-bit IPv6 Address.</p> <p>The first 64 bits (higher order bits) of IPv6 Address so provided, specifies the network, while the remaining specify a particular address in the network. Hence IPv6 Addresses in one network have same first 64 bits and are called “prefix”.</p> <p>On-link - Select to set the prefix to be “On-link”. With attribute “On-link” set, the devices with IPv6 Addresses that are within this prefix are reachable on the subnet without a need of router.</p> <p>By default, this flag is set</p> <p>Autonomous - Select to set the prefix attribute “Autonomous”. On being set, the global IPv6 Address is automatically generated by appending 64 bit interface identifier to prefix (prefix /64) advertised in the Prefix Information.</p> <p>Only those prefixes that has Autonomous flag set gets a “Stateless Address Auto Configuration (SLAAC)” IPv6 Address.</p> <p>Default – Set</p> <p>Preferred Life Time - Specify the time in minutes for a valid address to remain in the preferred state. The use of preferred address is unrestricted.</p> <p>On expiry of the valid life time, the preferred address becomes deprecated. The use of the deprecated address must be avoided, however it is not forbidden and can be continued to be used as source address for existing communication.</p> <p>The IPv6 Address will continue to remain in Preferred state as long as it is refreshed by prefixes in Router Advertisement or by any other means or are renewed by DHCPv6.</p> <p>Acceptable Range (Seconds) - 0 to Infinite</p> <p>Default - 240 minutes</p> <p>Specify the attribute value as “-1” for infinite preferred life time.</p> <p>Valid Life Time - Specify the time in minutes for an address to remain in the valid state.</p>
--	---

	<p>This value determines the time for an address to be in valid state. Until the time expires, the prefix is considered to be on-link and auto-configured addresses using the prefix can be used.</p> <p>On expiry of the valid life time, the IPv6 Address becomes invalid and cannot be used to send or receive traffic.</p> <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>The value of attribute “Valid Life Time” must be greater than or equal to value of “Preferred Life Time.</li> </ul> </div> <p>Acceptable Range (Seconds) - 0 to Infinite</p> <p>Default - 1440 minutes</p> <p>Specify the attribute value as “-1” for infinite valid life time.</p> <p>Use  and  icons to add or remove a prefix.</p>
<p><b>Advanced Settings</b></p> <p><b>Using Network Discovery Protocol (NDP) the devices on the same interface discovers the presence of each other and the respective link-layer addresses finds gateway routers and maintains the reachability information about the active paths to the peers.</b></p>	
<p><b>Link MTU</b></p>	<p>Specify the Maximum Transmission Unit (MTU) in bytes for the packets sent on this interface.</p> <p>Default - 0</p> <p>Acceptable Range - 1280 to 1500 bytes</p> <p>If link MTU is set to zero, the information will not be advertised by the interface.</p>
<p><b>Reachable Time</b></p>	<p>Specify the reachable time in seconds that the client will use to assume a neighbor is reachable after having received a reachability confirmation message.</p> <p>Default – 0</p> <p>Acceptable Range (Seconds) - 0 to 3600</p>
<p><b>Retransmit Time</b></p>	<p>Specify the retransmission time in seconds that the client will use to determine how long it should wait before retransmitting neighbor solicitation messages.</p> <p>Default – 0</p>

	Acceptable Range (Seconds) - 0 to 60
<b>Hop Limit</b>	<p>Specify the hop limit value.</p> <p>This value determines the number of hops that a packet is limited to. The hop value is decremented by each router along the route. On reaching zero, the packet is destroyed.</p> <p>Default – 64</p> <p>Acceptable Range - 0 to 255</p>

**Table – Router Advertisement Settings screen elements**

## DHCP

Dynamic Host Configuration Protocol (DHCP) automatically assigns IP Address for the hosts on a network reducing the Administrator's configuration task. Instead of requiring administrators to assign, track and change (when necessary) for every host on a network, DHCP does it all automatically. Furthermore, DHCP ensures that duplicate addresses are not used.

The Appliance acts as a DHCP server and assigns a unique IP Address to a host, releases the address as host leaves and re-joins the network. Host can have different IP Address every time it connects to the network. In other words, it provides a mechanism for allocating IP Address dynamically so that addresses can be re-used.

Deploying DHCP in a single segment network is easy. All DHCP messages are IP broadcast messages, and therefore all the computers on the segment can listen and respond to these broadcasts. But things get complicated when there is more than one subnet on the network. This is because the DHCP broadcast messages do not, by default, cross the router interfaces.

The DHCP Relay Agent allows to place DHCP clients and DHCP servers on different networks. Relay Agent makes it possible for DHCP broadcast messages to be sent over routers that do not support forwarding of these types of messages. The DHCP Relay Agent enables DHCP clients to obtain IP Addresses from a DHCP server on a remote subnet, or which is not located on the local subnet. If DHCP Relay Agent is not configured, clients would only be able to obtain IP Addresses from the DHCP server which is on the same subnet.

- [Server](#)
- [Lease](#)
- [Relay](#)





## DHCP Server

Each internal Interface can act as a DHCP server. You can disable or change this DHCP Server configuration. The Appliance cannot act as DHCP server and DHCP Relay Agent simultaneously. Hence, if the Appliance is configured as DHCP server, you will not be able to configure it as a Relay agent and vice-versa.

### Manage DHCP Server list

The DHCP Server page displays a list of all the configured DHCP servers and you can filter this list based on IP Family. The page also provides option to add a new server, update parameters of existing servers, or remove the DHCP server settings.

To manage DHCP servers, go to **Network > DHCP > Server**.

Add		Delete				
<input type="checkbox"/>	Name	Interface	Lease Detail		IP Family	Manage
			Dynamic	Static		
<input type="checkbox"/>	<u>1_1411140364</u>	PortA - 172.16.16.16	172.16.16.17 - 172.16.16.254	-	IPv4	 


Add Delete

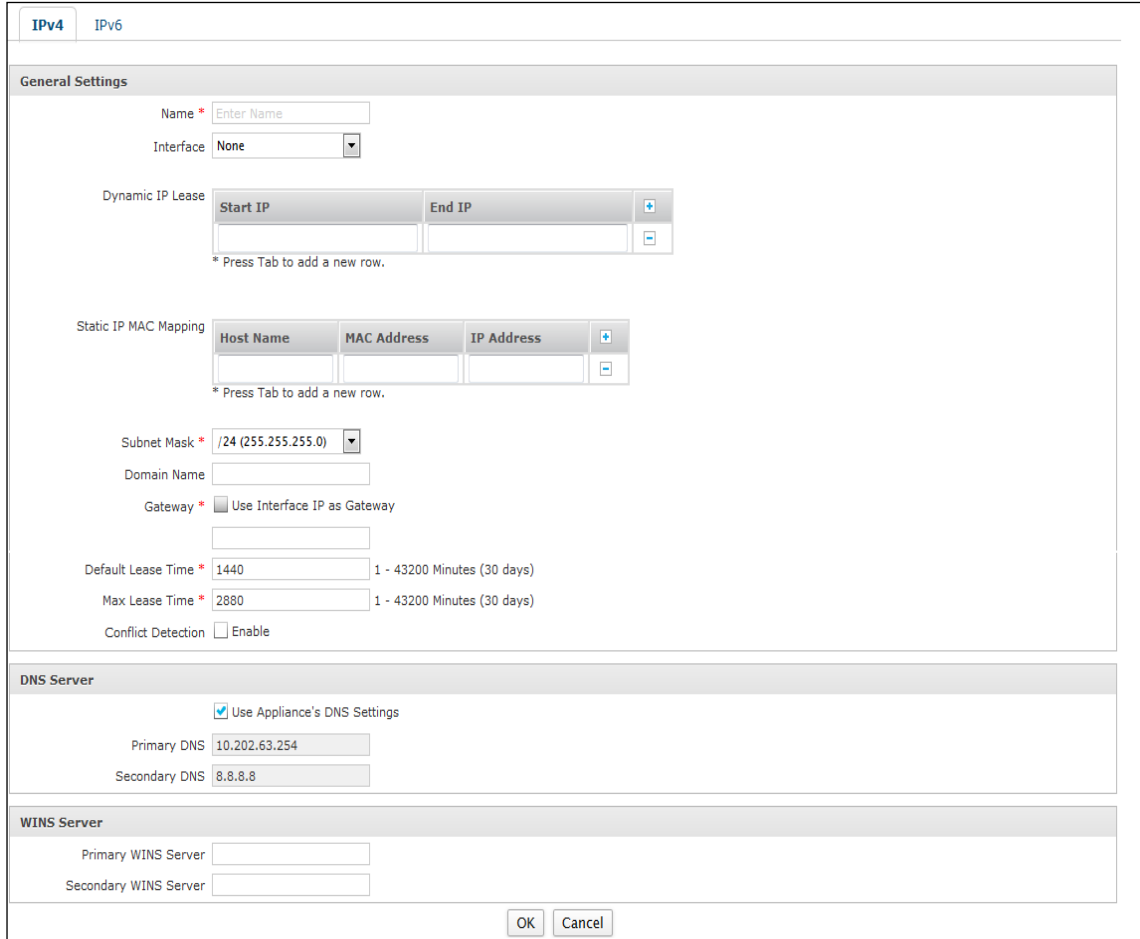
Screen – Manage DHCP Servers

Screen Element	Description
<b>Name</b>	DHCP Server Name.
<b>Interface</b>	Internal interface – Port C or Port A (LAN or DMZ).
<b>Lease Detail</b>	Type of Lease – Static or Dynamic Also, displays the IP Address range for Dynamic Lease type and MAC–IP Mapping list for Static Lease type.
<b>IP Family</b>	Displays the IP Family – IPv4 Address or IPv6 Address.

Table – Manage DHCP Server screen elements



## Configuring Interface as DHCPv4 Server

To add or edit a DHCP server, go to Network > DHCP > Server. Click the Add button to add a DHCP server. To update the details, click on the DHCP server or Edit icon  in the Manage column against the DHCP server you want to modify.



The screenshot shows the configuration page for an IPv4 DHCP server. It includes sections for General Settings, DNS Server, and WINS Server. The General Settings section contains fields for Name, Interface, Dynamic IP Lease (with Start and End IP ranges), Static IP MAC Mapping (with Host Name, MAC Address, and IP Address), Subnet Mask, Domain Name, Gateway, Default Lease Time, Max Lease Time, and Conflict Detection. The DNS Server section has a checkbox for 'Use Appliance's DNS Settings' and fields for Primary and Secondary DNS. The WINS Server section has fields for Primary and Secondary WINS Servers. At the bottom are OK and Cancel buttons.

Screen – Add IPv4 DHCP Server

Screen Element	Description
<b>General Settings</b>	
<b>Name</b>	Specify a name to identify DHCP server uniquely.
<b>Interface</b>	Select any internal interface to set it as DHCPv4 server. DHCP service can be configured on virtual sub-interface but cannot be configured on Interface alias.
<b>Dynamic IP Lease</b>	Specify range of IP Address from which DHCP server must assign to the clients and subnet mask for the IP Address range. It is also possible to configure multiple IP range for a same interface. You can provide multiple IP range for the DHCP Server.  Use icon  and icon  to add or delete the range.
<b>Static IP MAC Mapping</b>	If you always want to assign specific IP Addresses to some or all clients, you can define static MAC Address to IP Address



	<p>mappings. For defining, MAC-IP mapping, you should know the MAC Address of the client's network card. The MAC Address is usually specified in a hexadecimal digits separated by colons (for example, 00:08:76:16:BC:21). Specify host name, MAC Address and IP Address. You can provide multiple MAC-IP mappings for the DHCP Server.</p> <p>Use icon  and icon  to add or delete the MAC-IP mapping.</p>
<b>Subnet Mask</b>	Select subnet mask for the server.
<b>Domain Name</b>	Specify domain name that the DHCP server will assign to the DHCP Clients.
<b>Gateway</b>	<p>Enable to use Interface IP as Gateway.</p> <p>Specify IP Address for default Gateway or click "Use Interface IP as Gateway".</p>
<b>Default Lease Time</b>	<p>Specify default lease time and maximum lease time.</p> <p>Default - 1440 minutes</p> <p>Acceptable Range - 1 to 43200 minutes (30 days).</p>
<b>Max Lease Time</b>	<p>Specify maximum lease time. DHCP client must ask the DHCP server for new settings after the specified maximum lease time.</p> <p>Default - 2880 minutes</p> <p>Acceptable Range - 1 to 43200 minutes (30 days).</p>
<b>Conflict Detection</b>	Enable IP conflict detection to check the IP Address before leasing. If enabled the already leased IP Address will not be leased again
<b>DNS Server</b>	
<b>Use Appliance's DNS Settings</b>	<p>Click to use Appliance DNS Server. In this case the first two configured DNS will be utilized.</p> <p>If not enabled, then provide Primary and Secondary DNS to be used.</p>
<b>Primary DNS</b>	Specify IP Address of Primary DNS server.
<b>Secondary DNS</b>	Specify IP Address of Secondary DNS server.
<b>WINS Server</b>	
<b>Primary WINS Server</b>	Specify IP Address of Primary WINS server.
<b>Secondary WINS Server</b>	Specify IP Address of Secondary WINS server.

Table – Add IPv4 DHCP server screen elements

## Configuring Interface as DHCPv6 Server

IPv4
IPv6

**General Settings**

Name \*

Interface None

Dynamic IP Lease

Start IP	End IP	
		+
		-

\* Press Tab to add a new row.

Static IP DUID Mapping

Host Name	DUID	IP Address	
			+
			-

\* Press Tab to add a new row.

Preferred Time \*  1 - 43200 Minutes (30 days)

Valid Time \*  1 - 43200 Minutes (30 days)

**DNS Server**

Use Appliance's DNS Settings

Primary DNS

Secondary DNS

**Screen – Add DHCPv6 Server**

Screen Element	Description
<b>General Settings</b>	
<b>Name</b>	Enter a name to identify DHCPv6 server uniquely.
<b>Interface</b>	Select any internal interface to set it as DHCPv4 server. DHCP service can be configured on virtual sub-interface but cannot be configured on Interface alias.
<b>Dynamic IP Lease</b>	<p>Specify range of IPv6 Address from which DHCP server must assign to the clients and subnet mask for the IPv6 Address range. It is also possible to configure multiple IPv6 range for a same interface.</p> <p>You can provide multiple IP range for the DHCP Server.</p> <p>Click icon  and icon  to add and delete the range.</p>
<b>Static IP DUID Mapping</b>	If you always want to assign specific IP Addresses to some or all clients, you can define static DUID Address to IP Address mappings. For defining, DUID-IP mapping, you should know the DHCP Unique Identifier (DUID) of the client. The DUID Address is usually specified in groups of two hexadecimal digits separated by colons.



	<p>Specify host name, DUID and IP Address. You can provide multiple DUID-IP mappings for the DHCP Server.</p> <p>Use icon  and icon  to add or delete the DUID-IP mapping.</p>
<b>Preferred Time</b>	<p>Specify the preferred time. Preferred time should be less than valid time.</p> <p>Default - 540 minutes</p> <p>Acceptable Range - 1 to 43200 minutes</p>
<b>Valid Time</b>	<p>Specify the valid time.</p> <p>Default - 720 minutes</p> <p>Acceptable Range - 1 to 43200 minutes</p>
<b>DNS Server</b>	
<b>Use Appliance's DNS Settings</b>	<p>Click to use Appliance DNS Server. In this case the first two configured DNS will be utilized.</p> <p>If not enabled, then provide Primary and Secondary DNS to be used.</p>
<b>Primary DNS</b>	Specify IPv6 Address of Primary DNS server.
<b>Secondary DNS</b>	Specify IPv6 Address of Secondary DNS server.

Table – Add DHCPv6 server screen elements

## DHCP Lease

The Appliance acting as a DHCP server assigns or leases an IP Address from an address pool to a host DHCP client. The IP Address is leased for a determined period of time or until the client relinquishes the address. The page displays a list of all the IP Addresses leased dynamically and you can filter list based on Leased IP, or Client Physical Address.

### IPv4 Address

The following information is displayed for the leased IPv4 addresses:

- Leased IP Address
- Lease start and end time
- Client Physical Address
- Client Host Name
- Leased Type

### IPv6 Addresses

The following information is displayed for the leased IPv6 addresses:

- Leased IP Address
- Lease start and end time
- Client Physical Address
- DUID

List will display IP Addresses leased dynamically only

IPv4 Lease						
Leased IP	Leased Start Time	Leased End Time	Client Physical Address	Client Host-Name	Lease Type	
10.10.13.6	Mon 03 Feb 18:03:47 2014	Wed 05 Feb 18:03:47 2014	28:cf:e9:0f:e1:df	Frontends-Mini	Dynamic	
10.10.13.8	Wed 05 Feb 09:51:25 2014	Thu 06 Feb 09:51:25 2014	8c:3a:e3:97:77:a7	android-aaa2887215dcb110	Dynamic	
10.10.13.2	Wed 05 Feb 10:24:23 2014	Thu 06 Feb 10:24:23 2014	10:9a:dd:1c:db:d7	Nisargs-iPhone	Dynamic	
10.10.13.7	Tue 04 Feb 18:02:13 2014	Thu 06 Feb 18:02:13 2014	68:09:27:39:28:a1	AutomatcsiPhone	Dynamic	

IPv6 Lease				
Leased IP	Leased Start Time	Leased End Time	Client Physical Address	DUID
No Records Found.				

Screen – Lease DHCP Server

## DHCP Relay

The DHCP Relay Agent allows place DHCP clients and DHCP servers on different networks. Deploying DHCP in a single segment network is easy. All DHCP messages are IP broadcast messages, and therefore all the computers on the segment can listen and respond to these broadcasts. But things get complicated when there is more than one subnet on the network. This is because the DHCP broadcast messages do not, by default, cross the router interfaces.

The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers that do not support forwarding of these type of messages. The DHCP Relay Agent enables DHCP clients to obtain IP Addresses from a DHCP server on a remote subnet, or which is not located on the local subnet. If DHCP Relay Agent is not configured, clients would only be able to obtain IP Addresses from the DHCP server which is on the same subnet.

### Note

- DHCP Relay and Server cannot be configured at the same time.

The DHCP Relay page displays list of all the interfaces configured as a relay agent and you can filter the list based on relay agent name and IP Family. The page also provides option to add a new relay agent, update parameters, or delete an agent.

## Manage DHCP Relay Agent list

To manage DHCP relay agents, go to **Network > DHCP > Relay**.


<input type="checkbox"/>	Name	Interface	DHCP Server IP	IP Family	Manage
<input type="checkbox"/>	Test	PortD	2::a	IPv6	 

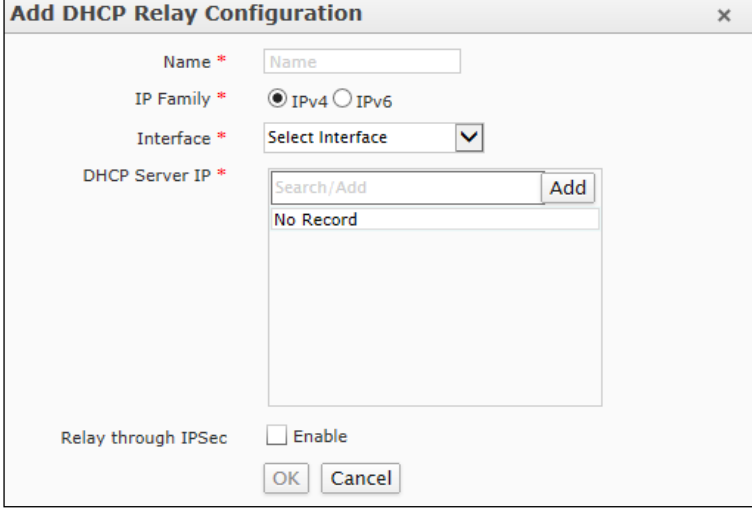
Screen – Manage DHCP Relay Agent

Screen Element	Description
Interface	Internal Interface which is configured as Relay Agent.
DHCP Server IP	DHCP Server IP Address.
IP Family	Displays the IP Family – IPv4 Address or IPv6 Address.

Table – Manage DHCP Relay Agent screen elements

## Configuring an Interface as a DHCP Relay Agent

To add or edit a DHCP relay agent, go to **Network > DHCP > Relay**. Click the Add button to add a relay agent. To update the details, click on the relay agent or Edit icon  in the Manage column against the relay agent you want to modify.



Screen – Add DHCP Relay Agent

Screen Element	Description
<b>Name</b>	Enter a name to identify DHCP Relay Agent.
<b>IP Family</b>	Select the IP Family for DHCP Relay Agent.  <b>Available Options:</b> <b>IPv4</b> <b>IPv6</b>
<b>Interface</b>	Select internal interface.  Each internal Interface can act as a DHCP Relay Agent. The Appliance cannot act as a DHCP server and DHCP Relay Agent simultaneously. Hence if the Appliance is configured as a DHCP Relay Agent, you will not be able to configure it as a server and vice-versa.  DHCP Relay agent can be configured on virtual sub-interface but cannot be configured on Interface alias.
<b>DHCP Server IP</b>	Specify the DHCP Server IP Address.  DHCP requests arriving on the interface selected in above step will be forwarded to this DHCP server.
<b>Relay through IPsec (Only if IP Family is IPv4)</b>	Click to enable Relay through IPsec.



**Table – Add DHCP Relay Agent screen elements**

## **ARP-NDP**

TCP/IP uses ARP (Address Resolution Protocol) protocol to translate IPv4 Address into MAC Address (physical network address). In other words, it maps layer 3 (IPv4 Addresses) to layer 2 (physical or MAC Addresses) to enable communications between hosts residing on the same subnet. Similarly to translate IPv6 Addresses, NDP (Neighbor Discovery Protocol) is used.

ARP is used by hosts that are directly connected on a local network and uses either or both unicast and broadcast transmissions directly to each other. Host finds the physical address of another host on its network by sending an ARP query packet that includes the IP Address of the receiver. As a broadcast protocol, it can create excessive amounts of network traffic on your network. To minimize the broadcast traffic, an ARP cache is maintained to store and reuse previously learned ARP information.

NDP in IPv6 is similar to ARP in IPv4. The main purpose of both the protocols is to enable a host (node) to determine the link layer address (MAC Address) of the node it wants to communicate with, in the local network and to find out the link layer address of the router through which it can access a node in an external network. Thus, the actual exchange of messages can take place between the two nodes. Apart from neighbor discovery, NDP functionality includes router discovery, neighbor presence, redirects, network options (as in DHCP options) and stateless auto-configuration. Similar to ARP, NDP is also susceptible to flooding and poisoning attacks.

NDP has Neighbor solicitations analogous to ARP request and Neighbor Advertisements analogous to ARP replies. Unsolicited neighbor advertisements in IPv6 correspond to gratuitous ARP replies in IPv4. Static Neighbor configuration protects the Neighbor cache for trusted or vulnerable nodes in the network. Static Neighbor Discovery helps in not making solicit request for configured entries and ignores any incoming solicit or advertised ND for configured entries.

## Neighbors

ARP and NDP traffic is vital communication on a network and is enabled on Appliance interfaces by default.

Static Neighbor entry allows binding of the MAC Address to the designated IP Address and port. Once the MAC Address is bound to a port and IP Address, the Appliance will not update its Neighbor table dynamically and will not respond to that IP-MAC pair on any other port. It will also remove any dynamically cached references to that IP Address that might be present, and will not allow additional static mappings of that IP Address.

These entries will be stored in Static Neighbor as well as IPv4 and IPv6 Neighbor Cache table. The Appliance performs the neighbor lookup in the static neighbor table when it receives the request on a particular port. If there is any mismatch in IP Address or MAC Address, the Appliance considers it as a neighbor poisoning attempt and does not update its Neighbor Cache. If entry is not available in the table, the Appliance will look it up in the IPv4 or IPv6 Neighbor Cache and add the MAC Address to Neighbor Cache if required.

Consider an example when IP1 is mapped with MAC1 and IP1-MAC1 pair is bounded to Port A. Similarly IP2 is mapped with MAC1 and IP2-MAC1 pair is bounded to Port A.

IP Address	MAC Address	Port	Neighbor poisoning attempt
IP1	MAC1	A	No
IP1	MAC1	Any other Port than Port A	Yes
IP1	MAC2	A	Yes
IP1	MAC2	Any Other Port	Yes
IP3	MAC1	No static ARP	No
IP2	MAC1	A	No
IP2	MAC1	Any other Port than Port A	Yes

**Table – Showing an example of having IPs having bounded MAC and Port addresses.**

## Neighbor Configuration

The Appliance maintains 3 (three) types of tables for ARP entries: Static Neighbor table, IPv4 Neighbor Cache and IPv6 Neighbor Cache.

### IPv4/IPv6 Neighbor Cache table

IPv4/IPv6 Neighbor Cache table stores static and dynamic Neighbor entries. Static Neighbor entries are defined by Administrators and are permanent while dynamic Neighbor entries are the learned entries and are updated dynamically. Such dynamic entries can be flushed by clicking on the “Flush” button.

Go to **System > ARP-NDP > Neighbors** and select “IPv4 Neighbor Cache” or “IPv6 Neighbor Cache” to view the large number of Neighbor entries. Page allows navigating and managing the Neighbor entries in all the three tables. Select the table type from the dropdown list to view the Neighbor entries in the respective table. It lists IP Address, MAC Address, interface and type of the entry. Entry type can be static or dynamic. If everything is working properly with Neighbor, dynamic Neighbor entry will be displayed as “Complete, Dynamic”. “Complete, Dynamic” means both MAC and IP values are there in the table while “Incomplete, Dynamic” means that the Neighbor request was sent but no reply has yet been received.

**Screen – ARP Configuration**

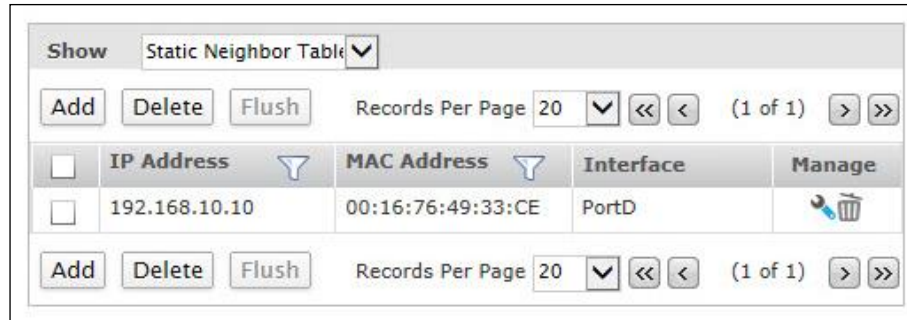
Screen Element	Description
<b>Neighbor Configuration</b>	
<b>Neighbor Cache Entry Time Out</b>	<p>Specify time interval after which the entries in the cache should be flushed.</p> <p>Default - 2 minutes</p> <p>Input range - 1 to 500 minutes</p> <p>Flush the IPv4/IPv6 Neighbor cache whenever the host IP Address on the network changes. As the IP Address is linked to a physical address, it can change but can still be associated with the physical address in the IPv4/IPv6 Neighbor Cache. Flushing the IPv4/IPv6 Neighbor Cache allows new information to be gathered and stored in the IPv4/IPv6 Neighbor Cache.</p>
<b>Log Possible Neighbor Poisoning Attempts</b>	Enable to log the poisoning attempts.

**Table – ARP Configuration screen elements**

## Static Neighbor

### Manage Static ARP list

Manage Static ARP in Appliance; go to **Network > ARP-NDP > Neighbor**.



Screen – Static Neighbor Cache

Screen Element	Description
IP Family	Displays the IP Family for DHCP Relay Agent – IPv4 or IPv6.
IP Address	IP Address (Ipv4/IPv6) of the host.
MAC Address	Physical Address of the host.
Interface	Physical Interface of the host.

Table – Static Neighbor Cache

### Static Neighbor Parameter

To Manage Static ARP in , go to **Network > ARP-NDP > Neighbor**.

Screen – Add Static Neighbor

Screen Element	Description
IP Family	Select the IP Family for DHCP Relay Agent.  <b>Available Options:</b>

	<b>IPv4</b> <b>IPv6</b>
<b>IPv4/IPv6 Address</b>	Specify IPv4/IPv6 Address of the host outside the firewall.
<b>MAC Address</b>	Specify the MAC Address of the host
<b>Interface</b>	Specify the physical Interface. Port A, Port B, Port C or Port D
<b>Add as Trusted MAC entry in Spoof Prevention</b>	If enabled, adds MAC/IP pair in the trusted MAC list.  By default, it is enabled.

**Table – Add Static Neighbor screen elements**

## ARP-NDP Cache

### Manage ARP Cache list

To Manage ARP Cache in Appliance, go to **Network > ARP-NDP > Neighbor**.

The screenshot shows a web interface for managing the ARP Cache. At the top, there is a 'Show' dropdown menu set to 'ARP Cache'. Below this are 'Add' and 'Delete' buttons. The main area contains a table with the following columns: IP Address, MAC Address, Interface, Type, and Manage. The table lists four entries. The first entry has IP 10.10.1.5, MAC -, and Interface PortC, with a status of 'Incomplete'. The second entry has IP 10.103.6.1, MAC 00:e0:20:65:b7:a5, and Interface PortB, with a status of 'Complete,Dynamic'. The third entry has IP 192.168.1.1, MAC 10:12:13:14:15:16, and Interface PortC, with a status of 'Complete,Static'. The fourth entry has IP 10.103.7.1, MAC 00:90:fb:2f:81:70, and Interface PortB, with a status of 'Complete,Dynamic'. Each row has a checkbox on the left and a trash icon on the right. At the bottom, there are 'Add' and 'Delete' buttons, a 'Records Per Page' dropdown set to 20, and navigation arrows.

IP Address	MAC Address	Interface	Type	Manage
10.10.1.5	-	PortC	Incomplete	
10.103.6.1	00:e0:20:65:b7:a5	PortB	Complete,Dynamic	
192.168.1.1	10:12:13:14:15:16	PortC	Complete,Static	
10.103.7.1	00:90:fb:2f:81:70	PortB	Complete,Dynamic	

Screen – ARP Cache Configuration

Screen Element	Description
IP Address	IP Address of the host.
MAC Address	Physical Address of the host.
Interface	Physical Interface of the host.
Type	Type of ARP Table.
Edit Icon	Edit the Static ARP.
Delete Button	Delete the Static ARP.

Table – ARP Cache Configuration screen elements

## Dynamic DNS

Dynamic DNS (Domain Name Service) is a method of keeping a static domain/host name linked to a dynamically assigned IP Address allowing your server to be more easily accessible from various locations on the Internet.

Powered by Dynamic Domain Name System (DDNS), you can now access your Appliance by the domain name and not the dynamic IP Address. DDNS will tie a domain name (for example, myAppliance.com, or mycompany.myAppliance.com) to your dynamic IP Address.

### Manage Dynamic DNS list

The Appliance supports following Dynamic DNS providers:

- DynDNS
- ZoneEdit
- EasyDNS
- DynAccess
- Cyberoam

The page displays list of all the configured DDNS and also provides an option to add, update or delete the configuration.

To manage Dynamic DNS, go to **Network > Dynamic DNS > Dynamic DNS**.

<input type="checkbox"/>	Name	Interface	Service Provider	Last Updated IP	Last Updated Status	Last Updated Time	Failure Reason	Manage
<input type="checkbox"/>	Cyberoam.com	PortB	EasyDNS	0.0.0.0	FAILURE	2013-01-21 13:10:31	Unknown Error	 

Screen – Manage Dynamic DNS

Screen Element	Description
<b>Name</b>	Displays the name of the Host on DDNS server.
<b>Interface</b>	External Interface selected.
<b>Service Provider</b>	Service Provider with whom Hostname is registered.
<b>Last Updated IP</b>	Recently updated IP Address.
<b>Last Updated Status</b>	Recently updated Status.
<b>Last Updated Time</b>	Time of the recent update.
<b>Failure Reason</b>	Reason for failure.


Table – Manage Dynamic DNS

## Configuring Dynamic DNS

### Prerequisite:

Registered Account with any of the following Dynamic DNS providers:

- DynDNS
- ZoneEdit
- EasyDNS
- DynAccess

To add or edit DDNS, go to **Network > Dynamic DNS > Dynamic DNS**. Click the Add button to add a DDNS. To update the details, click on the DDNS name or Edit icon  in the Manage column against the DDNS you want to modify.

**Host Details**

Host Name\*  (Example: google.com)

Interface\*  ▼

IPv4 Address\*  Use Port IP  NATed Public IP

IP Edit Checking Interval\*  4 - 60 Minutes

---

**Service Provider's Details**

Service Provider\*  ▼

Login Name\*

Password\*

Screen – Add DDNS Account

Screen Element	Description
<b>Host Details</b>	
<b>Host Name</b>	Specify a name to identify the host that you want to use on the DDNS server. It is the domain name that you registered with your DDNS service provider for example cyber.com  In case you are configuring <b>DynAccess</b> as a Service Provider, provide host name in the following format: <b>&lt;accountname&gt;.dynaccess.com.</b>



	<p>In case you are configuring <b>Cyberoam</b> as a Service Provider, provide host name in the following format:</p> <p><b>&lt;host name&gt;.ddns.cyberoam.com</b></p> <p>For example, <b>mycompany.ddns.cyberoam.com</b></p>
<b>Interface</b>	Select External Interface. IP Address of the selected interface will be bound to the specified host name
<b>IP Address</b>	Select IPv4 Address source: Port IP or NATed Public IP.
<b>IP Edit Checking Interval</b>	<p>Specify the time interval after which Cyberoam should check and edit the IP Address of your server if changed.</p> <p>Default - 20 minutes</p> <p>Acceptable Range - 4 to 60 minutes</p> <p>For example, if time interval is set to 10 minutes, after every 10 minutes, Cyberoam will check for any changes in your server IP Address.</p>
<b>Service Provider's Details</b>	
<b>Service Provider</b>	<p>Select Service provider with whom you have registered your hostname.</p> <p>In case you are configuring <b>Cyberoam</b> as a Service Provider, login name and password is not required.</p>
<b>Login Name</b>	<p>Specify your DDNS account's Login name.</p> <p>In case you are configuring <b>DynAccess</b> as a Service Provider, provide host name in the following format:</p> <p><b>&lt;accountname&gt;.dynaccess.com.</b></p> <p>Provide login name as <b>accountname</b>.</p>
<b>Password</b>	Specify your DDNS account's Password.

Table – Add DDNS Account screen elements

# Identity

Once you have deployed the Appliance, default access policy is automatically applied which will allow complete network traffic to pass through the Appliance. This will allow you to monitor user activity in your Network based on default policy.

As the Appliance monitors and logs user activity based on IP Address, all the reports are also generated based on the IP Address. To monitor and log user activities based on User names or log on names, you have to configure the Appliance for integrating user information and authentication process. Integration will identify access request based on User names and generate reports based on Usernames.

When the user attempts to access, the Appliance requests a user name and password and authenticates the user's credentials before giving access. User level authentication can be performed using the local user database on the External ADS server, LDAP, RADIUS or TACACS+ server.

To set up user database:

Integrate ADS, LDAP, RADIUS or TACACS+, if external authentication is required.

Configure for local authentication.

Register user

- [Authentication](#)
- [Groups](#)
- [Users](#)
- [Guest Users](#)
- [Policy](#)
- [Live Users](#)

### Authentication

The Appliance provides policy-based filtering that allows defining individual filtering plans for various users of your organization. You can assign individual policies to users (identified by IP Address), or a single policy to a number of users (Group).

The Appliance detects users as they log on to Windows domain in your network via client machines. Users are allowed or denied access based on username and password. In order to authenticate user(s), you must select at least one database against which the Appliance should authenticate users.

To filter Internet requests based on policies assigned, the Appliance must be able to identify a user making a request.

Administrator can configure authentication based on the type of – Administrator, Firewall, VPN and SSL VPN with multiple servers.

- [Authentication Server](#)
- [Firewall](#)
- [VPN](#)
- [Admin](#)

## Authentication Server

The Appliance supports user authentication against:

- an Active Directory
- an LDAP server
- an RADIUS server
- TACACS+ server
- an internal database defined in the Appliance

User authentication can be performed using local user database, RADIUS, TACACS+, LDAP, Active Directory or any combination of these.

## Local Authentication

The Appliance provides a local database for storing user and group information. You can configure the Appliance to use this local database to authenticate users and control their access to the network. Choose local database authentication over ADS, LDAP, RADIUS or TACACS+ when the number of users accessing the network is relatively small. Registering dozens of users and groups takes time, although once the entries are in place they are not difficult to maintain. For networks with larger number of users, user authentication using ADS, LDAP, RADIUS or TACACS+ servers can be more efficient.

A combination of external and local authentication is useful in large networks where it is required to provide guest user accounts for temporary access while a different authentication mechanism like RADIUS for VPN and SSL VPN users provides better security as password is not exchanged over the wire.

Administrator can configure up to twenty authentication servers. In case of multiple servers, authentication request will be forwarded as per the server order configured in the Server Priority list.








External Authentication Servers can be integrated with the Appliance for providing secure access to the users of those servers. The external authentication servers support IPv4 and IPv6 Addresses. You can configure following external servers:

- [Active Directory](#)
- [LDAP Server](#)
- [RADIUS Server](#)
- [TACACS+ Server](#)

The page displays list of all the configured external servers. The page provides option to add a server, update, or delete the server settings. Page also provides option to [import AD user groups](#) in case Active Directory is configured.

## Manage Authentication Servers

To manage external authentication servers, go to **Identity > Authentication > Authentication Server**.

<input type="checkbox"/>	Name	IP	Port	Type	Domain / Admin	Manage
<input type="checkbox"/>	<a href="#">Cyberoam</a>	192.158.10.10	389	Active Directory	Cyberoam	  
<input type="checkbox"/>	<a href="#">Frontend</a>	192.168.16.10	389	LDAP	n/a	 
<input type="checkbox"/>	<a href="#">Elitecore</a>	10.10.1.2	1812	RADIUS	n/a	 

Screen – Manage External Authentication Server

Screen Element	Description
<b>Name</b>	Name of the Server.
<b>IP</b>	IP Address (IPv4/IPv6) of the server.
<b>Port</b>	Port through which the server communicates.
<b>Type</b>	Type of Server – ADS, LDAP or RADIUS.
<b>Domain/Admin</b>	Domain/Admin Name for the ADS Server.
<b>Import Icon</b>	Import the Authentication Server.

Table – Manage External Authentication Server

## Configuring External Authentication Server

### 1. Configuring Active Directory Server Settings

ADS integration feature allows the Appliance to map the users and groups from ADS for the purpose of authentication. This enables the Appliance to identify the network users transparently. Appliance communicates with Windows Directory Services – Active directory (AD) to authenticate user based on groups, domains and organizational units.

Whenever the existing user(s) in ADS logs on for the first time after configuration, user is automatically created in the Appliance and assigned to the default group. If the Groups are already created in the Appliance, User(s) will be created in the respective Groups i.e. the ADS User Groups will be mapped to the Appliance User Groups. In case user is already created and there is a change in expiry date or group name, user will be logged in with the changes.

#### ADS Authentication Process

User has to be authenticated by the Appliance before accessing any resources controlled by the Appliance.


This authentication mechanism allows users to access using their Windows authentication tokens (login/user name and password) in the Windows-based directory services.


User sends the log on request/user authentication request to ADS and ADS authenticates user against the directory objects created in ADS. Once the user is authenticated, Appliance communicates with ADS to get these additional authorization data such as user name, password, user groups, and expiry date as per the configuration, which is used to control the access.

#### Note

- If ADS is down, the authentication request always returns with “Wrong username/password” message.

To configure and manage ADS, go to **Identity > Authentication > Authentication Server**. You can:

- [Configure](#) – Configure ADS Server to communicate with the Appliance
- [Import AD Group](#) – Click Import icon  in the Manage column against the ADS Server for which you want to import the Active Directory Group.
- [NetBIOS Name, FQDN and Search DN](#) – The details of NetBIOS Name, FQDN and Search DN is available from the ADS server.

To configure ADS, go to **Identity > Authentication > Authentication Server**. Click Add Button and select the server type as ‘Active Directory’ to add a server. To update the details, click on the Server or Edit icon  in the Manage column against the AD server you want to modify.

**Add External Server**
✕

Server Type  ▼

Server Name \*

Server IP / Domain \*

Port \*

NetBIOS Domain \*

ADS Username \*

Password \*

Connection Security \*  ▼

Integration Type \*  Loose Integration  Tight Integration

Domain Name \*

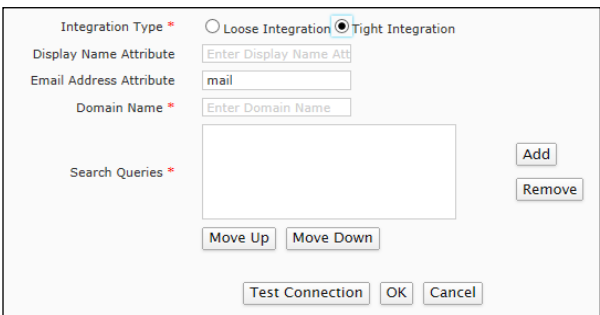
Search Queries \*

Screen – Add Active Directory Server

Screen Element	Description
<b>Server Type</b>	Select the Active Directory Service. If a user is required to authenticate using ADS, Appliance needs to communicate with ADS server for authentication.
<b>Server Name</b>	Specify name to identify the server.
<b>Server IP</b>	Specify ADS server IP Address(IPv4/IPv6) or Domain Name.
<b>Port</b>	Specify Port number through which the server communicates.  Default – 389.
<b>NetBIOS Domain</b>	Specify NetBIOS Domain for ADS server.
<b>ADS Username</b>	Specify username for the user with Administrative privileges for ADS server.
<b>Password</b>	Provide Password for the user with Administrative privileges for ADS server.
<b>Connection Security</b>	Select the type of security to be implemented on the established connection. It provides a method to login to the external server by sending the username and password in encrypted format instead of clear text. We strongly recommend using the encryption method to protect user credentials.

	<p>Available Options:</p> <ul style="list-style-type: none"> <li>• <b>Simple</b> – Select to send the user credentials in un-encrypted or clear text format. The default port number is TCP 389.</li> <li>• <b>SSL</b> – Select to login to external server. This is the most common method used for secured connection. The default port number is TCP 636.</li> <li>• <b>STARTTLS</b> – Select to use same port for simple connection as well as secured connection. In case of the latter, the connection is switched to TLS for security. The default port is 389.</li> </ul> <p>Default – Simple</p>
<p><b>Validate Server Certificate (For Secured Connection – SSL, STARTTLS)</b></p>	<p>Select to validate the certificate of the external server.</p> <p>By default the certificate is not validated.</p>
<p><b>Integration Type</b></p>	<p>Select implementation type of Integration. Integration type is used in setting the user group membership. It provides an added layer of protection by authenticating user based on the group membership apart from authentication attribute.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Loose integration</b> – With loose integration, Administrators require to manage the User Groups themselves. Administrator can modify the group membership. The Appliance does not synchronize groups with the AD Server automatically when user logs into the Appliance.</li> <li>• By default, users are the members of the Appliance default group irrespective of the AD Server group. Appliance uses authentication attribute for authenticating users with AD Server.</li> <li>• <b>Tight integration</b> – With tight integration, Appliance synchronizes groups with AD Server every time the user logs in. The group membership of each user is as defined in the AD Server. Hence, even if the group of a user is changed in the Appliance, on subsequent log on attempt, user logs on as the member of the same group as configured in AD Server.</li> <li>• If the user is a member of multiple AD groups, the Appliance decides the user group based on the order of the groups defined in the Appliance. The Appliance searches group list from top to bottom to determine the membership. The first group that matches is considered as the group of the user and that group policies are applied to the user.</li> </ul>



	 <p style="text-align: center;">Screen – Tight Integration</p> <ul style="list-style-type: none"> <li>• <b>Display Name Attribute</b> – Specify the alias to be displayed for the configured ADS to the user.</li> <li>• <b>Email Address Attribute</b> – It is the alias that is displayed to the user for the configured Email Address.</li> </ul> <p>Default Email Attribute – mail.</p>
<b>Domain Name</b>	Specify the Domain name to which the query is to be added.
<b>Search Queries</b>	<p>Click the “Add” button to enter the search query. Use the Move Up and Move Down buttons to move the search queries in the list.</p> <p>If you do not know search DN, refer to NetBIOS name, FQDN and Search DN.</p>
<b>Test Connection</b>	Click to check the connectivity between ADS and Appliance. It also validates Active Directory user credentials.

**Table – Add Active Directory Server screen elements**

**Note**

- Whenever the existing user(s) in ADS logs on, user is automatically created in Appliance and assigned to the default group.


If the Groups are already created in the Appliance, Users are created in the respective Groups and the ADS User Groups will be mapped to the Appliance User Groups.

In case user is already created and there is a change in expiry date or group name, user will be logged in with the changes.

**Note**

- Connection to ADS is enabled automatically during Active Directory setup, but as ADS server is used for authenticating users it is necessary to check whether the Appliance is able to connect to ADS or not.

## Importing AD User Group

Once you have configured and added AD details select **Identity > Authentication > Authentication Server** and click Import Group icon  against the AD server from which AD groups are to be imported. Follow the on-screen steps:

Step 1. Specify Base DN. Appliance fetches AD Groups or OU Groups from the specified Base DN.



**Cyberoam** | Import Group Wizard Help

**Overview**

Step 1. Provide Base DN for Groups

Step 2. Select AD groups to Import

Step 3. Select common policies for Groups

Step 4. Select Specific policies for Groups(if required)

Step 5. Review Selection

Step 6. View Results

**Overview**

The Import group wizard will help you import Active Directory Groups into Appliance using following steps.

Step 1. Provide Base DN for Groups

Step 2. Select AD groups to import

Step 3. Select common policies for Groups

Step 4. Select Specific policies for Groups(if required)

Step 5. Review Selection

Step 6. View Results

Once you have performed above steps ,your selected groups will be imported from Active Directory to the Appliance and selected policies will be attached to them.

**Start** **Cancel**

The screenshot displays the 'Import Group Wizard' interface. The top header features the 'Cyberoam' logo on the left and the title 'Import Group Wizard' on the right. A left-hand navigation pane lists the following steps: Overview, Step 1. Provide Base DN for Groups (which is the current step), Step 2. Select AD groups to Import, Step 3. Select common policies for Groups, Step 4. Select Specific policies for Groups (if required), Step 5. Review Selection, and Step 6. View Results. The main content area is titled 'Step 1: Provide Base DN for groups' and contains the text: 'Currently, Authentication is integrated with Active Directory. Here, Provide Base DN for groups.' Below this text is a dropdown menu labeled 'Base DN\*' with the value 'DC=Cyberoam,DC=com' selected. At the bottom right of the wizard, there are navigation buttons: a back arrow, a forward arrow, and a 'Cancel' button.

Screen – Define Base DN

Step 2. Select the AD Groups or OU Groups to be imported in the Appliance. Use <Ctrl> + Click to select multiple groups.

If you import OU then OU will also be imported as a Group in the appliance. Once the OU is imported, OU is listed on the Manage Groups page in the format for example, OU=Marketing,DC=Cyberoam,DC=com where OU=<ou name as defined in AD>,DC=<DC as defined in AD>.

The Appliance will not allow importing those groups which are already in the Appliance.



Screen – Select AD Groups to Import

Step 3. Select various policies (Surfing Quota, QoS, Web Filter, Application Filter, Data transfer and SSL VPN) and user authentication time out to be applied on the group members. All the security policies can be applied on OU group also.

Same policy is attached to all the imported groups. If you want to specify different policies for different groups, do not enable the policy.

For example, if you want to specify different Internet policy to different groups, do not enable "Attach to all the Groups".

**Cyberoam** | Import Group Wizard

**Overview**

- Step 1. Provide Base DN for Groups
- Step 2. Select AD groups to Import
- ⇒ Step 3. Select common policies for Groups**
- Step 4. Select Specific policies for Groups (if required)
- Step 5. Review Selection
- Step 6. View Results

**Step 3: Select Common Policies for Groups**

This page helps you select common policies that will be attached to all the groups.

If you do not want to attach common policy to all the groups, then leave "Attach to all the Groups?" checkbox for that policy unchecked. By doing this you can attach different policies to groups in the next step.

		Attach to all the Groups?
Surfing Quota*	Unlimited Internet Access	<input checked="" type="checkbox"/>
Access Time*	Allowed all the time	<input checked="" type="checkbox"/>
Web Filter*	Allow All	<input checked="" type="checkbox"/>
Application Filter*	Allow All	<input checked="" type="checkbox"/>
Bandwidth Policy	Select Here	<input checked="" type="checkbox"/>
Data Transfer	Select Here	<input checked="" type="checkbox"/>

Navigation: Previous, Next, Cancel

**Screen – Define policies for the Groups**

Step 4. If common policies are not to be applied, specify policies to be applied to each group.

**Cyberoam** | Import Group Wizard

**Overview**

- Step 1. Provide Base DN for Groups
- Step 2. Select AD groups to Import
- Step 3. Select common policies for Groups
- Step 4. Select Specific policies for Groups (If required)**
- Step 5. Review Selection
- Step 6. View Results

**Step 4: Select specific Policies for Groups**

You have decided to attach specific policies for groups. This page helps you achieve that.

Select specific policies for each group listed. If you do not want to attach a policy to the group then select do not attach.

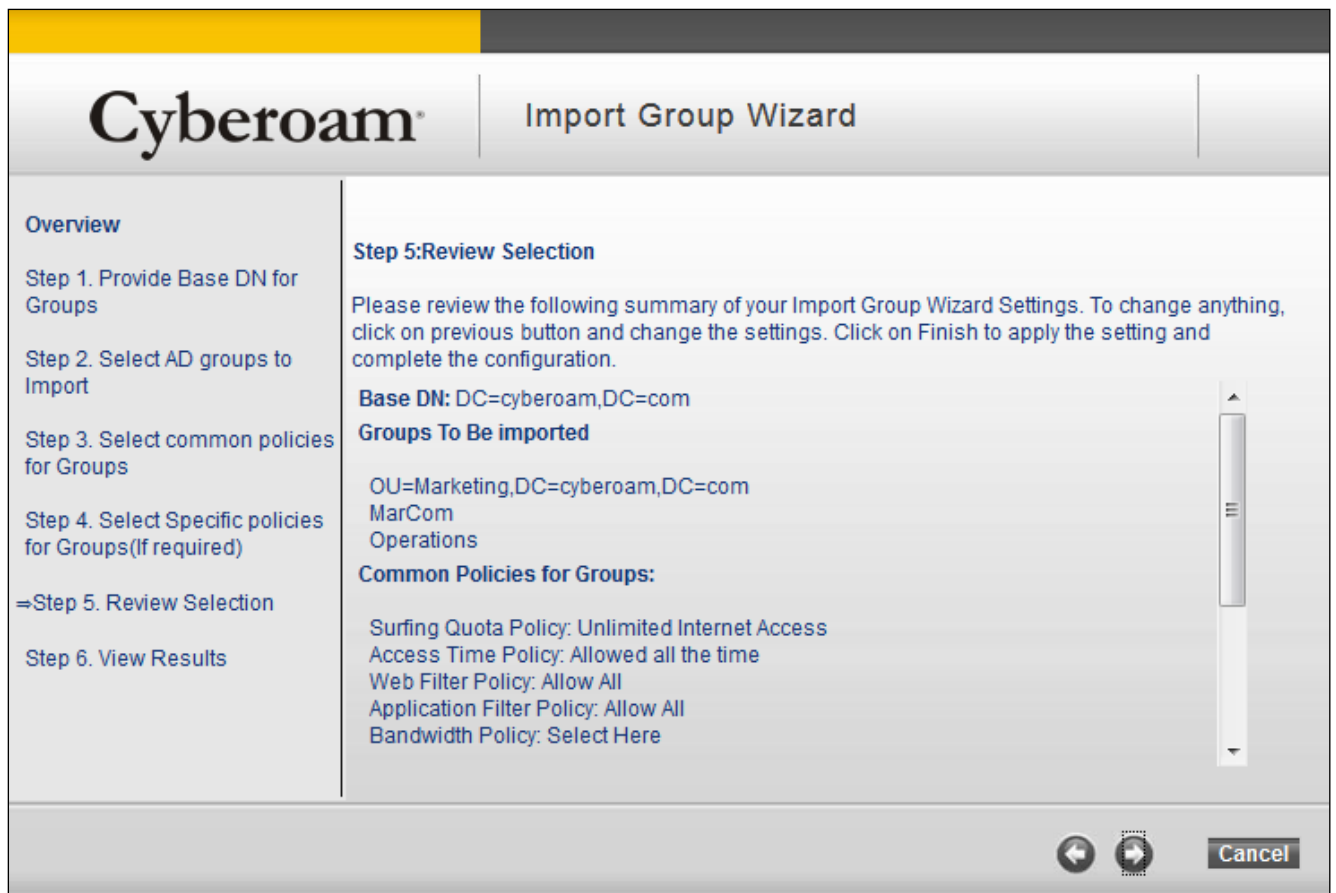
Group Name	Data Transfer
OU=Marketing,DC=cyberoam,DC=com	Do not Attach
MarCom	Do not Attach
Operations	Do not Attach

Do not Attach  
Daily 10 MB  
100 MB Total Data Transfer policy

← → Cancel

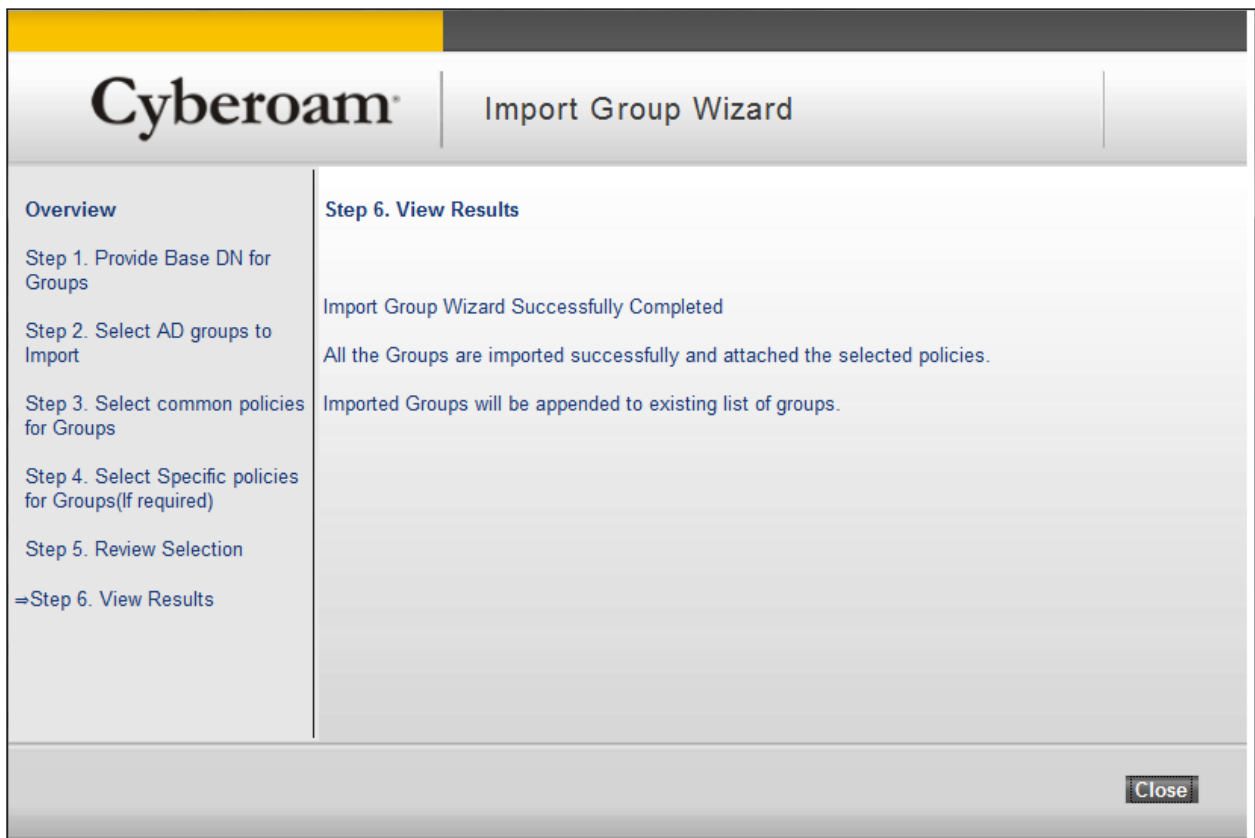
Screen – Define specific policy for a Group

Step 5. View the summary of the groups and policies to be imported. You can also go back and change the configuration.



Screen – Groups imported and specific policies attached to specific Group

Step 6. View Results page displays successful message if groups are imported and policies are successfully attached else appropriate error message will be displayed. Once you close the Wizard, it remains on the Authentication Server page only. All the imported groups are appended at the end of the list.



**Screen – Groups imported and common policies attached successfully**

If the user is a member of multiple AD groups, the Appliance will decide the user group based on the order of the groups defined in the appliance. Appliance searches the Group ordered list from top to bottom to determine the user group membership. The first group that matches is considered as the group of the user and that group policies are applied to the user.

User belonging to OU will be a member of OU group in Cyberoam. Group priority will depend on the group sequence implemented in Cyberoam.

Importing OU is supported only when Active Directory is tightly integrated with CyberoamOS.



## NetBIOS Name, FQDN and Search DN

On the ADS server:

- Go to **Start > Programs > Administrative Tools > Active Directory Users and Computers**
- Right Click the required domain and go to Properties tab
- Search DN will be based on the FQDN. In the given example FQDN is google.com and Search DN will be DC=google, BC=com


## 2. Configure LDAP Authentication Settings

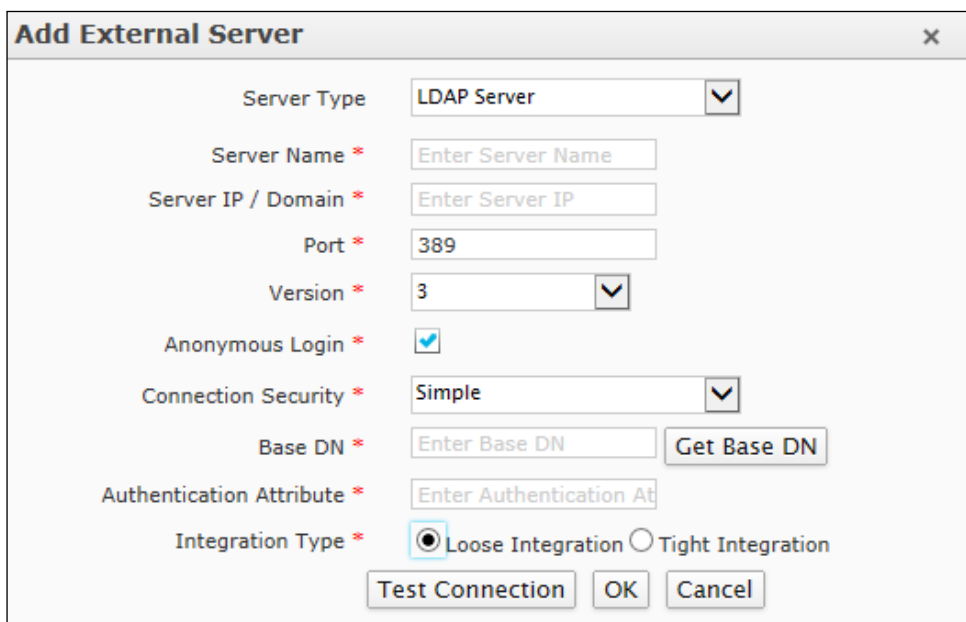
When Appliance is installed in Windows environment with LDAP server, it is not necessary to create users again in the Appliance. The Appliance provides a facility to automatically create user(s) on first log on. Whenever the LDAP users logs on for the first time after configuration, user is automatically created in the Appliance and is assigned to the default group.

This reduces Administrator's burden of creating the same users in the Appliance.

User has to be authenticated by Appliance before granting access to the Internet. Appliance sends the user authentication request to LDAP and LDAP server authenticates user as per supplied tokens. User can log on using their Windows authentication tokens (login/user name and password).

### Configure LDAP Server

To configure LDAP, go to **Identity > Authentication > Authentication Server**. Click Add Button and select the server type as 'LDAP' to add a server. To update the details, click on the Server or Edit icon  in the Manage column against the LDAP server you want to modify.



Screen – Add LDAP Server

Screen Element	Description
Server Type	Select LDAP Server. If the user is required to authenticate using an LDAP server, Appliance needs to communicate with LDAP server for authentication.
Server Name	Specify a name to identify the server.
Server IP / Domain	Specify LDAP Server IP Address (IPv4/IPv6) or Domain Name.
Port	Specify Port number through which Server communicates.  Default – 389
Version	<ul style="list-style-type: none"> <li>Select LDAP version. For example, 2</li> </ul>

<b>Anonymous Login</b>	<p>Disable if identity (username and password) and authentication of Administrator is required to log on to the LDAP server to retrieve information. If disabled, specify a domain or local administrator username and password to log on to the LDAP server.</p> <p>If Anonymous Login is enabled, you connect as the anonymous user on LDAP server and there is no need to supply username and password.</p>
<b>Connection Security</b>	<p>Select the type of security to be implemented on the established connection. It provides a method to login to the external server by sending the username and password in encrypted format instead of clear text. We strongly recommend using one of the encryption method to protect user credentials.</p> <p>Available Options:</p> <ul style="list-style-type: none"> <li>• <b>Simple</b> – Select to send the user credentials in un-encrypted format i.e. clear text. The default port number is TCP 389.</li> <li>• <b>SSL</b> – Select to login to external server. This is the most common method used for secured connection. The default port number is TCP 636.</li> <li>• <b>STARTTLS</b> – Select to use the same port for simple connection as well as secured connection. In case of the latter, the connection is switched to TLS for security. The default port is 389.</li> </ul> <p>Default – Simple</p>
<b>Validate Server Certificate (For Secured Connection – SSL, STARTTLS)</b>	<p>Select to validate the certificate on the external server.</p> <p>By default, the certificate is not validated.</p>
<b>Client Certificate (For Secured Connection – SSL, STARTTLS)</b>	<p>Select a client certificate from the list to establish a secured connection.</p> <p>By default, the Appliance Certificate is used.</p>
<b>Base DN</b>	<p>Specify the base distinguished name (Base DN) of the directory service, indicating the starting point for searching user in the directory service. If you are not aware about Base DN, click Get Base DN to retrieve the base DN.</p> <p>The top level of the LDAP directory tree is the base, referred to as the "Base DN". A base DN usually takes one of the three forms: Organization name, Company's Internet Domain name or DNS domain name. For example dc=google, dc=com</p>
<b>Authentication Attribute</b>	<p>Set authentication attribute. It is the attribute used to perform a user search.</p>

	By default, LDAP uses Unique Identification (UID) attribute to identify user entries. If you want to use a different attribute (such as a given name), specify the attribute name in this field.
<b>Integration Type</b>	<p>Select implementation type of Integration. Integration type is used in setting the user group membership.</p> <p>It provides an added layer of protection by authenticating user based on the group membership apart from authentication attribute. One needs to configure both Group Name attribute and authentication attribute for authentication. Group membership of each User and expiry day as defined in LDAP server.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Loose integration</b> – With loose integration, Administrators require to manage the User Groups themselves. Administrator can modify the group membership. The Appliance does not synchronize groups with LDAP Server automatically when user logs into the Appliance.</li> <li>• By default, users are the member of Appliance default group irrespective of LDAP Server group. Appliance uses authentication attribute for authenticating users with LDAP Server.</li> <li>• <b>Tight integration</b> – With tight integration, Appliance synchronizes groups with LDAP Server every time the user logs in. The group membership of each user is as defined in the LDAP Server. Hence, even if the group of a user is changed in Appliance, on subsequent log on attempt, user logs on as the member of the same group as configured in LDAP Server.</li> <li>• If the user is a member of multiple LDAP groups, the Appliance decides the user group based on the order of the groups defined in the Appliance. searches group list from top to bottom to determine the membership. The first group that matches is considered as the group of the user and that group policies are applied to the user.</li> </ul> <div data-bbox="655 1585 1402 1888" style="border: 1px solid black; padding: 5px;"> <p>Integration Type * <input type="radio"/> Loose Integration <input checked="" type="radio"/> Tight Integration</p> <p>Display Name Attribute <input type="text" value="Enter Display Name Att"/></p> <p>Email Address Attribute <input type="text" value="mail"/></p> <p>Group Name Attribute * <input type="text" value="Enter Group Name Attr"/></p> <p>Expire Date Attribute * <input type="text" value="Enter Expire Date Attr"/></p> <p style="text-align: center;"><input type="button" value="Test Connection"/> <input type="button" value="OK"/> <input type="button" value="Cancel"/></p> </div> <p style="text-align: center;"><b>Screen – Tight Integration</b></p>

	<ul style="list-style-type: none"> <li>• <b>Display Name Attribute</b> – Specify the alias to be displayed for the configured ADS to the user.</li> <li>• <b>Email Address Attribute</b> – It is the alias that is displayed to the user for the configured Email Address. <b>By default, the Email Address Attribute is “mail”.</b></li> <li>• <b>Group Name Attribute</b> – Specify the alias to be displayed to the user for the configured Group Name.</li> <li>• <b>Expire Date Attribute</b> – Specify the attribute to be displayed to the user against which the expiry date is configured.</li> </ul>
<b>Test Connection</b>	Click to check the connectivity between LDAP and Appliance. It also validates LDAP user credentials.

Table – Add LDAP Server screen elements

**Note**

**Whenever the existing user(s) in LDAP logs on, user is automatically created in the Appliance and assigned to the default group.**

If the Groups are already created in the Appliance, Users are added in the respective Groups and the LDAP User Groups are mapped to Appliance User Groups.


### 3. Configure RADIUS Server Settings

RADIUS stands for Remote Authentication Dial In User Service and is a protocol for allowing network devices to authenticate users against a central database. In addition to user information, RADIUS can store technical information used by network devices such as protocols supported, IP Addresses, telephone numbers, routing information, and so on. Together this information constitutes a user profile that is stored in a file or database on the RADIUS server.

RADIUS servers provide authentication, authorization, and accounting functions but the Appliance uses only the authentication function of the RADIUS server.

Before you can use RADIUS authentication, you must have a functioning RADIUS server on the network.

#### Configure RADIUS Server

To configure RADIUS, go to **Identity > Authentication > Authentication Server**. Click Add Button and select the server type as 'RADIUS' to add a server. To update the details, click on the Server or Edit icon  in the Manage column against the RADIUS server you want to modify.

**Add External Server**

Server Type:

Server Name \*:

Server IP \*:

Authentication Port \*:

Enable RADIUS-based Accounting

Accounting Port:

Shared Secret \*:

Integration Type \*:  Loose Integration  Tight Integration

Screen – Add RADIUS Server

Screen Element	Description
<b>Server Type</b>	Select RADIUS Server. If user is required to authenticate using a RADIUS server, Appliance needs to communicate with RADIUS server for authentication.
<b>Server Name</b>	Specify name to identify the RADIUS Server.
<b>Server IP</b>	Specify RADIUS Server IP Address (IPv4/IPv6).
<b>Authentication Port</b>	Specify Port number through which Server communicates.  Default – 1812

<p><b>Enable RADIUS-based Accounting</b></p>	<p>Select to enable accounting on RADIUS server.</p> <p>Appliance sends following information to the RADIUS server as soon as the user logs in:</p> <ul style="list-style-type: none"> <li>• Accounting Start Request</li> <li>• User logon time</li> </ul> <p>Appliance sends following information to the RADIUS server the moment the user logs out:</p> <ul style="list-style-type: none"> <li>• Accounting Stop Request</li> <li>• User log out time</li> </ul> <p><b>Supported Client Types:</b> Windows Client, HTTP Client, Linux Client, Android, iOS, iOS HTTP Client, Android HTTP Client, API Client.</p> <p><b>Note:</b> Accounting stop message is not sent to RADIUS server when Cyberoam shuts down or reboots.</p>
<p><b>Accounting Port</b></p>	<p>Specify RADIUS port number through which the appliance can communicate with RADIUS.</p>
<p><b>Shared Secret</b></p>	<p>Provide share secret, which is to be used to encrypt information passed to the Appliance.</p>
<p><b>Integration Type</b></p>	<p>Select Integration type. Integration type is used in setting the user group membership.</p> <p>Select Tight Integration with the Appliance if you want to use vendor specific attribute for setting the user group membership and specify group name attribute.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Loose integration</b> – With loose integration, Administrators require to manage the User Groups themselves. Administrator can modify the group membership. The Appliance does not synchronize groups with RADIUS Server automatically when user logs into the Appliance.</li> <li>• By default, users are the member of Appliance default group irrespective of RADIUS Server group. Appliance uses authentication attribute for authenticating users with RADIUS Server.</li> <li>• <b>Tight integration</b> – With tight integration, Appliance synchronizes groups with RADIUS Server every time the user logs in. The group membership of each user is as defined in the RADIUS Server. Hence, even if the group of a user is changed in Appliance, on subsequent log on attempt, user logs on as the member of the same group as configured in RADIUS Server.</li> </ul>

	<ul style="list-style-type: none"> <li>If the user is a member of multiple RADIUS groups, the Appliance decides the user group based on the order of the groups defined in the Appliance. Appliance searches group list from top to bottom to determine the membership. The first group that matches is considered as the group of the user and that group policies are applied to the user.</li> </ul> <div data-bbox="655 436 1401 595" style="border: 1px solid black; padding: 5px;"> <p>Integration Type * <input type="radio"/> Loose Integration <input checked="" type="radio"/> Tight Integration</p> <p>Group Name Attribute * <input type="text" value="Enter Group Name Attr"/></p> <p><input type="button" value="Test Connection"/> <input type="button" value="OK"/> <input type="button" value="Cancel"/></p> </div> <ul style="list-style-type: none"> <li>Group Name Attribute</li> <li>Specify the name to be displayed to the user for the configured Group Name.</li> </ul>
<b>Test Connection Button</b>	Click to check the connectivity between RADIUS and Appliance. It also validates RADIUS user credentials.

Table – Add RADIUS Server screen elements

**Note**

- Whenever the existing user(s) in RADIUS logs on, user is automatically created in Appliance and assigned to the default group.

If the Groups are already created in the Appliance, Users are created in the respective Groups and the RADIUS User Groups will be mapped to the Appliance User Groups.




## 4. Configure TACACS+ Server Settings

TACACS+ (Terminal Access Controller Access Control System Plus) provides access control for routers, network access servers and other networked computing devices via one or more centralized servers.

TACACS+ provides separate authentication, authorization and accounting services but the appliance uses only the authentication function of the TACACS+ server.

Before you can use TACACS+ authentication, you must have a functioning TACACS+ server on the network.

### Configure TACACS+ Server

To configure TACACS+, go to **Identity > Authentication > Authentication Server**. Click Add Button and select the server type as 'TACACS+ Server' to add a server. To update the details, click on the Server or Edit icon  in the Manage column against the TACACS+ server you want to modify.

#### Add External Server

Server Type	<input type="text" value="TACACS+ Server"/>
Server Name *	<input type="text" value="Enter Server Name"/>
Server IP *	<input type="text" value="Enter Server IP"/>
Port *	<input type="text" value="49"/>
Shared Secret *	<input type="text" value="Shared Secret"/>

Screen – Add TACACS+ Server

Screen Element	Description
<b>Server Type</b>	Select TACACS+ Server.  If user is required to authenticate using a TACACS+ server, Appliance needs to communicate with TACACS+ server for authentication.
<b>Server Name</b>	Specify name to identify the TACACS+ Server.
<b>Server IP</b>	Specify TACACS+ Server IP Address.
<b>Port</b>	Specify port number on the TACACS+ server to which the appliance sends the authentication request.  Default – 49
<b>Shared Secret</b>	Provide share secret, which is to be used to encrypt information passed to the Appliance.

---

<b>Test Connection Button</b>	Click to check the connectivity between the TACACS+ server and the appliance. It also validates TACACS+ user credentials.
-------------------------------	---

**Table – Add TACACS+ Server screen elements**

**Note**

- Cyberoam supports CHAP & PAP authentication methods to authenticate L2TP/PPTP users against TACACS+ server.
- Cyberoam supports PAP authentication protocol to authenticate Firewall/Administrator/VPN users against TACACS+ server.

## Firewall

To configure and manage authentication settings for Firewall, go to **Identity > Authentication > Firewall**.

**Authentication Methods**

Authentication Server List	Selected Authentication Server
<input type="text" value="Search"/> <input checked="" type="checkbox"/> Local	<input checked="" type="checkbox"/> Local

List order indicates priority

Default Group:  ▼

---

**Global Settings**

Maximum Session Timeout \*  Unlimited  Minutes (Between 3-1440)

Simultaneous Logins \*  Unlimited  (1 - 99)

---

**CTAS Settings**

User Inactivity  Enable  Disable

Inactivity Time  Minutes (Between 3-1440)

Data Transfer Threshold  Bytes

---

**NTLM Settings**

Inactivity Time  Minutes (Between 6-1440)

Data Transfer Threshold  Bytes

HTTP challenge redirect on Intranet Zone  Enable

---

**Web Client Settings ( iOS, Android and API )**

Inactivity Time  Minutes (Between 6-1440)

Data Transfer Threshold  Bytes

---

**SSO using radius accounting request**

Radius Client IPv4	Shared Secret	Show Shared Secret	Edit
		Show	Edit

---

**Captive Portal Settings**

Unauthenticated users redirection  Yes  No ( Access Denied )

Unauthenticated users settings  Captive Portal  Custom Message

HTTPS Redirection  Enable

My Account Link  Enable

URL Redirection after Login  Enable

URL to redirect  User requested URL  Custom URL

Preserve captive portal after login  Yes  No

Keep Alive Request For Captive Portal  Enable  Disable

User Inactivity Timeout  Unlimited  Minutes (Between 3-1440)

Data Transfer Threshold  Bytes

**Screen – Firewall Authentication**

## Parameters

Screen Element	Description
<b>Authentication Methods</b>	
<b>Authentication Server List</b>	<p>Select Authentication server.</p> <p>“Authentication Server List” displays all the configured servers while “Selected Authentication Server” List displays servers that will be used for authentication when user tries to login.</p> <p>In case of multiple servers, authentication request will be forwarded as per the order configured in the Selected Authentication server List.</p>
<b>Default Group</b>	Select the default group for Firewall authentication.
<b>Global Settings</b>	
<b>Maximum Session Timeout</b>	<p>Specify timeout duration in minutes.</p> <p>Acceptable Range (Minutes) – 3 to 1440</p> <p>Authentication Session timeout is the time in minutes a user is logged into the Appliance. Exceeding the period, user will be logged out automatically and user must re-authenticate. This is applicable to administrative sessions only.</p> <p>Enable “Unlimited” to allow the users to remain logged in.</p>
<b>Simultaneous Logins</b>	<p>Customize the maximum number of concurrent logins allowed to the user.</p> <p>Specify number of concurrent logins allowed to the user.</p> <p>Acceptable Range – 1 to 99 concurrent users</p> <p>OR</p> <p>Enable “Unlimited” to allow unlimited concurrent logins to the user.</p> <p>Login restriction is applicable to only those users who are added after this configuration.</p>
<b>CTAS Settings</b>	
<b>User Inactivity</b>	<p>Select to enable or disable User Inactivity.</p> <p>When users logs in the Appliance and performs no activity, remaining idle for specific time span, they are considered inactive.</p>

	By default, User Inactivity is disabled.
<b>Inactivity Time</b>	<p>Specify the inactivity time in minutes.</p> <p>User Inactivity timeout is the inactive/idle time in minutes after which the user will be logged out and has to re-authenticate.</p> <p>Inactivity Time Range (Minutes): 3 – 1440</p> <p>Default - 3 minutes</p>
<b>Data Transfer Threshold</b>	<p>Specify the minimum data to be transferred.</p> <p>If the minimum data is not transferred within the specified time, the user will be marked as inactive.</p> <p>Default – 100 Bytes</p>
<b>NTLM Settings</b>	
<b>Inactivity Time</b>	<p>Specify the inactivity time in minutes.</p> <p>User Inactivity timeout is the inactive/idle time in minutes after which user will be logged out and has to re-authenticate.</p> <p>Inactivity Time Range (Minutes): 6 – 1440</p> <p>Default – 6</p>
<b>Data Transfer Threshold</b>	<p>Specify the minimum data to be transferred.</p> <p>If the minimum data is not transferred within the specified time, the user will be marked as inactive.</p> <p>Default Value – 1024 Bytes</p>
<b>HTTP challenge redirect on Intranet Zone</b>	<p>Select to Enable or Disable the redirection of NTLM HTTP challenge on Intranet Zone.</p> <p>Default - Enable</p>
<b>Web Client Settings (iOS and Android)</b>	
<b>Inactivity Time</b>	<p>Specify the inactivity time in minutes.</p> <p>User Inactivity timeout is the inactive/idle time in minutes after which user will be logged out and has to re-authenticate.</p> <p>Inactivity Time Range (Minutes): 6 – 1440</p> <p>Default – 6 minutes</p>

<b>Data Transfer Threshold</b>	<p>Specify the minimum data to be transferred.</p> <p>If the minimum data is not transferred within the specified time, the user will be marked as inactive.</p> <p>Default Value – 1024 Bytes</p>
<b>SSO using radius accounting request</b>	
<b>Radius Client IPv4</b>	<p>Specify IPv4 Address of Radius Client.</p> <p>Only request from specified IP Address will be considered for SSO.</p>
<b>Shared Secret</b>	Provide Shared Secret for authentication.
<b>Show Shared Secret</b>	Click Show to view the configured Shared Secret.
<b>Captive Portal Settings</b>	
<b>Unauthenticated users redirection</b>	<p>Select "Yes" to redirect the access request of unauthenticated user either to the Captive Portal or Custom Message page.</p> <p>Select "No" to display "Access Denied" message to unauthorized user.</p>
<b>Unauthenticated users settings</b>	<p>Configure where the unauthenticated user access requests should be redirected.</p> <p>Select Captive Portal, if an unauthenticated user access request is to be forwarded to captive portal.</p> <p><b>HTTPS Redirection</b></p> <ul style="list-style-type: none"> <li>• Enable to provide access of the Captive portal page through secure channel.</li> </ul> <p><b>My Account Link</b></p> <ul style="list-style-type: none"> <li>• Enable/Disable to make the "My Account" link available on the Captive Portal page.</li> <li>• Default – Enable</li> </ul> <p><b>URL Redirection after Login</b></p> <ul style="list-style-type: none"> <li>• Enable to redirect request to the user requested page or custom page. If request is to be redirected to the custom page, click Custom URL and specify URL.</li> </ul> <p><b>Preserve captive portal after login</b></p> <ul style="list-style-type: none"> <li>• Select "Yes" to minimize the captive portal popup, once the user is successfully authenticated.</li> <li>• Selecting "No" lets the Captive Portal to be displayed on system screen after successful authentication.</li> </ul>

	<p><b>Keep Alive Request For Captive Portal</b></p> <ul style="list-style-type: none"><li>• Keep-Alive request is constantly exchanged between the Appliance and user to check whether user has logged out or is idle. If the Appliance does not receive the response, user is logged out automatically.</li><li>• More number of concurrent HTTP Captive Portal users, more number of keep-alive requests. In case of more concurrent HTTP Captive Portal users we recommend to disable it.</li><li>• Default – Enable</li><li>• If disabled, user is logged out after the configured inactivity time. If disabled, specify user inactivity time and data transfer threshold.</li></ul> <p><b>User Inactivity Timeout</b></p> <ul style="list-style-type: none"><li>• User Inactivity timeout is the inactive/idle time in minutes after which user will be logged out and has to re-authenticate.</li><li>• Enable and specify timeout duration in minutes.</li><li>• Acceptable Range - 3 to 1440 minutes.</li><li>• Default - Disable</li></ul> <p><b>Data Transfer Threshold</b></p> <ul style="list-style-type: none"><li>• Specify threshold value in Bytes for Data Transfer.</li><li>• If the minimum data is not transferred within the specified time, the user will be marked as inactive.</li><li>• Select Custom Message, unauthenticated user is to be displayed custom message.</li></ul> <p><b>Windows Corporate Client Download Link</b></p> <ul style="list-style-type: none"><li>• Enable to publish a link to download the Windows Corporate Client in the custom message.</li></ul> <p><b>Linux Corporate Client Download Link</b></p> <ul style="list-style-type: none"><li>• Enable to publish a link to download the Linux Corporate Client in the custom message.</li></ul> <p><b>MAC Corporate Client Download Link</b></p> <ul style="list-style-type: none"><li>• Enable to publish a link to download the MAC Corporate Client in the custom message.</li></ul>
--	---

	<p><b>Page Header Image</b></p> <ul style="list-style-type: none"><li>• Display the default image shipped with the Appliance at the top of the custom message page or use Browse and upload the custom image.</li><li>• Supported Image format - JPG, PNG or GIF</li><li>• Size - 700 X 80 pixels</li></ul> <p><b>Page Footer Image</b></p> <ul style="list-style-type: none"><li>• Display the default image shipped with the Appliance at the bottom of the custom message page or use Browse and upload the custom image.</li><li>• Supported Image format - JPG, PNG or GIF</li><li>• Size - 700 X 80 pixels</li></ul> <p><b>Custom Message</b></p> <ul style="list-style-type: none"><li>• Specify message. You can customize the message to include client IP Address, category, and URL.</li><li>• Enable Blink Custom Message to display blinking message.</li></ul> <p><b>Preview</b></p> <ul style="list-style-type: none"><li>• Preview and check how message will be displayed before saving the configuration.</li></ul>
--	---

**Table – Firewall Authentication screen elements**



## Configuring Authentication for VPN Traffic

To configure and manage authentication settings for VPN, go to **Identity > Authentication > VPN**.

**VPN (IPSec/L2TP/PPTP) Authentication Methods**

Set Authentication Methods Same As Firewall

Authentication Server List	Selected Authentication Server
<input type="text" value="Search"/> <input checked="" type="checkbox"/> Local	<input checked="" type="checkbox"/> Local

List order indicates priority

---

**SSL VPN Authentication Methods**

Same as VPN  
 Same as Firewall  
 Set Authentication Method for SSL VPN

Authentication Server List	Selected Authentication Server
<input type="text" value="Search"/> <input checked="" type="checkbox"/> Local	<input checked="" type="checkbox"/> Local

List order indicates priority

---

**Single Sign On For VPN Users**

Enable Single Sign On For

IPSec Users  
 L2TP Users  
 PPTP Users  
 SSL VPN Users

**Screen – VPN authentication screen**

### Parameters

Screen Element	Description
VPN (IPSec/L2TP/PPTP) Authentication Methods	
<b>Set Authentication Methods Same As Firewall</b>	<p>Enable to use the same authentication method as configured for firewall traffic. If enabled all the authentication servers configured for the firewall traffic will be available for VPN traffic authentication configuration.</p> <p>Authentication Server List displays all the configured servers while “Selected Authentication Server” List displays servers that will be used for authentication when user tries to login.</p>

	<p>Override authentication method for VPN traffic by selecting or deselecting any Authentication server.</p> <p>In case of multiple servers, authentication request will be forwarded as per the order configured in the Selected Authentication server List.</p> <p>If RADIUS server authenticates users then PPTP and L2TP connections established using MSCHAPv2 or CHAP protocol can be authenticated through RADIUS.</p>
<b>SSL VPN Authentication Methods</b>	
	<p>Enable to use the same authentication method as configured for VPN or Firewall or configure authentication server for SSL VPN.</p> <p>Authentication Server List displays all the configured servers while “Selected Authentication server” list displays servers that will be used for authentication when user tries to login.</p> <p>Override authentication method for SSL VPN traffic by selecting or deselecting any Authentication server.</p> <p>In case of multiple servers, authentication request will be forwarded as per the order configured in the Selected Authentication server List.</p>
<b>Single Sign On For VPN Users</b>	
<b>Enable Single Sign On For</b>	<p>Click to enable Single Sign On for VPN users.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>IPSec Users</b></li> <li>• <b>L2TP Users</b></li> <li>• <b>PPTP Users</b></li> <li>• <b>SSL VPN Users</b></li> </ul> <p>If enabled, the user will not need to re-authenticate in Cyberoam after VPN connection is established. Also, the user will be automatically logged out from Cyberoam when VPN tunnel is disconnected.</p>

Table – VPN Authentication screen elements

## Configuring Authentication for Admin Traffic

The Administrator can configure and manage authentication settings for all the Administrator users except for the Super Administrator from this page.

To configure and manage authentication settings for all the Administrator user except for the global Super Administrator “admin” , go to **Identity > Authentication > Admin**.

Screen – Administrator Authentication screen

Screen Element	Description
Administrator Authentication Methods	
<b>Set Authentication Methods Same As Firewall</b>	<p>Enable to use the same authentication method as configured for firewall traffic. If enabled all the authentication servers configured for the firewall traffic will be available for administrator traffic authentication configuration.</p> <p>The Authentication Server List displays all the configured servers while Selected Authentication Server list displays servers that will be used for authentication when user tries to login.</p> <p>Override authentication method for VPN traffic by selecting or deselecting any Authentication server.</p> <p>In case of multiple servers, authentication request will be forwarded as per the order configured in the Selected Authentication server List.</p>

Table – Administrator Authentication settings page screen elements

## User Groups

Group is a collection of users having common policies that can be managed as a single unit and a mechanism of assigning various policies to a number of users in one operation/step. Users that belong to a particular group are referred to as a group user.

Instead of attaching individual policies to the user, create group of policies and simply assign the appropriate Group to the user and user will automatically inherit all the policies added to the group which simplifies the user configuration.

A group can contain default as well as custom policies.












Various policies that can be grouped are:

- Surfing Quota policy which specifies the duration of surfing time and the period of subscription
- Access Time policy which specifies the time period during which the user will be allowed access
- Web Filter Policy which controls and blocks access to inappropriate web sites
- Application Filter Policy which controlling access to application like IM and P2P, VOIP
- QoS policy which specifies the bandwidth usage limit of the user
- Data Transfer Policy which specifies the data transfer quota of the user
- SSL VPN Policy which determines the access mode and controls access to private network resources.

### Manage User Group list

The Groups page displays the list of all the default and custom groups and provides option to add new group, update group parameters, add new members to the existing group, viewing user group membership, reorder groups or delete a group. Reordering groups defines the priority of the group in which the user would be added in case the user is a member of multiple groups.

To manage user groups, go to **Identity > Groups > Group**.


<input type="checkbox"/>	Group Name 	Web Filter	Application Filter	QoS	Manage
<input type="checkbox"/>	<a href="#">Open Group</a>	Allow All	Allow All	No Policy	 
<input type="checkbox"/>	<a href="#">Clientless Open Group(C)</a>	Allow All	Allow All	No Policy	 
<input type="checkbox"/>	<a href="#">VPN Group</a>	Allow All	Allow All	No Policy	 
<input type="checkbox"/>	<a href="#">Group1</a>	Allow All	Allow All	No Policy	 
<input type="checkbox"/>	<a href="#">HR</a>	Allow All	Allow All	No Policy	 

Screen – Manage Groups

Screen Element	Description
<b>Group Name</b>	Displays the name of the group.
<b>Web Filter</b>	Displays the Web Filter Policy applied to all the group users.  Point to the policy link to view or edit the policy details.
<b>Application Filter</b>	Displays the Application Filter Policy applied to all the group users.  Point to the policy link to view or edit the policy details.
<b>QoS</b>	Displays the QoS Policy applied to all the group users.  Point to the policy link to view or edit the policy details.
<b>MAC Binding (Not applicable to Clientless Group)</b>	<b>Disable</b> – User MAC Binding disabled for all the group users. <b>Enable</b> – User MAC Binding enabled for all the group users.
<b>Access Time (Not applicable to Clientless Group)</b>	Displays the Access Time Policy applied to all the group users.  Point to the policy link to view or edit the policy details.
<b>Surfing Quota (Not applicable to Clientless Group)</b>	Displays the Surfing Quota Policy applied to all the group users.  Point to the policy link to view or edit the policy details.
<b>PPTP (Not applicable to Clientless Group)</b>	<b>Disable</b> – PPTP access disabled for all the group users. <b>Enable</b> – PPTP access enabled for all the group users.
<b>L2TP (Not applicable to Clientless Group)</b>	<b>Disable</b> – L2TP access disabled for all the group users. <b>Enable</b> – L2TP access enabled for all the group users.
<b>Login Restriction (Not applicable to Clientless Group)</b>	Displays the Login Restriction applied – Any, Selected Nodes or Range.
<b>Data Transfer (Not applicable to Clientless Group)</b>	Displays the Data Transfer Policy applied to all the group users.  Point to the policy link to view or edit the policy details.

Table – Manage Groups screen elements

### Creating a new User Group

To add or edit user group details, go to **Identity > Groups**. Click the Add Button to add a new user group or Edit Icon  to modify the details of the user group.

Group Name\*

Description

Group Type\*

**Policies**

Web Filter\*  ⓘ

Application Filter\*  ⓘ

Surfing Quota\*  ⓘ

Access Time\*  ⓘ

Data Transfer  ⓘ

QoS  ⓘ

SSL VPN\*  ⓘ

Quarantine Digest\*  Enable  Disable

MAC Binding  Enable  Disable

LZTP  Enable  Disable

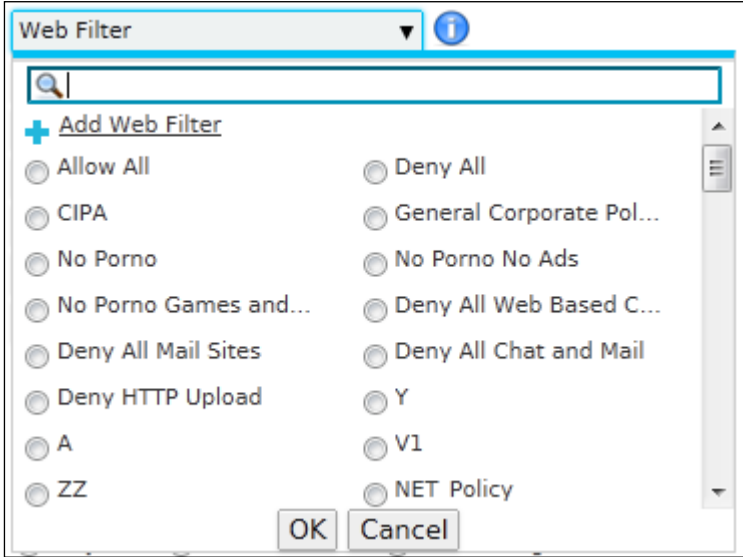
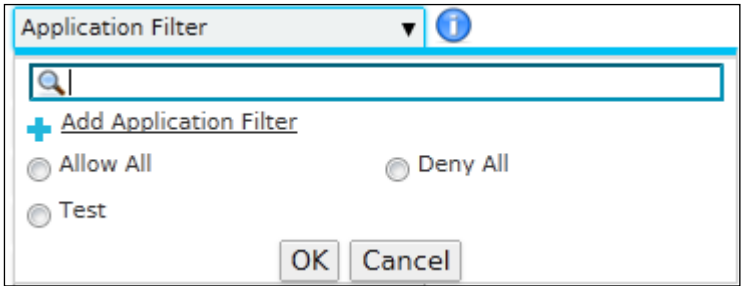
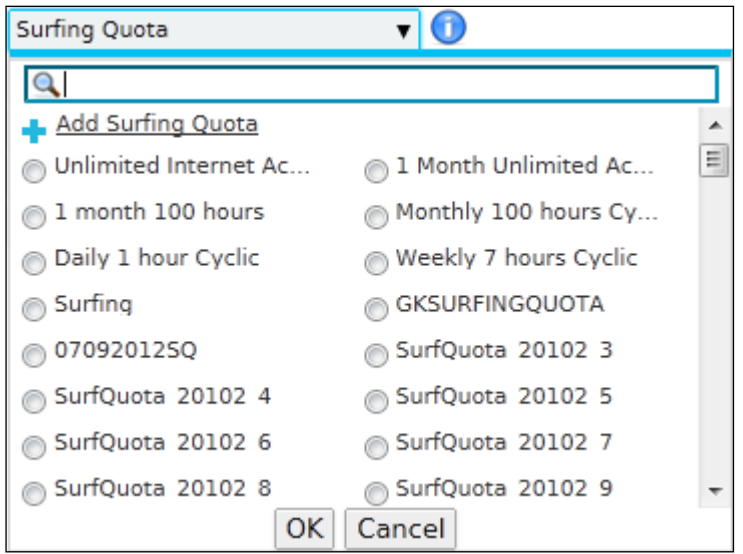
PPTP  Enable  Disable

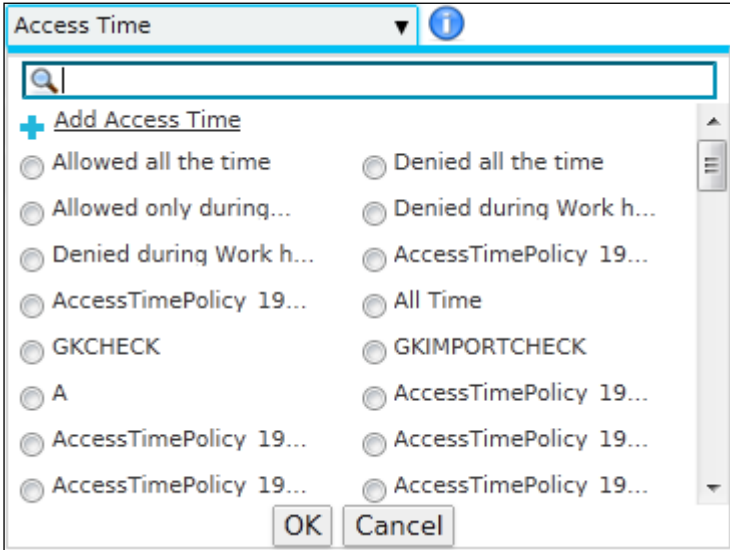
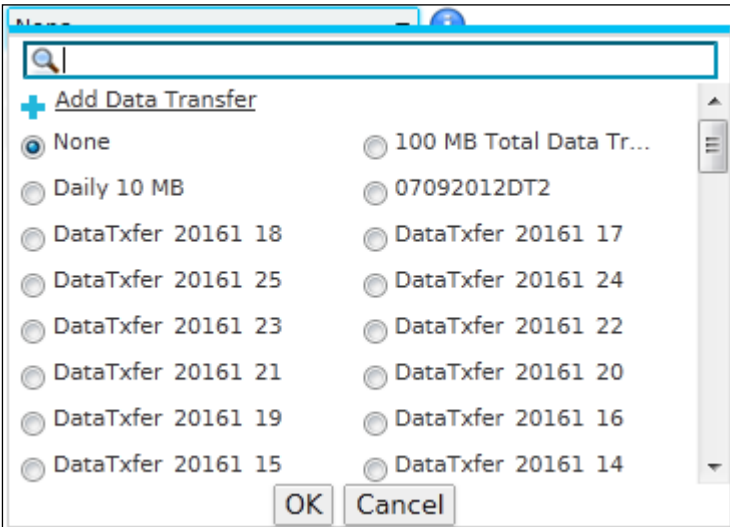
Login Restriction\*  Any Node  Selected Nodes  Node Range

Screen – Add Group

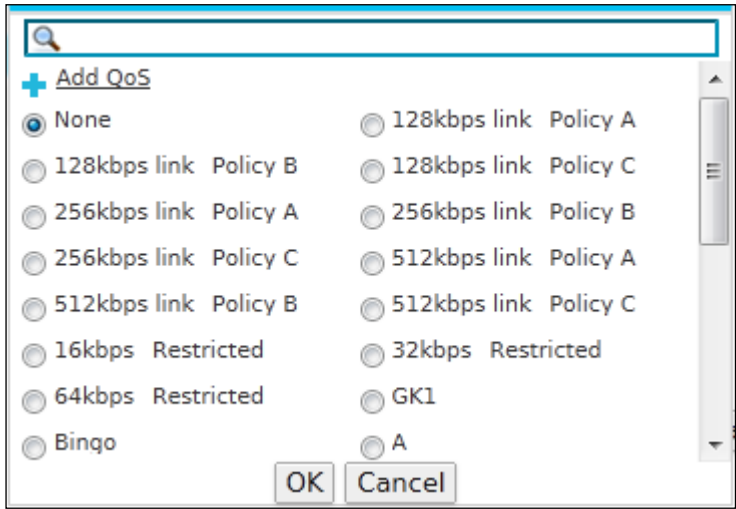
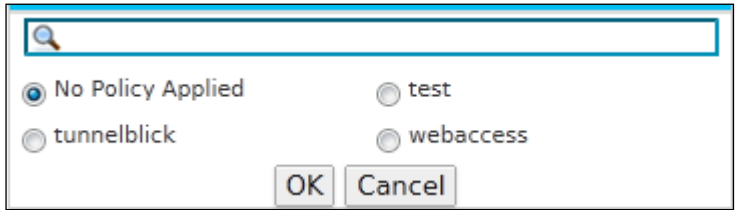
## Parameters

Screen Element	Description
<b>Group Name</b>	Provide a name to identify the group.
<b>Description</b>	Provide group description.
<b>Group Type</b>	Select Group Type.  <b>Available Options:</b> <ul style="list-style-type: none"> <li><b>Normal</b> – User of this group needs to log on using the Appliance Client to access the Internet.</li> <li><b>Clientless</b> – User of this group need to log on using the Appliance Client to access the Internet and is symbolically represented as Group name(C). Access control is placed on the IP Address.</li> </ul>
<b>Policies</b>	
<b>Web Filter</b>	Select the Web Filter Policy from the list.

	 <p>Configured policy will be applicable to all the users who are member of this group.</p>
<b>Application Filter</b>	<p>Select the Application Filter Policy from the list.</p>  <p>Configured policy will be applicable to all the users who are member of this group</p>
<b>Surfing Quota</b>	<p>Select the Surfing Quota Policy from the list.</p> 

	<p><b>Note</b></p> <ul style="list-style-type: none"> <li>Ultimate policy is automatically applied to Clientless Group.</li> </ul>
<p><b>Access Time</b> (Not applicable to Clientless Group)</p>	<p>Select the Access Time Policy from the list.</p>  <p><b>Note</b></p> <ul style="list-style-type: none"> <li>Ultimate policy is automatically applied to Clientless Group.</li> </ul>
<p><b>Data Transfer</b> (Not applicable to Clientless Group)</p>	<p>Select the Data Transfer Policy from the list.</p> 



	Configured policy will be applicable to all the users who are member of this group.
<b>QoS</b>	<p>Select the QoS Policy from the list.</p>  <p>Configured policy will be applicable to all the users who are member of this group.</p>
<b>SSL VPN (Not applicable to Clientless Group)</b>	<p>Select SSL VPN policy from the list.</p>  <p>If user is not to be provided the SSL VPN access then select “No Policy Applied”.</p>
<b>Quarantine Digest</b>	<p>Enable Quarantine Digest. Quarantine Digest is an Email and contains a list of quarantined spam messages filtered by the Appliance and held in the user quarantine area. If configured, the Appliance will mail the Quarantine Digest every day to the user. Digest provides a link to User My Account from where user can access his quarantined messages and take the required action.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Enable</b> – User will receive the Quarantine Digest daily and overrides Group setting.</li> <li>• <b>Disable</b> – User will not receive Quarantine Digest and overrides Group setting.</li> </ul>
<b>MAC Binding (Not applicable to Clientless Group)</b>	<p>Enable/disable “MAC Binding”. By binding User to MAC Address, you are mapping user with a group of MAC Addresses.</p>


<b>L2TP</b> (Not applicable to Clientless Group)	Enable if group users can get access through L2TP connection.
<b>PPTP</b> (Not applicable to Clientless Group)	Enable if group users can get access through PPTP connection.
<b>Login Restriction</b> (Not applicable to Clientless Group)	<p>Select the appropriate option to specify the login restriction for the user group.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Any Node</b> – Select to allow user to login from any of the nodes in the network.</li> <li>• <b>Selected Nodes</b> – Select to allow user to login from the specified nodes only. Specify IP Address and click Add button to add more nodes and remove icon  to delete nodes.</li> <li>• <b>Node Range</b> – Select to allow range of IP Address. Specify IP Address range.</li> </ul>


Table – Add Group screen elements

**Note**

**User configuration – MAC binding and policies is given precedence over Group configuration.**



**Adding Users to the existing Groups**

To add a user to the existing group, follow the below steps:

1. Edit the Group in which you want to add the users by clicking Manage icon  in the Manage column.
2. Click Add Member(s) button. A pop-up Add Group Member appears providing list all the users along their details that can be added in the group. To search user filter the list based on user name and/or current group.
3. Select the user you want to add in the group. You can select a single or multiple users on a single page.
4. Click Apply and click OK to confirm adding member in the group.

**Viewing List of Group Members**

To view group members, follow the below steps:

1. Edit the Group in which you want to add the users by clicking Manage icon  in the Manage column.
2. Click Show Group Member(s) button. A pop-up Group Member appears providing the list all the users with the details who are member of the selected group.
3. Click Close button or Close  icon to close the Group Member pop-up.

## Users

Users are identified by an IP Address or a user name and are assigned to a user group. All the users in a group inherit the policies defined for that group.

Media Access Control (MAC) Address is a unique identifier (hardware address) assigned to a host by the manufacturer for identification and is intended to be immutable. MAC Addresses are 48 bit values that are expressed in 6 byte hex-notation separated by colon for example 01:23:45:67:89:AB.

To improve the security of your network and provide spoofing protection, you can enable User-MAC Address binding. By binding User to MAC Address, you are mapping the user with a group of MAC Addresses. It means a user would be able to login through a group of pre-specified machines only making it more difficult for a hacker using random MAC Addresses or spoofing a MAC Address to gain access to your network.

### User types

The Appliance supports five types of Users:

- Normal
- Clientless
- Single Sign on
- Thin Client User
- WWAN User

Normal User has to log on to the Appliance. Requires client (client.exe) on the User machine or user can use HTTP Client component and all the policy-based restriction are applied.

Clientless does not require client component (client.exe) on the User machines. Symbolically represented as User name (C)

If User is configured for Single sign on, whenever User logs on to Windows, he/she is automatically logged to the Appliance. Symbolically represented as User name (S)

Use the given decision matrix below to choose which type of the user should be created.

Decision matrix for creation of User

Feature	Normal User	Clientless User	Single Sign On User
User Login required	Yes	No	No
Type of Group			
Normal	Yes	No	Yes
Clientless	No	Yes	No
Apply Login restriction	Yes	Yes	Yes
Apply Surfing Quota policy	Yes	No	No

Apply Access Time policy	Yes	No	No
Apply QoS policy	Yes	Yes	Yes
Apply Web Filter Policy	Yes	Yes	Yes
Apply Application Filter policy	Yes	Yes	Yes
Apply Data Transfer policy	Yes	No	Yes

- [Users](#)
- [Clientless Users](#)

## Users

To manage users, go to **Identity > Users > Users**. You can:

- [Import](#)
- Export – Click the “Export” button to download the user details in a csv file. csv file is generated with the following headers: Name, Username, Enc\_password, Email Address, and Group.

## Manage User list

The Users page displays list of all the users added in the Appliance. You can filter the list of users Name, User Name, Group, Web and Application Filter policy applied to the user, and date on which users were added. The page also provides option to add new users manually or by importing user details from the file, exporting user details, purging AD users, changing status of the user, or deleting user.

Total Active User 4 Out of 4											
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Import"/> <input type="button" value="Export"/> <input type="button" value="Change Status"/> <input type="button" value="Purge AD Users"/>											
<span>Select Columns</span> <span>Records Per Page 20</span> <span>&lt;&lt;</span> <span>&lt;</span> <span>(1 of 1)</span> <span>&gt;</span> <span>&gt;&gt;</span>											
<input type="checkbox"/>	User Id	Name	User Name	Type	Profile	Group	Status	Web Filter	Application Filter	Manage	
<input type="checkbox"/>	262	Elitecore	admin1	User	-	Open Group	Active	Allow All	Allow All		
<input type="checkbox"/>	3	cyberoam	cyberoam	Administrator	Administrator	Open Group	Active	Allow All	Allow All		
<input type="checkbox"/>	265	John Smith	john.smith	User	-	Open Group	Active	AllowSpecificY	Allow All		
<input type="checkbox"/>	8	marie	marie	Administrator	Administrator	VPN Group	Active	Allow All	Allow All		

Screen – Manage Users


Screen Element	Description
<b>Import Button</b>	<p>Browse and select a .csv file to import all the user details.</p> <p>Format of .csv File</p> <ul style="list-style-type: none"> <li>• First row of the csv file must be the header row, divided into following fields separated by comma (“,”)</li> <li>• Username - Compulsory field</li> <li>• Password - Optional field</li> <li>• Name - Optional field</li> <li>• Group Name - Optional field</li> <li>• Email ID - Optional field</li> </ul>

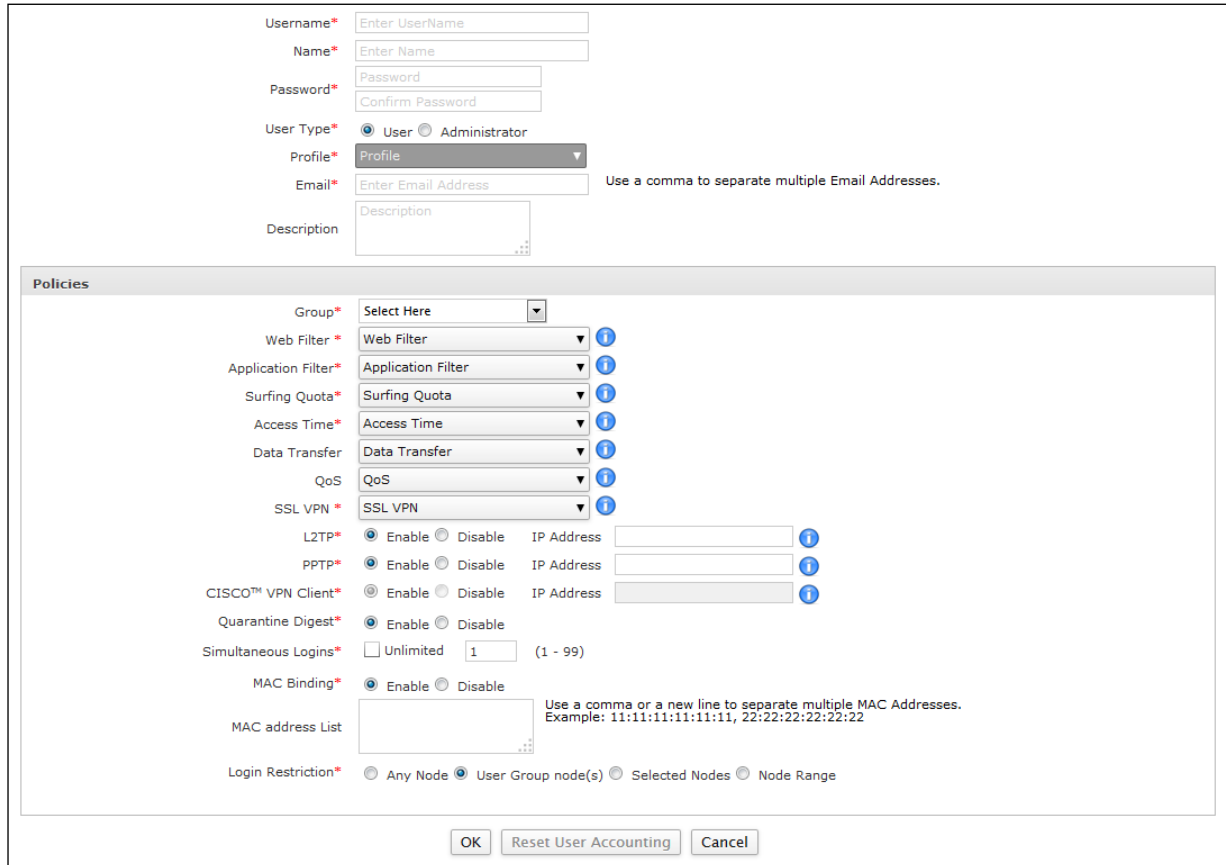
	<ul style="list-style-type: none"> <li>• The remaining rows are values corresponding to the header fields.</li> <li>• Number of fields in each row must be same as those within the header row.</li> <li>• An error message is displayed, if data is missing for any field within the header.</li> <li>• If a Password field is not included in the header, then the field will be set same as that of the Username.</li> <li>• If a Name field is not included in the header, then the field will be set same as that of the Username.</li> <li>• If a Group Name field is not included in the header, then it can be configured by the Administrator during the migration.</li> <li>• All the blank rows will be ignored.</li> </ul>
<b>Export Button</b>	Click to export all the user details.
<b>Change Status</b>	Click to change the status of the user from Active to Inactive and vice-versa.
<b>Purge AD Users</b>	<p>Click to purge and sync Appliance Active Directory users with external Active Directory server.</p> <p>Purge operation will not interrupt user login/logout and accounting events.</p> <p>User details are deleted from both, the Primary Appliance as well as Auxiliary Appliance at the same time.</p>
<b>User ID</b>	Displays a unique ID for the user.
<b>Name</b>	Displays name of the user.
<b>User Name</b>	Specify a unique username to identify the user.
<b>Type</b>	Type of User selected – User or Administrator.
<b>Profile</b>	Profile applied to the Administrator if the User Type is Administrator.
<b>Group</b>	<p>Name of the user group.</p> <p>Point to the group link to view or edit the group details.</p>
<b>Status</b>	<p>Status of the User.</p> <p><b>Inactive</b> – Inactive user.</p> <p><b>Active</b> – Active user.</p>
<b>Web Filter</b>	Web Filter Policy applied to the user.

	Point to the policy link to view or edit the policy details.
<b>Application Filter</b>	Application Filter Policy applied to the user.  Point to the policy link to view or edit the policy details.
<b>QoS</b>	QoS Policy applied to the user.  Point to the policy link to view or edit the policy details.
<b>L2TP</b>	<b>Disable</b> – L2TP access disabled for the user. <b>Enable</b> – L2TP access enabled for the user.
<b>PPTP</b>	<b>Disable</b> – PPTP access disabled for the user. <b>Enable</b> – PPTP access enabled for the user.
<b>MAC Address</b>	MAC Address list.
<b>Data Transfer</b>	Data Transfer Policy applied to the user.  Point to the policy link to view or edit the policy details.
<b>MAC Binding</b>	<b>Disable</b> – User MAC Binding disabled. <b>Enable</b> – User MAC Binding enabled.
<b>Access Time</b>	Access Time Policy applied to the user.  Point to the policy link to view or edit the policy details.
<b>Surfing Quota</b>	Surfing Quota Policy applied to the user.  Point to the policy link to view or edit the policy details.
<b>Login Restriction</b>	Login Restriction applied – Any, User Group Nodes, Selected Nodes or Range.
<b>Created Date</b>	Creation date of the user.
<b>Simultaneous Logins</b>	Simultaneous Logins allowed to the user.

Table – Manage Users screen elements

## Adding a new User

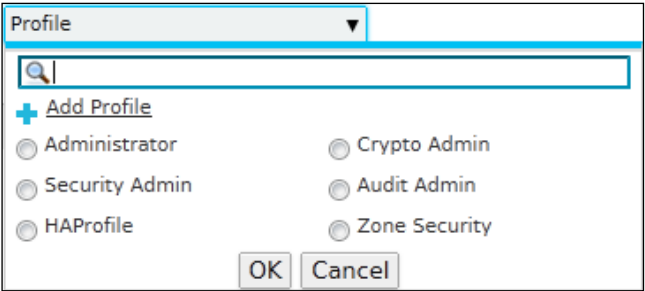
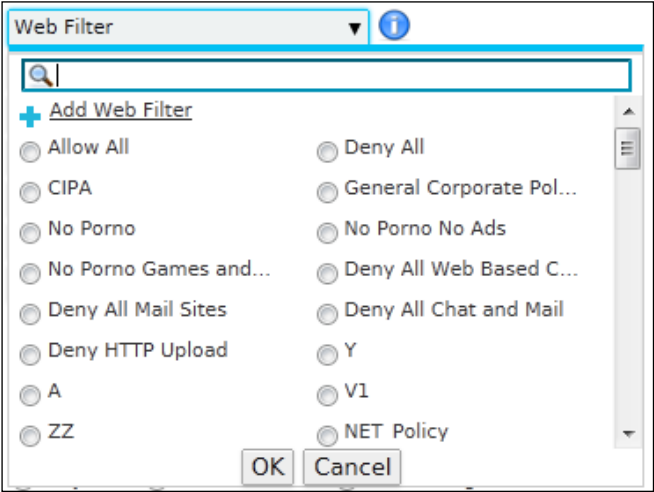
To add or edit user details, go to **Identity > User > User**. Click Add Button to register a new user. To update the details, click on the username or Edit icon  in the Manage column against the user you want to modify.



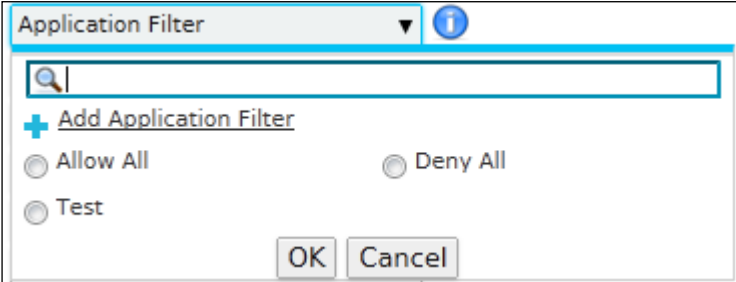
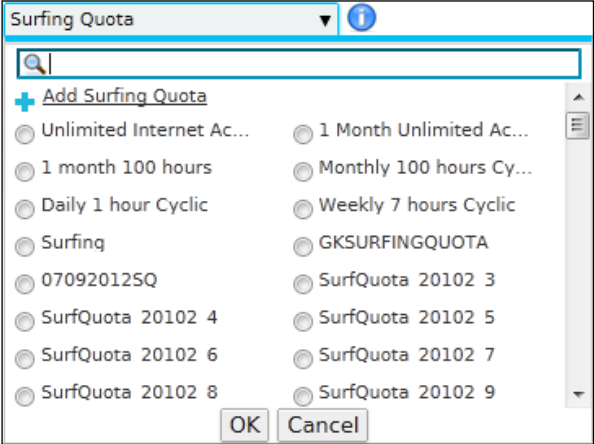
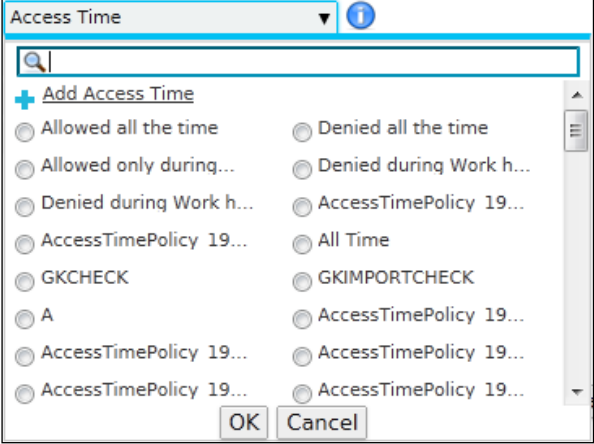
Screen – Add User

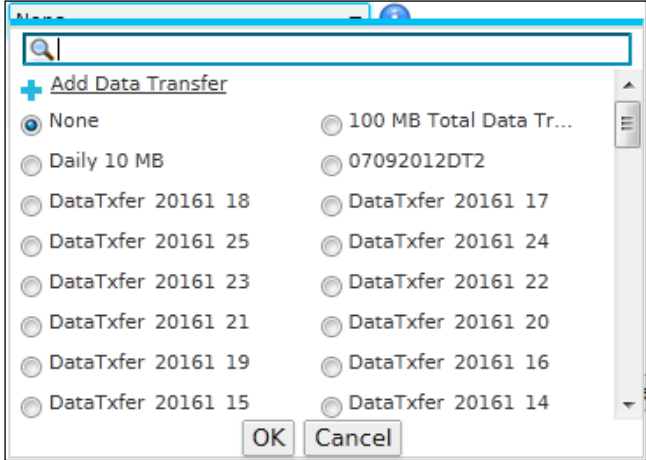
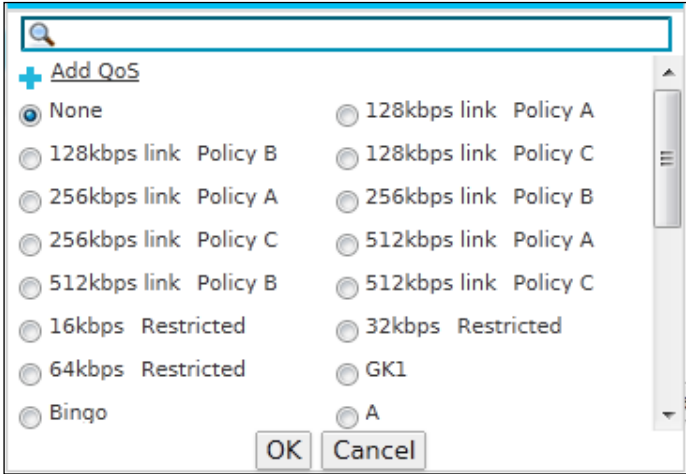
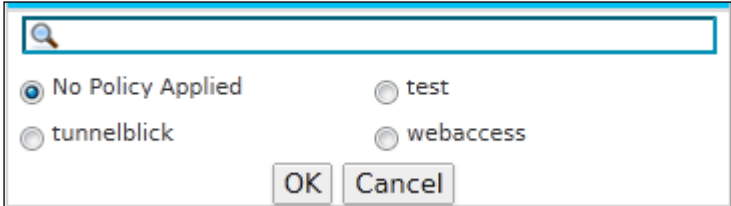
## Parameters

Screen Element	Description
<b>Username</b>	Provide username, which uniquely identifies user and will be used for login.
<b>Name</b>	Provide a Name of the User.
<b>Password</b>	Enter password and re-enter same password for confirmation. Password is case sensitive.
<b>User Type</b>	Select the type of user from the available options.  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• <b>User</b></li> <li>• <b>Administrator</b></li> </ul>
<b>Profile (Only when the User Type)</b>	Select the Administrator Profile. Administrator will get access of various Web Admin Console menus as per the configured profile.

<p><b>“Administrator” is selected)</b></p>	 <p>Create a new profile directly from this page or from the Profile page.</p>
<p><b>Email</b></p>	<p>Specify Email Address of the user.</p> <p>Use comma to separate multiple Email Addresses.</p>
<p><b>Description</b></p>	<p>Provide user description.</p>
<p><b>Policies</b></p>	
<p><b>Group</b></p>	<p>Select Group in which the user is to be added. User will inherit all the policies assigned to the group.</p>
<p><b>Web Filter</b></p>	<p>By default, user will inherit its group policy. To override the group policy, select the policy from the list.</p>  <p>You can create also a new policy directly from this page itself or from <b>Web Filter &gt; Policy</b> page.</p>
<p><b>Application Filter</b></p>	<p>By default, the user will inherit its group policy. To override the group policy, select the policy from the list.</p>



	 <p>You can create also a new policy directly from this page itself or from <b>Application Filter &gt; Policy</b> page.</p>
<p><b>Surfing Quota</b></p>	<p>By default, user will inherit its group policy. To override the group policy, select the policy from the list.</p>  <p>You can create also a new policy directly from this page itself or from <b>Identity &gt; Policy &gt; Surfing Quota</b> page.</p>
<p><b>Access Time</b></p>	<p>By default, user will inherit its group policy. To override the group policy, select the policy from the list</p>  <p>You can create also a new policy directly from this page itself or from <b>Identity &gt; Policy &gt; Access Time</b> page.</p>

<p><b>Data Transfer</b></p>	<p>By default, user will inherit its group policy. To override the group policy, select the policy from the list.</p>  <p>You can create also a new policy directly from this page itself or from Identity &gt; Policy &gt; Data Transfer page.</p>
<p><b>QoS</b></p>	<p>By default, user will inherit its group policy. To override the group policy, select the policy from the list.</p>  <p>You can create also a new policy directly from this page itself or from QoS &gt; Policy page.</p>
<p><b>SSL VPN</b></p>	<p>By default, user will inherit its group policy. To override the group policy, select the policy from the list.</p> 

	<ul style="list-style-type: none"> <li>You can create also a new policy directly from this page itself or from SSL VPN &gt; SSL &gt; Policy page.</li> <li>If user is not to be provided the SSL VPN access then select “No Policy Applied”.</li> </ul>
<b>L2TP</b>	<p>By default, user is provided remote access through L2TP. Disable if remote access is not to be provided to the user.</p> <p>Provide the IP Address (IPv4 / IPv6) to be leased to the user for L2TP access.</p>
<b>PPTP</b>	<p>By default, user is provided remote access through PPTP. Disable if remote access is not to be provided to the user.</p> <ul style="list-style-type: none"> <li>Provide the IP Address (IPv4 / IPv6) to be leased to the user for PPTP access.</li> </ul>
<b>CISCO™ VPN Client</b>	<p>By default, user is provided remote access through CISCO VPN Client. Disable if remote access is not to be provided to the user.</p> <p>Provide the IP Address (IPv4/IPv6) to be leased to the user for CISCO VPN access.</p> <ul style="list-style-type: none"> <li>Note: To use this feature, CISCO™ VPN Client needs to be configured from VPN &gt; CISCO™ VPN Client.</li> </ul>
<b>Quarantine Digest</b>	<p>Configure Quarantine Digest.</p> <p>Quarantine digest is an Email containing a list of quarantined spam messages filtered by the Appliance and held in the user quarantine area. If configured, Appliance will mail the digest at the configured frequency to the user. Digest also provides a link to User My Account from where user can access and take the action quarantined messages.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li><b>Enable</b> – User receives the spam digest daily and overrides Group setting.</li> <li><b>Disable</b> – User does not receive a spam digest and overrides Group setting.</li> </ul>
<b>Simultaneous Logins</b>	<p>Specify number of concurrent logins that will be allowed to user OR Click ‘Unlimited’ for allowing unlimited Concurrent logins.</p> <p>Default - 1</p> <p>Acceptable Range - 1 to 99</p> <p>The specified setting overrides the global setting specified in the client preferences.</p>

<p><b>MAC Binding</b></p>	<p>Enable/disable “MAC Binding”. By binding User to MAC Address, you are mapping user with a group of MAC Addresses.</p> <p>If enabled, specify MAC Addresses for example 01:23:45:67:89:AB.</p> <p>Once you enable MAC binding, user will be able to login through pre-specified machines only.</p> <p>To configure multiple MAC Addresses use comma. For example 01:23:45:67:89:AB, 01:23:45:67:89:AC</p>
<p><b>Login Restriction</b></p>	<p>Select the appropriate option to specify the login restriction for the user.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Any Node</b> – User will be able to login from any of the nodes in the network.</li> <li>• <b>User Group Node(s)</b> – User will be able to login only from the nodes assigned to her group.</li> <li>• <b>Selected Nodes</b> – User will be able to login from the specified nodes only.</li> <li>• <b>Node Range</b> – User will be able to login from any of the IP Address from the configured range.</li> </ul>
<p><b>Administrator Advanced Settings (Only if User Type is selected as “Administrator”)</b></p>	
<p><b>Schedule for Appliance Access</b></p>	<p>Schedule the Appliance access.</p> <p>Administrator will be able to access the Appliance only during the time configured in schedule.</p>
<p><b>Login Restriction for Appliance Access</b></p>	<p>Select the appropriate option to specify the login restriction for the user.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Any Node</b> – Administrator will be able to login from any of the nodes in the network.</li> <li>• <b>Selected Nodes</b> – Administrator will be able to login from the specified nodes only.</li> <li>• <b>Node Range</b> – Administrator will be able to login from any of the IP Address from the configured range</li> </ul>
<p><b>Reset User Accounting (Displayed only after user is added)</b></p>	<p>Click to reset the usage accounting i.e. internet usage time and data transfer of the user.</p>
<p><b>View Usage (Displayed only after user is added)</b></p>	<p>Click to view the Internet usage and data transfer usage.</p>

**Table – Add User screen elements**

**Note**

- User configuration is given precedence over Group configuration.

## Import Users' Information

Instead of creating users again in the Appliance, if you already have users detail in a csv file, you can upload csv file.

Click the Import Button to import csv file. Select the complete path for migrating user's information file.

.csv file format and processing:

1. Header (first) row should contain field names. Format of header row:
2. Compulsory field: username
3. Optional fields: password, name, group, Email Address
  - Fields can be configured in any order.
  - Subsequent rows should contain values corresponding to the each field in header row
  - Number of fields in each row should be same as in the header row
  - Error will be displayed if data is not provided for any field specified in the header
  - Blank rows will be ignored
  - If password field is not included in the header row then it will set same as username
  - If group name is not included in the header row, administrator will be able to configure group at the time of migration

## Purging Active Directory (AD) Users

Click Purge AD Users button to synchronize the Appliance's Active Directory users with external Active Directory server.

**Note**

- Purge operation will not interrupt user login/logout and accounting events.
- If HA is configured, user details are deleted from both, the Primary Appliance as well as Auxiliary Appliance at the same time.
- To successfully initialize Purging of AD Users, the Appliance should be connected/authenticated to/by at least one (or more) one or more AD servers.

## Exporting Users

Click the Export button to export the user details in a csv file. csv file is generated with the following headers: Name, Username, Enc\_password, Email Address, and Group.

## Clientless Users

Clientless Users are the users who can bypass Client login to access the Internet and are managed by the Appliance itself. As clientless users can bypass Appliance login, create clientless users when your network has few Non-windows machines, VOIP boxes, or servers.

### Manage Clientless User list

The page displays the list of all the clientless users. You can filter the list based on name or username of the user, IP address, group of the user, web and application filter policy, or created date. The page also provides option to add a single clientless user or multiple users, delete or change status of the user. The administrator can also reset user accounting data or view the usage statistics.

To manage Clientless users, go to **Identity > User > Clientless User**.

ID	Name	User Name	IP Address	Group	Status	Manage
5	1.1.1.1	<a href="#">1.1.1.1</a>	1.1.1.1	Clientless Open Group	Active	
17	1.1.1.10	<a href="#">1.1.1.10</a>	1.1.1.10	Clientless Open Group	Active	
111	1.1.1.104	<a href="#">1.1.1.104</a>	1.1.1.104	Clientless Open Group	Inactive	
114	1.1.1.107	<a href="#">1.1.1.107</a>	1.1.1.107	Clientless Open Group	Inactive	
115	1.1.1.108	<a href="#">1.1.1.108</a>	1.1.1.108	Clientless Open Group	Inactive	
117	1.1.1.110	<a href="#">1.1.1.110</a>	1.1.1.110	Clientless Open Group	Inactive	

Screen – Manage Clientless Users

Screen Element	Description
<b>Add Range</b>	Click to add the range of IP Address for Clientless User.
<b>Change Status</b>	Click to change the status of clientless user from active to inactive and vice-versa.
<b>ID</b>	Displays the User ID for a Clientless User.
<b>Name</b>	Displays the name of the user.
<b>User Name</b>	Unique username to identify the User.
<b>IP Address</b>	Displays the IP Address of Clientless user – IPv4 or IPv6.
<b>Group</b>	Displays Group to which user belongs.
<b>Status</b>	Status of the Clientless User: <b>Inactive</b> – Inactive user. <b>Active</b> – Active user.
<b>Web filter</b>	Web Filter policy applied to the traffic.  Point to the policy link to view or edit the policy details.
<b>Application filter</b>	Application filter policy applied to the traffic.

	Point to the policy link to view or edit the policy details.
<b>QoS</b>	QoS policy applied to the traffic.  Point to the policy link to view or edit the policy details.

Table – Manage Clientless Users screen elements

### Clientless User Parameters



To add or edit Clientless user details, go to **Identity > Users > Clientless Users**. Click Add Button to register a new clientless user or Edit Icon to modify the details of the clientless user.

<b>Username</b>	<b>IP Address</b>	<b>Group</b>	<b>Name</b>	<b>Email</b>	<b>Quarantine Digest</b>	+
<input type="text"/>	<input type="text"/>	Clientless Open Gro	<input type="text"/>	<input type="text"/>	Apply Group's Settin	-
<input type="button" value="OK"/> <input type="button" value="Cancel"/>						

Screen – Add Clientless User

### Parameters


Screen Element	Description
<b>Username</b>	Specify username, which uniquely identifies user and will be used for login.
<b>IP Address</b>	Specify IP Address (IPv4/IPv6) for the Clientless user.
<b>Group</b>	Select Group in which user is to be added. User will inherit all the policies assigned to the group.  Change the policies applied to the user by editing the user details.
<b>Name</b>	Provide a name of the User.
<b>Email</b>	Provide an Email Address.

<b>Quarantine Digest</b>	<p>Configure Quarantine Digest. Quarantine digest is an Email and contains a list of quarantined spam messages filtered by the Appliance and held in the user quarantine area. If configured, Appliance will mail the spam digest every day to the user. Digest provides a link to User My Account from where user can access his quarantined messages and take the required action.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Enable</b> – User will receive the spam digest daily and overrides Group setting.</li> <li>• <b>Disable</b> – User will not receive spam digest and overrides Group setting.</li> <li>• <b>Apply Group's Settings</b> - User will receive Spam Digests as per configured for the Group user belongs to.</li> </ul>
<b>Add Icon</b>	Click the Add  Icon to add a new Clientless User.
<b>Remove Icon</b>	Click the Remove  Icon to delete a Clientless User

**Table – Add Clientless User screen elements**

You can change the policies applied to the user by updating the user details. If you change the policies for the user, user specific policies will take precedence over user group policies. Refer to Change Policies Parameters to change the policies.

### Change Policies Parameters

To change the policies applied to the clientless user, go to **Identity > Users > Clientless Users** and click Edit icon  against the user whose policies are to be changed.

Username\* john

Name\*

IP Address\*


Group\*  ▼


Email \*


Internet Usage Time 00:00 (HH:MM)

---

**Policies**

Web Filter\*  ▼ 

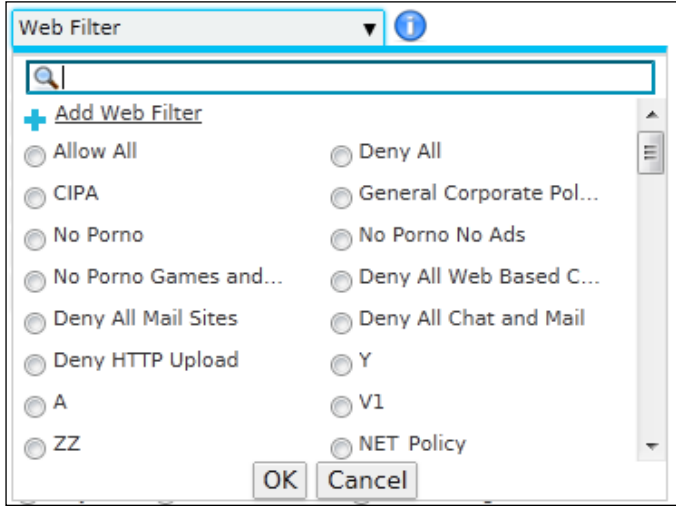
Application Filter\*  ▼ 

QoS  ▼ 

Quarantine Digest\*  Enable  Disable

**Screen – Add Clientless User (Change Policies)**



Screen Element	Description
<b>Username</b>	Name with which user logs on.
<b>Name</b>	Name of the User.
<b>IP Address</b>	IP Address from which user logs on.
<b>Group</b>	Group in which the user is added. User will inherit all the policies assigned to the group.  Change the group, if required.
<b>Email</b>	Email ID of the user.
<b>Internet Usage Time</b>	Displays total Internet usage time information.
<b>Policies</b>	
<b>Web Filter</b>	<p>Web filter policy applied to the user.</p> <p>Change the policy, if required.</p> <p>Policy applied here will take the precedence over the group policy.</p> 
<b>Application filter</b>	<p>Application filter policy applied to the user.</p> <p>Change the policy, if required.</p> <p>Policy applied here will take the precedence over the group policy.</p>

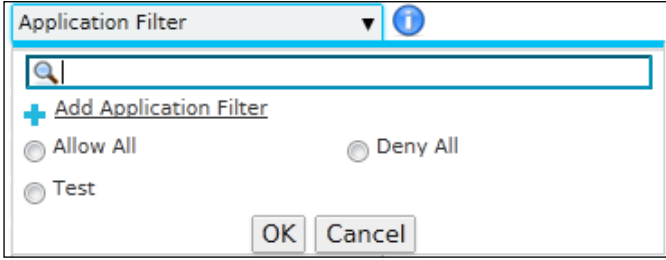
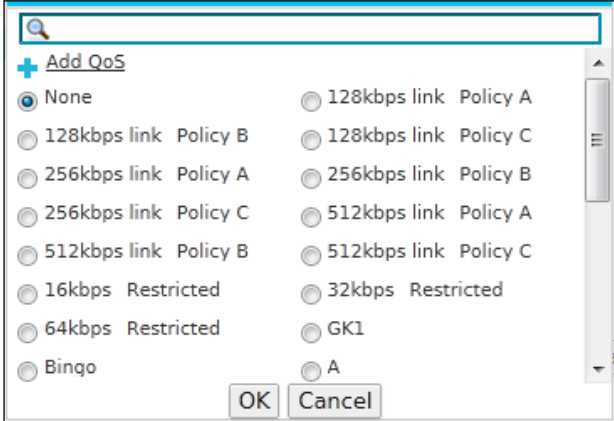
	
<p><b>QoS</b></p>	<p>QoS Policy applied to the user.</p> <p>Change the policy, if required.</p> <p>Policy applied here will take the precedence over the group policy.</p> 
<p><b>Quarantine Digest</b></p>	<p>Configure Quarantine Digest. Quarantine digest is an Email and contains a list of quarantined spam messages filtered by the Appliance and held in the user quarantine area. If configured, Appliance will mail the spam digest every day to the user. Digest provides a link to User My Account from where user can access his quarantined messages and take the required action.</p> <p><b>Available Options:</b></p> <p><b>Enable – User will receive the spam digest daily and overrides Group setting.</b></p> <p><b>Disable – User will not receive spam digest and overrides Group setting.</b></p>
<p><b>Reset User Accounting</b> (Displayed only after user is added)</p>	<p>Click to reset the usage accounting i.e. internet usage time and data transfer of the user.</p>
<p><b>View Usage</b> (Displayed only after user is added)</p>	<p>Click to view the Internet usage and data transfer usage.</p>

Table – Edit Clientless User screen elements

## Add Multiple Clientless Users

To add multiple Clientless users, go to **Identity > Users > Clientless Users** and click Add Range button to configure following parameters:

The screenshot shows a dialog box with the following elements:

- From\***: A text input field containing the placeholder text "Enter IP Address".
- To\***: A text input field containing the placeholder text "Enter IP Address".
- Group\***: A dropdown menu with "Clientless Open Group" selected.
- Buttons**: "OK" and "Cancel" buttons at the bottom left.

**Screen – Add Multiple Clientless User**

Screen Element	Description
<b>From</b>	Specify Starting IP Address for the range.
<b>To</b>	Specify Ending IP Address for the range.
<b>Group</b>	<p>Select Group for users. Users will inherit all the policies assigned to the group.</p> <p>You can change the policies applied to the user by editing the user details. If you change the policies for the user, user specific policies will take precedence over user group policies. Refer to Change Policies Parameters to change the policies.</p>

**Table – Add Multiple Clientless User screen elements**

## Guest Users

Users without a pre-existing user account wanting to access internet using a hotspot, or via a network available at airport, hotels, hostels, etc. are called “Guest Users”. These users, that are otherwise considered unauthenticated and/or denied access, are allowed to make request to connect to the Internet for a limited period by authenticating themselves. On being authenticated, these users are authorized to access internet using as a Guest Users. At such locations, Internet access is secured by configuring access policies to restrict any malicious use of the network.

Cyberoam allows the Administrator to pre-configure single or multiple Guest Users using Web Admin Console. The credentials of Guest Users configured via Web Admin Console can be printed and handed over to Guest User. Alternately, Guest Users can register themselves using Guest User Portal. The credentials and Internet access details of Guest Users registered via Guest User Portal can either be sent via SMS or can be printed.

In case of successful authentication Guest User is granted access according to applicable group, else is be redirected captive portal page.

- [General Settings](#)
- [Guest Users](#)
- [SMS Gateway](#)

## General Settings

The page allows configuring general parameters to provide secured internet access for guest user

To configure General Settings, go to **Identity > Guest Users > General Settings**.

### Guest User General Settings

Username Prefix\*

Group\*

Password Length

Password Complexity

Disclaimer

Auto Purge on Expiry

### Guest User Registration Settings

Enable Guest Users Registration

SMS Gateway\*

Guest Username\*  Use Cell Number as Username

User Validity (Duration in Days)\*

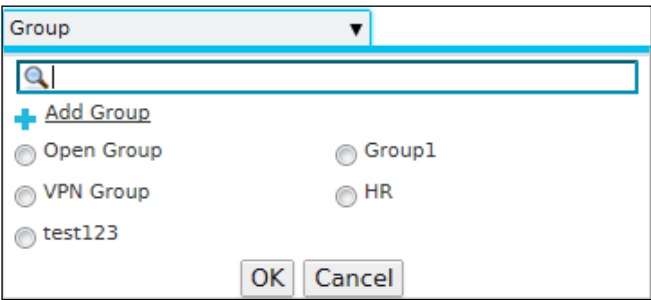
Default Country Code

CAPTCHA Verification  Enable

Note: Guest user will be authenticated locally.

**Screen – Manage Guest User General Settings**

## Parameters

Screen Element	Description
<b>Guest User General Settings</b>	
<b>Username Prefix</b>	Provide prefix to be used for Auto-Generation of username for guest users.
<b>Group</b>	<p>Select a group of policies to assign to Guest users.</p>  <p>Alternately, you can also add group of policies.</p>
<b>Password Length</b>	<p>Specify the length of the auto-generated password for Guest Users.</p> <p>Minimum password length: 3 characters  Maximum password length: 60 characters  Default password length: 8 characters</p> <p>The password length is a basic security parameter, the value of which affects the strength of password against brute force attack..</p>
<b>Password Complexity</b>	<p>Select a type of password from the available options to be used for complexity of an auto-generated password:</p> <p>Available Options:</p> <ul style="list-style-type: none"> <li>• <b>Numeric Password</b> – Password will include only numeric characters.</li> <li>• <b>Alphabetic Password</b> – Password will include only alphabetic characters.</li> <li>• <b>Alphanumeric Password</b> – Password will include numeric as well as alphabetic characters.</li> <li>• <b>Alphanumeric with Special Character Password</b> – Password will include numeric, alphabets and special characters.</li> </ul> <p>The password strength is a function of its length and complexity. Combining password length with password complexity makes a password difficult to guess.</p>


<b>Disclaimer</b>	<p>Provide the disclaimer message to be printed below every user's login credentials.</p> <div style="border: 1px solid gray; padding: 5px; background-color: #f0f0f0;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>Disclaimer once configured can be edited but cannot be removed.</li> </ul> </div>
<b>Auto Purge on Expiry</b>	<p>Check to enable automatic purging of user details on expiry of user validity.</p> <div style="border: 1px solid gray; padding: 5px; background-color: #f0f0f0;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>Details of a user who is bound to rules (like Firewall, IM, etc) does not get purged automatically.</li> </ul> </div>
<b>Guest User Registration Settings</b>	
<b>Enable Guest Users Registration</b>	<p>Enable to allow secured Internet access to guest users. Rest of the options in this field can only be configured after you have selected this option.</p>
<b>SMS Gateway</b>	<p>Select the Gateway using which the SMS should be sent.</p> <div style="border: 1px solid gray; padding: 10px; background-color: #f0f0f0;"> <p>SMS Gateway <span style="float: right;">▼</span></p> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;"> <input type="text"/> </div> <p>+ <a href="#">Add Gateway</a></p> <p><input type="radio"/> Turkcell <span style="margin-left: 100px;"><input type="radio"/> Sms GUPSHUP</span></p> <p><input type="radio"/> Netcore</p> <p style="text-align: right;"><input type="button" value="OK"/> <input type="button" value="Cancel"/></p> </div> <p>Alternately you may add the SMS gateway from "SMS Gateway" tab.</p>
<b>Guest Username</b>	<p>Select the method of generating Username using the following options:</p> <ul style="list-style-type: none"> <li>Use Cell Number as Username</li> <li></li> </ul> <p>If the option is not selected then new username will be generated with the value specified in Username Prefix.</p>
<b>User Validity (Duration in Days)</b>	<p>Specify guest user validity period in days.</p>
<b>Default Country Code</b>	<p>Enable to configure a default country code on the Guest User Registration page.</p> <p>Selected country is displayed as default option in Cell Number selection at Guest User registration page.</p>
<b>CAPTCHA Verification</b>	<p>Select to Enable or Disable CAPTCHA (Completely Automated Public Turing Test To Tell Computers and Humans Apart) code verification on Guest User Registration page to ensure the request is received for human being.</p>

	<p>By enabling CAPTCHA Verification, the user will be displayed a picture with characters that user must insert in a provided textbox below picture. The administrator can therefore protect Cyberoam against attacks generated by automated programs.</p> <p>Default - Enable</p>
--	--

**Table – Manage Guest User General Setting screen elements**

## Manage Guest Users

To manage Guest Users, go to **Identity > Guest Users > Guest Users**. You can:

- [Add Single Guest User](#) – Click “Add Single” button to add a single Guest User.
- [Add Multiple Guest Users](#) – Click “Add Multiple” button to add multiple Guest Users.
- Resend Credential – Click the Resend Credential icon  in the Manage column against a User registered via Guest User Portal to whom the access detail's SMS are to be resent.

The page displays the list of all the guest users added. You can filter the list based on name or username of the user, cell number of the user, validity of the user account, Email address of the user, web or application filter policy, or group of the user. The page also provides option to add single or multiple users, distributing credentials for the Internet access, update user parameters, view or reset the data transfer usage.

<input type="checkbox"/>	Name	User Name	Cell Phone Number	Create Date	Valid From	Validity	Expiry Date
<input type="checkbox"/>	john	9100001	-	17-09-2013	17-09-2013	1 day(s)	18-09-2013

Screen – Manage Guest Users

Screen Element	Description
<b>Print Button</b>	Click to Print the credentials of the selected Guest User(s).
<b>Name</b>	Name of Guest User.
<b>User Name</b>	Username of the Guest User.
<b>Cell Phone Number</b>	Cell Phone Number of the Guest User.
<b>Create Date</b>	Date on which the Guest User was created.
<b>Valid From</b>	Date on which the Guest User was created.
<b>Validity</b>	Duration till which the Guest User remains active.
<b>Expiry Date</b>	Date at which the user gets expired.
<b>Web Filter</b>	Web Filter Policy applied to the user.  Point to the policy link to view or edit the policy details.
<b>Data Transfer</b>	Data Transfer Policy applied to the user.  Point to the policy link to view or edit the policy details.
<b>MAC Address</b>	MAC Address list.
<b>Quarantine Digest</b>	<b>Disable</b> – Quarantine Digest disabled for the user. <b>Enable</b> – Quarantine Digest enabled for the user.
<b>SSL VPN</b>	SSL VPN Policy applied to the user.  Point to the policy link to view or edit the policy details.



<b>Email Address</b>	Email Address of the user.
<b>Application Filter</b>	Application Filter Policy applied to the user.  Point to the policy link to view or edit the policy details.
<b>QoS</b>	QoS Policy applied to the user.  Point to the policy link to view or edit the policy details.
<b>Access Time</b>	Access Time Policy applied to the user.  Point to the policy link to view or edit the policy details.
<b>L2TP</b>	<b>Disable</b> – L2TP access disabled for the user. <b>Enable</b> – L2TP access enabled for the user.
<b>MAC Binding</b>	<b>Disable</b> – User MAC Binding disabled. <b>Enable</b> – User MAC Binding enabled.
<b>Login Restriction</b>	Login Restriction applied – Any, User Group Nodes, Selected Nodes or Range.
<b>Surfing Quota</b>	Surfing Quota Policy applied to the user.  Point to the policy link to view or edit the policy details.
<b>PPTP</b>	<b>Disable</b> – PPTP access disabled for the user. <b>Enable</b> – PPTP access enabled for the user.
<b>Status</b>	Status of the User.  <b>Inactive</b> – Inactive user. <b>Active</b> – Active user.
<b>Group</b>	Name of the user group.  Point to the group link to view or edit the group details.

Table – Manage Guest User screen elements

## Registering Single Guest User Parameters

To add a single Guest User, go to **Identity > Guest Users > Guest Users**. Click “Add Single” button to add the details of a single Guest User.

Screen – Add Single Guest User Parameters

Screen Element	Description
<b>Username</b>	Auto-Generated password.
<b>Password</b>	Auto-Generated password.
<b>Name</b>	Specify name of the Guest User.
<b>Email</b>	Specify Email Address of the Guest User.
<b>User Validity (Duration in Days)</b>	Specify the validity of a Guest User in days.
<b>Validity Start</b>	Select the type when a user's validity should begin.  Available Options: <ul style="list-style-type: none"> <li>• <b>Immediately</b> – Validity is counted from the time a Guest User is created.</li> <li>• <b>After First Login</b> – Validity is counted from the time after a Guest User logs into the network for the first time.</li> </ul>
<b>Add</b>	Click to add a Guest User.
<b>Add and Print</b>	Navigates to a printable HTML page which contains user Internet Access Credentials. Click the Print command to simultaneously Print and Add the Guest User.
<b>Export</b>	Click to download guest user list.

Table – Add Single Guest User screen elements

## Registering Multiple Guest User Parameters

To add multiple Guest Users, go to **Identity > Guest Users > Guest Users**. Click “Add Multiple” button to add the details of multiple Guest Users.

Screen – Add Multiple Guest User Parameters

Screen Element	Description
<b>Number of Users</b>	Specify the number of Guest Users to be created.
<b>User Validity (Duration in Days)</b>	Specify the validity of multiple Guest Users in days.
<b>Validity Start</b>	Select the type from when a user's validity should be counted.  Available Options: <ul style="list-style-type: none"> <li>• <b>Immediately</b> – Validity is counted from the time a Guest User is created.</li> <li>• <b>After First Login</b> – Validity is counted from the time after a Guest User logs into the network for the first time.</li> </ul>
<b>Add</b>	Click to add multiple Guest Users.
<b>Add and Print</b>	Navigates to a printable HTML page which contains user Internet Access Credentials. Click the Print command to simultaneously Print and Add the Guest User(s).
<b>Export</b>	Click to download guest user list.

Table – Add Multiple Guest User screen elements

## Registering Guest User(s) through Captive Portal

1. Browse to the Captive Portal using `http://<LAN IP Address assigned to your Appliance>:8090`.
2. Click the hyperlink [Click here to get a username to access the Internet](#).

**Cyberoam Captive Portal**

**Cyberoam**  
www.cyberoam.com

Username

Password

Login

- [Click here for User My Account](#)
- [Click here to get a username to access the Internet](#)

**Note : On closing this window, you will be logged out.**

3. Provide guest user details for registration and click OK button.

**Guest User Registration**

Name\*

Email

Cell Number\*

Enter the mobile number without any prefix e.g. "0", "+"

Enter the text below\*

## Updating Guest User Configuration

To edit user details, go to **Identity > Guest Users > Guest Users**. Click Edit Icon  to modify the details of the user.

### Edit User

Username\* 9100001

Name\*

Password\* \*\*\*\*\* [Change Password](#)

Cell Number\*


Email\*


Internet Usage Time 00:00 (HH:MM)


---


#### Policies


Group\*


Web Filter\*  


Application Filter\*  


Surfing Quota\*  


Access Time\*  

Data Transfer  

QoS  

SSL VPN\*  

L2TP\*  Enable  Disable IP Address  

PPTP\*  Enable  Disable IP Address  

Quarantine Digest\*  Enable  Disable

Simultaneous Logins\*  Unlimited  (1 - 99)

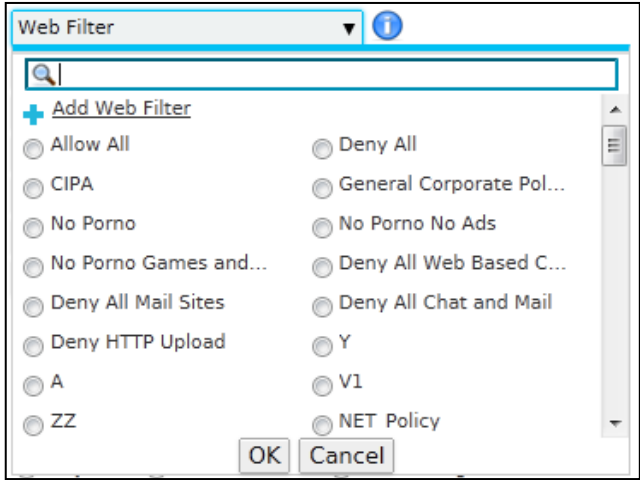
MAC Binding\*  Enable  Disable

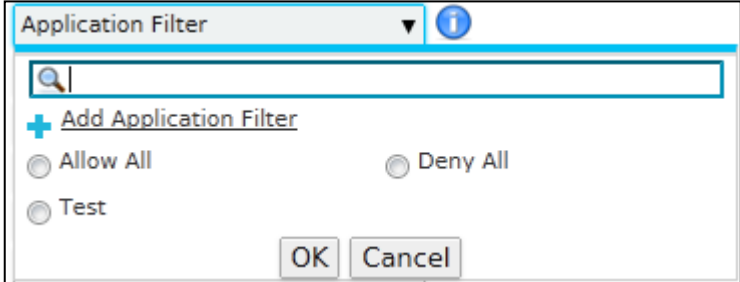
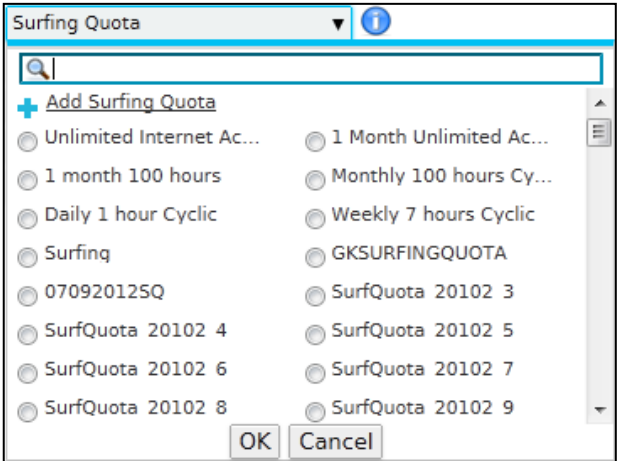
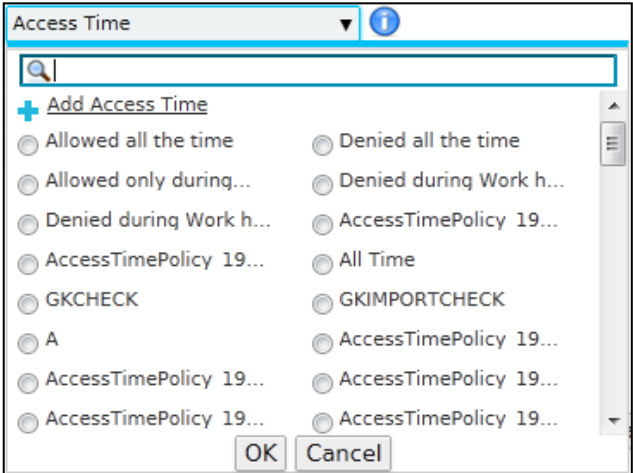
MAC address List  Use comma or newline to separate mac addresses. For Example - 11:11:11:11:11:11,22:22:22:22:22:22

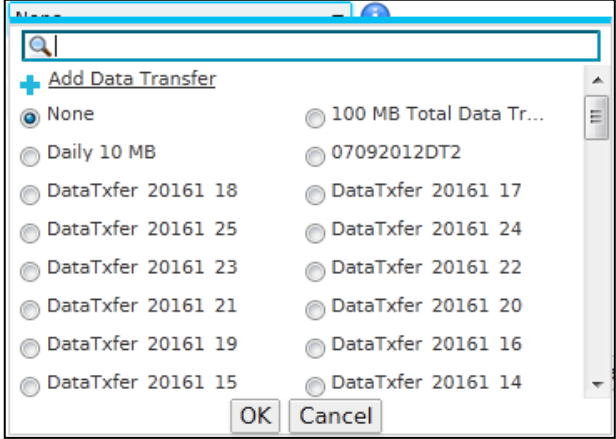
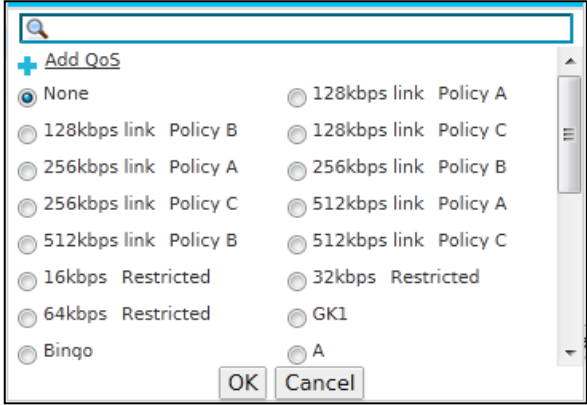
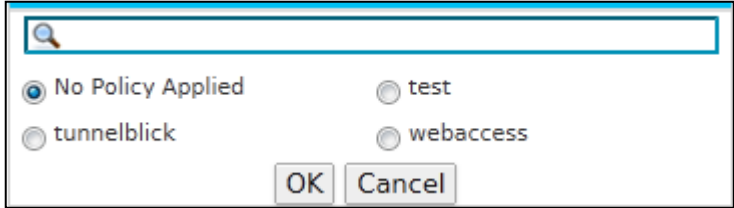
Login Restriction\*  Any Node  User Group node(s)  Selected Nodes  Node

Screen – Edit Guest User Parameters

## Parameters

Screen Element	Description
<b>Username</b>	Displays username of the Guest User.
<b>Name</b>	Provide a name of the Guest User.
<b>Password</b>	Displays the password in encrypted format.  One can also change the password by clicking on “Change Password” link.
<b>Cell Number</b>	Displays Cell phone number.
<b>Email</b>	Provide Email Address of the user.
<b>Internet Usage time</b>	Displays the Internet Usage Time in HH:MM format.
<b>Policies</b>	
<b>Group</b>	Group in which user belongs. User will inherit all the policies assigned to the group.
<b>Web Filter</b>	<p>Select the Web Filter Policy from the list.</p> <p>You can also create a new policy directly from this page itself and attach to the user.</p> 
<b>Application Filter</b>	<p>Select the Application Filter Policy from the list.</p> <p>You can also create a new policy directly from this page itself and attach to the user.</p>

	
<p><b>Surfing Quota</b></p>	<p>Select the Surfing Quota Policy from the list.</p> <p>You can also create a new policy directly from this page itself and attach to the user.</p> 
<p><b>Access Time</b></p>	<p>Select the Access Time Policy from the list.</p> <p>You can also create a new policy directly from this page itself and attach to the user.</p> 

<p><b>Data Transfer</b></p>	<p>Select the Data Transfer Policy from the list.</p> <p>You can also create a new policy directly from this page itself and attach to the user.</p> 
<p><b>QoS</b></p>	<p>Select the QoS Policy from the list.</p> <p>You can also create a new policy directly from this page itself and attach to the user.</p> 
<p><b>SSL VPN</b></p>	<p>Select SSL VPN policy from the list.</p> <p>If user is not to be provided the SSL VPN access then select “No Policy Applied”.</p> 



<b>L2TP</b>	Enable if you want to allow user to get access through L2TP connection.
<b>PPTP</b>	Enable if you want to allow user to get access through PPTP connection.
<b>Quarantine Digest</b>	<p>Configure Quarantine Digest. Quarantine Digest is an Email and contains a list of quarantined spam messages filtered by the Appliance and held in the user quarantine area. If configured, Appliance will mail the Quarantine Digest every day to the user. Digest provides a link to User My Account from where user can access his quarantined messages and take the required action.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Enable</b> – User will receive the Quarantine Digest daily and overrides Group setting.</li> <li>• <b>Disable</b> – User will not receive Quarantine Digest and overrides Group setting.</li> </ul>
<b>Simultaneous Logins</b>	<p>Specify number of concurrent logins that will be allowed to user OR Click 'Unlimited' for allowing unlimited Concurrent logins.</p> <p>The specified setting overrides the global setting specified in the client preferences.</p> <p>Default login allowed – 1 Simultaneous Login Range : 1 to 99</p> <p>Select "Unlimited" to avoid restriction on number of simultaneous logins.</p>
<b>MAC Binding</b>	<p>Enable/disable "MAC Binding". By binding User to MAC Address, you are mapping user with a group of MAC Addresses.</p> <p>Only IPv4 Address must be provided for options Selected Node and Node Range.</p>
<b>MAC Address List</b>	<p>Specify MAC Addresses for example 01:23:45:67:89:AB.</p> <p>Once you enable MAC binding, user will be able to login through pre-specified machines only.</p> <p>To configure multiple MAC Addresses use comma. For example 01:23:45:67:89:AB, 01:23:45:67:89:AC</p>
<b>Login Restriction</b>	<p>Select the appropriate option to specify the login restriction for the user.</p> <p><b>Available Options:</b></p>

	<ul style="list-style-type: none"> <li>• <b>Any Node</b> – User will be able to login from any of the nodes in the network.</li> <li>• <b>User Group Node(s)</b> – User will be able to login only from the nodes assigned to her group.</li> <li>• <b>Selected Nodes</b> – User will be able to login from the specified nodes only.</li> <li>• <b>Node Range</b> – User will be able to login from any of the IP Address from the configured range.</li> </ul>
<b>Reset User Accounting (Displayed only after Guest User is added)</b>	Click to reset the user accounting details.
<b>View Usage (Displayed only after Guest User is added)</b>	Displays the detailed Internet usage.


Table – Guest User Parameter screen elements

Note	
<ul style="list-style-type: none"> <li>• User configuration is given precedence over Group configuration that is, User MAC binding and policies configuration is given priority over Group configuration.</li> </ul>	

### Distributing Access Credentials to Guest Users

Guest Users can be registered from Guest User Portal as well as Web Admin Console.

If the guest user is registered from the Web Admin Console, the login credentials and the Internet access details can be printed and distributed. Option is provided to print the credentials at the time of registering or can be printed later also.

If the guest user is registered from the Guest User Portal, the login credentials and the Internet access details are SMSed on the registered cell phone number or printed and distributed. The administrator can resend the credentials to guest users through SMS by clicking Resend icon  against the Guest User under the Manage column or can also print them.

## SMS Gateway

An SMS Gateway allows sending and receiving Short Service Message (SMS) to/from a home network for Guest User registration. The Appliance supports HTTP and HTTPS protocol based SMS service.

The page displays list of all the configured SMS Gateways and provides option to delete and edit the SMS gateway configuration.

To manage users, go to **Identity > Guest Users > SMS Gateway**.

Add		Delete		
<input type="checkbox"/>	Name	URL	Response Format	Manage
<input type="checkbox"/>	Turkcell	http://api.teknomart.com.tr/direct/	HataKodu={0}&HataAciklama={1}	 
<input type="checkbox"/>	Sms_GUPSHUP	http://enterprise.smsgupshup.com/GatewayAPI/rest	{0} {1} {2}	 

Add Delete


















Screen – SMS Gateway

Screen Element	Description
Name	Displays name of the SMS Gateway.
URL	Displays URL of the SMS Gateway.
Response Format	Displays the Response Format.

Table – SMS Gateway screen elements

## SMS Gateway Parameters

To add SMS Gateway details, go to **Identity > Guest Users > SMS Gateway**. Click Add Button to register a new SMS Gateway.

Name*	<input type="text" value="Enter Name"/>										
URL*	<input type="text" value="Enter URL"/>										
Http Method*	<input type="radio"/> Get <input checked="" type="radio"/> Post										
Cell Number Format*	<input type="checkbox"/> Use Country Code with Cell Number										
Number Prefix	<input type="text"/>										
Request Parameters*	<table border="1"> <thead> <tr> <th>Name</th> <th>Value</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td></td> </tr> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td></td> </tr> </tbody> </table>	Name	Value		<input type="text"/>	<input type="text"/>		<input type="text"/>	<input type="text"/>		
Name	Value										
<input type="text"/>	<input type="text"/>										
<input type="text"/>	<input type="text"/>										
Response Format*	<input type="text" value="Enter Response Format"/>										
Response Parameters*	<table border="1"> <thead> <tr> <th>Parameter Index</th> <th>Name</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td></td> </tr> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td></td> </tr> </tbody> </table>	Parameter Index	Name		<input type="text"/>	<input type="text"/>		<input type="text"/>	<input type="text"/>		
Parameter Index	Name										
<input type="text"/>	<input type="text"/>										
<input type="text"/>	<input type="text"/>										

Test Connection OK Cancel

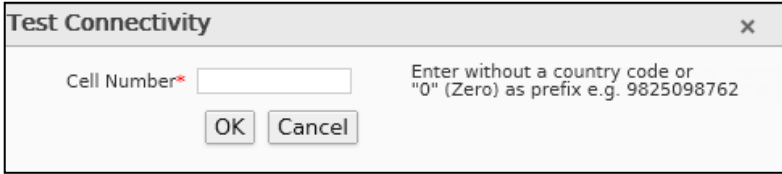
Screen – Add SMS Gateway

Screen Element	Description																										
<b>Name</b>	Specify Name of the SMS Gateway.																										
<b>URL</b>	Specify URL of the SMS Gateway.																										
<b>Http Method</b>	<p>Select the method for sending SMS request to SMS Gateways from the options available:</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Get</b></li> <li>• <b>Post</b></li> </ul>																										
<b>Cell Number Format</b>	Check to use country code with cell number.																										
<b>Number Prefix</b>	<p>Specify the prefix value to be used with the cell number. Number Prefix can include alpha-numeric and ASCII special characters.</p> <p>It can be up to 4 characters long.</p>																										
<b>Request Parameters</b>	<p>Specify the following request parameters to configure the SMS Gateway.</p> <ul style="list-style-type: none"> <li>• <b>Name:</b> Name for the value. Name is a descriptor used to describe the meaning of the value. E.g. username, password, mobile</li> <li>• <b>Value:</b> Value of variables that are defined against name</li> </ul>																										
<div style="border: 1px solid black; padding: 10px;"> <p>Example</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>HTTP://www.beat2day.co.in/sms.aspx?user=joey&amp;pass=joey123&amp;mbno=9876543210&amp;msg=Test Message</p> <table style="margin-left: auto; margin-right: auto; border-collapse: collapse;"> <tr> <td style="text-align: center; padding: 2px;">↑</td> <td style="text-align: center; padding: 2px;">↑</td> <td style="text-align: center; padding: 2px;">↑</td> <td style="text-align: center; padding: 2px;">↑</td> <td style="text-align: center; padding: 2px;">↑</td> <td style="text-align: center; padding: 2px;">↑</td> <td style="text-align: center; padding: 2px;">↑</td> <td style="text-align: center; padding: 2px;">↑</td> </tr> <tr> <td style="text-align: center; padding: 2px;">Name</td> <td style="text-align: center; padding: 2px;">Value</td> <td style="text-align: center; padding: 2px;">Name</td> <td style="text-align: center; padding: 2px;">Value</td> <td style="text-align: center; padding: 2px;">Name</td> <td style="text-align: center; padding: 2px;">Value</td> <td style="text-align: center; padding: 2px;">Name</td> <td style="text-align: center; padding: 2px;">Value</td> </tr> </table> <p style="text-align: center; margin-top: 5px;">Request Format</p> </div> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th style="width: 30%;">Name</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>user</td> <td>joey</td> </tr> <tr> <td>pass</td> <td>joey123</td> </tr> <tr> <td>mbno</td> <td>{mobileno}</td> </tr> <tr> <td>msg</td> <td>{msg}</td> </tr> </tbody> </table> <p style="margin-top: 5px;">Mobile number and message must follow "{mobileno}" and "{msg}" respectively.</p> </div>		↑	↑	↑	↑	↑	↑	↑	↑	Name	Value	Name	Value	Name	Value	Name	Value	Name	Value	user	joey	pass	joey123	mbno	{mobileno}	msg	{msg}
↑	↑	↑	↑	↑	↑	↑	↑																				
Name	Value	Name	Value	Name	Value	Name	Value																				
Name	Value																										
user	joey																										
pass	joey123																										
mbno	{mobileno}																										
msg	{msg}																										
<b>Response Format</b>	<p>Response describes delivery status of the message such as success, failed, limit exceeded. Status message can be in various formats. Few of them are described below:</p> <p>For Example Response Format</p>																										

	<p>{0}   {1}   {2}</p> <p>Response Received success   mbno   msgid/transactionid</p> <p>Response Format &lt;status&gt;500&lt;/status&gt;&lt;transactionid&gt;{0}&lt;/transactionid&gt;&lt;reason&gt;{1}&lt;/reason&gt;</p> <p>Response Received &lt;status&gt;500&lt;/status&gt;&lt;transactionid&gt;2323&lt;/transactionid&gt;&lt;reason&gt;Limit Exceeded&lt;/reason&gt;</p> <p>When the response format is different for success and failure, it is recommended that the response format string should have a single content holder. E.g. {0}</p>
<p><b>Response Parameters</b></p>	<p>Response Parameter is the value presented by content holder {0,1, 2...n} that will be displayed in log viewer.</p> <p>Parameter Index: Parameter Index is the content holder value {0, 1, 2...n}.</p> <p>Name: Name represents the content holder in the Log Viewer.</p> <p>Example 1 0 – Status 1 – Recipient 2 – SMSID</p> <p>Example 2 0 – SMSID – 2323 1 – SMS Status Message – Length Exceeded</p>

**Table – Add SMS Gateway screen elements**

## Testing Connectivity with SMS Gateway



**Screen – Test Connectivity with SMS Gateway**


Once you configure the SMS Gateway, check whether you are able to connect with the gateway or not. Click the Test Connection button and provide cell phone number. You will receive SMS through the gateway configured if you are able to connect to the gateway.

### Changing Status of a User

To change the status of a User go to, **Identity > Users > Users** or **Identity > Users > Clientless Users**. Select the user and click the Change Status button. User Status can be changed from Active to Inactive and vice versa.

### Resetting User Accounting

To reset the User accounting go to, **Identity > Users > Users** or **Identity > Users > Clientless Users** or **Identity > Users > Guest Users** and follow the below steps:


1. Edit the User account of the user whose data accounting you want to reset by clicking Manage icon  in the Manage column.
2. Click Reset User Accounting button and click OK button to confirm.

#### Note

- You cannot reset user accounting for the live user.

### Viewing Internet and Data Transfer Usage of a User

To view Internet and data transfer usage of a user go to, **Identity > Users > Users** or **Identity > Users > Clientless Users** or **Identity > Users > Guest Users** and follow the below steps:

1. Edit the User account of the user whose data usage you want to view by clicking Manage icon  under the Manage column.
2. Click View Usage button.
3. A pop-up displays information of policies applied on the user account, upload and download data transferred by the user.

## Policy

The Appliance allows controlling access to various resources with the help of Policy.

The Appliance allows defining following types of policies:

1. Schedule Internet access for individual users by defining Access time policy. (See [Access time policy](#) for more details)
2. Control individual user surfing time by defining Surfing quota policy. (See [Surfing Quota policy](#) for more details)
3. Limit total as well as individual upload and/or download data transfer by defining data transfer policy. (See [Data transfer policy](#) for more details).

Appliance comes with several predefined policies. These predefined policies are immediately available for use until configured otherwise.

- [Access Time Policy](#)
- [Surfing Quota Policy](#)
- [Data Transfer Policy](#)

## Access Time Policy

Access time is the time period during which user can be allowed/denied Internet access. An example would be “only office hours access” for a certain set of users.

Access time policy enables to set time interval - days and time - for the Internet access with the help of schedules. See Schedules for more details.

A time interval defines days of the week and times of each day of the week when the user will be allowed/denied the Internet access.

Two strategies based on which Access time policy can be defined:















- Allow strategy - By default, allows access during the schedule
- Deny strategy - By default, disallows access during the schedule

Appliance comes with the following predefined policies: Allowed all the time, Denied all the time, Allowed only during Work Hours, Denied during Work hours. These predefined policies are immediately available for use until configured otherwise. You can also define custom policies to define different levels of access for different users to meet your organization’s requirements.

## Manage Access Time Policy list

The Access Time page displays list of all the default as well as custom policies. The page also provides option to add, update, or delete the access time policies.

To manage Access Time Policies, go to **Identity > Policy > Access Time**.

<input type="checkbox"/>	Name	Strategy	Schedule	Description	Manage
<input type="checkbox"/>	<a href="#">AccessTimePolicy_19987_12</a>	Allow	All The Time	Automated	 
<input type="checkbox"/>	<a href="#">AccessTimePolicy_19987_22</a>	Allow	All The Time	Automated	 
<input type="checkbox"/>	<a href="#">AccessTimePolicy_19987_6</a>	Allow	All The Time	Automated	 
<input type="checkbox"/>	<a href="#">AccessTimePolicy_19987_10</a>	Allow	All The Time	Automated	 
<input type="checkbox"/>	<a href="#">AccessTimePolicy_19987_21</a>	Allow	All The Time	Automated	 
<input type="checkbox"/>	<a href="#">AccessTimePolicy_19987_4</a>	Allow	All The Time	Automated	 
<input type="checkbox"/>	<a href="#">Allowed only during Work Hours</a>	Allow	Work hours (5 Day week)	Allow log on access to Cyberoam only during Work	 

Screen – Manage Access Time Policy


Screen Element	Description
<b>Name</b>	Displays the name for the Policy.
<b>Strategy</b>	Displays the Type of Strategy selected: Allow or Deny.

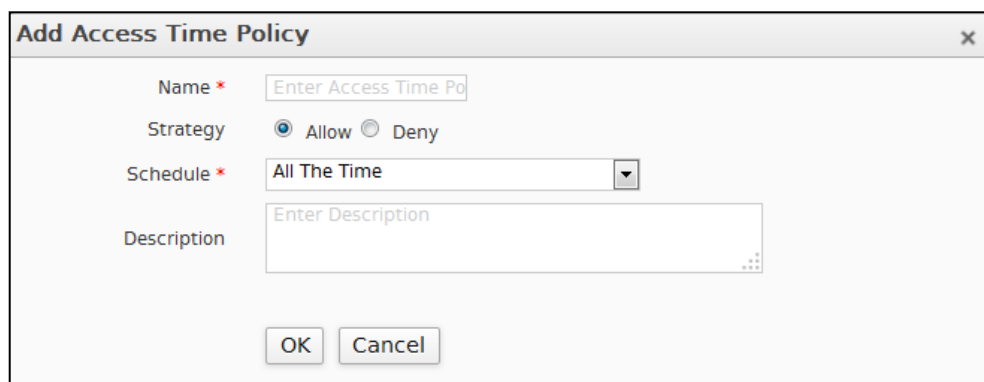


<b>Schedule</b>	Displays the Type of Schedule selected.
<b>Description</b>	Policy Description.

Table – Manage Access Time Policies screen elements

### Access Time Policy Parameters

To add or edit an access time policy, go to **Identity > Policy > Access Time**. Click the Add button to add a new policy. To update the details, click on the policy or Edit icon  in the Manage column against the policy you want to modify.



Screen – Add Access Time Policy

Screen Element	Description
<b>Name</b>	Provide a Name to identify the Policy.
<b>Strategy</b>	Specify strategy to be applied during the scheduled time interval.  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• <b>Allow</b> – Allows the Internet access during the scheduled time interval.</li> <li>• <b>Deny</b> – Does not allow the Internet access during the scheduled time interval.</li> </ul>
<b>Schedule</b>	Select Schedule. Only Recurring schedule can be applied.  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• <b>All The Time</b></li> <li>• <b>Work hours (5 Day Week)</b></li> <li>• <b>Work hours (6 Day week)</b></li> <li>• <b>All Time on Weekdays</b></li> <li>• <b>All Time on Weekends</b></li> <li>• <b>All Time on Sunday</b></li> <li>• <b>All Days 10:00 to 19:00</b></li> </ul>

---

	Depending on the policy strategy, access will be allowed/denied for the scheduled time interval.
<b>Description</b>	Provide Policy Description.

**Table – Add Access Time Policy screen elements**

Note

- A change made in a policy becomes effective immediately on saving the changes.

## Surfing Quota Policy

Surfing quota policy defines the duration of Internet surfing time. Surfing time duration is the allowed time in hours for a Group or an Individual User to access Internet.

Surfing Quota Policy:















- Allows allocating Internet access time on a cyclic or non-cyclic basis.
- Single policy can be applied to number of Groups or Users.

The Appliance comes with the following predefined policies: Unlimited Internet Access, 1 Month Unlimited Access, 1 month 100 hours, Monthly 100 hours Cyclic, Daily 1 hour Cyclic, Weekly 7 hours Cyclic. These predefined policies are immediately available for use until configured otherwise. You can also define custom policies to define different levels of access for different users to meet your organization's requirements.

### Manage Surfing Quota Policy list

The Surfing Quota page displays list of all the default as well as custom policies. The page also provides option to add, update, or delete surfing quota policies.

To manage surfing quota policies, go to **Identity > Policy > Surfing Quota**.


<input type="checkbox"/>	Name	Time allowed (HH)	Validity	Cycle Type	Cycle Time	Description	Manage
<input type="checkbox"/>	<a href="#">SurfQuota_6095_33</a>	Unlimited	Unlimited	DAILY	1:00		 
<input type="checkbox"/>	<a href="#">SurfQuota_6095_34</a>	Unlimited	Unlimited	DAILY	1:00		 
<input type="checkbox"/>	<a href="#">SurfQuota_20102_3</a>	Unlimited	Unlimited	DAILY	1:00		 
<input type="checkbox"/>	<a href="#">SurfQuota_6095_35</a>	Unlimited	Unlimited	DAILY	1:00		 
<input type="checkbox"/>	<a href="#">SurfQuota_5936_29</a>	Unlimited	Unlimited	DAILY	1:00		 
<input type="checkbox"/>	<a href="#">SurfQuota_5936_28</a>	Unlimited	Unlimited	DAILY	1:00		 
<input type="checkbox"/>	<a href="#">SurfQuota_20102_10</a>	Unlimited	Unlimited	DAILY	1:00		 

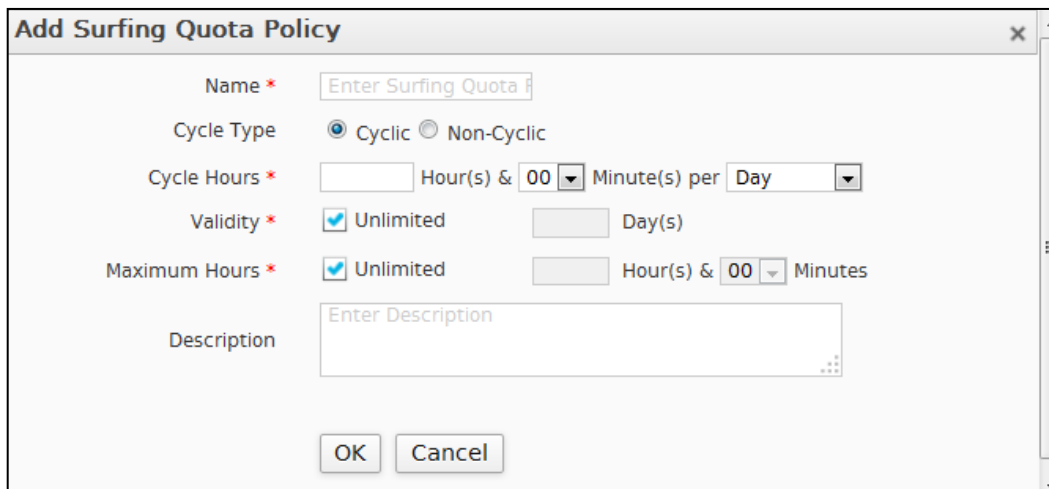
Screen – Manage Surfing Quota Policy

Screen Element	Description
<b>Name</b>	Displays the name for the Policy.
<b>Time Allowed (HH)</b>	Maximum Time in a day for which the policy remains active.
<b>Validity</b>	Specify the time period in day(s) for which the policy remains active.
<b>Cycle Type</b>	Displays the Type of Cycle: Cyclic or Non-Cyclic.
<b>Cycle Time</b>	Displays the Hours for which the cycle is active.
<b>Description</b>	Policy Description.

Table – Manage Surfing Quota Policies screen elements

## Surfing Quota Policy Parameters

To add or edit a surfing quota policy, go to **Identity > Policy > Surfing Quota**. Click the Add button to add a new policy. To update the details, click on the policy or Edit icon  in the Manage column against the policy you want to modify.



Screen – Add Surfing Quota Policy

Screen Element	Description
<b>Name</b>	Specify name to identify the Policy. Duplicate names are not allowed.
<b>Cycle Type</b>	Select Cycle type.  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• <b>Cyclic</b> – Restricts surfing hours up to cycle hours defined on predefined time duration.</li> <li>• <b>Non-Cyclic</b> – Surfing hour restriction is defined by total allotted days and time.</li> </ul>
<b>Cycle Hours</b>	Specify Cycle Hours. Cycle hours define the upper limit of surfing hours for cyclic types of policies i.e. Daily, Weekly, Monthly and Yearly.  At the end of each Cycle, cycle hours are reset to zero i.e. for "Weekly" Cycle type, cycle hours will to reset to zero every week even if cycle hours are unused.
<b>Validity</b>	Specify Validity in number of days. Validity defines the upper limit of total surfing days allowed i.e. restricts total surfing days to valid allotted days.  OR Click Unlimited Days, if you do not want to restrict the total surfing days.
<b>Maximum Hours</b>	Specify Maximum Hours. Maximum hours define the upper limit of total surfing hours allowed i.e. restricts total surfing hours to maximum hours.

---

	OR Click Unlimited Hours, if you do not want to restrict the total surfing hours.
<b>Description</b>	Provide description for Surfing Quota Policy.

**Table – Add Surfing Quota Policy screen elements**

## Data Transfer Policy

Once the user logs on, the bandwidth is available and the total available bandwidth is shared amongst all the active users at the particular time. Bandwidth being a limited resource, its shortage and congestion problems are common. Appliance allows limiting data transfer allowed to individual user according to the requirement. Bandwidth is limited using the Bandwidth policy while data transfer policy defines the upper limit for data transfer carried out by the user.

Data transfer policy:

- Allows limiting data transfer on a cyclic or non-cyclic basis.
- Single policy can be applied to number of Groups or Users.

Data transfer restriction can be based on:

- Total Data transfer (Upload + Download)
- Individual Upload and/or Download

The Appliance comes with the following predefined policies: 100 MB Total Data Transfer policy, Daily 10 MB. These predefined policies are immediately available for use until configured otherwise. You can also define custom policies to define different levels of access for different users to meet your organization's requirements.

## Manage Data Transfer Policy list

To manage data transfer policies, go to **Identity > Policy > Data Transfer**.


	Name	Cycle Type	Absolute Limit (MB)			Cycle Limit (MB)			Manage
			Up	Down	Total	Up	Down	Total	
<input type="checkbox"/>	DataTxfer_20161_11	DAILY	-	-	Unlimited	-	-	1	
<input type="checkbox"/>	DataTxfer_20161_12	DAILY	-	-	Unlimited	-	-	1	
<input type="checkbox"/>	DataTxfer_20161_13	DAILY	-	-	Unlimited	-	-	1	
<input type="checkbox"/>	DataTxfer_20161_21	DAILY	-	-	Unlimited	-	-	1	
<input type="checkbox"/>	DataTxfer_20161_22	DAILY	-	-	Unlimited	-	-	1	

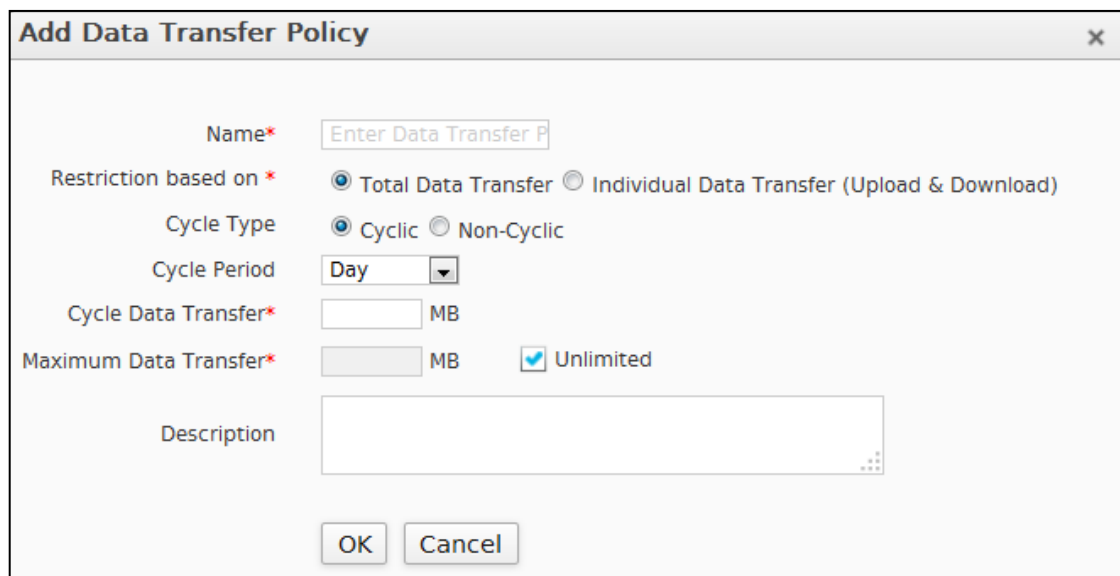
Screen – Manage Data Transfer Policy

Screen Element	Description
<b>Name</b>	Displays the name for the Policy.
<b>Cycle Type</b>	Displays the Type of Cycle: Cyclic or Non-Cyclic.
<b>Absolute Limit (MB)</b>	Absolute Data transfer limit in MB including upload, download and total data transfer.
<b>Cycle Limit (MB)</b>	Cyclic Data transfer limit in MB including upload, download and total data transfer.

Table – Manage Data Transfer Policies screen elements

## Data Transfer Policy Parameters

To add or edit a data transfer policy, go to **Identity > Policy > Data Transfer**. Click the Add button to add a new policy. To update the details, click on the policy or Edit icon  in the Manage column against the policy you want to modify.



Screen – Add Data Transfer Policy

Screen Element	Description
<b>Name</b>	Name to identify the Policy. Duplicate names are not allowed.
<b>Restriction Based On</b>	Specify whether the data transfer restriction is on total data transfer or on individual data transfer (upload and download).
<b>Cycle Type</b>	Select Cycle type.  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• <b>Cyclic</b> – Restricts surfing hours up to cycle hours defined on predefined time duration.</li> <li>• <b>Non Cyclic</b> – Surfing hour restriction is defined by total allotted days and time duration</li> </ul>
Based on the options selected for the Restriction and Cycle Type, specify the following details.	
<b>Restriction based on Total Data Transfer and Cyclic Policy</b>	
<b>Cycle Period</b>	Specify Cycle Period. Cycle period defines the duration for cyclic types of policies i.e. Day, Week, Month and Year.
<b>Cycle Data Transfer</b>	Specify Cycle Data Transfer limit. It is the limit of data transfer allowed to the user per cycle. User will be disconnected if limit is reached.  OR  If you do not want to restrict data transfer per cycle, click Unlimited Cycle Data transfer.

<b>Maximum Data Transfer</b>	Specify the Maximum Data Transfer limit. It is the data transfer allowed to the user and if the limit is reached, user will not be able to log on until the policy is renewed.  OR  If you do not want to restrict maximum data transfer, click Unlimited Maximum Data Transfer.
<b>Restriction based on Total Data Transfer and Non-Cyclic Policy</b>	
<b>Maximum Data Transfer</b>	Specify the Maximum Data Transfer limit. It is the data transfer allowed to the user and if the limit is reached user will not be able to log on until the policy is renewed.  OR  If you do not want to restrict maximum data transfer, click Unlimited Maximum Data Transfer.
<b>Restriction based on Individual Data Transfer and Cyclic Policy</b>	
<b>Cycle Period</b>	Specify Cycle Period. Cycle period defines the duration for cyclic types of policies i.e. Day, Week, Month and Year.
<b>Cycle Upload Data Transfer</b>	Specify Cycle Upload Data Transfer limit. It is the upper limit of upload data transfer allowed to the user per cycle. User will be disconnected if limit is reached.  OR  If you do not want to restrict upload data transfer per cycle, click Unlimited Cycle Upload Data transfer.
<b>Cycle Download Data Transfer</b>	Specify Cycle Download Data Transfer limit. It is the upper limit of download data transfer allowed to the user per cycle. User will be disconnected if limit is reached.  OR  If you do not want to restrict download data transfer per cycle, click Unlimited Cycle Download Data transfer.
<b>Maximum Upload Data Transfer</b>	Specify the Maximum Upload Data Transfer limit. It is the maximum upload data transfer allowed to the user and if the limit is reached user will not be able to log on until the policy is renewed.  OR  If you do not want to restrict maximum upload data transfer, click Unlimited Upload Data Transfer.
<b>Maximum Download Data Transfer</b>	Specify Maximum Download Data Transfer limit. It is the maximum download data transfer allowed to the user and if the limit is reached user will not be able to log on until the policy is renewed.  OR  If you do not want to restrict maximum download data transfer, click Unlimited Download Data Transfer.
<b>Restriction based on Individual Data Transfer and Non-Cyclic Policy</b>	
<b>Maximum Upload Data Transfer</b>	Specify Maximum Upload Data Transfer limit. It is the maximum upload data transfer allowed to the user and if the limit is reached user will not be able to log on until the policy is renewed.



	<p>OR</p> <p>If you do not want to restrict maximum upload data transfer, click Unlimited Upload Data Transfer.</p>
<b>Maximum Download Data Transfer</b>	<p>Specify Maximum Download Data Transfer limit. It is the maximum download data transfer allowed to the user and if the limit is reached user will not be able to log on until the policy is renewed.</p> <p>OR</p> <p>If you do not want to restrict maximum download data transfer, click Unlimited Download Data Transfer.</p>
<b>Description</b>	Provide Policy Description.

**Table – Add Data Transfer Policy screen elements**

**Note**

- Cycle Data Transfer limit cannot be greater than Maximum Data Transfer limit.

## Live Users

Live users in the Appliance can be managed from a single page. All the active normal users, Clientless Users and Single Sign On users are visible from the Live Users. The Administrator can disconnect these users from this page directly.

### User types

Appliance supports five types of Users:

- Normal
- Clientless
- Single Sign on
- Thin Client User
- WWAN User

Normal User has to log on to the Appliance. Requires client (client.exe) on the User machine or user can use HTTP Client component and all the policy-based restriction are applied.

Clientless does not require client component (client.exe) on the User machines.


If User is configured for Single sign on, whenever User logs on to Windows, he/she is automatically logged to the Appliance.

If the User is a thin client user, whenever user logs on, he/she is visible on Live Users page.

If a wireless user is configured and connected, he/she is visible on Live User page.

## Live Users


**Identity > Live Users > Live Users** page displays list of currently logged on users and their important parameters. You can:


- Disconnect – Click the Disconnect icon  in the Manage column against a live user to be disconnected. A dialog box is displayed asking you to specify a customized message for the user that is to be disconnected. Click OK to disconnect the User. To disconnect multiple live users, select them  and click the Disconnect button.

### View Live User List

The page displays list of currently logged on users and their important parameters. Page also provides option to disconnect the user.

### To disconnect a user:


1. Click the Disconnect icon  under the Manage column against a user.
2. Specify the message in a dialog box.

3. Click the OK button to disconnect the User. To disconnect multiple live users, select them  and click the Disconnect button.

**Note**

- Configured Message would not be sent to a Clientless User.

To view and disconnect live users in Cyberoam, go to **Identity > Live Users > Live User**.

Concurrent Sessions: 1												
Disconnect												
Records Per Page 50 (1 of 1)												
<input type="checkbox"/>	User ID	User Name	Client Type	Host IP	IP Family	MAC	Start Time	Upload	Download	Data Transfer Rate (bits/sec)	Internet Usage Time (HH:MM)	Manage
<input type="checkbox"/>	7	test	Clientless	22::a	IPv4	-	2014-02-06 18:18	0.00 KB	0.00 KB	0.00 K	00:01	
Disconnect												
Records Per Page 50 (1 of 1)												

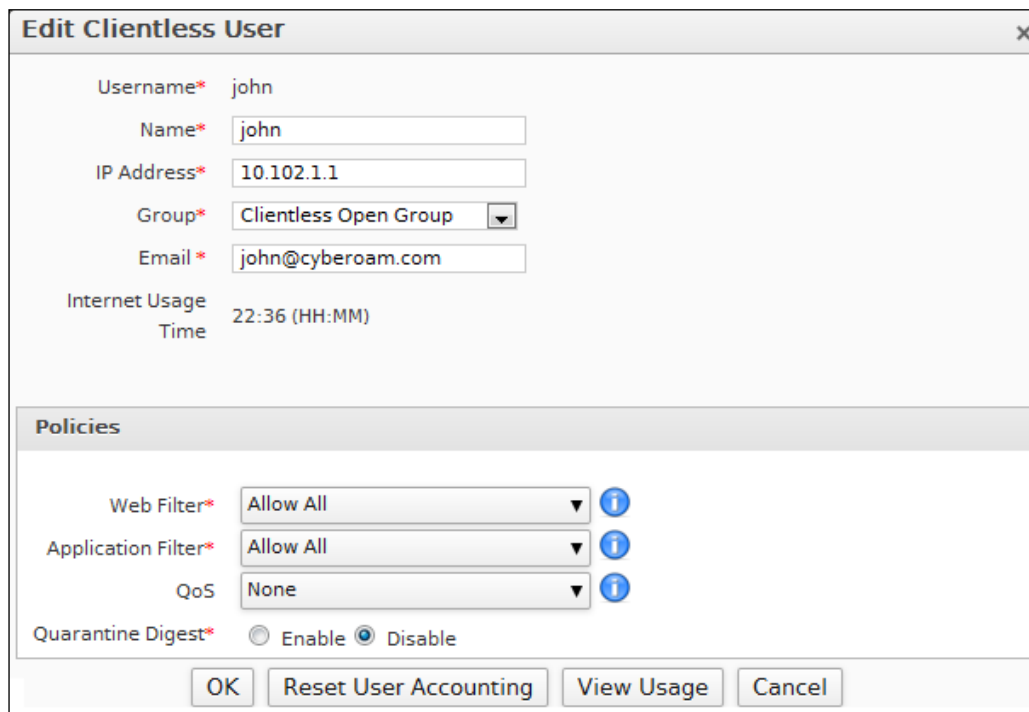
**Screen – Live Users**

Screen Element	Description
<b>User ID</b>	Displays the User Identification number.
<b>User Name</b>	Displays the name of the user with which she has logged in.
<b>Client Type</b>	Displays the name of the Group to which user belongs.
<b>Host IP</b>	Displays IP Address from which user has logged on.
<b>IP Family</b>	Displays the IP Family – IPv4 and IPv6.
<b>MAC</b>	MAC Address of the machine from which user had logged in.
<b>Start Time</b>	Session start time or login time.
<b>Upload / Download</b>	Data uploaded and Download during the session
<b>Data Transfer Rate (bits/sec)</b>	Bandwidth used during the session
<b>Internet Usage Time (HH:MM)</b>	Internet usage during the session.
<b>Disconnect Icon</b>	Disconnect the Live User.

**Table – Live Users screen elements**

## Live User Parameters

To edit user details, go to **Identity > User > Live User**. Click the Edit Icon  to modify the details of the live user.



**Edit Clientless User**

Username\* john

Name\* john

IP Address\* 10.102.1.1

Group\* Clientless Open Group

Email\* john@cyberoam.com

Internet Usage Time 22:36 (HH:MM)

**Policies**

Web Filter\* Allow All

Application Filter\* Allow All

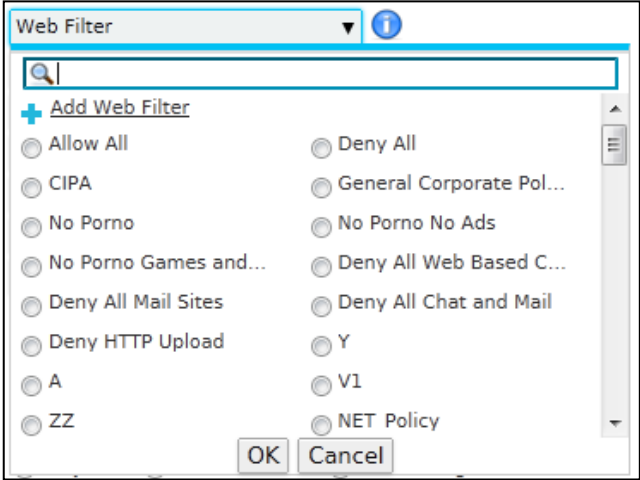
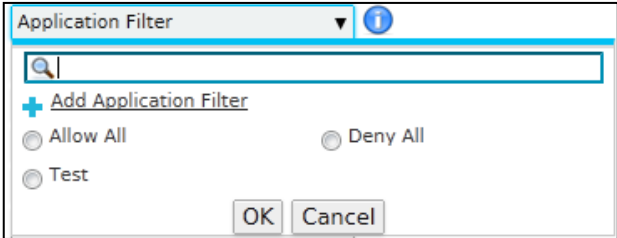
QoS None

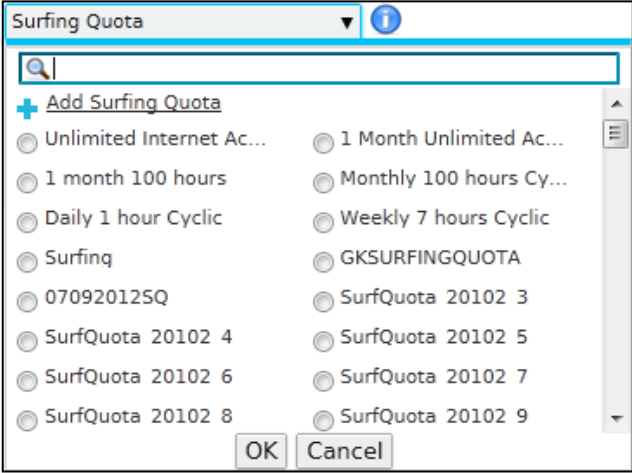
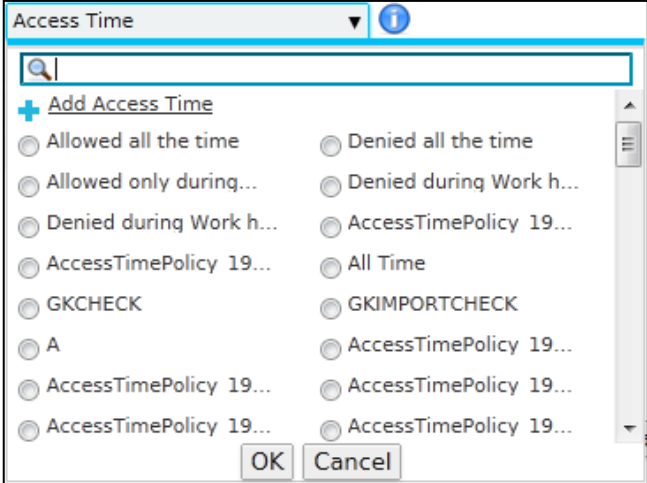
Quarantine Digest\*  Enable  Disable

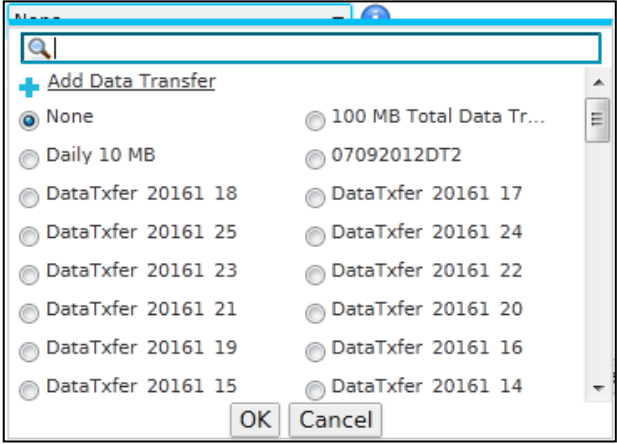
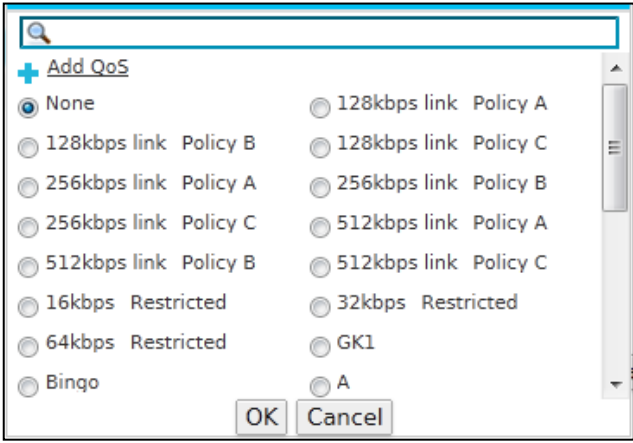
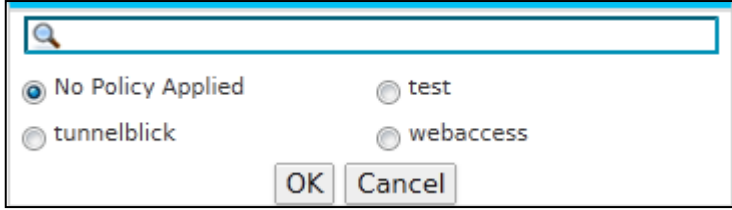
OK Reset User Accounting View Usage Cancel

Screen – Edit Live User

Screen Element	Description
<b>Username</b>	Specify a unique username to identify the user and for login.
<b>Name</b>	Name of the User.
<b>IP Address</b>	Specify the IP Address.
<b>Group</b>	Select Group for any live user.
<b>Email</b>	Specify Email ID.
<b>Internet Usage Time</b>	Displays total Internet usage time information.
<b>Policies</b>	
<b>Web Filter</b>	<p>Select the Web Filter Policy.</p> <p>You can also add and edit the details of web filter policy from the Clientless User Page itself. But, policy details can only be modified once the User is created.</p> <p>By default, "Allow All" Web filter Policy is applied to the user.</p>

	
<p><b>Application Filter</b></p>	<p>Select the Application Filter Policy.</p> <p>You can also add and edit the details of application filter policy from the Clientless User Page itself. But, policy details can only be modified once the User is created.</p> <p>By default, “Allow All” Application filter Policy is applied to the user.</p> 
<p><b>Surfing Quota (Not applicable to Clientless user)</b></p>	<p>Select the Surfing Quota Policy from the list.</p> <p>You can also create a new policy directly from this page itself and attach to the user.</p>

	
<p><b>Access Time</b> (Not applicable to Clientless user)</p>	<p>Select the Access Time Policy from the list.</p> <p>You can also create a new policy directly from this page itself and attach to the user.</p> 
<p><b>Data Transfer</b> (Not applicable to Clientless user)</p>	<p>Select the Data Transfer Policy from the list.</p> <p>You can also create a new policy directly from this page itself and attach to the user.</p>

	
<p><b>QoS</b></p>	<p>Select the QoS Policy.</p> <p>You can also add and edit the details of QoS policy from the Clientless User Page itself. But, policy details can only be modified once the User is created.</p> 
<p><b>SSL VPN</b></p>	<p>Select an SSL VPN policy from the list.</p> <p>If user is not to be provided the SSL VPN access then select “No Policy Applied”.</p> 
<p><b>L2TP</b></p>	<p>Enable if you want to allow user to get access through L2TP connection.</p>

<b>(Not applicable to Clientless user)</b>	
<b>PPTP</b> <b>(Not applicable to Clientless user)</b>	Enable if you want to allow user to get access through PPTP connection.
<b>Quarantine Digest</b>	Enable/Disable Quarantine Digest.
<b>Simultaneous Logins</b> <b>(Not applicable to Clientless user)</b>	Specify the number of concurrent logins that will be allowed to user OR Click 'Unlimited' for allowing unlimited Concurrent logins.  <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>The specified setting will override the global setting specified in the client preferences.</li> </ul> </div>
<b>MAC Binding</b> <b>(Not applicable to Clientless user)</b>	Enable/disable "MAC Binding". By binding User to MAC Address, you are mapping user with a group of MAC Addresses.
<b>MAC Address List</b> <b>(Not applicable to Clientless user)</b>	Specify MAC Addresses for example 01:23:45:67:89:AB.  Once you enable MAC binding, user will be able to login through pre-specified machines only.  To configure multiple MAC Addresses use comma. For example 01:23:45:67:89:AB, 01:23:45:67:89:AC
<b>Login Restriction</b> <b>(Not applicable to Clientless user)</b>	Select the appropriate option to specify the login restriction for the user.  Available Options: <ul style="list-style-type: none"> <li><b>Any Node</b> – Select to allow user to login from any of the nodes in the network.</li> <li><b>User Group Node(s)</b> – Select to allow user to login only from the nodes assigned to her group.</li> <li><b>Selected Nodes</b> – Select to allow user to login from the specified nodes only.</li> <li><b>Node Range</b> – Select to allow range of IP Address and specify IP Address range.</li> </ul>
<b>Administrator Advanced Settings</b>	
<b>Schedule for Appliance Access</b>	Schedule the Appliance access.  Administrator will be able to access the Appliance only during the time configured in schedule.
<b>Login Restriction for Appliance Access</b>	Select the appropriate option to specify the login restriction for the user.  Available Options:



	<ul style="list-style-type: none"><li>• <b>Any Node</b> – Administrator will be able to login from any of the nodes in the network.</li><li>• <b>Selected Nodes</b> – Administrator will be able to login from the specified nodes only.</li><li>• <b>Node Range</b> – Administrator will be able to login from any of the IP Address from the configured range.</li></ul>
<b>Reset User Accounting</b> (Displayed only after user is added)	Click to reset the usage accounting i.e. internet usage time and data transfer of the user.
<b>View Usage</b> (Displayed only after user is added)	Click to view the Internet usage and data transfer usage.

Table – Edit Live Users screen elements

# Firewall

A Firewall protects the network from unauthorized access and typically guards the LAN and DMZ networks against malicious access; however, Firewalls may also be configured to limit the access to harmful sites for LAN users.

The responsibility of Firewall is to grant access from Internet to DMZ or Service Network according to the Rules and Policies configured. It also keeps a watch on the state of connection and denies any traffic that is out of the connection state.

Firewall Rule provides centralized management of security policies. From a single Firewall Rule, you can define and manage an entire set of Appliance security policies.

Use Firewall Rule to:

- **Monitor and scan VPN traffic.**
- Define **inbound and outbound access** based on source and destination hosts/network.
- **Enable scanning for HTTP, HTTPS, FTP, SMTP, SMTP over SSL, POP3 or IMAP traffic** – for Email spam filtering, virus security and also get spyware, malware and phishing protection. To apply Anti Virus protection and spam filtering, you need to subscribe Gateway Anti Virus and Gateway Anti Spam modules individually. Refer to Licensing section for details.
- **Define IPS policy** – for protection against threats and attacks originating from external world and internal network. To apply IPS policy you need to subscribe for Intrusion Prevention System module. Refer to Licensing section for details.
- **Attach Gateway routing policy** – for load balancing and gateway failover protection in case of multiple gateways
- **Define Web filtering policy** – for web access control and block access to inappropriate web sites. To control access based on custom web categories, you need to subscribe Web and Application Filter module. Refer to Licensing section for details.
- **Define Applications filtering policy** – for controlling access to applications like IM, P2P and VOIP. To control access based on custom web categories, you need to subscribe Web and Application Filter module. Refer to Licensing section for details.
- **Schedule access**
- **Attach QoS policy** – to control and schedule bandwidth usage per user, group or prioritize bandwidth usage for particular application.

## How it works

Firewall Rules control traffic passing through the Appliance. Depending on the instruction in the rule, the Appliance decides on how to process the access request. When the Appliance receives the request, it checks for the source address, destination address and the services and tries to match with the Firewall Rule. If Identity match is also specified, Firewall will search in the Live Users Connections for the Identity check i.e. will check whether the user is allowed access or not. If Identity (User) is found in the Live User Connections and all other matching criteria are fulfilled, access is allowed or denied based on the action configured in the rule.

By default, the Appliance blocks any traffic to LAN.

## IPv6

Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP). It is a routable protocol, that provides identification and location system for devices on networks and routes traffic across the Internet. The Internet Engineering Task Force (IETF), an open standards organization that develops and promotes Internet standards, has developed IPv6 to deal with the long-anticipated problem of IPv4 address exhaustion.

IPv6 replaces IPv4, the existing Internet Protocol.

Benefits of IPv6:

- Large address space
- New and simplified header format
- Efficient and hierarchical addressing and routing
- Stateless and stateful address configuration
- Built-in security and interoperability
- In-built mobility
- Mandatory Multicast support
- Better support for QoS
- ICMPv6 based new protocol for neighboring node interaction
- Extensibility in packet headers

## IPv6 Features supported in CyberoamOS

You will be able to use IPv6 as well as IPv4 for the following:

- Networking
  1. Alias and VLAN (needs the IP Address of the same family on the respective physical interface)
  2. Alias over WLAN
  3. LAG
  4. Multiport Bridge
  5. Gateway
  6. Route – Static and Dynamic
  7. DNS and DHCP Services
  8. Router Advertisement
  9. Neighbor Discovery Protocol
- Firewall Security
  1. QoS Policy
  2. Application Filter Policy
  3. Web Filter Policy
  4. Intrusion Prevention System (IPS) Policy
  5. AV and AS Scanning
  6. DoS and Spoof Prevention
  7. Host, Host Group, MAC Group
  8. IPv6 Services
  9. NAT Policy (NAT66)
  10. Scheduling
  11. Virtual Host
- Layer 8 Identity over IPv6
  1. Authentication – AD, LDAP, Radius

- 2. Clientless Users
- 3. IPv6 Captive Portal
  
- Logging and Reporting
  - 1. Traffic Discovery (For User and Source IP Address)
  - 2. Logs and Reports
  - 3. 4-Eye Authentication
  
- Diagnostic
  - 1. Packet Capture
  - 2. Connection List
  - 3. Ping6
  - 4. Tracert6
  - 5. Name Lookup
  - 6. Route Lookup
  - 7. System Graphs
  
- SNMP
- SYSLOG
- NTP
- IPv6 Certificate
- Scheduled Backup on IPv6 Server
- Backup Restore
- High Availability
- IPSec VPN
- Web Proxy
- Parent Proxy

## Default Firewall Rules

At the time of deployment, the Appliance allows to define one of the following access policies through Network Configuration Wizard:

- Monitor only
- General Internet policy
- Strict Internet policy

### Default Firewall Rules for “Monitor only” policy

Masquerade and allow entire LAN to WAN traffic for all the authenticated users after applying following policies:

- Web Filter Policy – User specific
- Application Filter Policy – User specific
- QoS Policy – User specific
- Anti Virus & Anti Spam policy – Allows SMTP, SMTP over SSL, POP3, IMAP, HTTP and HTTPS traffic without scanning

Masquerade and allow entire LAN to WAN traffic for all the users without scanning SMTP, SMTP over SSL, POP3, IMAP, HTTP and HTTPS traffic

### Default Firewall Rules for “General Internet policy” policy

Masquerade and allow entire LAN to WAN traffic for all the authenticated users after applying following policies:

- Web Filter Policy – User specific
- Application Filter Policy – User specific
- QoS Policy – User specific
- Anti Virus & Anti Spam policy – Scan SMTP, SMTP over SSL, POP3, IMAP, HTTP and HTTPS traffic

Masquerade and allow entire LAN to WAN traffic for all the users after applying following policies:

- Web Filter & Application Filter policy – Applies ‘General Corporate Policy’ to block Porn, Nudity, Adult Content, URL Translation Sites, Drugs, Crime and Suicide, Gambling, Militancy and Extremist, Phishing and Fraud, Violence, Weapons categories
- IPS – General policy
- Anti Virus & Anti Spam policy – Scan SMTP, SMTP over SSL, POP3, IMAP, HTTP and HTTPS traffic

### Default Firewall Rules for “Strict Internet policy” policy

Masquerade and Allow entire LAN to WAN traffic for all the authenticated users after applying following policies:

- Web Filter Policy – User specific
- Application Filter Policy – User specific
- QoS Policy – User specific
- Anti Virus & Anti Spam policy – Scan SMTP, SMTP over SSL, POP3, IMAP, HTTP and HTTPS traffic

Drop entire LAN to WAN traffic for all the users

#### Note

- Default Firewall Rules can be modified as per the requirement but cannot be deleted.
- IPS policy will not be effective until Intrusion Prevention System (IPS) module is subscribed.
- Virus and Spam policy will not be effective until Gateway Anti Virus and Gateway Anti Spam modules are subscribed respectively.
- If access Policy is not set through Network Configuration Wizard at the time of deployment, the entire traffic is dropped.

Additional Firewall Rules for any of the zones can be defined to extend or override the default rules. For example, rules can be created that block certain types of traffic such as FTP from the LAN to the WAN, or allow certain types of traffic from specific WAN hosts to specific LAN hosts, or restrict use of certain protocols such as Telnet to authorized users on the LAN.

Custom rules evaluate network traffic's source IP Addresses, destination IP Addresses, User, IP protocol types, and compare the information to access rules created on the Appliance. Custom rules take precedence, and override the default Appliance Firewall Rules.

- [Rule](#)
- [Virtual Host](#)
- [NAT Policy](#)
- [Spoof Prevention](#)
- [DoS](#)

# Rule

## IPv4 Firewall Rule

The Appliance's Identity based Firewall allows creation of Firewall Rules embedding user identity into the Firewall Rule matching criteria. It also allows to bind identity and device by embedding device MAC Address through MAC Host in Firewall Rule.

Firewall Rule matching criteria now includes:

- Source and Destination Zone and Host. The direction of traffic is determined by source and destination zone. The same zone cannot be defined as both the source or destination zone.
- User
- Service
- Schedule

Attach all the Unified Threat Control policies to the Firewall Rule as per the defined matching criteria:

- Intrusion Prevention System (IPS)
- Anti Virus
- Anti Spam
- Web Filter
- Application Filter
- QoS
- User and application based Routing policies

To create a Firewall Rule, you should:

- Define matching criteria
- Associate action to the matching criteria
- Attach the threat management policies

For example, now you can:

- Restrict the bandwidth usage to 256kb for the user John every time he logs on from the IP Address 192.168.2.22
- Restrict the bandwidth usage to 1024kb for the user Mac if he logs on in working hours from the IP Address 192.168.2.22

The rule page displays list of default and custom firewall rules. All the firewall rules are grouped by its source and destination zone. The page also provides option to add or insert a new rule, update the existing rule, changing the rule order, or delete a rule.

### Viewing Firewall Rules between two Zones



To view the firewall rules for the specific zones, select zones. For example, if you select LAN and WAN, all the Firewall Rules created for LAN zone to WAN zone will be displayed.

Firewall rule controls the traffic flowing through the Appliance and are created for a pair of source and destination zone which determines the traffic direction.









Processing of firewall rules is top downwards and the first suitable rule found is applied.

Hence, while adding multiple rules, it is necessary to put specific rules before general rules. Otherwise, a general rule might allow a packet that you specifically have a rule written to deny later in the list. When a packet matches the rule, the packet is immediately dropped or forwarded without being tested by the rest of the rules in the list.














As the firewall rules are grouped source and destination zone wise, rule can be added at the bottom of the list or can be inserted in the group.

- **Inserting a Firewall Rule** – To insert a rule for a particular source and destination zone click the Insert icon  under the Manage column against a firewall rule for the required source and destination zone. For example, if you have already added a firewall rule for LAN to DMZ zone and want to add another rule for the same zones then click Insert icon against the firewall rule for LAN to DMZ zone. It will add a new firewall rule for the same zones.
- **Reordering Firewall Rules** – Rules are ordered by their priority. When the rules are applied, they are processed from the top down and the first suitable rule found is applied. Hence, while adding multiple rules, it is necessary to put specific rules before the general rules. Otherwise, a general rule might allow a packet that you specifically have a rule to deny later in the list. When a packet matches the rule, the packet is immediately dropped or forwarded without being tested by the rest of the rules in the list. To change order of the rule, click the Move icon  against the rule whose order is to be changed. Move the rule by dragging and dropping to a required position.
- **Clear All Filters** – To clear all the search filters applied on the source, destination or identity columns, click the “Clear All Filters” button. This helps in removing filters on multiple columns at a time.
- **View Firewall Rules between two Zones** – To view Firewall Rules for the selected zones, select zones. For example, if you select LAN and WAN, all the Firewall Rules created for LAN zone to WAN zone will be displayed.

### Icons and their Meaning in Firewall Rule

Icon	Meaning	Appearing under Column
	Firewall rule is enabled and is currently applied to the traffic.	Enable
	Firewall rule is disabled.	Enable
	Firewall rule is enabled but is not currently applied. It will be applied to the traffic as per the time configured in the schedule.	Enable
 	Enabled Disabled	IM Scanning, WAF, Logging, Bypass User Accounting
 	SMTP Scanning enabled. SMTP Scanning disabled.	AV & AS Scanning
	SMTP over SSL Scanning enabled	AV & AS Scanning



	SMTP over SSL Scanning disabled	
 	POP Scanning enabled. POP Scanning disabled.	AV & AS Scanning
 	IMAP Scanning enabled. IMAP Scanning disabled.	AV & AS Scanning
 	HTTP Scanning enabled. HTTP Scanning disabled.	AV & AS Scanning
 	FTP Scanning enabled. FTP Scanning disabled.	AV & AS Scanning
 	HTTPS Scanning enabled. HTTPS Scanning disabled.	AV & AS Scanning
	Inserts rule before the existing rule.	Manage
	Changes order of the rule.	Manage

## Manage Firewall Rule List


Firewall Rules control the traffic flowing through Appliance. **Firewall > Rule > IPv4 Rule** page displays a list of Firewall Rules and provides a way to manage rules.

Rules are created for a pair of source and destination zone which determines the traffic direction.

ID	Rule Name	Enable	Source	Destination	Service	Action	Identity	IM Scanning	Routing Through Gateway	Backup Gateway	Manage
LAN - WAN ( Total 2 )											
2	#LAN_WAN_LiveUserTraffic	<input checked="" type="checkbox"/>	Any Host	Any Host	Any Service	Accept	Any Live User	<input checked="" type="checkbox"/>	Load Balance	None	
1	#LAN_WAN_AnyTraffic	<input checked="" type="checkbox"/>	Any Host	Any Host	Any Service	Accept	-	<input checked="" type="checkbox"/>	Load Balance	None	

Screen – Firewall Rule

Screen Element	Description
<b>ID</b>	Firewall Rule ID which is generated automatically at the time of creation.
<b>Rule Name</b>	Firewall Rule name to identify the Firewall Rule.
<b>Enable</b>	Click to activate/deactivate the rule. If you do not want to apply the Firewall Rule temporarily, disable rule instead of deleting.
<b>Source</b>	Source Host to which the rule applies.
<b>Destination</b>	Destination Host to which the rule applies.
<b>Service</b>	Service for which the rule is created.
<b>Action</b>	Displays the action to be taken when the rule matches a connection attempt.
<b>Identity</b>	Displays user or user group on which the firewall rule is applied.  If Identity is configured, user based policies will be applied to the traffic.
<b>Web Filter</b>	A Web Filter policy to be applied to the traffic.  Point to the policy link to view or edit the policy details.
<b>Application Filter</b>	An Application Filter policy to be applied to the traffic.  Point to the policy link to view or edit the policy details.
<b>NAT</b>	NAT policy to be applied to the traffic.  Point to the policy link to view or edit the policy details.
<b>IPS</b>	IPS policy to be applied to the traffic.
<b>QoS Policy</b>	QoS policy to be applied to the traffic.  Point to the policy link to view or edit the policy details.


<b>IM Scanning</b>	Displays whether IM Scanning is enabled or disabled.
<b>AV &amp; AS Scanning</b>	Displays the protocols selected for AV & AS Scanning.
<b>Schedule</b>	<p>A Schedule that controls when the rule should be active.</p> <p>Point to the schedule link to view or edit the schedule details.</p> <div data-bbox="837 474 1212 721" style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <p>Schedule <a href="#">edit</a> </p> <p>Schedule Name abc</p> <p>Schedule Type Recurring</p> <p>Start Date -</p> <p>End Date -</p> <p>Days Friday</p> <p>Start Time 10:45</p> <p>Stop Time 11:15</p> </div>
<b>Logging</b>	Firewall Rule logging.
<b>Description</b>	Firewall Rule Description.
<b>Routing through Gateway</b>	Routing policy applied to the traffic.
<b>Backup Gateway</b>	Backup gateway for the traffic.
<b>Upload Data</b>	Displays total outgoing traffic.
<b>Download Data</b>	Displays total incoming traffic.
<b>DSCP Marking</b>	Displays DSCP value for rule.
<b>WAF</b>	Displays whether WAF is active mode or inactive mode for a rule.
<b>Bypass User Accounting</b>	Displays whether Bypass User Accounting is enabled or disabled.

**Table - Manage IPv4 Firewall Rule screen elements**

## Change Firewall Rule order

Rule order defines the rule processing priority. When the rules are applied, they are processed from the top down and the first suitable rule found is applied.

Hence, while adding multiple rules, it is necessary to put specific rules before general rules. Otherwise, a general rule might allow a packet that you specifically have a rule written to deny later in the list. When a packet matches the rule, the packet is immediately dropped or forwarded without being tested by the rest of the rules in the list.

Go to **Firewall > Rule > IPv4 Rule**. Click the move rule  against the rule whose order is to be changed.

- Click on the rule to be moved and then drag & drop the rule in the desired order.
- Click close to save the order.

Add Delete Clear All Filters All Zones to All Zones Go Select Columns

<input type="checkbox"/>	ID	Rule Name	Enable	Source	Destination	Service	Action	Schedule	Manage
VPN - VPN ( Total 3 )									
LAN - WAN ( Total 5 )									
<input type="checkbox"/>	25	testRule		PULL_Request	Any Host	Any Service	Accept	All The Time	
<input type="checkbox"/>	18	Allow_Internet1		Any Host	Any Host	Any Service	Accept	Work hours (5 Day week)	
<input type="checkbox"/>	22	test		PULL_Request	Any Host	Any Service	Accept	abc	
<input checked="" type="checkbox"/>	2	#LAN_WAN_LiveUserTraffic		Any Host	Any Host	Any Service	Accept	All The Time	Move
<input checked="" type="checkbox"/>	1	#LAN_WAN_AnyTraffic		Any Host	Any Host	Any Service	Accept	All The Time	
VPN - LAN ( Total 2 )									
<input type="checkbox"/>	9	Rule_9		Any Host	Any Host	Any Service	Accept	All The Time	
<input type="checkbox"/>	8	Rule_8		Any Host	Any Host	Any Service	Accept	All The Time	


### Move Firewall Rule

Name	Source Host	Destination Host	Service	Action
testRule	PULL_Request	Any Host	Any Service	Accept
Allow_Internet1	Any Host	Any Host	Any Service	Accept
test	PULL_Request	Any Host	Any Service	Accept
#LAN_WAN_LiveUserTraffic	Any Host	Any Host	Any Service	Accept
#LAN_WAN_AnyTraffic	Any Host	Any Host	Any Service	Accept

Close

Screen – Move IPv4 Firewall Rule

## IPv4 Firewall Rule Parameters

To add or edit Firewall Rules, go to **Firewall > Rule > IPv4 Rule**. Click Add Button to add a new rule or the Edit Icon  in the Manage column against the Firewall Rule to modify the details of the rule. Firewall Rule [Parameters](#) are given below.

**General Settings**

**Rule Name**

Name \*

Description

---

**Basic Settings**

	Source	Destination
Zone *	<input type="text" value="LAN"/>	<input type="text" value="Select Destination Zone"/>
Attach Identity	<input checked="" type="checkbox"/>	<input type="checkbox"/> Exclude traffic from data accounting for selected user(s)
Identity *	<input type="text" value="Any User"/>	<input type="text" value="Any IP Address"/>
Network / Host *	<input type="text" value="Any IP Address"/>	
Services *	<input type="text" value="Any Services"/>	
Schedule	<input style="border: 1px solid #ccc;" type="text" value="All The Time"/>	
Action *	<input checked="" type="radio"/> Accept <input type="radio"/> Drop <input type="radio"/> Reject	
<input type="checkbox"/> Apply NAT	<input type="text" value="MASQ"/>	

**Advanced Settings (Security Policies, QoS, Routing Policy, Log Traffic)**

**Security Policies**

Application Filter	<input type="text" value="User's policy applied"/>	<input type="checkbox"/> Apply Application based QoS Policy
Web Filter	<input type="text" value="User's policy applied"/>	<input type="checkbox"/> Apply Web Category based QoS Policy
IPS	<input type="text" value="None"/>	
ICAP	<input type="text" value="None"/>	
IM Scanning	<input type="checkbox"/> Enable	
WAF	<input type="checkbox"/> Enable	
AV & AS Scanning	<input type="checkbox"/> SMTP <input type="checkbox"/> SMTPS <input type="checkbox"/> POP3 <input type="checkbox"/> IMAP <input type="checkbox"/> FTP <input type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS	

**QoS & Routing Policy**

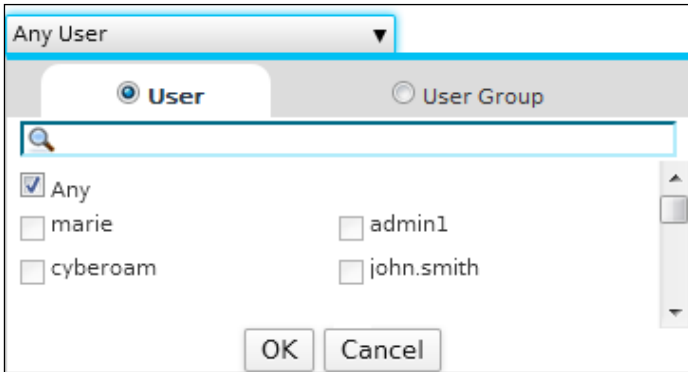
QoS	<input type="text" value="User's policy applied"/>	
DSCP Marking	<input type="text" value="Select DSCP Marking"/>	
Route Through Gateway	<input type="text" value="Load Balance"/>	(Applicable only in case of Multiple Gateways)
Backup Gateway	<input type="text" value="None"/>	

**Log Traffic**

Log Firewall Traffic  Enable

Screen - Add IPv4 Firewall Rule

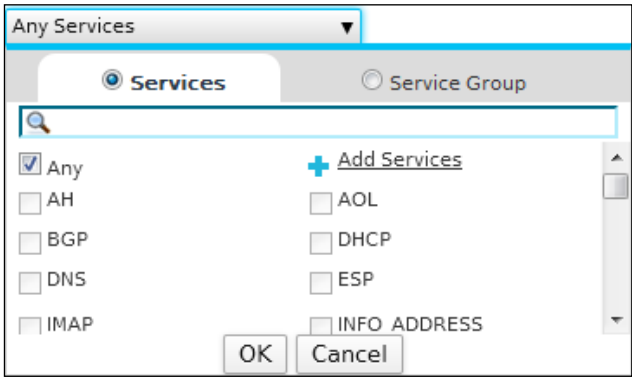
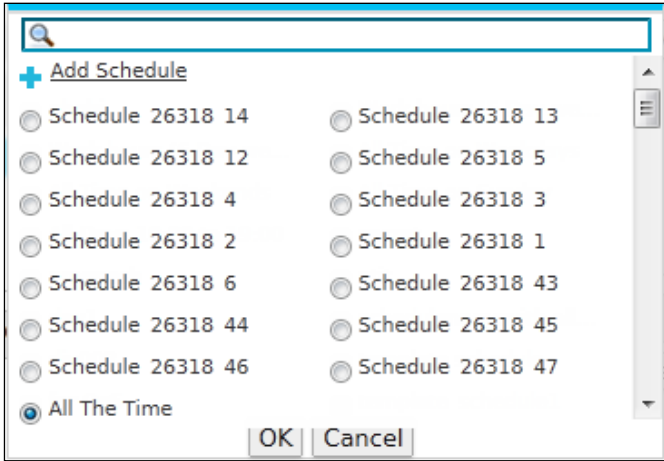
## Parameters

Screen Element	Description
<b>General Settings</b>	
<b>Rule Name</b>	
<b>Name</b>	Specify a name to identify the Firewall Rule.
<b>Description</b>	Provide description for the rule.
<b>Basic Settings</b>	
<b>Zone</b>	Select the source and destination zone to which the rule applies.
<b>Attach Identity (Only if source zone is LAN/DMZ/VPN)</b>	<p>Attach Identity allows you to check whether the specified user/user group from the selected zone is allowed to access the selected service or not.</p> <p>This feature is not available in case WAN is selected and the Source Zone.</p> <p>Click to attach the user identity.</p>  <p>Enable check identity to apply following policies per user:</p> <ul style="list-style-type: none"> <li>• Web policy and Application policy for Content Filtering (User's policy will be applied automatically but will not be effective till the Web and Application Filtering module is subscribed).</li> <li>• Schedule Access.</li> <li>• IPS (User's IPS policy will be applied automatically but will not be effective till the IPS module is subscribed).</li> <li>• Anti Virus scanning (User's anti virus scanning policy will be applied automatically but it will not be effective till the Gateway Anti Virus module is subscribed).</li> <li>• Anti Spam scanning (User's anti spam scanning policy will be applied automatically but it will not be effective till the Gateway Anti Spam module is subscribed).</li> <li>• QoS policy – User's QoS policy will be applied automatically.</li> </ul>

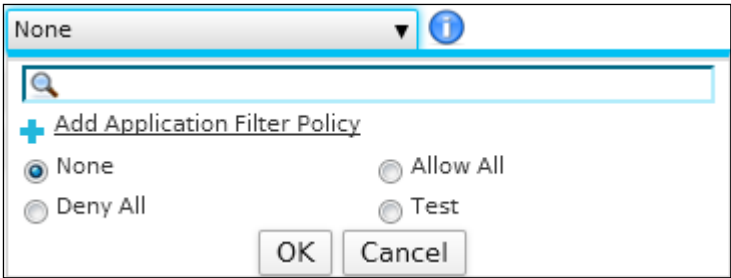
	<ul style="list-style-type: none"> <li>• WAF (User's WAF policy will be applied automatically but will not be effective till the WAF module is subscribed).</li> <li>• Policy selected in the "Route through Gateway" field is the static routing policy that is applicable only if more than one gateway is defined and used for load balancing.</li> <li>• Limit access to available services.</li> </ul>
<b>Identity</b>	Select user/user group for the selected zone to allow/deny access the selected service.
<b>Exclude traffic from data accounting for selected user(s)</b>	<p>By default user's network traffic is considered in data accounting. Select to exclude certain traffic user data accounting. The traffic allowed through this firewall rule will not be accounted towards data transfer for the user.</p> <p>This option is available only if the parameter "Attach Identity" is enabled.</p> <p>This traffic will not be included in the user accounting reports - Internet Usage report and My Account reports, but will be included in the firewall activity reports.</p> <p>Example:</p> <p>A User is added from <b>Identity &gt; Users &gt; Users</b></p> <ul style="list-style-type: none"> <li>• User Name – Cyberoam</li> <li>• Maximum Data Transfer limit for User Cyberoam – 100 MB</li> <li>•</li> </ul> <p>An IPv4 Firewall Rule is created</p> <ul style="list-style-type: none"> <li>• Firewall Rule Name – Bypass Data Transfer</li> <li>• Firewall Rule for zones – LAN to WAN</li> <li>• Attached Identity – Enabled (User – Cyberoam)</li> <li>• Bypass User Data Transfer Accounting – Enabled</li> </ul> <p>User Activity</p> <ul style="list-style-type: none"> <li>• The user transfers data in LAN to LAN Zone – 50 MB</li> <li>• The user transfers data in LAN to WAN Zone – 10 MB</li> <li>•</li> </ul> <p>Accounted Data Transfer</p> <ul style="list-style-type: none"> <li>• Calculated Total Data Transfer – 50 MB</li> </ul> <p>Reason – Only the data transferred on LAN to LAN zone is considered i.e. 50MB. Data transferred on LAN to WAN Zone i.e. 10 MB is not calculated and bypassed by the Administrator as per the IPv4 Firewall Rule "Bypass Data Transfer".</p>

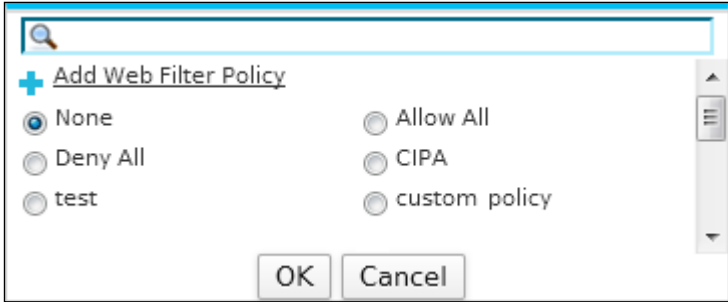
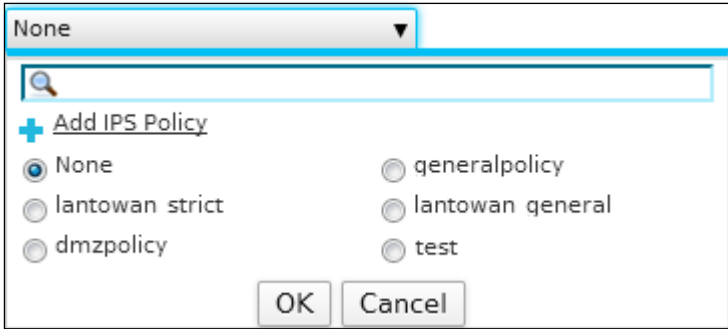
<p><b>Network/Host</b></p>	<p>Specify source and destination host or network address to which the rule applies.</p> <p>Host dropdown list also displays MAC based host, dynamic hosts and host groups which are automatically added on creation of VPN Road warrior connections(IPSec and SSL). It will also display the default hosts created for road warrior connection - ##ALL_RW, ##ALL_IPSEC_RW, ##ALL_SSLVPN_RW, ##WWAN1 (when WWAN is enabled)</p> <p>You can also define a new IP host, IP host group, MAC host, virtual host, FQDN host, FQDN host group, country host, country host group and Web Server directly from this page.</p> <div data-bbox="375 705 1284 1142"> </div> <div data-bbox="383 1232 1276 1545"> </div>
<p><b>Services</b></p>	<p>Services represent the types of Internet data transmitted via particular protocols or applications.</p> <p>Select Services/Service Group to which the rule applies.</p> <p>If Virtual host is selected as Destination host, you will be able to configure services only if the selected virtual host is not port forwarded.</p>

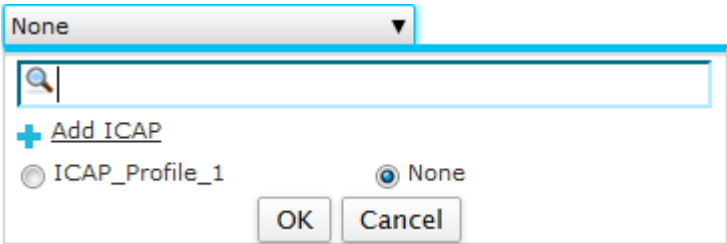


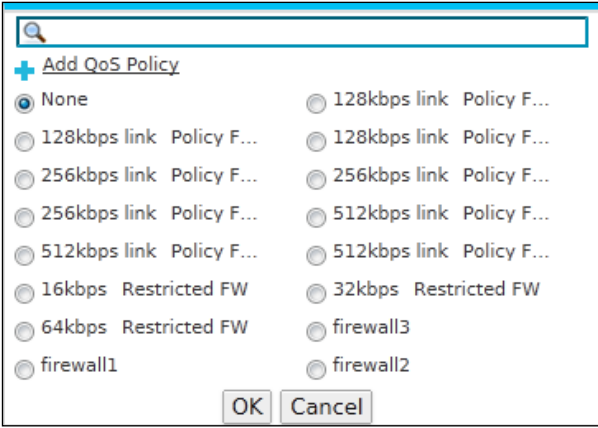
	<p>You can also add a custom service or service group from this page itself.</p> <p>Protect by configuring rules to:</p> <ul style="list-style-type: none"> <li>• block services at specific zone.</li> <li>• limit some or all users from accessing certain services</li> <li>• allow only specific user to communicate using specific service</li> </ul> 
<p><b>Schedule</b></p>	<p>Select Schedule for the rule.</p> <p>You can also add a new schedule directly from this.</p> 
<p><b>Action</b></p>	<p>Select rule action.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Accept</b> – Allow access</li> <li>• <b>Drop</b> – Silently discards</li> <li>• <b>Reject</b> – Denies access and “ICMP port unreachable” message will be sent to the source.</li> </ul>

	<p>While sending a response it might be possible that response is sent using a different interface than the one on which request was received. This may happen depending on the Routing configuration done on Appliance.</p> <p>For Example,</p> <p>If the request is received on the LAN port using a spoofed IP Address (public IP Address or the IP Address not in the LAN zone network) and specific route is not defined, Appliance will send a response to these hosts using default route. Hence, response will be sent through the WAN port.</p>
<p><b>Apply NAT (Only if Action is 'ACCEPT')</b></p>	<p>On enabling "Allow NAT" access is allowed only after replacing the source IP Address with the IP Address specified in the NAT policy.</p> <p>Select NAT Policy for the Firewall Rule. Traffic from this rule will pass as per the NAT Policy selected for all gateways.</p> <p>Default - MASQ</p> <p>You can also use NAT policy configured for the gateway from <b>Network &gt; Gateway &gt; Gateway</b>. All traffic passing from this rule is NATed as per the gateway's default NAT policy.</p> <p>You can also override this gateway specific NAT policy by selecting a NAT policy. Multiple Gateways and NAT Policy can be added. If enabled the overridden policy is applied instead of gateway's default NAT policy.</p> <p>Select None NATing is not required for a particular gateway.</p> <div data-bbox="699 1355 1390 1480" style="border: 1px solid black; background-color: #f0f0f0; padding: 5px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>This option is available if Appliance is deployed as Gateway.</li> </ul> </div>
<p>Advanced Settings</p> <p>Toggle Drill Down icon – Click to apply different protection settings to the traffic controlled by Firewall. You can:</p> <ul style="list-style-type: none"> <li>Enable load balancing and failover when multiple links are configured. Applicable only if Destination Zone is WAN</li> <li>Configure antivirus protection and spam filtering for SMTP, IMAP, POP3, and HTTP policies. To apply antivirus protection and spam filtering, you need to subscribe for Gateway Anti Virus and Gateway Anti Spam modules individually. Refer to Licensing section for details.</li> <li>Implement Intrusion Prevention System. To apply IPS policy you need to subscribe for Intrusion Prevention System module. Refer to Licensing section for details.</li> </ul>	

<ul style="list-style-type: none"> <li>• Configure content filtering policies. To apply content filtering you need to subscribe for Web and Application Filter module. Refer to Licensing section for details.</li> <li>• Apply QoS policy</li> </ul>	
<b>Security Policies</b>	
<b>Application Filter</b>	<p>Select Application Filter Policy for the rule. One can apply policy on following traffic:</p> <p>Incoming traffic (source zone configured as WAN)</p> <p>Cyberoam destined traffic (destination zone configured as LOCAL)</p> <p>It controls access to application like IM and P2P, VOIP.</p> <p>You can also create a new policy directly from this page and attach to the user.</p> 
<b>Apply Application Based QoS Policy</b>	<p>Click to restrict bandwidth for the applications categorized under the Application category.</p> <p>A three step configuration is required as follows:</p> <ul style="list-style-type: none"> <li>• Create QoS policy from menu item <b>"QoS &gt; Policy &gt; Policy &gt; Add"</b>.</li> <li>• Assign above created QoS policy to the Application category from menu item "Application Filter". Policy can be assigned to application categories.</li> <li>• Enable "Application Category based QoS Policy" from Firewall Rule.</li> </ul> <p>Above configured policy will be applicable, whenever the application falling under the Application category is accessed.</p>
<b>Web Filter</b>	<p>Select the Web Filter Policy for the rule. One can apply the policy on following traffic:</p> <ul style="list-style-type: none"> <li>• Incoming traffic (source zone configured as WAN)</li> <li>• Cyberoam destined traffic (destination zone configured as LOCAL)</li> </ul>

	<p>It controls web access control and blocks access to inappropriate web sites.</p> <p>You can also create a new policy directly from this page and attach to the user.</p> 
<p><b>Apply Web Category Based QoS Policy</b></p>	<p>Click to restrict bandwidth for the URLs categorized under the Web category.</p> <p>A three step configuration is required as follows:</p> <ul style="list-style-type: none"> <li>• Create QoS policy from menu item “<b>QoS &gt; Policy &gt; Policy &gt; Add</b>”</li> <li>• Assign above created QoS policy to the Web category from menu item “<b>Web Filter</b>”. Policy can be assigned to the default as well as custom web categories.</li> <li>• Enable “Web Category based QoS Policy” from Firewall Rule</li> </ul> <p>Above configured policy will be applicable, whenever the URL falling under the Web category is accessed.</p>
<p><b>IPS</b></p>	<p>Select IPS policy for the rule.</p> <p>To use IPS, you have to subscribe for the module. Refer to Licensing for more details.</p> <p>You can also create a new policy directly from this page and attach to the user.</p> 

<p><b>ICAP</b></p>	<p>Select ICAP Policy for the rule.</p> <p>You can also create a new policy directly from this page.</p>  <ul style="list-style-type: none"> <li>This feature is supported in 'iNG' series appliances CR50iNG and above.</li> </ul>
<p><b>IM Scanning</b></p>	<p>Click to enable IM scanning.</p> <p>If enabled, all the messaging applications' traffic is scanned.</p>
<p><b>WAF</b></p>	<p>Click to enable WAF.</p> <p>If enabled, WAF policies will be applied.</p>
<p><b>AV &amp; AS Scanning</b></p>	<p>Click the protocol for which the virus and spam scanning is to be enabled</p> <p>Default – Disable</p> <p>To implement Anti Virus and Anti Spam scanning, you have to subscribe for the Gateway Anti Virus and Anti Spam modules individually. Refer to Licensing for more details.</p>
<p><b>QoS and Routing Policy</b></p>	
<p><b>QoS</b></p>	<p>Select QoS policy for the rule.</p> <p>QoS policy allocates &amp; limits the maximum bandwidth usage of the user.</p> <p>You can also create a new policy directly from this page and attach to the user.</p>

	
<b>DSCP Marking</b>	<p>Select DSCP Marking.</p> <p>DSCP (DiffServ Code Point) classifies flow of packets as they enter the local network depending upon QoS. Flow is defined by 5 elements; Source IP Address, Destination IP Address, Source port, Destination port and the transport protocol.</p> <p>For available options, refer <a href="#">DSCP Values</a>.</p>
<b>Route Through Gateway (Available only if Appliance is deployed as Gateway)</b>	<p>Select the routing policy. Option is available only if more than one gateway is configured.</p>
<b>Backup Gateway</b>	<p>Specify the backup gateway.</p> <p>The traffic will be routed through the configured gateway in case gateway configured in "Route Through Gateway" goes down.</p> <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>This Option is available only if "Load Balance" is not selected for "Route Through Gateway"</li> </ul> </div>
<b>Log Traffic</b>	
<b>Log Firewall Traffic</b>	<p>Click to enable traffic logging for the rule i.e. traffic permitted and denied by the Firewall Rule.</p>

**Table - Add IPv4 Firewall Rule screen elements**

## DSCP Values

DiffServ Code Point (DSCP) uses the 6 bits, thereby giving  $2^6 = 64$  different values (0 to 63). "Table – Standard DSCP Marking" describes the standard DSCP values. Remaining DSCP values can be customized as per the QoS requirement.

Decimal	DSCP	Description
0	Default	Best Effort
8	CS1	Class 1 (CS1)
10	AF11	Class 1, Gold (AF11)
12	AF12	Class 1, Silver (AF12)
14	AF13	Class 1, Bronze (AF13)
16	CS2	Class 2 (CS2)
18	AF21	Class 2, Gold (AF21)
20	AF22	Class 2, Silver (AF22)
22	AF23	Class 2, Bronze (AF23)
24	CS3	Class 3 (CS3)
26	AF31	Class 3, Gold (AF31)
28	AF32	Class 3, Silver (AF32)
30	AF33	Class 3, Bronze (AF33)
32	CS4	Class 4 (CS4)
34	AF41	Class 4, Gold (AF41)
36	AF42	Class 4, Silver (AF42)
38	AF43	Class 4, Bronze (AF43)
40	CS5	Class 5 (CS5)
46	EF	Expedited Forwarding (EF)
48	CS6	Control (CS6)
56	CS7	Control (CS7)

**Table – Standard DSCP Marking**

## IPv6 Firewall Rules

The Appliance's Identity based Firewall allows creation of Firewall Rules embedding user identity into the Firewall Rule matching criteria. It also allows to bind identity and device by embedding device MAC Address through MAC Host in Firewall Rule.

Firewall Rule matching criteria now includes:

- Source and Destination Zone and Host. The direction of traffic is determined by source and destination zone. The same zone cannot be defined as both the source or destination zone.
- User
- Service
- Schedule

To create a Firewall Rule, you should:

- Define matching criteria
- Associate action to the matching criteria
- Attach the threat management policies

For example, now you can:

- Restrict the bandwidth usage to 256kb for the user John every time he logs on from the IP Address FEC2::1
- Restrict the bandwidth usage to 1024kb for the user Mac if he logs on in working hours from the IP Address FEC1::5

The rule page displays list of default and custom firewall rules. All the firewall rules are grouped by its source and destination zone. The page also provides option to add or insert a new rule, update the existing rule, changing the rule order, or delete a rule.

### Viewing Firewall Rules between two Zones

To view the firewall rules for the specific zones, select zones. For example, if you select LAN and WAN, all the Firewall Rules created for LAN zone to WAN zone will be displayed.



Firewall rule controls the traffic flowing through Appliance and are created for a pair of source and destination zone which determines the traffic direction.

Processing of firewall rules is top downwards and the first suitable rule found is applied.

Hence, while adding multiple rules, it is necessary to put specific rules before general rules. Otherwise, a general rule might allow a packet that you specifically have a rule written to deny later in the list. When a packet matches the rule, the packet is immediately dropped or forwarded without being tested by the rest of the rules in the list.

As the firewall rules are grouped source and destination zone wise, rule can be added at the bottom of the list or can be inserted in the group.








- Inserting a Firewall Rule – To insert a rule for a particular source and destination zone click the Insert icon  under the Manage column against a firewall rule for the required source and destination zone. For example, if you have already added a firewall rule for LAN to DMZ zone and want to add another rule for the same zones then click Insert icon against the firewall rule for LAN to DMZ zone. It will add a new firewall rule for the same zones.
- Reordering Firewall Rules – Rules are ordered by their priority. When the rules are applied, they are processed from the top down and the first suitable rule found is applied. Hence, while adding multiple rules, it is necessary to put specific rules before the general rules. Otherwise, a general rule might allow a packet that you specifically have a rule to deny later in the list. When a packet matches the rule, the packet is immediately dropped or forwarded without being tested by the rest of the rules in the list. To change order of the rule, click the Move icon  against the rule whose order is to be changed. Move the rule by dragging and dropping to a required position.
- Clear All Filters – To clear all the search filters applied on the source, destination or identity columns, click the “Clear All Filters” button. This helps in removing filters on multiple columns at a time.
- View Firewall Rules between two Zones – To view Firewall Rules for the selected zones, select zones. For example, if you select LAN and WAN, all the Firewall Rules created for LAN zone to WAN zone will be displayed.



## Manage Firewall Rule List

Firewall Rules control the traffic flowing through Appliance. **Firewall > Rule > IPv6 Rule** page displays a list of Firewall Rules and provides a way to manage rules.

Rules are created for a pair of source and destination zone which determines the traffic direction.

### Icons and their Meaning in Firewall Rule

Icon	Meaning	Appearing under Column
	Firewall rule is enabled and is currently applied to the traffic.	Enable
	Firewall rule is disabled.	Enable
	Firewall rule is enabled but is not currently applied. It will be applied to the traffic as per the time configured in the schedule.	Enable
	Inserts rule before the existing rule.	Manage
	Changes order of the rule.	Manage

ID	Rule Name	Enable	Source	Destination	Service	Action	Identity	Manage
LAN - LAN ( Total 1 )								
3	Test		Any Host	Any Host	Any Service	Accept	-	

Screen – IPv6 Firewall Rule

Screen Element	Description
<b>ID</b>	Firewall Rule ID which is generated automatically at the time of creation.
<b>Rule Name</b>	Firewall Rule name to identify the Firewall Rule.
<b>Enable</b>	Click to activate/deactivate the rule. If you do not want to apply the Firewall Rule temporarily, disable rule instead of deleting.
<b>Source</b>	Source Host to which the rule applies.
<b>Destination</b>	Destination Host to which the rule applies.
<b>Service</b>	Service for which the rule is created.
<b>Action</b>	Displays the action to be taken when the rule matches a connection attempt.
<b>Identity</b>	Displays user or user group on which the firewall rule is applied.

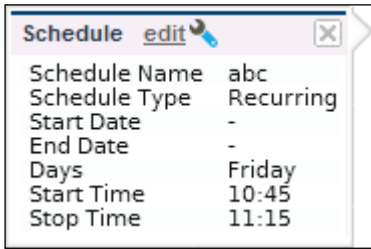

	If Identity is configured, user based policies will be applied to the traffic.
<b>Web Filter</b>	A Web Filter policy to be applied to the traffic.  Point to the policy link to view or edit the policy details.
<b>Application Filter</b>	An Application Filter policy to be applied to the traffic.  Point to the policy link to view or edit the policy details.
<b>NAT</b>	NAT policy to be applied to the traffic.  Point to the policy link to view or edit the policy details.
<b>IPS</b>	IPS policy to be applied to the traffic.
<b>QoS Policy</b>	QoS policy to be applied to the traffic.  Point to the policy link to view or edit the policy details.
<b>AV &amp; AS Scanning</b>	Displays the protocols selected for AV & AS Scanning.
<b>Schedule</b>	A Schedule that controls when the rule should be active.  Point to the schedule link to view or edit the schedule details.  
<b>Logging</b>	Firewall Rule logging.
<b>Description</b>	Firewall Rule Description.
<b>Routing through Gateway</b>	Routing policy applied to the traffic.
<b>Backup Gateway</b>	Backup gateway for the traffic.
<b>Upload Data</b>	Displays total outgoing traffic.
<b>Download Data</b>	Displays total incoming traffic.
<b>DSCP Marking</b>	Displays DSCP value for rule.
<b>Bypass User Accounting</b>	Displays whether Bypass User Accounting is enabled or disabled.

Table - Manage IPv6Firewall Rule screen elements

## Change Firewall Rule Order

Rule Order defines the rule processing priority. When the rules are applied, they are processed from the top down and the first suitable rule found is applied.

Hence, while adding multiple rules, it is necessary to put specific rules before general rules. Otherwise, a general rule might allow a packet that you specifically have a rule written to deny later in the list. When a packet matches the rule, the packet is immediately dropped or forwarded without being tested by the rest of the rules in the list.

Go to **Firewall > Rule > IPv6 Rule**. Click the move rule  against the rule whose order is to be changed.

- Click on the rule to be moved and then drag & drop the rule in the desired order.
- Click close to save the order.

ID	Rule Name	Enable	Source	Destination	Service	Action	Schedule	Manage
VPN - VPN ( Total 3 )								
LAN - WAN ( Total 5 )								
25	testRule		PULL_Request	Any Host	Any Service	Accept	All The Time	
18	Allow_Internet1		Any Host	Any Host	Any Service	Accept	Work hours (5 Day week)	
22	test		PULL_Request	Any Host	Any Service	Accept	abc	
2	#LAN_WAN_LiveUserTraffic		Any Host	Any Host	Any Service	Accept	All The Time	<b>Move</b>
1	#LAN_WAN_AnyTraffic		Any Host	Any Host	Any Service	Accept	All The Time	
VPN - LAN ( Total 2 )								
9	Rule_9		Any Host	Any Host	Any Service	Accept	All The Time	
8	Rule_8		Any Host	Any Host	Any Service	Accept	All The Time	

Name	Source Host	Destination Host	Service	Action
testRule	PULL_Request	Any Host	Any Service	Accept
Allow_Internet1	Any Host	Any Host	Any Service	Accept
test	PULL_Request	Any Host	Any Service	Accept
#LAN_WAN_LiveUserTraffic	Any Host	Any Host	Any Service	Accept
#LAN_WAN_AnyTraffic	Any Host	Any Host	Any Service	Accept

Screen – Move IPv6 Firewall Rule

## IPv6 Firewall Rule Parameters

To add or edit Firewall Rules, go to **Firewall > Rule > IPv6 Rule**. Click the Add button to add a new rule or Edit Icon in the Manage column against the Firewall Rule to modify the details of the rule. Firewall Rule [Parameters](#) are given below.

**General Settings**

**Rule Name**

Name \*

Description

**Basic Settings**

<b>Zone *</b>	Select Source Zone	<b>Destination</b>	Select Destination Zone
Attach Identity	<input type="checkbox"/>		
Network / Host *	Any IP Address		Any IP Address
Services *	Any Services		
Schedule	All The Time		
Action *	<input type="radio"/> Accept <input checked="" type="radio"/> Drop <input type="radio"/> Reject		
<input type="checkbox"/> Apply NAT	Select NAT Policy		

**Advanced Settings (Security Policies, QoS, Routing Policy, Log Traffic)**

**Security Policies**

Application Filter: None  Apply Application based QoS Policy

Web Filter: None  Apply Web Category based QoS Policy

IPS: None

AV & AS Scanning:  SMTP  SMTPS  POP3  IMAP  HTTP  HTTPS

**QoS & Routing Policy**

QoS: None

DSCP Marking: Select DSCP Marking

Route Through Gateway: Load Balance (Applicable only in case of Multiple Gateways)

Backup Gateway: None

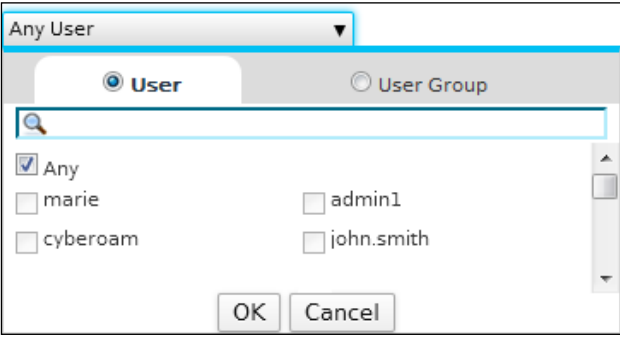
**Log Traffic**

Log Firewall Traffic  Enable

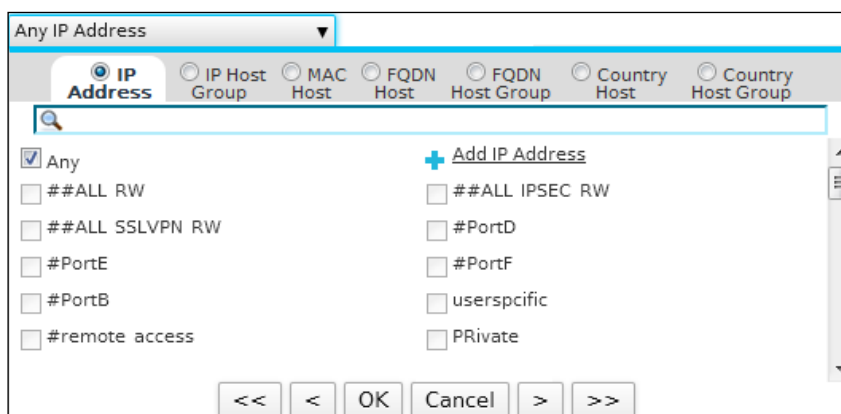
Screen - Add IPv6 Firewall Rule

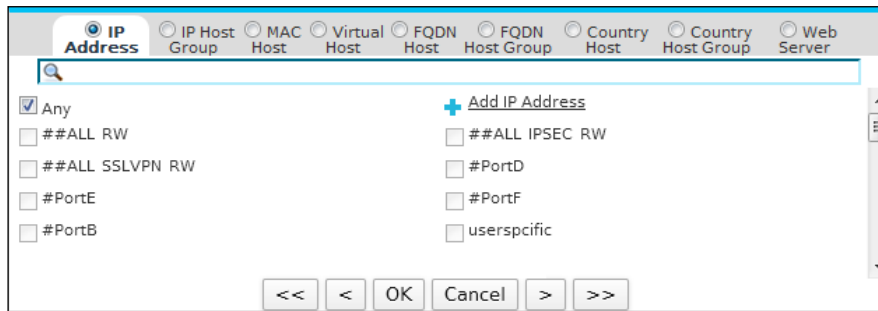
### Parameters

Screen Element	Description
<b>General Settings</b>	
<b>Rule Name</b>	
<b>Name</b>	Specify a name to identify the Firewall Rule.
<b>Description</b>	Provide description for the rule.
<b>Basic Settings</b>	
<b>Zone</b>	Select source and destination zone to which the rule applies.
	<b>Note</b>

	<ul style="list-style-type: none"> <li>• VPN Zone is not available for IPv6.</li> </ul>
<p><b>Attach Identity</b> (Only if source zone is LAN/DMZ/VPN)</p>	<p>Attach identity allows you to check whether the specified user/user group from the selected zone is allowed to access the selected service or not. Click to attach the user identity.</p>  <p>Enable check identity to apply following policies per user:</p> <ul style="list-style-type: none"> <li>• Schedule Access.</li> <li>• IPS (User's IPS policy will be applied automatically but will not be effective till the IPS module is subscribed).</li> <li>• Anti Virus scanning (User's Anti Virus scanning policy is applied automatically but will not be effective till the Gateway Anti Virus module is subscribed).</li> <li>• Anti Spam scanning (User's Anti Spam scanning policy is applied automatically but will not be effective till the Gateway Anti Spam module is subscribed).</li> <li>• QoS policy – User's QoS policy will be applied automatically.</li> <li>• Policy selected in the "Route through Gateway" field is the static routing policy that is applicable only if more than one gateway is defined and used for load balancing.</li> <li>• Limit access to available services.</li> </ul>
<p><b>Identity</b></p>	<p>Select user/user group for the selected zone to allow/deny access the selected service.</p>
<p><b>Exclude traffic from data accounting for selected user(s)</b></p>	<p>By default user's network traffic is considered in data accounting. Select to exclude certain traffic user data accounting. The traffic allowed through this firewall rule will not be accounted towards data transfer for the user.</p> <p>This option is available only if the parameter "Attach Identity" is enabled.</p> <p>This traffic will not be included in the user accounting reports - Internet Usage report and My Account reports, but will be included in the firewall activity reports.</p> <p>Example:</p>

	<p>A User is added from <b>Identity &gt; Users &gt; Users</b></p> <ul style="list-style-type: none"> <li>• User Name – Cyberoam</li> <li>• Maximum Data Transfer limit for User Cyberoam – 100 MB</li> <li>•</li> </ul> <p>An IPv4 Firewall Rule is created</p> <ul style="list-style-type: none"> <li>• Firewall Rule Name – Bypass Data Transfer</li> <li>• Firewall Rule for zones – LAN to WAN</li> <li>• Attached Identity – Enabled (User – Cyberoam)</li> <li>• Bypass User Data Transfer Accounting – Enabled</li> </ul> <p>User Activity</p> <ul style="list-style-type: none"> <li>• The user transfers data in LAN to LAN Zone – 50 MB</li> <li>• The user transfers data in LAN to WAN Zone – 10 MB</li> </ul> <p>Accounted Data Transfer</p> <ul style="list-style-type: none"> <li>• Calculated Total Data Transfer – 50 MB</li> </ul> <p>Reason – Only the data transferred on LAN to LAN zone is considered i.e. 50MB. Data transferred on LAN to WAN Zone i.e. 10 MB is not calculated and bypassed by the Administrator as per the IPv4 Firewall Rule “Bypass Data Transfer”.</p>
<p><b>Network/Host</b></p>	<p>Specify source and destination host or network address to which the rule applies.</p> <p>Host dropdown list also displays MAC based host, dynamic hosts and host groups which are automatically added on creation of VPN Road warrior connections(IPSec and SSL). It will also display the default hosts created for road warrior connection - <code>##ALL_RW</code>, <code>##ALL_IPSEC_RW</code>, <code>##ALL_SSLVPN_RW</code>, <code>##WWAN1</code>(when WWAN is enabled)</p> <p>You can also define a new IP host, IP host group, MAC host, virtual host, FQDN host, FQDN host group, country host, country host group and Web Server directly from this page.</p>





**Services**

Services represent the types of Internet data transmitted via particular protocols or applications.

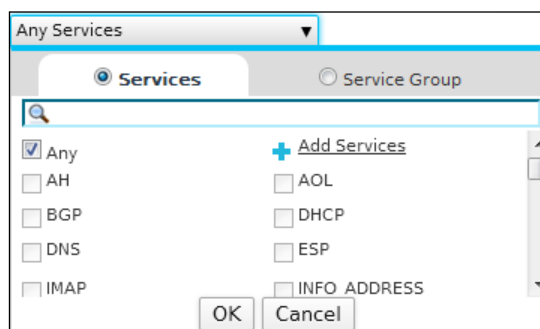
Select Services/Service Group to which the rule applies.

If Virtual host is selected as Destination host, you will be able to configure services only if the selected virtual host is not port forwarded.

You can also add a custom service or service group from this page itself.

Protect by configuring rules to:

- block services at specific zone.
- limit some or all users from accessing certain services
- allow only specific user to communicate using specific service

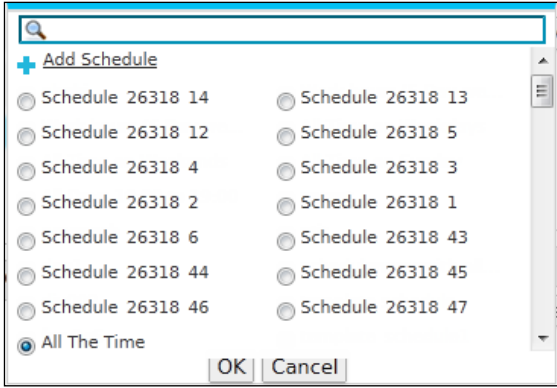


**Schedule**

Select Schedule for the rule.

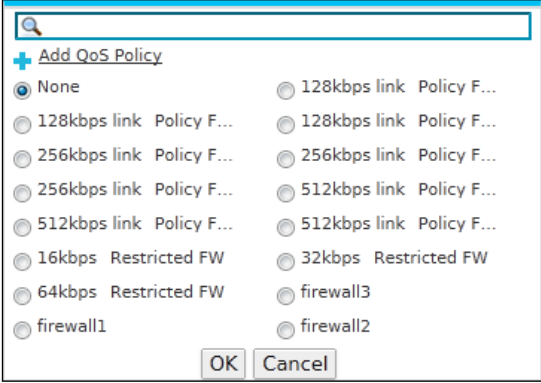
You can also add a new schedule directly from this.



	
<p><b>Action</b></p>	<p>Select rule action.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Accept</b> – Allow access</li> <li>• <b>Drop</b> – Silently discards</li> <li>• <b>Reject</b> – Denies access and “ICMP port unreachable” message will be sent to the source.</li> </ul> <p>When sending response it might be possible that response is sent using a different interface than the one on which request was received. This may happen depending on the Routing configuration done on the Appliance.</p> <p>For Example,</p> <p>If the request is received on the LAN port using a spoofed IP Address (public IP Address or the IP Address not in the LAN zone network) and specific route is not defined, the Appliance will send a response to these hosts using default route. Hence, response will be sent through the WAN port.</p>
<p><b>Apply NAT (Only if Action is ‘ACCEPT’)</b></p>	<p>Enabling “Allow NAT” access is allowed only after replacing the source IP Address with the IP Address specified in the NAT policy.</p> <p>Select the NAT Policy for the Firewall Rule. Traffic from this rule will pass as per the NAT Policy selected for all gateways.</p> <p>By default, MASQ NAT Policy is selected.</p> <p>You can also use the NAT policy configured for the gateway from <b>Network &gt; Gateway &gt; Gateway</b>. All traffic passing from this rule is NATed as per the gateway’s default NAT policy.</p> <p>You can also override this gateway specific NAT policy by selecting a NAT policy. Multiple Gateways and NAT Policy can be added. If enabled the overridden policy is applied instead of gateway’s default NAT policy.</p>

	<p>Select None if NATing is not required for a particular gateway.</p> <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>This option is available if Appliance is deployed as Gateway.</li> </ul> </div>
<p><b>Advanced Settings</b></p> <p>Toggle Drill Down icon – Click to apply different protection settings to the traffic controlled by the firewall.</p> <ul style="list-style-type: none"> <li>Enable load balancing and failover when multiple links are configured. Applicable only if Destination Zone is a WAN.</li> <li>Configure antivirus protection and spam filtering for SMTP, SMTP over SSL, IMAP, POP3, HTTP and HTTPS protocols. To apply antivirus protection and spam filtering, you need to subscribe for Gateway Anti Virus and Gateway Anti Spam modules individually. Refer to the Licensing section for details.</li> <li></li> <li>Implement Intrusion Prevention System. To apply IPS policy you need to subscribe for the Intrusion Prevention System module. Refer to the Licensing section for details.</li> <li>Configure content filtering policies. To apply content filtering you need to subscribe to Web and Application Filter module. Refer to the Licensing section for details.</li> <li>Apply QoS policy</li> </ul>	
<p><b>Security Policies</b></p>	
<p><b>Application Filter</b></p>	<p>Select Application Filter Policy for the rule. Policy is not applicable on incoming traffic (source zone configured as WAN) and Cyberoam destined traffic (destination zone configured as Local).</p> <p>It controls access to application like IM and P2P, VOIP.</p> <p>You can also create a new policy directly from this page and attach to the user.</p>
<p><b>Apply Application Based QoS Policy</b></p>	<p>Click to restrict bandwidth for the applications categorized under the Application category.</p> <p>A three step configuration is required as follows:</p> <ul style="list-style-type: none"> <li>Create QoS policy from QoS &gt; Policy &gt; Policy &gt; Add.</li> <li>Assign above created QoS policy to the Application category from Application Filter. Policy can be assigned to multiple application categories.</li> <li>Enable Application Category based QoS Policy from Firewall Rule.</li> </ul>

	Above configured policy will be applicable only when the application included in the Application Category is accessed.
<b>Web Filter</b>	<p>Select Web Filter Policy for the rule. Policy is not applicable on incoming traffic (source zone configured as WAN) and Cyberoam destined traffic (destination zone configured as Local).</p> <p>It controls web access control and blocks access to inappropriate web sites.</p> <p>You can also create a new policy directly from this page and attach to the user.</p>
<b>Apply Web Category Based QoS Policy</b>	<p>Click to restrict bandwidth for the URLs categorized under the Web category.</p> <p>A three step configuration is required as follows:</p> <ul style="list-style-type: none"> <li>• Create QoS policy from the QoS &gt; Policy &gt; Policy &gt; Add.</li> <li>• Assign above created a QoS policy to the Web category from the Web Filter. Policy can be assigned to the default as well as custom web categories.</li> <li>• Enable Web Category based QoS Policy from IPv4 Firewall Rule.</li> </ul> <p>Above configured policy will be applicable, whenever the URL falling under the Web category is accessed.</p>
<b>IPS</b>	<p>Select IPS policy for the rule.</p> <p>To use IPS, you have to subscribe for the module. Refer to Licensing for more details.</p> <p>You can also create a new policy directly from this page and attach to the user.</p>
<b>AV &amp; AS Scanning</b>	<p>Click the protocol for which the virus and spam scanning is to be enabled.</p> <p>Default - Disable</p> <p>To implement Anti Virus and Anti Spam scanning, you have to subscribe for the Gateway Anti Virus and Anti Spam modules individually. Refer to Licensing for more details.</p>
<b>QoS and Routing Policy</b>	
<b>QoS</b>	<p>Select QoS policy for the rule.</p> <p>QoS policy allocates &amp; limits the maximum bandwidth usage of the user.</p>

	<p>You can also create a new policy directly from this page and attach to the user.</p> 
<p><b>DSCP Marking</b></p>	<p>Select DSCP Marking.</p> <p>DSCP (DiffServ Code Point) classifies flow of packets as they enter the local network depending upon QoS. Flow is defined by 5 elements; Source IP Address, Destination IP Address, Source port, Destination port and the transport protocol.</p> <p>For available options, refer <a href="#">DSCP Values</a>.</p>
<p><b>Route Through Gateway (Available only if Appliance is deployed as Gateway)</b></p>	<p>Select routing policy. Option is available only if more than one gateway is configured.</p>
<p><b>Backup Gateway</b></p>	<p>Specify the backup gateway.</p> <p>The traffic will be routed through the configured gateway in case gateway configured in "Route Through Gateway" goes down.</p> <div data-bbox="699 1384 1390 1512" style="border: 1px solid gray; padding: 5px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>This Option is available only if "Load Balance" is not selected for "Route Through Gateway"</li> </ul> </div>
<p><b>Log Traffic</b></p>	
<p><b>Log Firewall Traffic</b></p>	<p>Click to enable traffic logging for the rule i.e. traffic permitted and denied by the Firewall Rule.</p>

**Table – Add IPv6 Firewall Rule screen elements**

## Virtual Host







Virtual Host maps services of a public IP Address to services of a host in a private network.

A Virtual Host can be a single IP Address or an IP Address range or the Appliance interface itself.

The Appliance will automatically respond to the ARP request received on the WAN zone for the external IP Address of Virtual Host. Default LAN to WAN (Any Host to Any Host) Firewall Rule will allow traffic to flow between the Virtual Host and the network.

The Virtual Host page displays list of all the available virtual hosts. You can filter the list based on IP Family or sort the list based on virtual host name. The page also provides option to add a new virtual host, update the parameters of the existing virtual hosts, or delete a host.

To manage virtual hosts, go to **Firewall > Virtual Host > Virtual Host**.


<input type="button" value="Add"/> <input type="button" value="Delete"/>		<input type="checkbox"/>	Name ▲	Public Address	Mapped Address	Public Port	Mapped Port	IP Family	Manage
<input type="checkbox"/>	<a href="#">BO_RDP_Server</a>	10.103.6.148	172.16.16.10	3389(TCP)	3389(TCP)	IPv4	 		
<input type="checkbox"/>	<a href="#">Virtual Host</a>	10.10.1.1	3.3.3.3			 	 		

Screen – Manage Virtual Host

Screen Element	Description
<b>Name</b>	Displays the name of Virtual Host.
<b>Public Address</b>	Public IP Address through which Internet users access internal Server/host.
<b>Mapped Address</b>	Mapped IP Address type is the IP Address of the internal server/host.
<b>Public Port</b>	Public port used when Port Forwarding is configured.
<b>Mapped Port</b>	The Mapped port number on destination network when Port Forwarding is enabled.
<b>IP Family</b>	Displays the IP Family – IPv4 or IPv6.

Table – Manage Virtual host screen elements

### Virtual Host Parameters

To add or edit a virtual host, go to **Firewall > Virtual Host → Virtual Host**. Click the Add button to add a new virtual host. To update the details, click on the virtual host or Edit icon  in the Manage column against the host that you want to modify.

**General Settings**

**Basic Settings**

Name \*

Description

IP Family \*  IPv4  IPv6

External IP \*

Mapped IP \*

Physical Zone \*

**Port Forwarding**

Enable Port Forwarding

Protocol \*  TCP  UDP

External Port Type \*  Port  Port Range  Port List

External Port \*  -

Mapped Port Type \*  Port  Port Range  Port List

Mapped Port \*  -

**Advanced Settings**

Enable Load Balancing

Method \*

Enable Health Check (For failover)

Health Check Method  TCP Probe  ICMP Probe

Port \*  (Range:1 - 65535)

Interval \*  Seconds

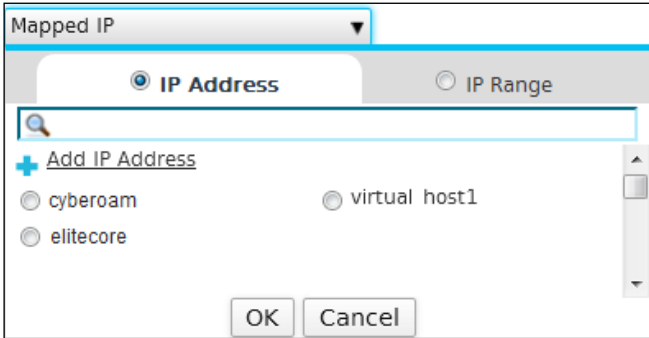
Timeout \*  Seconds

Retries \*

Screen – Add Virtual host

Screen Element	Description
<b>General Settings</b>	
<b>Basic Settings</b>	
<b>Name</b>	Specify a name to identify the Virtual Host.
<b>Description</b>	Provide description for the Virtual Host.
<b>IP Family</b>	Select the IP Family to create the Virtual Host  Available Options: <ul style="list-style-type: none"> <li>• <b>IPv4</b> – A virtual host configured for this option must have IPv4 IP Address for both, external IP Address(s) and mapped IP Address(s).</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>IPv6</b> – A virtual host configured for this option must have IPv6 IP Address for both, external IP Address(s) and mapped IP Address(s).</li> </ul> <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• External IP Address and Mapped IP Address of a virtual host must be of the same IP Family.</li> </ul> </div>
<p><b>External IP</b></p>	<p>External IP Address is the IP Address through which Internet users access internal server/host.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>IP Address</b> – Specified IP Address is mapped to a corresponding mapped single or range of IP Address. If single IP Address is mapped to a range of IP Address, Appliance uses round robin algorithm to load balance the requests.</li> <li>• <b>IP Range</b> – Specified IP Address range is mapped to a corresponding range of mapped IP Address. The IP range defines the start and end of an address range. The start of the range must be lower than the end of the range.</li> <li>• <b>Interface IP</b> – Select when any of the Appliance Port, Alias or Virtual LAN (VLAN) sub-interface is required to be mapped to the destination host or network.</li> <li>• This option is only available for IPv4 family.</li> </ul> <p>If “IP Address” or “IP Range” option is selected, Appliance automatically responds to the ARP request received on the WAN zone for the external IP Address.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>External IP <span style="float: right;">▼</span></p> <p><input checked="" type="radio"/> <b>Interface IP</b>    <input type="radio"/> IP Address    <input type="radio"/> IP Range</p> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;"> <input type="text"/> </div> <p> <input type="radio"/> #PortD-Disconnected    <input type="radio"/> #PortE-Disconnected  <input type="radio"/> #PortC-10.10.1.1    <input type="radio"/> #PortB-10.103.6.148  <input type="radio"/> #PortA-172.16.16.16 </p> <p style="text-align: right;"> <input type="button" value="OK"/>    <input type="button" value="Cancel"/> </p> </div> <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• If the IPv4 Family is selected, only IPv4 Address will be available for configuration.</li> <li>• If the IPv6 Family is selected, only IPv6 Address will be available for configuration.</li> </ul> </div>
<p><b>Mapped IP</b></p>	<p>Mapped IP is the IP Address to which the external IP Address is mapped. This is the actual private IP Address of the host being accessed using the Virtual Host.</p>

	<p>Mapped IP Address is the IP Address of the internal server/host.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>IP Address</b> – External IP Address is mapped to the specified IP Address.</li> <li>• <b>IP Range</b> – External IP Address Range is mapped to the specified IP Address Range.</li> <li>• <b>IP List</b> – External IP Address is mapped to the specified IP list.</li> <li>• <b>FQDN</b> – External IP Address is mapped to the specified FQDN. Internal mapped server can be accessed by FQDN.</li> <li>• This option is only available for IPv4 Virtual Host.</li> <li>•</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• All the mapped servers must be bound to the same zone..</li> <li>•</li> </ul>
<p><b>Physical Zone</b></p>	<p>LAN, WAN, DMZ, VPN or custom zone of the mapped IP Addresses. For example, if mapped IP Address represents any internal server then the zone in which server resides physically.</p> <p>Default – LAN Zone</p>  <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• VPN zone is not supported for IPv6.</li> </ul>
<p><b>Port Forwarding</b></p>	
<p><b>Enable Port Forwarding</b></p>	<p>Click to enable service port forwarding.</p> <p>Protocol – Select the protocol TCP or UDP that you want the forwarded packets to use.</p> <p>External Port Type – Select the type of external port from the available options:</p>



	<p>Available Options:</p> <ul style="list-style-type: none"> <li>• Port</li> <li>• Port Range</li> <li>• Port List</li> </ul> <p>External Port – Select the public port number for which you want to configure port forwarding.</p> <p>Mapped Port Type – Select the type of mapped port from the available options:</p> <p>Available Options:</p> <ul style="list-style-type: none"> <li>• Port</li> <li>• Port Range</li> <li>• Port List</li> </ul> <p>Mapped Port – Specify mapped port number on the destination network to which the public port number is mapped..</p>
<b>Advanced Settings</b>	
<p><b>Enable Load Balancing</b> Click to enable load balancing.</p> <p>This option is available if incoming traffic is to be distributed to more than one internal server (Mapping of single “External Port” to multiple “Mapped Ports”).</p>	
<p><b>Method</b></p>	<p>Select the method for load balancing from the available options.</p> <p>Available Options:</p> <ul style="list-style-type: none"> <li>• <b>Round Robin</b> - In this method, requests are served in a sequential manner where the first request is forwarded to the first server, second request to the second server and so on. When a request is received, Cyberoam checks to see which the last server that was assigned a request was. It then assigns this new request to the next available server. This method is can be used when equal distribution of traffic is required and there is no need for session-persistence.</li> <li>• <b>First Alive</b> - In this method, all incoming requests are served by the first server (the first IP Address that is configured in the IP Range). This server is considered as the primary server and all others are considered as backup. Only when the first server fails, the requests are forwarded to the next server in line. This method is used for failover scenarios.</li> <li>• <b>Random</b> - In this method, the requests are forwarded to the servers randomly. Although, Cyberoam makes sure that all configured servers receive equally distributed load. Hence, this method is also called uniform random distribution. This method can be used when equal distribution of traffic is required and there is no need for session-persistence or order of distribution.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Sticky IP</b> - In this method, Along with Round Robin distribution of traffic, Cyberoam forwards incoming traffic according to the Source IP Address. All traffic from a particular source is forwarded only to its mapped Server. This means that all requests for a given source IP are sent to the same application server instance. This method is useful in cases where all requests or sessions are required to be processed by the same server. For example: Banking websites, E-Commerce websites.</li> </ul>
<p><b>Enable Health Check (For failover)</b> Click to enable checking for failover.</p> <p>This option is available only if Load Balancing is enabled.</p>	
<b>Health Check Method</b>	<p>Select the method to check the health of the server from the available options.</p> <p>Available Options:</p> <ul style="list-style-type: none"> <li>• TCP Probe</li> <li>• ICMP Probe</li> </ul>
<b>Port</b>	<p>Specify the Port number on the server health is monitored.</p> <p>Acceptable Range: 1 - 65535</p> <p>This option is available only if TCP Probe Health Check Method is selected.</p>
<b>Interval</b>	<p>Specify the time interval in seconds after which the health will be monitored.</p> <p>Acceptable Range (Seconds): 5 – 65535</p> <p>Default - 60 seconds.</p>
<b>Timeout</b>	<p>Specify the time interval in seconds within which the server must respond.</p> <p>Timeout (Seconds): 1 – 10</p> <p>Default - 2 Seconds</p>
<b>Retries</b>	<p>Specify the number of tries to probe the health of the server, after which the server will be declared unreachable</p> <p>Retries Range: 1 – 10</p> <p>Default – 3</p>

Table – Add Virtual host screen elements

**Note**

- Deleting Virtual host will remove all its dependent configurations including:
- Interface-Zone binding
- DHCP Server or Relay
- Alias based Firewall Rules
- ARP – Static & Proxy
- Virtual Hosts and Virtual Host based Firewall Rules
- Interface based Hosts and reference from Host Groups
- Routes – Unicast, Multicast

Once the virtual host is added, you can add a firewall rule for it at the same time or later from the firewall page

Once the Virtual Host is created successfully, Appliance automatically creates a loopback Firewall Rule for the zone of the mapped IP Address. For example, if Virtual Host is created for the LAN mapped IP zone then LAN to LAN Firewall Rule is created for the Virtual Host. Firewall Rule is created for the service specified in Virtual Host. If port forwarding is not enabled in Virtual Host then Firewall Rule with “All Services” is created. Verify the creation of loopback rule from Firewall page.

For Appliance to reply to the ARP requests received on any other zones than WAN zone for External IP Address, create proxy ARP from Appliance Console option of CLI Console.

#### Virtual hosts have following restrictions:

- Virtual Host name cannot be same as host or host group name.
- External IP Address range cannot be mapped with the single Mapped IP Address.
- The number of IP Addresses in mapped External address range and Mapped IP Address range must be same.
- The number of port in mapped External ports range and Mapped port range must be same.
- Virtual Host with the same pair of External IP and Port cannot be created.
- Different Virtual Hosts can have same External IP Address only if port forwarding is enabled for different public port. For example,

```
Virtual_host1
External IP Address – 192.168.1.1/ FEC0::1
Mapped IP Address – 10.10.10.12/ FEC1::1
Port forward – External port – 25
Mapped port – 35
Virtual_host2
External IP Address – 192.168.1.1/ FEC0::1
Mapped IP Address – 10.10.10.1 /FEC2::1
Port forward – External port – 42
Mapped port – 48
```

- Different Virtual Hosts cannot have same External IP Address, if port forwarding is enabled in one Virtual Host and disabled in another Virtual Host. For example, Appliance will not allow you the creation of:

```
Virtual_host1
External IP Address – 192.168.1.15/FEC0::1
Mapped IP Address – 10.10.10.1/FEC1::1
Virtual_host2
External IP Address – 192.168.1.15/FEC0::1
```

Mapped IP Address – 10.10.10.2/FEC2::1  
 Port forward – External port – 42  
 Mapped port – 48

- Virtual Host cannot be created with overlapping IP Address. For example, Appliance will not allow you to create:

Virtual\_host1  
 External IP Address – 192.168.1.15-192.168.1.20/FEC0::1 - FEC0::5  
 Mapped IP Address – 10.10.10.15-10.10.10.20/FEC1::1 – FEC1::5  
 Virtual\_host2  
 External IP Address – **192.168.1.18/FEC0::3**  
 Mapped IP Address – 10.10.10.18/FEC2::1

- Virtual Host cannot be created with overlapping ports. For example, Appliance will not allow you to create:

Virtual\_host1  
 External IP Address – 192.168.1.15/FEC0::1  
 Mapped IP Address – 10.10.10.1/FEC1::1  
 Port forward - External port – **20-80**  
 Mapped port – 20-80  
 Virtual\_host2  
 External IP Address -- 192.168.1.15/FEC0::1  
 Mapped IP Address – 10.10.10.2/FEC2::1  
 Port forward – External port – **25**  
 Mapped port – 25

## Adding a Firewall Rule for Virtual Host list

Once the virtual host is added, you can add a firewall rule for it at the same time or later from the firewall page. Below given parameters can be configured if you add the firewall rule at the time of adding virtual host.

**Add Firewall Rules For Virtual Host** x

Virtual Host " WebServers" is successfully created.  
 Do you want to allow access to "WebServers" from a particular zone?  
 Add a firewall rule for each source zone from which you want to allow access to this virtual host.

Add Firewall Rule(s) For Virtual Host

Firewall Rule Name	Source Zone	Service	Apply NAT	AV & AS Scanning	Log Traffic	Create Reflexive Rule	+
#WebServers_Auto1	WAN	#WebServers	None	None	No	Yes	

Screen – Firewall Rule for Virtual Host

Screen Element	Description
<b>Add Firewall Rule(s) For Virtual Host</b>	Enable to add a Firewall Rule(s) once the Virtual Host is configured.
<b>Firewall Rule Name</b>	Name of Firewall Rule for the configured Virtual Host.

<b>Source Zone</b>	Select a Source Zone.
<b>Service</b>	A service for which the rule is created.  If port forwarding is enabled then services for that virtual host is uneditable.
<b>Apply NAT</b>	Select the NAT policy to be applied.  It allows access after replacing the source IP Address to the IP Address specified in the NAT policy.
<b>AV &amp; AS Scanning</b>	Select the protocol for which the virus and spam scanning is to be enabled.  To implement Anti Virus and Anti Spam scanning, you have to subscribe for the Gateway Anti Virus and Anti Spam modules individually. Refer to Licensing for more details.
<b>Log Traffic</b>	Select Yes to enable logging of traffic permitted and denied by the Firewall Rule.
<b>Create Reflexive Rule</b>	Select Yes to automatically create a reflexive firewall rule for the Virtual Host.  Reflexive rule has same firewall rule policies as those configured for the virtual host but instead of source zone to destination zone, this rule is applicable on traffic from destination zone to source zone.  Consider a Mail server deployed in LAN. To publish internal Mail server, a virtual host is created for WAN to LAN zone. The traffic traverses from Public Internet to internal Server using the created virtual host. On creating virtual host, firewall rules can be configured for inbound traffic. If selected to create a reflexive rule, a firewall rule is automatically created for outbound traffic LAN to WAN zone with same policies applied for WAN to LAN zone. All the outbound traffic like email sent passes from reflexive rule  By default, the reflexive rule is not created.
<b>Add Firewall Rule(s) For Virtual Host</b>	Enable to add a Firewall Rule(s) once the Virtual Host is configured.
<b>Firewall Rule Name</b>	Name of Firewall Rule for the configured Virtual Host.
<b>Source Zone</b>	Select a Source Zone.

Table – Firewall Rule for Virtual Host screen elements

## NAT Policy

Network Address Translation (NAT) is the process of rewriting the source addresses of IP packets as they pass through a router or Firewall. Mostly NAT is used to enable multiple hosts on a private network to access the Internet using a single public IP Address. When a client sends an IP packet to the router, NAT translates the sending address to a different, public IP Address before forwarding the packet to the Internet. When a response packet is received, NAT translates the public address into the original address and forwards it to the client.

NAT policy tells Firewall Rule to allow access but only after changing source IP Address i.e. source IP Address is substituted by the IP Address specified in the NAT policy.



Use NAT to change or remap source or destination address of the packet.

Using NAT eliminates the need for public IP Addresses for all computers on your LAN. It is a way to conserve IP Addresses available from the pool of Public IP Addresses for the Internet. NAT also allows you to conceal the addressing scheme of your network.

The NAT Policy page displays the list of all the NAT policies and you can sort the list based on policy name. The page also provides options to add a new policy, update the parameters of the existing policy, or delete a policy.

### Manage NAT Policy list

To manage NAT policies, go to **Firewall > NAT Policy > NAT Policy**.

Add Delete			
<input type="checkbox"/> Name	IP Family	IP Mapped To	Manage
<input type="checkbox"/> MASQ		MASQUERADE	
<input type="checkbox"/> NAT1	IPv4	User1 (10.202.22.9)	 


Add Delete

Screen – Manage NAT Policy

Screen Element	Description
<b>Name</b>	Displays name of the NAT Policy.
<b>IP Family</b>	Displays the IP Family – IPv4 or IPv6.
<b>IP Mapped To</b>	Source IP/Range is replaced with the specified IP/Range.

Table – Manage NAT Policy screen elements

### NAT Policy Parameters

To add or edit NAT policies, go to **Firewall > NAT Policy**. Click the Add button to add a new policy. To update the details, click on the Policy or Edit icon  in the Manage column against the policy you want to modify.

Screen – Add NAT Policy

Screen Element	Description
<b>Name</b>	Specify a name to identify the NAT Policy.
<b>IP Address</b>	<p>Select IP Address for Source Typo.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>IP Address</b> – It replaces source IP Address with the specified IP Address</li> <li>• <b>IP Range</b> – It replaces source IP Address with any of the IP Address from the specified range</li> </ul> <p>You can search and select a particular IP Address based on the Host name. If IP Host or range is not already added, it can be added from here itself or can be added from <b>Objects &gt; Hosts &gt; IP Hosts</b>.</p>

Table – Add NAT Policy screen elements

**Note**

- MASQ is a default policy and cannot be updated or deleted.

## Spoof Prevention

You can configure MAC and/or IP Address pair entry in the IP-MAC trusted list to improve the security of your network. Using MAC Address filtering makes it more difficult for a hacker to guess and use a random MAC Address or spoof a MAC Address to gain access to your network as the traffic does not even reach your Firewall.

Similarly, it is also possible to filter packets based on IP-MAC pair. It prevents hosts which try to violate trusted IP-MAC. To make the restriction more granular, one can enable over zones.

- [General Settings](#)
- [Trusted MAC](#)

### Configuring Spoof Prevention Settings

To enable Spoof Prevention for LAN, WAN and DMZ zones go to **Firewall > Spoof Prevention > General Settings**.

If enabled, the Appliance provides 3 ways to prevent spoofing using IP-MAC trusted list:

- **IP Spoofing** – Packets will be dropped if matching route entry is not available.
- **MAC Filter** – Packets will be dropped if the MAC Addresses are not configured in the “Trusted MAC” list.
- **IP-MAC Pair Filter** – Packets will be dropped if IP and MAC do not match with any entry in the IP-MAC trusted list.

Enable “Restrict Unknown IP on Trusted MAC” if you want to drop traffic from any IP Address not in the trusted list for the trusted MAC Address.

By default, it is disabled. When disabled, traffic from any IP Address not in the trusted list will be allowed even if it is coming from the trusted MAC Address. It is enabled automatically when Spoof Prevention is enabled.

Enable Spoof Prevention

Restrict Unknown IP on Trusted MAC

	IP Spoofing	MAC Filter	IP-MAC Pair Filter
LAN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WAN		<input type="checkbox"/>	
DMZ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Screen – General Settings

Zone	LAN	WAN	DMZ
------	-----	-----	-----



<p><b>IP Spoofing</b></p> <p>If enabled:</p> <ul style="list-style-type: none"> <li>• Enable at least for one zone</li> <li>• The Appliance will reverse lookup for the route of source network and if not available, packets will be dropped and logged.</li> </ul> <p>By default, it is not enabled for any zone.</p>	Yes	No	Yes
<p><b>MAC Filter</b></p> <ul style="list-style-type: none"> <li>• It restricts the access of your network to the external hosts. As the Appliance will drop all the requests from the MAC Address not configured in the trusted list, please make sure to include MAC Addresses of all your internal devices.</li> <li>• If enabled, it is to be enabled for at least one zone.</li> </ul> <p>By default, it is not enabled for any zone.</p>	Yes	Yes	Yes
<p><b>IP-MAC Pair Filter</b></p> <p>Appliance will drop the request considering it as a spoofed request if:</p> <ul style="list-style-type: none"> <li>• MAC Address differs for the trusted IP Address</li> <li>• IP Address differs for the trusted MAC Address</li> </ul> <p>But, the request will be allowed if IP or MAC Address does not exist at all in the list. Request is dropped if IP-MAC pair does not exist in the trusted list.</p> <ul style="list-style-type: none"> <li>• If enabled, it is to be enabled for at least one zone.</li> </ul> <p>By default, it is not enabled for any zone.</p>	Yes	No	Yes

Table – General Settings

## Trusted MAC

You can enable MAC Address and/or IP Address pair filtering to improve security. By enabling filtering, you define the devices that can access your network. It is also possible to import the trusted MAC list through CSV (Comma Separated Value) file. When a user attempts to access the network, the Appliance checks the MAC Address and/or IP Address from the list. User gets access to the network only if the MAC Address and/or IP Address is on the trusted MAC list else the request is rejected.

### Manage Trusted MAC list

The Trusted MAC page displays list of all the MAC addresses configured as trusted MAC. The page also provides option to add a new MAC address, update the existing addresses, and import the list of addresses.

To manage Trusted MAC list, go to **Firewall > Spoof Prevention > Trusted MAC**.

<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Import"/>						
<input type="checkbox"/>	MAC Address	IPv4 Association	IPv4 Address	IPv6 Association	IPv6 Address	Manage
<input type="checkbox"/>	00:1B:63:84:45:E6	DHCP	-	DHCP	-	
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Import"/>						

Screen – Manage Trusted MAC list

Screen Element	Description
<b>Import Button</b>	Import a Trusted MAC.
<b>MAC Address</b>	MAC Address of the user.
<b>IPv4 Association</b>	Displays the type of IP Association selected: Static, DHCP or None.
<b>IPv4 Address</b>	IPv4 Address bound to MAC Address, incase of static IP association.
<b>IPv6 Association</b>	Displays the type of IP Association selected: Static, DHCP or None.
<b>IPv6 Address</b>	IPv6 Address bound to MAC Address, incase of static IP association.

Table – Manage Trusted MAC screen elements

## Trusted MAC Parameters

To add Trusted MAC list, go to **Firewall > Spoof Prevention > Trusted MAC**. Click the Add button to add a Trusted MAC.

Screen – Add Trusted MAC list

Screen Element	Description
<b>MAC Address</b>	Specify the MAC Address to be added to a Trusted MAC list.
<b>IPv4 Address</b>	<p>Specify the IPv4 Address to bind with the MAC Address. Packets will be rejected if either MAC or IPv4 Address does not match.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Static</b> – IP Address to bind to the MAC Address. Packets will be rejected if either MAC or IP Address does not match. Multiple IP Addresses separated by comma can be provided.</li> <li>• <b>DHCP</b> – MAC Address will be bind to the IP Address leased by the Appliance DHCP server as and when the IP is leased. Entry will be updated automatically when the leased IP Address is updated.</li> <li>•</li> </ul> <p>To unbind IPv4 Address, select “None”.</p>
<b>IPv6 Address</b>	<p>Specify the IPv6 Address to bind with the MAC Address. Packets will be rejected if either MAC or IPv6 Address does not match.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Static</b> – IP Address to be bound to the MAC Address. Packets will be rejected if either MAC or IP Address does</li> </ul>

	<p>not match. Multiple IP Addresses separated by comma can be provided.</p> <ul style="list-style-type: none"> <li>• <b>DHCP</b> – MAC Address will be bind to the IP Address leased by the Appliance DHCP server as and when the IP is leased. Entry will be updated automatically when the leased IP Address is updated.</li> <li>•</li> </ul> <p>To unbind IPv6 Address, select “None”.</p>
--	--

**Table – Add Trusted MAC list**

### Import Trusted MAC Address

Instead of adding the trusted entries individually, Appliance provides a facility to import the trusted list from a CSV (Comma Separated Value) file. Click the Import button to import a CSV file. The format for the CSV file should be as follows:

First row of the CSV file has to be the header row: MAC Address, IP Association, IP Address

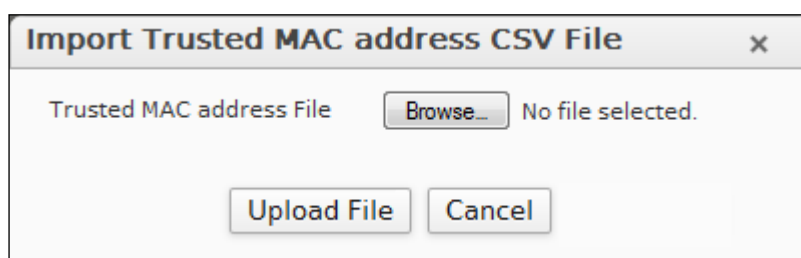
The rest of the rows are values corresponding to the header fields

Blank rows will be ignored

Error Message is displayed only for invalid rows

Format of values:

- Compulsory fields: MAC Address and IP Association
- Optional fields: IP Address
- IP Association must be Static or DHCP or None
- For Static IP Association, IP Address must be available
- For None/DHCP type of IP Association, IP-Address is not required
- For Invalid MAC/IP Address or IP Association entry will be discarded
- Use comma to insert multiple static IP Addresses



**Screen – Import Trusted MAC Address**

## DoS

The Appliance provides several security options that cannot be defined by the Firewall Rules. This includes protection from several kinds of “Denial of Service attacks”. These attacks disable computers and circumvent security.

Denial of Service (DoS) attack is a method that hackers use to prevent or deny legitimate users access to a service.

DoS attacks are typically executed by sending many request packets to a targeted server (usually Web, FTP, or Mail server), which floods the server's resources, making the system unusable. Their goal is not to steal the information but disable or deprive a device or network so that users no longer have access to the network services/resources.

All servers can handle traffic volume up to a limit, beyond which they become disabled. Hence, attackers send a very high volume of redundant traffic to a system so it cannot examine and allow permitted network traffic. Best way to protect against the DoS attack is to identify and block such redundant traffic.

### Packet rate per Source

Total number of connections or packets allowed to a particular user.

### Burst rate per Source

Maximum number of packets allowed to a particular user at a given time.

### Packet rate per Destination

Total number of connections or packets allowed from a particular user.

### Packet rate per Destination

Maximum number of packets allowed from a particular user at a given time.

## How it works

When the burst rate is crossed, the Appliance considers it as an attack. The Appliance provides DoS attack protection by dropping all the excess packets from the particular source/destination. It will continue to drop the packets till the attack subsides. Because the Appliance applies threshold value per IP Address, traffic from the particular source/destination will only be dropped while the rest of the network traffic will not be dropped at all i.e. traffic from the remaining IP Addresses will not be affected at all.

Time taken to re-allow traffic from the blocked source/destination = time taken to subside the attack + 30 seconds

**For example,**

Packet rate per Source – 100 packets per second

Burst rate per Source – 200 packets per second

.Initially, the user will be able to send 200 packets per second. However once these 200 packets are received, the user the user will only be allowed to send 100 packets per second. So in the next phase, if the user sends 150 packets per second, the Appliance will consider it as an attack and drop the last 50 (101-150) packets and will only accept traffic from that user 30 seconds after the time that it dropped the first packet.

**Threshold values**

The Appliance uses packet rate and burst rate values as a threshold value to detect DoS attack. These values depend on various factors like:

- Network bandwidth
- Nature of traffic
- Capacity of servers in the network

These values are applicable to the individual source or destination i.e. requests per user/IP Address and not globally to the entire network traffic. For example, if source rate is 2500 packets/minute and the network consists of 100 users then each user is allowed packet rate of 2500 packets per minute.

Configuring high values will degrade the performance and too low values will block the regular requests. Hence it is very important to configure appropriate values for both source and destination IP Address.

- [Settings](#)
- [Bypass Rules](#)

## Settings

Define the attack definition from **Firewall > DoS > Settings**

(Attack definition can be defined both for source and destination)

Attack Type	Source				Destination			
	Packet rate per Source (Packet/min)	Burst rate per Source (Packet/sec)	Apply Flag	Source Traffic Dropped	Packet rate per Destination (Packet/min)	Burst rate per Destination (Packet/sec)	Apply Flag	Destination Traffic Dropped
SYN Flood	<input type="text" value="12000"/>	<input type="text" value="100"/>	<input type="checkbox"/>	0	<input type="text" value="12000"/>	<input type="text" value="100"/>	<input type="checkbox"/>	0
UDP Flood	<input type="text" value="12000"/>	<input type="text" value="100"/>	<input type="checkbox"/>	0	<input type="text" value="18000"/>	<input type="text" value="100"/>	<input type="checkbox"/>	0
TCP Flood	<input type="text" value="12000"/>	<input type="text" value="100"/>	<input type="checkbox"/>	0	<input type="text" value="12000"/>	<input type="text" value="100"/>	<input type="checkbox"/>	0
ICMP/ICMPv6 Flood	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="checkbox"/>	0	<input type="text" value="300"/>	<input type="text" value="100"/>	<input type="checkbox"/>	0
Dropped Source Routed Packets	-	-	-	-	-	-	<input checked="" type="checkbox"/>	-
Disable ICMP/ICMPv6 Redirect Packet	-	-	-	-	-	-	<input checked="" type="checkbox"/>	-
Disable ARP Flooding	-	-	-	0	-	-	<input type="checkbox"/>	-

Screen – DoS Settings

## Parameters

Screen Element	Description
<b>SYN Flood</b>	<p>Configure Packet Rate (packets/minute) and Burst Rate (packets/second) for source and destination.</p> <p>Click “Apply Flag” checkbox to apply the SYN flood definition and control allowed number of packets.</p> <p>Source Traffic Dropped displays number of source packets dropped in case source packet rate control is applied.</p> <p>Destination Traffic Dropped displays number of packets dropped in case destination packet rate control is applied.</p> <p>Click “SYN Flood” to view the real-time updates on flooding. It displays the source IP Address - which was used for flooding and IP Address which was targeted.</p> <p>SYN Flood is the attack in which large numbers of connections are sent so that the backlog queue overflows. The connection is created when the victim host receives a connection request and allocates for it some memory resources. A SYN flood attack creates so many half-open connections that the system becomes overwhelmed and cannot handle incoming requests any more.</p>
<b>UDP Flood</b>	<p>Configure Packet Rate (packets/minute) and Burst Rate (packets/second) for source and destination.</p>

	<p>Click “Apply Flag” checkbox to apply the UDP flood definition and control the allowed number of packets.</p> <p>Source Traffic Dropped displays number of source packets dropped in case source packet rate control is applied.</p> <p>Destination Traffic Dropped displays number of packets dropped in case destination packet rate control is applied.</p> <p>Click ‘UDP Flood’ to view the real time updates on flooding. It displays the source IP Address - which was used for flooding and IP Address which was targeted.</p> <p>User Datagram Protocol (UDP) Flood links two systems. It hooks up one system’s UDP character-generating service, with another system’s UDP echo service. Once the link is made, the two systems are tied up exchanging a flood of meaningless data.</p>
<p><b>TCP Flood</b></p>	<p>Configure Packet Rate (packets/minute) and Burst Rate (packets/second) for source and destination.</p> <p>Click “Apply Flag” checkbox to apply the TCP flood definition and control the allowed number of packets.</p> <p>Source Traffic Dropped displays number of source packets dropped in case source packet rate control is applied.</p> <p>Destination Traffic Dropped displays number of packets dropped in case destination packet rate control is applied.</p> <p>TCP attack sends huge amount of TCP packet so that the host/victim computer cannot handle.</p>
<p><b>ICMP/ICMPv6 Flood</b></p>	<p>Configure Packet Rate (packets/minute) and Burst Rate (packets/second) for source and destination.</p> <p>Click “Apply Flag” checkbox to apply the ICMP/ICMPv6 flood definition and control allowed number of packets.</p> <p>Click “ICMP/ICMPv6 Flood” to view the real time updates on flooding. It displays the source IP Address - which was used for flooding and IP Address which was targeted.</p> <p>ICMP/ICMPv6 attack sends huge amount of packet/traffic so that the protocol implementation of the host/victim computer cannot handle.</p>



<b>Dropped Source Routed Packets</b>	Click “Apply Flag” checkbox to enable. This will block any source routed connections or any packets with internal address from entering your network.
<b>Disable ICMP Redirect Packet</b>	An ICMP redirect packet is used by routers to inform the hosts what the correct route should be. If an attacker is able to forge ICMP redirect packets, he or she can alter the routing tables on the host and possibly weaken the security of the host by causing traffic to flow via another path.
<b>Disable ARP Flooding</b>	Click “Disable ARP Flooding” to drop invalid ARP request.  ARP attack sends ARP requests at a very high rate to the server. Because of this, server is overloaded with requests and will not be able to respond to the valid requests. Appliance protects by dropping such invalid ARP requests.

**Table – DoS Settings screen elements**

## Bypass Rules

The Appliance allows you to bypass the DoS rule in case you are sure that the specified source will not be used for flooding or ignore if flooding occurs from the specified source. By default, VPN zone traffic is also subjected to DoS inspection. You can also bypass DoS inspection of the traffic coming from certain hosts of VPN zone.

### Manage DoS Bypass Rule List

To manage Bypass Rules, go to **Firewall > DoS > Bypass Rules**.

The DoS Bypass Rule page displays the list of all the bypass rule(s). You can filter the list based on IP Family. The page provides option to add a new rule, update the existing rule, or delete a rule.


<input type="button" value="Add"/>		<input type="button" value="Delete"/>					
<input type="checkbox"/>	Source IP	Source Port	Destination IP	Destination Port	Protocol	IP Family	Manage
<input type="checkbox"/>	<u>192.168.1.1</u>	80	172.16.16.16	81	TCP	IPv4	
<input type="button" value="Add"/>		<input type="button" value="Delete"/>					

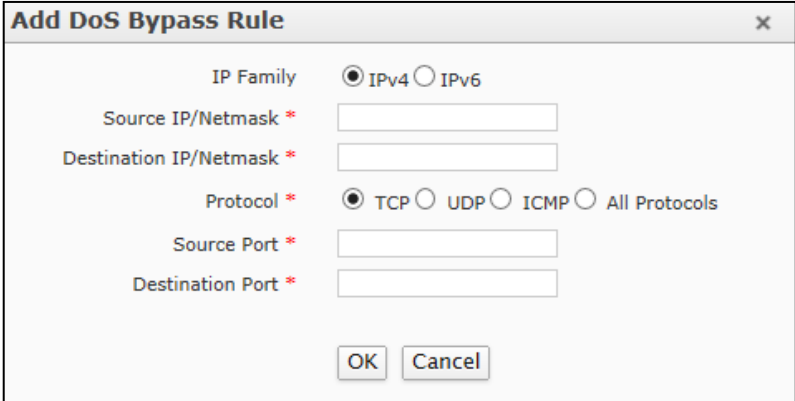
Screen – Manage DoS Bypass Rules

Screen Element	Description
Source IP	Source IP/Netmask to be bypassed.
Source Port	Source Port Number to be bypassed.
Destination IP	Destination IP/Netmask to be bypassed.
Destination Port	Destination Port Number to be bypassed.
Protocol	Protocols to be bypassed.
IP Family	Displays the IP Family – IPv4 or IPv6.

Table – Manage DoS Bypass rule screen elements

## DoS Bypass Rule Parameters

To add or edit a DoS Bypass Rule, go to **Firewall > DoS > Bypass Rules**. Click the Add button to add a new rule. To update the details, click on the Rule or Edit icon  in the Manage column against the rule you want to modify.



Screen – Add Bypass Rule

Screen Element	Description
<b>IP Family</b>	Select the IP Family to configure a DoS Bypass Rule.
<b>Source IP/Netmask (only IPv4)</b>	Specify Source IP/Netmask. Specify * if you want to bypass entire network.
<b>Destination IP/Netmask (Only IPv4)</b>	Specify Destination IP/Netmask. Specify * if you want to bypass entire network.
<b>Source IP/Netmask (only IPv6)</b>	Specify Source IP/Prefix. Specify * if you want to bypass entire network.
<b>Destination IP/Netmask (Only IPv6)</b>	Specify Destination IP/Prefix. Specify * if you want to bypass entire network.
<b>Protocol</b>	Select protocol whose traffic is to be bypassed if generated from the specified source to destination.  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> <li>• All Protocols</li> </ul> <p>For example, if you select TCP protocol then DoS rules will not be applied on the TCP traffic from the specified source to destination.</p>
<b>Source Port</b>	Specify Port Number for Source. Specify * if you want to bypass entire network.

---

<b>Destination Port</b>	Specify Port Number for Destination. Specify * if you want to bypass entire network.
-------------------------	---

**Table – Add DoS bypass rule screen elements**

# Web Filter

Web Filter menu allows to configure and manage Web Filtering through the Appliance. The traffic coming from the web is filtered by various policies and categories.

- [Settings](#)
- [Category](#)
- [Policy](#)

## Settings

Use this page to enable Safe Search feature and Pharming protection useful in filtering Web traffic.

**Safe Search** – This feature allows you to enforce safe searching into your search engines, thus helping you against malicious sites.

**Pharming Protection** – This feature allows you to stop Pharming by various attacker sites by Domain Name resolution.

### Web Filter Setting Parameters

Configure Web Filter Settings from **Web Filter > Settings > Settings**.

Enforce Safe Search	<input checked="" type="checkbox"/>	Enabling this option would enforce safe search in search engines when Porn, AdultContent and Nudity categories are denied in WebFilter Policy
Enable Pharming Protection	<input checked="" type="checkbox"/>	On Enabling this option Appliance would protect users against pharming by re-resolving the domain name of the website using the DNS configured on the appliance
Denied Message	<input checked="" type="checkbox"/>	Override Default Denied Message
		<div style="border: 1px solid #ccc; height: 40px;"></div>
Denied Message Image	<input type="radio"/> Default <input checked="" type="radio"/> Custom	
Top Image	<input type="text"/> <input type="button" value="Browse..."/>	Maximum 125x70 pixels ( .jpg, .jpeg)
Bottom Image	<input type="text"/> <input type="button" value="Browse..."/>	Maximum 70x60 pixels ( .jpg, .jpeg)
<input type="button" value="Apply"/> <input type="button" value="Preview &gt;&gt;"/>		

Screen – Configure Settings

Screen Element	Description
<b>Enforce Safe Search</b>	Enable safe search so that web sites containing pornography and explicit sexual content are blocked from the Google, Yahoo, AltaVista and Bing search results.

	This will be applicable only when access to Porn, Adult Content and Nudity categories are denied in the Web Filter Policy.
<b>Enable Pharming Protection</b>	<p>Enable to protect against Pharming attacks and direct users to the legitimate websites instead of fraudulent websites.</p> <p>Pharming attacks require no additional action from the user from their regular web surfing activities. Pharming attack succeeds by redirecting the users from legitimate websites instead of similar fraudulent websites that has been created to look like the legitimate site.</p>
<b>Denied Message</b>	<p>Specify default deny message to be displayed for all the web categories.</p> <p>Enable Override Default Denied Message to display a customized message for all the web categories.</p>
<b>Denied Message Image</b>	Specify whether the default or custom image should be displayed on the Denied message page.
<b>Top Image</b>	<p>Specify the image which is to be displayed at the top of the message page.</p> <p>Dimension of Image should be 125 x 70 pixels and jpg file only.</p>
<b>Bottom Image</b>	<p>Specify the image which is to be displayed at the bottom of the message page.</p> <p>Dimension of Image should be 700 * 80 pixels and jpg file only.</p>

Table – Configure Settings screen elements

## Temporary Access Setting

Configure Temporary Access Settings from **Web Filter > Settings > Temporary Access Setting**.

Web filtering can be done through statically configured policies. Using this feature, administrator can allow temporary access to the websites/domains that are blocked by the organizational policy.

This feature will be useful in educational institutes that require students to access few domains on temporary basis for their Project work. Also, administrator can use this feature in cases where he/she wants the group leader to control Internet access for his/her team.

A Temporary Access Portal is provided to the users selected on this page where they can submit the list of websites/domains they need to access temporarily. On submission of the list, a temporary access token is generated. When user browses any domain from the list, "Access Denied page" will be displayed. On the page, user can enter the token and access the blocked website/domain.

The token will be valid for a specified period of time after which the domains/websites will be blocked again as per the organizational policy. Temporary Access Settings configured will be applicable for all the temporary Access requests.

Additionally, administrator can also configure domains/categories of domains which would never be granted temporary access

**Screen – Configure Temporary Access Setting**

Screen Element	Description
<b>Enable Portal</b>	Select to enable/disable Temporary Access Portal.
<b>Temporary Access Portal URL</b>	Displays the URL of Temporary Access Portal. Click the link to view the portal.  You can Create/View/Delete/Enable/Disable temporary access requests from the portal.
<b>Allowed User</b>	Select users that will be allowed access to the portal.
<b>Maximum Time</b>	Specify maximum amount of time in hours for the token to be valid.  Tokens should not be generated with time more than the maximum time.

<b>Maximum Categories</b>	Specify maximum number of categories that could be accessed per temporary access request.
<b>Maximum Domains</b>	Specify maximum number of domains that could be accessed per temporary access request.
<b>Prohibited Categories</b>	Select Categories that should never be allowed temporary access.
<b>Prohibited Domains</b>	Specify domains that should never be allowed temporary access.

**Table – Configure Temporary Access Setting screen elements**

## Web Category

Web Category is the grouping of Domains and Keywords used for Internet site filtering. Domains and any URL containing the keywords defined in the Web Category will be blocked.

Each category is classified according to the type of sites in the category. Categories are grouped into four types specifying whether surfing those categories is considered as productive or not:

- Neutral
- Productive
- Non-working
- Un-healthy

For your convenience, database of default web categories is provided. You can use these or even create new web categories to suit your needs. To use the default web categories, the add-on module Web and Application Filter should be registered.

Depending on the organization's requirement, allow or deny access to the categories with the help of policies by groups, individual user, time of day, and many other criteria. It is also possible to restrict the bandwidth based on the web category. For example, to reserve 512 kbps for SAP applications, define a QoS Policy of 512 kbps and assign this policy to the SAP Web Category and Firewall Rule. Users accessing any URLs falling under the SAP Web Category will get 512 kbps. 512 kbps bandwidth will be shared among all the users when more than one user is accessing.

The Appliance provides pre-defined categories which can be used to block the malicious and objectionable content. The page displays the list of pre-defined as well as custom categories.

The page allows you to manage default web categories and create custom web categories. You can also add or remove specific domains or keywords in the category. Appliance also provides pre-defined categories which can be used to block the malicious and objectionable contents.

Custom web category is given priority over default category while allowing/restricting the access.



## Manage Web Category List

To manage web categories, go to **Web Filter > Category > Category**.


Name	Type	Classification	QoS Policy	Manage
<a href="#">ALLWebTraffic</a>	Default	Neutral		
<a href="#">Activex</a>	Default	Non Working		
<a href="#">AdultContent</a>	Default	UnHealthy		
<a href="#">Advertisements</a>	Default	Non Working		
<a href="#">AlcoholandTobacco</a>	Default	Non Working		

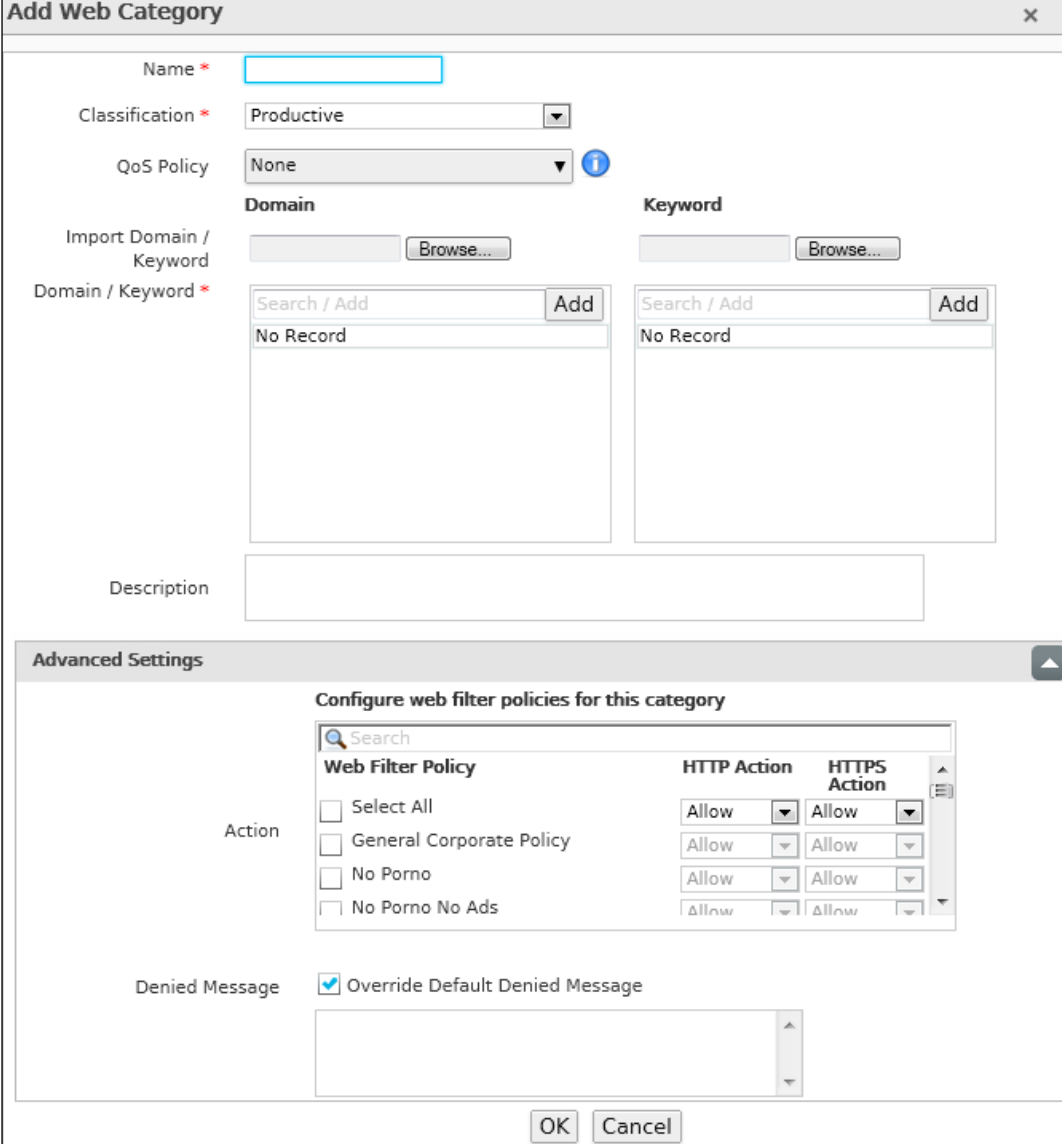
**Screen – Manage Web Categories**

Screen Element	Description
<b>Name</b>	Displays name of the Web Filter Category.
<b>Type</b>	Displays type of Policy – Default OR Custom.
<b>Classification</b>	Category Classification – Unhealthy, Non-working, Neutral, Productive.
<b>QoS Policy</b>	Displays the QoS Policy applied on the category.

**Table – Manage Web Categories screen elements**

## Web Category Parameters

To add or edit a web category, go to **Web Filter > Category > Category**. Click the Add button to add a new web category. To update the details, click on the web category or Edit icon  in the Manage column against the web category you want to modify.



**Add Web Category**

Name \*

Classification \* Productive

QoS Policy None

Domain  Browse...

Keyword  Browse...

Domain / Keyword \*  Add

Keyword \*  Add

No Record

No Record

Description

**Advanced Settings**

Configure web filter policies for this category

Search

Web Filter Policy	HTTP Action	HTTPS Action
<input type="checkbox"/> Select All	Allow	Allow
<input type="checkbox"/> General Corporate Policy	Allow	Allow
<input type="checkbox"/> No Porno	Allow	Allow
<input type="checkbox"/> No Porno No Ads	Allow	Allow

Action

Denied Message  Override Default Denied Message

OK Cancel

Screen – Add Web Category

Screen Element	Description
<b>Name</b>	Specify a name to identify the Web Category name. Name cannot be same as the default category name.
<b>Classification</b>	Select the type of classification for the category from the available options.  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• Neutral</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Productive</b></li> <li>• <b>Non-working</b></li> <li>• <b>Healthy</b></li> </ul>
<b>QoS Policy</b>	Select the QoS Policy, if bandwidth restriction is to be applied from the “QoS Policy” dropdown list.
<b>Configure Category (Applicable only while adding a Category)</b>	<p>Select to create a web category from the options available.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Local</b> – Select to create a Web Category with URL stored in the local Appliance.</li> <li>• <b>External URL Database</b> – Select to create a Web Category with external webcat URL located anywhere on the Internet.</li> </ul>
<b>Import Domain/Keyword (Only if “Local” Configure Category is selected)</b>	<p>Import a file consisting of all the configured URL/Keyword from the white list domain of an existing web categorization solution to Cyberoam Appliance.</p> <p>This will automatically include the domains/keywords in the “Domain / Keyword” list.</p>
<b>Domain/Keyword (Only if “Local” Configure Category is selected)</b>	Specify Domain / Keyword to include it under a Web Category.
<b>URL (HTTP or FTP) (Only if “External URL Database” Configure Category is selected)</b>	<p>Specify URL of external Web Category URL database. The Appliance will fetch database from the specified URL. The database of URLs should be in following file types: .tar, .tar.gz, .gz, .bz2, or plain text file.</p> <p>Use Add button to add multiple URLs.</p>
<b>Description</b>	Specify Category Description.
<b>Advanced Settings</b>	
<b>Action (Only applicable while adding a Category)</b>	<p>List displays all the policies available.</p> <p>Select Web Filter policy. Multiple categories can also be selected. You can also search the category name from the search text box provided.</p> <p>Specify action Allow OR Deny for HTTP and HTTPS traffic.</p>
<b>Denied Message</b>	Click to override default denied message and set your custom message.

Table – Add Web Category screen elements

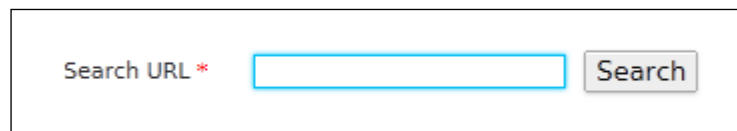
## Search URL

Use Search URL to search whether the URL is categorized or not. It searches the specified URL and displays Category name under which the URL is categorized along with the category description.

When a custom category is created with a Domain/URL which is already categorized in default category then the custom category overrides the default category and the search result displays custom category name and not the default category name.

To search a URL

Select **Web Filter > Category > Search URL**



The screenshot shows a search interface with the text "Search URL \*" on the left, a text input field in the center, and a "Search" button on the right. The entire interface is enclosed in a rectangular border.

**Screen – Search URL**

Enter URL to be searched in Search URL

Click Search

## URL Group

When you want to configure same rule for multiple URLs, create a URL Group and instead of adding web filter rule for individual URLs, and create a single the rule for the group.

The page allows you to group URLs and manage URL Groups. When you want to configure same rule for multiple URLs, create URL Group and instead of adding Web Filter Rule for individual URL, you add rule for the Group.

### Manage URL Group list

To manage URL Groups, go to **Web Filter > Category > URL Group**.

<input type="checkbox"/>	URL Group Name ▲	URL	Description	Manage
<input type="checkbox"/>	Test	aa.com	test	

Screen – URL Group

Screen Element	Description
URL Group Name	Displays a name of the URL Group.
URL	Displays a list of URL(s) grouped.
Description	Displays Group description.

Screen – URL Group screen elements

### Parameters

To add or edit a web category, go to **Web Filter > Category > URL Group**. Click the Add button to add a new web category. To update the details, click on the web category or Edit icon in the Manage column against the web category you want to modify.

Screen – Add URL

Screen Element	Description
URL Group Name	Specify a name to identify the URL Group.
URL(s)	Provide the URL.  Use a comma to separate multiple URLs.  Single URL can be member of multiple groups.
Description	Provide group description, if required.

**Table – Add URL screen elements**

## Web Filter Policy

Web Filter Policy controls user's web access. It specifies which user has access to what sites and allows defining powerful security policies based on almost limitless policy parameters like:

- Individual users
- Groups of users
- Time of day
- Location/Port/Protocol type
- Content type
- Bandwidth usage (for audio, video and streaming content)

You can control access to an entire application category, or individual file extensions within a category with the help of policy. For example, you can define a policy that blocks access to all audio files with .mp3 extensions.

Two strategies based on which Web Filter Policy can be defined are:

- **Allow:** By default, allows access to all the categories except the specified categories. Access to the specified categories depends on the strategy defined for each category.
- **Deny:** By default, denies access to all the categories except the specified categories. Access to the specified categories depends on the strategy defined for each category.

Appliance is shipped with the following predefined policies: Allow All, CIPA, Deny all and General Corporate Policy. These predefined policies are immediately available for use until configured otherwise. You can also define custom policies to define different levels of access for different users to meet your organization's requirements.

The Web Filter policy page displays list predefined and custom policies. You can filter or sort the list based on policy name. The page provides option to add new policy, update, or delete a policy.

To manage Web Filter Policies, go to **Web Filter > Policy > Policy**.

Name	Default Action	Reporting	Description	Manage
<input type="checkbox"/> A	Allow	Enabled	A	
<input checked="" type="checkbox"/> Allow All	Allow	Enabled	Allow all Internet Access	
<input checked="" type="checkbox"/> CIPA	Allow	Enabled	Internet Access Policy for Children's Internet Protection Act	
<input checked="" type="checkbox"/> Deny All	Deny	Enabled	Deny Internet Access	
<input type="checkbox"/> Deny All Chat and Mail	Allow	Enabled	Deny All Chat and Mail	
<input type="checkbox"/> Deny All Mail Sites	Allow	Enabled	Deny All Mail Sites	

Screen – Manage Web Filter Policies

Screen Element	Description
<b>Name</b>	Displays a name of Web Filter Policy.
<b>Default Action</b>	Displays default Action: Allow or Deny.

<b>Reporting</b>	Displays whether reporting is Enabled or Disabled.
<b>Description</b>	Displays Policy Description.

Table – Manage Web Filter Policy screen elements

## Web Filter Policy Parameters

To add or edit Web Filter Policies, go to **Web Filter > Policy > Policy**. Click Add Button to add a new policy or Edit Icon to modify the details of the policy.

**Add Web Filter Policy**

Name\*

Template

Enable Reporting

Download File Size Restriction\*  MB (Enter 0 for No Restriction)

YouTube Education Filter

Description

---

Category Name	Type	Schedule	Web Action	Exception
No Records Found.				

Screen – Web Filter Policy

Screen Element	Description
<b>Add Web Filter Policy</b>	
<b>Name</b>	Provide a name to identify the Policy. Duplicate names are not allowed.
<b>Template</b>	Select a template. A new policy will be based on the selected template and will inherit all the category restrictions defined in the template.
<b>Enable Reporting</b>	By default, Internet usage report is generated for all the users. But Appliance allows to bypass reporting of certain users.  Clear Enable Reporting to bypass reporting. Internet usage reports will not include access details of all the users to whom this policy will be applied.
<b>Download File Size Restriction</b>	Specify the file size (in MB) in the textbox against “Download File Size Restriction” to configure the maximum allowed file download size.  User will not be allowed to download file greater than the configured size.



	<p>This restriction is applicable only if HTTPS scanning is enabled in the corresponding firewall rule for which Web Filter Policy is configured.</p> <p>Specify 0 for no restriction.</p> <p>Web Categories – HTTPS Upload, ActiveX, Applets and Cookies, will work only if HTTPS scanning is enabled.</p>
<b>YouTube Education Filter</b>	<p>Specify the unique ID provided by “YouTube for Schools” while registration.</p> <p>“YouTube for Schools”, makes available a collection/ wide range of educational videos that can be accessible while being within a school network. On registering for “YouTube for Schools” a custom HTTP Header with a unique ID will be provided.</p> <p>E.g. X-YouTube-Edu-Filter:HMtp1sl9lxt0KA\pcg88kQ</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p><b>Field Name: X-YouTube-Edu-Filter</b>  <b>Field Value Format: Alphanumeric [a-z][A-Z][0-9]</b>  <b>Field Value Length: up to 44 characters</b></p> <p><b>Ensure the following top-level domains are not blocked</b>  <b>youtube.com</b>  <b>yting.com</b>  <b>Videos</b></p> </div>
<b>Description</b>	Provide Policy Description.

Table – Web Filter Policy screen elements

### Manage Web Filter Policy Rule list

Once the policy is created, policy rules can be added to schedule the implementation of the policy. Rules can be added for custom policies only.

<input type="button" value="Add"/>		<input type="button" value="Delete"/>					
<input type="checkbox"/>	Category Name	Type	Schedule	Web Action		Exception	Manage
	WebBasedEmail	Web	All The Time	HTTP	HTTPS	-	
				✘	✘		
<input type="button" value="Add"/>		<input type="button" value="Delete"/>					

Screen – Web Filter Policy Rule

Screen Element	Description
<b>Category Name</b>	Displays a name of the Web Filter Category.

<b>Type</b>	Displays type of Policy.
<b>Schedule</b>	Displays schedule for the category.
<b>Web Action</b>	Displays action for HTTP and HTTPS traffic.
<b>Exception</b>	Selected Category of File Type.

Table – Web Filter Policy Rule screen elements

### Web Filter Policy Rules Parameters

To add a policy rule, edit the policy in which you want to add a rule.

Web Filter Policy rules can be added to custom web filter policies. To add Web Filter Policy rules, go to **Web Filter > Policy > Policy**.

Screen – Add Web Filter Policy Rule


### Web Filter Policy Rule Parameters

Screen Element	Description
<b>Category Type (Only while adding a Web Filter Policy Rule)</b>	<p>Select category Type for which the rule is to be added. You can configure rule for 4 types of categories:</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Web Category</b></li> <li>• <b>File Type</b></li> <li>• <b>URL Group</b></li> <li>• <b>Dynamic Category.</b></li> </ul> <p>URL Group is a custom group of URLs Dynamic Category includes Cookies, Applets, ActiveX and HTTP Upload category.</p>
<b>Category</b>	Select Category for which the rule is to be added. Multiple categories can also be selected.

	You can also search the category name from the search text box provided.
<b>HTTP Action</b>	Specify action Allow or Deny for HTTP traffic.
<b>HTTPS Action</b>	Specify action Allow or Deny for HTTPS traffic.
<b>Exception link</b>	<p>Click to add the file type category exception rule for a selected category type and select file type category.</p> <p>For Example: If you want to allow Sport category and deny video file from Sport category then specify Allow action for Sport category and add Video File in Exception list.</p> <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>Exception Link is available only for Web Category and URL Group.</li> </ul> </div>
<b>Schedule</b>	Select the Schedule for categories selected from the list available.

Table – Add Web Filter Policy Rule screen elements

### Edit Web Filter Policy Rule

Click the Edit icon  in the Manage column against the Web Filter Policy to which rules are to be added. Edit Web Filter Policy window is displayed for modifications. You can add or delete rules from this page.

**Edit Web Filter Policy Rules** ✕

Category\* WebBasedEmail

HTTP Action  Allow  Deny

HTTPS Action  Allow  Deny

Exception

Schedule All the Time ▼

Screen – Edit Web Filter Policy Rule

Screen Element	Description
<b>Category</b>	Category for which the rule is to be added. Multiple categories can also be selected.
<b>HTTP Action</b>	Specify action Allow or Deny for HTTP traffic.
<b>HTTPS Action</b>	Specify action Allow or Deny for HTTPS traffic.

<b>Exception link</b>	<p>Click to add the file type category exception rule for a selected category type and select file type category.</p> <p>For Example: If you want to allow Sports category and deny video file from Sports category then specify the Allow action for Sport category and add Video File in Exception list.</p> <div data-bbox="692 472 1385 607"><b>Note</b><ul style="list-style-type: none"><li>• Exception Link is available only for Web Category and URL Group.</li></ul></div>
<b>Schedule</b>	Select the Schedule for categories selected from the list available.

**Table – Edit Web Filter Policy Rule screen elements**

## ICAP

Internet Content Adaption Protocol (ICAP) is a lightweight protocol that encapsulates underlying HTTP/HTTPS request and response to/from ICAP Server. It allows ICAP Clients to pass HTTP messages to ICAP Servers for transformation/adaption and thereby offloading the primary server. These ICAP Servers are focused on specific functions like ad insertion, content filtering, virus scanning etc.

Appliance can be deployed in heterogeneous enterprise environments and can hand over HTTP traffic to ICAP Server for malware scanning, content filtering and DLP scanning or other processing. Cyberoam after applying its Web Filter Policy will forward the Web traffic to ICAP server which in turn can apply data usage policies, antivirus scanning policies and content filtering policies. Depending on the services configured in the ICAP server, user either receives access denied message or virus detection message from Cyberoam or ICAP server.

Cyberoam can be seamlessly integrated using ICAP-compliant DLP/AV Scanning/Web Filtering applications:

- Symantec DLP
- Symantec Protection Engine 7.0
- Trend Micro Interscan Web Security Virtual Appliance
- Sophos Anti Virus
- Commtouch Anti Virus

Single ICAP profile with Request and Response mode are supported. Administrator can view all the events logs from the Log Viewer.

### Note

- This feature is supported in 'iNG' series appliances CR50iNG and above.

## Server

The ICAP Server page displays list of configured ICAP Servers. You can filter or sort the list based on Server Name. The page provides option to add, update, or delete Server.

### Manage ICAP Server

To manage ICAP Server, go to **Web Filter > ICAP > Server**.

Server Name	IP	Port	Service	Manage
<input type="checkbox"/> request_icap_1	10.20.20.246	1344	OMSScanReq-AV	
<input type="checkbox"/> response_icap_1	10.20.20.246	1344	OMSScanResp...	


Screen – Manage ICAP Server

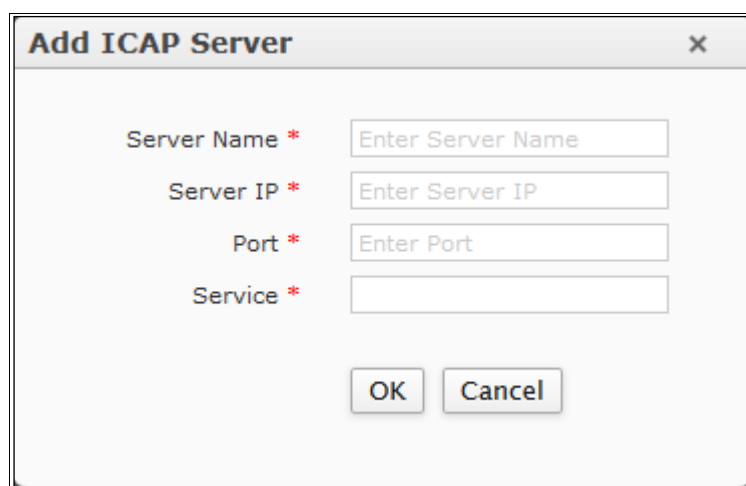
Screen Element	Description
Server Name	Displays name of the ICAP Server.

<b>IP</b>	Displays IPv4 Address of ICAP Server.
<b>Port</b>	Displays port number on which ICAP Server is running
<b>Service</b>	Displays the name of ICAP Service.

Table – Manage ICAP Server screen elements

### ICAP Server Parameters

To add or edit ICAP Server, go to **Web Filter > ICAP > Server**. Click the Add button to add a new ICAP Server. To update the details, click on the Server name or Edit icon  in the Manage column against the Server you want to modify.



Screen – Add ICAP Server

Screen Element	Description
<b>Server Name</b>	Specify name for ICAP Server.
<b>Server IP</b>	Specify IPv4 Address of ICAP Server.
<b>Port</b>	Specify the port number on which ICAP Server is running.
<b>Service</b>	Specify the name of ICAP Service.



Table – ICAP Server screen elements

### Policy

The ICAP Policy page displays list of configured ICAP Policies. You can filter or sort the list based on Policy Name. The page provides option to add, update, or delete a policy.

### Manage ICAP Policy

To manage ICAP Policy, go to **Web Filter > ICAP > Policy**.


Policy Name	Request Server	Response Server	Max Connections	Content Limit	Manage
ICAP Profile 1	request_icap_1	response_icap_1	32	51200	 

### Screen – Manage ICAP Policy

Screen Element	Description
<b>Policy Name</b>	Displays name of the ICAP Policy.
<b>Request Server</b>	Displays configured Request Server.
<b>Response Server</b>	Displays configured Response Server.
<b>Max Connections</b>	Displays the maximum concurrent connections.
<b>Content Limit</b>	Displays the Content limit.

Table – Manage ICAP Policy screen elements

### ICAP Policy Parameters

To add or edit ICAP Policy, go to **Web Filter > ICAP > Policy**. Click the Add button to add a new ICAP Policy. To update the details, click on the Policy name or Edit icon  in the Manage column against the Policy you want to modify.

**Add ICAP Policy** ✕

Policy Name \*

Request Modifications  Enable

Request Server \*

Response Modifications  Enable

Response Server \*

Max Connections \*  (1-32)

Content Limit \*  (0-51200 KB, Enter 0 for default 25600 KB)

DLP Mode  Enable

Bypass Error  Enable

### Screen – Add ICAP Policy

Screen Element	Description
<b>Policy Name</b>	Specify name for the Policy.
<b>Request Modifications</b>	Enable to configure ICAP Server in Request mode.

<b>Request Server</b>	Select configured Request Server.
<b>Response Modifications</b>	Enable to configure ICAP Server in Response mode.
<b>Response Server</b>	Select configured Response Server.
<b>Max connections</b>	<p>Specify maximum concurrent connections to be allowed with the ICAP Server.</p> <p>Default – 16</p> <p>Note: Maximum connection limit and acceptable range differs as per appliance model as below:</p> <p><b>For Appliance models: CR50iNG, CR100iNG, CR200iNG, CR200iNG-XP, CR300iNG, CR300iNG-XP</b></p> <p>Max connections – 32 Acceptable Range – 1 to 32</p> <p><b>For Appliance models: CR500iNG-XP, CR750iNG-XP</b></p> <p>Max connections – 64 Acceptable Range – 1 to 64</p> <p><b>For Appliance models: CR1000iNG-XP, CR1500iNG-XP, CR2500iNG, CR2500iNG-XP</b></p> <p>Max connections – 128 Acceptable Range – 1 to 128</p>
<b>Content Limit</b>	<p>Specify the content limit for ICAP Server to process.</p> <p>Default – 0 KB</p> <p>Acceptable Range (KB) – 0 to 51200</p> <p>Note: When content limit is set to 0, the default limit set is 25000KB.</p>
<b>DLP Mode</b>	Enable to process only DLP methods. If enabled, ICAP Server will only process POST/PUT methods.
<b>Bypass Error</b>	Enable to bypass error messages.

Table – ICAP Policy screen elements



# Application Filter

Application Filter menu allows configuring and managing filtering on various applications. The traffic coming from the web is filtered by various policies and categories.

- [Application List](#)
- [Category](#)
- [Policy](#)

## Application List

The Appliance can identify and control applications which use standard Port 80, 443, non-standard ports, port hopping or tunnel through encrypted SSL traffic. The feature enables prioritization of applications based on user identity, time, applications, and bandwidth, allowing great flexibility, visibility, and control. The Appliance also provides implementation of application-based bandwidth management, accelerating critical applications while blocking malware-laden sites through Web Filtering. Organizations can group applications as per their requirements into business-critical, entertainment, communication, collaboration and control access through Firewall policies.

### Note

- Web and Application Filter module is a subscription module that needs to be subscribed before use. Check the features of the module by subscribing free trial subscription of the module. (See **System > Maintenance > Licensing**)

The Appliance is shipped with a set of predefined applications. This applications are classified based on their risk level, characteristics and technology, offering more granular controls.

### Note

- Web and Application Filter module is a subscription module that needs to be subscribed before use. Check the features of the module by subscribing free trial subscription of the module. (See **System > Maintenance > Licensing**)

The total number of application signatures included depends on the Application Signatures Database used by the Appliance. Appliance Information doclet in the Dashboard provides the version of Application Signatures Database used by your Appliance.

The Application List page displays total number of applications available for use and list of all the applications including information describing category it belongs to, risk factors, its characteristics and technology.

The application list can be filtered based on name of the application, category of the application, risk, characteristics, and technology.

## Manage Applications list

To view and search applications, go to **Application Filter > Application List > Application List**.

Total Applications : 2222 Records Per Page 50 (1 of 45)

Name	Category	Risk	Characteristics	Technology
1 & 1 Webmail	Web Mail	2 - Low	Widely Used,Transfer files	Browser Based
100BAO P2P	P2P	4 - High	Vulnerabilities,Transfer files...	P2P
126 Mail	Web Mail	2 - Low	Transfer files,Widely Used	Browser Based
163 Alumni	Social Networking	2 - Low	Widely Used,Loss of productivity	Browser Based
163 BBS	Social Networking	2 - Low	Excessive Bandwidth,Loss of pr...	Browser Based
1Fichier Download	Download Applications	3 - Medium	Transfer files,Loss of product...	Browser Based
1Fichier Upload	File Transfer	2 - Low	Transfer files,Loss of product...	Browser Based
2CH	Social Networking	2 - Low	Loss of productivity,Widely Used	Browser Based
2shared Download	Download Applications	2 - Low	Transfer files,Loss of product...	Browser Based
2shared Upload	File Transfer	2 - Low	Transfer files,Loss of product...	Browser Based
360Buy	General Internet	2 - Low	Loss of productivity,Widely Used	Browser Based
360Quan	Social Networking	2 - Low	Loss of productivity	Browser Based
3COM-Tsmux	Network Services	1 - Very Low	Widely Used	Network Protocol
43things Website	Social Networking	2 - Low	Loss of productivity,Excessive...	Browser Based
4everproxy Proxy	Proxy and Tunnel	3 - Medium	Prone to misuse,Can bypass fir...	Browser Based

Records Per Page 50 (1 of 45)

### Screen – Manage Application List

Screen Element	Description
<b>Name</b>	Displays the Application Name.
<b>Category</b>	Displays the name of the category.
<b>Risk</b>	Displays the type of risk.
<b>Characteristics</b>	Displays the characteristics of an application.
<b>Technology</b>	Displays the technology name used by an application.


Table – Manage Application List screen parameters

## Application Filter Category










The applications shipped with the Appliance are grouped into categories. These categories can be used in filtering policy and bandwidth restriction can be applied. Bandwidth restriction can be applied on the category or on the individual application within the category. Appliance

The Category page displays list of all the categories. The categories list can be filtered based on name of the category. Use plus or minus toggle besides the category name to expand and collapse list of applications grouped in the respective category.

### Configuring QoS Policy for Category or Application

The Category page provides a list of default Application Filter Categories on the Web Admin Console like Conferencing, Desktop Mail etc. Each of the categories contains sub categories and can be viewed by clicking the  icon against the category.

To edit the Application Filter Category, go to **Application Filter > Category > Category**.

	Category Name	QoS Policy	Bandwidth Usage Type	Manage
	Conferencing	No Policy	-	
	Desktop Mail	No Policy	-	
	Download Applications	No Policy	-	
	File Transfer	No Policy	-	
	Gaming	No Policy	-	
	General Business	No Policy	-	

Screen – Manage Application Filter Categories

Screen Element	Description
<b>Category Name</b>	Displays the name of Category.
<b>QoS Policy</b>	Select QoS Policy to be applied.  QoS policy allocates and limits the maximum bandwidth usage of the user.  You can create a new policy directly from this page or from <b>QoS &gt; Policy &gt; Policy</b> page.
<b>Bandwidth Usage Type</b>	Displays the bandwidth usage allotted to the QoS Policy. Shared or Individual.

Table – Manage Application Filter Category screen elements

### Edit Category

Screen – Edit Category

Screen Element	Description
<b>Name</b>	Name of the Application Filter Category. Category Name cannot be changed.
<b>QoS Policy</b>	<p>Select QoS Policy to be applied to the Application Filter Category.</p> <p>QoS policy allocates &amp; limits the maximum bandwidth usage of the user.</p> <p>You can also create a new policy directly from this page and attach to the category.</p>

Table – Edit Category screen elements

## Application Filter Policy

The Application Filter Policy controls the user's application access. It specifies which user has access to which applications and allows defining powerful security policies based on almost limitless policy parameters like:

- Individual users
- Groups of users
- Time of day

Application Filter Policy strategies:

- **Allow:** By default, allows access to all the categories except the specified categories. Access to the specified categories depends on the strategy defined for each category.
- **Deny:** By default, denies access to all the categories except the specified categories. Access to the specified categories depends on the strategy defined for each category.

Appliance is shipped with the following predefined policies for applications: Allow All and Deny All. These two predefined policies are immediately available for use until configured otherwise. You can also define custom policies to define different levels of access for different users to meet your organization's requirements.

The Application Filter policy page displays a list of all the predefined and custom policies. The page also provides option to add a new policy, update parameters of the existing policy, delete a policy, add a filtering rule to a policy or delete a filtering rule attached to a policy.

### Manage Application Filter Policies

To manage application filter policies, go to **Application Filter > Policy > Policy**.

Name	Default Action	Description	Manage
Allow All	Allow	Allow All Policy.	
AppPolicy_31079_1	Allow	Automated	
AppPolicy_31079_10	Allow	Automated	

Screen – Manage Application Filter Policies

Screen Element	Description
<b>Name</b>	Displays name of the Application Filter Policy.
<b>Default Action</b>	Default Action: Allow or Deny.
<b>Description</b>	Policy Description.

Table – Manage Application Filter Policies screen elements

## Application Filter Policy Parameters

To add or edit an Application Filter Policy, go to **Application Filter > Policy > Policy**. Click the Add button to add an Application Filter Policy. Application Filter Policy [Parameters](#) are given below.

### Parameters

Screen – Add Application Filter Policy

Screen Element	Description
<b>Name</b>	Specify a name to identify the Application Filter Policy.
<b>Description</b>	Provide describe for the Application Filter Policy.
<b>Enable Micro App Discovery</b>	Enable to scan and classify microapps using HTTPS protocol for communication. Microapps are applications that are used within web browsers.  To allow/deny microapps, you need to specify action accordingly.
<b>Template</b>	Select template for the Application Filter Policy.

Table – Add Application Filter Policy screen elements

### Edit Application Filter Policy Rule

To update the details, click on the policy or Edit icon  in the Manage column against the policy to be modified.

Name \*

Description

Enable Micro App Discovery

	Application	Application Filter Criteria	Schedule	Action	Manage
<input type="checkbox"/>	SOCK4 Proxy, SOCK5 Proxy	<b>Category</b> = Proxy and Tunnel <b>Risk</b> = 3-Medium <b>Characteristics</b> = Prone to misuse, Tun... <b>Technology</b> = Browser Based	All the Time	Allow	

Screen – Edit Application Filter Policy

Screen Element	Description
<b>Name</b>	Name of the Application Filter Policy to be edited.
<b>Description</b>	Description of the Application Filter Policy to be edited.
<b>Application</b>	Displays a list of the selected applications.
<b>Application Filter Criteria</b>	Displays the criteria selected for the Application Filter Policy Rule.
<b>Schedule</b>	Displays the selected schedule.
<b>Action</b>	Displays the selected Action.

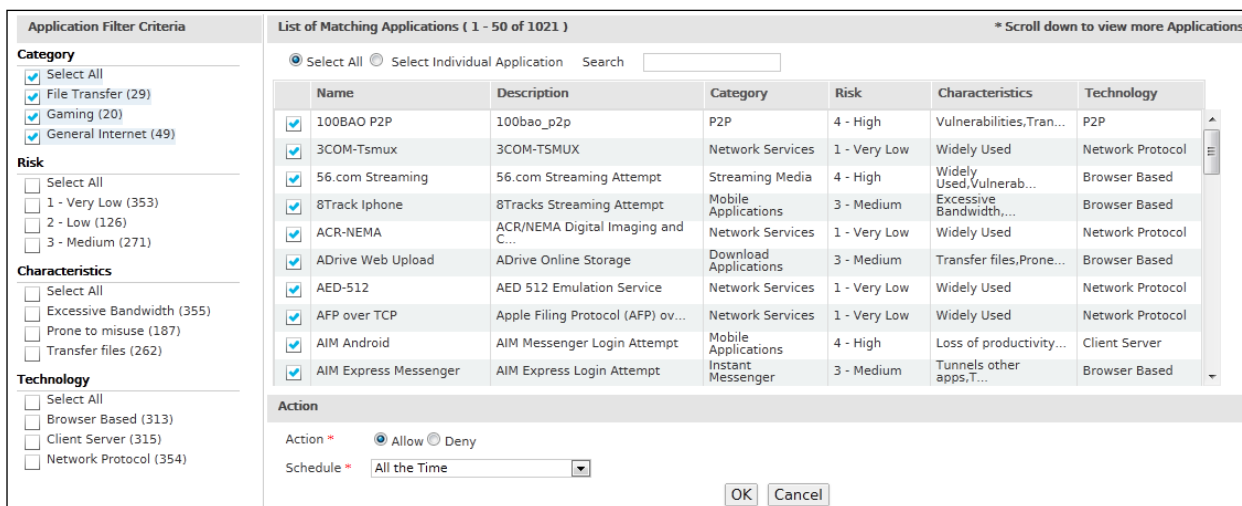
Table – Edit Application Filter Policy screen elements

### Application Filter Policy Rules Parameters

Once the policy is created, policy rules can be added to schedule the implementation of the policy.

#### Note

- Rules can be added for custom policies only.




Screen – Add Application Filter Policy Rules

Parameters

Screen Element	Description
<b>Application Filter Criteria</b>	
<b>Category</b>	Select the Application Category from the list of available categories.
<b>Risk</b>	Select the type of risk from the available options.  Available Options: <ul style="list-style-type: none"> <li>• Select All</li> <li>• 1 - Very Low</li> <li>• 2 – Low</li> <li>• 3 – Medium</li> <li>• 4 – High</li> <li>• 5 – Very High</li> </ul>
<b>Characteristics</b>	Select the characteristics from the available options.  Available Options: <ul style="list-style-type: none"> <li>• Select All</li> <li>• Can bypass firewall policy</li> <li>• Excessive Bandwidth</li> <li>• Loss of productivity</li> <li>• Prone to misuse</li> <li>• Transfer files</li> <li>• Tunnels other apps</li> <li>• Vulnerabilities</li> <li>• Widely Used</li> </ul>
<b>Technology</b>	Select the technology from the available options.



	<p>Available Options:</p> <ul style="list-style-type: none"> <li>• Select All</li> <li>• Browser Based</li> <li>• Client Server</li> <li>• Network Protocol</li> <li>• P2P</li> </ul>
<b>List of Matching Applications</b>	
<b>Select All</b>	<p>Select the option “Select All” to choose all the Applications listed for the selected criteria.</p> <p>Based on the Application Filter Criteria the applications are made available.</p>
<b>Select Individual Application</b>	<p>Select the option “Select Individual Application” to customize the choice of Applications list for the selected criteria.</p> <p>Based on the Application Filter Criteria the applications are made available.</p>
<b>Search</b>	<p>Specify the Application Name in the textbox to search an Application.</p> <p>This option is available, only if option “Select Individual Application” is selected.</p>
<b>Name</b>	Displays name of the Applications under the Category selected. You can also select more than one application using the checkbox.
<b>Description</b>	Displays description of the Application.
<b>Category</b>	Displays category of the Application.
<b>Risk</b>	Displays the risk factor involved with the Application.
<b>Characteristics</b>	Displays the characteristics of the Application.
<b>Technology</b>	Displays the technology utilized for the Application.
<b>Action</b>	
<b>Action</b>	<p>Select an Action for the Policy from the available options.</p> <p>Available Options:</p> <ul style="list-style-type: none"> <li>• Allow</li> <li>• Deny</li> </ul>
<b>Schedule</b>	Select Schedule from the list of Schedules available in the dropdown list.

	 <p>The screenshot shows a vertical list of application filter policy rules. The items are: 'All the Time', 'Schedule_26318_34', 'Schedule_26318_33', 'Schedule_26318_31', 'Schedule_26318_36', 'Work hours (6 Day week)', 'All Time on Weekdays', and 'All Days 10:00 to 19:00'. The list is contained within a rectangular box with a scrollbar on the right side.</p>
--	--

**Table – Add Application Filter Policy Rules screen elements**

# IM

IM (Instant Messaging) allows configuring and managing restrictions on Instant Messaging services provided by the Yahoo and MSN messengers. The traffic coming from web in the form of files and chat is filtered by various rules and content filtering strategies. You can add an IM Contact or IM Contact Group for configuring the rules.

- [IM Contact](#)
- [IM Rules](#)
- [Content Filter](#)

## IM Contact

IM Contact is used to register various Yahoo and MSN messaging application users. A Contact can be created for a user having access to any of the two IM applications. Along with the contacts, IM Contact Groups can also be created. Once the users are registered, various IM rules can be created for monitoring them. The rules can be set on groups as well as on users individually.

- [IM Contact](#)
- [IM Contact Group](#)

The IM Contact page is used to create and manage contacts. These contacts can either be Yahoo or MSN Email IDs. Any of the Email ID created through Yahoo or MSN are valid for creating IM Contacts.

### Note

- Contact cannot be deleted, If a Contact Group exists for the user.

## Manage IM Contact list

To manage IM contacts, go to **IM > IM Contact > IM Contact**.

Add		Delete		Records Per Page	20	<<	<	(1 of 1)	>	>>
<input type="checkbox"/>	Protocol	Username		Manage						
<input type="checkbox"/>	Yahoo	test@yahoo.com		 						
Add		Delete		Records Per Page	20	<<	<	(1 of 1)	>	>>

Screen – Manage IM Contacts

Screen Element	Description
Protocol	Displays the protocol that suggests the messenger application in use. Yahoo or MSN.


<b>Username</b>	Displays the username provided for the IM contact.
-----------------	--

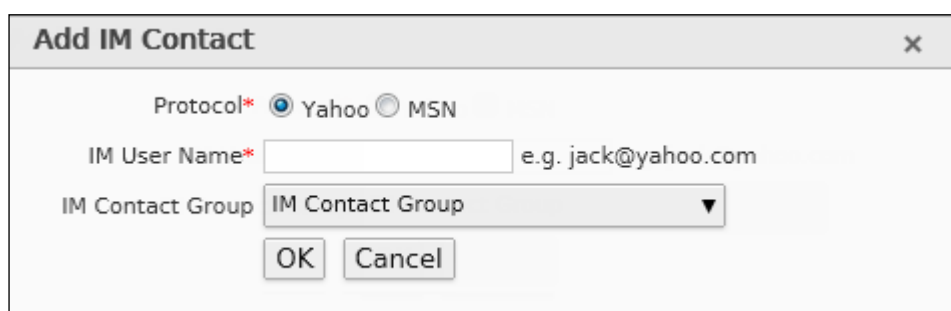
Table – Manage IM Contacts screen elements

**Note**

- A Contact cannot be deleted, if a Contact Group exists for the user.

**Adding an IM Contacts**

To add or edit an IM contact, go to **IM > IM Contact > IM Contact**. Click the Add button to add IM contact. To update the details, click on the contact or Edit icon  in the Manage column against the contact you want to modify.



Screen – Add IM Contact

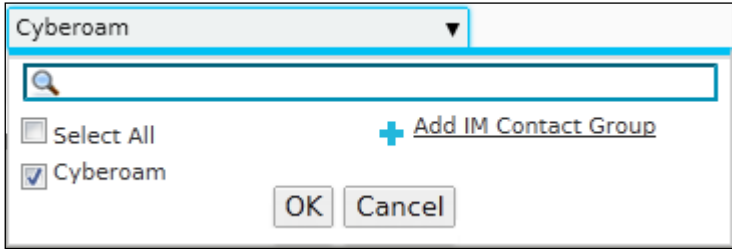
Screen Element	Description
<b>Protocol</b>	Select the application used for Instant Messaging.  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• Yahoo</li> <li>• MSN</li> </ul>
<b>IM User Name</b>	Specify the username to identify the IM Contact. The username can either be an Email Address or name of the user.
<b>IM Contact Group</b>	Select the IM Contact Group to which an IM Contact will be assigned.  

Table – Add IM Contact screen elements



## IM Contact Group

A Group is a collection of users that are managed as a single unit. By creating a group, filtering rules can be applied to a number of contacts simultaneously. Contacts that belong to a particular group are referred to as group contacts.

IM Contact Group page is used to create and manage contact groups. These contact groups have IM Contacts. A single IM Contact can be added to multiple contact groups. Rules to the user get applied in the order in which they are created.

### Manage IM Contact Group list

To manage IM contact groups, go to **IM > IM Contact > IM Contact Group**.


Name	Description	Manage
<input type="checkbox"/> <a href="#">Cyberoam</a>	Cyberoam Team	 

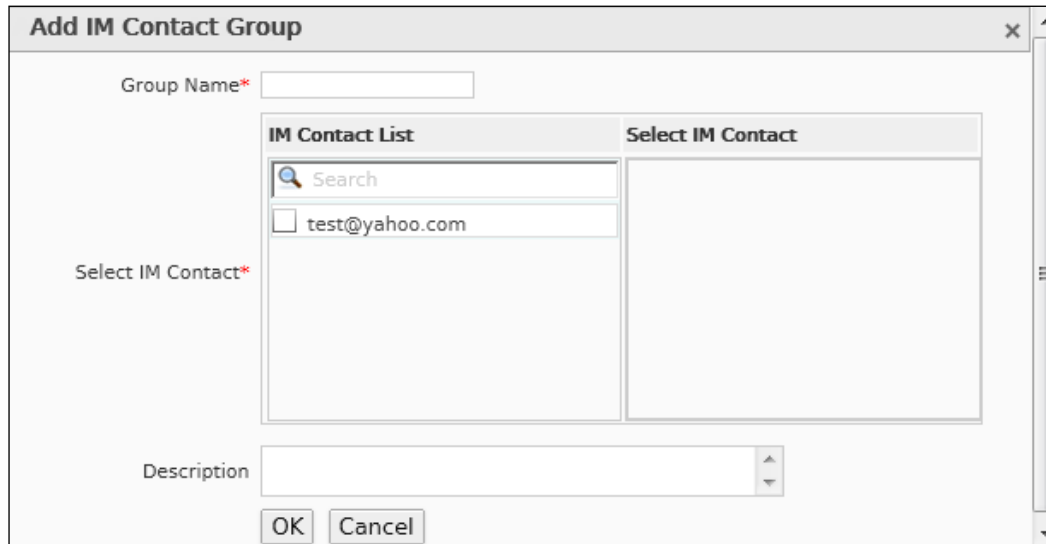
Screen – Manage IM Contact Groups

Screen Element	Description
<b>Name</b>	Displays name of the IM Contact Group.
<b>Description</b>	Displays description for an IM Contact Group.

Table – Manage IM Contact Group screen elements

## Creating IM Address Group Parameters

To add or edit an IM contact group, go to **IM > IM Contact > IM Contact Group**. Click the Add button to add IM contact group. To update the details, click on the contact group or Edit icon  in the Manage column against the contact group you want to modify.



Screen – Add IM Contact Group

Screen Element	Description
<b>Group Name</b>	Specify a name to identify the IM Contact Group.
<b>Select IM Contact</b>	<p>“IM Contact” List displays all the IM Contacts.</p> <p>Click the checkbox to select the contacts. All the selected contacts are moved to “Selected IM Contact” list.</p> <p>Single IM Contact can be a member of multiple IM Contact Groups.</p>
<b>Description</b>	Provide description for IM Contact Group.

Table – Add IM Contact Group screen elements

## IM Rules

IM Rule controls the user's Instant Messaging access. It specifies which users have access to what IM applications. Processing of IM Rules is top downwards and the first suitable rule found is applied. Individual rules for Login, Conversation (chats), File Transfer and Webcam access can be defined based on parameters like:

- One-to-One Conversation – One-to-One conversations can be allowed/denied between individual contacts or contacts within groups.
- Group Conversation – Group conversations between multiple users can be allowed/denied.
- Content Filtering
- Virus Scanning
- Archiving
- Maintaining Logs

Allow/Deny access can be set for an IM Contact or entire IM Contact Group, or even normal users or User Groups. For example, you can define a rule that blocks access to all one-to-one conversations between an IM Contact Group and a User Group.

For ease of configuration, Appliance provides default rules for Login, Conversation, File Transfer and Webcam. A custom rule can also be created to meet an organization's requirements.





If IM access between contacts is restricted, an access denied message is displayed in the conversation window.

- [Login](#)
- [Conversation](#)
- [File Transfer](#)
- [Webcam](#)

## Login

Login page allows you to configure and manage Login Rules for IM Contact, IM Contact Group, User and User Group.

To manage login rules for contacts, go to **IM > IM Rules > Login**.

<input type="button" value="Add"/> <input type="button" value="Delete"/>						
<input type="checkbox"/>	Name	Participants	Action	Logging	Logging Level	Manage
<input type="checkbox"/>	rule1	test@yahoo.com	Deny	On	MetaData	 
<input type="checkbox"/>	imloginrule2	Any other MSN Contacts	Allow	On	MetaData	
<input type="checkbox"/>	imloginrule1	Any other Yahoo Contacts	Allow	On	MetaData	

Screen – Manage Login Rules

### Note

- Default Login Rules cannot be deleted.

Screen Element	Description
<b>Name</b>	Displays the name of the Login Rule.
<b>Participants</b>	Username or IM Contact name of the participant for whom the Login Rule is established.
<b>Action</b>	Displays the type of Action selected – Allow or Deny.
<b>Logging</b>	Displays whether logging is “On” or “Off”.
<b>Logging Level</b>	Displays the level of login for a rule.

Table – Manage Login Rule screen elements

## Creating an IM Login Rule

To add or edit a login rule, go to **IM > IM Rules > Login**. Click the Add button to add login rule. To update the details, click on the rule or Edit icon  in the Manage column against the rule you want to modify.

**Add Login Rule** ✕

Name\*

User / IM contact \*

Action  Allow  Deny

Privacy Disclaimer  Enable

Logging  Enable

Logging Level

Screen – Add Login Rule



Screen Element	Description
<b>Name</b>	Specify a name for the Login Rule.
<b>User / IM Contact</b>	<p>Select the Participants between whom the Login Rule is to be defined.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• IM Contact</li> <li>• IM Contact Group</li> <li>• User</li> <li>• User Group</li> </ul> <p>You can also add above contacts from the Add Login Rule Page itself.</p>
<b>Action</b>	<p>Select an Action for login.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• Allow</li> <li>• Deny</li> </ul>
<b>Privacy Disclaimer</b>	<p>If the Login is allowed, you can enable the Privacy Disclaimer checkbox to inform the IM Contacts about the privacy policy.</p> <p>Default Privacy Disclaimer is displayed when the contact logs into an IM application.</p>
<b>Logging</b>	<p>Enable Logging, if the log has to be maintained for the contacts.</p> <p>If logging is enabled, the logs can be viewed from <b>Logs &amp; Reports &gt; Log Viewer</b>. Select "IM" from "Log Modules" list.</p>
<b>Logging Level</b>	<p>Select the Logging Level if the Logging is enabled.</p> <ul style="list-style-type: none"> <li>• <b>Meta Data</b> – Meta Data contains the information about the Login time, logout time, login action configured and name of the User or Group logged in.</li> </ul>

Table – Add Login Rule screen elements

## Conversation

The Conversation page allows configuring and managing Conversation Rules between any of the two identities: IM Contact, IM Contact Group, User and User Group. The IM conversation between these two contacts can be monitored and logged.

Appliance provides a default Conversation Rule that can be applied. This rule allows all the conversations but logs the content of the conversation.

### Note

- Default Conversation Rules cannot be deleted.

## View the list of Conversation Rules

To manage default and custom conversation rules between contacts, go to **IM > IM Rules > Conversation**.

<input type="checkbox"/>	Name	Participant	Participant	One-to-One Conversation	Group Conversation	Logging	Logging Level	Manage
<input type="checkbox"/>	conversationrule1	Any	Any	Allow	Allow	On	MetaData	


Screen – Manage Conversation Rules

Screen Element	Description
<b>Name</b>	Displays name of the Conversation Rule.
<b>Participant</b>	Displays the first participant involved in the conversation.
<b>Participant</b>	Displays the second participant involved in the conversation.
<b>One-to-One Conversation</b>	Displays the type of One-to-One-Conversation selected- Allow OR Deny.
<b>Group Conversation</b>	Displays the type of Group Conversation selected- Allow OR Deny.
<b>Logging</b>	Displays whether Conversation Logs are On or Off.  If logging is enabled, the logs can be viewed from <b>Logs &amp; Reports &gt; Log Viewer</b> . Select "IM" from "Log Modules" list.
<b>Logging Level</b>	Displays the Logging Level selected – Full Data or Meta Data. <ul style="list-style-type: none"> <li>• <b>Full Data</b> – Full Data contains the entire information about conversation including the content of the chat, the Login time, logout time. Name of User or Groups between whom the conversation happened and duration of the conversation.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Meta Data</b> – Meta Data contains the information about the Login time, logout time. Name of User or Groups between whom the conversation happened and duration of the conversation.</li> </ul>
--	--

Table – Manage Conversation Rule screen elements

## Creating IM Conversation Rule

To add or edit a conversation rule, go to **IM > IM Rules > Conversation**. Click the Add button to add conversation rule. To update the details, click on the rule or Edit icon  in the Manage column against the rule you want to modify.

**Add Conversation Rule** x

Name\*

Between User / IM contact \*  And

One-to-One Conversation \*  Allow  Deny

Group Conversation \*  Allow  Deny

Content Filter \*  Enable

Logging \*  Enable

Logging Level \*

Screen – Add Conversation Rule

Screen Element	Description
<b>Name</b>	Specify a Name for the Conversation Rule.
<b>Between User / IM Contact</b>	<p>Select the Participants between whom the Conversation Rule is to be defined.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• IM Contact</li> <li>• IM Contact Group</li> <li>• User</li> <li>• User Group</li> </ul> <p>You can also add above contacts from the Add Conversation Rule Page itself.</p>
<b>One-to-One Conversation</b>	Specify Action for the one-to-one conversation - Allow OR Deny.
<b>Group Conversation</b>	Specify Action for the group conversation or chat - Allow OR Deny.
<b>Content Filter</b>	Enable Content Filtering.

<b>Logging</b>	Enable Logging, if the log has to be maintained for the conversation.  If logging is enabled, the logs can be viewed from <b>Logs &amp; Reports &gt; Log Viewer</b> . Select 'IM' from 'Log Modules' list
<b>Logging Level</b>	Select the Logging Level if the Logging is enabled.  <b>Available Options:</b> <ul style="list-style-type: none"><li>• <b>Full Data</b> – Full Data contains the entire information about conversation including the content of the chat, the Login time, logout time. Name of User or Groups between whom the conversation happened and duration of the conversation.</li><li>• <b>Meta Data</b> – Meta Data contains the information about the Login time, logout time. Name of User or Groups between whom the conversation happened and duration of the conversation.</li></ul>


**Table – Add Conversation Rule screen elements**

## File Transfer

File Transfer page allows the user to configure and manage File Transfer Rules between any of the two identities: IM Contact, IM Contact Group, User and User Group. The file transfers between these two identities is monitored and logged.

If the file transfer access between contacts is restricted and contact tries to transfer a file, an access denied message is displayed in the conversation window.

To manage file transfer rules between contacts, go to **IM > IM Rules > File Transfer**.


<input type="checkbox"/>	Name	Participant	Participant	Action	Virus Scanning	Logging	Logging Level	Manage
<input checked="" type="checkbox"/>	filetransferrule2	Any	Any	Allow	On	On	MetaData	

Screen – Manage File Transfer Rules

Screen Element	Description
<b>Name</b>	Displays name of the File Transfer Rule.
<b>Participant</b>	Displays the first participant involved in transferring the file.
<b>Participant</b>	Displays the second participant involved in transferring the file.
<b>Action</b>	Displays the type of Action selected for File transferring – Allow or Deny.
<b>Virus Scanning</b>	Displays whether Virus Scanning is On or Off.
<b>Logging</b>	Displays whether File Transfer logs is On or Off.  If logging is enabled, the logs can be viewed from <b>Logs &amp; Reports &gt; Log Viewer</b> . Select “IM” from “Log Modules” list.
<b>Logging Level</b>	Logging Level. <ul style="list-style-type: none"> <li><b>Meta Data</b> – Meta Data contains the information about the Login time, logout time. Name of User or Groups between whom the conversation happened and duration of the conversation.</li> </ul>

Table – Manage File Transfer Rule screen elements

### Creating IM File Transfer Rule

To add or edit a file transfer rule, go to **IM > IM Rules > File Transfer**. Click the Add button to add file transfer rule. To update the details, click on the rule or Edit icon  in the Manage column against the rule you want to modify.

Screen – Add File Transfer Rule

Screen Element	Description
<b>Name</b>	Specify a name for the File Transfer Rule.
<b>Between User / IM Contact</b>	<p>Select the Participants between whom the File Transfer Rule is to be defined.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• IM Contact</li> <li>• IM Contact Group</li> <li>• User</li> <li>• User Group</li> </ul> <p>You can also add above contacts from the Add File Transfer Rule Page itself.</p>
<b>Action</b>	<p>Select the type of Action.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• Allow</li> <li>• Deny</li> </ul>
<b>Virus Scanning</b>	Enable Virus Scanning, if the file transferred between contacts is to be scanned.
<b>Logging</b>	<p>Enable Logging, if the log has to be maintained for the transfer of files.</p> <p>If logging is enabled, the logs can be viewed from <b>Logs &amp; Reports &gt; Log Viewer</b>. Select “IM” from “Log Modules” list.</p>
<b>Logging Level</b>	<p>Select the Logging Level if you have enabled Logging.</p> <ul style="list-style-type: none"> <li>• <b>Meta Data</b> – Meta Data contains the information about the File Transferred including Login time, logout time, file transfer action defined and name of User or Groups between whom the file transfer happened.</li> </ul>

Table – Add File Transfer Rule screen elements

## Webcam

The Webcam page allows configuring and managing Webcam Rules between any of the two identities: IM Contact, IM Contact Group, User and User Group. The video conversations via Webcam between these two contacts are monitored and logged.

If video conversation access between contacts is restricted and the contact tries to use the Webcam, an access denied message is displayed in the conversation window.

To manage webcam rules between contacts, go to **IM > IM Rules > Webcam**.


Add		Delete					
<input type="checkbox"/>	Name	Participant	Participant	Action	Logging	Logging Level	Manage
<input type="checkbox"/>	webcamrule3	Any	Any	Allow	On	MetaData	
Add		Delete					

Screen – Manage Webcam Rules

Screen Element	Description
<b>Name</b>	Displays the name of the Webcam Rule.
<b>Participant</b>	Displays the first participant involved in video conversation.
<b>Participant</b>	Displays the second participant involved in video conversation.
<b>Action</b>	Displays Action taken for the Webcam viewing:  <b>Available Options:</b> <ul style="list-style-type: none"> <li>• Allow</li> <li>• Deny</li> </ul>
<b>Logging</b>	Displays whether logging of Video Conversation is On or Off.  If logging is enabled, the logs can be viewed from <b>Logs &amp; Reports &gt; Log Viewer</b> . Select "IM" from "Log Modules" list.
<b>Logging Level</b>	Logging Level. <ul style="list-style-type: none"> <li>• <b>Meta Data</b> – Meta Data contains the information about the Login time, logout time. Name of User or Groups between whom the conversation happened and duration of the conversation.</li> </ul>

Table – Manage Webcam Rule screen elements

### Creating IM Webcam Rule

To add or edit a webcam rule, go to **IM > IM Rules > Webcam**. Click the Add button to add webcam rule. To update the details, click on the rule or Edit icon  in the Manage column against the rule you want to modify.

Screen – Add Webcam Rule

Screen Element	Description
<b>Name</b>	Specify a name for the Webcam Rule.
<b>Between User / IM Contact</b>	<p>Select the Participants between whom the Webcam Rule is to be defined.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• IM Contact</li> <li>• IM Contact Group</li> <li>• User</li> <li>• User Group</li> </ul> <p>You can also add above contacts from the Add Webcam Rule Page itself.</p>
<b>Action</b>	<p>Select an Action for the webcam viewing or video chat from the available options:</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• Allow</li> <li>• Deny</li> </ul>
<b>Logging</b>	<p>Enable Logging, if the log has to be maintained for the contacts.</p> <p>If logging is enabled, the logs can be viewed from <b>Logs &amp; Reports &gt; Log Viewer</b>. Select "IM" from "Log Modules" list.</p>
<b>Logging Level</b>	<p>Select the Logging Level if you have enabled Logging.</p> <p>Meta Data – Meta Data contains the information about the Login time, logout time, webcam rule defined, name of User or Groups between whom the video conversation happened and duration of the conversation.</p>

Table – Add Webcam Rule screen elements

## Content Filter

Content Filtering functionality is applied to Instant Messaging applications wherein content can be removed from the conversation if appears in the conversation.



The Content Filter page allows you to specify a list of keywords and regular expressions to be blocked, if encountered in any of the chat conversation. If content filtering is enabled from IM Conversation Rule, the configured keywords are removed and an error message is displayed for the same.

## Configure Settings

To configure content filtering expressions, go to **IM > Content Filter > Content Filter**.

Screen – Configure Content Filter Settings





Screen Element	Description
<b>RegEx Settings</b>	<p>Specify Regular Expressions to be removed from the IM applications. For example, if the string AB* is specified in the RegEx list, all the strings starting with AB would be dropped from the conversation and an error message would be displayed.</p> <p>You can add multiple regular expressions. Click Add icon  to add more expressions and remove icon  to delete expressions.</p>
<b>Keyword Settings</b>	<p>Specify Keywords to be removed from the IM applications. For example, if the strings like ammunition and terrorism are specified in the keywords list, all such strings would be dropped from the conversation and an error message would be displayed.</p> <p>You can add multiple keywords. Click Add icon  to add more keywords and remove icon  to delete keywords.</p>

Table – Configure Content Filter Setting screen elements

# QoS

Bandwidth is the amount of data passing through a media over a period of time and is measured in terms of kilobytes per second (kbps) or kilobits per second (kbits) (1 Byte = 8 bits).

The primary objective of QoS (Quality of Service) policy is to manage and distribute the total bandwidth on certain parameters and user attributes. QoS policy allocates & limits the maximum bandwidth usage of the user and controls the web and network traffic.

To configure QoS policy:

- [Define for whom you want to create policy](#)
- [Define Type of policy](#)
- [Define the Implementation strategy of the policy](#)
- [Define Bandwidth Usage](#)

## Settings

Use Settings page to configure default QoS settings. Administrator can also configure it from Command Line Interface (CLI). All the bandwidth related data are displayed only with unit KB (Kilo bytes per second).

**QoS Settings**

Bandwidth maximum limit \*  (1 - 2560000)KB

Allocation Behavior \*  Normal  Real Time

Guarantee \*  Lenient  Enforced

Default Policy \* Guaranteed  (1 - 2560000)KB

Burstable  (1 - 2560000)KB

Priority  ▾

Screen – QoS Settings

Screen Element	Description
<b>Bandwidth maximum limit</b>	<p>Specify maximum bandwidth limit in KB. It is generally a sum of all WAN links maximum limits.</p> <p>Default – 100000 KB</p> <p>Acceptable Range (KB) - 1 to 2560000</p>
<b>Allocation Behavior</b>	<p>Select bandwidth allocation behavior from the available options. It allows the administrator to handle traffic as normal or give priority to real time traffic like VOIP.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• Normal</li> <li>• Real Time</li> </ul> <p>If the bandwidth behavior is normal then priority will be applicable only for excess bandwidth i.e. bandwidth remaining after guaranteed bandwidth allocation.</p> <p>If the bandwidth behavior is real time then Real-time traffic (QoS policy with priority 0) like VOIP will be given precedence over all other traffic.</p>
<b>Guarantee</b>	<p>Select Guarantee type from the available options. Administrator can enforce all internet bound traffic to be handled by any QoS Policy applied on it. If there is no policy applied on the traffic then it will be handled by the Default Policy.</p>

	<p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• Lenient</li> <li>• Enforced</li> </ul> <p>Select 'Enforced' to enforce bandwidth restriction on the traffic on which the bandwidth policy is not applied.</p> <ul style="list-style-type: none"> <li>• Select 'Lenient' if you do not want to enforce bandwidth restriction on the traffic on which the bandwidth policy is not applied. It will only handle traffic on which QoS Policy is applied.</li> </ul>
<p><b>Default Policy</b></p> <p><b>(Available only if “Enforced” is selected)</b></p>	<p>Default Policy will be applicable on the traffic which does not have any bandwidth policy applied.</p> <p><b>Guaranteed:</b> Specify bandwidth which is the minimum guaranteed bandwidth that the user can use.</p> <p>Default – 1 KB Acceptable Range (KB) - 1 to 2560000</p> <p><b>Burstable:</b> Specify burstable bandwidth which is the maximum bandwidth that the user can use, if available.</p> <p>Default – 100000 KB Acceptable Range (KB) - 1 to 2560000</p> <p><b>Priority:</b> Set the bandwidth priority. Priority can be set from 0 (highest) to 7 (lowest) depending on the traffic required to be shaped.</p> <p>0 – Real Time For example, VOIP 1 – Business Critical 2 to 5 – Normal 6 – Bulky - FTP 7 – Best Effort – e.g. P2P</p>
<p><b>Show Bandwidth Usage</b></p>	<p>Click to view Bandwidth Usage.</p>

**Table – QoS Settings screen elements**

## QoS Policy

### Policy can be defined/created for:

- **User** – It restricts the bandwidth of a particular user.
- **Firewall Rule** – It restricts the bandwidth for any entity to which the Firewall Rule is applied.
- **Web Category** – It restricts the bandwidth for the URL categorized under the Web Category. To implement restriction, policy is to be assigned through Firewall Rule.
- **Application** – It restricts the bandwidth for the application. To implement restriction, policy is to be assigned through Firewall Rule.

### Types of Policy

Two types of bandwidth restriction can be placed:

**Strict** – In this type of bandwidth restriction, user cannot exceed the defined bandwidth limit.

**Committed** – In this type of bandwidth restriction, user is allocated the guaranteed amount of bandwidth and can draw bandwidth up to the defined burst-able limit, if available.

It enables to assign fixed minimum and maximum amounts of bandwidth to the users. By borrowing the excess bandwidth when available, users are able to burst above guaranteed minimum limits, up to the burst-able rate. Guaranteed rates also assure minimum bandwidth to critical users for receiving constant levels of bandwidth during peak and non-peak traffic periods.

Guaranteed represents the minimum guaranteed bandwidth and burst-able represents the maximum bandwidth that the user can use, if available.

### Implementation strategy

The Policy can be implemented in two ways depending on the policy Type:

- Total (Upload + Download)
- Individual Upload and Individual Download

### Strict policy

In this type of bandwidth restriction, the user cannot exceed the defined bandwidth limit. There are two ways to implement strict policy:

- Total (Upload + Download)
- Individual Upload and Individual Download

Implementation on	Bandwidth specified	Example
Total (Upload + Download)	Total bandwidth	Total bandwidth is 20 kbps upload and download combined cannot cross 20 kbps
Individual (Upload / Download)	Individual bandwidth i.e. separate for both	Upload and Download bandwidth is 20 kbps then either cannot cross 20 kbps

## Committed policy

Implementation on	Bandwidth specified	Example
Total (Upload + Download)	Guaranteed bandwidth	Guaranteed bandwidth is 20 kbps upload and download combined will get 20 kbps guaranteed (minimum) bandwidth.
	Burst-able bandwidth	Burst-able bandwidth is 50 kbps upload and download combined can get up to 50 kbps of bandwidth (maximum), if available.
Individual (Upload / Download)	Individual Guaranteed and Burstable bandwidth i.e. separate for both	Individual guaranteed bandwidth is 20 kbps Individually get 20 kbps guaranteed (minimum) bandwidth.  Individual burstable bandwidth is 50 kbps Individually get maximum bandwidth up to 50 kbps, if available.

## Bandwidth Usage

Policy can be configured for two types of bandwidth usage:

- **Individual** – Allocated bandwidth is for the particular user only.
- **Shared** – Allocated bandwidth is shared amongst all the users who have been assigned this policy.

The Appliance is shipped with predefined QoS policies. These predefined policies are immediately available for use until configured otherwise. You can also define custom policies to meet your organization's requirements.

## Manage QoS Policy list

To manage QoS Policies, go to **QoS > Policy > Policy**.

The Policy page displays a list of predefined and custom policies and provides option to create a new QoS policy, schedule QoS policy, update parameters, or delete the policy.

To Schedule the QoS policy:

- Navigate to **QoS > Policy > Policy** page.
- Edit the policy to which you want to add schedule configuration.
- Click Add and update the schedule details.

Add		Delete		Records Per Page 20				(1 of 6)	
<input type="checkbox"/>	Name	Restriction Type	Total Bandwidth (in KB)(Min/Max)	Upload Bandwidth (in KB)(Min/Max)	Download Bandwidth (in KB)(Min/Max)	Manage			
<input type="checkbox"/>	128kbps link_Policy A	User Based Individual	8/16	-	-				
<input type="checkbox"/>	128kbps link_Policy A	User Based Individual	8/16	-	-				
<input type="checkbox"/>	128kbps link_Policy A	User Based Individual	8/16	-	-				
<input type="checkbox"/>	128kbps link_Policy B	User Based Individual	4/16	-	-				
<input type="checkbox"/>	128kbps link_Policy FWR	Firewall Rule Based	4/16	-	-				

Records Per Page 20 (1 of 6)

Screen – Manage QoS Policies

**Note**

- QoS Policy assigned to any Group or User cannot be deleted.

Screen Element	Description
<b>Name</b>	Displays the name of the QoS Policy.
<b>Restriction Type</b>	Displays the type of restriction based on Bandwidth Usage and Policy implemented.
<b>Total Bandwidth (in KB) (Min/Max)</b>	Displays the Total Bandwidth provided including Upload and Download in KB.  For example, 8/16 for min/max size.
<b>Upload Bandwidth (in KB) (Min/Max)</b>	Displays the Upload Bandwidth provided in KB.  For example, 8/16 KB for min/max size.
<b>Download Bandwidth (in KB) (Min/Max)</b>	Displays the Download Bandwidth provided in KB.  For example, 8/16 KB for min/max size.

Table – Manage QoS Policies screen elements

**Creating a new QoS Policy**

To add or edit a QoS policy, go to **QoS > Policy → Policy**. Click the Add button to add QoS policy. To update the details, click on the policy or Edit icon in the Manage column against the policy you want to modify.

**Add QoS Policy**

Name \*

Policy Based On  User  Firewall Rule  Web Category  Application

Policy Type  Strict  Committed

Implementation On  Total (Upload + Download)  Individual (Upload / Download)

Priority \*

Total Bandwidth (in KB) \*  (Must be a number between 2 and 10240000)

Bandwidth Usage Type  Individual  Shared

Description

OK Cancel

Screen – Add a QoS Policy

Screen Element	Description
<b>Add QoS Policy</b>	
<b>Name</b>	Specify a name to identify the Policy. Duplicate names are not allowed.
<b>Policy Based On</b>	<p>Select an option to specify for whom the policy is to be created. receive</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>User</b> – Restricts the bandwidth of a particular user.</li> <li>• <b>Firewall Rule</b> – Restricts the bandwidth of any entity to which Firewall Rule is applied.</li> <li>• <b>Web Category</b> – Restricts the bandwidth for the URL categorized under the Web category.</li> <li>• <b>Application</b> – Restricts the bandwidth for the applications categorized under the Application category.</li> </ul>
<b>Policy Type</b>	<p>Select the type of policy.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Strict</b> – In this type of policy, user cannot exceed the defined bandwidth limit.</li> <li>• <b>Committed</b> – In this type of policy, user is allocated the guaranteed amount of bandwidth and can draw bandwidth up to the defined burst-able limit, if available.</li> </ul> <p>It enables to assign fixed minimum and maximum amounts of bandwidth to the users. By borrowing excess bandwidth when available, users are able to burst above guaranteed minimum limits, up to the burst-able rate. Guaranteed rates also assure minimum bandwidth to critical users to receive constant levels of bandwidth during peak and non-peak traffic periods.</p> <p>Guaranteed represents the minimum guaranteed bandwidth and burst-able represents the maximum bandwidth that the user can use, if available.</p>



<b>Implementation On</b>	Select any one option to specify implementation strategy of policy. See <a href="#">Implementation Strategy</a> for more details.
<b>Priority</b>	<p>Set the bandwidth priority. Priority can be set from 0 (highest) to 7 (lowest) depending on the traffic required to be shaped.</p> <p>0 – Real Time e.g. VOIP  1 – Business Critical  2 to 5 - Normal  6 – Bulky - FTP  7 – Best Effort e.g. P2P</p> <p>By default, priority is given to the real time traffic. However, if administrator does not want this preference, feature can be disabled using CLI command - set bandwidth allocation-behavior normal. If required, it can be enabled by CLI command - set bandwidth allocation-behavior real-time.</p> <p>If the bandwidth behavior is normal then priority will be applicable only for excess bandwidth i.e. bandwidth remaining after guaranteed bandwidth allocation.</p> <p>If the bandwidth behavior is real-time then Real-time traffic (QoS policy with priority 0) like VOIP will be given precedence over all other traffic.</p> <p>As priority is given to the real time traffic, it is possible that some non real-time traffic will not get their minimum guaranteed bandwidth. Specifically, if sum of burstable (max allowed) of all bandwidth policies (real-time and non real-time) is greater than total max-limit then guarantee of the real-time policies will be fulfilled but non real-time might not get the minimum guaranteed bandwidth.</p>
<b>Total Bandwidth (in KB)</b>	<p>Specify allowed Total or Individual and Guaranteed-Burst-able bandwidth depending on <a href="#">Policy Type</a> and <a href="#">Implementation strategy</a>.</p> <p>Total Bandwidth Range: 2 – 10240000KB.</p> <p>Burst-able bandwidth should be greater than or equal to guaranteed bandwidth.</p>
<b>Bandwidth Usage Type</b>	<p>Select the type of bandwidth usage.</p> <p><b>Available Options:</b></p> <ul style="list-style-type: none"> <li>• <b>Individual</b> – Allocated bandwidth is for the particular user only.</li> <li>• <b>Shared</b> – Allocated bandwidth is shared among all the users who have been assigned this policy.</li> </ul>


<b>Description</b>	Provide Policy Description.
--------------------	-----------------------------

Table – Add a QoS Policy screen elements

## Scheduling QoS Policy

You can implement the QoS at the schedule time or override the QoS policy parameters for certain time period defined in the schedule. Navigate to QoS > Policy > Policy page and edit the policy which you want to schedule.

## Manage Schedule list

Go to **QoS > Policy > Policy**. Click Edit icon  against a QoS policy to manage Schedule wise QoS Policy Details.

**Edit QoS Policy**

Name \*

Policy Based On  User  Firewall Rule  Web Category  Application

Policy Type  Strict  Committed

Implementation On  Total (Upload + Download)  Individual (Upload / Download)

Priority \*



Guaranteed - Burstable (in KB) \*  -  (between 2-10240000 KB)

Bandwidth Usage Type  Individual  Shared

Description

**Add Schedule wise QoS Policy Details to override default QoS Policy Details.**

Records Per Page    (1 of 1)

<input type="checkbox"/>	Schedule	Policy Type	Bandwidth (Min/Max)	Upload Bandwidth (Min/Max)	Download Bandwidth (Min/Max)	Manage
<input type="checkbox"/>	All Days 10:00 to 19:00	Strict	2/234	-	-	 


Records Per Page    (1 of 1)

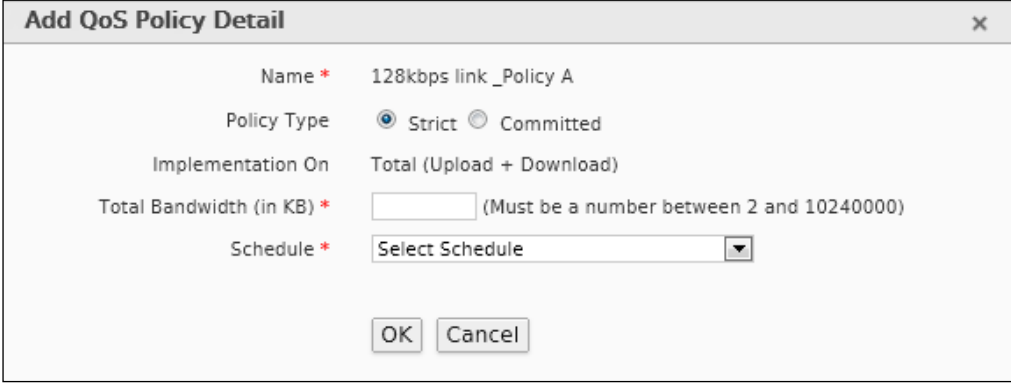
Screen – Add a QoS Policy Schedule

Screen Element	Description
<b>Add Schedule wise QoS Policy Details to override the default QoS Policy Details</b>	
<b>Schedule</b>	Displays the schedule for Policy selected.
<b>Policy Type</b>	Displays the type of Policy: Strict or Committed.
<b>Bandwidth (Min/Max)</b>	Displays the Total Bandwidth provided including Upload and Download in KB. For example, 8/16 for min/max size.
<b>Upload Bandwidth (Min/Max)</b>	Displays the Download Bandwidth provided in KB For example, 8/16 KB for min/max size.
<b>Download Bandwidth (Min/Max)</b>	Displays the Upload Bandwidth provided in KB For example, 8/16 KB for min/max size.

Table – Manage Schedule screen elements

## Policy Schedule Parameters

Go to **QoS > Policy > Policy** and click Edit icon  against a QoS policy. Click the Add button to configure Schedule wise QoS Policy Detail.



Screen – Add a QoS Policy Schedule

Screen Element	Description
<b>Name</b>	Displays policy name.
<b>Policy Type</b>	Displays default Policy Type set at the time of creation of policy, modify if required.  Configured policy type overrides the default policy and is applicable only for the selected scheduled time interval.
<b>Implementation On</b>	Displays default Implementation strategy set at the time of creation of policy, modify if required.  Configured policy type overrides the default policy and is applicable only for the selected scheduled time interval.
<b>Total Bandwidth (in KB)</b>	Displays allocated Total or Individual and Guaranteed -Burstable bandwidth depending on Policy Type and Implementation strategy. Modify if required.  The modified bandwidth restriction is applicable only for the selected time interval.
<b>Schedule</b>	Select Schedule from the list available during which the QoS policy will be applied.  Only Recurring Schedule can be applied.  If you are not sure about the Schedule details, select Schedule to view the Schedule details.

Table – Add a QoS Policy Schedule screen elements

# Logs & Reports

The Appliance provides extensive logging capabilities for traffic, system and network protection functions. Detailed log information and reports provide historical as well as current analysis of network activity to help identify security issues and reduce network abuse.

The Appliance can either store logs locally or send logs to external syslog servers for storage and archival purposes.

The Appliance can log many different network activities and traffic including:

- Firewall log
- Anti Virus infection and blocking
- Web filtering, URL and HTTP content blocking
- Signature and anomaly attack and prevention
- Spam filtering
- IM logs
- Administrator logs
- User Authentication logs
- VPN – IPSec, L2TP, PPTP
- WAF logs
- ICAP logs

The Appliance can either store logs locally or send to the syslog servers. Traffic Discovery logs can be stored locally only.

- [Configuration](#)
- [Log Viewer](#)
- [4-Eye Authentication](#)

## Configuration

Syslog is an industry standard protocol/method for collecting and forwarding messages from devices to a server running a Syslog daemon usually via UDP Port 514. Syslog is a remote computer running a Syslog Server. Logging to a central Syslog Server helps in aggregation of logs and alerts.

The Appliance sends a detailed log to an external Syslog server in addition to the standard event log. Syslog support requires an external server running a Syslog daemon on any of the UDP Port. When configuring logging to a Syslog server, one needs to configure the facility, severity and log file format. One can also specify logging location if multiple Syslog servers are defined.

The Appliance captures all log activity and includes every connection source and destination IP Address (IPv4/IPv6), IP service, and number of bytes transferred.

A SYSLOG service simply accepts messages, and stores them in files or prints. This form of logging is the best as it provides a central logging facility and a protected long-term storage for logs. This is useful both in routine troubleshooting and in incident handling.

- [Syslog Servers](#)
- [Log Settings](#)
- [Netflow](#)

## Syslog Servers

The Syslog Servers page displays a list of configured syslog servers. You can sort this list based on server name. The page also provides option to add, update, or delete the server.

### Manage Syslog Server list

To manage Syslog servers, go to **Logs & Reports > Configuration > Syslog Server**.

<input type="checkbox"/>	Name	Server IP	Port	Facility	Severity	Format	Manage
<input type="checkbox"/>	Central_Management	10.103.7.1	514	DAEMON	Debug	CyberoamStandardFormat	
<input type="checkbox"/>	Cyberoam	1.1.1.1	80	DAEMON	Emergency	CyberoamStandardFormat	

Screen – Manage Syslog Servers

Screen Element	Description
<b>Name</b>	Displays name of the Syslog Server.
<b>Server IP</b>	IP Address of the server.
<b>Port</b>	Displays the server port.
<b>Facility</b>	Displays the facility configured for log messages.
<b>Severity</b>	Displays the severity level configured for logged messages.
<b>Format</b>	Displays log format.

Table – Manage Syslog Server screen elements

### Syslog Server Parameters

You can configure maximum five syslog servers.

To add or edit Syslog Server details, go to **Logs & Reports > Configuration > Syslog Servers**. Click Add Button to add a new server or Edit Icon to modify the details of the server.

Name *	<input type="text" value="Enter Name"/>
IP Address / Domain *	<input type="text" value="Enter IP Address"/>
Port *	<input type="text" value="Enter Port"/>
Facility *	DAEMON ▾
Severity Level *	Emergency ▾
Format *	CyberoamStandardFormat ▾
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Screen – Add Syslog Server

Screen Element	Description
<b>Name</b>	Provide a unique name for Syslog Server.
<b>IP Address / Domain</b>	Specify IP Address (IPv4/IPv6) or domain name of the Syslog Server. Messages from the Appliance will be sent to the server.
<b>Port</b>	Specify the port number for communication with the Syslog Server. The Appliance will send messages using the configured port.
<b>Facility</b>	<p>Select Syslog facility for log messages to be sent to the Syslog Server.</p> <p>Facility indicates to the Syslog Server the source of a log message. It is defined by the Syslog protocol. You can configure facility to distinguish log messages from different Appliances. In other words, it can be helpful in identifying the device that recorded the log file.</p> <p>The Appliance supports following Syslog facilities for log messages received from the remote servers and network devices:</p> <p>Available Options:</p> <ul style="list-style-type: none"> <li>• <b>DAEMON</b> – Daemon logs (Information of Services running in Appliance as daemon).</li> <li>• <b>KERNEL</b> – Kernel log</li> <li>• <b>LOCAL0</b> – LOCAL7 – Log level information.</li> <li>• <b>USER</b> – Logging based on users who are connected to the Server.</li> </ul>
<b>Severity Level</b>	<p>Specify severity levels of logged messages.</p> <p>Severity level is the severity of the message that has been generated.</p> <p>Appliance logs all the messages at and above the logging severity level you select. For example, select 'ERROR' to log</p>

	<p>all messages tagged as 'ERROR,' as well as any messages tagged with 'CRITICAL,' 'ALERT' and 'EMERGENCY' and select 'DEBUG' to log all messages.</p> <p>Appliance supports following Syslog levels:</p> <ul style="list-style-type: none"> <li>• EMERGENCY – System is not usable</li> <li>• ALERT – Action must be taken immediately</li> <li>• CRITICAL – Critical condition</li> <li>• ERROR – Error condition</li> <li>• WARNING – Warning condition</li> <li>• NOTIFICATION – Normal but significant condition</li> <li>• INFORMATION – Informational</li> <li>• DEBUG – Debug - level messages.</li> </ul>
<b>Format</b>	Appliance produces logs in the specified format. The Appliance currently produces logs in its own Cyberoam Standard Format.

**Table – Add Syslog Server screen elements**

Once you add the server, go to **Logs & Reports > Configuration > Log Settings** page and enable all those logs, which are to be sent to the Syslog Server.



## Log Settings

After configuring Syslog server, configure logs to be sent to the Syslog server. If multiple Syslog servers are configured, you can send various logs on different servers.

To record logs you must enable the respective log and specify logging location. The Administrator can choose between On-Appliance (local) logging and Syslog logging. The Administrator can also disable logging temporarily.

### Manage Log Type list

To manage Syslog servers, go to **Logs & Reports > Configuration > Log Settings**.

Log Type(System)	Local	Syslog	
		Central_Management	Cyberoam
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Firewall	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> IPS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Anti Virus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Anti Spam	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Content Filtering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Events	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> WAF	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Screen – Configure Log Settings

Screen Element	Description
Log Type(System)	Displays the various logs.
Local	Displays the logging location.
<b>Syslog</b>	
Central_Management	Displays Central Management logs.
Cyberoam	Displays Cyberoam Logs

Table – Configure Log Setting screen elements

The Appliance logs many different network activities and traffic including:

## Firewall Log

Firewall Log records invalid traffic, local ACL traffic, DoS attack, ICMP redirected packets, source routed and fragmented traffic. Firewall logs can be disabled or send to the remote syslog server only but cannot be stored locally.

- **Firewall Rules**  
Log records the entire traffic for Firewall.
- **Invalid Traffic Log**  
Log records the dropped traffic that does not follow the protocol standards, invalid fragmented traffic and the traffic whose packets or Appliance is not able to relate to any connection.
- **Local ACLs Log**  
Log records the entire (allowed and dropped) incoming traffic.
- **DoS Attack Log**  
The DoS Attack Log records attacks detected and prevented by the Appliance i.e. dropped TCP, UDP and ICMP packets.

To generate logs, go to **Firewall > DoS > Settings** and click “Apply Flag” against SYN Flood, UDP Flood, TCP Flood, and ICMP Flood individually.

- **Dropped ICMP Redirected Packet Log**  
Log records all the dropped ICMP redirect packets.  
  
To generate log, go to **Firewall > DoS > Settings** and click “Apply Flag” against “Disable ICMP redirect Packets”.

- **Dropped Source Routed Packet Log**  
Log records all the dropped source routed packets.  
  
To generate log, go to **Firewall > DoS > Settings** and click “Apply Flag” against “Drop Source Routed Packets”.

- **Dropped Fragmented Traffic**  
Log records the dropped fragmented traffic.
- **MAC Filtering**  
Log records the dropped packets when filtering is enabled from Spoof prevention.
- **IP-MAC Pair Filtering**  
Log records the dropped packets when filtering is enabled from Spoof prevention.
- **IP Spoof Prevention**  
Log records the dropped packets when filtering is enabled from Spoof prevention.
- **SSL VPN**  
Log records of SSL VPN traffic.

- **Virtual Host**  
Log records of Virtual Host traffic.
- **ICMP Error Message**  
Log records of ICMP error messages such as network/host/port unreachable, destination network/host unknown and so on.

### **IPS Logs**

Records detect and drop attacks based on unknown or suspicious patterns (anomaly) and signatures.

### **Anti Virus Logs**

Viruses detected in HTTP, SMTP, FTP, POP3, IMAP4, HTTPS and IM traffic. HTTP and FTP logs can be disabled or sent to the remote log server only.

### **Anti Spam Logs**

SMTP, POP3, IMAP4 spam and probable spam mails.

### **Content Filtering Logs**

Web Filtering, Application Filtering and IM logs.

### **Event Logs**

Admin Events, Authentication Events and System Events.

### **WAF Logs**

Alert Events and Allowed Events.



#### **Note**

- WAF logs are not available in CR10iNG, CR15i, CR15wi, CR15iNG, CR15wiNG, CR25ia, CR25wi, CR35ia and CR35wi Cyberoam Appliances.

## Netflow

To configure Netflow, go to **Logs & Reports > Configuration > Netflow**.

Netflow is a flow technology used for network bandwidth monitoring. Details of the traffic passing through the firewall rule can be exported as NetFlow records to the Netflow Server. Based on the records received by the Netflow Server, data analyzing tools like Open Source Data Analyzer and PRTG software can generate reports.

The Netflow page displays list of configured netflow servers. The page also provides option to add, update, or delete the server. Use  to add and  to delete Netflow Server.

### Note

- Only traffic of Firewall rules where "Log Firewall Traffic" is enabled will be sent to the NetFlow Server.
- You can configure maximum five Netflow Servers.
- Cyberoam supports NetFlow v5 and all the parameters of v5 can be exported.

Netflow Configuration			
Netflow Configuration	Server Name	Netflow Server IP/Domain	Netflow Server Port
	Cyberoam	1.1.1.1	2055
<input type="button" value="Apply"/>			

### Screen – Add Netflow Servers

Screen Element	Description
<b>Netflow Configuration</b>	
<b>Server Name</b>	Specify a unique name for Netflow server.
<b>Netflow Server IP/Domain</b>	Specify IP Address (IPv4 / IPv6) or domain name of the Netflow Server.
<b>Netflow Server Port</b>	Specify the UDP port number for communication with the Netflow Server. NetFlow records will be sent on the specified port.  Default - 2055

Table – Add Netflow Server screen elements

## Log Viewer

View the logs for modules like IPS, Web Filter, Anti Spam, Anti Virus and Firewall from Log Viewer page. This page gives consolidated information about all the events that have occurred.

To view and manage logs, go to **Logs & Reports > Log Viewer > Log Viewer**.

- [View Log Modules](#)
- Set Refresh Interval – Select the refresh interval for refreshing the logs automatically. Choose the time or click Refresh button to refresh the logs.
- [De-Anonymize](#)

### View Log Modules

- [System](#) – System logs provide information about all the system related logs. System logs also include logs for VPN events.  
Note: MAC Address is displayed under Message for Log Comp – DHCP.
- [Web Filter](#) – Web Filter logs provide information about the users that were detected accessing restricted URLs and the action taken by the Appliance.
- [Application Filter](#) – Application Filter logs provide information about applications whose access was denied by the Appliance.
- [IM](#) – IM logs provide information about Instant Messaging logs that are enabled. Logging, Conversation, File Transfer and Webcam.
- [Anti Virus](#) – Anti Virus logs provide information about the Viruses identified by Appliance.
- [Anti Spam](#) – Anti Spam logs provide information about the spam mails identified by Appliance.
- [Firewall](#) – Firewall logs provide information about how much traffic passes through a particular Firewall rule and through which interfaces.
- [IPS](#) – IPS logs provide information about the signatures that were detected.
- [Authentication](#) – Authentication logs provide information about all the authentication logs including Firewall, VPN and My Account authentication.
- [Admin](#) – Admin logs provide information about administrator event and tasks.
- [WAF](#) – WAF logs provide information about HTTP/S requests and action taken on the same.
- [ICAP](#) – ICAP logs provide information about the ICAP events.

### View list of System events

Screen Element	Description
<b>Time</b>	Time when the event occurred.
<b>Log Comp</b>	Displays the Log Components of the System event.  Type of Log Components – HTTP, HA, Central Management, IPSec, L2TP, PPTP, SSL VPN, Appliance, DHCP Server, Interface, Gateway, DDNS, Web cat, IPS, Anti Virus, Dial-In, Quarantine, WLAN, HTTPS, Guest User, Virtual Host, Wireless Protection and CTA.
<b>Status</b>	Successful or failed.

<b>User Name</b>	Username of the user.
<b>Message</b>	Message for the type of system event.
<b>Message ID</b>	Message ID of the message.

### View list of Web Filter events

Screen Element	Description
<b>Time</b>	Time when the event occurred.
<b>Action</b>	Allowed or Denied.
<b>User Name</b>	Username of the user that accessed the URL.
<b>Source IP</b>	Source IP Address (IPv4/IPv6).
<b>Destination IP</b>	Destination IP Address (IPv4/IPv6).
<b>Category</b>	Category under which the URL comes.
<b>URL</b>	URL accessed.
<b>Bytes Transfer</b>	No. of bytes transferred.
<b>Message ID</b>	Message ID of the message.

### View list of Application Filter events

Screen Element	Description
<b>Time</b>	Time when the event occurred.
<b>Action</b>	Denied
<b>User Name</b>	Username of the user that accessed the application.
<b>Source IP</b>	Source IP Address (IPv4/IPv6).
<b>Destination IP</b>	Destination IP Address (IPv4/IPv6).
<b>Application Category</b>	Category under which the Application is categorized.
<b>Application</b>	Name of the application denied.
<b>Firewall Rule</b>	Firewall rule ID applied to the traffic.
<b>Message ID</b>	Message ID of the message.

### View list of IM events

Screen Element	Description
<b>Time</b>	Time when the event occurred.
<b>IM Action</b>	Displays the IM Action.  Action: Message, File transfer, Webcam, Login and Logout.
<b>Rule Action</b>	Rule action defined – Allowed or Denied.
<b>Protocol</b>	Type of Protocol used – Yahoo or MSN.

<b>User Name</b>	Username of the user.
<b>IP Address</b>	IP Address (IPv4/IPv6) of the user.
<b>Protected Contact</b>	Displays the Email ID of the participant protected by Cyberoam.
<b>Peer Contact</b>	Displays the Email ID of the other participant.  This participant may/may not be protected by Cyberoam.
<b>Message</b>	Message for the type of IM event.
<b>Message ID</b>	Message ID of the message.

### View list of Anti Virus events

Screen Element	Description
<b>Time</b>	Time when the event occurred.
<b>Protocol</b>	Displays name of the protocol.  Types of protocol: HTTP, HTTPS, FTP, POP, IMAP, SMTP and SMTPS.
<b>User Name</b>	Username on the user on whose system virus was detected.
<b>Source IP</b>	Source IP Address (IPv4/IPv6)
<b>Destination IP</b>	Destination IP Address (IPv4/IPv6).
<b>Virus</b>	Name of the Virus detected.
<b>Message</b>	Message for the Virus detected.
<b>Message ID</b>	Message ID of the message.

### View list of Anti Spam events

Screen Element	Description
<b>Time</b>	Time when the event occurred.
<b>Log Comp</b>	Displays the Log Components of the Anti Spam events.  Types of Log Components: SMTP, SMTPS, POP and IMAP.
<b>Action</b>	Displays action taken against any Anti Spam events.  Actions: Reject, Drop, Accept, Change Recipient and Prefix Subject.
<b>User Name</b>	Username on the user on whose system, spam was detected.
<b>Source IP</b>	Source IP Address (IPv4/IPv6).
<b>Destination IP</b>	Destination IP Address (IPv4/IPv6).
<b>Email Sender</b>	Spam Email sender IP Address.
<b>Email Receiver</b>	Spam Email recipient IP Address.

<b>Email Subject</b>	Subject of the Email.
<b>Message</b>	Message for the Virus detected.
<b>Message ID</b>	Message ID of the message.

### View list of Firewall events

Screen Element	Description
<b>Time</b>	Time when the event occurred.
<b>Log Comp</b>	Displays the Log Components of the Firewall events.  Types of Log Components: Firewall Rule, Invalid Traffic, Local ACL, DoS Attack, ICMP Redirection, Source Routed, Fragmented Traffic, Foreign Host, IPMAC Filter, IP Spoof, Virtual Host and ICMP Error Message.
<b>Action</b>	Allowed or Denied.
<b>User Name</b>	Username of user on which Firewall rule is applied.
<b>Firewall Rule</b>	Firewall Rule ID.
<b>In Interface</b>	Interface through which the traffic is coming in.
<b>Out Interface</b>	Interface through which the traffic is going out.
<b>Source IP</b>	Source IP Address (IPv4/IPv6).
<b>Destination IP</b>	Destination IP Address (IPv4/IPv6).
<b>Message ID</b>	Message ID for the Virus detected.

### View list of IPS events

Screen Element	Description
<b>Time</b>	Time when the event occurred.
<b>Log Comp</b>	Displays the Log Components of IPS events.  Types of Log Components: Anomaly and Signatures.
<b>Action</b>	Detect or Drop.
<b>User Name</b>	Username of the user that triggered the signature.
<b>Source IP</b>	Source IP Address (IPv4/IPv6).
<b>Destination IP</b>	Destination IP Address (IPv4/IPv6).
<b>Signature ID</b>	Signature ID of the signature.
<b>Signature Name</b>	Name for the detected Signature.
<b>Firewall Rule</b>	Firewall Rule applied.
<b>Message ID</b>	Message ID of the message.



## View list of Authentication events

Screen Element	Description
<b>Time</b>	Date and Time when the event occurred.
<b>Log Comp</b>	Displays the Log Components of Authentication events.  Type of Log Components: Firewall Authentication, VPN Authentication, SSL VPN Authentication, My Account Authentication, Dial-In Authentication, and NTLM Authentication.
<b>Status</b>	Successful or failed.
<b>User Name</b>	Username of the user.
<b>IP Address</b>	IP Address of the user.
<b>Auth. Client</b>	Authentication client which is used for authentication: Web Client, Corporate Client or CTA.
<b>Auth. Mechanism</b>	Type of Authentication Mechanism: Local or External Server (AD, LDAP or RADIUS).
<b>Message</b>	Message for the type of authentication event.
<b>Message ID</b>	Message ID of the message.

## View list of Admin events

Screen Element	Description
<b>Time</b>	Time when the event occurred.
<b>Log Comp</b>	Displays type of Log Components of Admin events.  Types of Log Components: GUI, CLI, Console, Central Management.
<b>Status</b>	Successful or failed.
<b>User Name</b>	Username of the admin user.
<b>IP Address</b>	IP Address of the admin user.
<b>Message</b>	Message for the type of Admin event.
<b>Message ID</b>	Message ID of the message.

## View list of WAF events

Screen Element	Description
<b>Time</b>	Time when the event occurred.
<b>Action</b>	Displays action taken against any Web Application events.
<b>Web Server Name</b>	Displays a name for the web server,
<b>Source IP/Name</b>	Source IP Address or Name.

<b>Message</b>	Message for the WAF event.
<b>URL</b>	URL accessed.
<b>Reason</b>	Reason for the action taken on any Web Application.
<b>Status Code</b>	Status code of the action taken on the Web Application.
<b>Bytes Transferred</b>	Displays the bytes of information transferred.
<b>Message ID</b>	Message ID of the message.

### View list of ICAP events



Screen Element	Description
<b>Time</b>	Time when the event occurred.
<b>Action</b>	Displays action taken by server from the below: <ul style="list-style-type: none"> <li>• No Change</li> <li>• Body Modified</li> <li>• Header modified</li> <li>• 4xx_Error</li> <li>• 5xx_Error</li> <li>• Denied</li> </ul>
<b>Mode</b>	Mode in which ICAP Server is configured (Request/Response)
<b>User Name</b>	Username of user that accessed the URL.
<b>Source IP</b>	Source IPv4 Address.
<b>Destination IP</b>	Destination IPv4 Address.
<b>URL</b>	URL accessed.
<b>Bytes Transferred</b>	Displays number of bytes transferred from the appliance to ICAP Server.
<b>Server Tag</b>	Unique tag used by Server.
<b>X-Info</b>	Displays messages sent by server.
<b>Message ID</b>	Message ID of the message.

## De-Anonymize

The Appliance anonymizes all the user identities - Username, IP Address, MAC Address, Email Address and IM Contact ID in all logs / reports. It means user identities in all the reports are displayed in encrypted form.

To view the actual details, IT Administrator has to de-anonymize. To de-anonymize, approval from one of the authorizers configured on the Settings page is required.

To de-anonymize:

1. Click Copy icon  against the Username, IP Address, MAC Address, Email Address or IM Contact ID to be de-anonymized.
2. Click De-anonymize icon . It will open a pop-up.
3. Select the authorizer and enter the authorizer's password.
4. Select for how long the de-anonymized data is to be kept. Available options: For this search, Session and Permanent.
5. Select the type of string to be de-anonymized - Username, IP Address (IPv4/IPv6), MAC Address, Email Address or IM Contact ID

## 4-Eye Authentication

Appliance logs and reports provide organizations with visibility into their networks for high levels of security, data confidentiality while meeting the requirements of regulatory compliance.

Cyberoam collects current log data and provides near real-time reports in graphical and tabular format. It offers user identity-based reporting across applications, protocols and multiple Appliances allowing organizations to see “Who is doing What” anywhere in the network. It offers wide spectrum of 1000+ unique reports to get in-depth network visibility help organizations to take corrective and preventive measures.

For legal compliant logging, reporting and archiving, it is important that an organization follows all the obligations for keeping relevant information archived and accessible all the time. To maintain the security, it also required to monitor the logs related to user-specific activities. On the other hand, the organization must also not invade its employee’s privacy.

Monitoring user-specific activities without the consent or the presence of the employee or their delegate is illegal. Internal protection is necessary when a person can access activity logs of other employees.

In an organization, usually the IT Administrator has access permissions to view the user activity logs to ensure security. However, administrator can violate the organization’s privacy regulations and have insight to confidential documents and can misuse to track user activities.

To prevent a single administrator from having complete control over the logs, Appliance has implemented a Four-Eye authentication. It enhances the already existing logging and security mechanisms by adding an additional administrator, without whose permission access cannot be granted.

In this system, Administrator can view user (employee) specific activities / logs /reports only if an Independent Authorized person approves it.

Once it is enabled, Four-Eye authentication can be used to prevent unauthorized access to private data. To view user specific logs, two authorized administrators must log on. Additionally, data can also be anonymized to enhance privacy protection.

- [Settings](#)
- [De-Anonymize](#)

## Settings

Enable Four-Eye Authentication for IT Administrator to view or download user-specific activities, logs or reports. Apart from the IT Administrator, at least one independent authorizer with the administrative privileges is required.

Once enabled:

1. All the user identities - Username, IP Address (IPv4 / IPv6), MAC Address, Email Address and IM Contact ID in all logs /activities / reports are anonymized.
2. If the IT administrator wants to de-anonymize the above mentioned user details, an approval is required from all the authorizers.
3. To disable Four-Eye Authentication, approval from both the authorized people is required.

Screen – 4-Eye Authentication

Screen Element	Description
<b>Enable 4-Eye Authentication</b>	Enable “4-Eye Authentication” to enable administrator to view or download user-specific activities, logs or reports.
<b>Select Authorizer</b>	“Administrator List” displays all the administrators.  Click the checkbox to select the administrator. All the selected administrators are moved to “Selected Authorizer” list.

Table – 4-Eye Authentication

## De-Anonymize

To comply with the Data Privacy Law, it is necessary to protect individual data. The Appliance anonymizes data to achieve this by encrypting the log data in a random manner.

The Appliance anonymizes all the user identities - Username, IP Address (IPv4/IPv6), MAC Address, Email Address and IM Contact ID in all logs /activities / reports. It means user identities in all the reports are displayed in encrypted form.

To view the actual details, the IT Administrator has to de-anonymize. To de-anonymize, approval from one of the authorizers configured on the Settings page is required.

Screen Element	Description
<b>Users</b>	Select Username(s) to be de-anonymized.
<b>IP</b>	Add IP Address(s) (IPv4/IPv6) to be de-anonymized.
<b>Advanced Settings (MAC Address, Email, IM Contact)</b>	
<b>MAC</b>	Add MAC Address to be de-anonymized.
<b>Email</b>	Add Email Address to be de-anonymized.
<b>IM Contact</b>	Add IM Contact to be de-anonymized.

**Table – De-Anonymize**

Users

User List	Selected User
<input type="checkbox"/> cyberoam	
<input type="checkbox"/> admin	
<input type="checkbox"/> 1.1.1.1	
<input type="checkbox"/> 192.168.10.1	
<input type="checkbox"/> marie	
<input type="checkbox"/> 1.1.1.2	
<input type="checkbox"/> 1.1.1.3	
<input type="checkbox"/> 1.1.1.4	
<input type="checkbox"/> 1.1.1.5	

IP

Search / Add Add

192.168.10.10

Advanced Settings (MAC Address, Email, IM Contact)

MAC

Search / Add Add

01:02:03:04:05:06

Email

Search / Add Add

test@cyberoam.com

IM Contact

Search / Add Add

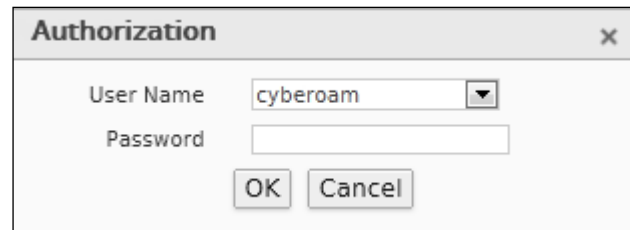
Test

Apply

### Screen – De-Anonymize

Once approved, all the logs and reports are displayed with the actual user details and not in the encrypted form. Click the Apply button. An Authorization Window will pop-up.

In addition, you can De-Anonymize from the Reports.



The screenshot shows a dialog box titled "Authorization". It has a close button (X) in the top right corner. The dialog contains two input fields: "User Name" with a dropdown menu showing "cyberoam" and a small downward arrow, and "Password" with a text input field. Below the input fields are two buttons: "OK" and "Cancel".

**Screen – Authorization**

Screen Elements	Description
User Name	Select the User Name.
Password	Provide the password for approval.

**Table – Authorization**