



www.cyberoam-iview.org

Administrator Guide

Document Version 1.0- 10.01.0472-28/01/2011



Eliteco

Table of Contents

Preface	3
Intended Audience.....	3
Guide Organization.....	3
Typographic Conventions.....	4
Part 1: Cyberoam iView Basics	5
Introduction.....	5
Accessing Cyberoam iView.....	5
Understanding Interface – Web Admin Console	7
Dashboard	9
Part 2: Configuration.....	35
Application Group Management.....	35
Custom View Management	45
Report Notification Management.....	50
Data Management.....	54
Bookmark Management	58
Part 3: Archives.....	60
Archive Files	60
IM Archive Logs.....	65
Live Archive Logs	72

Preface

Welcome to Cyberoam iView Administrator's Guide.

Intended Audience

This Guide is intended for the people who want to access reports generated by Cyberoam iView. A basic TCP/IP networking concepts knowledge is required.

Guide Organization

This Guide provides information regarding the administration and customization of Cyberoam iView and helps you manage and customize Cyberoam iView to meet your organization's various requirements.

This Guide is organized into three parts:

Part 1 – Cyberoam iView Basics

It describes how to start using Cyberoam iView.

Part 2 – Configuration

It describes minimum configuration settings required to generate reports using Cyberoam iView, which includes application management, custom view management, configure mail server and email schedule for mailing reports.

Part 3 – Archives

It describes how to access archive log files, IM archive files and real time logs for forensic analysis and trouble shooting purpose.

Part 4 – Reports

It describes how to access and navigate through the drilldown reports. It also provides description of all the reports generated by Cyberoam iView. Refer to Cyberoam iView Reports Guide.

Part 5 – Compliance Reports

It describes various types of compliance reports provided by Cyberoam iView and how to access and navigate through the drilldown reports. It also provides description of all the compliance reports generated by Cyberoam iView.

Part 6 - Trend Reports

It describes various types of trend reports to interpret the pattern of the network activities.

Part 7 - Search Reports

It describes how to retrieve various reports based on multiple search parameters.

Typographic Conventions

Material in this guide is presented in text or screen display notations.

Item	Convention	Example
Cyberoam – iView Server		Machine where Cyberoam iView is installed
Part titles	Bold and shaded font typefaces	Report
Topic titles	Shaded font typefaces	Introduction
Subtitles	Bold & Black typefaces	Notation conventions
Navigation link	Normal typeface	System → Configuration → User it means, to open the required page click on System then on Configuration and finally click User menu
Notes and Prerequisites	Bold typeface between the black borders	Note

Part 1: Cyberoam iView Basics

Introduction

Cyberoam iView is a logging and reporting solution that provides organizations with visibility into their networks for high levels of security, data confidentiality while meeting the requirements of regulatory compliance.

Cyberoam iView offers a single view of the entire network activity. This allows organizations not just to view information across hundreds of users, applications and protocols; it also helps them correlate the information, giving them a comprehensive view of network activity.

With Cyberoam iView, organizations receive logs and reports related to intrusions, attacks, spam and blocked attempts, both internal and external, enabling them to take rapid action throughout their network anywhere in the world.

Accessing Cyberoam iView

Access Web Admin Console, a browser-based Interface to configure and manage Cyberoam iView as well as view reports.

Web Browser should meet the following requirements:

- Microsoft Internet Explorer 6.0+
- Mozilla Firefox 2.0+ (Best view)
- Google Chrome

Log on using default username 'admin' and password admin.



Screen–Cyberoam iView Web Admin Console

Screen Elements	Description
Username	Specify user login name. Default username is 'admin'
Password	Specify password. Default password is 'admin'
Login button	Logs on to Web Admin Console Click to login

Table - Login screen elements

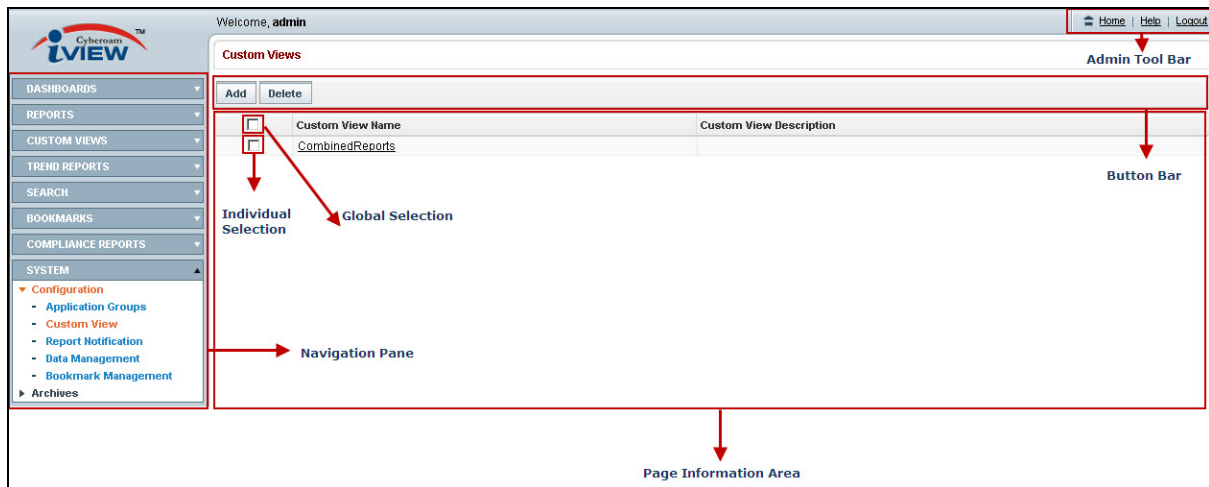
Cyberoam iView displays Main Dashboard as soon as you logon to the Web Admin Console.

Log out procedure

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

Understanding Interface – Web Admin Console

Screen components

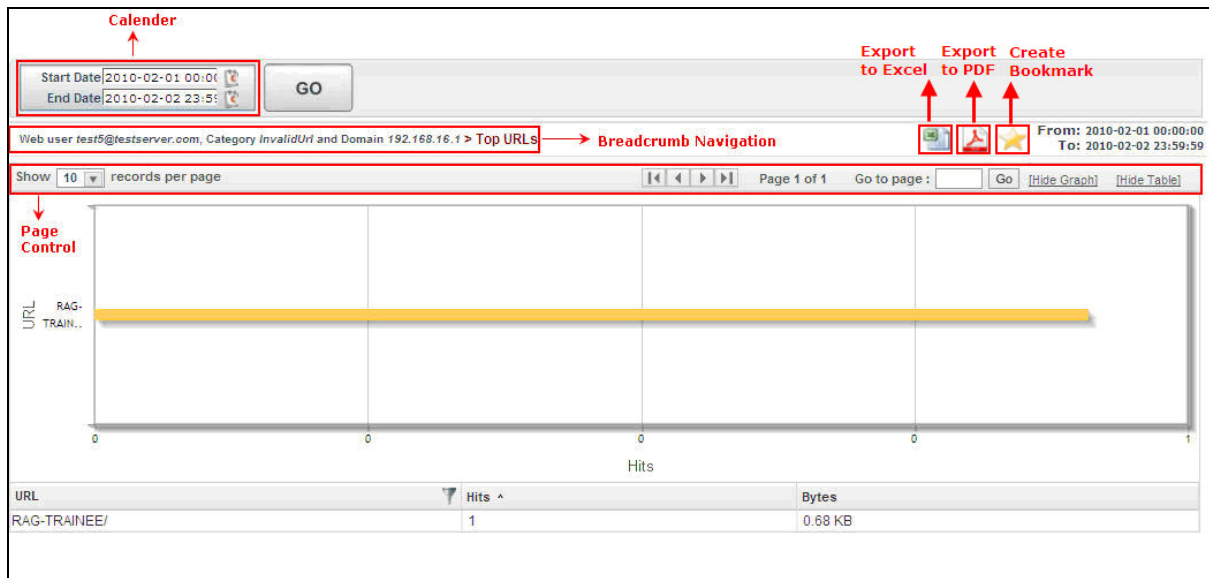


Screen – Basic Screen Components

Screen Elements	Description
Navigation Pane	<p>Navigation Pane on the leftmost side consists of multi-level drop-down Main menu. Main menu has following items:</p> <ul style="list-style-type: none"> • Dashboards • Reports • Custom View (if created) • System <p>Click the menu item to access the next level menu.</p>
Admin Tool Bar	<p>A bar includes collection of links provides access to most common and often used functions like:</p> <ul style="list-style-type: none"> • Home: Click to return to main dashboard • Help: Click to access context sensitive online help • Logout: Click to log out from Cyberoam iView <p>Bar appears on upper rightmost corner of every page.</p>
Button Bar	<p>A bar that includes a collection of buttons provides an easy way to perform tasks like add or delete on clicking them.</p> <p>Bar appears at the top left hand corner of the Information Area of every page.</p>
Global Selection Checkbox	Click to select all items.
Individual Selection Checkbox	Click to select individual item.
Page Information Area	Displays page information corresponding to the selected menu.

Table – Basic Screen Elements

Reports Menu Screen components



Screen – Report Screen Components

Screen Elements	Description
Calendar	Click to select date and time range. Reports will be generated and displayed for the selected time.
Breadcrumb Navigation	Displays the path that the user has taken to arrive at the current page.
Export to Excel	Exports displayed report in MS-Excel format.
Page Controls	Select number of rows to be displayed on each page. Use page controls to navigate to a specific page of the report.

Table – Report Screen Elements

Dashboard

Cyberoam iView displays Main Dashboard as soon as you logon to the Web Admin Console. Dashboard provides a summary view of web and mail traffic including what is happening on the network, such as top attacks or top spammers.

By default, Cyberoam iView provides following dashboards:

- [Main Dashboard](#): Provides network traffic overview of the device.
- Custom Dashboard
- [User Dashboard](#) : Provides Internet behavior overview of the selected user.
- [Source Host Dashboard](#): Provides overview of traffic generated by the selected source host.
- [Email Address Dashboard](#): Provides the Internet activities conducted through the selected email address.



To return to the Main Dashboard from any other page of the Web Admin console, click “Home” link provided in Admin Tool bar.

Main Dashboard

Main Dashboard provides a quick overview of device network activities, which includes web usage, blocked attempts, viruses, attacks, email activities and spam traffic traveled through the device.

It displays graphical and tabular overview of device network activities in Widget form.

Widget displays report in graphical as well as tabular format. By default, the report is displayed for the current date. Report date can be changed through the Calendar available on the topmost row of the page.

Click  button to close the widget and  button to minimize the widget. You need to refresh the page to retrieve the closed report widget.

- [Top Web Users](#)
- [Top Denied Web Users](#)
- [Top Viruses](#)
- [Top Attacks](#)
- [Top Mail Senders](#)
- [Top Spam Senders](#)
- [Mail Traffic Summary](#)
- [User Surfing Pattern](#)

Top Web Users widget

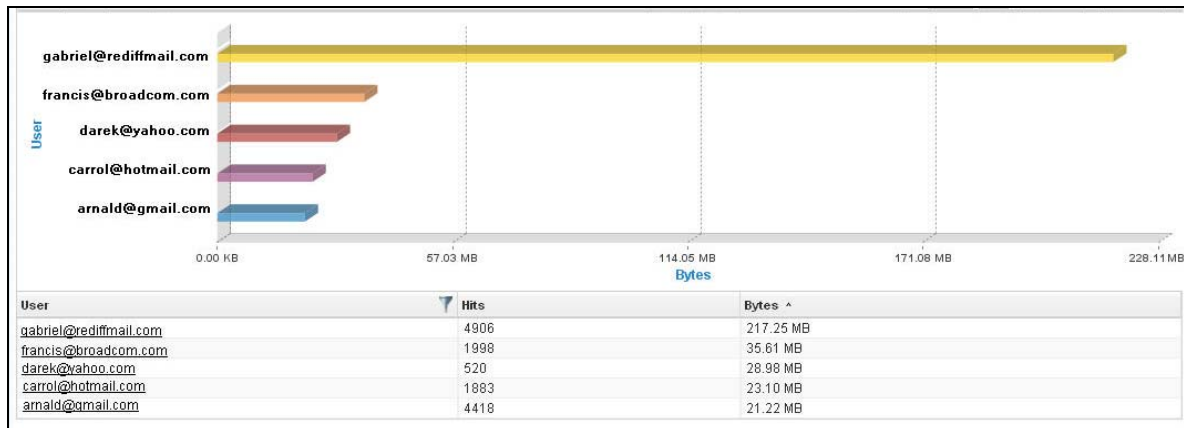
Widget report displays list of top web users along with the number of connections that generate the most traffic for various applications, hosts, destinations, domains and categories.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays number of connections and amount of data transferred per user while tabular report contains following information:

- User: Username of the user as defined in the monitored device. If User is not defined in the monitored device then it will be considered as traffic generated by 'Unknown' user.
- Connections: Number of connections to the user
- Bytes: Amount of data transferred



Screen – Top Web Users

Top Denied Web Users widget

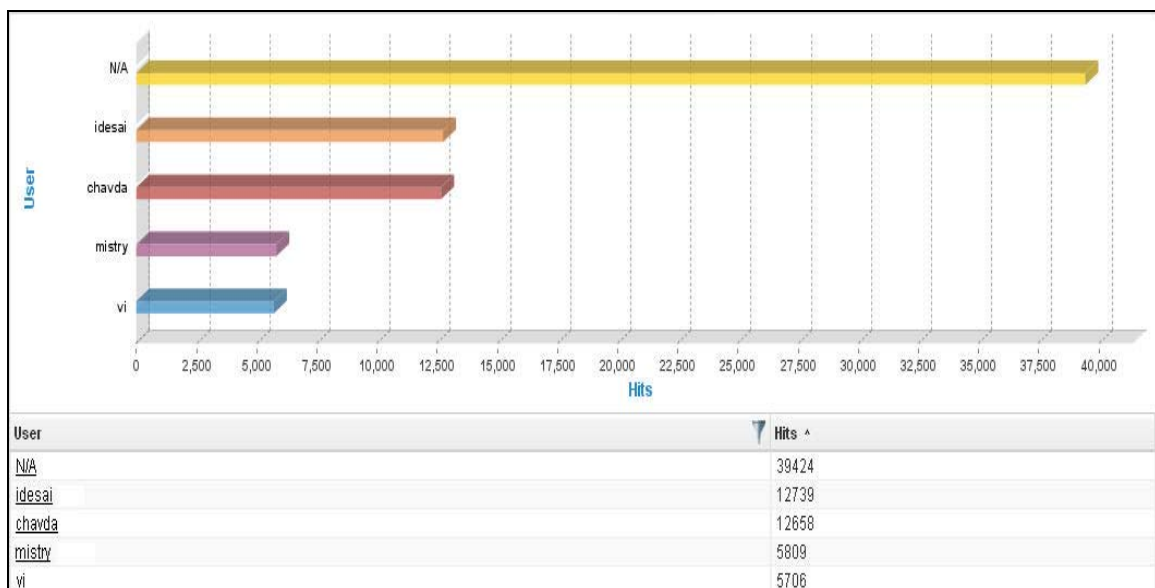
Widget report displays a list of top users who made the most attempts to access the blocked sites.

Report is displayed using a graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays list of users while tabular report contains following information:

- User: Name of the User
- Connections: Number of Connections



Screen –Top Denied Web Users

Top Viruses widget

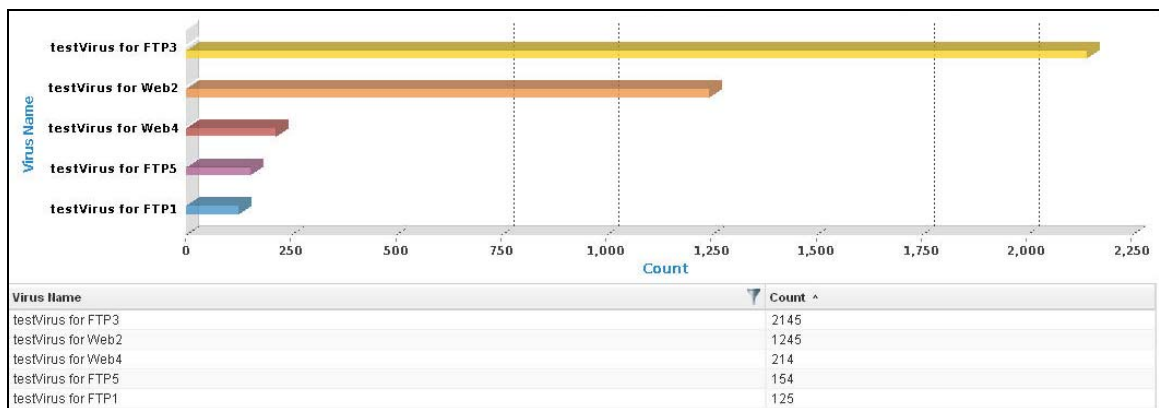
Widget report displays list of top viruses along with the number of connections.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays number of connections per virus while tabular report contains following information:

- Virus Name: Name of the virus identified by monitored device
- Connections: Number of connections to the virus



Screen –Top Viruses

Top Attacks widget

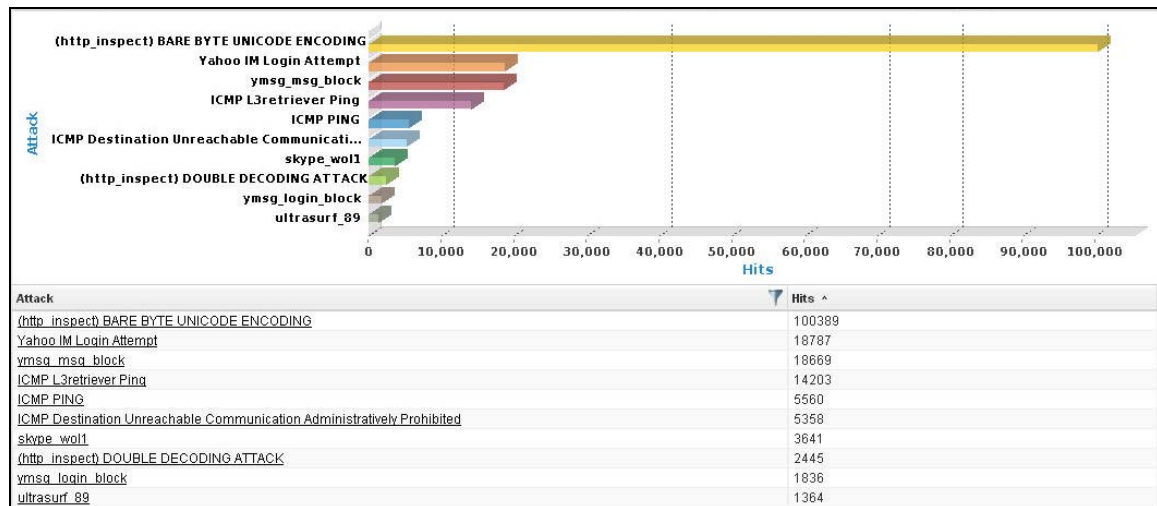
Widget report enables to view the details of the attack that has hit the system and gives the detailed disintegration of attackers, victims and applications through individual reports.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays the number of connections under each attack, while tabular report contains following information

- Attack: Name of the attack launched
- Connections: Number of connections for each attack



Screen –Top Attacks

Top Mail Senders widget

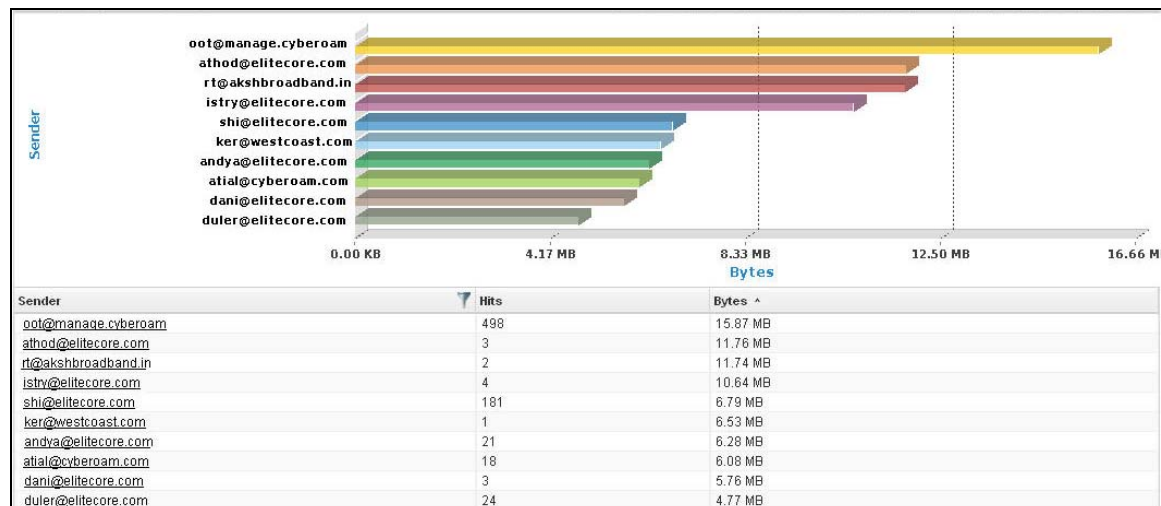
Widget report displays list of top email senders along with the number of connections that generate the most traffic for various users, destinations, hosts and applications.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount of data transferred by each sender while tabular report contains following information:

- Sender: Email ID of the sender
- Connections: Number of connections to the sender
- Bytes: Amount of data transferred



Screen – Top Mail Senders

Top Spam Senders widget

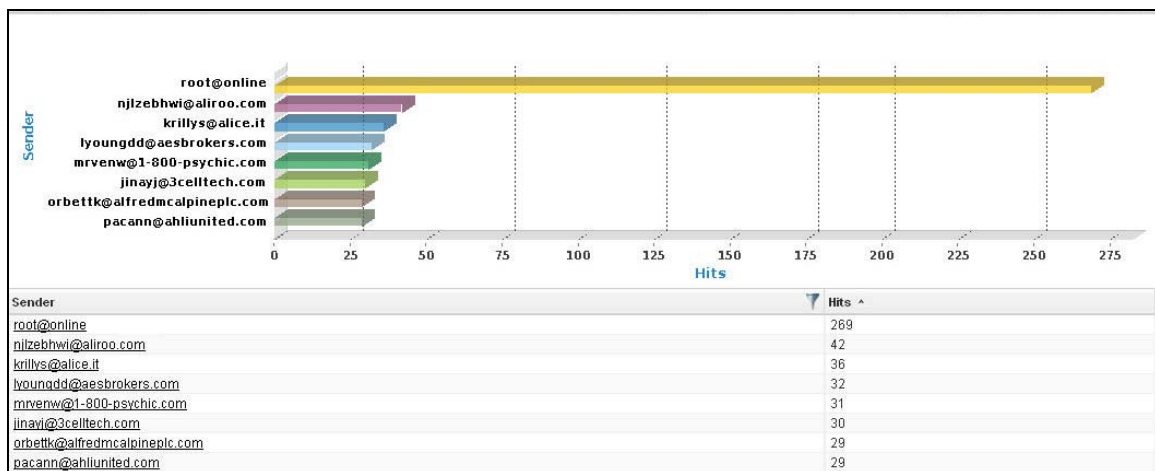
Widget report displays list of top spam senders along with the number of connections that generate the most traffic for various spam recipients, users, destinations, source hosts and applications.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays number of connections per spam sender while tabular report contains following information:

- Sender: Email ID of the sender
- Connections: Number of connections to the sender



Screen –Top Spam Senders

Mail Traffic Summary widget

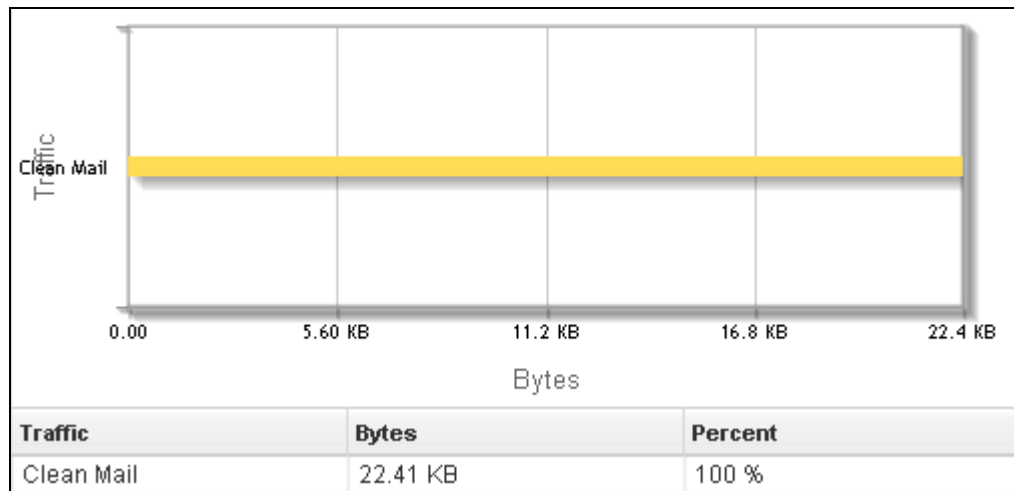
Report displays type of email traffic along with number of bytes and percentage of the traffic.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount of traffic per traffic type while tabular report contains following information:

- Traffic: Type of email traffic. Possible types are :
 - Clean Mail
 - Spam
 - Probable Spam
 - Virus
- Bytes: Number of bytes per email traffic type
- Percent: Type of traffic in percentage



Screen –Mail Traffic Summary

User Surfing Pattern widget

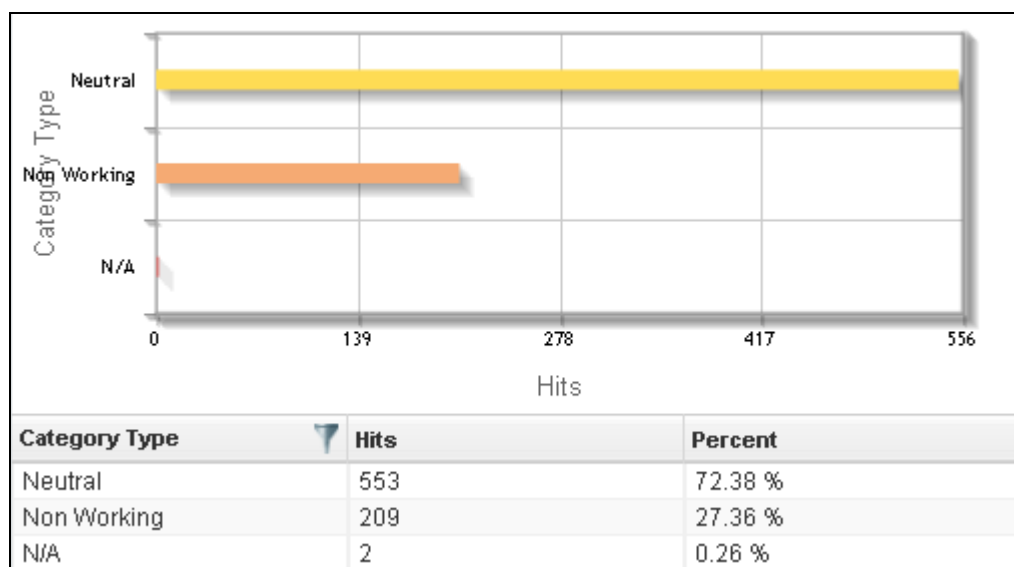
Report displays type of web category along with number of bytes and percentage of the traffic.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount of traffic per category type while tabular report contains following information:

- Category Type: Type of web category as defined in the monitored device
- Connections: Number of connections per category type
- Percent: Type of traffic in percentage



Screen – User Surfing Pattern

Custom Dashboard

- Cyberoam iView provides option to generate custom dashboard based on username, source host and email address.
- [User Dashboard](#) : Provides Internet behavior overview of the selected user.
- [Source Host Dashboard](#): Provides overview of traffic generated by the selected source host.
- [Email Address Dashboard](#): Provides the Internet activities conducted through the selected email address.

User Dashboard

Cyberoam iView user dashboard provides snapshot of user's activities in your network.

To view the User Dashboard:

- Go to Dashboards → Custom Dashboard.
- Select Username in Criteria drop-down and specify the username.
- Click **Go** to view user based dashboard.



Screen – User Criteria

User Dashboard displays following reports in Widget form:

- [Top Web Categories](#)
- [Top Files Uploaded via FTP](#)
- [Top Files Downloaded via FTP](#)
- [Top Denied Categories](#)
- [Top Web Viruses](#)
- [Internet Usage](#)

Top Web Categories widget

Widget report displays number of connections and amount of data transferred per category for the selected user.

View report from Dashboards → Custom Dashboard → Username.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount of data transferred per category while tabular report contains following information:

- Category: Displays name of the category as defined in monitored device. If category is not defined in the monitored device then this field will display 'None' at place of category name.
- Connections: Number of connections to the category
- Bytes: Amount of data transferred



Screen – Top Web Categories

Top Files Uploaded via FTP widget

Widget report displays number of connections and amount of data transferred per file for the selected user.

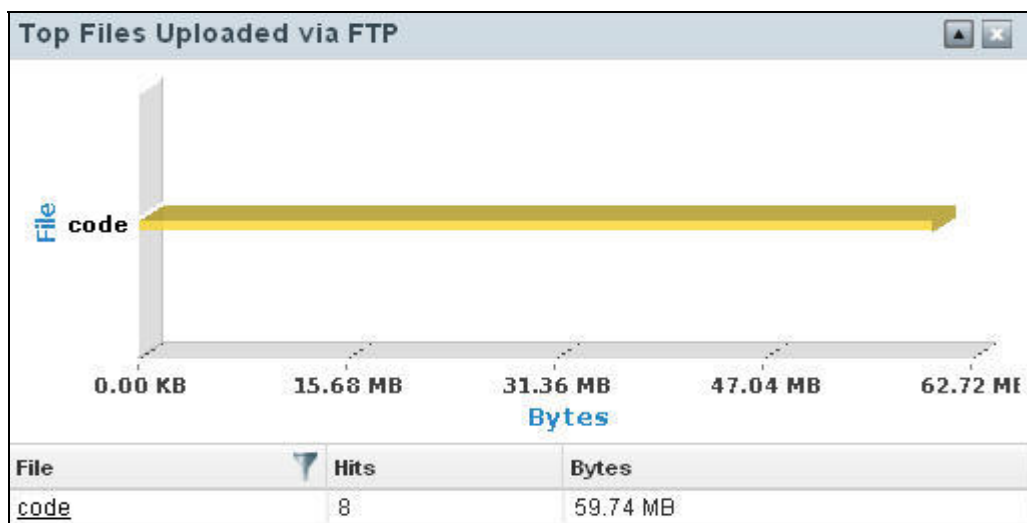
View report from Dashboards → Custom Dashboard → Username.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount of data transferred per file while tabular report contains following information:

- File: Name of the file uploaded
- Connections: Number of connections to the file
- Bytes: Amount of data uploaded



Screen – Top Files Uploaded via FTP

Top Files Downloaded via FTP widget

Widget report displays number of connections and amount of data transferred per file for the selected user.

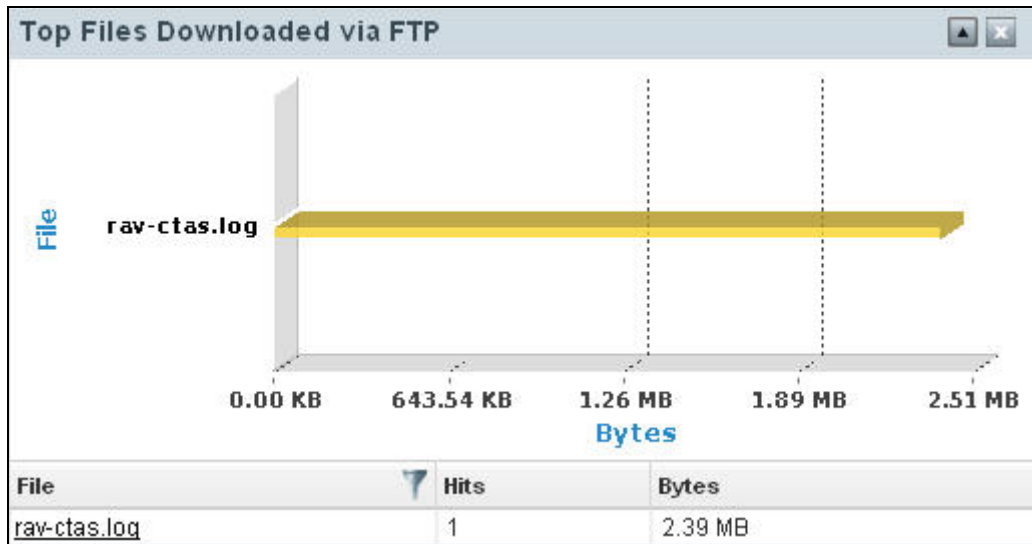
View report from Dashboards → Custom Dashboard → Username.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount of data transferred per file while tabular report contains following information:

- File: Name of the file downloaded
- Connections: Number of connections to the file
- Bytes: Amount of data downloaded



Screen – Top Files Downloaded via FTP

Top Denied Categories widget

Widget report displays number of connections per category for the selected user.

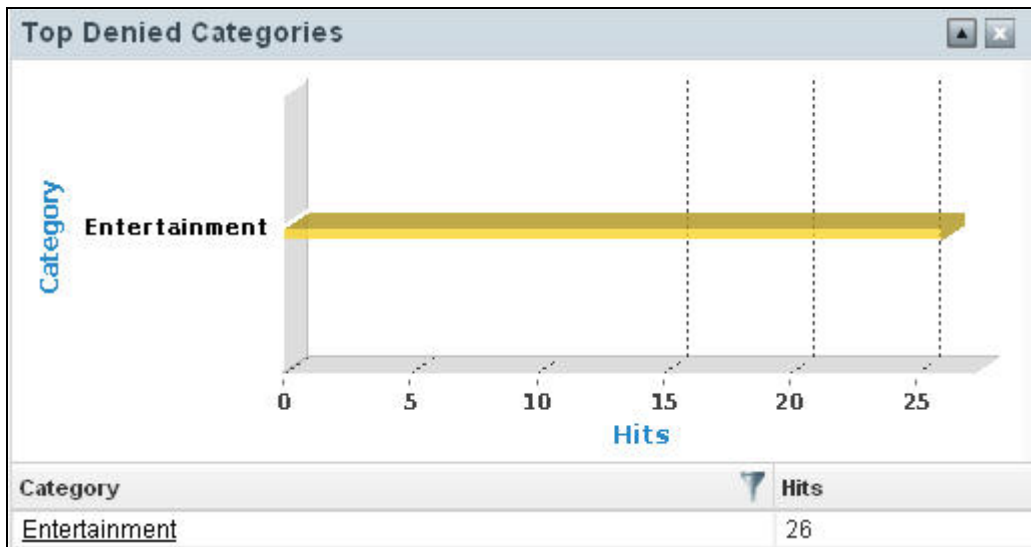
View report from Dashboards → Custom Dashboard → Username.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays number of connections per category while tabular report contains following information:

- Category: Displays name of the category as defined in monitored device.
- Connections: Number of connections to the category



Screen – Top Denied Categories

Top Web Viruses widget

Widget report displays number of connections per virus for the selected user.

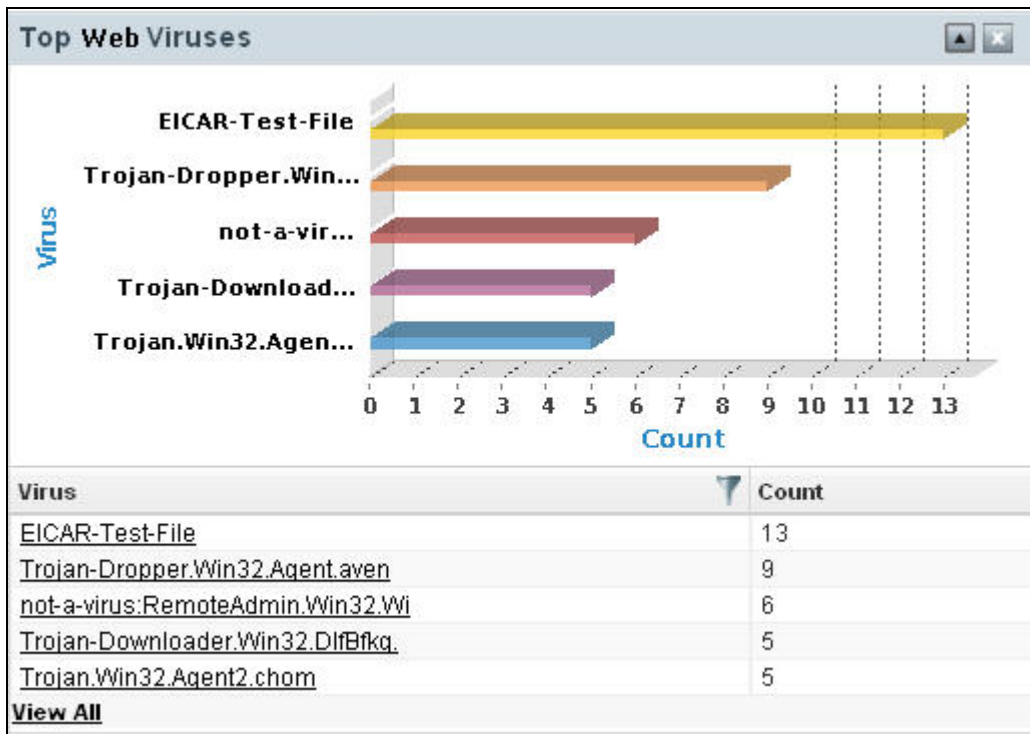
View report from Dashboards → Custom Dashboard → Username.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page

Bar graph displays number of connections per virus while tabular report contains following information:

- Virus: Name of the virus as identified by monitored device
- Connections: Number of connections to the virus



Screen – Top Web Viruses

Internet Usage widget

Widget report displays total amount of data transfer and surfing time for the selected user.

View report from Dashboards → Custom Dashboard → Username

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page

Bar graph displays total amount of data transfer per user while tabular report contains following information:

- User Name: Name of the user as defined in monitored device
- Data Transfer: Total amount of data transfer
- Used Time: Total surfing time

Source Host Dashboard

Cyberoam iView Source Host dashboard provides snapshot of traffic generated by individual host.

To view the Source Host Dashboard:

- Go to Dashboards → Custom Dashboard
- Select Source Host in Criteria drop-down and specify the source host IP address.
- Click **Go** to view source host based dashboard.



Screen – Source Host Criteria

Source Host Dashboard displays following reports in Widget form:

- [Top Web Categories](#)
- [Top Files Uploaded via FTP](#)
- [Top Files Downloaded via FTP](#)
- [Top Denied Categories](#)
- [Top Attacks Received](#)
- [Top Attacks Generated](#)
- Internet Usage

Top Web Categories widget

Widget report displays number of connections and amount of data transferred per category for the selected host.

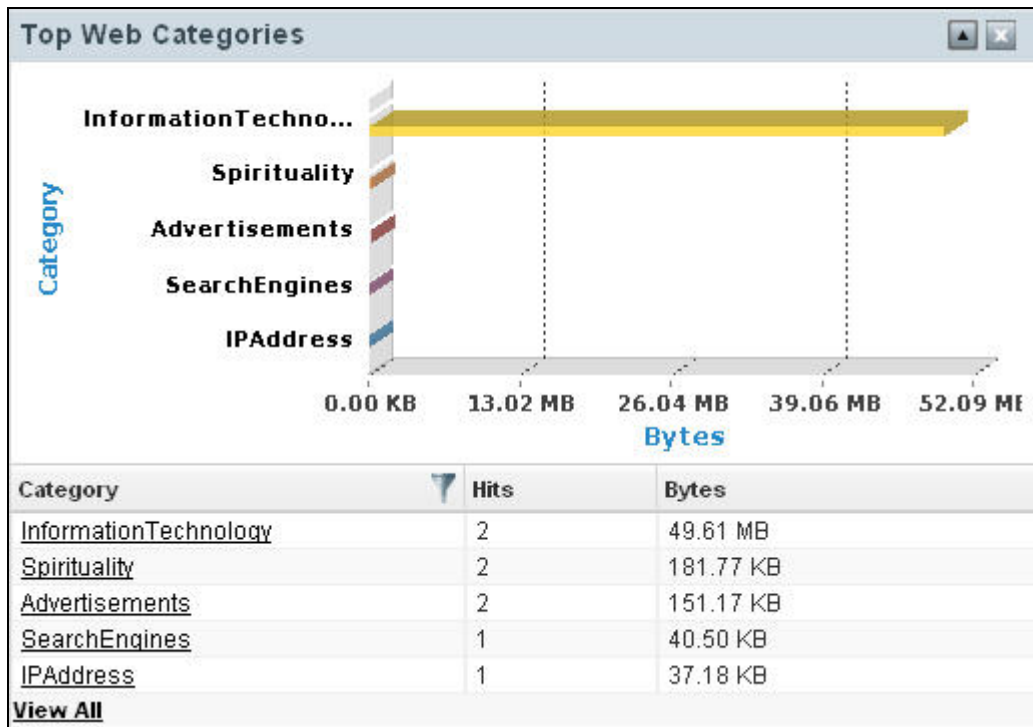
View report from Dashboards → Custom Dashboard → Source Host IP Address.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount of data transferred per category while tabular report contains following information:

- Category: Displays name of the category as defined in monitored device. If category is not defined in the monitored device then this field will display 'None' at place of category name.
- Connections: Number of connections to the category
- Bytes: Amount of data transferred



Screen – Top Web Categories

Top Files Uploaded via FTP widget

Widget report displays number of connections and amount of data transferred per file for the selected host.

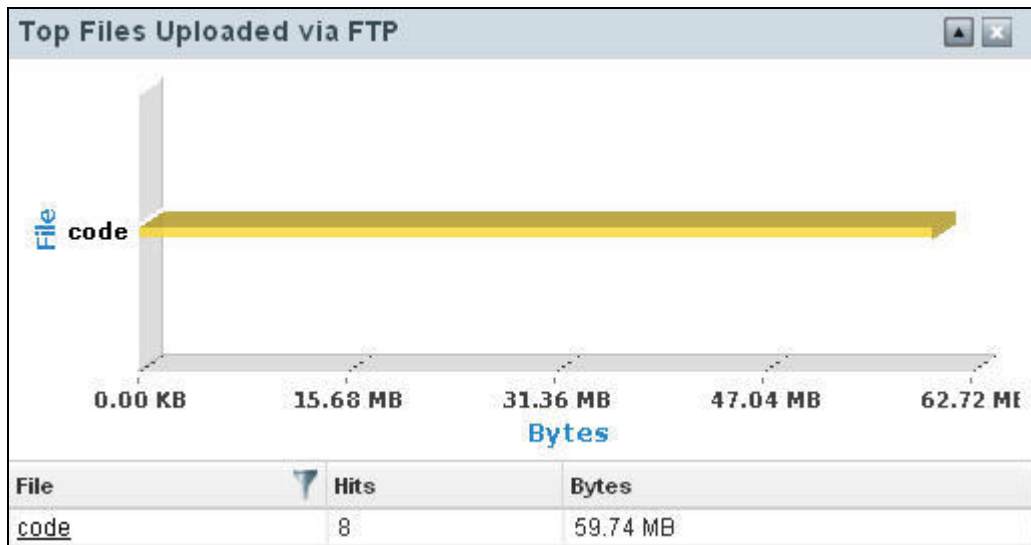
View report from Dashboards → Custom Dashboard → Source Host IP Address.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount of data transferred per file while tabular report contains following information:

- File: Name of the file uploaded
- Connections: Number of connections to the file
- Bytes: Amount of data uploaded



Screen – Top Files Uploaded via FTP

Top Files Downloaded via FTP widget

Widget report displays number of connections and amount of data transferred per file for the selected user.

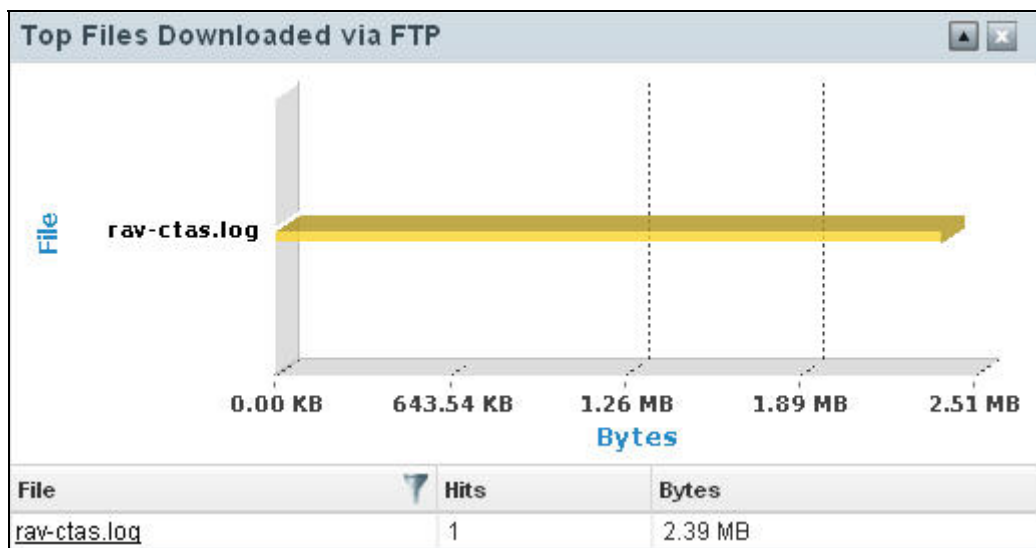
View report from Dashboards → Custom Dashboard → Source Host IP Address

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount of data transferred per file while tabular report contains following information:

- File: Name of the file downloaded
- Connections: Number of connections to the file
- Bytes: Amount of data downloaded



Screen – Top Files Downloaded via FTP

Top Denied Categories widget

Widget report displays number of connections per category for the selected host.

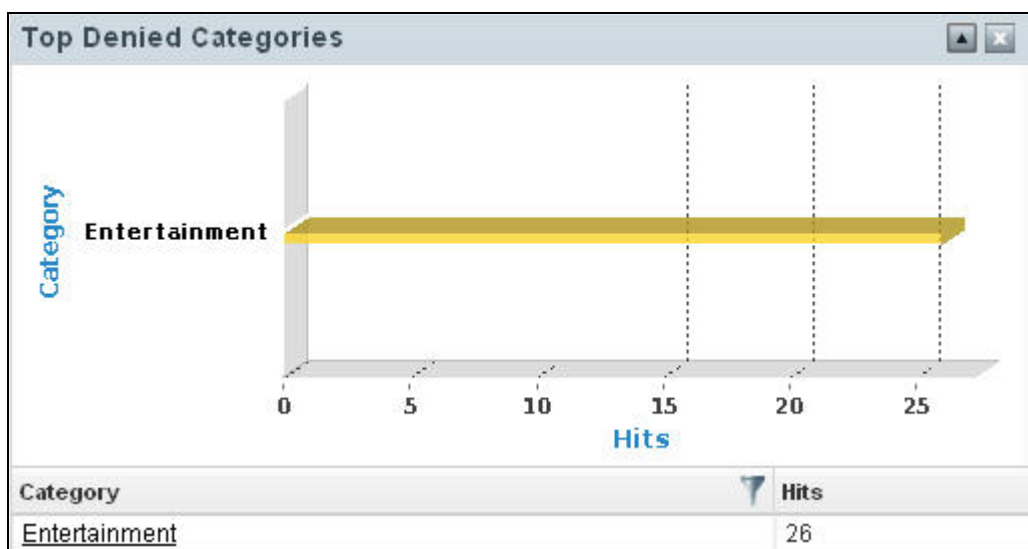
View report from Dashboards → Custom Dashboard → Source Host IP Address.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays number of connections per category while tabular report contains following information:

- Category: Displays name of the category as defined in monitored device.
- Connections: Number of connections to the category



Screen – Top Denied Categories

Top Attacks Received Widget

Widget report displays list of top attacks received along with the number of connections.

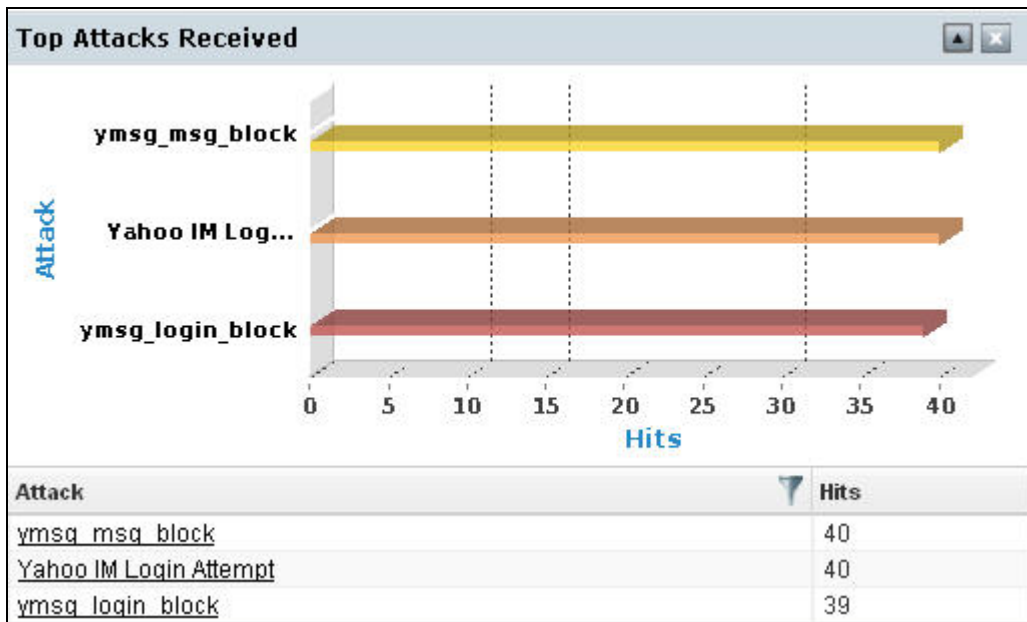
View report from Dashboards → Custom Dashboard → Source Host IP Address.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount of number of connections per attack while tabular report contains following information:

- Attack: Name of the attack as identified by monitored device
- Connections: Number of connections to the attack



Screen – Top Attacks Received

Top Attacks Generated Widget

Report displays list of top attacks generated along with the number of connections.

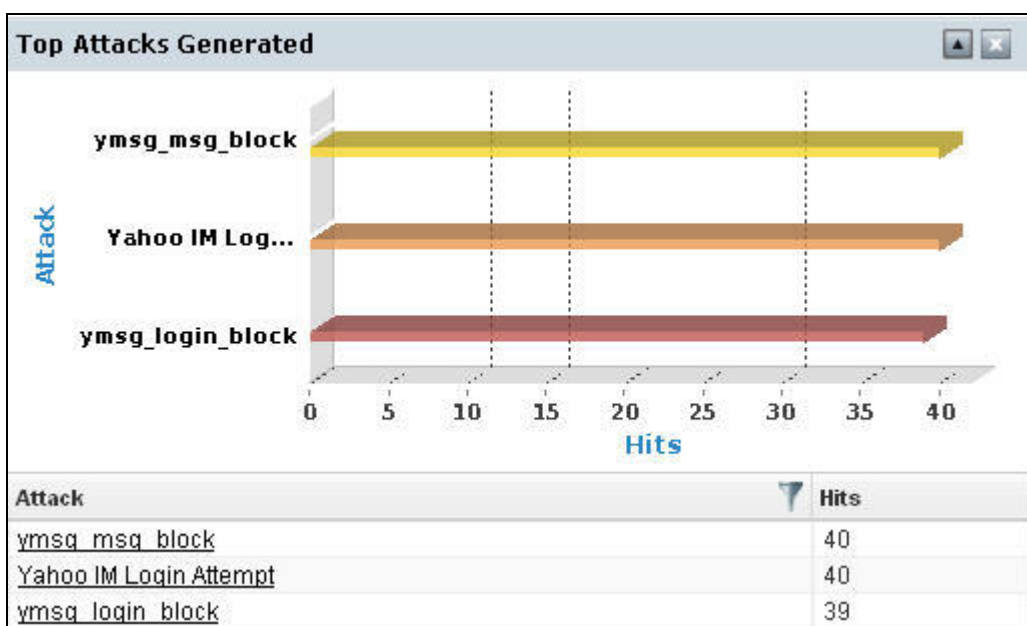
View report from Dashboards → Custom Dashboard → Source Host IP Address.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays number of connections per attack while tabular report contains following information:

- Attack: Name of the attack as identified by monitored device
- Connections: Number of connections to the attack



Screen – Top Attacks Generated

Internet Usage Widget

Widget report displays total amount of data transfer and surfing time for the selected host.

View report from Dashboards → Custom Dashboard → Source Host IP Address

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page

Bar graph displays total amount of data transfer per host while tabular report contains following information:

- Host : IP address of the host
- Data Transfer: Total amount of data transfer
- Used Time: Total surfing time

Email Address Dashboard

Cyberoam iView provides snapshot of email traffic generated by selected email address.

To view the Email Address Dashboard

- Go to Dashboards → Custom Dashboard.
- Select Email Address in Criteria drop-down and specify the email address.
- Click Go to view email address based dashboard.



Screen – Email Address Criteria

Email Address Dashboard displays following reports in Widget form:

- [Top Mails Sent to](#)
- [Top Mails Received From](#)
- [Top Sender Hosts](#)
- [Top Recipients Hosts](#)
- [Top Sender Destinations](#)
- [Top Recipient Destinations](#)
- [Top Sender Users](#)
- [Top Recipient Users](#)
- [Top Spam Received](#)
- [Top Spam Sent](#)

Top Mails Sent to Widget

Widget report displays list of top recipients along with the number of connections and amount of data transferred.

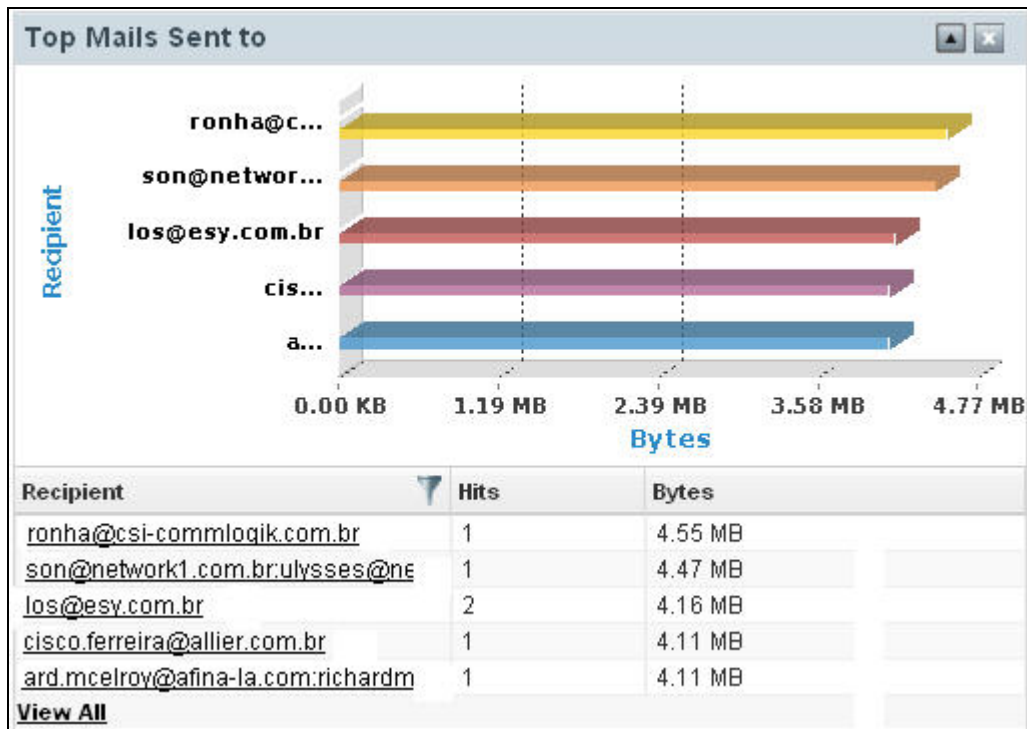
View report from Dashboards → Custom Dashboard → Email Address.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount data transferred per recipient, while tabular report contains following information:

- Recipient: Email address of the recipient
- Connections: Number of connections to the recipient
- Bytes: Amount of data transferred



Screen – Top Mails Sent to

Top Mails Received from Widget

Widget report displays list of top senders along with the number of connections and amount of data transferred.

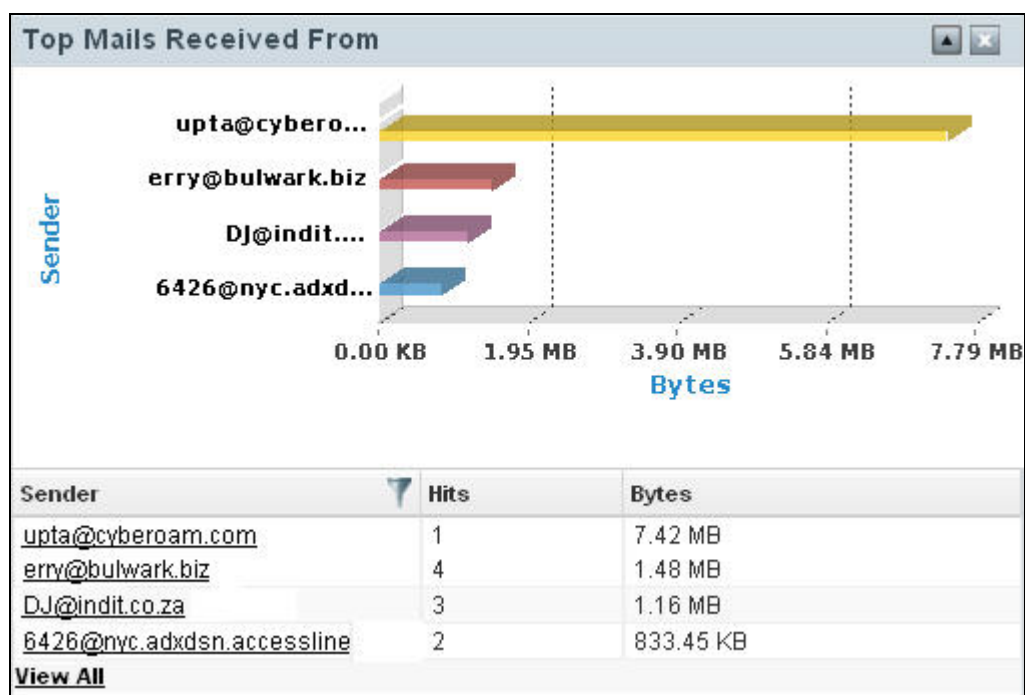
View report from Dashboards → Custom Dashboard → Email Address.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount data transferred per sender, while tabular report contains following information:

- Sender: Email address of the sender
- Connections: Number of connections to the sender
- Bytes: Amount of data transferred



Screen – Top Mails Received from

Top Sender Hosts Widget

Widget report displays list of top sender hosts along with the number of connections and amount of data transferred.

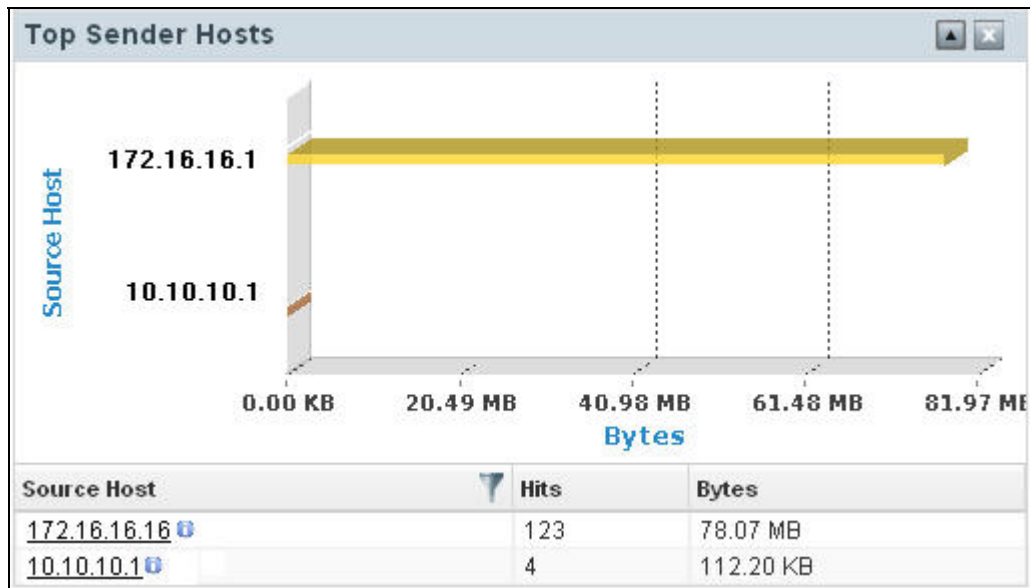
View report from Dashboards → Custom Dashboard → Email Address.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount data transferred per source host, while tabular report contains following information:

- Source Host: IP address of the host
- Connections: Number of connections to the host
- Bytes: Amount of data transferred



Screen – Top Sender Hosts

Top Recipient Hosts Widget

Widget report displays list of top recipient hosts along with the number of connections and amount of data transferred.

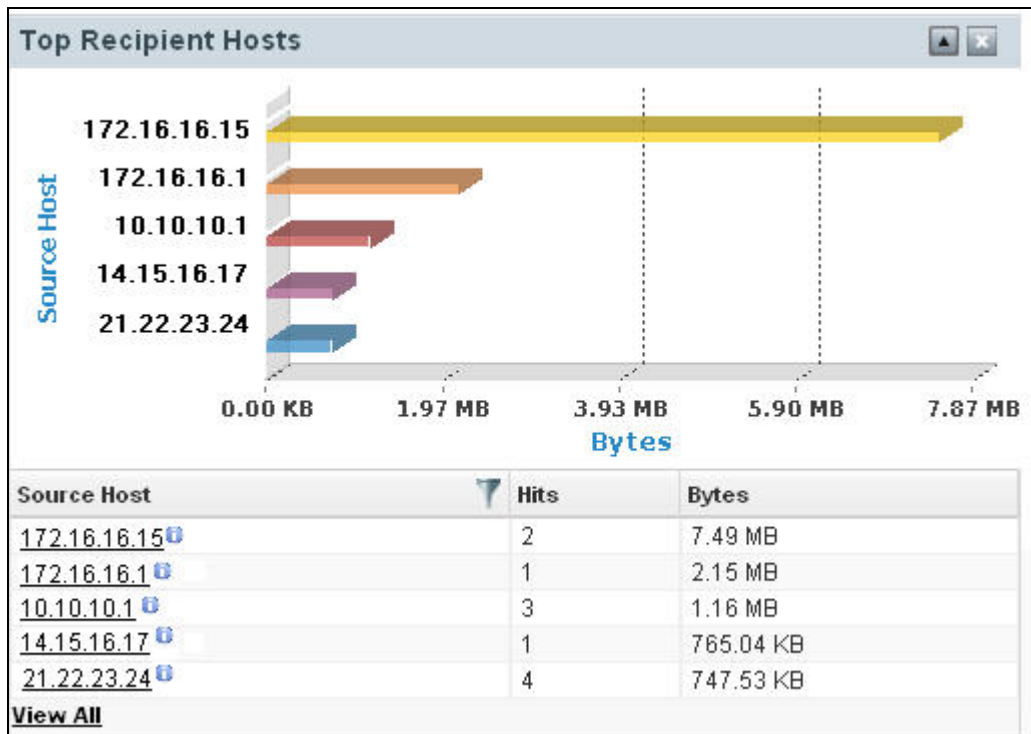
View report from Dashboards → Custom Dashboard → Email Address.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount data transferred per recipient host, while tabular report contains following information:

- Source Host: IP address of the host
- Connections: Number of connections to the host
- Bytes: Amount of data transferred



Screen – Top Recipient Hosts

Top Sender Destinations Widget

Widget report displays list of top sender destinations along with the number of connections and amount of data transferred.

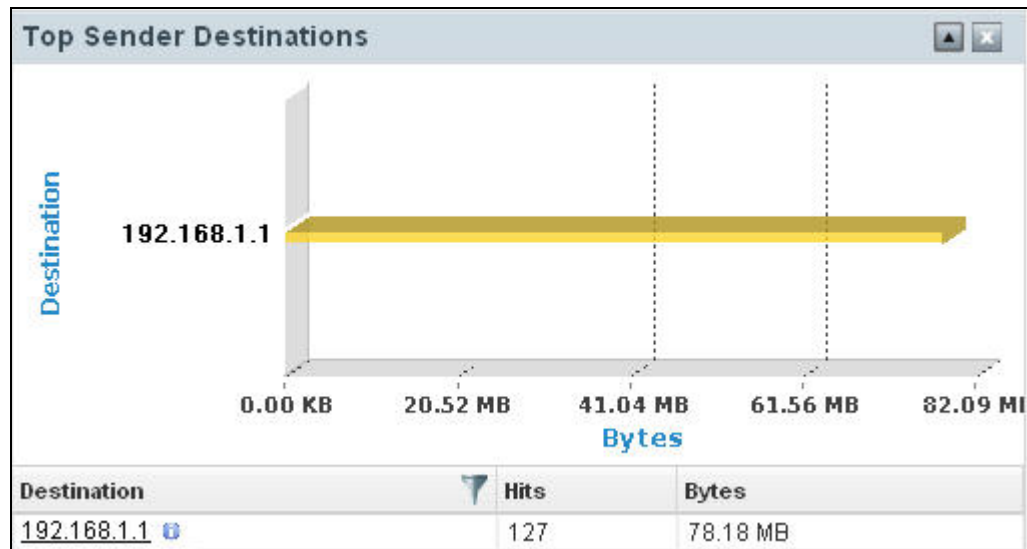
View report from Dashboards → Custom Dashboard → Email Address.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount data transferred per sender destination, while tabular report contains following information:

- Destination: URL name or IP address of the destination
- Connections: Number of connections to the destination
- Bytes: Amount of data transferred



Screen – Top Sender Destinations

Top Recipient Destinations Widget

Widget report displays list of top recipient destinations along with the number of connections and amount of data transferred.

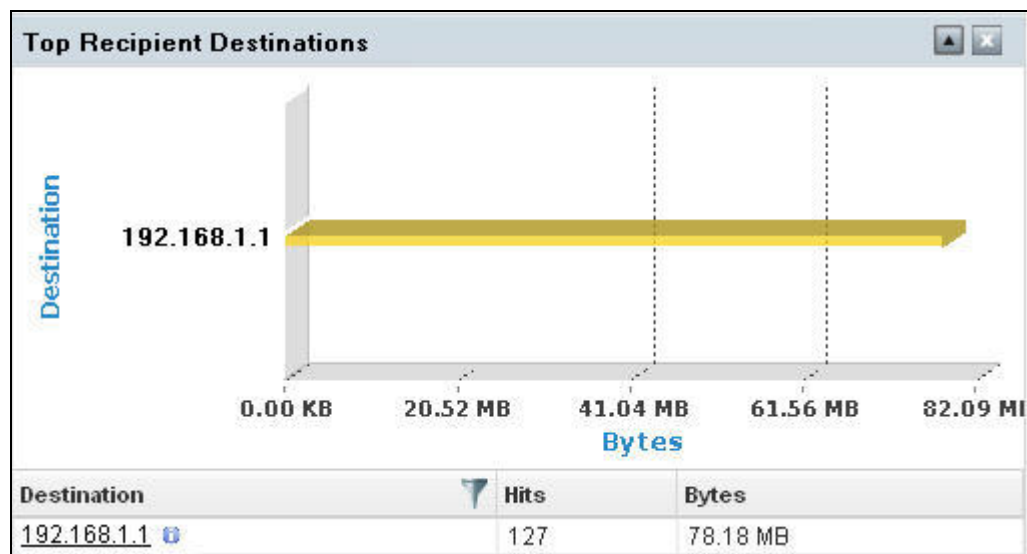
View report from Dashboards → Custom Dashboard → Email Address.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount data transferred per recipient destination, while tabular report contains following information:

- Destination: URL name or IP address of the destination
- Connections: Number of connections to the destination
- Bytes: Amount of data transferred



Screen – Top Recipient Destinations

Top Sender Users Widget

Widget report displays list of top sender users along with the number of connections and amount of data transferred.

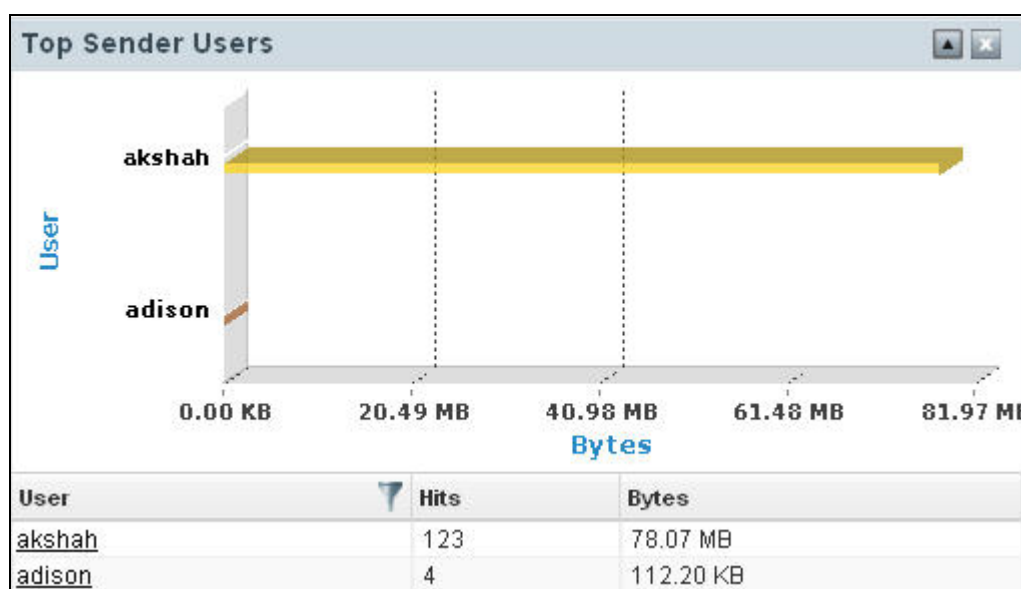
View report from Dashboards → Custom Dashboard → Email Address.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount data transferred per sender user, while tabular report contains following information:

- User: Username of the user as defined in the monitored device. If username is not defined in the monitored device then it will be considered as traffic generated by 'Unknown' user
- Connections: Number of connections to the user
- Bytes: Amount of data transferred



Screen – Top Sender Users

Top Recipient Users Widget

Widget report displays list of recipient users along with the number of connections and amount of data transferred.

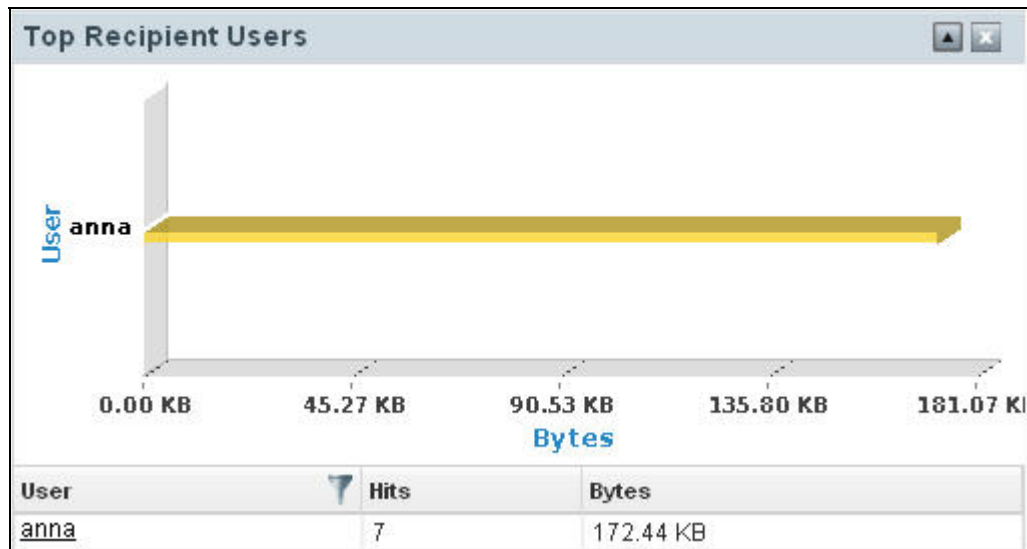
View report from Dashboards → Custom Dashboard → Email Address.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays amount data transferred per recipient user, while tabular report contains following information:

- User: Username of the user as defined in the monitored device. If username is not defined in the monitored device then it will be considered as traffic generated by 'Unknown' user
- Connections: Number of connections to the user
- Bytes: Amount of data transferred



Screen – Top Recipient Users

Top Spam Received Widget

Widget report displays list of top spam senders along with the number of connections.

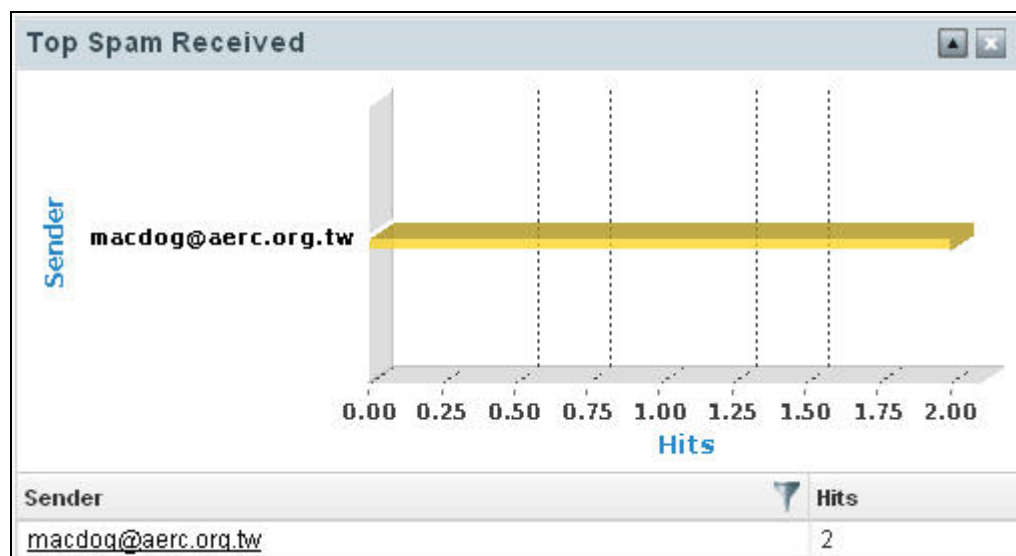
View report from Dashboards → Custom Dashboard → Email Address.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays number of connections per spam sender, while tabular report contains following information:

- Sender: Email address of the spam sender
- Connections: Number of connections to the sender



Screen – Top Spam Received

Top Spam Sent Widget

Widget report displays list of top spam recipient along with the number of connections.

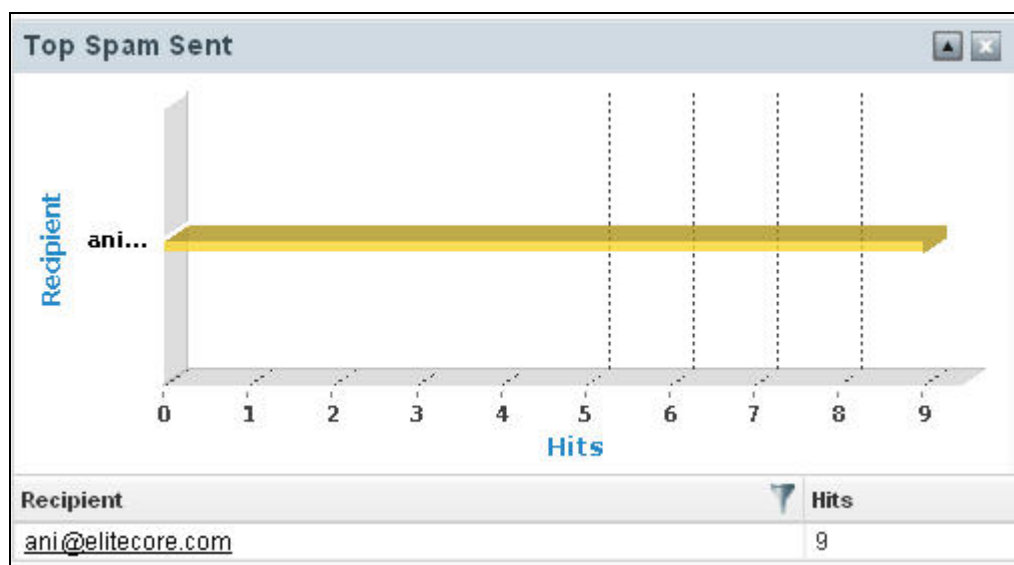
View report from Dashboards → Custom Dashboard→ Email Address.

Report is displayed as graph as well as in tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays number of connections per spam recipient, while tabular report contains following information:

- Recipient: Email address of the spam recipient
- Connections: Number of connections to the recipient



Screen – Top Spam Sent

Part 2: Configuration

Cyberoam iView provides number of configuration options for customization as per your network requirement. You can create and manage applications and application groups, configure mail server to send report notifications, perform search in archives, create custom views and many more.

This chapter covers following sections:

- [Application Group Management](#)
- [Custom View Management](#)
- [Report Notification Management](#)
- [Data Management](#)
- Bookmark Management

Application Group Management

Cyberoam iView generates reports based on application groups. The application group is a logical grouping of applications based on their functions, for example, all FTP related applications are part of FTP application group. Cyberoam iView has grouped the most common applications under 27 pre-defined application groups.

Each Application has an identifier in the form of protocol and port number through which it is identified. E.g., Web-Proxy application is identified through protocol TCP and port number 8080. If application is not defined in Cyberoam iView then instead of application name, protocol and port number will be displayed in reports. Cyberoam iView also allows the administrator to add custom applications and application groups.

This section describes how to:

- [Add Custom Application](#)
- [Update Application](#)
- [Delete Application](#)
- [Add Application Group](#)
- [Update Application Group](#)
- [Update Application Group Membership](#)
- [Delete Application Group](#)
- [Reset to Default Applications](#)

Use System → Configuration → Application Groups page to add and manage applications in Cyberoam iView.

Application Groups			
<div> Add Application Add Application Group Reset to Default </div>			
Application Groups	Description		Delete
▶ Database Application	Database Applications		✗
▶ File Sharing	This group is customize group.		✗
▶ FTP	FTP		✗
▶ ICMP	ICMP		✗
▶ Licensing	This group is customize group.		✗
▶ Mail	E-Mail		✗
▶ Messaging	This group is customize group.		✗
▶ Name Service	Name Service		✗
▶ Network Management	This group is customize group.		✗
▶ Network Security	Network Security		✗
▶ News	News		✗
▶ Point2Point	Point2Point Protocol		✗
▶ Printer	Unix Printer		✗
▶ Routing	This group is customize group.		✗
▶ Secure Shell	Secure Shell		✗
▶ Services	This group is customize group.		✗
▶ SNMP	SNMP		✗
▶ Streaming	Streaming		✗
▶ TCP Requests	TCP Requests		✗
▶ Telnet	Telnet		✗
▶ testgroup	testgroup description1		✗
▶ Time server			✗
▶ TL1	TL1		✗
▶ UDP Requests	UDP Requests		✗
▶ Unassigned	Protocols for which Groups are yet to be assigned		
▶ Voip	This group is customize group.		✗
▶ Web	Web Browsing		✗
▶ Windows Protocols	This group is customize group.		✗

Screen – Application Groups Management

Screen Elements	Description
Add Application Button	Click to add a new application.
Add Application Group Button	Click to add a new application group.
Reset to Default Button	Click to restore all applications, application groups and application identifiers to the default state.
Application Group	Displays name of the application group.
Description	Description of the application group
Delete option	Click to delete application group.

Table – Application Group Screen Elements

Add Custom Application

There are two steps to add a custom application in the Cyberoam iView.

- Add Application

Go to System → Configuration → Application Groups and click **Add Application** to add a new application.

Application Groups			
<div> Add Application Add Application Group Reset to Default </div>			
Application Groups	Description		Delete
▶ Database Application	Database Applications		✗
▶ File Sharing	This group is customize group.		✗
▶ FTP	FTP		✗
▶ ICMP	ICMP		✗
▶ Licensing	This group is customize group.		✗
▶ Mail	E-Mail		✗
▶ Messaging	This group is customize group.		✗
▶ Name Service	Name Service		✗
▶ Network Management	This group is customize group.		✗
▶ Network Security	Network Security		✗
▶ News	News		✗
▶ Point2Point	Point2Point Protocol		✗
▶ Printer	Unix Printer		✗
▶ Routing	This group is customize group.		✗
▶ Secure Shell	Secure Shell		✗
▶ Services	This group is customize group.		✗
▶ SNMP	SNMP		✗
▶ Streaming	Streaming		✗
▶ TCP Requests	TCP Requests		✗
▶ Telnet	Telnet		✗
▶ testgroup	testgroup description1		✗
▶ Time server			✗
▶ TL1	TL1		✗
▶ UDP Requests	UDP Requests		✗
▶ Unassigned	Protocols for which Groups are yet to be assigned		
▶ Voip	This group is customize group.		✗
▶ Web	Web Browsing		✗
▶ Windows Protocols	This group is customize group.		✗

Screen – Application Groups Management

Add Application

Application Name*

Application Group*

Screen – Add Application

Screen Elements	Description
Application Name	Specify name of the application, application name can be any combination of alphanumeric characters and special characters “_”, “@” and “.”.
Application Group	Select application group from the drop down. If the Application Group is not selected, by default, new Application is added to the “Unassigned” group.
Done Button	Click to add new application.
Cancel Button	Click to return to application group management page.

Table – Add Application Screen Elements

- Add Application Identifier

Go to System → Configuration → Application Groups, expand application group tree, and click the newly added application.

Application Groups

Add Application Add Application Group Reset to Default

Application added successfully.

Application Groups	Description	Delete
Database Application	Database Applications	X
Application		
dbase		X
ibm-db2		X
ingres		X
ingres-net		X
ms-sql-m		X
ms-sql-s		X
msql		X
mssql		X
mysql		X
oracle		X
passgo		X
rda		X
sqlnet		X
sql*net		X
sqlserv		X
sqlsrv		X
sybase		X
tacacs-ds		X
File Sharing	This group is customize group.	X
FTP	FTP	X
ICMP	ICMP	X
Licensing	This group is customize group.	X
Mail	E-Mail	X
Messaging	This group is customize group.	X
Name Service	Name Service	X
Network Management	This group is customize group.	X
Network Security	Network Security	X
News	News	X
Point2Point	Point2Point Protocol	X
Printer	Unix Printer	X
Routing	This group is customize group.	X
Secure Shell	Secure Shell	X
Services	This group is customize group.	X
SNMP	SNMP	X
Streaming	Streaming	X
TCP Requests	TCP Requests	X
Telnet	Telnet	X
testgroup	testgroup description1	X
Time server		X
TL1	TL1	X
UDP Requests	UDP Requests	X
Unassigned	Protocols for which Groups are yet to be assigned	X
Voip	This group is customize group.	X
Web	Web Browsing	X
Windows Protocols	This group is customize group.	X

Screen – View Application

Edit dbase Application

Add Application Identifier

Application Group* Database Application

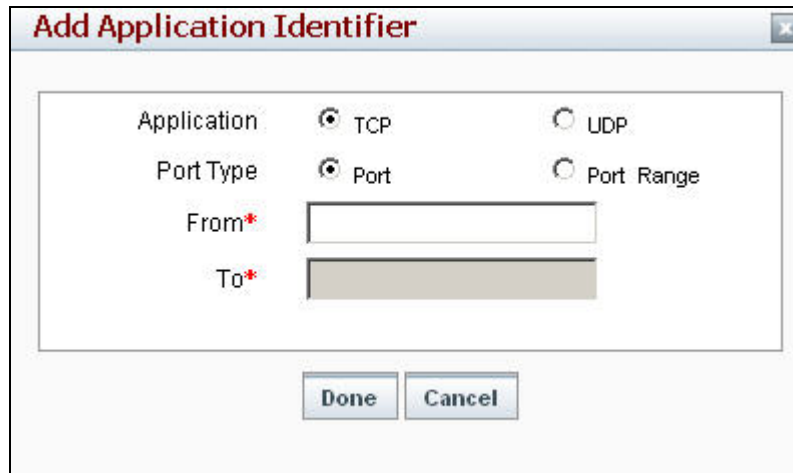
Done Cancel

Screen – Edit Application

Screen Elements	Description
Add Application Identifier	Click to add application identifier to the created custom application.
Application Group	Displays name of the application group.
Done Button	Click to add new application.
Cancel Button	Click to return to application group management page.

Table – Edit Application Screen Elements

Click **Add Application Identifier** to assign an identifier to the application.



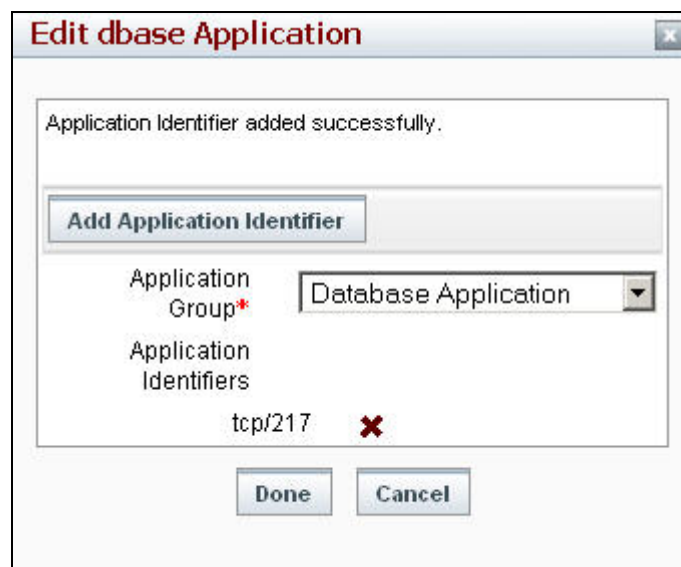
The dialog box titled "Add Application Identifier" contains the following elements:

- Application:** Radio buttons for TCP (selected) and UDP.
- Port Type:** Radio buttons for Port (selected) and Port Range.
- From*:** A text input field.
- To*:** A text input field.
- Buttons:** "Done" and "Cancel" buttons at the bottom.

Screen – Add Application Identifier

Screen Elements	Description
Application	Select application type as TCP or UDP.
Port Type	Select port type as port or port range.
From	If port range is selected as port type then specify From value for port range.
To	If port range is selected as port type then specify To value for port range. To port value must be greater than from port value.
Done Button	Click to add application identifier.
Cancel Button	Click to return to application group management page.

Table – Add Application Identifier Screen Elements



The dialog box titled "Edit dbase Application" displays the following information:

- Message:** "Application Identifier added successfully."
- Buttons:** "Add Application Identifier" button.
- Application Group*:** A dropdown menu showing "Database Application".
- Application Identifiers:** A list containing "tcp/217" with a red "X" icon next to it.
- Buttons:** "Done" and "Cancel" buttons at the bottom.

Screen –Application Identifier added

Screen Elements	Description
Application Identifier	Displays application identifier as combination of application and port number.
✗	Click to delete application identifier.

Table – Application Identifier Screen Elements

Note

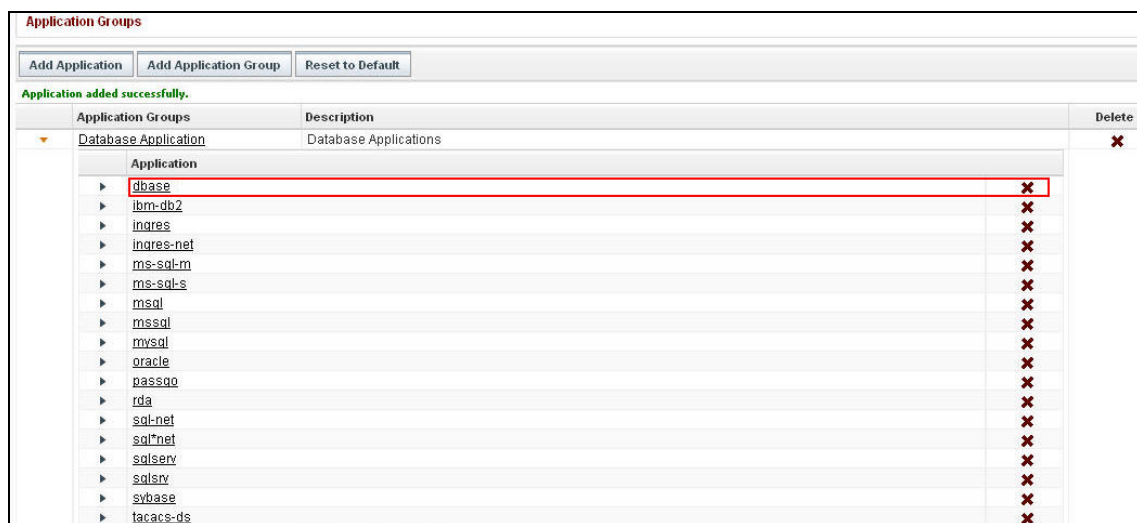
An application cannot be the member of multiple application groups. To change the group membership, first remove an application from the current group and then add in the required application group.

Update Application

- Go to System → Configuration → Application Groups.
- Expand Application Group tree and click application to be modified.
- Refer to [Add Application](#) for information on each parameter.

Delete Application

Go to System → Configuration → Application Groups and expand application tree to view list of applications.



Screen –Delete Application

Screen Elements	Description
Application	Displays application name.
✗	Click to delete application.

Table – Delete Application Screen Elements

Add Application Group

Go to System → Configuration → Application Groups and click **Add Application Group** to add a new application group.

Application Groups			
<div> Add Application Add Application Group Reset to Default </div>			
Application Groups	Description		Delete
▶ Database Application	Database Applications		✗
▶ File Sharing	This group is customize group.		✗
▶ FTP	FTP		✗
▶ ICMP	ICMP		✗
▶ Licensing	This group is customize group.		✗
▶ Mail	E-Mail		✗
▶ Messaging	This group is customize group.		✗
▶ Name Service	Name Service		✗
▶ Network Management	This group is customize group.		✗
▶ Network Security	Network Security		✗
▶ News	News		✗
▶ Point2Point	Point2Point Protocol		✗
▶ Printer	Unix Printer		✗
▶ Routing	This group is customize group.		✗
▶ Secure Shell	Secure Shell		✗
▶ Services	This group is customize group.		✗
▶ SNMP	SNMP		✗
▶ Streaming	Streaming		✗
▶ TCP Requests	TCP Requests		✗
▶ Telnet	Telnet		✗
▶ testgroup	testgroup description1		✗
▶ Time server			✗
▶ TL1	TL1		✗
▶ UDP Requests	UDP Requests		✗
▶ Unassigned	Protocols for which Groups are yet to be assigned		
▶ Voip	This group is customize group.		✗
▶ Web	Web Browsing		✗
▶ Windows Protocols	This group is customize group.		✗

Screen –Application Group Management

Add Application Group

Group Name*

Description

Unassigned Applications

3com-tsmux
9pfs
acap
acas
accessbuilder
accessnetwork
aci
acmaint_dbd
acmaint_transd
acmsoda

Selected Applications*

>
<

Done
Cancel

Screen –Add Application Group

Screen Elements	Description
Group Name	Specify name of application group, application group name can be any combination of alphanumeric characters and special characters “_”, “@” and “.”.
Description	Specify description, if required.
Unassigned Applications List	Displays list of all available unassigned applications.
Selected Applications List	Displays list of selected applications.
Move Button	Click to move applications from 'Unassigned Applications' list to the 'Selected Applications' list. At least one Application is to be added. Selected application(s) will be the member of the newly added Application Group.
Done Button	Click to add application group.
Cancel Button	Click to return to application group management page.

Table – Add Application Group Screen Elements

Update Application Group

Go to System → Configuration → Application Groups and click the application group that has to be updated.

Screen –Update Application Group

Screen Elements	Description
Description	Displays description of application group, modify if required.
Move Button	Click to move application from Selected Applications list to Unassigned Applications list or vice versa.
Done	Click to save the changes in application group.
Cancel	Click to return to application group management page.

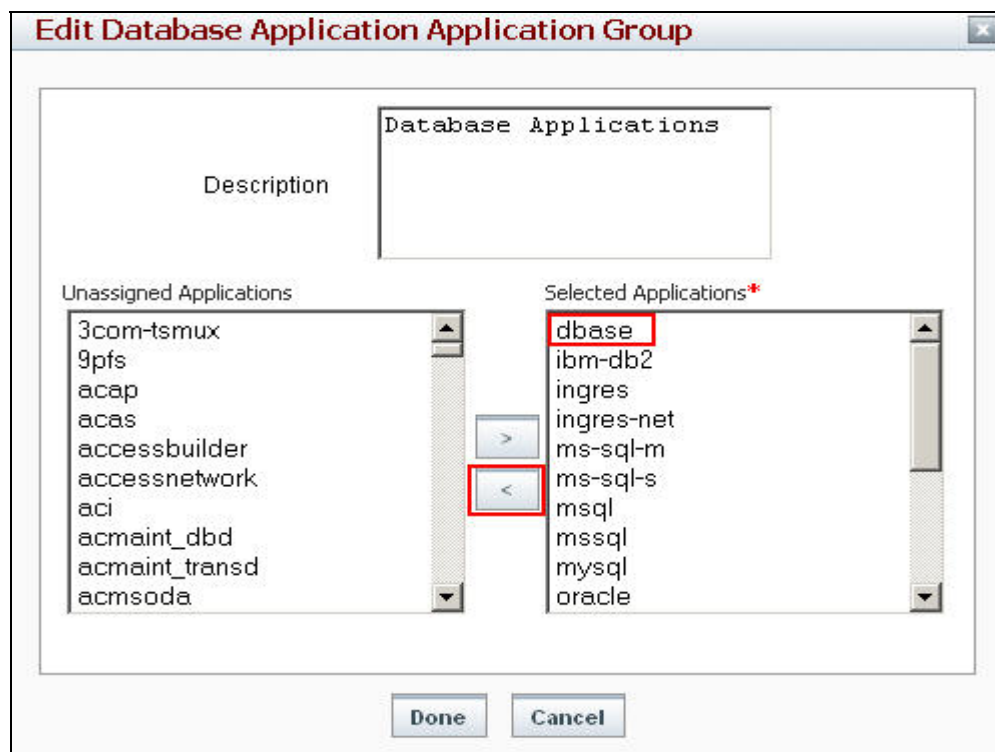
Table –Update Application Group Screen Elements

Note

All fields are editable except application group name.

Update Application Group Membership

Go to System → Configuration → Application Groups and click current application group of the application.



Screen –Update Application Group Membership

Screen Elements	Description
Description	Displays description of application group, modify if required.
Move Button	Click to move application from Selected Applications list to Unassigned Applications list.
Done	Click to save the changes.
Cancel	Click to return to application group management page.

Table –Update Application Group Screen Elements

Refer [Add Application Group](#) and [Update Application Group](#) for details.

Note

You can also change application group membership from [Update Application](#).

Delete Application Group

Go to System → Configuration → Application Groups to view list of application groups.

Application Groups			
<div> Add Application Add Application Group Reset to Default </div>			
Application Groups	Description		Delete
▶ Database Application	Database Applications		
▶ File Sharing	This group is customize group.		
▶ FTP	FTP		
▶ ICMP	ICMP		
▶ Licensing	This group is customize group.		
▶ Mail	E-Mail		
▶ Messaging	This group is customize group.		
▶ Name Service	Name Service		
▶ Network Management	This group is customize group.		
▶ Network Security	Network Security		
▶ News	News		
▶ Point2Point	Point2Point Protocol		
▶ Printer	Unix Printer		
▶ Routing	This group is customize group.		
▶ Secure Shell	Secure Shell		
▶ Services	This group is customize group.		
▶ SNMP	SNMP		
▶ Streaming	Streaming		
▶ TCP Requests	TCP Requests		
▶ Telnet	Telnet		
▶ testgroup	testgroup description1		
▶ Time server			
▶ TL1	TL1		
▶ UDP Requests	UDP Requests		
▶ Unassigned	Protocols for which Groups are yet to be assigned		
▶ Voip	This group is customize group.		
▶ Web	Web Browsing		
▶ Windows Protocols	This group is customize group.		

Screen –Delete Application Group

Screen Elements	Description
Application Group	Displays application group name.
Description	Displays description of application group.
	Click to delete application group.

Table –Delete Application Group Screen Elements

Note

When you delete an application group, applications under that group will also be deleted.

Reset to Default Applications

Go to System → Configuration → Application Groups and click **Reset to Default** to restore all applications, application groups and application identifiers to the default state.

Note

This option will delete custom applications and application group.

Custom View Management

Custom view of reports allows grouping of the most pertinent reports that requires the special attention for managing the network. Reports from different report groups can also be grouped in a single view.

In a View, maximum eight reports can be grouped. Custom view provides a single page view of all the grouped reports.

This section describes how to:

- [Add Custom View](#)
- [Update Custom View](#)
- [Delete Custom View](#)

Use System → Configuration → Custom View to create and manage custom views in iView.

Custom Views		
<div> <div>Add</div> <div>Delete</div> </div>		
<input type="checkbox"/>	Custom View Name	Custom View Description
<input type="checkbox"/>	Combined Reports	Reports from different categories

Screen –Custom View Management

Screen Elements	Description
Add Button	Click to add a new custom view.
Delete Button	Click to delete a custom view.
Custom View Name	Displays custom view name.
Custom View Description	Displays description of custom view.

Table –Custom View Management Screen Elements

Add Custom View

Go to System → Configuration → Custom View and click **Add** to create new Custom View.

Custom Views		
<div> <div>Add</div> <div>Delete</div> </div>		
<input type="checkbox"/>	Custom View Name	Custom View Description
<input type="checkbox"/>	Combined Reports	Reports from different categories

Screen –Custom View Management

Custom View

Add Custom View

Custom View

Custom View Description :

Select Report : You can select 8 reports

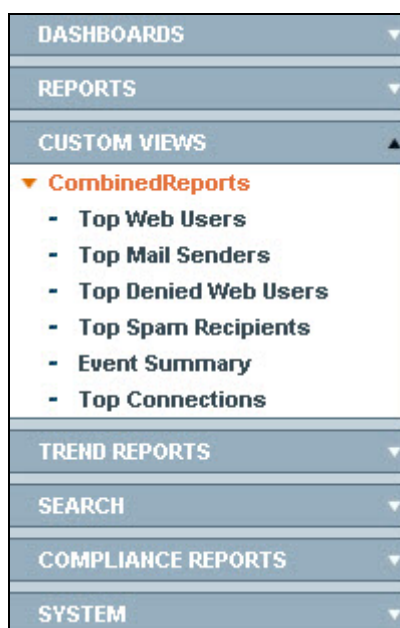
Report Groups	
▼	Web Usage
<input type="checkbox"/>	Top Web Users
<input type="checkbox"/>	Top Web User Groups
<input type="checkbox"/>	Top Categories
<input type="checkbox"/>	Top Category Types
<input type="checkbox"/>	Top Domains
<input type="checkbox"/>	Top Content
<input type="checkbox"/>	Top Web Hosts
<input type="checkbox"/>	Top Applications
<input type="checkbox"/>	Top File Upload
▼	Mail Usage
<input type="checkbox"/>	Top Mail Senders
<input type="checkbox"/>	Top Mail Recipients
<input type="checkbox"/>	Top Mail Users
<input type="checkbox"/>	Top Mail Hosts
<input type="checkbox"/>	Top Mail Applications
▼	FTP Usage
<input type="checkbox"/>	Top Files Uploaded via FTP
<input type="checkbox"/>	Top Files Downloaded via FTP
<input type="checkbox"/>	Top FTP Users (Upload)
<input type="checkbox"/>	Top FTP Users (Download)
<input type="checkbox"/>	Top FTP Hosts (Upload)
<input type="checkbox"/>	Top FTP Hosts (Download)
<input type="checkbox"/>	Top FTP Servers
▼	Blocked Web Attempts
<input type="checkbox"/>	Top Denied Web Users
<input type="checkbox"/>	Top Denied Categories
<input type="checkbox"/>	Top Denied Domains
<input type="checkbox"/>	Top Denied Web Hosts
▼	Attacks
<input type="checkbox"/>	Severity wise break-down
<input type="checkbox"/>	Top Attacks
<input type="checkbox"/>	Top Attackers
<input type="checkbox"/>	Top Victims
<input type="checkbox"/>	Top Applications used by Attacks
▼	Spam
<input type="checkbox"/>	Top Spam Recipients
<input type="checkbox"/>	Top Spam Senders
<input type="checkbox"/>	Top Applications used for Spam
▼	Virus
<input type="checkbox"/>	Top Applications
<input type="checkbox"/>	Top Viruses
<input type="checkbox"/>	Web Viruses
<input type="checkbox"/>	Mail Viruses
<input type="checkbox"/>	FTP Viruses
▼	Event
<input type="checkbox"/>	Event Summary
<input type="checkbox"/>	Admin Events
<input type="checkbox"/>	Authentication Events
<input type="checkbox"/>	System Events
▼	Search Engine
<input type="checkbox"/>	Google Search
<input type="checkbox"/>	Yahoo Search
<input type="checkbox"/>	Bing Search
<input type="checkbox"/>	Wikipedia Search
<input type="checkbox"/>	Rediff Search
<input type="checkbox"/>	eBay Search
▼	IM Usage
<input type="checkbox"/>	Top Protected Contact
<input type="checkbox"/>	Top User
<input type="checkbox"/>	Top Host
▼	Blocked IM Attempts
<input type="checkbox"/>	Top Denied Protected Contact
<input type="checkbox"/>	Top Denied User
▼	Internet Usage
<input type="checkbox"/>	Top Data transfer
<input type="checkbox"/>	Top Surfing Time
<input type="checkbox"/>	Date wise Usage Summary
<input type="checkbox"/>	Exclusive Report by Group
▼	VPN
<input type="checkbox"/>	Top Connections
<input type="checkbox"/>	Top L2TP Users
<input type="checkbox"/>	Top PPTP Users

Add Cancel

Screen –Add Custom View

Screen Elements	Description
Custom View Name	Specify Custom View Name, custom view name can be any combination of alphanumeric characters and special characters “_”, “@” and “.”.
Custom View Description	Specify description of the Custom View, if required.
Select Report	Expand report group and click against the report to be added in custom view. Maximum 8 reports can be added.
Add Button	Click to add a new custom view.
Delete Button	Click to delete a custom view.

Table – Add Custom View Screen Elements



Screen – Custom View display in Navigation Pane

Note

Added custom views will be displayed under Custom Views Sub menu of navigation pane.

Update Custom View

Go to System → Configuration → Custom View and click custom view name to be updated.

Custom View

Edit Custom View

Custom View

CombinedReports

Custom View Description :

Select Report :

You can select 8 reports

	Report Groups
<input type="checkbox"/>	Web Usage * (1)
<input type="checkbox"/>	Mail Usage * (1)
<input type="checkbox"/>	FTP Usage
<input type="checkbox"/>	Blocked Web Attempts * (1)
<input type="checkbox"/>	Attacks
<input type="checkbox"/>	Spam * (1)
<input type="checkbox"/>	Virus
<input type="checkbox"/>	Event * (1)
<input type="checkbox"/>	Search Engine
<input type="checkbox"/>	IM Usage
<input type="checkbox"/>	Blocked IM Attempts
<input type="checkbox"/>	Internet Usage
<input type="checkbox"/>	VPN * (1)

Update

Cancel

Screen – Update Custom View

Screen Elements	Description
Description	Displays description of custom view, modify if required.
Select Report	Expand report group tree to view current reports of custom view. You can add or remove reports by clicking checkbox against them. Number of selected reports from each report group will be displayed against group name. Maximum 8 reports can be added to a single custom view.
Update Button	Click to save changes in custom View.
Cancel Button	Click to return to custom view management page.

Table – Update Custom View Screen Elements

Note

All fields except Custom View Name are editable.

Delete Custom View

Go to System → Configuration → Custom View to view list of custom views.

Custom Views		
<div> <div>Add</div> <div>Delete</div> </div>		
<input type="checkbox"/>	Custom View Name	Custom View Description
<input checked="" type="checkbox"/>	<u>Combined Reports</u>	Reports from different categories

Screen – Delete Custom View

Screen Elements	Description
Global Selection	Click to select all custom views.
Individual Selection	Click to select individual custom view.
Delete Button	Click to delete selected custom View.

Table – Delete Custom View Screen Elements

Report Notification Management

Cyberoam iView can mail reports in PDF format to specified email addresses as per the configured frequency.

This section describes how to:

- [Add Report Notification](#)
- [Update Report Notification](#)
- [Delete Report Notification](#)

Use the System → Configure → Report Notification to create and manage report notifications.

Report Notification						
<input type="button" value="Add"/> <input type="button" value="Delete"/>						
<input type="checkbox"/>	Name	Report Group	Device Name	Email Frequency	To Email Address	Last Sent Time
<input type="checkbox"/>	Firewall Reports	Firewall Rule B...	Ahm_5thfloor_HA...	Daily at 10 hrs.	iView@cyberoam....	Not sent

Screen – Report Notification Management

Screen Elements	Description
Add Button	Click to add a new report notification.
Delete Button	Click to delete a report notification.
Name	Name of the report notification
Report Group	Category of the reports
Device Name	Name of reported device(s)
Email Frequency	Report notification frequency- daily or weekly;
To Email Address	Email ID of recipient(s);
Last Sent Time	Last time when the report notification was sent

Table – Report Notification Management Screen Elements

Add Report Notification

Go to System → Configuration → Report Notification and click **Add** to create a new report notification.

Report Notification						
<div><div>Add</div><div>Delete</div></div>						
<input type="checkbox"/>	Name	Report Group	Device Name	Email Frequency	To Email Address	Last Sent Time
<input type="checkbox"/>	Firewall Reports	Firewall Rule B...	Ahm_5thfloor_HA...	Daily at 10 hrs.	iView@cyberoam...	Not sent

Screen – Report Notification Management

Add Report Notification

Name*

Description

To Email Address*

☒ Report Group
☐ Bookmark

Report Group*

Bookmarks*

☒ Daily
☐ Weekly

Email Frequency*
Send email at Hour(s) on every

☐ Sunday
☐ Monday
☐ Tuesday
☐ Wednesday

☐ Thursday
☐ Friday
☐ Saturday

Screen – Add Report Notification

Screen Elements	Description
Name	Specify Report Name. Report name can be any combination of alphanumeric characters and special characters “_”, “@” and “.”.
Description	Specify description of the report notification, if required.
To Email Address	Specify Email address of the recipient in ‘To Email Address’ field. Use comma to separate multiple E-mail IDs.
Report Group Radio Button	Select to send available reports in report notification.
Bookmark Radio Button	Select to send available bookmarks in report notification.
Report Group	Select report category from the Report Group drop down list. Reports from selected category will be sent to the recipients.
Bookmark	Select bookmark from the Bookmarks drop down list. Selected bookmarks will be sent to the recipients.
Email Frequency	Set E-mail frequency and time. Reports can be mailed daily or weekly,

	<p>as per configured interval.</p> <ul style="list-style-type: none"> In case of daily notification, reports from previous day or same day can be sent on configured time. The administrator can also customize the time interval for generating reports. In case of weekly notification, select day of the week and time of the day to send report notification.
Add Button	Click to add a new report notification.
Cancel Button	Click to return to report notification management page.

Table – Add Report Notification Screen Elements**Update Report Notification**

Go to System → Configuration → Report Notification and select report notification to be updated.

Screen – Update Report Notification

Screen Elements	Description
Description	Displays description of the report notification, modify if required.
To Email Address	Displays Email address of the recipient in 'To Email Address' field, modify if required.
Report Group	Displays report category to send report notification, change if required.
Email Frequency	Displays e-mail frequency and time. Reports can be mailed daily or weekly at the configured interval. In case of weekly notification, select day of the week.
Update Button	Click to save the changes in report notification.
Cancel Button	Click to return to report notification management page.

Table – Update Report Notification Screen Elements

Note

All fields except Report Notification name are editable.

Delete Report Notification

Go to System → Configuration → Report Notification to view list of report notifications.

Report Notification						
<div> <div>Add</div> <div>Delete</div> </div>						
<input type="checkbox"/>	Name	Report Group	Device Name	Email Frequency	To Email Address	Last Sent Time
<input checked="" type="checkbox"/>	Mail Usage	Mail Usage	cyberlite	Daily at 10 hrs.	admin@cyberlite...	Not sent

Screen – Delete Report Notification

Screen Elements	Description
Global Selection	Click to select all report notifications.
Individual Selection	Click to select individual report notification.
Delete Button	Click to delete selected report notifications.

Table – Delete Report Notification Screen Elements

Data Management

Prerequisite

Super Admin privilege required to access and manage Data Management sub menu of System menu.

Retention of data and log archives use enormous amount of disk space. To control and optimize the disk space usage, configure the data retention period of detailed and summarized table. Depending on the compliance requirement, configure the log retention period.

This section describes how to:

- [Configure Retention Period](#)

Use System → Configuration → Data Management page to configure retention period of various data tables.

Data Management	
Log Retention	Period
Retain Web Surfing Logs For Last	6 Months ▼
Retain Mail Logs For Last	6 Months ▼
Retain IM and Blocked IM Logs For Last	6 Months ▼
Retain FTP Logs For Last	6 Months ▼
Retain VPN Logs For Last	1 Day ▼
Retain Internet Usage Logs For Last	1 Month ▼
Retain Blocked Web Attempts Logs For Last	6 Months ▼
Retain IPS (Attacks) Logs For Last	6 Months ▼
Retain Spam Logs For Last	6 Months ▼
Retain Virus Logs For Last	6 Months ▼
Retain Appliance Audit Logs For Last	1 Day ▼
Archived Logs	3 Month ▼

Screen – Data Management

Screen Elements	Description
Log Retention	<p>Displays types of logs to be retained.</p> <ul style="list-style-type: none"> • Web Surfing Logs: Web surfing logs can be retained for time interval starting from 6 months to 3 Years. <p>Cyberoam iView has set default storage of 6 months for web surfing logs but you can configure 1 year, 1.5 years, 2 years, 2.5 years or 3 years.</p>

	<ul style="list-style-type: none"> • Mail Logs: Mail logs can be retained for time interval starting from 6 months to 3 Years. Cyberoam iView has set default storage of 6 months for mail logs, but you can configure 1 year, 1.5 years, 2 years, 2.5 years or 3 years. • IM and Blocked IM Logs: IM and blocked IM logs can be retained for time interval starting from 6 months to 3 Years. Cyberoam-iView has set default storage of 6 months for IM and Blocked IM logs, but you can configure 1 year, 1.5 years, 2 years, 2.5 years or 3 years. • FTP Logs: FTP logs can be retained for time interval starting from 6 months to 3 Years. Cyberoam iView has set default storage of 6 months for FTP logs, but you can configure 1 year, 1.5 years, 2 years, 2.5 years or 3 years. • VPN Logs: VPN logs can be retained for time interval starting from 1 day to 1 month. Cyberoam iView has set default storage of 2 days for VPN logs, but you can configure 1 day, 3 days, 5 days, 7 days or 1 month. • Internet Usage Logs: Internet usage logs can be retained for time interval starting from 1 day to 3 months. Cyberoam-iView has set default storage of 1day for Internet usage logs, but you can configure 1 day, 2 days, 3 days, 5 days, 7 days, 1 month or 3 months • Blocked Web Attempts Logs: Blocked Web Attempts logs can be retained for time interval starting from 6 months to 3 Years. Cyberoam iView has set default storage of 6 months for Blocked Web Attempts logs, but you can configure 1 year, 1.5 years, 2 years, 2.5 years or 3 years • IPS (Attacks) Logs: IPS (Attacks) logs can be retained for time interval starting from 6 months to 3 Years. Cyberoam iView has set default storage of 6 months for IPS (Attacks) logs, but you can configure 1 year, 1.5 years, 2 years, 2.5 years or 3 years • Spam Logs: Spam logs can be retained for time interval starting from 6 months to 3 Years. Cyberoam iView has set default storage of 6 months for spam logs, but you
--	--

	<p>can configure 1 year, 1.5 years, 2 years, 2.5 years or 3 years</p> <ul style="list-style-type: none"> • Virus Logs: Virus logs can be retained for time interval starting from 6 months to 3 Years. Cyberoam iView has set default storage of 6 months for virus logs, but you can configure 1 year, 1.5 years, 2 years, 2.5 years or 3 years • Appliance Audit Logs: Appliance audit logs can be retained for time interval starting from 1 day to 1 month. Cyberoam iView has set default storage of 2 days for appliance audit logs, but you can configure 1 day, 3 days, 5 days, 7 days or 1 month. • Archived logs: Archive logs are collection of historical records, which have accumulated over the course of an organization's lifetime. The Super Administrator can configure retention period for archive logs as <ul style="list-style-type: none"> • Days - 1, 2 or 5 • Weeks - 1 or 2 • Months – 1, 3, 6 • Year - 1, 3 , 7 • Forever • Disable • Please note that Configuring more number of storage days will affect performance because of the time granularity.
Period	Displays retention period of the table
Apply Button	Click to apply changes in database configuration

Table – Database Configuration Screen Elements

Configure Retention Period

Go to System → Configuration → Data Management.

Data Management	
Log Retention	Period
Retain Web Surfing Logs For Last	6 Months
Retain Mail Logs For Last	6 Months
Retain IM and Blocked IM Logs For Last	6 Months
Retain FTP Logs For Last	6 Months
Retain VPN Logs For Last	1 Day
Retain Internet Usage Logs For Last	1 Month
Retain Blocked Web Attempts Logs For Last	6 Months
Retain IPS (Attacks) Logs For Last	6 Months
Retain Spam Logs For Last	6 Months
Retain Virus Logs For Last	6 Months
Retain Appliance Audit Logs For Last	1 Day
Archived Logs	3 Month

Apply

Screen –Configure Retention Period

Screen Elements	Description
Period	Specify retention period value for <ul style="list-style-type: none"> • Web Surfing Logs • Mail Logs • IM and Blocked IM Logs • FTP Logs • VPN logs • Internet Usage Logs • Blocked Web Attempt Logs • IPS(Attack) Logs • Spam Logs • Virus Logs • Appliance Audit Logs • Archived Logs
Apply Button	Click to apply changes. Changes in the retention period will be applied at 12:00 O' clock in the night.

Table – Configure Retention Period Screen Elements

Note

Based on configured retention period, data from the tables will be deleted on day-by-day basis.

Bookmark Management

Bookmark management allows the user to create bookmark of any Cyberoam-iView report at any level of report drill-down. It provides administrator with great level of network visibility based on any criterion. E.g. the administrator can monitor web usage of a particular user by creating bookmark of user based web usage report.

Every bookmark should be a part of a defined bookmark group; if the bookmark group is not created then bookmarks will be members of Default group.

Every bookmark can be sent to specified email address(s) in the form of report notification.

Use **System** → **Configuration** → **Bookmark Management** to create bookmark groups in Cyberoam-iView.

Add Bookmark Group		
	Bookmark Groups	Delete
▶	Default	
▶	cyberoam	✖

Screen – Bookmark Management

Screen Elements	Description
Add Bookmark Group Button	Click to add a new bookmark group.
Bookmark Groups	Name of the bookmark group
Delete Button	Click to delete a bookmark group.

Table – Bookmark Management Screen Elements

This section describes, how to

- [Add Bookmark Group](#)
- [Delete Bookmark Group](#)

Add Bookmark Group

Go to **System** → **Configuration** → **Bookmark Management** and click **Add** to create bookmark group

Add Bookmark Group		
	Bookmark Groups	Delete
▶	Default	
▶	cyberoam	✖

Screen – Bookmark Management

Add Bookmark Group

BookmarkGroup Name :

Screen – Add Bookmark Group

Screen Elements	Description
Bookmark Group Name	Specify Bookmark Group Name, name can be any combination of alphanumeric characters and special characters “_”, “@” and “.”
Add Button	Click to add a new bookmark group
Close Button	Click to return to bookmark management page.

Table – Add Bookmark Group Screen Elements

Note

Created bookmarks will be displayed under Bookmarks Sub menu of navigation pane.

Delete Bookmark Group

Go to **System → Configuration → Bookmark Management** to view list of bookmark groups

Add Bookmark Group		
	Bookmark Groups	Delete
▶	Default	
▶	cyberoam	

Screen – Delete Bookmark Group


Screen Elements	Description
Bookmark Group	Displays bookmark group name
	Click to delete bookmark group

Table – Delete Bookmark Group Screen Elements

Note

Removing a bookmark group will remove the bookmark from Cyberoam iView

Part 3: Archives

Cyberoam-iView provides historical archived logs as well live archived logs to provide historical as well real time view of network activities:

- [Archive File](#)
- [IM Archive Logs](#)
- [Live Archive Logs](#)

Archive Files

Archive logs are collection of historical records, which are the initial line of forensic investigation. Cyberoam-iView retains archive log data for the configured period. Data Retention period can be configured from the System → Configuration → Data Management page. For further details, refer to [Data Management](#) section.

Use **System** → **Archives** → **Archive Files** page to view archived log files generated by Cyberoam-iView:

This section describes how to:

- [Load Archived Files](#)
- [Search in Archived Files](#)
- [Backup Archived Files](#)
- [Download Backup Files](#)
- [Restore Archived Files](#)
- [Unload Archived Files](#)

Go to System → Archives → Archive Files to view archived log files.

Date	File Details	Total Size	Action
2009/12/18	<input type="checkbox"/> 18_23hrs.log (0.00 KB) <input checked="" type="checkbox"/> 12_17hrs.log (468.02 MB) <input type="checkbox"/> 06_11hrs.log (378.01 MB) <input type="checkbox"/> 00_05hrs.log (268.01 MB)	1.09 GB	Load Unload Search BackUp

Screen – Archived Files

Screen Elements	Description
Date	Date of archive logs
File Details	<p>Cyberoam-iView stores archived data for a specified day in four different logs. Every 4 hours, the summarized data from one log is rotated to another log. Report for the time interval of less than 4 hours is generated from the actual data hence is the most accurate report. While report for the larger time interval is generated from the summarized logs hence less precise. Depending on the requirement, select the archive file to generate the report.</p> <p>This column displays file for individual part with respective data size. Cyberoam-iView can display archive files for maximum of 15 days per page.</p>
Total Size	Total size of archive data for the specified day.

Action	Action that can be performed on archived data: <ul style="list-style-type: none"> • Load: Load archived file from your local drive to the iView database. • Unload: Unload archived file from Cyberoam iView database. • Search: Perform a refined search based on multiple criteria. • Backup: Take backup of selected file on the machine on which iView is installed.
--------	--

Table – Archived Files Screen Elements

Load Archived Files

Administrator needs to load the files in Cyberoam iView database to:

- [Search archived files](#)
- [Unload archived files](#)

Go to System → Archives → Archive Files

Date	File Details	Total Size	Action
2009/12/18	<input type="checkbox"/> 18_23hrs.log (0.00 KB) <input checked="" type="checkbox"/> 12_17hrs.log (468.02 MB) <input checked="" type="checkbox"/> 06_11hrs.log (378.01 MB) <input type="checkbox"/> 00_05hrs.log (268.01 MB)	1.09 GB	Load Unload Search BackUp

Screen – Load Archived Files

Screen Elements	Description
Date	Displays date of archive log files.
File Details	It will display list of all log files . Click the checkbox against file to be loaded in Cyberoam iView database.
Load	Click to load selected file in Cyberoam iView database. The checkbox will be disabled once the file is loaded.

Table – Load Archived Files Screen Elements

Date	File Details	Total Size	Action
2009/12/22	<input type="checkbox"/> 18_23hrs.log (0.00 KB) <input type="checkbox"/> 12_17hrs.log (60.00 MB) <input checked="" type="checkbox"/> 06_11hrs.log (188.01 MB) 28.00 MB Loaded... <input type="checkbox"/> 00_05hrs.log (120.00 MB)	396.02 MB	Load Search BackUp

Partially loaded Archived File

Screen – Partially Loaded Archived Files

Date	File Details	Total Size	Action
2009/12/22	<input type="checkbox"/> 18_23hrs.log (0.00 KB) <input type="checkbox"/> 12_17hrs.log (70.00 MB) <input checked="" type="checkbox"/> 06_11hrs.log (216.01 MB) <input type="checkbox"/> 00_05hrs.log (120.00 MB)	406.02 MB	Load Unload Search BackUp

Loaded Archived File

Screen – Fully Loaded Archived Files

Search in Archive Files

Prerequisite

Loading of appropriate archived file is required.

Go to System → Archives → Archive Files and click **Search** to perform search in loaded archived file.

Screen – Search in Archived Files

Screen Elements	Description
Advanced Search options	Logs search criteria can be based on either of the following: Match to All of the following - Click to get search results based on all mentioned criteria. Match any of the following - Click to get search results based on any of the mentioned criterion.
Search Criteria	Available search criteria for Formatted Logs and Raw Logs: <ul style="list-style-type: none"> • Protocol • Source • Destination • User • URL • Data Sent (in Bytes) • Data Received (in Bytes) • Rule
Add Criteria Button	Click to add a new search criterion.
Remove Criteria Button	Click to remove the added criterion.
Formatted Logs	Click to view logs in iView format.
Raw Logs	Click to view logs in raw format i.e. syslog format.

Table – Search Criteria Section Elements

Screen Elements	Description
Date Time	Displays date and time for the log.
Device Name	Displays device name
Firewall Rule ID	Displays firewall rule ID as configured in the device.
Username	Displays name of the user as defined in the device.
URL	Displays IP address or URL name accessed by the user.
Source IP	Displays source IP address.
Destination IP	Displays destination IP address
Protocol	Displays protocol number.
Sent Bytes	Displays number of bytes sent.
Received Bytes	Displays number of bytes received.

Table – Search Result Screen Elements

Note

Blank fields in result show unavailability of the data.

Backup Archived Files**Prerequisite**

Unloading of the archived file is required to take backup.

Go to System → Archives → Archive Files to take backup of archived files on Cyberoam iView machine.

Archived Files		Backup Files	Restore Files	From: 2009-12-18 00:00:00 To: 2009-12-18 23:59:59
Show 5 days per page	Page 1 of 1		Go to page :	Go
Date	File Details	Total Size	Action	
2009/12/18	<input type="checkbox"/> 18_23hrs.log (0.00 KB)	762.03 MB	Load Search BackUp	
	<input type="checkbox"/> 12_17hrs.log (116.00 MB)			
	<input type="checkbox"/> 06_11hrs.log (378.01 MB)			
	<input checked="" type="checkbox"/> 00_05hrs.log (268.01 MB)			

Screen – Backup Archived Files

Screen Elements	Description
Date	Displays date of archive log files.
File Details	It will display list of all the log files. Select checkbox against the file to take backup on the Cyberoam iView machine.
BackUp	Click to take backup of the selected files If the archived file is partially loaded, then the backup of only unloaded data will be taken. Once the backup file is created, Administrator can download the backup file on any machine including Cyberoam iView machine itself.

Table – Backup Archived Files Screen Elements

Archived Files Backup Files Restore Files From: 2009-12-22 00:00:00 To: 2009-12-22 23:59:59

Backup file created successfully, to download it press "Backup Files" button

Show days per page Page 1 of 1 Go to page: Go

Date	File Details	Total Size	Action
2009/12/22	<input type="checkbox"/> 18_23hrs.log (0.00 KB)	442.02 MB	Load Unload Search BackUp
	<input type="checkbox"/> 12_17hrs.log (106.01 MB)		
	<input checked="" type="checkbox"/> 06_11hrs.log (216.01 MB)		
	<input type="checkbox"/> 00_05hrs.log (120.00 MB)		

Screen – Successful Backup of Archived Files

Backup file naming convention

To help identify the backup of each device, Backup file is named as <Device ID_YYYYMMDDStartHourEndHour>

Where:

- Device ID - As configured in Cyberoam iView
- YYYYYMMDD - Date as displayed on Archive Files page under Date column
- Start Hour End Hour – Time as displayed on Archive Files page under File Details column

Download Backup file

Go to System → Archives → Archive Files and click **Backup Files** button to download the backup on local machine from where Cyberoam iView Web Admin Consoles accessed.

BackupFiles

Filename	Delete	Download
C0504-TYGJD3_200912180005.zip	Delete	Download
C00504-TYGJD3_200912180611.zip	Delete	Download

Screen – Download Archived Files

Screen Elements	Description
Filename	List of all the zipped backup files will be displayed..
Delete	Click to delete backup file
Download	Click to download backup files on the local machine

Table – Download Archived Files Screen Elements

Restore Archived file

Go to System → Archives → Archive Files and click **Restore Files** button to restore the backup.

RestoreFiles

Filename	Action
C:\Documents and Settings\... Browse...	Add
C:\Documents and Settings\... Browse...	Delete

Restore Cancel

Screen – Restore Files

Screen Elements	Description
Filename	Displays path of the file to be restored
Add	Click to add another file.
Delete	Click to delete the selected file
Restore Button	Click to restore the selected file(s)
Cancel Button	Click to return on Archived Files page

Table – Restore Files Screen Elements

Unload Archived Files

Prerequisite

Loading of appropriate archived file is required.

To manage available storage space, the Administrator can unload the archived files once the search has been performed. Please note that unloading file does not delete the data from the Cyberoam iView.

Go to System → Archives → Archive Files

Archived Files		Backup Files	Restore Files	From: 2009-12-18 00:00:00 To: 2009-12-18 23:59:59
Show 5 days per page	Page 1 of 1 Go to page : Go			
Date	File Details	Total Size	Action	
2009/12/18	<input type="checkbox"/> 18_23hrs.log (0.00 KB)	806.03 MB	Load Unload Search BackUp	
	<input checked="" type="checkbox"/> 12_17hrs.log (160.01 MB)			
	<input type="checkbox"/> 06_11hrs.log (378.01 MB)			
	<input type="checkbox"/> 00_05hrs.log (268.01 MB)			

Screen – Unload Archived Files

Screen Elements	Description
Date	Displays date of archive logs.
File Details	Displays list of archived log files generated by Cyberoam iView
Unload	Click to unload loaded file(s) from Cyberoam iView database

Table – Unload Archived Files Screen Elements

Note

Unload option will unload all the loaded files. User will not have option to unload individual file.

IM Archive Logs

IM archive logs are collection of historical records of instant messenger activities. Cyberoam-iView retains archive log data for the configured period. Data Retention period can be configured from the System → Configuration → Data Management page. For further details, refer to [Data Management](#) section

Use **System** → **Archives** → **IM Archive Logs** page to view archived log files generated by Cyberoam-iView:

This section describes how to:

- [Load Archived Files](#)
- [Search in Archived Files](#)
- [Backup Archived Files](#)
- [Download Backup Files](#)
- [Restore Archived Files](#)
- [Unload Archived Files](#)

Go to System → Archives → IM Archive Logs to view archived log files.

Date	File Details	Total Size	Action
2009/12/18	<input type="checkbox"/> 18_23hrs.log (0.00 KB) <input checked="" type="checkbox"/> 12_17hrs.log (468.02 MB) <input type="checkbox"/> 06_11hrs.log (378.01 MB) <input type="checkbox"/> 00_05hrs.log (268.01 MB)	1.09 GB	Load Unload Search BackUp

Screen – Archived Files

Screen Elements	Description
Date	Date of archive logs
File Details	<p>Cyberoam-iView stores archived data for a specified day in four different logs. Every 4 hours, the summarized data from one log is rotated to another log. Report for the time interval of less than 4 hours is generated from the actual data hence is the most accurate report. While report for the larger time interval is generated from the summarized logs hence less precise. Depending on the requirement, select the archive file to generate the report.</p> <p>This column displays file for individual part with respective data size. Cyberoam-iView can display archive files for maximum of 15 days per page.</p>
Total Size	Total size of archive data for the specified day.
Action	<p>Action that can be performed on archived data:</p> <ul style="list-style-type: none"> • Load: Load archived file from your local drive to the iView database. • Unload: Unload archived file from Cyberoam iView database. • Search: Perform a refined search based on multiple criteria. • Backup: Take backup of selected file on the machine on which iView is installed.

Table – Archived Files Screen Elements

Load Archived Files

Administrator needs to load the files in Cyberoam iView database to:

- [Search archived files](#)
- [Unload archived files](#)

Go to System → Archives → IM Archive Logs

Date	File Details	Total Size	Action
2009/12/18	<input type="checkbox"/> 18_23hrs.log (0.00 KB)	1.09 GB	Load Unload Search BackUp
	<input checked="" type="checkbox"/> 12_17hrs.log (468.02 MB)		
	<input checked="" type="checkbox"/> 06_11hrs.log (378.01 MB)		
	<input type="checkbox"/> 00_05hrs.log (268.01 MB)		

Screen – Load Archived Files

Screen Elements	Description
Date	Displays date of archive log files.
File Details	It will display list of all log files. Click the checkbox against file to be loaded in Cyberoam iView database.
Load	Click to load selected file in Cyberoam iView database. The checkbox will be disabled once the file is loaded.

Table – Load Archived Files Screen Elements

Date	File Details	Total Size	Action
2009/12/22	<input type="checkbox"/> 18_23hrs.log (0.00 KB)	396.02 MB	Load Search BackUp
	<input type="checkbox"/> 12_17hrs.log (60.00 MB)		
	<input checked="" type="checkbox"/> 06_11hrs.log (188.01 MB) 28.00 MB Loaded...		
	<input type="checkbox"/> 00_05hrs.log (120.00 MB)		

Partially loaded Archived File

Screen – Partially Loaded Archived Files

Date	File Details	Total Size	Action
2009/12/22	<input type="checkbox"/> 18_23hrs.log (0.00 KB)	406.02 MB	Load Unload Search BackUp
	<input type="checkbox"/> 12_17hrs.log (70.00 MB)		
	<input checked="" type="checkbox"/> 06_11hrs.log (216.01 MB)		
	<input type="checkbox"/> 00_05hrs.log (120.00 MB)		

Loaded Archived File

Screen – Fully Loaded Archived Files

Search in Archive Files

Prerequisite

Loading of appropriate archived file is required.

Go to System → Archives → IM Archive Logs and click **Search** to perform search in loaded archived file.

Advanced Search

☒ Match all of the following ☐ Match any of the following

User is

Add Criteria Search

Remove Criteria Cancel

Formatted Logs Raw Logs

Show 10 results per page

Page 1 of 1 Go to page : Go

Timestamp Protected Contact Peer Contact Conversation Side Message User Source IP Application IM Action Rule Action

Search Result Section Search Criteria Section

Screen – Search in IM Archived Files

Screen Elements	Description
Advanced Search options	Logs search criteria can be based on either of the following: Match to All of the following - Click to get search results based on all mentioned criteria. Match any of the following - Click to get search results based on any of the mentioned criterion.
Search Criteria	Available search criteria for Formatted Logs and Raw Logs: <ul style="list-style-type: none"> • User • Source • Protected Contact • Peer Contact • Conversation side • Application • IM Action • Message • Rule
Add Criteria Button	Click to add a new search criterion.
Remove Criteria Button	Click to remove the added criterion.
Formatted Logs	Click to view logs in iView format.
Raw Logs	Click to view logs in raw format i.e. syslog format.

Table – Search Criteria Section Elements

Screen Elements	Description
Timestamp	Displays time of the IM activity in YYYY-MM-DD HH:MM:SS format
Protected Contact	Displays IM Username of the user who is protected by monitored device i.e. whose Internet traffic is passing through monitored device
Peer Contact	Displays IM Username of Peer contact
Conversation Site	Possible values <ul style="list-style-type: none"> 1: Send 2: Receive
Message	Displays full conversation between the protected contact and peer contact
User	Displays monitored device username of IM user
Source IP	Displays source IP address.
Application	Displays name of the application: <ul style="list-style-type: none"> 1.Yahoo 2.WSM
IM Action	Displays IM action: <ul style="list-style-type: none"> 0: Login 1: Message 2: Webcam 3: File Transfer 4: Logout
Rule Action	Displays rule action: <ul style="list-style-type: none"> 0: Allowed 1: Denied

Table – Search Result Screen Elements

Note

Blank fields in result show unavailability of the data.

Backup Archived Files**Prerequisite**

Unloading of the archived file is required to take backup.

Go to System → Archives → IM Archive Logs to take backup of archived files on Cyberoam iView machine.

Archived Files		Backup Files	Restore Files	From: 2009-12-18 00:00:00 To: 2009-12-18 23:59:59
Show	5 days per page	Page 1 of 1 Go to page : <input type="text"/> Go		
Date	File Details	Total Size	Action	
2009/12/18	<input type="checkbox"/> 18_23hrs.log (0.00 KB)	762.03 MB	Load Search BackUp	
	<input type="checkbox"/> 12_17hrs.log (116.00 MB)			
	<input type="checkbox"/> 06_11hrs.log (378.01 MB)			
	<input checked="" type="checkbox"/> 00_05hrs.log (268.01 MB)			

Screen – Backup Archived Files

Screen Elements	Description
Date	Displays date of archive log files.

File Details	It will display list of all the log files. Select checkbox against the file to take backup on the Cyberoam iView machine.
BackUp	Click to take backup of the selected files If the archived file is partially loaded, then the backup of only unloaded data will be taken. Once the backup file is created, Administrator can download the backup file on any machine including Cyberoam iView machine itself.

Table – Backup Archived Files Screen Elements

Archived Files

Backup file created successfully, to download it press "Backup Files" button

Show 5 days per page

Page 1 of 1 Go to page: Go

Date	File Details	Total Size	Action
2009/12/22	<input type="checkbox"/> 18_23hrs.log (0.00 KB)	442.02 MB	Load Unload Search BackUp
	<input type="checkbox"/> 12_17hrs.log (106.01 MB)		
	<input checked="" type="checkbox"/> 06_11hrs.log (216.01 MB)		
	<input type="checkbox"/> 00_05hrs.log (120.00 MB)		

Screen – Successful Backup of Archived Files

Backup file naming convention

To help identify the backup of each device, Backup file is named as <Device ID_YYYYMMDDStartHourEndHour>

Where:

- Device ID - As configured in Cyberoam iView
- YYYYYMMDD - Date as displayed on Archive Files page under Date column
- Start Hour End Hour – Time as displayed on Archive Files page under File Details column

Download Backup file

Go to System → Archives → IM Archive Logs and click **Backup Files** button to download the backup on local machine from where Cyberoam iView Web Admin Consoles accessed.

BackupFiles

Filename	Delete	Download
C0504-TYGJD3_200912180005.zip	Delete	Download
C00504-TYGJD3_200912180611.zip	Delete	Download

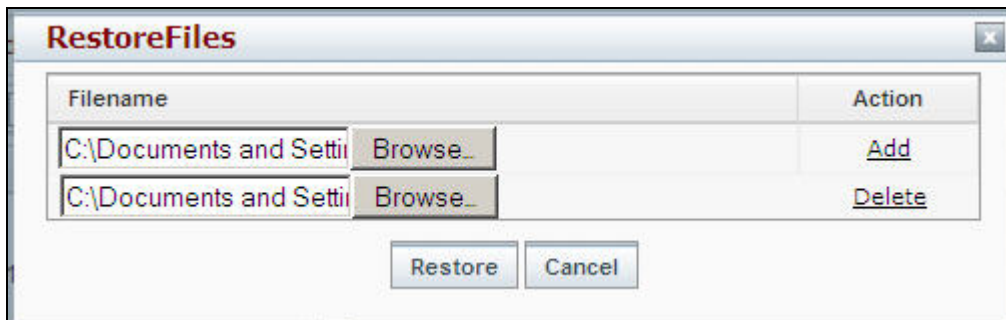
Screen – Download Archived Files

Screen Elements	Description
Filename	List of all the zipped backup files will be displayed..
Delete	Click to delete backup file
Download	Click to download backup files on the local machine

Table – Download Archived Files Screen Elements

Restore Archived file

Go to System → Archives → IM Archive Logs and click **Restore Files** button to restore the backup.



Screen – Restore Files

Screen Elements	Description
Filename	Displays path of the file to be restored
Add	Click to add another file.
Delete	Click to delete the selected file
Restore Button	Click to restore the selected file(s)
Cancel Button	Click to return on Archived Files page

Table – Restore Files Screen Elements

Unload Archived Files

Prerequisite

Loading of appropriate archived file is required.

To manage available storage space, the Administrator can unload the archived files once the search has been performed. Please note that unloading file does not delete the data from the Cyberoam iView.

Go to System → Archives → IM Archive Logs



Screen – Unload Archived Files

Screen Elements	Description
Date	Displays date of archive logs.
File Details	Displays list of archived log files generated by Cyberoam iView
Unload	Click to unload loaded file(s) from Cyberoam iView database

Table – Unload Archived Files Screen Elements

Note:

Unload option will unload all the loaded files. User will not have option to unload individual file.

Cyberoam iView Documentation Copyright

© 2009 Elitecore Technologies Ltd. All rights reserved worldwide.

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. Elitecore assumes no responsibility for any errors that may appear in this document. Information is subject to change without notice.

In no event shall Elitecore be liable for any direct, indirect, or incidental damages, including, damage to data arising out of the use or inability to use this manual.

No part of this work may be reproduced or transmitted in any form or by any means except as expressly permitted by Elitecore Technologies Ltd. This does not include those documents and software developed under the terms of the open source General Public License.

Cyberoam iView™ is the trademark of Elitecore Technologies Ltd.

If you need commercial technical support for this product please visit www.cyberoam-iview.com. You can visit open source Cyberoam iView forums at <https://sourceforge.net/projects/cyberoam-iview/support> to get support from the project community.

Cyberoam iView License Policy

Cyberoam iView is free software, if you are using and/or enhancing / developing open source applications: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

A copy of the GNU General Public License is available along with this program; see the COPYING file for the detailed license.

The interactive user interfaces in modified source and object code versions of this program must display Appropriate Legal Notices, as required under Section 5 of the GNU General Public License version 3.

In accordance with Section 7(b) of the GNU General Public License version 3, these Appropriate Legal Notices must retain the display of the "Cyberoam Elitecore Technologies Initiative" logo.



Cyberoam iView™ is the trademark of Elitecore Technologies Ltd.