Cyberoam®

Unified Threat Management

QUICK START GUIDE

CR750ia Appliance

Document Version: PL QSG 750ia/10000302-1.0-21/07/2010

1 DEFAULTS

Default IP addresses

Ethernet Port	IP Address	Zone
A	172.16.16.16/255.255.255.0	LAN
B	192.168.2.1/255.255.240.0	WAN

Default Username & Password

Web Admin Console	
*Username	cyberoam
*Password	cyber

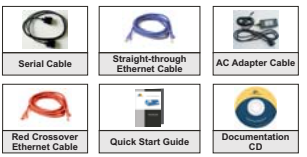
CLI Console (SSH/Serial Connection)	
*Password	admin

* Username and Password are case sensitive

Package Contents

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

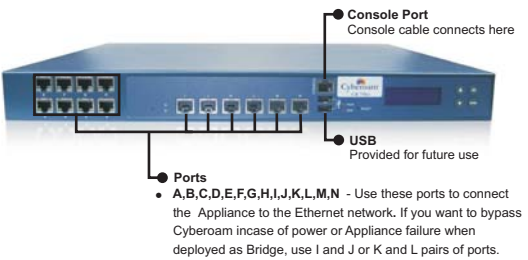
- One Cyberoam Appliance
- One Serial Cable (Null-Modem Cable)
- One Straight-through Ethernet Cable
- One AC Adapter Cable
- One Crossover Ethernet Cable
- One Cyberoam Quick Start Guide
- Documentation CD

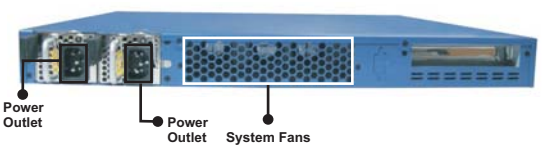


If any items from the package are missing. please contact Cyberoam Support at support@cyberoam.com

2 UNDERSTANDING THE APPLIANCE

► **FRONT 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.

3 PLANNING THE CONFIGURATION

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.

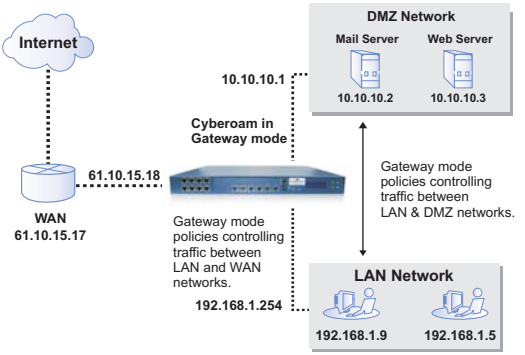
To control the Internet access through Cyberoam the entire Internet bound traffic from the LAN network should pass through Cyberoam.

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.

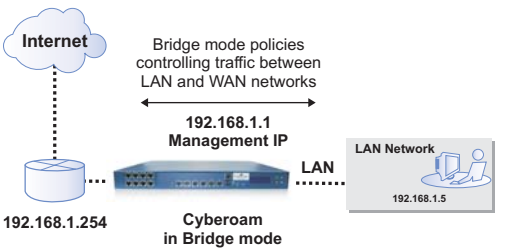


Bridge Mode

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.



*Cyberoam can be bypassed only if deployed as Bridge.

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
Port D	IP address Subnet Mask Zone Type	___.___.___.___ ___.___.___.___ LAN/WAN/DMZ
Port E	IP address Subnet Mask Zone Type	___.___.___.___ ___.___.___.___ LAN/WAN/DMZ
Port F	IP address Subnet Mask Zone Type	___.___.___.___ ___.___.___.___ LAN/WAN/DMZ
Port G	IP address Subnet Mask Zone Type	___.___.___.___ ___.___.___.___ LAN/WAN/DMZ

Port H	IP address Subnet Mask Zone Type	___.___.___.___ ___.___.___.___ LAN/WAN/DMZ
Port I	IP address Subnet Mask Zone Type	___.___.___.___ ___.___.___.___ LAN/WAN/DMZ
Port J	IP address Subnet Mask Zone Type	___.___.___.___ ___.___.___.___ LAN/WAN/DMZ
Port K	IP address Subnet Mask Zone Type	___.___.___.___ ___.___.___.___ LAN/WAN/DMZ
Port L	IP address Subnet Mask Zone Type	___.___.___.___ ___.___.___.___ LAN/WAN/DMZ
Port M	IP address Subnet Mask Zone Type	___.___.___.___ ___.___.___.___ LAN/WAN/DMZ
Port N	IP address Subnet Mask Zone Type	___.___.___.___ ___.___.___.___ LAN/WAN/DMZ

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

Bridge Mode

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

▶ GENERAL SETTINGS

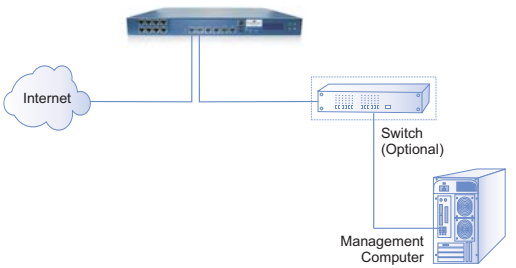
IP address of the Default Gateway A default gateway is required for Cyberoam to route connections to the Internet.	___.___.___.___
DNS IP Address	___.___.___.___
System Time Zone	_____
System Date and Time	_____
Email ID of the administrator where Cyberoam will send System Alerts	_____

5 CONNECTING CYBEROAM

Ethernet connection

1. Connect one end of the crossover cable into Port A on the Back panel of the Appliance and 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 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 & turn on the power.

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

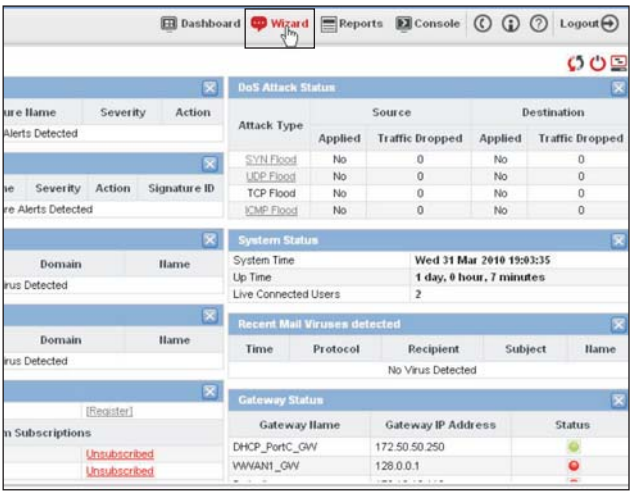
Note: If you change the LAN IP address (Gateway mode) or Bridge IP address (Bridge mode), you must use this address to reconnect to the Web Admin Console. You might also have to change the IP address of the management computer to be on the same subnet as the new IP address.

From the management computer:

1. Browse to https://172.16.16.16
2. Log on to the Cyberoam Web Admin Console using default username 'cyberoam' and password 'cyber'.
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.



Appliance LED Behavior

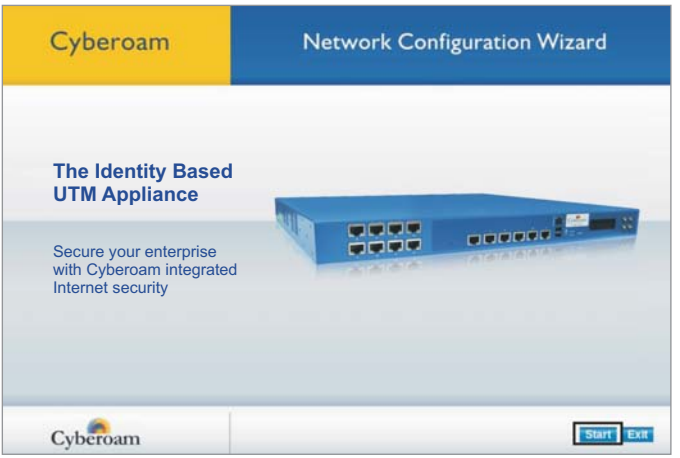
LED	State	Description
Power	Green	Cyberoam appliance in ON
	Off	Cyberoam appliance in OFF
HDD	Flashing Red	Activity going on
	Off	No activity
Ports - A,B,C,D,E,F,G, H,I,J,K,L,M,N (Front panel)	Flashing Amber (Left)	Network Activity at the Port
	Amber (Left)	Correct cable is used and power is on port
	Green (Right)	Port is connected at the 1000Mbps
	Off	No link

Refer to the documentation CD-ROM for information on how to control traffic, and how to configure antivirus protection, content filtering, spam filtering, intrusion prevention system (IPS), and virtual private networking (VPN).

6 CONFIGURING THE CYBEROAM APPLIANCE

Network Configuration Wizard will guide you step-by-step through 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.



► CONFIGURE MODE

Gateway mode

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

Follow the on screen steps to configure:

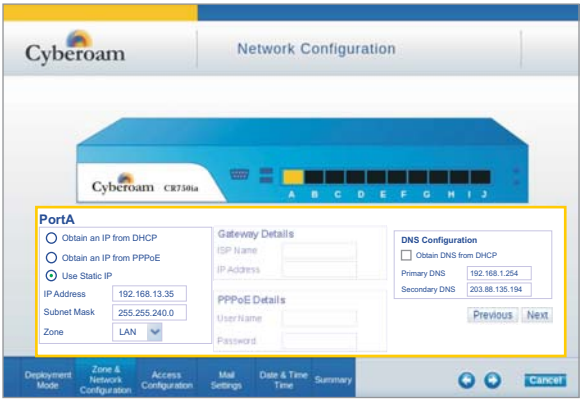
1. Configure DNS server address
   Click "Obtain an IP from DHCP" to override appliance DNS and use DNS received from the external DHCP server
2. Configure Interface
   To enable interface for PPPoE, provide PPPoE details: Username and Password (only for WAN zone)
3. Configure static IP address and subnet mask

Click **'Next'** button to repeat the above procedure for each port

Bridge mode

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

1. Configure Bridge IP address and subnet mask.
2. Provide Gateway and DNS IP address.



▶ CONFIGURE INTERNET ACCESS

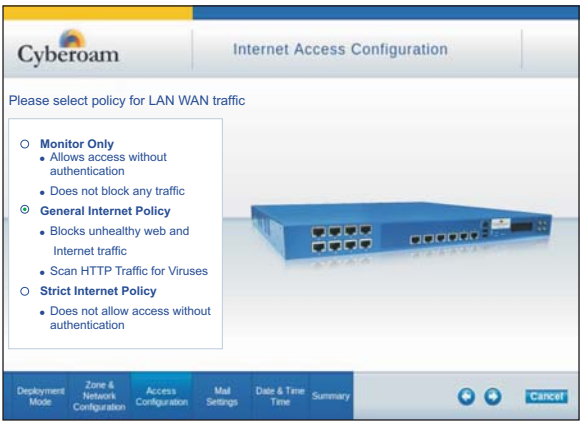
Configure Internet access policy for LAN to WAN traffic.

'Monitor Only' policy allows 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

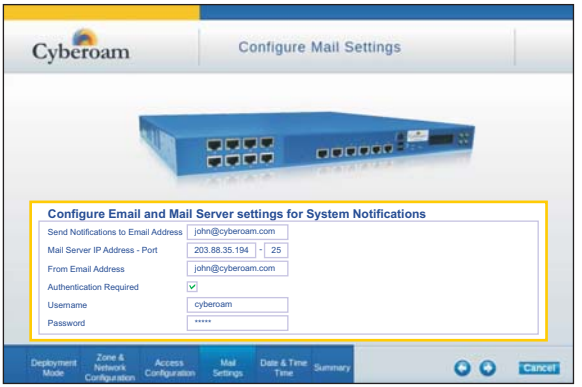


[1]Until Intrusion Prevention System module is subscribed, IPS scanning will not be effective.
[2]Until Gateway Anti Virus module is subscribed, virus scanning will not be effective.

▶ 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.

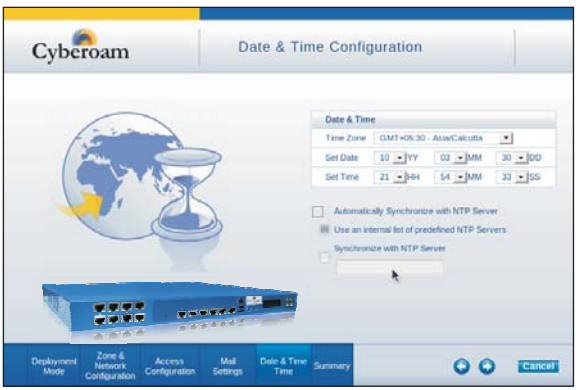
Click button for Date and Time zone configuration



▶ CONFIGURE DATE AND TIME ZONE

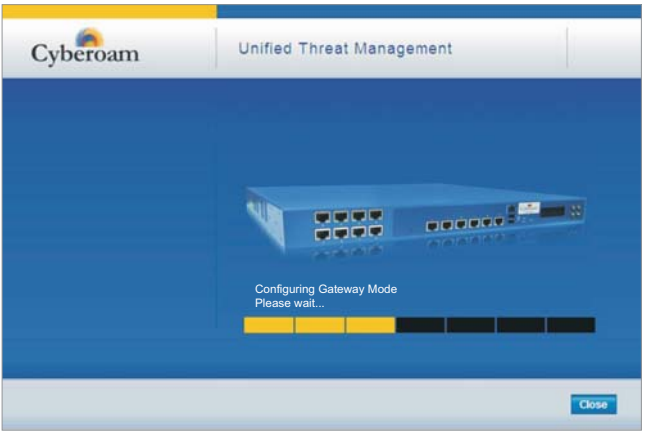
Set time zone and current date

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



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

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



On successful configuration following page will be displayed.

Cyberoam will take time to restart, please wait for some time before clicking the **URL** to access the Web Admin Console. Click **Close** button to close the Network Configuration Wizard window

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 will be 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 will create 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 credential 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 (cyberoam) and password (cyber).

   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 will be 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. For the below given steps, refer to Getting Started Guide (From Documentation CD supplied along with Appliance)
   - Verify Configuration
   - Configure Mail & Web server access.

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

8. 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
Online Video Training- https://connect.elitecore.com username: online.video@cyberoam.com password: onlinevideo

Important Notice

Elitecore 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. Elitecore assumes no responsibility for any errors that may appear in this document. Elitecore reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

User's License

The Appliance described in this document is furnished under the terms of Elitecore's End User license agreement. Please read these terms and conditions carefully before using the Appliance. By using this Appliance, you agree to be bound by the terms and conditions of this license. If you do not agree with the terms of this license, promptly return the unused Appliance and manual (with proof of payment) to the place of purchase for a full refund.

Limited Warranty

Software: Elitecore warrants for a period of ninety (90) days from the date of shipment from Elitecore: (1) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (2) the Software substantially conforms to its published specifications except for the foregoing, the software is provided AS IS. This limited warranty extends only to the customer as the original licenses. Customers exclusive remedy and the entire liability of Elitecore and its suppliers under this warranty will be, at Elitecore or its service center's option, repair, replacement, or refund of the software if reported (or, upon, request, returned) to the party supplying the software to the customer. In no event does Elitecore warrant that the Software is error free, or that the customer will be able to operate the software without problems or interruptions. Elitecore hereby declares that the anti virus and anti spam modules are powered by Kaspersky Labs and Commtouch respectively and the performance thereof is under warranty provided by Kaspersky Labs and Commtouch respectively. It is specified that Kaspersky Lab does not warrant that the Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

Hardware: Elitecore warrants that the Hardware portion of the Elitecore Products excluding power supplies, fans and electrical components will be free from material defects in workmanship and materials for a period of One (1) year. Elitecore's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. The replacement Hardware need not be new or of an identical make, model or part; Elitecore may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned product that Elitecore reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware.

Disclaimer Of Warranty

Except as specified in this warranty, all expressed or implied conditions, representations, and warranties including, without limitation, any implied warranty or merchantability, fitness for a particular purpose, non-infringement or arising from a course of dealing, usage, or trade practice, and hereby excluded to the extent allowed by applicable law.

In no event shall Elitecore or its supplier be liable for any lost revenue, profit, or data, or for special, indirect, consequential, incidental, or punitive damages however caused and regardless of the theory of liability arising out of the use of or inability to use the product even if Elitecore or its suppliers have been advised of the possibility of such damages. In no event shall Elitecore's or its supplier's liability to the customer, whether in contract, tort (including negligence) or otherwise, exceed the price paid by the customer. The foregoing limitations shall apply even if the above stated warranty fails of its essential purpose.

In no event shall Elitecore or its supplier be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Elitecore or its suppliers have been advised of the possibility of such damages.

Restricted Rights

Corporate Headquarters
Elitecore Technologies Ltd.
904, Silicon Tower
Off C.G. Road
Ahmedabad 380015
Gujarat, India.
Phone: +91-79-66065606
Fax: +91-79-26407640
Web site: www.elitecore.com

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:

Email: support@cyberoam.com
Web site: www.cyberoam.com

Visit **www.cyberoam.com** for the regional and latest contact information.

Cyberoam®
Unified Threat Management

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

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