Cyberoam
A SOPHOS Company

QUICK START GUIDE
CR10wiNG Appliance

Document Version: PL QSG 10wiNG/96000-10.6.1/14082014

1 DEFAULTS

Default IP addresses

Ethernet Port	IP Address	Zone
A	172.16.16.16/255.255.255.0	LAN
B	IP via DHCP	WAN

Default Username & Password

Web Admin Console	
*Username	admin
*Password	admin

CLI Console (SSH/Serial Connection)	
*Password	admin

* Username and Password are case sensitive

Package Contents

Checking the package contents - Check that the package contents are complete.

- Cyberoam Appliance
- Serial Cable
- AC Power Adapter
- Detachable WiFi Antennas
- Cyberoam Quick Start Guide
- Straight-through Ethernet Cable

Serial Cable

AC Power Adapter with Cable

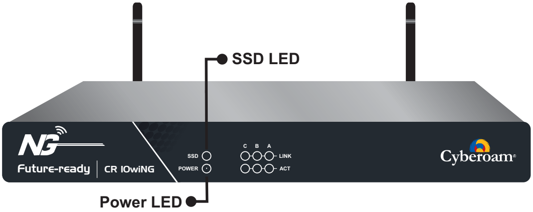
Quick Start Guide

Straight-through Ethernet Cable

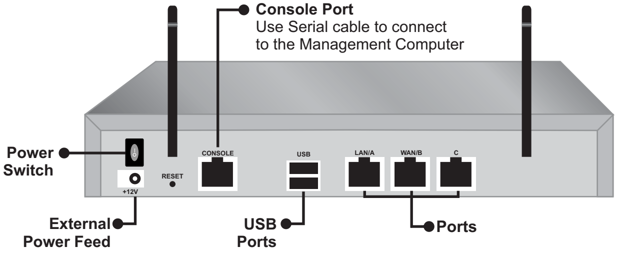
If any items from the package are missing. please contact Cyberoam Support at support@cyberoam.com

2 UNDERSTANDING THE APPLIANCE

► FRONT PANEL



► BACK PANEL



As Cyberoam does not pre-configure any ports for LAN, WAN, DMZ networks, it is not necessary to use any particular port for them. Usage of ports depends on how the physical connection is required or planned.

Before configuring, you need to plan the deployment mode of Cyberoam. Cyberoam can be placed in Bridge or Gateway/Route mode according to your requirement.

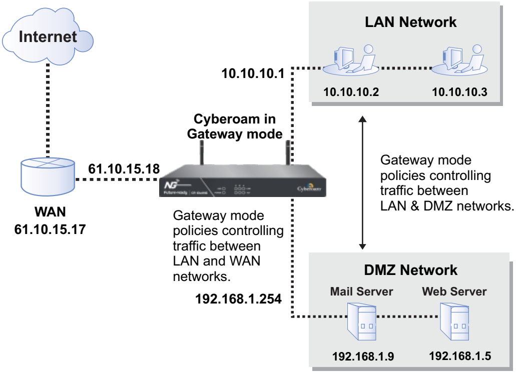
To control the Internet access through Cyberoam the entire Internet bound traffic from the LAN network should pass through Cyberoam.

Gateway Mode

Configure as Gateway if you want to use Cyberoam as

1. A firewall or replace an existing Firewall
2. A gateway for routing traffic
3. Link load balancer and implement gateway failover functionality

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

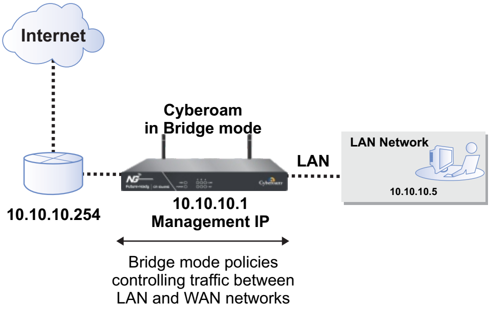


Bridge Mode

Configure as Bridge if

1. You have a private network behind an existing firewall or behind a router and you do not want to replace the firewall.

2. You are already masquerading outgoing traffic.



You will be able to manage and monitor the entire Internet traffic passing through Cyberoam, control web access and apply bandwidth and application restrictions, apply antivirus and antispam policy and IPS policy in either of the modes.

4 GETTING CONFIGURATION INFORMATION

Use the table given below to gather ISP (Internet Service Provider) information

If Internet connection is via	You are probably using	Get information	Cyberoam configuration from Network Configuration wizard
Cable modem, DSL with a Router	DHCP	-----------	Select “Obtain an IP from DHCP”
Home DSL/ADSL	PPPoE	Username Password	Select “Obtain an IP from PPPoE”
T1/E1, Static broadband, Cable or DSL with a static IP	Static	IP address Subnet mask Gateway IP address Primary DNS Secondary DNS How to get the information: From the PC connected to the Internet: open a command prompt window, type the command ipconfig.	Select “Use Static IP”

Use the tables given below to gather the information you need before proceeding to deploy the Appliance.

Gateway Mode

For all the required Ports

Port A	IP address	___.___.___.___
	Subnet Mask	___.___.___.___
	Zone Type	LAN/WAN/DMZ
Port B	IP address	___.___.___.___
	Subnet Mask	___.___.___.___
	Zone Type	LAN/WAN/DMZ
Port C	IP address	___.___.___.___
	Subnet Mask	___.___.___.___
	Zone Type	LAN/WAN/DMZ

Bridge Mode

Bridge IP address	IP address	___.___.___.___
	Subnet Mask	___.___.___.___

The LAN IP address and Subnet Mask must be valid for the respective networks.

▶ GENERAL SETTINGS

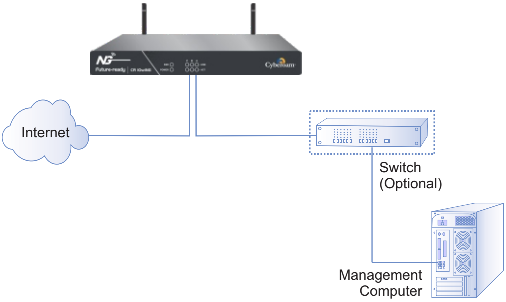
IP address of the Default Gateway A default gateway is required for Cyberoam to route connections to the Internet.	___.___.___.___
DNS IP Address	___.___.___.___
System Time Zone	______________
System Date and Time	______________
Email ID of the administrator where Cyberoam will send System Alerts	______________

5 CONNECTING CYBEROAM

Ethernet connection

1. Connect one end of the straight-through cable into Port A on the Back panel of the Appliance and the other end into the Ethernet Adapter port of Management computer. Change the IP address of the management computer to 172.16.16.2 and the subnet mask to 255.255.255.0.

2. Connect one end of an Ethernet cable into Port B on the Back panel of the Appliance and the other end to your Internet connection e.g. DSL modem or cable modem. It is possible that cable might already be connected between your computer and your modem. If so, disconnect it from your computer and connect into Port B.



3. Connect the AC Power connector into the Back panel of the Appliance and the other end into a standard AC receptacle and turn the power switch ON.

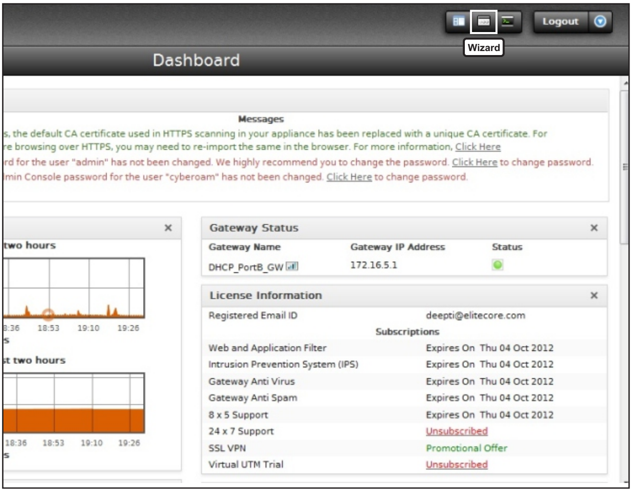
4. Start your management computer. Following Appliance LEDs light up:
   Power LED - Red indicating that Appliance is ON
   SSD - Green indicating that hard disk is Active
   Port A, Port B (Front panel) - Amber indicating an active connection

From the management computer:

1. Browse to https://172.16.16.16
2. Log on to the Cyberoam Web Admin Console using default username ‘admin’ and password ‘admin’.
3. Click Wizard icon to launch the Network Configuration wizard.

Prerequisite

1. Ethernet connection between management computer and Cyberoam.
2. Internet Explorer 7+ or Mozilla Firefox 1.5+ is required to access Cyberoam Web Admin Console.



Messages

s, the default CA certificate used in HTTPS scanning in your appliance has been replaced with a unique CA certificate. For re browsing over HTTPS, you may need to re-import the same in the browser. For more information, Click Here

rd for the user "admin" has not been changed. We highly recommend you to change the password. Click Here to change password.

min Console password for the user "cyberoam" has not been changed. Click Here to change password.

Gateway Status

Gateway Name	Gateway IP Address	Status
DHCP_PortB_GW	172.16.5.1	●

License Information

Registered Email ID	deepti@elitecore.com
Subscriptions	
Web and Application Filter	Expires On Thu 04 Oct 2012
Intrusion Prevention System (IPS)	Expires On Thu 04 Oct 2012
Gateway Anti Virus	Expires On Thu 04 Oct 2012
Gateway Anti Spam	Expires On Thu 04 Oct 2012
8 x 5 Support	Expires On Thu 04 Oct 2012
24 x 7 Support	Unsubscribed
SSL VPN	Promotional Offer
Virtual UTM Trial	Unsubscribed

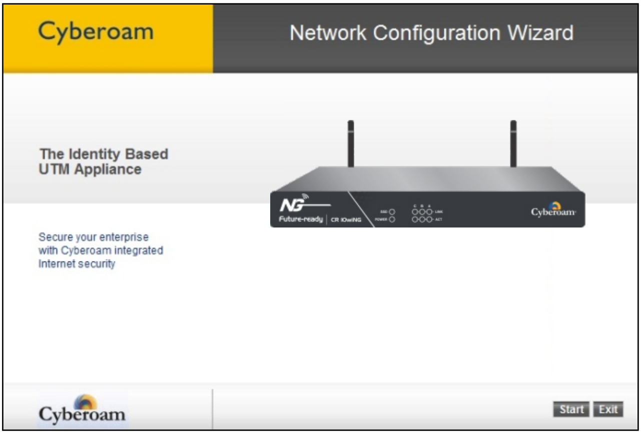
Appliance LED Behavior

LED	State	Description
Power	Red	Cyberoam appliance is ON
	Off	Cyberoam appliance is OFF
SSD	Flashing Green	Activity going on
	Off	No activity
Ports - A,B,C (Front Panel)	Off (Up), Yellow (Down)	Port connected at 10Mbps and Activity going on
	Green (Up), Yellow (Down)	Port connected at 100Mbps and Activity going on
	Amber (Up), Yellow (Down)	Port connected at 1000Mbps and Activity going on
	Off	No link

6 CONFIGURING THE CYBEROAM APPLIANCE

Network Configuration Wizard guides you step-by-step through the configuration of the network parameters like IP address, subnet mask, and default gateway for Cyberoam. Use the configuration settings you have noted in section 4.

Click **'Start'** to start the configuration.



Cyberoam Network Configuration Wizard

The Identity Based UTM Appliance

Secure your enterprise with Cyberoam integrated Internet security

Screen 1 - Network Configuration Wizard

▶ CONFIGURE MODE

Gateway mode

To configure Cyberoam in Gateway mode, select the option Gateway Mode and click ➔ button.

Follow the on-screen steps to:

1. Configure Interface: Configure IP Address, Subnet Mask and Zone for each port, where Zone is a logical grouping of Interfaces.

   By default, Cyberoam binds ports A, B and C to LAN, WAN and DMZ Zones respectively. To enable interface for PPPoE, provide PPPoE details: Username and Password (only for WAN Zone).

   Click **Next** to repeat the steps given above for each port.

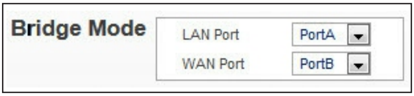
2. Configure DNS server address: Click "Obtain an IP from DHCP" to override appliance DNS and use DNS received from the external DHCP server

   Refer to the screen titled Screen 2 - Gateway Mode: Zone and Network Configuration.

Bridge mode

To configure Cyberoam in Bridge mode, select the option Bridge Mode and click ➔ button.

1. Select the LAN and WAN ports to be bridged. By default, Port A is a member of LAN and Port B is of WAN.

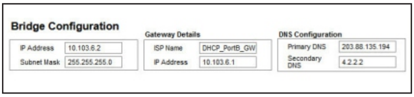


Bridge Mode

LAN Port: PortA

WAN Port: PortB

2. To manage the Cyberoam in your network, configure the IP Address and Subnet Mask. Provide the Gateway and DNS details to connect Cyberoam to the Internet. Refer to General Settings in Section 4.



Bridge Configuration

IP Address: 10.103.6.2

Subnet Mask: 255.255.255.0

Gateway Details

ISP Name: DHCP_PortB_GW

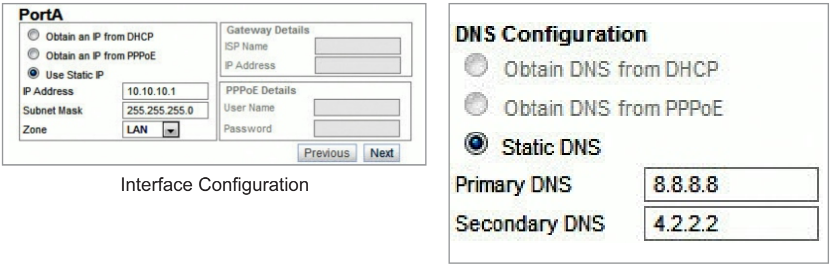
IP Address: 10.103.6.1

DNS Configuration

Primary DNS: 203.88.135.194

Secondary DNS: 4.2.2.2

Proceed to Configure Internet Access section on the next page.



PortA

○ Obtain an IP from DHCP
○ Obtain an IP from PPPoE
● Use Static IP

IP Address	10.10.10.1
Subnet Mask	255.255.255.0
Zone	LAN

Gateway Details

ISP Name	
IP Address	

PPPoE Details

User Name	
Password	

Interface Configuration

DNS Configuration

○ Obtain DNS from DHCP
○ Obtain DNS from PPPoE
● Static DNS

Primary DNS	8.8.8.8
Secondary DNS	4.2.2.2

DNS Configuration

Screen 2 - Gateway Mode: Zone and Network Configuration

▶ CONFIGURE INTERNET ACCESS

By default, Cyberoam applies 'General Internet Policy' as Internet access policy for LAN to WAN traffic. **Do not change the default setting**.

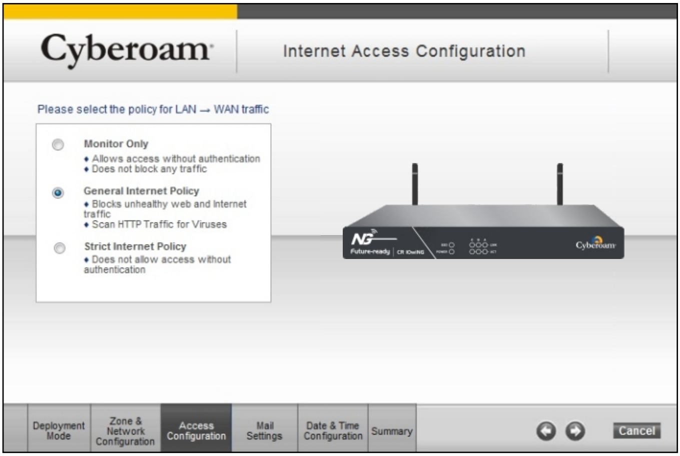
Cyberoam provides 3 types of policies:

'Monitor Only' policy allows all LAN to WAN traffic

'General Internet' policy enables IPS[1] and Virus[2] scanning and allows LAN to WAN traffic except Unhealthy Web and Internet traffic as defined by Cyberoam. This will include sites related to Adult contents, Drugs, Crime and Suicide, Gambling, Militancy and Extremist, Violence, Weapons, Phishing and Fraud and URL Translation sites.

'Strict Internet' policy enables IPS[1] and Virus[2] scanning and allows only authenticated LAN to WAN traffic.

Click ➡ button to configure the mail settings



Cyberoam

Internet Access Configuration

Please select the policy for LAN → WAN traffic

○ Monitor Only
- Allows access without authentication
- Does not block any traffic

● General Internet Policy
- Blocks unhealthy web and Internet traffic
- Scan HTTP Traffic for Viruses

○ Strict Internet Policy
- Does not allow access without authentication

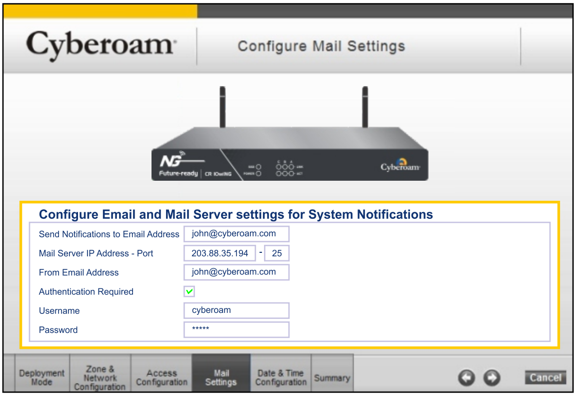
Screen 3 - Access Configuration

[1] Until Intrusion Prevention System module is subscribed, IPS scanning will not be effective.
[2] Until Gateway Anti Virus module is subscribed, virus scanning will not be effective.

▶ CONFIGURE MAIL SETTINGS

1. Specify Administrator Email ID
2. Specify Mail server IP address
3. Specify email address that should be used to send the System Alerts
4. Click “Authentication Required” to enable SMTP authentication, if required and specify username and password.

Click ➔ button for Date and Time zone configuration



Configure Email and Mail Server settings for System Notifications

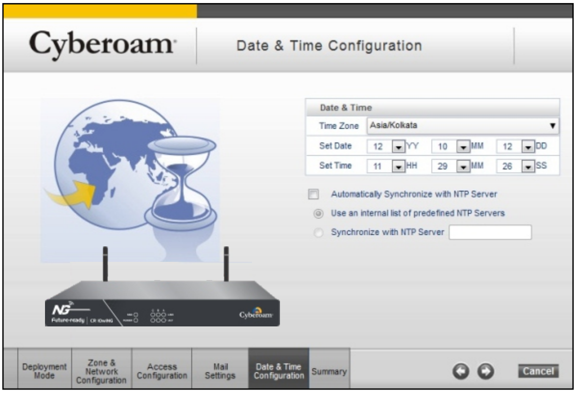
Send Notifications to Email Address	john@cyberoam.com
Mail Server IP Address - Port	203.88.35.194 - 25
From Email Address	john@cyberoam.com
Authentication Required	☑
Username	cyberoam
Password	*****

Screen 4 - Mail Settings

▶ CONFIGURE DATE AND TIME ZONE

Set time zone and current date

Enable clock synchronization with NTP server to tune Cyberoam's clock using global time servers.


Cyberoam
Date & Time Configuration
NG Future-ready | CR 10wiNG
Cyberoam
Deployment Mode
Zone & Network Configuration
Access Configuration
Mail Settings
Date & Time Configuration
Summary
Cancel

Date & Time

Time Zone	Asia/Kolkata		
Set Date	12 YY	10 MM	12 DD
Set Time	11 HH	29 MM	26 SS

□ Automatically Synchronize with NTP Server

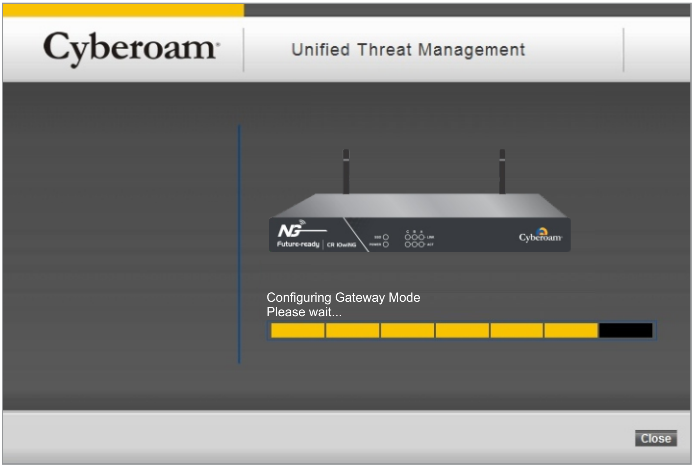
● Use an internal list of predefined NTP Servers

○ Synchronize with NTP Server

Screen 5 - Date and Time Configuration

Click ➔ button to view the configured details. Copy the configured details for future use.

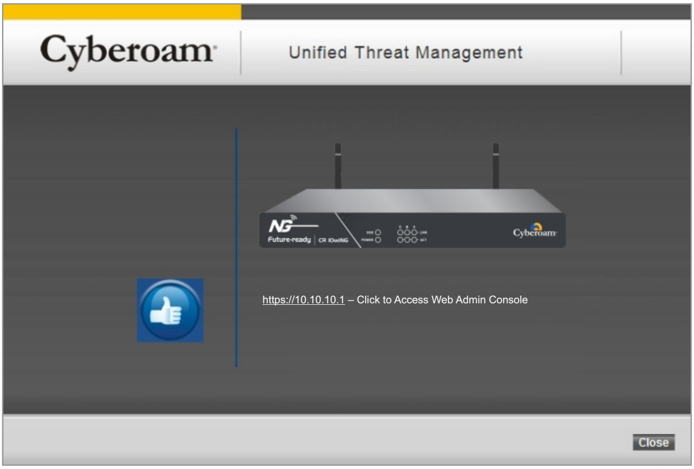
Click **'Finish'**. It will take a few minutes to save the configuration details.



Configuring Gateway Mode
Please wait...

Screen 6 - Network Configuration Wizard

On successful configuration the following page is displayed.



https://10.10.10.1 – Click to Access Web Admin Console

Screen 7 - Network Configuration Wizard

After a few seconds, click the URL to access the Web Admin Console. Click **Close** button to close the Network Configuration Wizard window.

Note:
If you change the LAN IP address (Gateway mode) or Bridge IP address (Bridge mode), you must use this address to reconnect to the Web Admin Console. You might also have to change the IP address of the management computer to be on the same subnet as the new IP address.

Refer to the ‘Guides’ section on http://docs.cyberoam.com for information on how to Control Traffic, and how to configure Anti-Virus Protection, Content Filtering, Spam Filtering, Intrusion Prevention System (IPS), and Virtual Private Networking (VPN).

Congratulations!!!

This finishes the basic configuration of Cyberoam.

Your network is now protected from Internet-based threats and access to Adult contents, Drugs, Crime and Suicide, Gambling, Militancy and Extremist, Violence, Weapons, Phishing and Fraud and URLTranslation sites are blocked.

7 WHAT NEXT?

1. Create Customer Account and register Appliance

   Browse to http://customer.cyberoam.com and click Register and follow the on-screen steps.
   It creates your customer account as well as register your appliance.
   To subscribe for free 15-days trial subscription of Web and Application Filtering, IPS, Anti Virus and Anti Spam, browse to http://customer.cyberoam.com and login with the credentials provided at the time of account creation.

2. Access Cyberoam Web Admin Console
   Browse to https://<IP address of cyberoam> and log on using the default username (admin) and password (admin).

   Note: Internet Explorer 7+ or Mozilla Firefox 1.5+ is required to access the Cyberoam Web Admin Console.

3. Go to menu System → Maintenance → Licensing page and synchronize the registration details. Registration and subscription details are displayed only after synchronization.

4. Configure the correct firewall rule for your Domain Name Server (DNS). You may not be able to access Internet if not configured properly.

5. Go to Firewall → Rule → Rule and edit default firewall rules to enable virus scanning.

6. Set authentication parameters
   Go to Identity → Authentication → Authentication Server to define the authentication parameters.

7. Access Help
   For accessing online help, click the Help button or F1 key on any of the screens to access the corresponding topic's help. Use the Contents and Index options to navigate through the entire online help.

Additional Resources

Visit following links for more information to configure Cyberoam
Technical Documentation - http://docs.cyberoam.com
Cyberoam Knowledge Base - http://kb.cyberoam.com
Cyberoam Security Center - http://csc.cyberoam.com
Cyberoam Upgrades - http://download.cyberoam.com

Important Notes:

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 is subject to acceptance of the terms and conditions of Cyberoam End User License Agreement (EULA) and Warranty Policy for Cyberoam Security Appliances. You will find the copy of the EULA at http://www.cyberoam.com/documents/EULA.html and the Warranty Policy for Cyberoam Security Appliances at http://kb.cyberoam.com

RESTRICTED RIGHTS

Cyberoam®
A SOPHOS Company

Toll Free Numbers
USA : +1-800-686-2360
India : 1-800-301-00013
APAC/MEA : +1-877-777-0368
Europe : +44-808-120-3958

Visit: www.cyberoam.com
Contact: sales@cyberoam.com

FCC Statement:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTICE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This device and it's antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.