Internet Content Inspector

ICI-1000 / ICI-2000

User Manual

v1.00

Important Notice
This user manual is delivered subjected to the following terms and conditions. The copyrights, intellectual property rights and trade secrets included in this user manual are owned by ICI. The user manual is provided to ICI customers for the sole purpose of obtaining information with respect to the installation, implementation and function of the ICI system and should not be used for any other purpose. The information contained in this user manual is proprietary to ICI and strictly confidential. It is strictly forbidden to copy, duplicate, reproduce or disclose this user manual or any part of this user manual without prior written permission from ICI.

The Management Team of Digital Data Communications Asia Ltd

Copyright

Disclaimer
LevelOne does not assume any liability arising out the application or use of any products, or software described herein. Neither does it convey any license under its parent rights not the parent rights of others. LevelOne further reserves the right to make changes in any products described herein without notice. The publication is subject to change without notice.

Trademarks
LevelOne is a registered trademark of Digital Data Communications Group. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Table of Contents

Introduction

Protecting Your Business
in the Cloud Era

Introducing LevelOne Internet Content Inspector
Telco Grade Solution for Small Medium Busness

- Visibility
- Control
- Protection

LevelOne Internet **C**ontent **I**nspector, **ICI** empowers your business security and operations teams by providing granular data monitoring and precise packet and session reconstruction capabilities. The solution is designed to combine process and technology into a single effective system for network forensics. Business can for the first time embrace Web 2.0 and maintain complete visibility and control, while significantly reducing total cost of ownership through device consolidation. ICI offers real innovation by enabling unprecedented visibility and control of applications and content with no performance degradation. It identify applications accurately - regardless of port, protocol, evasive tactic or SSL encryption – and scan content to stop threats and prevent data leakage.

It intercepts, captures and reconstruct Internet activities such as Email (POP3, SMTP, IMAP), Webmail Read and Sent (Yahoo Mail, Gmail, Windows Live Hotmail, Seednet etc.), Instant Messaging or Chat (Yahoo, Windows Live Messenger or MSN, ICQ, AOL, QQ, UT Chat Room, IRC, Gtalk, Skype Voice Call Duration Log), HTTP (URL Link, Content, Upload and Download, Video Streaming), File Transfer (P2P File Sharing, FTP), Online Games, VoIP (Yahoo Messenger) and Webcam (Yahoo Messenger and Windows Live Messenger - MSN), VoIP (RTP Voice Call) and Telnet sessions. ICI system encourages efficiency, prevents company network resource from abuses by employees, tracing culprits of information and confidential data leakage, and monitors activities and online behaviour of employees.

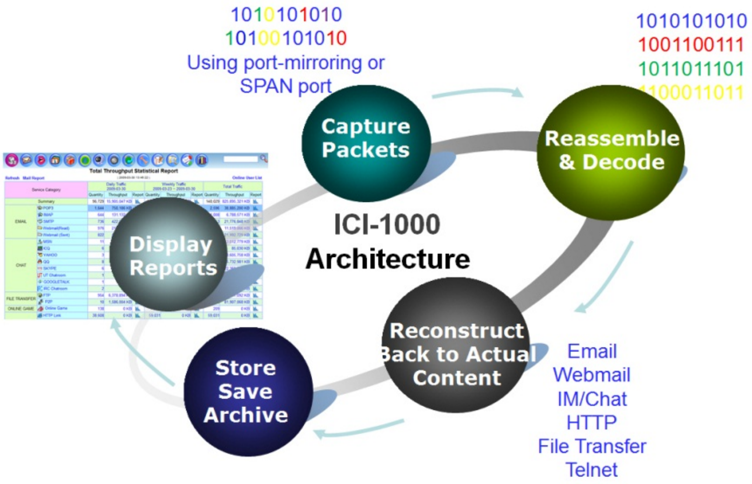
Ethernet LAN interception is an important approach to gather information of communications and digital evidence. Ethernet LAN interception solutions capture all the traffic on the LAN network and monitor the Internet activities. It is capable of live intercepting with real time capturing and decoding/reconstruction, category classifying, behaviour analysing, data mining, reporting with statistics etc.

ICI comes with wide variety of management and administrative functions. It provides you various types of report with Top-Down View. Reports that can be created include Total Throughput Statistical Report, Network Service Report (Daily, Weekly basis), Top Websites etc. All statistics can be displayed in per IP Address or per User Account basis.

ICI also provides varieties of search functions. It provides Free Text Search (search by Key Words with Boolean support), Conditional Search, Similar Search and Association with Relationship Search. It also comes with Alert and Notification (Throughput, Conditional and Key Words Alert) functions that allow the network Administrator to setup different alert rules and parameters. This allows alert to be triggered (email to be sent to Administrator) once the specified content is found in the captured and reconstructed content.

Backup function allows user to back up the captured raw data files or reconstructed contents. User can setup auto backup to backup these files to external drive (NAS or SAN) through FTP upload method. Besides, user can opt for manually backup these files by burning them into CD/DVD or even downloaded them to a local hard drive/PC.

Other functions available are like Bookmark, Capture File List (Comparing the content of two files), Online IP List, Authority Assignment, Syslog Server etc. Others functions include hashed export (backup), file content comparison etc.

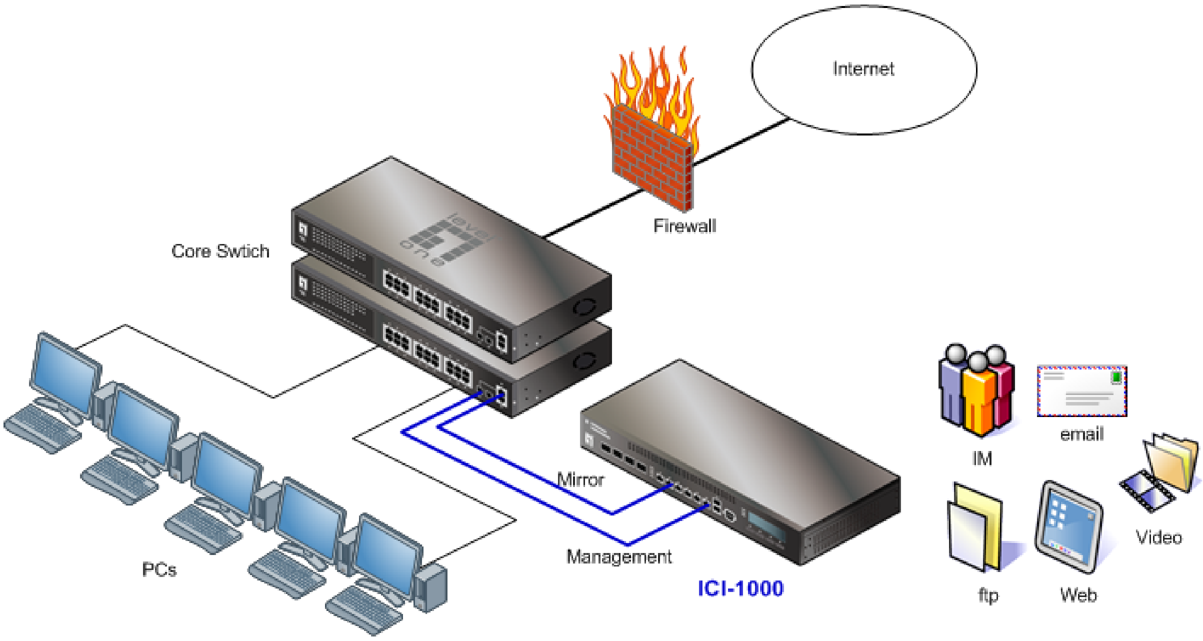


Who Need the ICI System

- Financial, Banking and Investment Organisations where all Internet transactions and communications need to be archived (Record Keeping).
- Marketing organizations, design house, high technology and R&D firms where critical confidential information need protected.
- Schools, colleges, institutions and universities that would like to monitor students and staffs online activities and behaviour.
- Government agencies and ministries such as Police Intelligence, Military Intelligence, Secret Service Agencies, National Security Agencies, Criminal Investigation Agencies, Counter Terrorism Agencies etc.
- Any company or organization that wants to monitor, backup and archive their daily Internet transaction and data.

Application and Implementation

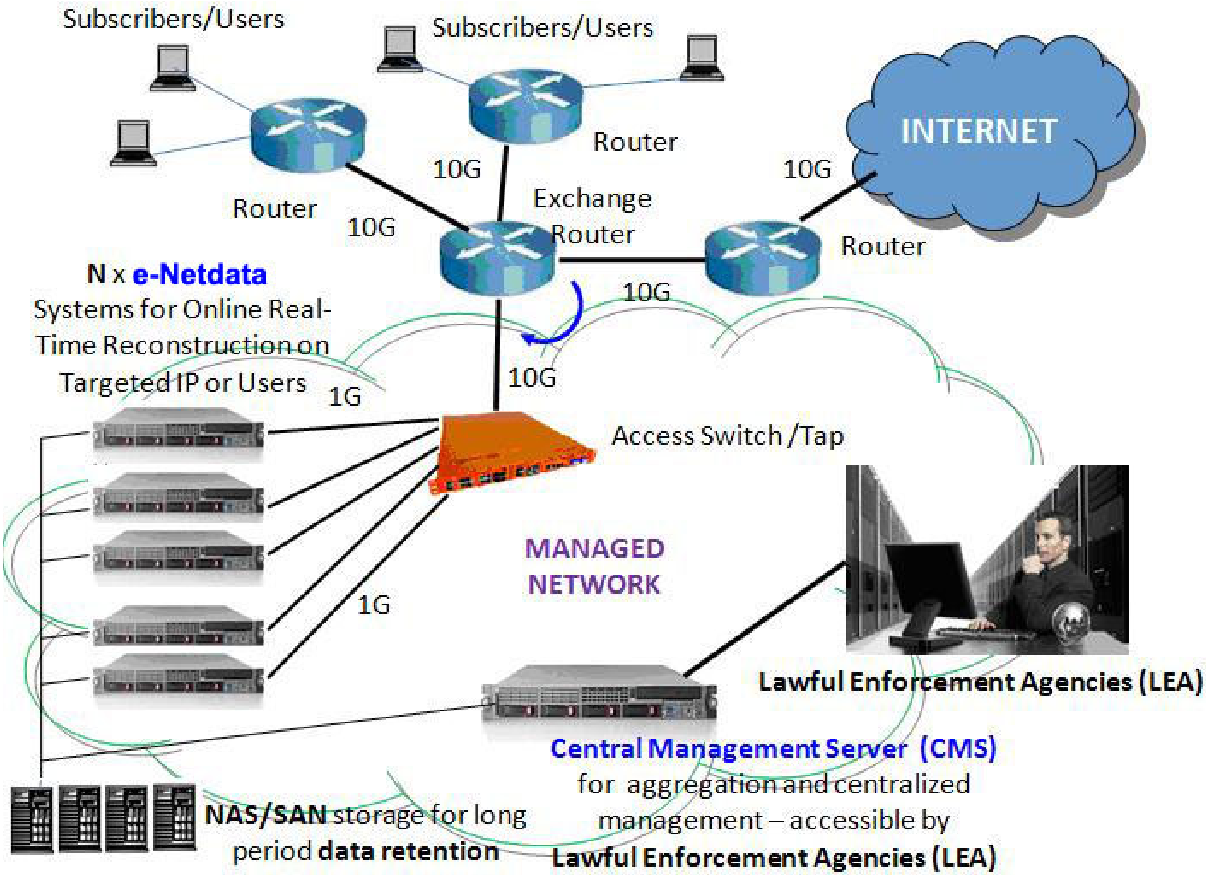
The diagram below is a common ICI application and implementation diagram which can be applied to any organization networks. ICI uses sniffer technology to sniff or capture network Internet packets through a port-mirroring capable switch (normally a smart switch or layer 2/3 switch; a HUB can be used too as HUB broadcast traffic to all ports). It then parses (decodes and reconstructs) the captured raw data packets, store them in system database and displays the reconstructed data with reports in original and readable format in the Web GUI.



Ethernet LAN Organization Network Monitoring and Interception

ICI can also be implementation at network with huge volume of traffic throughput such as mass interception and lawful interception at Telco or ISP networks. This implementation is normally for lawful enforcement agencies (LEA) such as cyber security agencies, national security agencies, criminal investigation bureau, police and military intelligence. Please contact LevelOne sales team for more details

sales@level1.com


Subscribers/Users
Subscribers/Users
Router
Router
10G
10G
INTERNET
Exchange Router
10G
Router
N x e-Netdata
Systems for Online Real-Time Reconstruction on Targeted IP or Users
1G
10G
10G
Access Switch /Tap
MANAGED NETWORK
1G
Lawful Enforcement Agencies (LEA)
Central Management Server (CMS)
for aggregation and centralized management – accessible by
Lawful Enforcement Agencies (LEA)
NAS/SAN storage for long period data retention

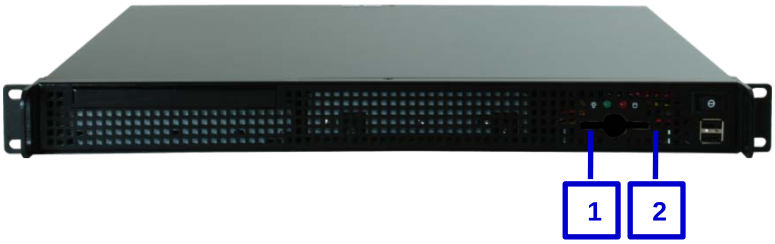
Telco or ISP lawful Internet Interception

Unpacking & Installing

Packing Checklist

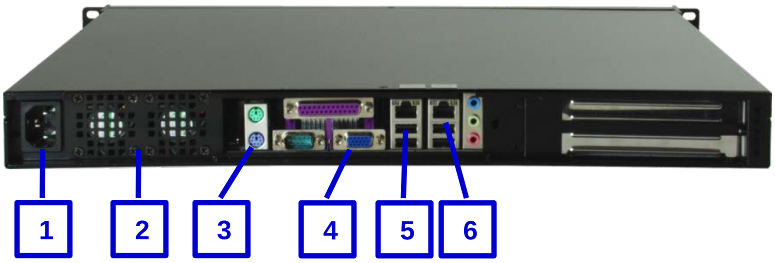
- ✓ 19 inch 1U Rack mountable Server x 1
- ✓ Quick Installation Guide x 1
- ✓ CD Manual x 1
- ✓ Mounting Bracket set x 1
- ✓ Power Cord x 1

Front Panel



1. Power LED
2. HDD LED

Rear Panel



1. Power Socket
2. Power Supply Unit
3. PS/2 KB & Mouse (for local console)
4. VGA Display (for local console)
5. Monitor Ethernet Port
6. Management Ethernet Port

Requirement

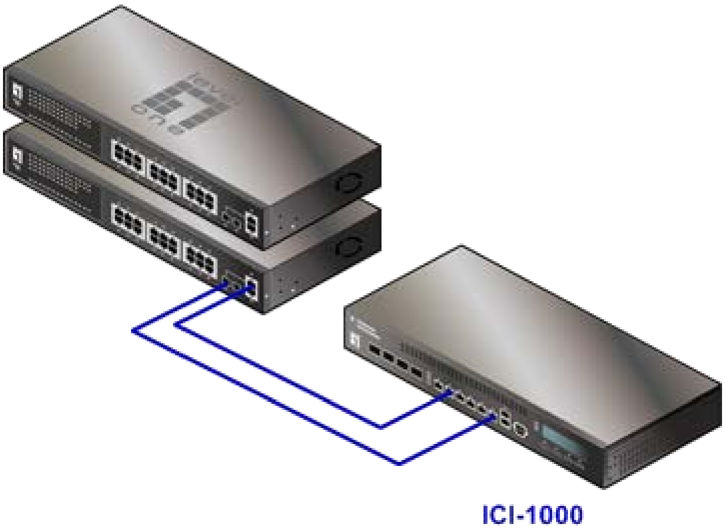
In order to get the ICI to capture your network activities successfully, a **Port-Mirroring** feature on the network Ethernet switch is must. User can monitor traffic from any source port to a target port for real-time analysis. Attach the ICI to the target port and study the traffic crossing the source port in a completely unobtrusive manner. Most the Web Smart and fully Managed Layer2 Ethernet switches support the **Port-Mirroring** feature

- ✓ Web Smart or Fully Managed Layer2/3 Switch with Port-Mirroring feature

For the best performance and keep disruption minimal, we introduce the **Mirror** mode implementation only which provides the Real-time Reconstruction and keep disruption minimal at the same time. The captured packets are saved in PCAP format

Installation

1. Connect the power cord to ICI power socket on the rear panel
2. Patch lead between Switch Mirror port and ICI Monitor port
3. Patch lead between Switch port (any available port) and ICI Management port



Default Settings

IP	192.168.1.60
Username	root
Password	000000 (six zero)

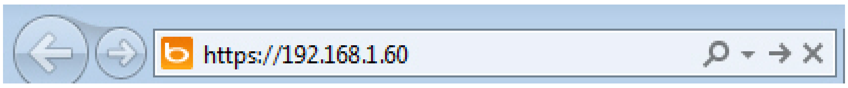
Note: Internet Explorer (IE ver6, 7 and 8) are recommended web browser for Web GUI management access of ICI system.

Getting Started

This chapter shows how to manage the ICI system via standard Web Browser over local network, also a quick guide about each function button from menu bar, as well as the examples of feature-rich of report feature.

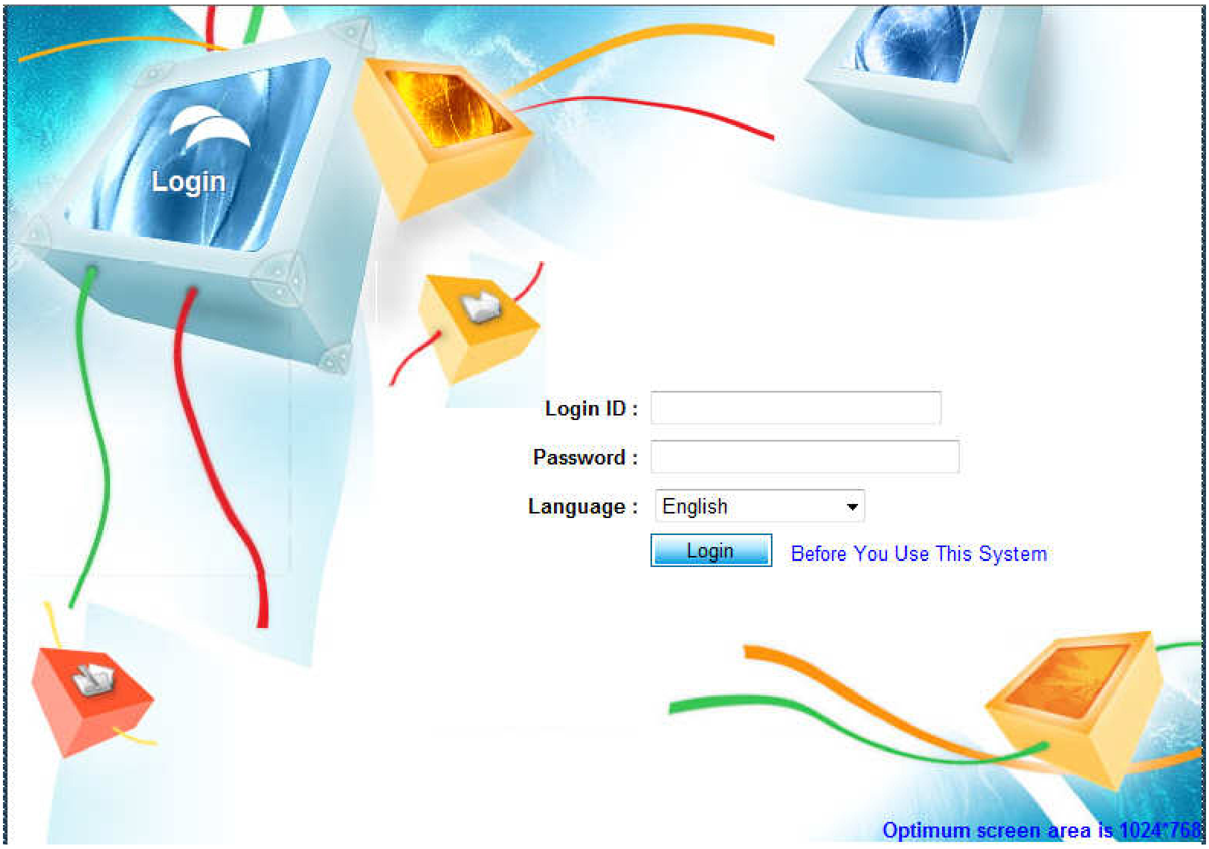
Web Management Interface

1. Use Internet Explorer (IE) Web Browser to access ICI system web management site. ICI system uses port 443 for secure web access. Please remember to key in https://x.x.x.x, for example https://192.168.1.60 (which is the default login).



https://192.168.1.60

2. Before you use this system, please make sure you have Java applet installed. Read the instruction on “Before You Use This System” at the login page.
3. Username: root & Password: 000000 (six zero)
4. Choose your preferred language [Traditional Chinese] or [English] and then click on the login button.



Login ID :

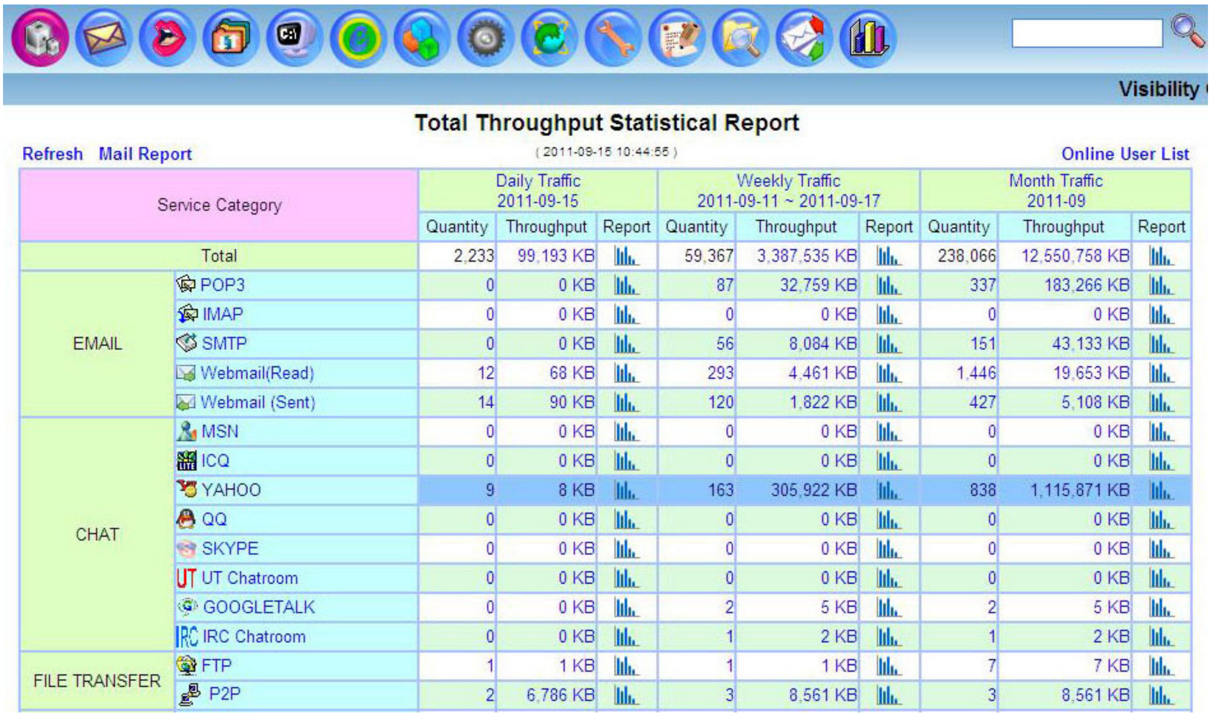
Password :

Language : English

Note: Internet Explorer (IE ver6, 7 and 8) are recommended web browser for Web GUI management access of ICI system.

System Main Page

The navigation icon bar is on the top section of the Web Management GUI. ICI Homepage provides information on the Total Throughput Statistical Report (as shown in diagram below) with Top-Down and Drilled-Down capabilities.



Total Throughput Statistical Report

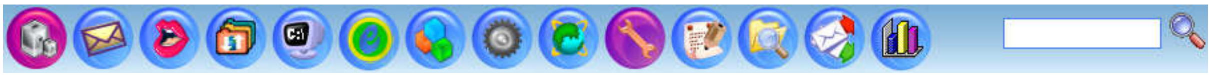
Refresh Mail Report

(2011-09-15 10:44:55)

Online User List

Service Category		Daily Traffic 2011-09-15			Weekly Traffic 2011-09-11 ~ 2011-09-17			Month Traffic 2011-09		
		Quantity	Throughput	Report	Quantity	Throughput	Report	Quantity	Throughput	Report
Total		2,233	99,193 KB	📊	59,367	3,387,535 KB	📊	238,066	12,550,758 KB	📊
EMAIL	POP3	0	0 KB	📊	87	32,759 KB	📊	337	183,266 KB	📊
	IMAP	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	SMTP	0	0 KB	📊	56	8,084 KB	📊	151	43,133 KB	📊
	Webmail(Read)	12	68 KB	📊	293	4,461 KB	📊	1,446	19,653 KB	📊
	Webmail (Sent)	14	90 KB	📊	120	1,822 KB	📊	427	5,108 KB	📊
CHAT	MSN	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	ICQ	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	YAHOO	9	8 KB	📊	163	305,922 KB	📊	838	1,115,871 KB	📊
	QQ	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	SKYPE	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	UT Chatroom	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	GOOGLETALK	0	0 KB	📊	2	5 KB	📊	2	5 KB	📊
	IRC Chatroom	0	0 KB	📊	1	2 KB	📊	1	2 KB	📊
FILE TRANSFER	FTP	1	1 KB	📊	1	1 KB	📊	7	7 KB	📊
	P2P	2	6,786 KB	📊	3	8,561 KB	📊	3	8,561 KB	📊

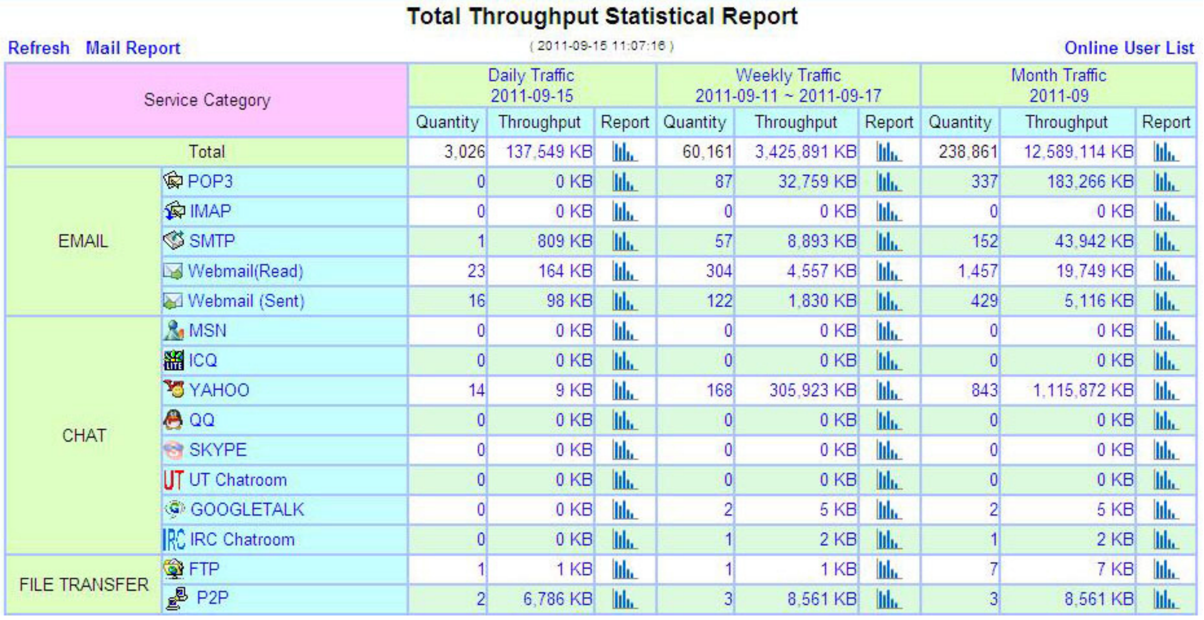
Icon Bar



Icon	Function	Icon	Function
✉	EMAIL RECORD	⟳	SYSTEM STATUS
👄	CHAT RECORD	🔧	SYSTEM TOOLS
📁	FILE TRANSFER RECORD	📝	REGISTER
●	OTHERS RECORD	🔍	DATA SEARCH
e	HTTP RECORD	✉	ALERT SERVICE
C:\	TELNET RECORD	📊	REPORT
⚙	SYSTEM SETTING	🖥	HOMEPAGE/LOGOUT

Main Page - Total Throughput Statistical Report

Total Throughput Statistical Report provides Daily, Weekly and Total Traffic statistic of different Internet service categories for the organization network. It shows the total traffic amount usage by the entire network as well as breaks them out into different service categories. Online User List will show the List of users (IP Address and Account).



Total Throughput Statistical Report

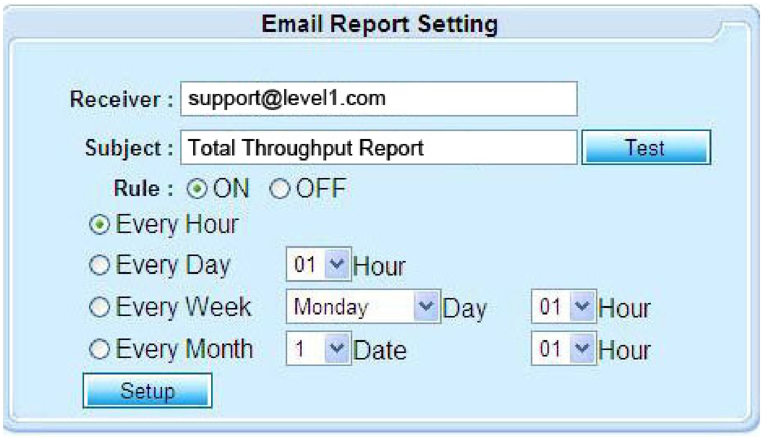
Refresh Mail Report

(2011-09-15 11:07:16)

Online User List

Service Category		Daily Traffic 2011-09-15			Weekly Traffic 2011-09-11 ~ 2011-09-17			Month Traffic 2011-09		
		Quantity	Throughput	Report	Quantity	Throughput	Report	Quantity	Throughput	Report
Total		3,026	137,549 KB	📊	60,161	3,425,891 KB	📊	238,861	12,589,114 KB	📊
EMAIL	POP3	0	0 KB	📊	87	32,759 KB	📊	337	183,266 KB	📊
	IMAP	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	SMTP	1	809 KB	📊	57	8,893 KB	📊	152	43,942 KB	📊
	Webmail(Read)	23	164 KB	📊	304	4,557 KB	📊	1,457	19,749 KB	📊
	Webmail (Sent)	16	98 KB	📊	122	1,830 KB	📊	429	5,116 KB	📊
CHAT	MSN	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	ICQ	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	YAHOO	14	9 KB	📊	168	305,923 KB	📊	843	1,115,872 KB	📊
	QQ	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	SKYPE	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	UT Chatroom	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	GOOGLETALK	0	0 KB	📊	2	5 KB	📊	2	5 KB	📊
	IRC Chatroom	0	0 KB	📊	1	2 KB	📊	1	2 KB	📊
FILE TRANSFER	FTP	1	1 KB	📊	1	1 KB	📊	7	7 KB	📊
	P2P	2	6,786 KB	📊	3	8,561 KB	📊	3	8,561 KB	📊

Mail Report allows Administrator to send different reports such as Total Throughput Statistical Report, Online IP List etc. to the specific Email account immediately or either by hourly, daily, weekly or monthly basis as shown below.



Email Report Setting

Receiver : support@level1.com

Subject : Total Throughput Report [Test]

Rule : ● ON ○ OFF

● Every Hour

○ Every Day 01 Hour

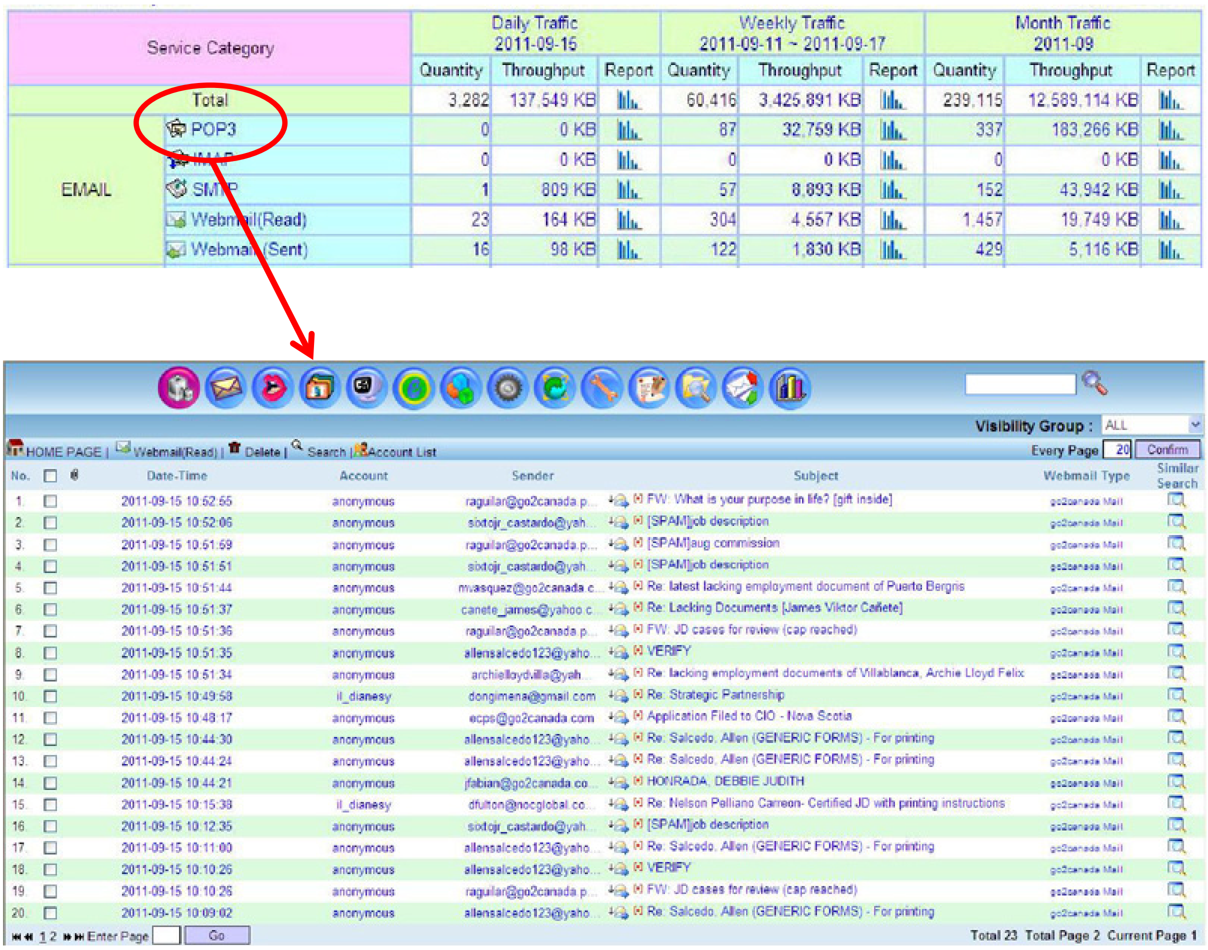
○ Every Week Monday Day 01 Hour

○ Every Month 1 Date 01 Hour

[Setup]

Example 1:

Click on the Email - POP3 Quantity of Daily Traffic, it will List down the entire POP3 Emails in the database.



Service Category		Daily Traffic 2011-09-15			Weekly Traffic 2011-09-11 ~ 2011-09-17			Month Traffic 2011-09		
		Quantity	Throughput	Report	Quantity	Throughput	Report	Quantity	Throughput	Report
Total		3,282	137,549 KB		60,416	3,425,891 KB		239,115	12,589,114 KB	
EMAIL	POP3	0	0 KB		87	32,759 KB		337	183,266 KB	
	IMAP	0	0 KB		0	0 KB		0	0 KB	
	SMTP	1	809 KB		57	8,893 KB		152	43,942 KB	
	Webmail(Read)	23	164 KB		304	4,557 KB		1,457	19,749 KB	
	Webmail(Sent)	16	98 KB		122	1,830 KB		429	5,116 KB	

Visibility Group : ALL

HOME PAGE | Webmail(Read) | Delete | Search | Account List

Every Page 20 Confirm

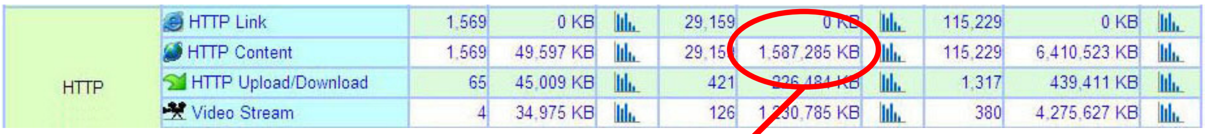
No.	□	Date-Time	Account	Sender	Subject	Webmail Type	Similar Search
1.	□	2011-09-15 10:52:55	anonymous	raguilar@go2canada.p...	FW: What is your purpose in life? [gift inside]	go2canada Mail	
2.	□	2011-09-15 10:52:06	anonymous	sixtojr_castardo@yah...	[SPAM]job description	go2canada Mail	
3.	□	2011-09-15 10:51:59	anonymous	raguilar@go2canada.p...	[SPAM]aug commission	go2canada Mail	
4.	□	2011-09-15 10:51:51	anonymous	sixtojr_castardo@yah...	[SPAM]job description	go2canada Mail	
5.	□	2011-09-15 10:51:44	anonymous	mvasquez@go2canada.c...	Re: latest lacking employment document of Puerto Bergris	go2canada Mail	
6.	□	2011-09-15 10:51:37	anonymous	canete_james@yahoo.c...	Re: Lacking Documents [James Viktor Cañete]	go2canada Mail	
7.	□	2011-09-15 10:51:36	anonymous	raguilar@go2canada.p...	FW: JD cases for review (cap reached)	go2canada Mail	
8.	□	2011-09-15 10:51:35	anonymous	allensalcedo123@yaho...	VERIFY	go2canada Mail	
9.	□	2011-09-15 10:51:34	anonymous	archielloydvilla@yah...	Re: lacking employment documents of Villablanca, Archie Lloyd Felix	go2canada Mail	
10.	□	2011-09-15 10:49:58	il_dianesy	dongimena@gmail.com	Re: Strategic Partnership	go2canada Mail	
11.	□	2011-09-15 10:48:17	anonymous	ecps@go2canada.com	Application Filed to CIO - Nova Scotia	go2canada Mail	
12.	□	2011-09-15 10:44:30	anonymous	allensalcedo123@yaho...	Re: Salcedo, Allen (GENERIC FORMS) - For printing	go2canada Mail	
13.	□	2011-09-15 10:44:24	anonymous	allensalcedo123@yaho...	Re: Salcedo, Allen (GENERIC FORMS) - For printing	go2canada Mail	
14.	□	2011-09-15 10:44:21	anonymous	jfabian@go2canada.co...	HONRADA, DEBBIE JUDITH	go2canada Mail	
15.	□	2011-09-15 10:15:38	il_dianesy	dfulton@nocglobal.co...	Re: Nelson Pelliano Carreon- Certified JD with printing instructions	go2canada Mail	
16.	□	2011-09-15 10:12:35	anonymous	sixtojr_castardo@yah...	[SPAM]job description	go2canada Mail	
17.	□	2011-09-15 10:11:00	anonymous	allensalcedo123@yaho...	Re: Salcedo, Allen (GENERIC FORMS) - For printing	go2canada Mail	
18.	□	2011-09-15 10:10:26	anonymous	allensalcedo123@yaho...	VERIFY	go2canada Mail	
19.	□	2011-09-15 10:10:26	anonymous	raguilar@go2canada.p...	FW: JD cases for review (cap reached)	go2canada Mail	
20.	□	2011-09-15 10:09:02	anonymous	allensalcedo123@yaho...	Re: Salcedo, Allen (GENERIC FORMS) - For printing	go2canada Mail	

1 2 Enter Page Go

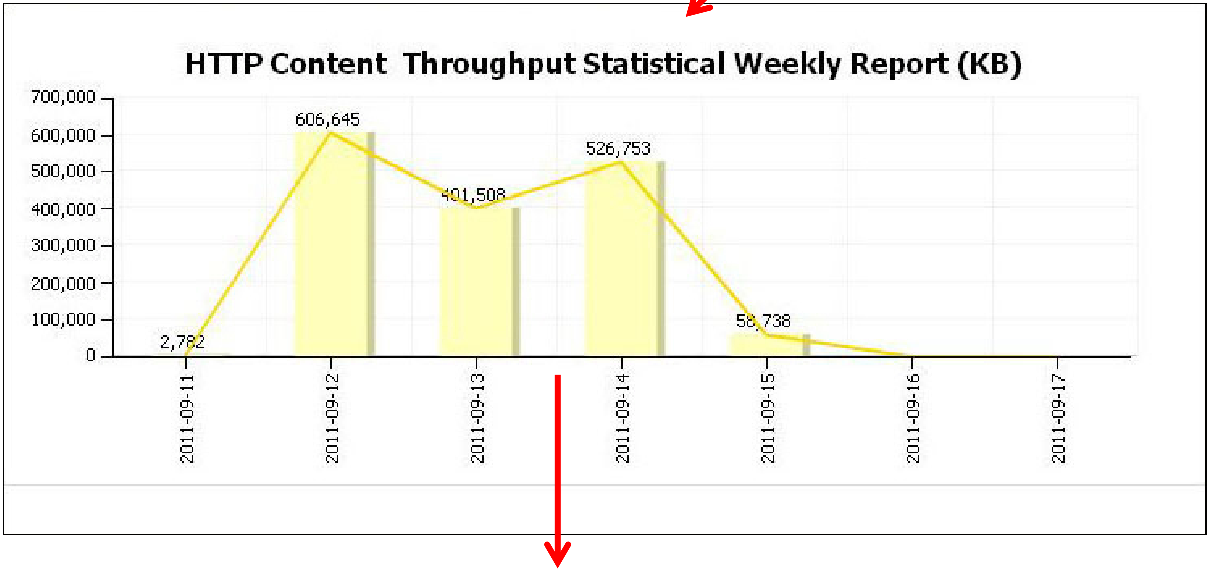
Total 23 Total Page 2 Current Page 1

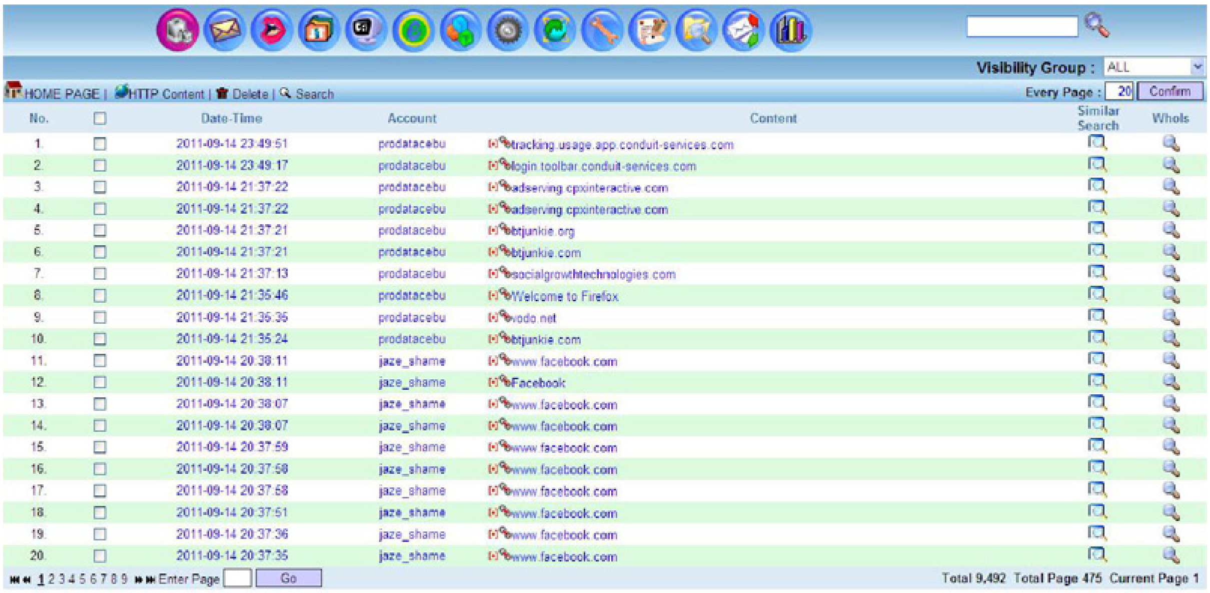
Example 2:

Click on the HTTP – HTTP Content weekly traffic throughput (KB), it will display the bar chart of the HTTP Content traffic for the entire week (7 days). By clicking bar chat (specific day), it will lead you to that day details content.



HTTP	HTTP Link	1,569	0 KB	📊	29,159	0 KB	📊	115,229	0 KB	📊
	HTTP Content	1,569	49,597 KB	📊	29,159	1,587,285 KB	📊	115,229	6,410,523 KB	📊
	HTTP Upload/Download	65	45,009 KB	📊	421	226,484 KB	📊	1,317	439,411 KB	📊
	Video Stream	4	34,975 KB	📊	126	1,230,785 KB	📊	380	4,275,627 KB	📊





Visibility Group : ALL

HOME PAGE | HTTP Content | Delete | Search

Every Page : 20 Confirm

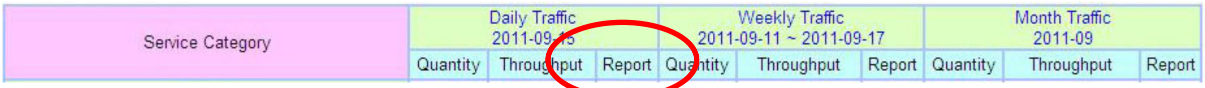
No.	□	Date-Time	Account	Content	Similar Search	WhoIs
1.	□	2011-09-14 23:49:51	prodatacebu	tracking.usage.app.conduit-services.com	🔍	🔍
2.	□	2011-09-14 23:49:17	prodatacebu	login.toolbar.conduit-services.com	🔍	🔍
3.	□	2011-09-14 21:37:22	prodatacebu	adserving.cpxinteractive.com	🔍	🔍
4.	□	2011-09-14 21:37:22	prodatacebu	adserving.cpxinteractive.com	🔍	🔍
5.	□	2011-09-14 21:37:21	prodatacebu	btjunkie.org	🔍	🔍
6.	□	2011-09-14 21:37:21	prodatacebu	btjunkie.com	🔍	🔍
7.	□	2011-09-14 21:37:13	prodatacebu	socialgrowthtechnologies.com	🔍	🔍
8.	□	2011-09-14 21:35:46	prodatacebu	Welcome to Firefox	🔍	🔍
9.	□	2011-09-14 21:35:35	prodatacebu	vodo.net	🔍	🔍
10.	□	2011-09-14 21:35:24	prodatacebu	btjunkie.com	🔍	🔍
11.	□	2011-09-14 20:38:11	jaze_shame	www.facebook.com	🔍	🔍
12.	□	2011-09-14 20:38:11	jaze_shame	Facebook	🔍	🔍
13.	□	2011-09-14 20:38:07	jaze_shame	www.facebook.com	🔍	🔍
14.	□	2011-09-14 20:38:07	jaze_shame	www.facebook.com	🔍	🔍
15.	□	2011-09-14 20:37:59	jaze_shame	www.facebook.com	🔍	🔍
16.	□	2011-09-14 20:37:58	jaze_shame	www.facebook.com	🔍	🔍
17.	□	2011-09-14 20:37:58	jaze_shame	www.facebook.com	🔍	🔍
18.	□	2011-09-14 20:37:51	jaze_shame	www.facebook.com	🔍	🔍
19.	□	2011-09-14 20:37:36	jaze_shame	www.facebook.com	🔍	🔍
20.	□	2011-09-14 20:37:35	jaze_shame	www.facebook.com	🔍	🔍

1 2 3 4 5 6 7 8 9 Enter Page Go

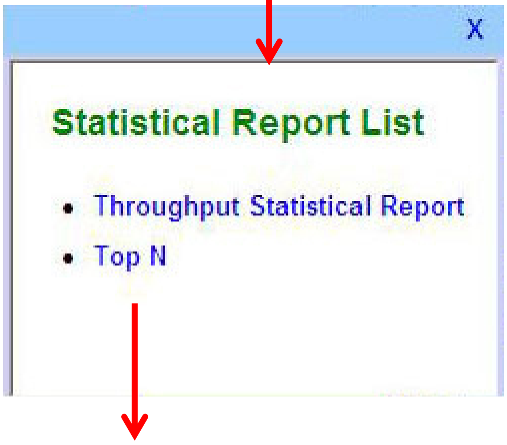
Total 9,492 Total Page 475 Current Page 1

Example 3:

Click on the Daily Traffic – Summary Report, it will pop out Statistical Report List window and you can select to click Throughput Statistical Report or Top N report. Click on the Top N, it will display the User Daily Traffic Top N by Listing the top user IP with information such as Who is?, Throughput (KB) and Statistical Report which includes Protocol Daily, Weekly and Summary Report.

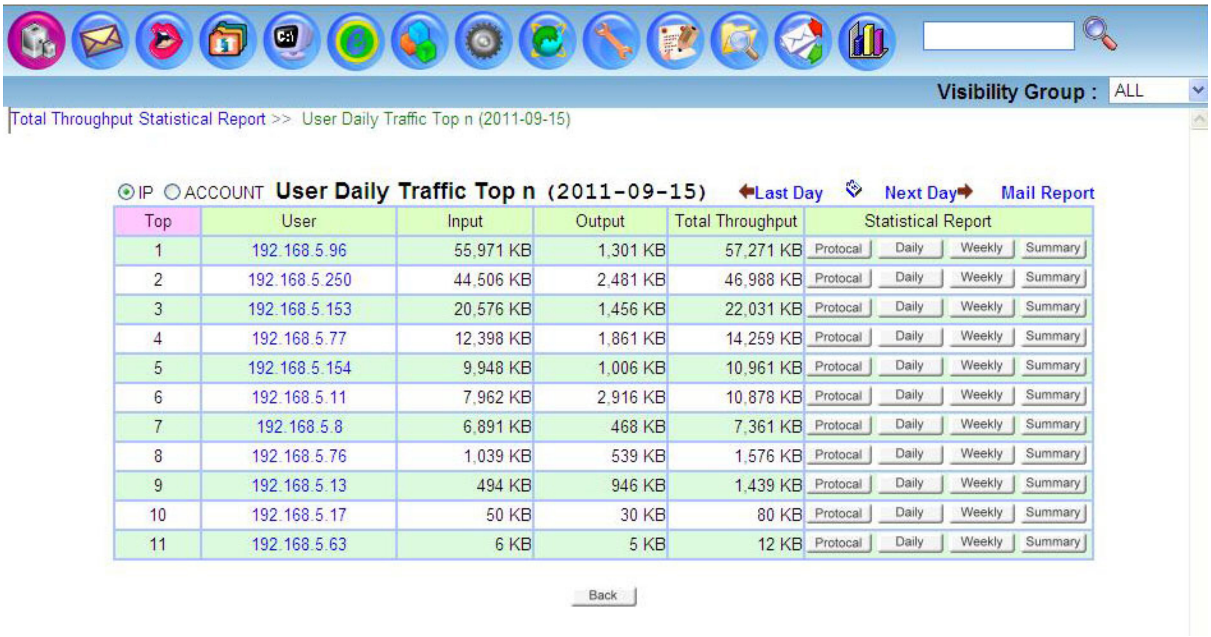


Service Category	Daily Traffic 2011-09-15			Weekly Traffic 2011-09-11 ~ 2011-09-17			Month Traffic 2011-09		
	Quantity	Throughput	Report	Quantity	Throughput	Report	Quantity	Throughput	Report



Statistical Report List

- Throughput Statistical Report
- Top N



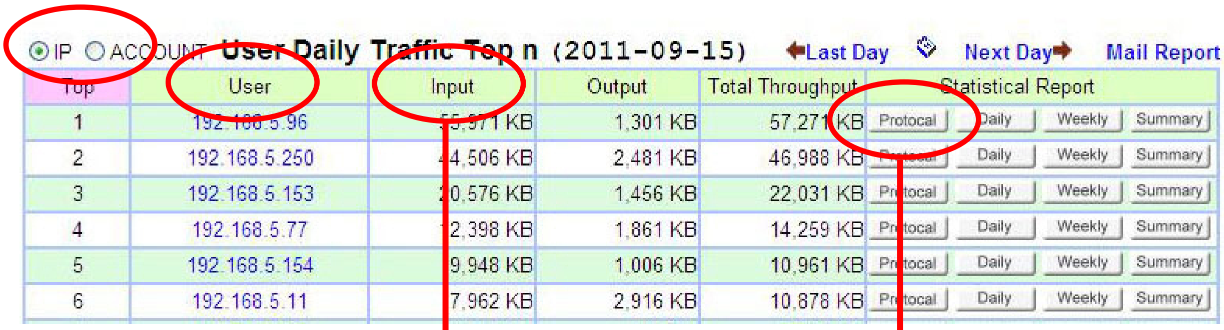
Visibility Group : ALL

Total Throughput Statistical Report >> User Daily Traffic Top n (2011-09-15)

● IP ○ ACCOUNT **User Daily Traffic Top n (2011-09-15)** Last Day Next Day Mail Report

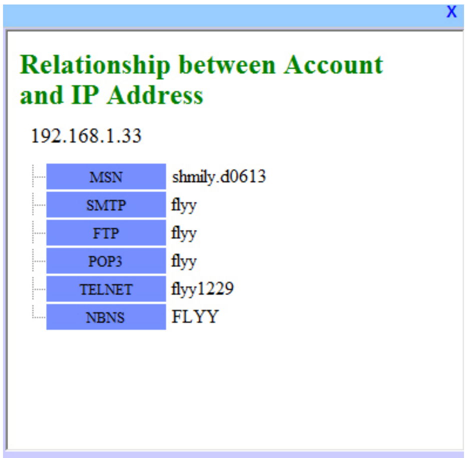
Top	User	Input	Output	Total Throughput	Statistical Report			
1	192.168.5.96	55,971 KB	1,301 KB	57,271 KB	Protocal	Daily	Weekly	Summary
2	192.168.5.250	44,506 KB	2,481 KB	46,988 KB	Protocal	Daily	Weekly	Summary
3	192.168.5.153	20,576 KB	1,456 KB	22,031 KB	Protocal	Daily	Weekly	Summary
4	192.168.5.77	12,398 KB	1,861 KB	14,259 KB	Protocal	Daily	Weekly	Summary
5	192.168.5.154	9,948 KB	1,006 KB	10,961 KB	Protocal	Daily	Weekly	Summary
6	192.168.5.11	7,962 KB	2,916 KB	10,878 KB	Protocal	Daily	Weekly	Summary
7	192.168.5.8	6,891 KB	468 KB	7,361 KB	Protocal	Daily	Weekly	Summary
8	192.168.5.76	1,039 KB	539 KB	1,576 KB	Protocal	Daily	Weekly	Summary
9	192.168.5.13	494 KB	946 KB	1,439 KB	Protocal	Daily	Weekly	Summary
10	192.168.5.17	50 KB	30 KB	80 KB	Protocal	Daily	Weekly	Summary
11	192.168.5.63	6 KB	5 KB	12 KB	Protocal	Daily	Weekly	Summary

Click on Who is ? This will display the user (IP) relationship with username, user login etc. Click on Protocol, it will display all applications and throughput (KB) used by this user (IP).



● IP ○ ACCOUNT **User Daily Traffic Top n (2011-09-15)** Last Day Next Day Mail Report

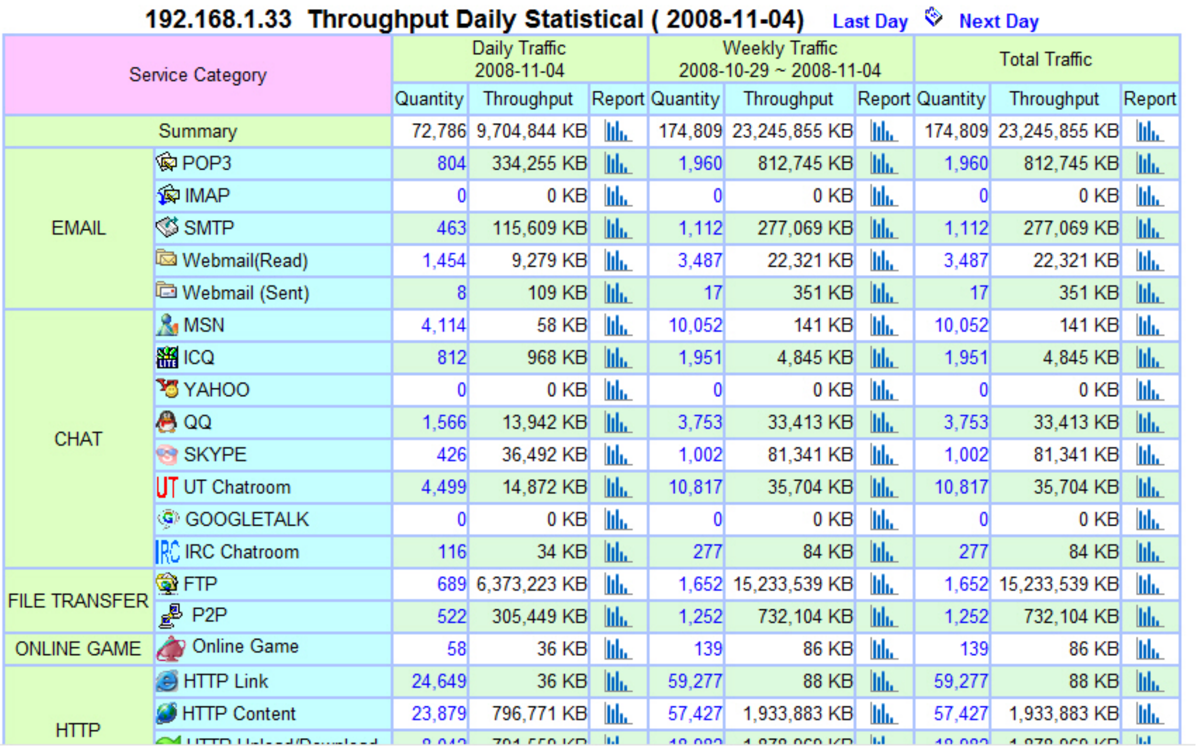
Top	User	Input	Output	Total Throughput	Statistical Report			
1	192.168.5.96	55,971 KB	1,301 KB	57,271 KB	Protocal	Daily	Weekly	Summary
2	192.168.5.250	44,506 KB	2,481 KB	46,988 KB	Protocal	Daily	Weekly	Summary
3	192.168.5.153	20,576 KB	1,456 KB	22,031 KB	Protocal	Daily	Weekly	Summary
4	192.168.5.77	12,398 KB	1,861 KB	14,259 KB	Protocal	Daily	Weekly	Summary
5	192.168.5.154	9,948 KB	1,006 KB	10,961 KB	Protocal	Daily	Weekly	Summary
6	192.168.5.11	7,962 KB	2,916 KB	10,878 KB	Protocal	Daily	Weekly	Summary



Relationship between Account and IP Address

192.168.1.33

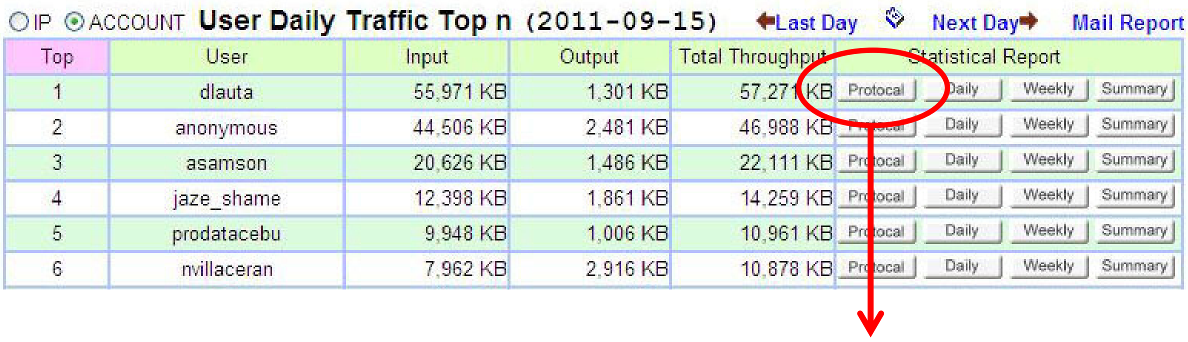
MSN	shmily.d0613
SMTP	flyy
FTP	flyy
POP3	flyy
TELNET	flyy1229
NBNS	FLYY



192.168.1.33 Throughput Daily Statistical (2008-11-04) Last Day Next Day

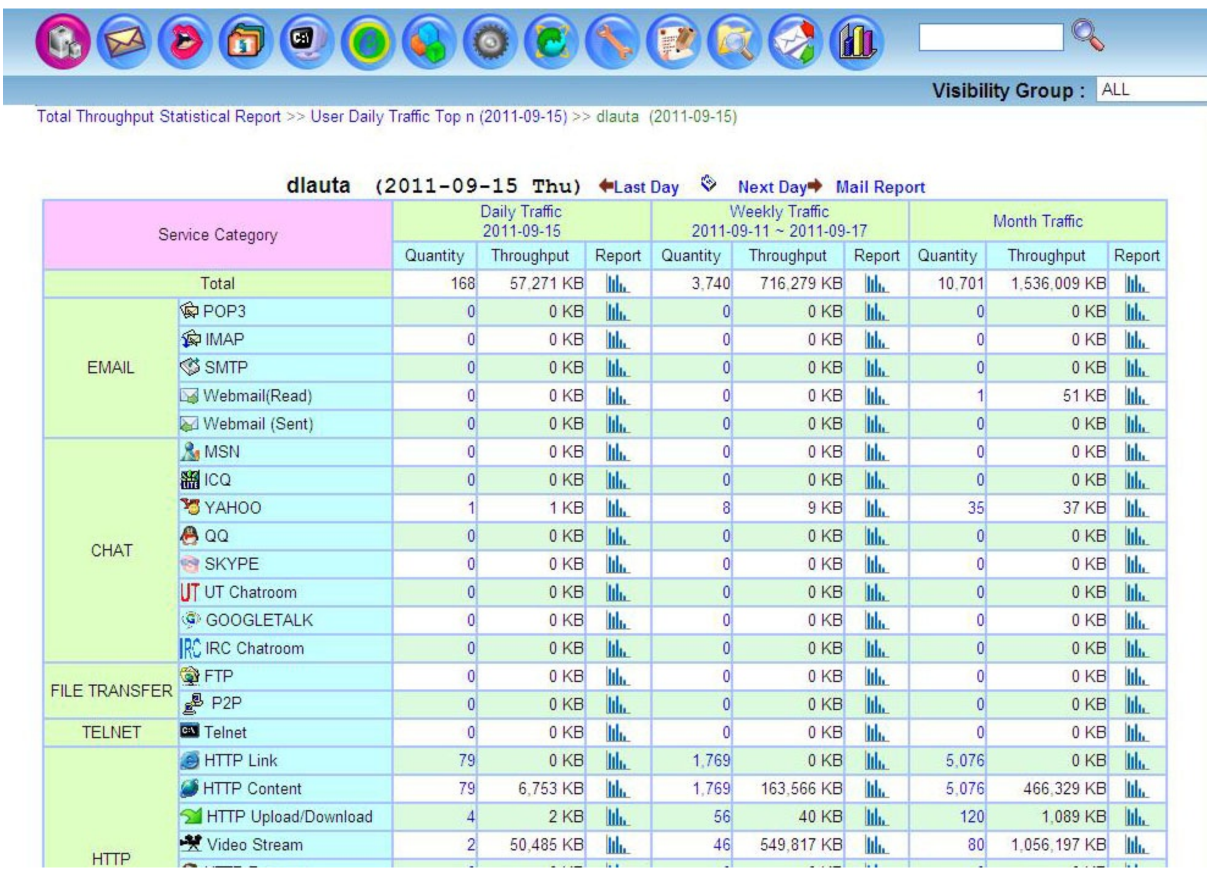
Service Category		Daily Traffic 2008-11-04			Weekly Traffic 2008-10-29 ~ 2008-11-04			Total Traffic		
		Quantity	Throughput	Report	Quantity	Throughput	Report	Quantity	Throughput	Report
Summary		72,786	9,704,844 KB	📊	174,809	23,245,855 KB	📊	174,809	23,245,855 KB	📊
EMAIL	POP3	804	334,255 KB	📊	1,960	812,745 KB	📊	1,960	812,745 KB	📊
	IMAP	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	SMTP	463	115,609 KB	📊	1,112	277,069 KB	📊	1,112	277,069 KB	📊
	Webmail(Read)	1,454	9,279 KB	📊	3,487	22,321 KB	📊	3,487	22,321 KB	📊
	Webmail (Sent)	8	109 KB	📊	17	351 KB	📊	17	351 KB	📊
CHAT	MSN	4,114	58 KB	📊	10,052	141 KB	📊	10,052	141 KB	📊
	ICQ	812	968 KB	📊	1,951	4,845 KB	📊	1,951	4,845 KB	📊
	YAHOO	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	QQ	1,566	13,942 KB	📊	3,753	33,413 KB	📊	3,753	33,413 KB	📊
	SKYPE	426	36,492 KB	📊	1,002	81,341 KB	📊	1,002	81,341 KB	📊
	UT Chatroom	4,499	14,872 KB	📊	10,817	35,704 KB	📊	10,817	35,704 KB	📊
	GOOGLETALK	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	IRC Chatroom	116	34 KB	📊	277	84 KB	📊	277	84 KB	📊
FILE TRANSFER	FTP	689	6,373,223 KB	📊	1,652	15,233,539 KB	📊	1,652	15,233,539 KB	📊
	P2P	522	305,449 KB	📊	1,252	732,104 KB	📊	1,252	732,104 KB	📊
ONLINE GAME	Online Game	58	36 KB	📊	139	86 KB	📊	139	86 KB	📊
HTTP	HTTP Link	24,649	36 KB	📊	59,277	88 KB	📊	59,277	88 KB	📊
	HTTP Content	23,879	796,771 KB	📊	57,427	1,933,883 KB	📊	57,427	1,933,883 KB	📊
	HTTP Upload/Download	8,043	791,550 KB	📊	18,083	1,878,960 KB	📊	18,083	1,878,960 KB	📊

Besides generating report by IP, Administrator can also generate report by Account basis.



○IP ◉ACCOUNT **User Daily Traffic Top n (2011-09-15)** Last Day Next Day Mail Report

Top	User	Input	Output	Total Throughput	Statistical Report			
1	dlauta	55,971 KB	1,301 KB	57,271 KB	Protocal	Daily	Weekly	Summary
2	anonymous	44,506 KB	2,481 KB	46,988 KB	Protocal	Daily	Weekly	Summary
3	asamson	20,626 KB	1,486 KB	22,111 KB	Protocal	Daily	Weekly	Summary
4	jaze_shame	12,398 KB	1,861 KB	14,259 KB	Protocal	Daily	Weekly	Summary
5	prodatacebu	9,948 KB	1,006 KB	10,961 KB	Protocal	Daily	Weekly	Summary
6	nvillaceran	7,962 KB	2,916 KB	10,878 KB	Protocal	Daily	Weekly	Summary



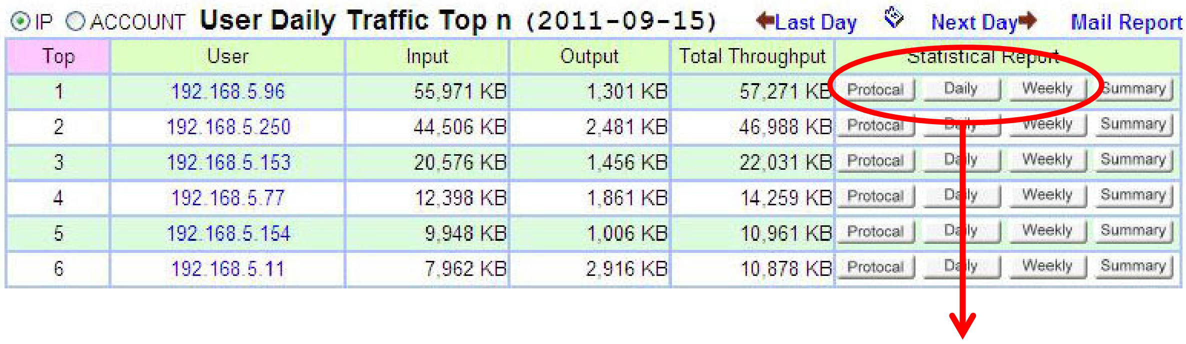
Visibility Group : ALL

Total Throughput Statistical Report >> User Daily Traffic Top n (2011-09-15) >> dlauta (2011-09-15)

dlauta (2011-09-15 Thu) Last Day Next Day Mail Report

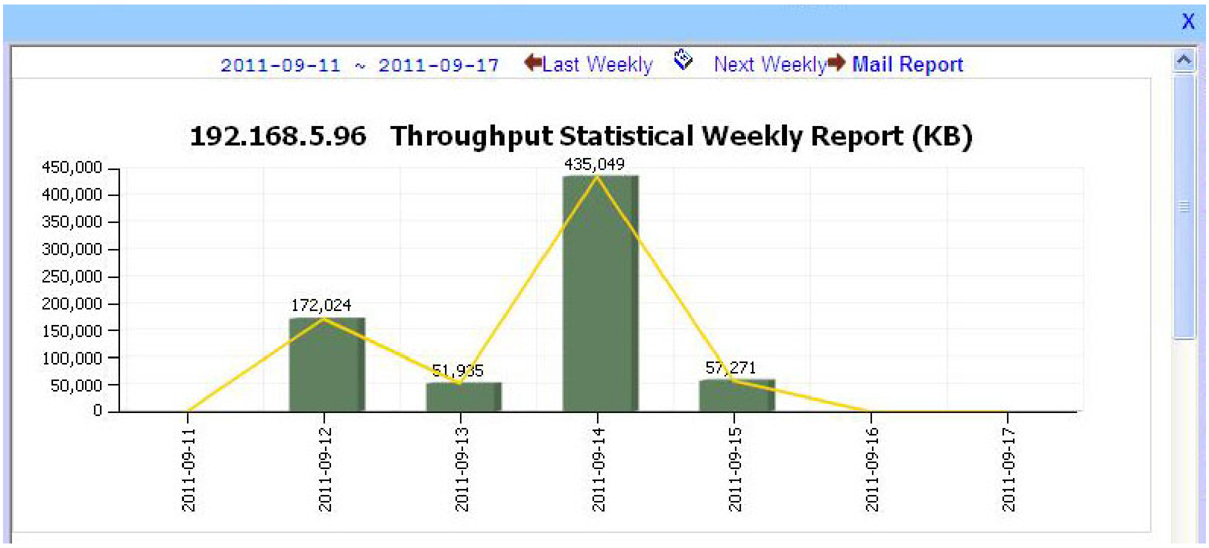
Service Category		Daily Traffic 2011-09-15			Weekly Traffic 2011-09-11 ~ 2011-09-17			Month Traffic		
		Quantity	Throughput	Report	Quantity	Throughput	Report	Quantity	Throughput	Report
Total		168	57,271 KB	📊	3,740	716,279 KB	📊	10,701	1,536,009 KB	📊
EMAIL	POP3	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	IMAP	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	SMTP	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	Webmail(Read)	0	0 KB	📊	0	0 KB	📊	1	51 KB	📊
	Webmail (Sent)	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
CHAT	MSN	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	ICQ	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	YAHOO	1	1 KB	📊	8	9 KB	📊	35	37 KB	📊
	QQ	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	SKYPE	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	UT Chatroom	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	GOOGLETALK	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	IRC Chatroom	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
FILE TRANSFER	FTP	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
	P2P	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
TELNET	Telnet	0	0 KB	📊	0	0 KB	📊	0	0 KB	📊
HTTP	HTTP Link	79	0 KB	📊	1,769	0 KB	📊	5,076	0 KB	📊
	HTTP Content	79	6,753 KB	📊	1,769	163,566 KB	📊	5,076	466,329 KB	📊
	HTTP Upload/Download	4	2 KB	📊	56	40 KB	📊	120	1,089 KB	📊
	Video Stream	2	50,485 KB	📊	46	549,817 KB	📊	80	1,056,197 KB	📊

Click on the Daily, Weekly or Summary Statistical Report of the particular user (IP), it will pop out a window display statistical on bar chart.



● IP ○ ACCOUNT **User Daily Traffic Top n** (2011-09-15) Last Day Next Day Mail Report

Top	User	Input	Output	Total Throughput	Statistical Report
1	192.168.5.96	55,971 KB	1,301 KB	57,271 KB	Protocal Daily Weekly Summary
2	192.168.5.250	44,506 KB	2,481 KB	46,988 KB	Protocal Daily Weekly Summary
3	192.168.5.153	20,576 KB	1,456 KB	22,031 KB	Protocal Daily Weekly Summary
4	192.168.5.77	12,398 KB	1,861 KB	14,259 KB	Protocal Daily Weekly Summary
5	192.168.5.154	9,948 KB	1,006 KB	10,961 KB	Protocal Daily Weekly Summary
6	192.168.5.11	7,962 KB	2,916 KB	10,878 KB	Protocal Daily Weekly Summary



2011-09-11 ~ 2011-09-17 Last Weekly Next Weekly Mail Report

Internet Content Reconstruction

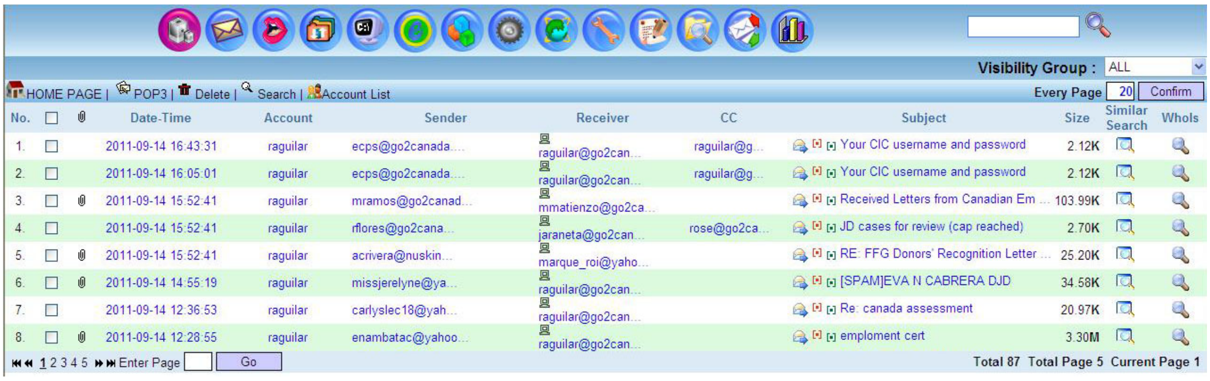
Email

ICI system captures and reconstructs Email content back to its original content view format. Various Email protocol types supported are as follow:

1. POP3 (Incoming)
2. IMAP (Incoming)
3. SMTP (Outgoing)
4. Webmail (Read)
5. Webmail (Sent)

POP3

Post Office Protocol 3 or POP3 (Incoming) Email obtainable information includes Date-Time, Account (with IP/MAC), Sender, Receiver, CC, Subject with Email content (with attachment if any) and Size.



Visibility Group : ALL

HOME PAGE | POP3 | Delete | Search | Account List

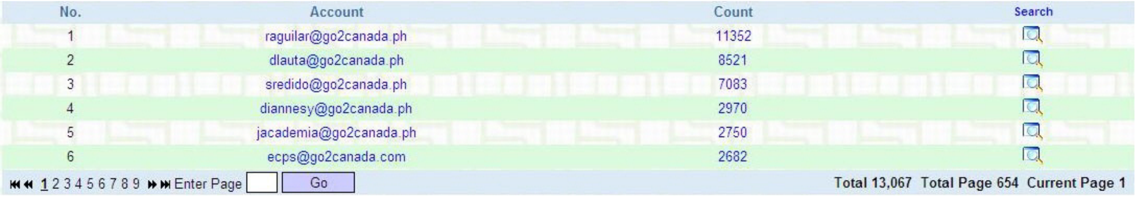
Every Page 20 Confirm

No.	☐	📎	Date-Time	Account	Sender	Receiver	CC	Subject	Size	Similar Search	WhoIs
1.	☐		2011-09-14 16:43:31	raguilar	ecps@go2canada....	raguilar@go2can...	raguilar@g...	Your CIC username and password	2.12K	🔍	🔍
2.	☐		2011-09-14 16:05:01	raguilar	ecps@go2canada....	raguilar@go2can...	raguilar@g...	Your CIC username and password	2.12K	🔍	🔍
3.	☐	📎	2011-09-14 15:52:41	raguilar	mramos@go2canad...	mmatienzo@go2ca...		Received Letters from Canadian Em ...	103.99K	🔍	🔍
4.	☐		2011-09-14 15:52:41	raguilar	rflores@go2cana...	jaraneta@go2can...	rose@go2ca...	JD cases for review (cap reached)	2.70K	🔍	🔍
5.	☐	📎	2011-09-14 15:52:41	raguilar	acrivera@nuskin...	marque_roi@yaho...		RE: FFG Donors' Recognition Letter ...	25.20K	🔍	🔍
6.	☐	📎	2011-09-14 14:55:19	raguilar	missjerelyne@ya...	raguilar@go2can...		[SPAM]EVA N CABRERA DJD	34.58K	🔍	🔍
7.	☐		2011-09-14 12:36:53	raguilar	carlyslec18@yah...	raguilar@go2can...		Re: canada assessment	20.97K	🔍	🔍
8.	☐	📎	2011-09-14 12:28:55	raguilar	enambatac@yahoo...	raguilar@go2can...		emploment cert	3.30M	🔍	🔍

⏮ ⏪ 1 2 3 4 5 ⏩ ⏭ Enter Page Go Total 87 Total Page 5 Current Page 1

Features in this POP3 GUI:

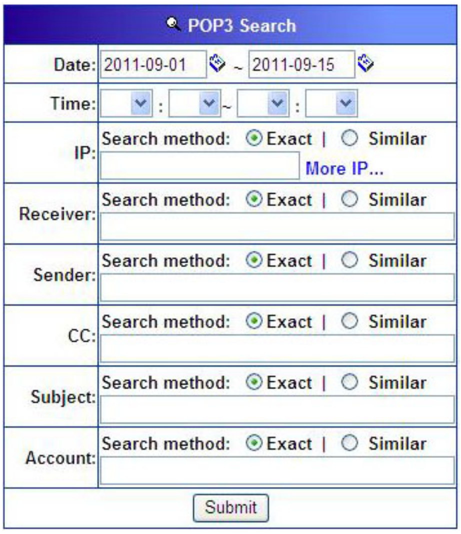
- POP3: Refresh the page content.
- Delete: Delete the Email (that has been checked or ticked).
- Account List: This section shows all the Email Account List.



No.	Account	Count	Search
1	raguilar@go2canada.ph	11352	🔍
2	dlauta@go2canada.ph	8521	🔍
3	sredido@go2canada.ph	7083	🔍
4	diannesy@go2canada.ph	2970	🔍
5	jacademia@go2canada.ph	2750	🔍
6	ecps@go2canada.com	2682	🔍

⏮ ⏪ 1 2 3 4 5 6 7 8 9 ⏩ ⏭ Enter Page Go Total 13,067 Total Page 654 Current Page 1

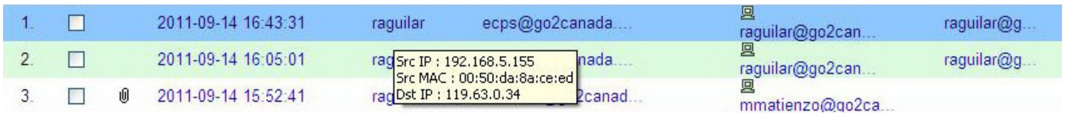
- Search: Search for Email based on the specified parameters such as Date, Time, IP, Receiver, Sender, CC, Subject and Account.



POP3 Search

Date:	2011-09-01 ~ 2011-09-15
Time:	: ~ :
IP:	Search method: ● Exact | ○ Similar More IP...
Receiver:	Search method: ● Exact | ○ Similar
Sender:	Search method: ● Exact | ○ Similar
CC:	Search method: ● Exact | ○ Similar
Subject:	Search method: ● Exact | ○ Similar
Account:	Search method: ● Exact | ○ Similar

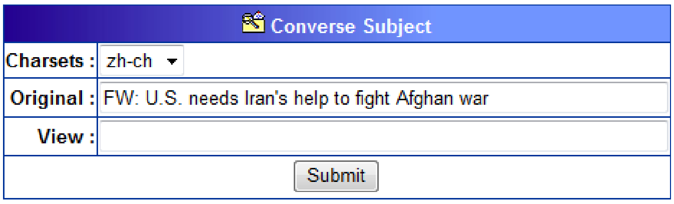
- Source, Destination IP Address and MAC Address by pointing the mouse to the account column.



1.	□		2011-09-14 16:43:31	raguilar	ecps@go2canada....	raguilar@go2can...	raguilar@g...
2.	□		2011-09-14 16:05:01	rag	nada....	raguilar@go2can...	raguilar@g...
3.	□		2011-09-14 15:52:41	rag	2canad...	mmatienzo@go2ca...	

Src IP : 192.168.5.155
Src MAC : 00:50:da:8a:ce:ed
Dst IP : 119.63.0.34

- Every Page 5 Confirm Display the number of record per page
- □ Checkbox: Check or tick the checkbox for deleting
- Attachment: This symbol shows there is attachment in the Email
- Shows the IP address
- Forward Email: Forward the Email to a specific Email account
- [•] Source Code: Shows the Email source and path.
- [•] Convertor: Convert the subject name to another language to be readable. This convertor coverts the character in different coding formats such as zh-ch (Chinese), zh-sg (Singapore), zh-tw (Taiwan), en (English), utf-8, JP (Japanese).

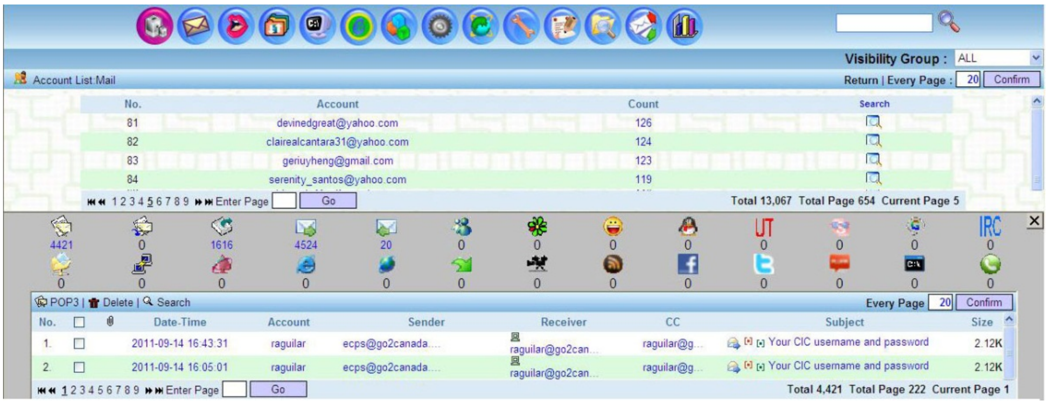


Converse Subject

Charsets :	zh-ch
Original :	FW: U.S. needs Iran's help to fight Afghan war
View :	

- Subject: Click on Email subject to view the content of the Email.

- Similar Search: Search for Email with similar content



Visibility Group : ALL

Account List:Mail

Return | Every Page : 20 Confirm

No.	Account	Count	Search
81	devinedgreat@yahoo.com	126	
82	clairealcantara31@yahoo.com	124	
83	geriuyheng@gmail.com	123	
84	serenity_santos@yahoo.com	119	

⏮ ⏪ 1 2 3 4 5 6 7 8 9 ⏩ ⏭ Enter Page Go Total 13,067 Total Page 654 Current Page 5

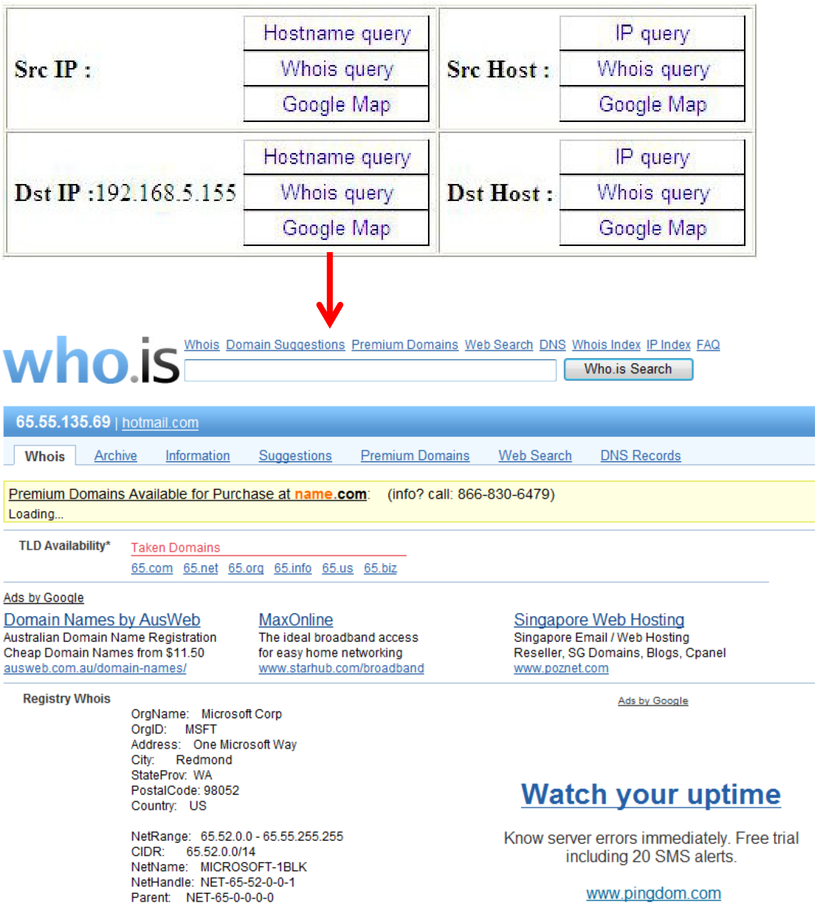
4421	0	1616	4524	20	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0

POP3 | Delete | Search Every Page 20 Confirm

No.	□		Date-Time	Account	Sender	Receiver	CC	Subject	Size
1.	□		2011-09-14 16:43:31	raguilar	ecps@go2canada....	raguilar@go2can...	raguilar@g...	Your CIC username and password	2.12K
2.	□		2011-09-14 16:05:01	raguilar	ecps@go2canada....	raguilar@go2can...	raguilar@g...	Your CIC username and password	2.12K

⏮ ⏪ 1 2 3 4 5 6 7 8 9 ⏩ ⏭ Enter Page Go Total 4,421 Total Page 222 Current Page 1

- Whois: Provide information of Source and Destination IP and Hostname. It allows you to search for the IP Address information through the Internet.



Src IP :	Hostname query Whois query Google Map	Src Host :	IP query Whois query Google Map
Dst IP :192.168.5.155	Hostname query Whois query Google Map	Dst Host :	IP query Whois query Google Map

who.is Whois Domain Suggestions Premium Domains Web Search DNS Whois Index IP Index FAQ

Who.is Search

65.55.135.69 | hotmail.com

Whois Archive Information Suggestions Premium Domains Web Search DNS Records

Premium Domains Available for Purchase at name.com: (info? call: 866-830-6479)
Loading...

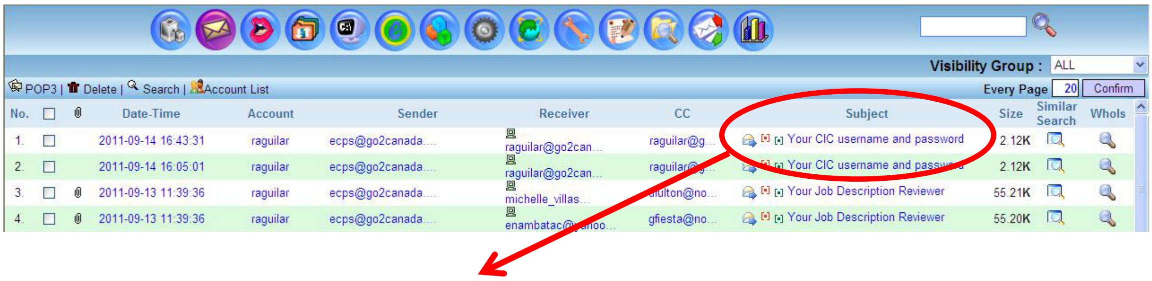
TLD Availability* Taken Domains
65.com 65.net 65.org 65.info 65.us 65.biz

Registry Whois

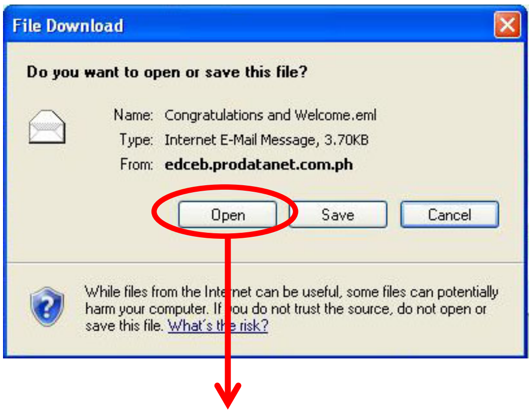
```
OrgName:   Microsoft Corp
OrgID:     MSFT
Address:   One Microsoft Way
City:      Redmond
StateProv: WA
PostalCode: 98052
Country:   US

NetRange:  65.52.0.0 - 65.55.255.255
CIDR:      65.52.0.0/14
NetName:   MICROSOFT-1BLK
NetHandle: NET-65-52-0-0-1
Parent:    NET-65-0-0-0-0
```

View Email Content

Click on the Email subject and Administrator can choose to open and view the Email content or save it into the hard drive of the Administrator PC.



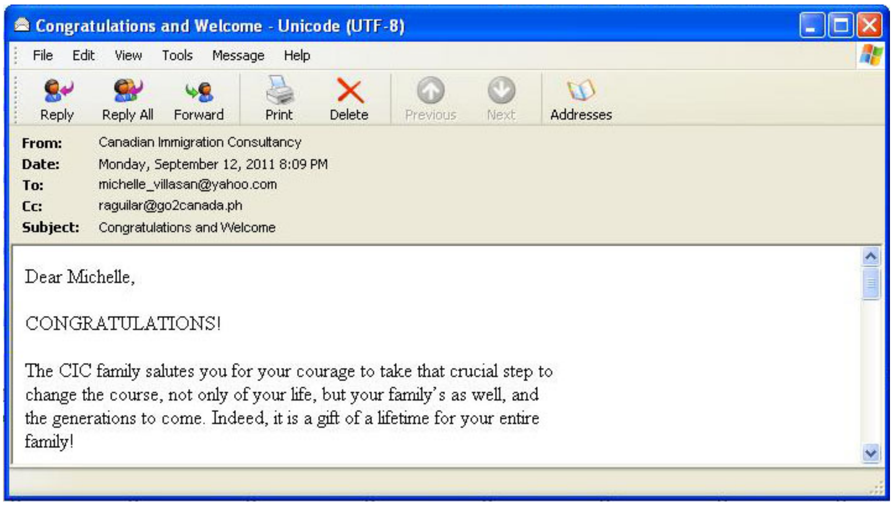
No.	□	📎	Date-Time	Account	Sender	Receiver	CC	Subject	Size	Similar Search	WhoIs
1.	□		2011-09-14 16:43:31	raguilar	ecps@go2canada....	raguilar@go2can...	raguilar@g...	Your CIC username and password	2.12K		
2.	□		2011-09-14 16:05:01	raguilar	ecps@go2canada....	raguilar@go2can...	raguilar@g...	Your CIC username and password	2.12K		
3.	□	📎	2011-09-13 11:39:36	raguilar	ecps@go2canada....	michelle_villas...	ulton@no...	Your Job Description Reviewer	55.21K		
4.	□	📎	2011-09-13 11:39:36	raguilar	ecps@go2canada....	enambatac@yahoo...	gfiesta@no...	Your Job Description Reviewer	55.20K		



Do you want to open or save this file?

Name: Congratulations and Welcome.eml
Type: Internet E-Mail Message, 3.70KB
From: **edceb.prodatanet.com.ph**

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?



From: Canadian Immigration Consultancy
Date: Monday, September 12, 2011 8:09 PM
To: michelle_villasan@yahoo.com
Cc: raguilar@go2canada.ph
Subject: Congratulations and Welcome

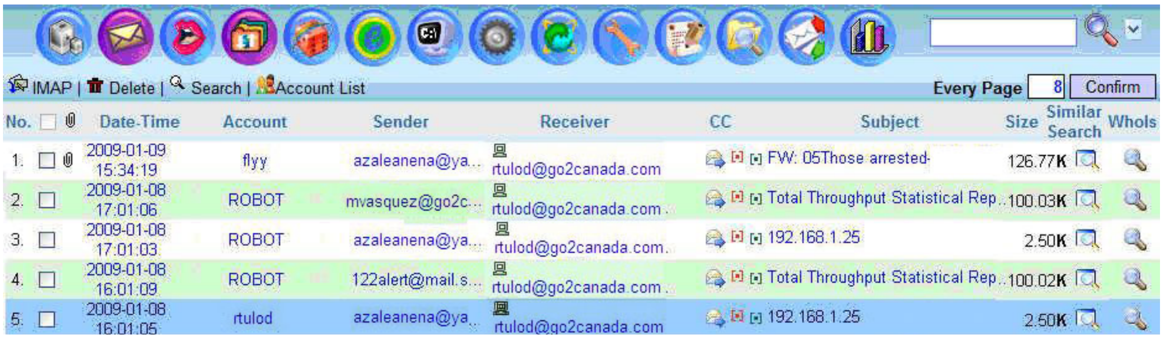
Dear Michelle,

CONGRATULATIONS!

The CIC family salutes you for your courage to take that crucial step to change the course, not only of your life, but your family's as well, and the generations to come. Indeed, it is a gift of a lifetime for your entire family!

IMAP

Internet Message Protocol (IMAP) obtainable information includes Date-Time, Account (with IP/MAC), Sender, Receiver, CC, Subject with Email content (with attachment if any) and Size.

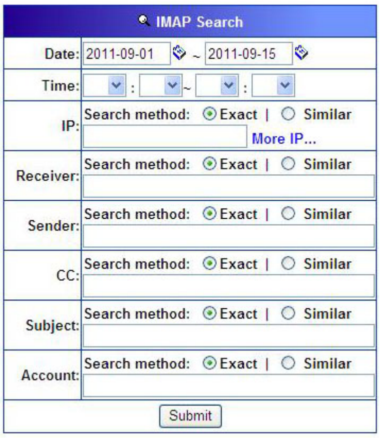


IMAP | Delete | Search | Account List   Every Page 8 Confirm

No.	□	Date-Time	Account	Sender	Receiver	CC	Subject	Size	Similar Search	WhoIs
1.	□	2009-01-09 15:34:19	flyy	azaleanena@ya...	rtulod@go2canada.com		[•] [•] FW: 05Those arrested-	126.77K		
2.	□	2009-01-08 17:01:06	ROBOT	mvasquez@go2c...	rtulod@go2canada.com .		[•] [•] Total Throughput Statistical Rep..	100.03K		
3.	□	2009-01-08 17:01:03	ROBOT	azaleanena@ya...	rtulod@go2canada.com.		[•] [•] 192.168.1.25	2.50K		
4.	□	2009-01-08 16:01:09	ROBOT	122alert@mail.s...	rtulod@go2canada.com .		[•] [•] Total Throughput Statistical Rep..	100.02K		
5.	□	2009-01-08 16:01:05	rtulod	azaleanena@ya..	rtulod@go2canada.com		[•] [•] 192.168.1.25	2.50K		

Features in this IMAP GUI:

- IMAP: Refresh the page content.
- Delete: Delete the Email (that has been checked or ticked).
- Account List: This section shows all the Email Account List. (Refer to 2.1.1)
- Search: Search for Email based on the specified parameters such as Date, Time, IP, Receiver, Sender, CC, Subject and Account.



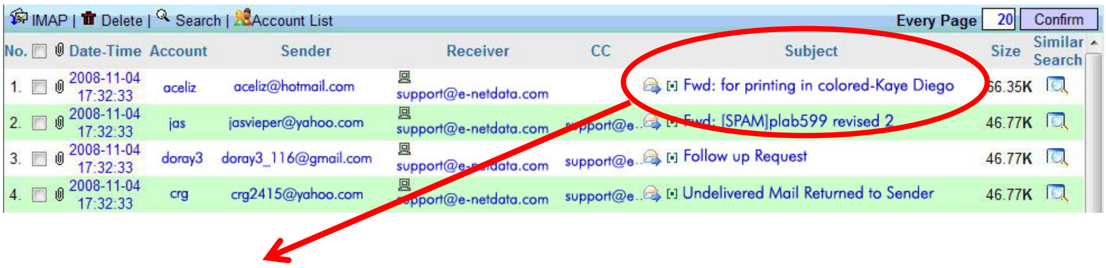
IMAP Search

Date:	2011-09-01 ~ 2011-09-15
Time:	: ~ :
IP:	Search method: ● Exact | ○ Similar More IP...
Receiver:	Search method: ● Exact | ○ Similar
Sender:	Search method: ● Exact | ○ Similar
CC:	Search method: ● Exact | ○ Similar
Subject:	Search method: ● Exact | ○ Similar
Account:	Search method: ● Exact | ○ Similar
	Submit

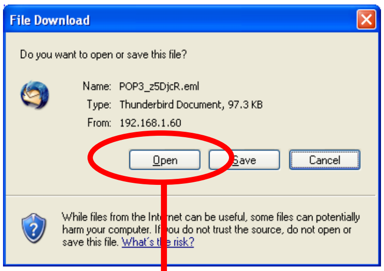
- Source, Destination IP Address and MAC Address by pointing the mouse to the account column
- Every Page 5 Confirm Display the number of record per page
- □ Checkbox: Check or tick the checkbox for deleting
- Attachment: This symbol shows there is attachment in the Email
- Shows the IP address
- Forward Email: Forward the Email to a specific Email account
- [•] Source Code: Shows the Email source and path.
- [•] Convertor: Convert the subject name to another language to be readable. This convertor coverts the character in different coding formats such as zh-ch (Chinese), zh-sg (Singapore), zh-tw (Taiwan), en (English), utf-8, JP (Japanese).
- Subject: Click on Email subject to view the content of the Email.
- Similar Search: Search for Email with similar content
- Whois: Provide information of Source and Destination IP and Hostname. It allows you to search for the IP Address information through the Internet.

View Email Content

Click on the Email subject and Administrator can choose to open and view the Email content or save it into the hard drive of the accessing PC.



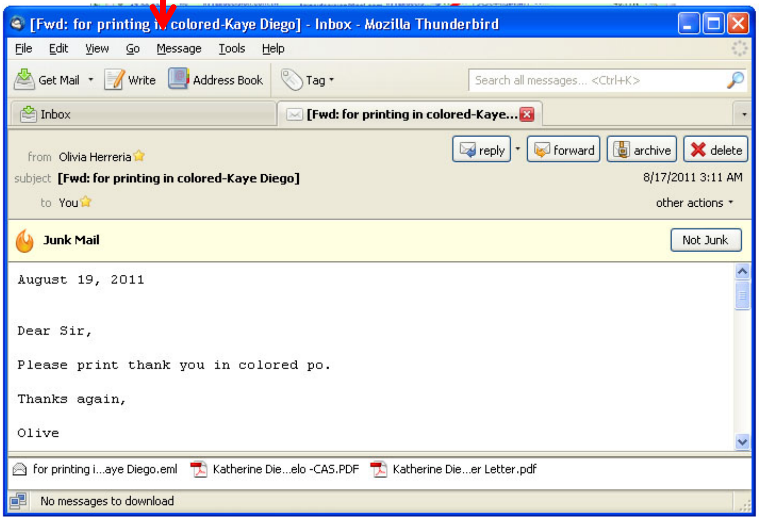
No.	Date-Time	Account	Sender	Receiver	CC	Subject	Size	Similar Search
1.	2008-11-04 17:32:33	aceliz	aceliz@hotmail.com	support@e-netdata.com		Fwd: for printing in colored-Kaye Diego	56.35K	
2.	2008-11-04 17:32:33	jas	jasvieper@yahoo.com	support@e-netdata.com	support@e..	Fwd: [SPAM]plab599 revised 2	46.77K	
3.	2008-11-04 17:32:33	doray3	doray3_116@gmail.com	support@e-netdata.com	support@e..	Follow up Request	46.77K	
4.	2008-11-04 17:32:33	crg	crg2415@yahoo.com	support@e-netdata.com	support@e..	Undelivered Mail Returned to Sender	46.77K	



Do you want to open or save this file?

Name: POP3_z5DjcR.eml
Type: Thunderbird Document, 97.3 KB
From: 192.168.1.60

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?


[Fwd: for printing in colored-Kaye Diego] - Inbox - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Address Book
Tag
Search all messages... <Ctrl+K>
Inbox
[Fwd: for printing in colored-Kaye...
reply
forward
archive
delete
other actions
Junk Mail
Not Junk

from Olivia Herreria
subject [Fwd: for printing in colored-Kaye Diego]
to You
8/17/2011 3:11 AM

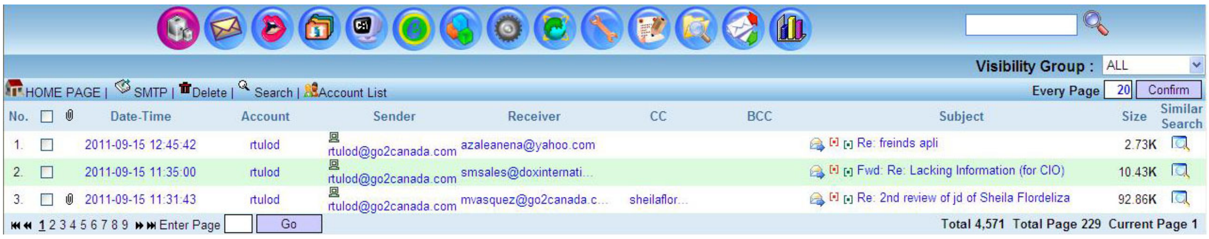
```
August 19, 2011


Dear Sir,

Please print thank you in colored po.

Thanks again,

Olive
```

for printing i...aye Diego.eml   Katherine Die...elo -CA5.PDF   Katherine Die...er Letter.pdf

No messages to download

SMTP (Outgoing)

Simple Mail Transfer Protocol or SMTP (Outgoing) obtainable information includes Date-Time, Account (with IP/MAC), Sender, Receiver, CC, BCC, Subject with Email content (with attachment if any) and Size.

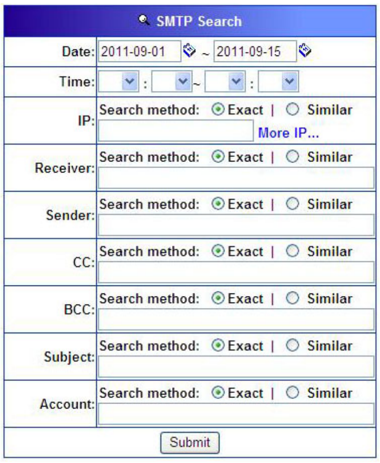


No.	□	Date-Time	Account	Sender	Receiver	CC	BCC	Subject	Size	Similar Search
1.	□	2011-09-15 12:45:42	rtulod	rtulod@go2canada.com	azaleanena@yahoo.com			[•] [•] Re: freinds apli	2.73K	
2.	□	2011-09-15 11:35:00	rtulod	rtulod@go2canada.com	smsales@doxinternati...			[•] [•] Fwd: Re: Lacking Information (for CIO)	10.43K	
3.	□	2011-09-15 11:31:43	rtulod	rtulod@go2canada.com	mvasquez@go2canada.c...	sheilaflor...		[•] [•] Re: 2nd review of jd of Sheila Flordeliza	92.86K	

1 2 3 4 5 6 7 8 9 Enter Page Go
Total 4,571 Total Page 229 Current Page 1

Features in this SMTP GUI:

- SMTP: Refresh the page content.
- Delete: Delete the Email (that has been checked or ticked).
- Account List: This section shows all the Email Account List. (Refer to 2.1.1)
- Search: Search for Email based on the specified parameters such as Date, Time, IP, Receiver, Sender, CC, Subject and Account.



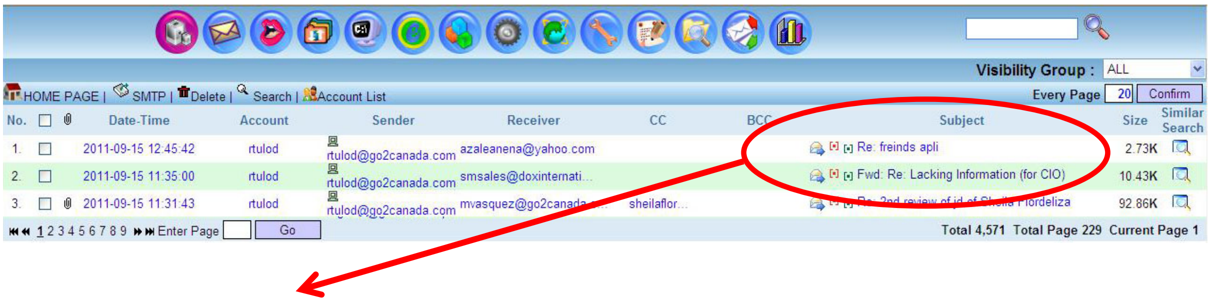
SMTP Search

Date:	2011-09-01 ~ 2011-09-15
Time:	: ~ :
IP:	Search method: ● Exact | ○ Similar More IP...
Receiver:	Search method: ● Exact | ○ Similar
Sender:	Search method: ● Exact | ○ Similar
CC:	Search method: ● Exact | ○ Similar
BCC:	Search method: ● Exact | ○ Similar
Subject:	Search method: ● Exact | ○ Similar
Account:	Search method: ● Exact | ○ Similar

- Source, Destination IP Address and MAC Address by pointing the mouse to the account column
- Every Page 5 Confirm Display the number of record per page
- □ Checkbox: Check or tick the checkbox for deleting
- Attachment: This symbol shows there is attachment in the Email
- Shows the IP address
- Forward Email: Forward the Email to a specific Email account
- [•] Source Code: Shows the Email source and path.
- [•] Convertor: Convert the subject name to another language to be readable. This convertor coverts the character in different coding formats such as zh-ch (Chinese), zh-sg (Singapore), zh-tw (Taiwan), en (English), utf-8, JP (Japanese).
- Subject: Click on Email subject to view the content of the Email.
- Similar Search: Search for Email with similar content
- Whois: Provide information of Source and Destination IP and Hostname. It allows you to search for the IP Address information through the Internet.

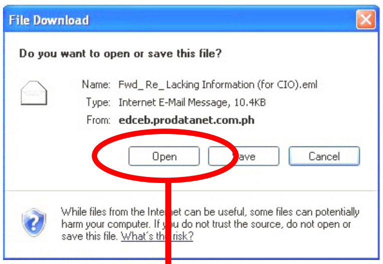
View Email Content

Click on the Email [Subject] link and you can choose to open and view the Email content or save it into the hard drive of your PC.



No.	□		Date-Time	Account	Sender	Receiver	CC	BCC	Subject	Size	Similar Search
1.	□		2011-09-15 12:45:42	rtulod	rtulod@go2canada.com	azaleanena@yahoo.com			Re: freinds apli	2.73K	
2.	□		2011-09-15 11:35:00	rtulod	rtulod@go2canada.com	smsales@doxinternati...			Fwd: Re: Lacking Information (for CIO)	10.43K	
3.	□		2011-09-15 11:31:43	rtulod	rtulod@go2canada.com	mvasquez@go2canada.c...	sheilaflor...		Re: 2nd review of id of Sheila Flordeliza	92.86K	

1 2 3 4 5 6 7 8 9 Enter Page Go
Total 4,571 Total Page 229 Current Page 1

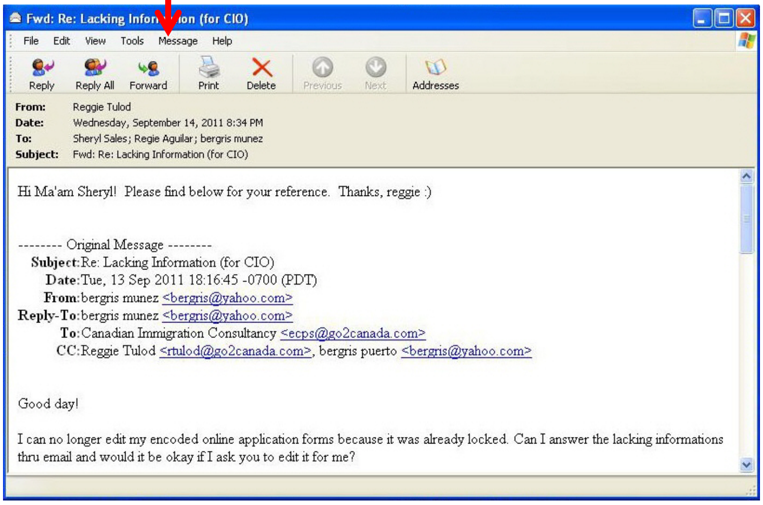


File Download

Do you want to open or save this file?

Name: Fwd_Re_Lacking Information (for CIO).eml
Type: Internet E-Mail Message, 10.4KB
From: edceb.prodatanet.com.ph

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?



Fwd: Re: Lacking Information (for CIO)
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses

From: Reggie Tulod
Date: Wednesday, September 14, 2011 8:34 PM
To: Sheryl Sales; Regie Aguilar; bergris munez
Subject: Fwd: Re: Lacking Information (for CIO)

Hi Ma'am Sheryl! Please find below for your reference. Thanks, reggie :)

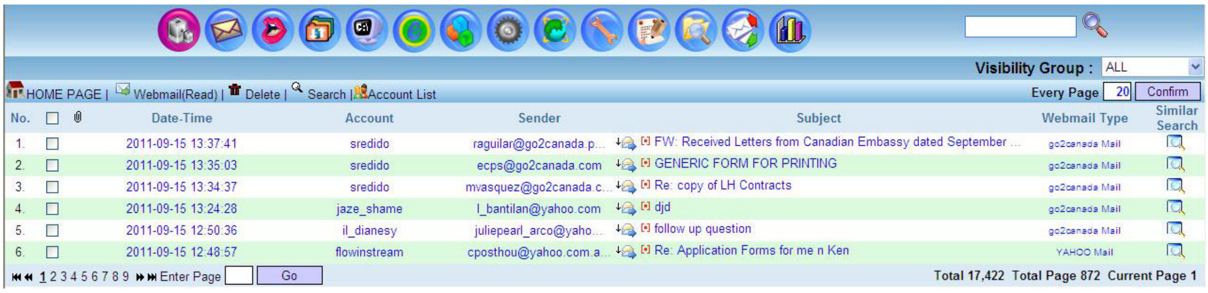
-------- Original Message --------
Subject:Re: Lacking Information (for CIO)
Date:Tue, 13 Sep 2011 18:16:45 -0700 (PDT)
From:bergris munez <bergris@yahoo.com>
Reply-To:bergris munez <bergris@yahoo.com>
To:Canadian Immigration Consultancy <ecps@go2canada.com>
CC:Reggie Tulod <rtulod@go2canada.com>, bergris puerto <bergris@yahoo.com>

Good day!

I can no longer edit my encoded online application forms because it was already locked. Can I answer the lacking informations thru email and would it be okay if I ask you to edit it for me?

Webmail Read

Webmail supported includes Yahoo Mail, Windows Live Hotmail, Gmail etc. Webmail (Read) obtainable information includes Date-Time, Account (with IP/MAC), Sender, Subject (with content) and Webmail Type.



Visibility Group : ALL

HOME PAGE | Webmail(Read) | Delete | Search | Account List

Every Page 20 Confirm

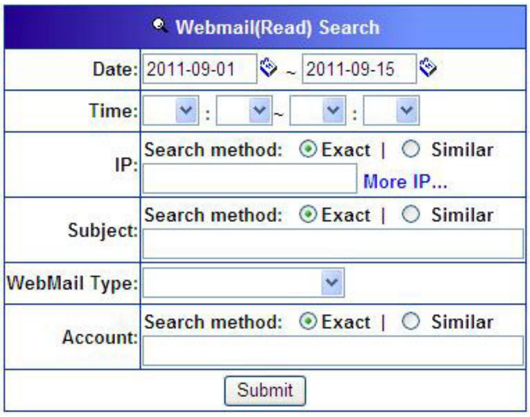
No.	□		Date-Time	Account	Sender	Subject	Webmail Type	Similar Search
1.	□		2011-09-15 13:37:41	sredido	raguilar@go2canada.p...	[•] FW: Received Letters from Canadian Embassy dated September ...	go2canada Mail	
2.	□		2011-09-15 13:35:03	sredido	ecps@go2canada.com	[•] GENERIC FORM FOR PRINTING	go2canada Mail	
3.	□		2011-09-15 13:34:37	sredido	mvasquez@go2canada.c...	[•] Re: copy of LH Contracts	go2canada Mail	
4.	□		2011-09-15 13:24:28	jaze_shame	l_bantilan@yahoo.com	[•] djd	go2canada Mail	
5.	□		2011-09-15 12:50:36	il_dianesy	juliepearl_arco@yaho...	[•] follow up question	go2canada Mail	
6.	□		2011-09-15 12:48:57	flowinstream	cposthou@yahoo.com.a...	[•] Re: Application Forms for me n Ken	YAHOO Mail	

1 2 3 4 5 6 7 8 9 Enter Page Go

Total 17,422 Total Page 872 Current Page 1

Features in this Webmail (Read) GUI:

- Webmail (Read): Refresh the page content.
- Delete: Delete the Email (that has been checked or ticked).
- Account List: This section shows all the Email Account List. (Refer to 2.1.1)
- Search: Search for Webmail based on the specified parameters such as Date, Time, IP, Receiver, Sender, CC, Subject and Account.



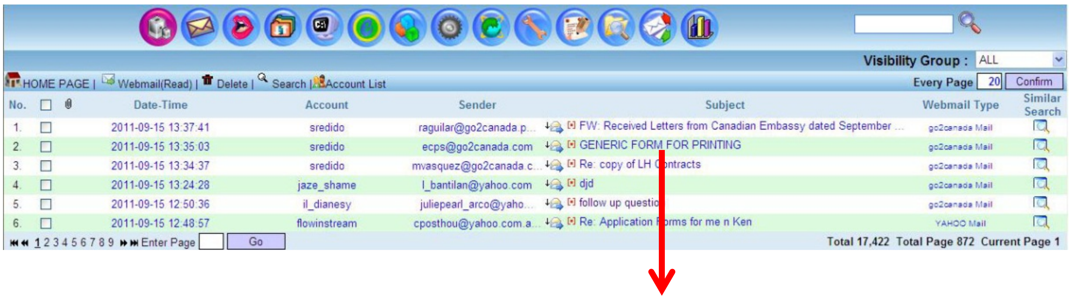
Webmail(Read) Search

Date:	2011-09-01 ~ 2011-09-15
Time:	: ~ :
IP:	Search method: ● Exact | ○ Similar More IP...
Subject:	Search method: ● Exact | ○ Similar
WebMail Type:	
Account:	Search method: ● Exact | ○ Similar
	Submit

- Source, Destination IP Address and MAC Address by pointing the mouse to the account column
- Every Page 5 Confirm Display the number of record per page
- □ Checkbox: Check or tick the checkbox for deleting
- Attachment: This symbol shows there is attachment in the Email
- Shows the IP address
- Forward Email: Forward the Email to a specific Email account
- [•] Source Code: Shows the Email source and path.
- [•] Convertor: Convert the subject name to another language to be readable. This convertor coverts the character in different coding formats such as zh-ch (Chinese), zh-sg (Singapore), zh-tw (Taiwan), en (English), utf-8, JP (Japanese).
- Subject: Click on Email subject to view the content of the Email.
- Similar Search: Search for Email with similar content
- Whois: Provide information of Source and Destination IP and Hostname. It allows you to search for the IP Address information through the Internet.

View Email Content

Click on the [Subject] link and the following GUI which is the Webmail read content will be displayed.



Visibility Group : ALL

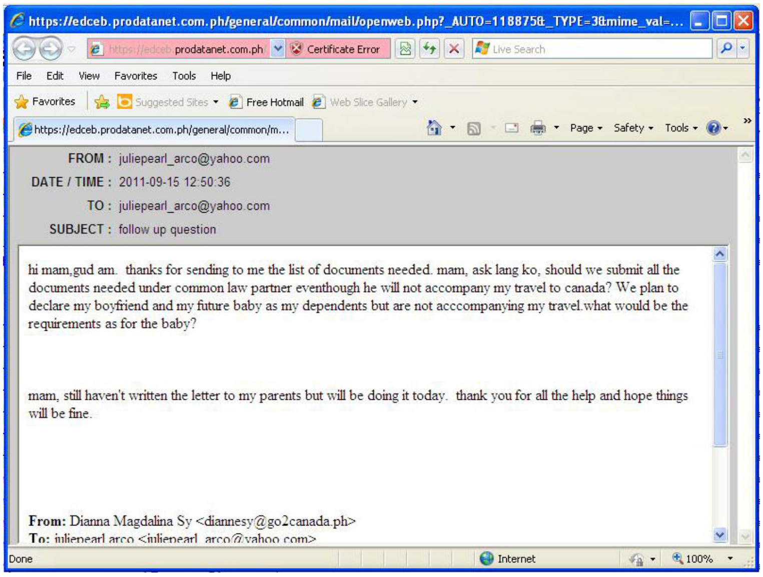
HOME PAGE | Webmail(Read) | Delete | Search | Account List

Every Page 20 Confirm

No.	□		Date-Time	Account	Sender	Subject	Webmail Type	Similar Search
1.	□		2011-09-15 13:37:41	sredido	raguilar@go2canada.p...	FW: Received Letters from Canadian Embassy dated September ...	go2canada Mail	
2.	□		2011-09-15 13:35:03	sredido	ecps@go2canada.com	GENERIC FORM FOR PRINTING	go2canada Mail	
3.	□		2011-09-15 13:34:37	sredido	mvasquez@go2canada.c...	Re: copy of LH Contracts	go2canada Mail	
4.	□		2011-09-15 13:24:28	jaze_shame	l_bantilan@yahoo.com	djd	go2canada Mail	
5.	□		2011-09-15 12:50:36	il_dianesy	juliepearl_arco@yaho...	follow up questio	go2canada Mail	
6.	□		2011-09-15 12:48:57	flowinstream	cposthou@yahoo.com.a...	Re: Application Forms for me n Ken	YAHOO Mail	

1 2 3 4 5 6 7 8 9 Enter Page Go

Total 17,422 Total Page 872 Current Page 1



https://edceb.prodatanet.com.ph/general/common/mail/openweb.php?_AUTO=118875&_TYPE=3&mime_val=...
https://edceb.prodatanet.com.ph/
Certificate Error
Live Search
File
Edit
View
Favorites
Tools
Help
Favorites
Suggested Sites
Free Hotmail
Web Slice Gallery
https://edceb.prodatanet.com.ph/general/common/m...
Page
Safety
Tools
Done
Internet
100%

FROM : juliepearl_arco@yahoo.com

DATE / TIME : 2011-09-15 12:50:36

TO : juliepearl_arco@yahoo.com

SUBJECT : follow up question

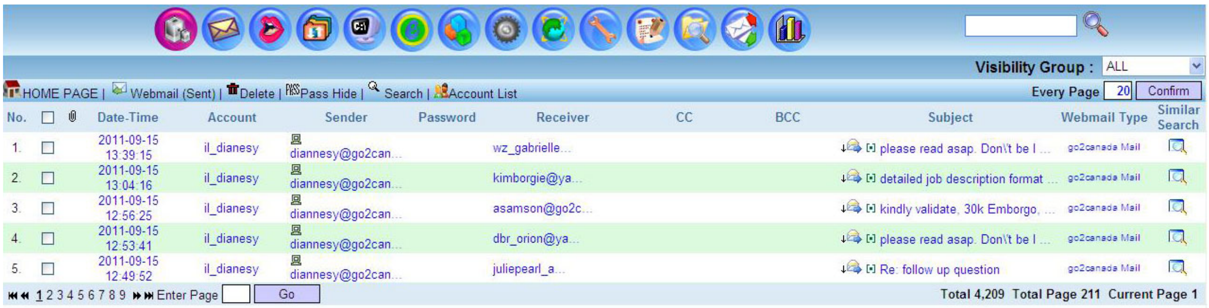
hi mam,gud am. thanks for sending to me the list of documents needed. mam, ask lang ko, should we submit all the documents needed under common law partner eventhough he will not accompany my travel to canada? We plan to declare my boyfriend and my future baby as my dependents but are not acccompanying my travel.what would be the requirements as for the baby?

mam, still haven't written the letter to my parents but will be doing it today. thank you for all the help and hope things will be fine.

From: Dianna Magdalina Sy <diannesy@go2canada.ph>
To: juliepearl arco <juliepearl_arco@yahoo.com>

Webmail Sent

Webmail (Sent) obtainable information includes Date-Time, Account (with IP/MAC), Sender, Password (if available), Receiver, CC, BCC, Subject with Webmail content (with attachment if any) and Webmail Type.



Visibility Group : ALL

HOME PAGE | Webmail (Sent) | Delete | Pass Hide | Search | Account List

Every Page 20 Confirm

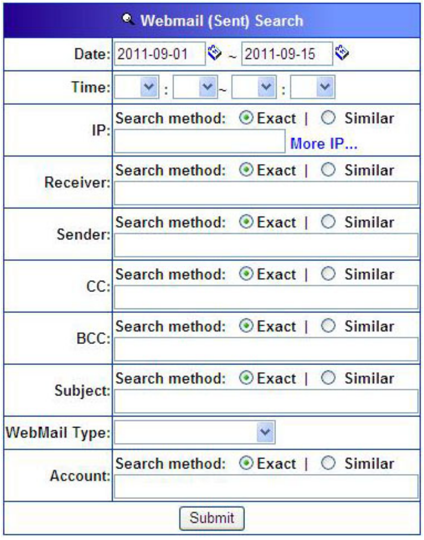
No.	☐	📎	Date-Time	Account	Sender	Password	Receiver	CC	BCC	Subject	Webmail Type	Similar Search
1.	☐		2011-09-15 13:39:15	il_dianesy	diannesy@go2can...		wz_gabrielle...			please read asap. Don\'t be l ...	go2canada Mail	
2.	☐		2011-09-15 13:04:16	il_dianesy	diannesy@go2can...		kimborgie@ya...			detailed job description format ...	go2canada Mail	
3.	☐		2011-09-15 12:56:25	il_dianesy	diannesy@go2can...		asamson@go2c...			kindly validate, 30k Emborgo, ...	go2canada Mail	
4.	☐		2011-09-15 12:53:41	il_dianesy	diannesy@go2can...		dbr_orion@ya...			please read asap. Don\'t be l ...	go2canada Mail	
5.	☐		2011-09-15 12:49:52	il_dianesy	diannesy@go2can...		juliepearl_a...			Re: follow up question	go2canada Mail	

1 2 3 4 5 6 7 8 9 Enter Page Go

Total 4,209 Total Page 211 Current Page 1

Features in this Webmail (Sent) GUI:

- Webmail (Sent): Refresh the page content
- Delete: Delete the Email (that has been checked or ticked)
- Pass Show: Shows the login password if available.
- Account List: This section shows all the Email Account List
- Search: Search for Webmail based on the specified parameters such as Date, Time, IP, Receiver, Sender, CC, BCC, Subject, Webmail Type and Account



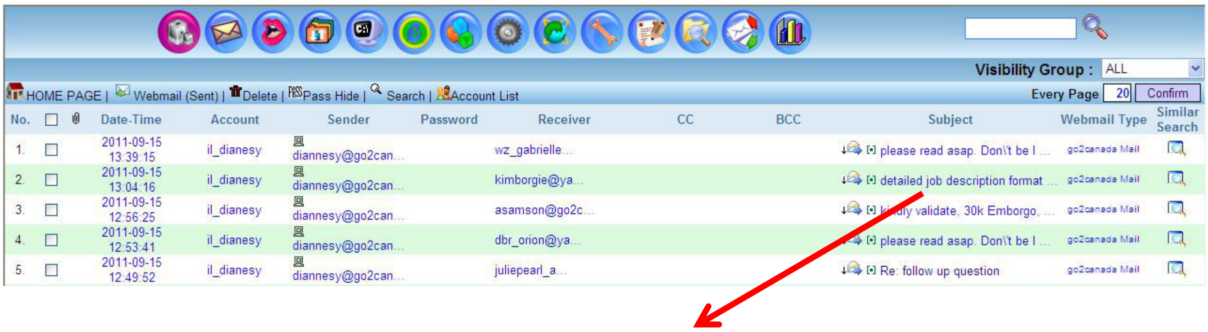
Webmail (Sent) Search

Date:	2011-09-01 ~ 2011-09-15
Time:	: ~ :
IP:	Search method: ● Exact | ○ Similar More IP...
Receiver:	Search method: ● Exact | ○ Similar
Sender:	Search method: ● Exact | ○ Similar
CC:	Search method: ● Exact | ○ Similar
BCC:	Search method: ● Exact | ○ Similar
Subject:	Search method: ● Exact | ○ Similar
WebMail Type:	
Account:	Search method: ● Exact | ○ Similar

Submit

- Source, Destination IP Address and MAC Address by pointing the mouse to the account column
- Every Page 5 Confirm Display the number of record per page
- ☐ Checkbox: Check or tick the checkbox for deleting
- Attachment: This symbol shows there is attachment in the Email
- Shows the IP address
- Forward Email: Forward the Email to a specific Email account
- [•] Source Code: Shows the Email source and path.
- [•] Convertor: Convert the subject name to another language to be readable. This convertor coverts the character in different coding formats such as zh-ch (Chinese), zh-sg (Singapore), zh-tw (Taiwan), en (English), utf-8, JP (Japanese).
- Subject: Click on Email subject to view the content of the Email.
- Similar Search: Search for Email with similar content
- Whois: Provide information of Source and Destination IP and Hostname. It allows you to search for the IP Address information through the Internet.

View Email Content
Click on the [Subject] link and the following GUI which is the Webmail sent content will be displayed.

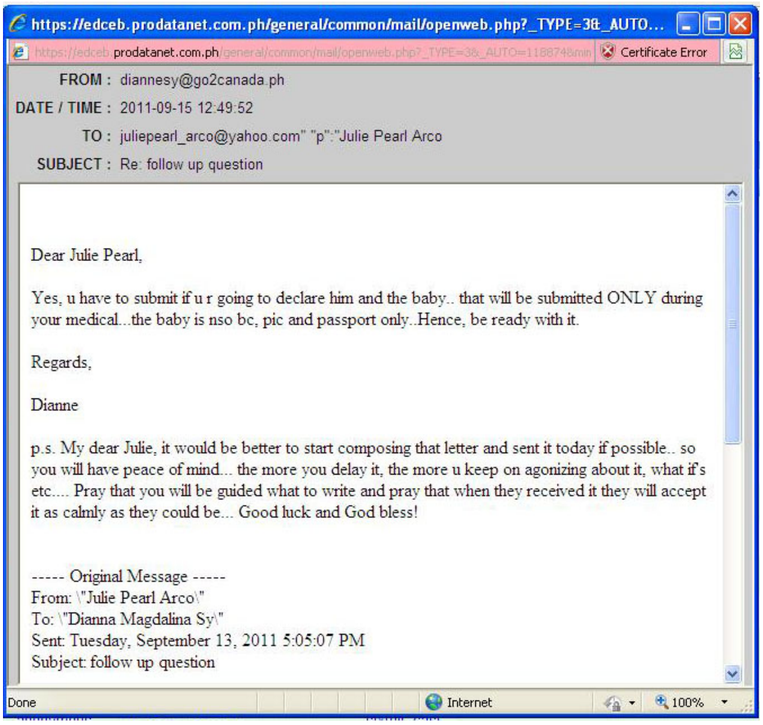


Visibility Group : ALL

HOME PAGE | Webmail (Sent) | Delete | Pass Hide | Search | Account List

Every Page 20 Confirm

No.	□		Date-Time	Account	Sender	Password	Receiver	CC	BCC	Subject	Webmail Type	Similar Search
1.	□		2011-09-15 13:39:15	il_dianesy	diannesy@go2can...		wz_gabrielle...			please read asap. Don\'t be l ...	go2canada Mail	
2.	□		2011-09-15 13:04:16	il_dianesy	diannesy@go2can...		kimborgie@ya...			detailed job description format ...	go2canada Mail	
3.	□		2011-09-15 12:56:25	il_dianesy	diannesy@go2can...		asamson@go2c...			kindly validate, 30k Emborgo, ...	go2canada Mail	
4.	□		2011-09-15 12:53:41	il_dianesy	diannesy@go2can...		dbr_orion@ya...			please read asap. Don\'t be l ...	go2canada Mail	
5.	□		2011-09-15 12:49:52	il_dianesy	diannesy@go2can...		juliepearl_a...			Re: follow up question	go2canada Mail	



https://edceb.prodatanet.com.ph/general/common/mail/openweb.php?_TYPE=3&_AUTO...

https://edceb.prodatanet.com.ph/general/common/mail/openweb.php?_TYPE=3&_AUTO=1188748min Certificate Error

FROM : diannesy@go2canada.ph

DATE / TIME : 2011-09-15 12:49:52

TO : juliepearl_arco@yahoo.com" "p":"Julie Pearl Arco

SUBJECT : Re: follow up question

Dear Julie Pearl,

Yes, u have to submit if u r going to declare him and the baby.. that will be submitted ONLY during your medical...the baby is nso bc, pic and passport only..Hence, be ready with it.

Regards,

Dianne

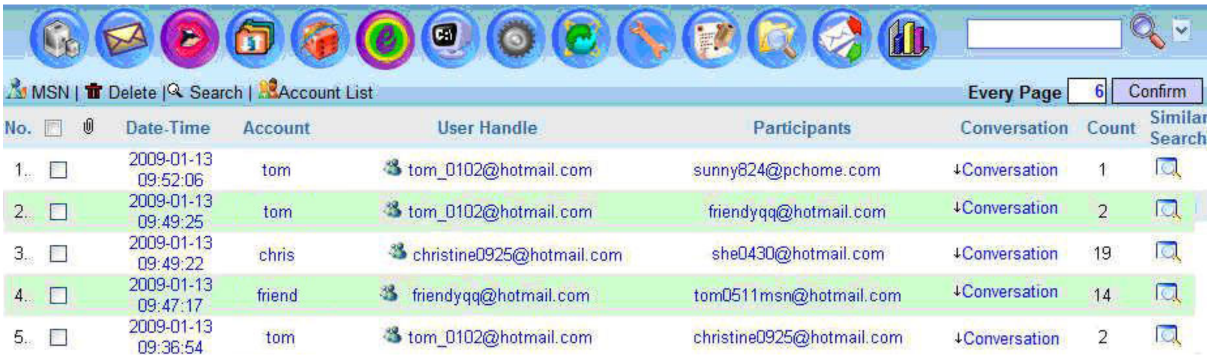
p.s. My dear Julie, it would be better to start composing that letter and sent it today if possible.. so you will have peace of mind... the more you delay it, the more u keep on agonizing about it, what if's etc.... Pray that you will be guided what to write and pray that when they received it they will accept it as calmly as they could be... Good luck and God bless!

----- Original Message -----
From: \"Julie Pearl Arco\"
To: \"Dianna Magdalina Sy\"
Sent: Tuesday, September 13, 2011 5:05:07 PM
Subject: follow up question

Instant Messaging & Chat

Windows Live Messenger (aka MSN)

MSN obtainable information includes Date-Time, Account (with IP/MAC), User Handle (User Account), Participant Account, Conversation with content which includes file transferred and MSN webcam (video) session.

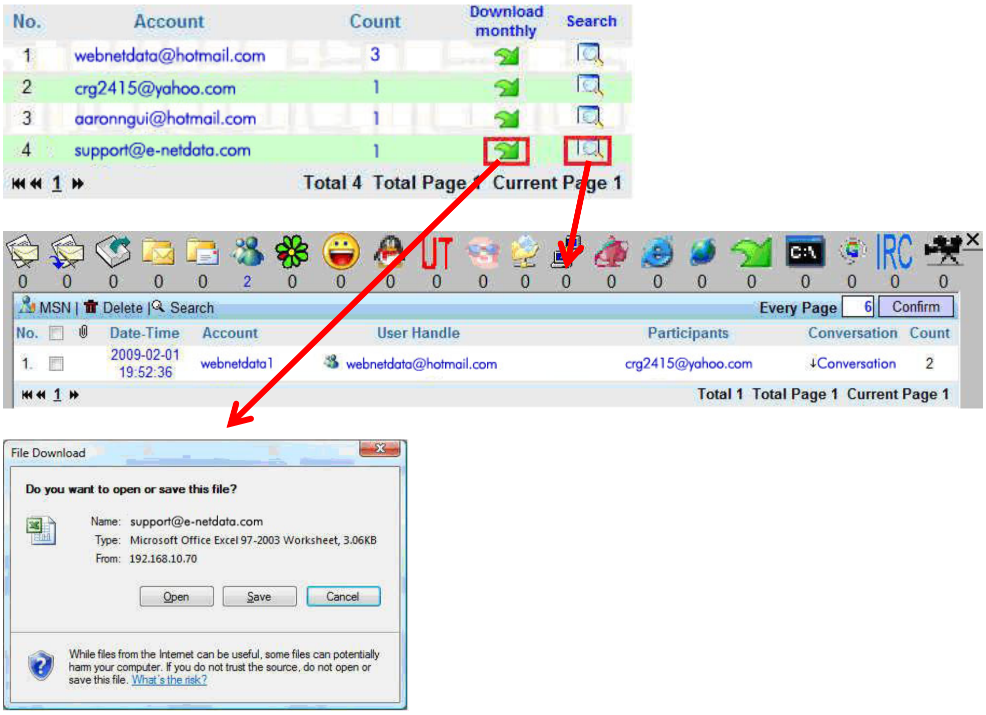


MSN | Delete | Search | Account List — Every Page 6 Confirm

No.	□		Date-Time	Account	User Handle	Participants	Conversation	Count	Similar Search
1.	□		2009-01-13 09:52:06	tom	tom_0102@hotmail.com	sunny824@pchome.com	↓Conversation	1	
2.	□		2009-01-13 09:49:25	tom	tom_0102@hotmail.com	friendyqq@hotmail.com	↓Conversation	2	
3.	□		2009-01-13 09:49:22	chris	christine0925@hotmail.com	she0430@hotmail.com	↓Conversation	19	
4.	□		2009-01-13 09:47:17	friend	friendyqq@hotmail.com	tom0511msn@hotmail.com	↓Conversation	14	
5.	□		2009-01-13 09:36:54	tom	tom_0102@hotmail.com	christine0925@hotmail.com	↓Conversation	2	

Features in this MSN GUI:

- MSN: Refresh the page content.
- Delete: Delete the MSN chat record (that has been checked or ticked).
- Account List: This section shows the MSN Account List. Administrator can download the monthly chat record (in Excel format) and search for the chat record as shown below.



No.	Account	Count	Download monthly	Search
1	webnetdata@hotmail.com	3		
2	crg2415@yahoo.com	1		
3	aaronngui@hotmail.com	1		
4	support@e-netdata.com	1		

1 — Total 4 Total Page 1 Current Page 1

MSN | Delete | Search — Every Page 6 Confirm

No.	□		Date-Time	Account	User Handle	Participants	Conversation	Count
1.	□		2009-02-01 19:52:36	webnetdata1	webnetdata@hotmail.com	crg2415@yahoo.com	↓Conversation	2

1 — Total 1 Total Page 1 Current Page 1

File Download

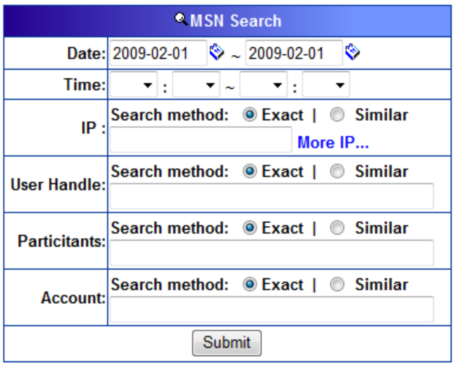
Do you want to open or save this file?

Name: support@e-netdata.com
Type: Microsoft Office Excel 97-2003 Worksheet, 3.06KB
From: 192.168.10.70

Open | Save | Cancel

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

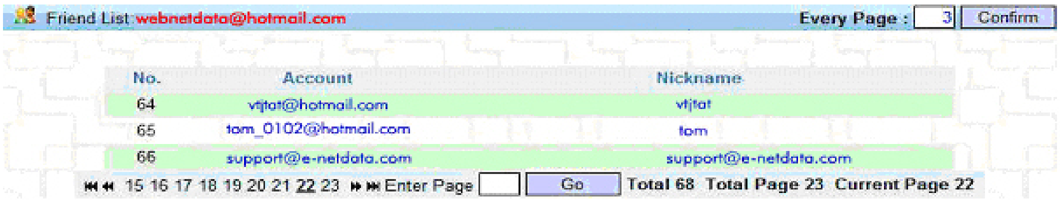
- Search: Search for MSN record based on the specified parameters such as Date, Time, IP, User Handle, Participants and Account.



MSN Search

Date:	2009-02-01 ~ 2009-02-01
Time:	: ~ :
IP :	Search method: ● Exact | ○ Similar More IP...
User Handle:	Search method: ● Exact | ○ Similar
Particitants:	Search method: ● Exact | ○ Similar
Account:	Search method: ● Exact | ○ Similar

- Every Page 5 Confirm Display the number of record per page
- □ Checkbox: Check or tick the checkbox for deleting
- File Transferred: This symbol shows there is file transferred over the MSN
- Friend List: This will show the entire friend list for the particular MSN account.

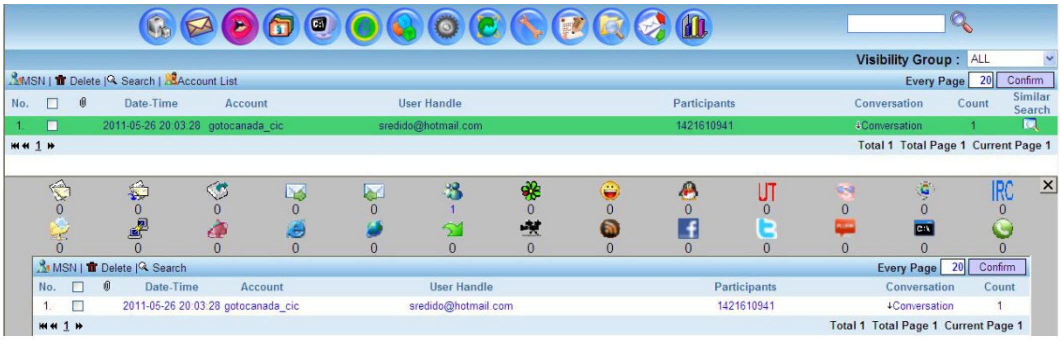


Friend List webnetdata@hotmail.com Every Page : 3 Confirm

No.	Account	Nickname
64	vtjtat@hotmail.com	vtjtat
65	tom_0102@hotmail.com	tom
66	support@e-netdata.com	support@e-netdata.com

⏮ ⏪ 15 16 17 18 19 20 21 22 23 ⏩ ⏭ Enter Page Go Total 68 Total Page 23 Current Page 22

- ↓ Download: Download the MSN chat record.
- Conversation: Click on Conversation to view the chat content.
- Similar Search: Search for chat record with similar content.



Visibility Group : ALL

MSN | Delete | Search | Account List Every Page 20 Confirm

No.	□		Date-Time	Account	User Handle	Participants	Conversation	Count	Similar Search
1.	□		2011-05-26 20:03:28	gotocanada_cic	sredido@hotmail.com	1421610941	↓Conversation	1	

⏮ ⏪ 1 ⏩ Total 1 Total Page 1 Current Page 1

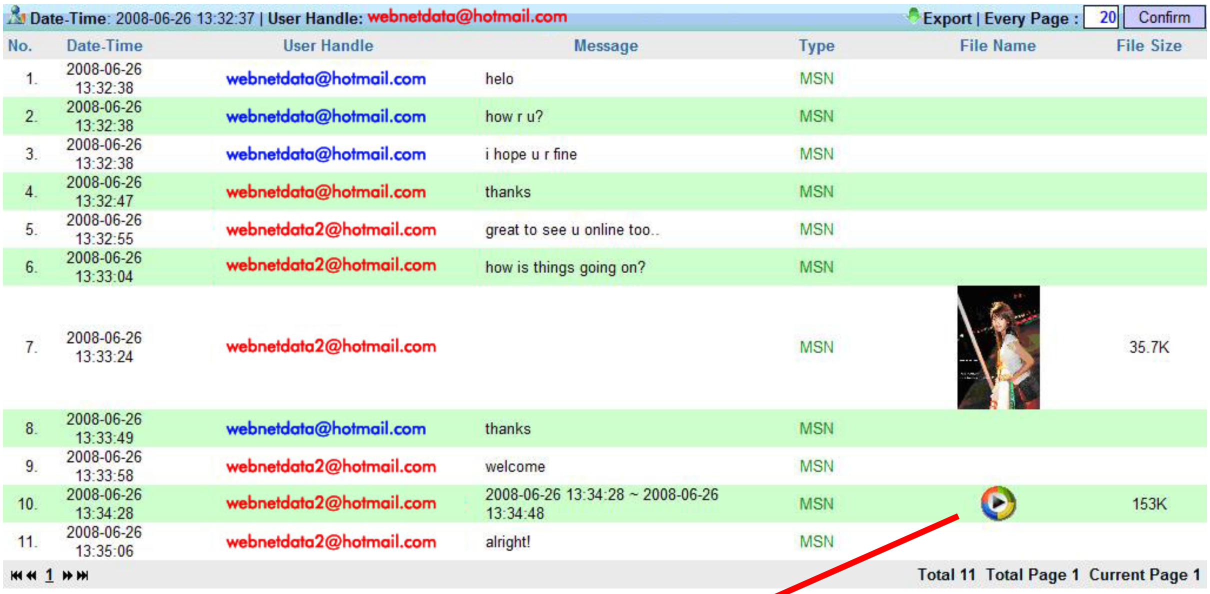
MSN | Delete | Search Every Page 20 Confirm

No.	□		Date-Time	Account	User Handle	Participants	Conversation	Count
1.	□		2011-05-26 20:03:28	gotocanada_cic	sredido@hotmail.com	1421610941	↓Conversation	1

⏮ ⏪ 1 ⏩ Total 1 Total Page 1 Current Page 1

MSN Conversation Content

Click on the [Conversation] link and the following GUI will pop up and you can view the whole chat session content. It includes chat text message, file transferred (which can be opened and downloaded) and webcam session reconstructed in ml20 format.

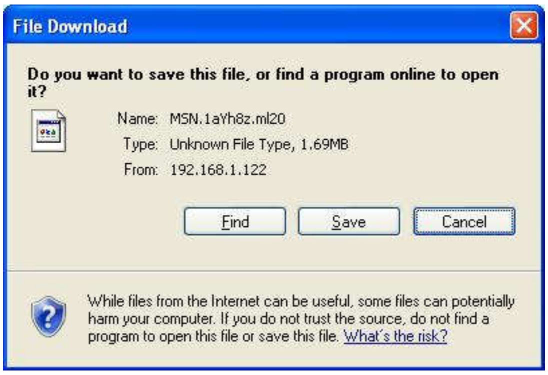


Date-Time: 2008-06-26 13:32:37 | User Handle: webnetdata@hotmail.com

No.	Date-Time	User Handle	Message	Type	File Name	File Size
1.	2008-06-26 13:32:38	webnetdata@hotmail.com	helo	MSN		
2.	2008-06-26 13:32:38	webnetdata@hotmail.com	how r u?	MSN		
3.	2008-06-26 13:32:38	webnetdata@hotmail.com	i hope u r fine	MSN		
4.	2008-06-26 13:32:47	webnetdata@hotmail.com	thanks	MSN		
5.	2008-06-26 13:32:55	webnetdata2@hotmail.com	great to see u online too..	MSN		
6.	2008-06-26 13:33:04	webnetdata2@hotmail.com	how is things going on?	MSN		
7.	2008-06-26 13:33:24	webnetdata2@hotmail.com		MSN		35.7K
8.	2008-06-26 13:33:49	webnetdata@hotmail.com	thanks	MSN		
9.	2008-06-26 13:33:58	webnetdata2@hotmail.com	welcome	MSN		
10.	2008-06-26 13:34:28	webnetdata2@hotmail.com	2008-06-26 13:34:28 ~ 2008-06-26 13:34:48	MSN	▶	153K
11.	2008-06-26 13:35:06	webnetdata2@hotmail.com	alright!	MSN		

1

Total 11 Total Page 1 Current Page 1



File Download

Do you want to save this file, or find a program online to open it?

Name: MSN.1aYh8z.ml20
Type: Unknown File Type, 1.69MB
From: 192.168.1.122

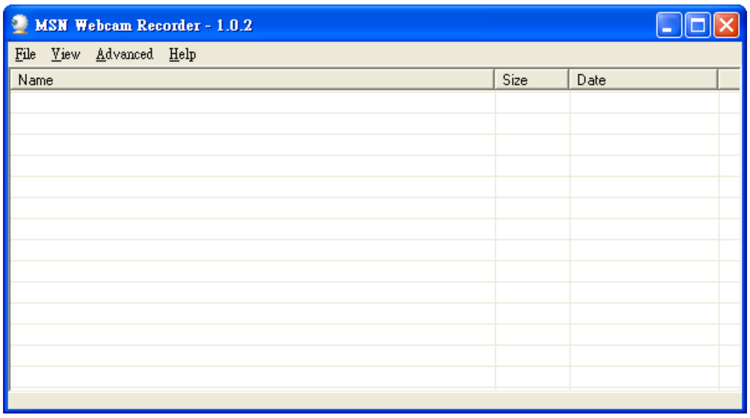
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

To playback the MSN webcam session, click on the video icon and download the webcam file (in ml20 format) to your PC and play back using the MSN web recorder tool.

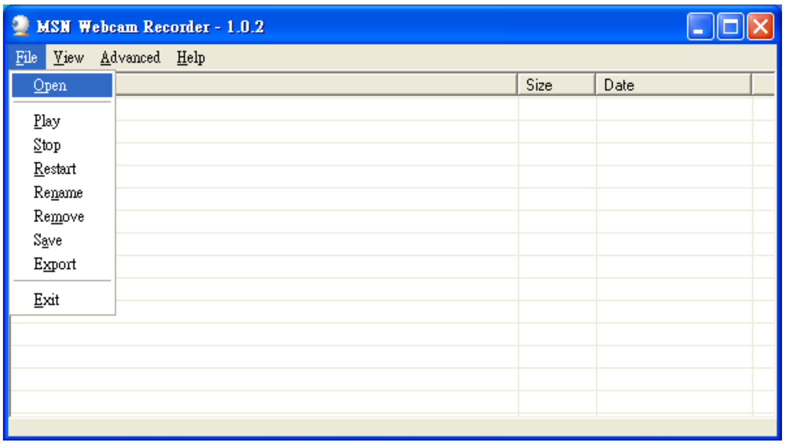
MSN Webcam Playback

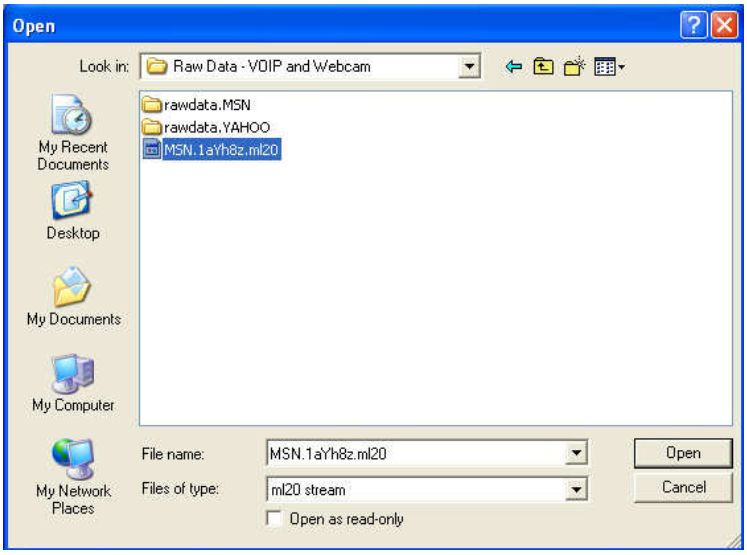
1. Download and install MSN web recorder 1.0.2 from the following website at http://ml20rc.msnfanatic.com/download.html

2. Start or execute the MSN web recorder



3. Open ml20 file: File - Open – OPEN and select the file to play

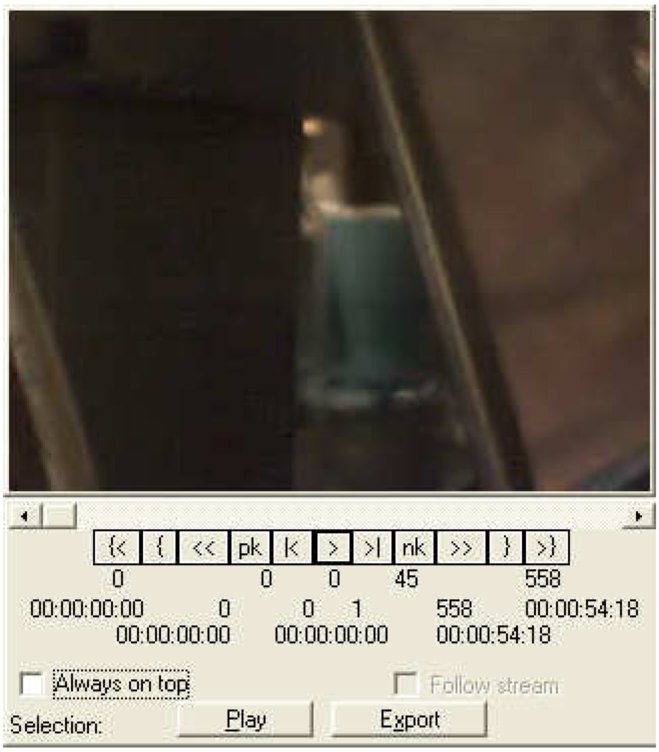




Look in: Raw Data - VOIP and Webcam

rawdata.MSN
rawdata.YAHOO
MSN.1aYh8z.ml20

File name: MSN.1aYh8z.ml20
Files of type: ml20 stream
□ Open as read-only



```
          0                 0       0      45              558
 00:00:00:00          0          0     1         558      00:00:54:18
          00:00:00:00     00:00:00:00     00:00:54:18
```

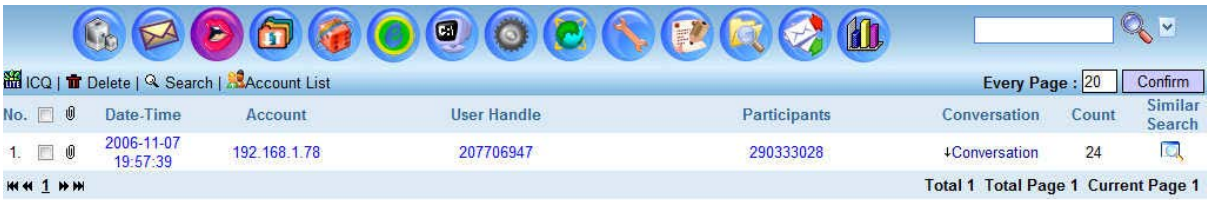
□ Always on top □ Follow stream

Selection:

4. Click on [Play] to play back the record MSN webcam session

ICQ

ICQ Messenger obtainable information includes Date-Time, Account (with IP/MAC), User Handle (User Account), Participant Account, Conversation with content and Count.



ICQ | Delete | Search | Account List

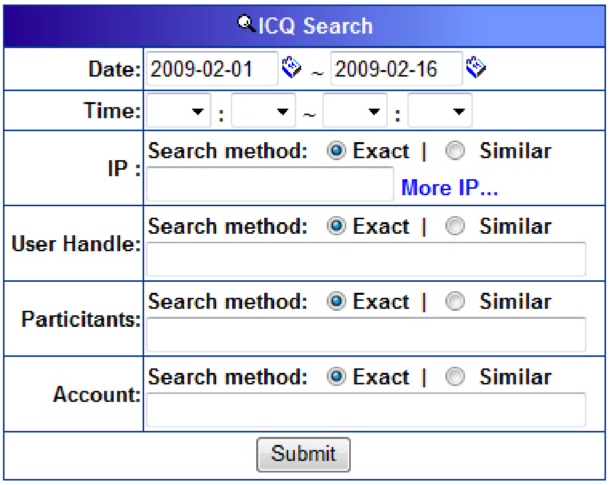
Every Page : 20 Confirm

No.	□		Date-Time	Account	User Handle	Participants	Conversation	Count	Similar Search
1.	□		2006-11-07 19:57:39	192.168.1.78	207706947	290333028	↓Conversation	24	

⏮ ⏪ 1 ⏩ ⏭ Total 1 Total Page 1 Current Page 1

Features in this GUI:

- ICQ: Refresh the page content.
- Delete: Delete the ICQ chat record (that has been checked or ticked)
- Account List: This section shows the ICQ Account List. Administrator can download the monthly chat record (in Excel format) and search for the chat record as shown below
- Search: Search for ICQ record based on the specified parameters such as Date, Time, IP, User Handle, Participants and Account



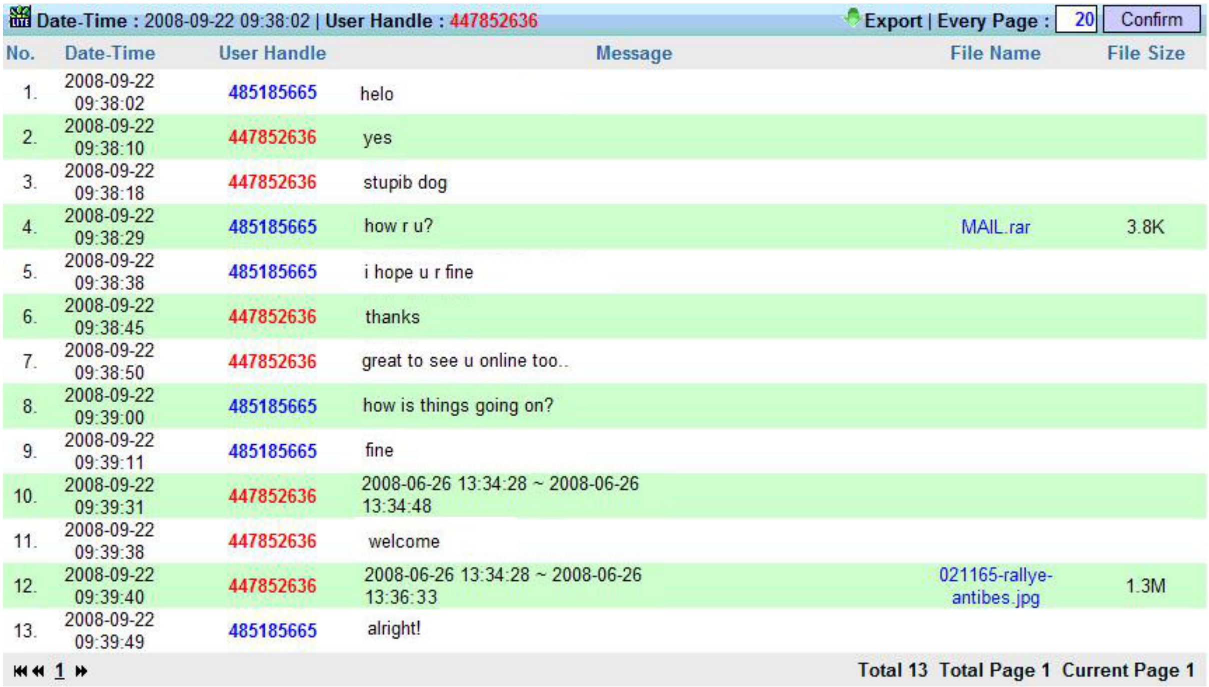
ICQ Search

Date:	2009-02-01 ~ 2009-02-16
Time:	: ~ :
IP :	Search method: ● Exact | ○ Similar More IP...
User Handle:	Search method: ● Exact | ○ Similar
Particitants:	Search method: ● Exact | ○ Similar
Account:	Search method: ● Exact | ○ Similar

Submit

- Every Page 5 Confirm Display the number of record per page
- □ Checkbox: Check or tick the checkbox for deleting
- File Transferred: This symbol shows there is file transferred over the ICQ
- Friend List: This will show the entire friend list for the particular ICQ account.
- ↓ Download: Download the ICQ chat record.
- Conversation: Click on Conversation to view the chat content.
- Similar Search: Search for chat record with similar content.

ICQ Conversation
Click on the [Conversation] link, the following conversation window content will pop up and you can view the entire chatting session and files transferred as shown in the diagram below.



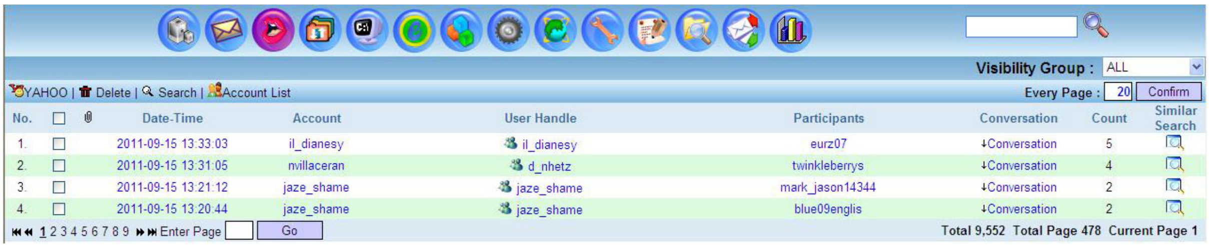
Date-Time : 2008-09-22 09:38:02 | User Handle : 447852636 Every Page : 20

No.	Date-Time	User Handle	Message	File Name	File Size
1.	2008-09-22 09:38:02	485185665	helo		
2.	2008-09-22 09:38:10	447852636	yes		
3.	2008-09-22 09:38:18	447852636	stupib dog		
4.	2008-09-22 09:38:29	485185665	how r u?	MAIL.rar	3.8K
5.	2008-09-22 09:38:38	485185665	i hope u r fine		
6.	2008-09-22 09:38:45	447852636	thanks		
7.	2008-09-22 09:38:50	447852636	great to see u online too..		
8.	2008-09-22 09:39:00	485185665	how is things going on?		
9.	2008-09-22 09:39:11	485185665	fine		
10.	2008-09-22 09:39:31	447852636	2008-06-26 13:34:28 ~ 2008-06-26 13:34:48		
11.	2008-09-22 09:39:38	447852636	welcome		
12.	2008-09-22 09:39:40	447852636	2008-06-26 13:34:28 ~ 2008-06-26 13:36:33	021165-rallye-antibes.jpg	1.3M
13.	2008-09-22 09:39:49	485185665	alright!		

⏮ ⏪ 1 ⏩ Total 13 Total Page 1 Current Page 1

Yahoo Messenger

Yahoo Messenger obtainable information includes Date-Time, Account (with IP/MAC), User Handle (User Account), Participant Account, Conversation (with content), file transferred, VOIP and Webcam session etc.



Visibility Group : ALL

YAHOO | Delete | Search | Account List

Every Page : 20 Confirm

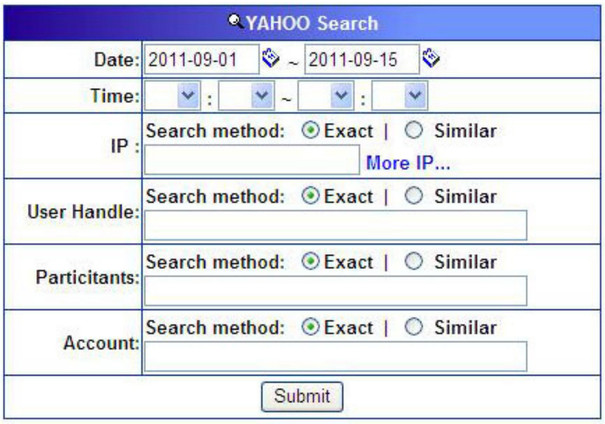
No.	□		Date-Time	Account	User Handle	Participants	Conversation	Count	Similar Search
1.	□		2011-09-15 13:33:03	il_dianesy	il_dianesy	eurz07	↓Conversation	5	
2.	□		2011-09-15 13:31:05	nvillaceran	d_nhetz	twinkleberrys	↓Conversation	4	
3.	□		2011-09-15 13:21:12	jaze_shame	jaze_shame	mark_jason14344	↓Conversation	2	
4.	□		2011-09-15 13:20:44	jaze_shame	jaze_shame	blue09englis	↓Conversation	2	

1 2 3 4 5 6 7 8 9 Enter Page Go

Total 9,552 Total Page 478 Current Page 1

Features in this GUI:

- YAHOO: Refresh the page content
- Delete: Delete the YAHOO chat record (that has been checked or ticked)
- Account List: This section shows the YAHOO Account List. Administrator can download the monthly chat record (in Excel format) and search for the chat record as shown below
- Search: Search for YAHOO record based on the specified parameters such as Date, Time, IP, User Handle, Participants and Account



YAHOO Search

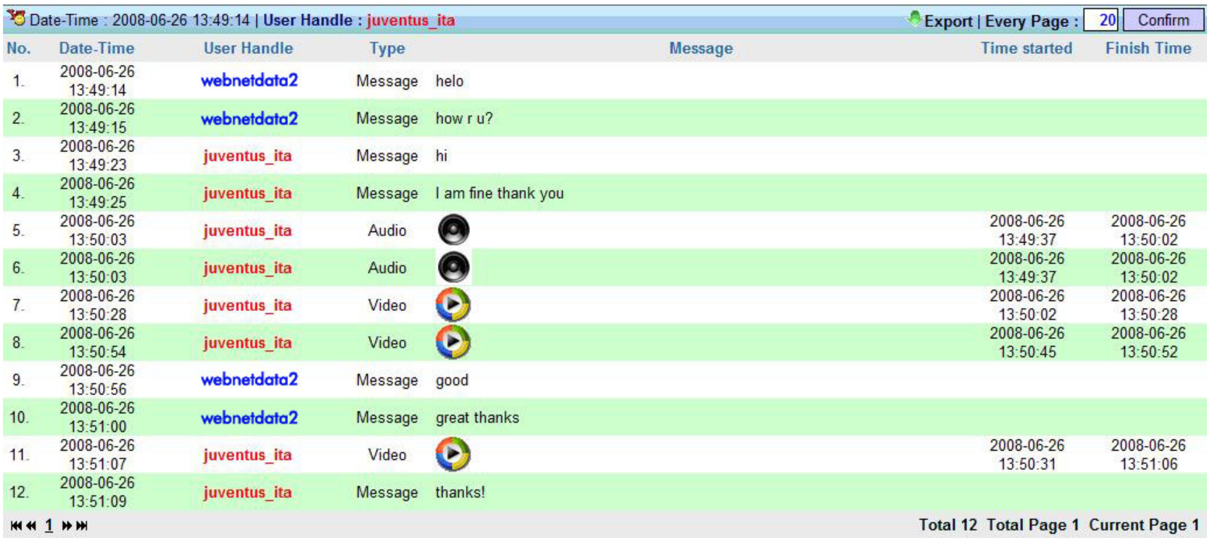
Date:	2011-09-01 ~ 2011-09-15
Time:	: ~ :
IP :	Search method: ● Exact | ○ Similar More IP...
User Handle:	Search method: ● Exact | ○ Similar
Particitants:	Search method: ● Exact | ○ Similar
Account:	Search method: ● Exact | ○ Similar

Submit

- Every Page 5 Confirm Display the number of record per page
- □ Checkbox: Check or tick the checkbox for deleting
- 📎 File Transferred: This symbol shows there is file transferred over the YAHOO
- Friend List: This will show the entire friend list for the particular YAHOO account.
- ↓ Download: Download the YAHOO chat record.
- Conversation: Click on Conversation to view the chat content.
- Similar Search: Search for chat record with similar content.

Yahoo Messenger Conversation, VOIP and Webcam Sessions

Click on the click the [Conversation] link and the following conversation window will pop up and you can view the entire text chat session, file transfer, VoIP (audio) and webcam (video) sessions. For webcam play back, you just need to click on the webcam (video) icon and it will play back the webcam video. For VoIP play back, you need to follow the instructions as follow.



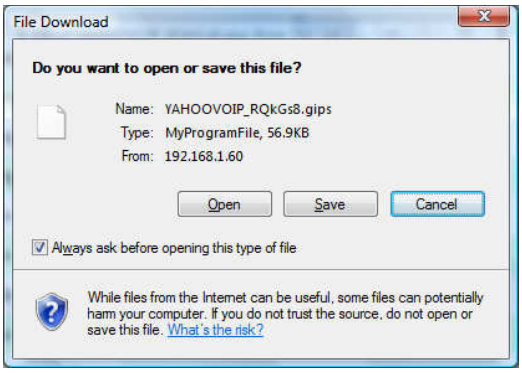
Date-Time : 2008-06-26 13:49:14 | User Handle : juventus_ita

No.	Date-Time	User Handle	Type	Message	Time started	Finish Time
1.	2008-06-26 13:49:14	webnetdata2	Message	helo		
2.	2008-06-26 13:49:15	webnetdata2	Message	how r u?		
3.	2008-06-26 13:49:23	juventus_ita	Message	hi		
4.	2008-06-26 13:49:25	juventus_ita	Message	I am fine thank you		
5.	2008-06-26 13:50:03	juventus_ita	Audio	◉	2008-06-26 13:49:37	2008-06-26 13:50:02
6.	2008-06-26 13:50:03	juventus_ita	Audio	◉	2008-06-26 13:49:37	2008-06-26 13:50:02
7.	2008-06-26 13:50:28	juventus_ita	Video	▶	2008-06-26 13:50:02	2008-06-26 13:50:28
8.	2008-06-26 13:50:54	juventus_ita	Video	▶	2008-06-26 13:50:45	2008-06-26 13:50:52
9.	2008-06-26 13:50:56	webnetdata2	Message	good		
10.	2008-06-26 13:51:00	webnetdata2	Message	great thanks		
11.	2008-06-26 13:51:07	juventus_ita	Video	▶	2008-06-26 13:50:31	2008-06-26 13:51:06
12.	2008-06-26 13:51:09	juventus_ita	Message	thanks!		

⏮ ◀ 1 ▶ ⏭ Total 12 Total Page 1 Current Page 1

Yahoo Messenger VoIP Play Back

To play back Yahoo VoIP session, you can click and download the VoIP (audio) file in GIPS format to your own PC. You must have GIPS Decoder installed on your PC in order to playback the GIPS VoIP (audio) file.



File Download

Do you want to open or save this file?

Name: YAHOOVOIP_RQkGs8.gips
Type: MyProgramFile, 56.9KB
From: 192.168.1.60

☑ Always ask before opening this type of file

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

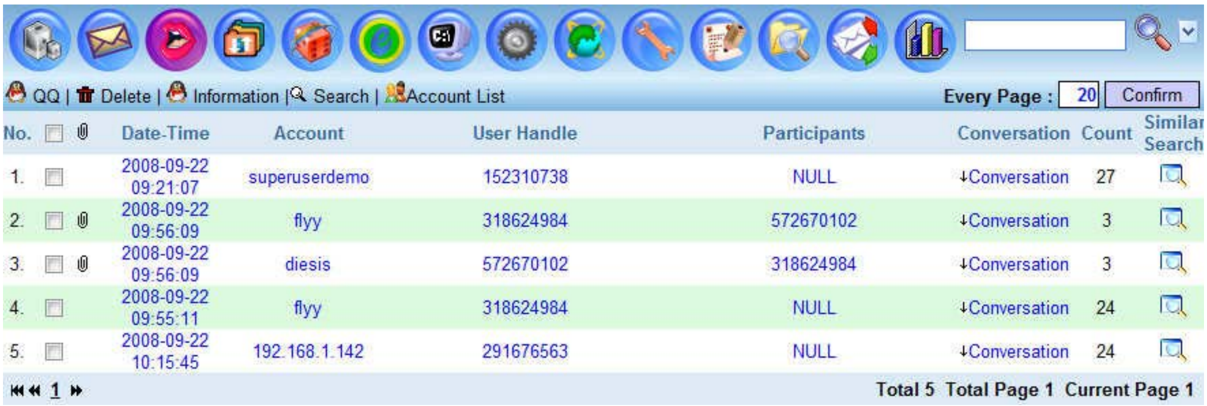
GIPS Decoder for Yahoo Messenger VoIP Play Back

This software is used to play back recorded Yahoo VOIP audio file (.GIPS file format). GIPS Decoder is provided and supported by GIPS community.

Note: GIPS Decoder is maintained by GIPS Community. User would be required to purchase GIPS Decoder directly from GIPS Community in order to play back Yahoo VoIP audio file.

QQ Messenger *

QQ chat obtainable information includes Date-time, account (with IP/MAC), user handle (user account), participant account, conversation with content and count.
* Optional Purchase License – Sniffer Agent for QQ 2010, QQ 2010 only supported by using Sniffer Agent (Sold as Optional License)

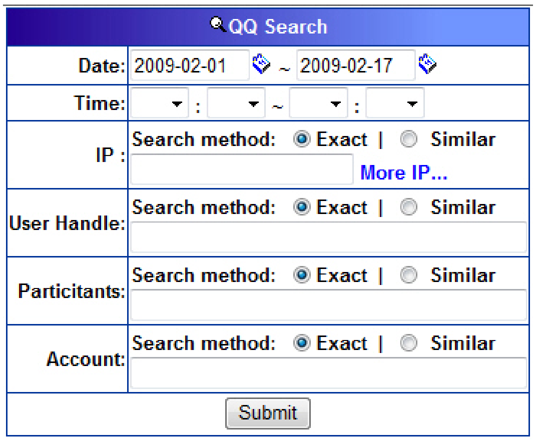


No.	□	📎	Date-Time	Account	User Handle	Participants	Conversation	Count	Similar Search
1.	□		2008-09-22 09:21:07	superuserdemo	152310738	NULL	↓Conversation	27	🔍
2.	□	📎	2008-09-22 09:56:09	flyy	318624984	572670102	↓Conversation	3	🔍
3.	□	📎	2008-09-22 09:56:09	diesis	572670102	318624984	↓Conversation	3	🔍
4.	□		2008-09-22 09:55:11	flyy	318624984	NULL	↓Conversation	24	🔍
5.	□		2008-09-22 10:15:45	192.168.1.142	291676563	NULL	↓Conversation	24	🔍

Total 5 Total Page 1 Current Page 1

Features in this QQ GUI:

- QQ: Refresh the page content.
- Delete: Delete the QQ chat record (that has been checked or ticked).
- Account List: This section shows QQ Account List. Administrator can download the monthly chat record (in Excel format) and search for the chat record as shown below. (Refer to 2.2.1)
- Search: Search for QQ record based on the specified parameters such as Date, Time, IP, User Handle, Participants and Account.



Date:	2009-02-01 ~ 2009-02-17
Time:	: ~ :
IP :	Search method: ● Exact | ○ Similar
User Handle:	Search method: ● Exact | ○ Similar
Particitants:	Search method: ● Exact | ○ Similar
Account:	Search method: ● Exact | ○ Similar

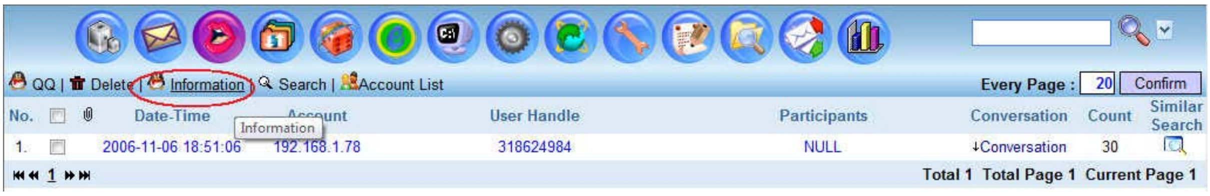
- Every Page 5 Confirm Display the number of record per page
- □ Checkbox: Check or tick the checkbox for deleting
- 📎 File Transferred: This symbol shows there is file transferred over the QQ
- 👥 Friend List: This will show the entire friend list for the particular QQ account.
- ↓ Download: Download the QQ chat record.
- Conversation: Click on Conversation to view the chat content.
- 🔍 Similar Search: Search for chat record with similar content.

How to view the encrypted conversation content for QQ?

The captured conversation in QQ is encrypted. This section explains the process on how to use the QQ cracker to decrypt the information.

Step 1 – Download the QQ cracker

The following diagram shows the steps to download the QQ cracker. Click on Information and a Window will pop up as shown below.

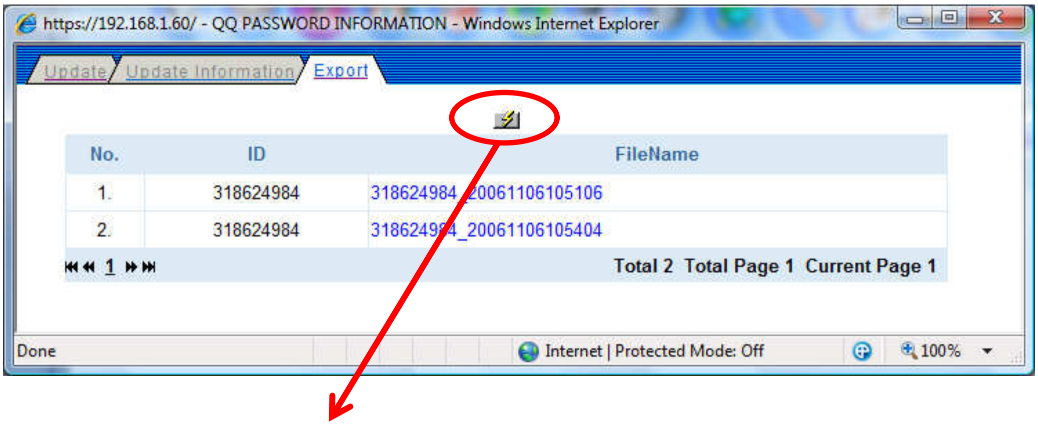


QQ | Delete | Information | Search | Account List Every Page : 20 Confirm

No.	☐		Date-Time	Account	User Handle	Participants	Conversation	Count	Similar Search
1.	☐		2006-11-06 18:51:06	192.168.1.78	318624984	NULL	↓Conversation	30	

⏮ ◀ 1 ▶ ⏭ Total 1 Total Page 1 Current Page 1

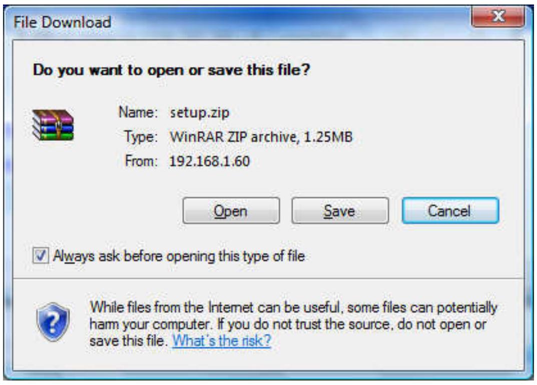
Click on the icon to download QQ Cracker Tool “setup.zip.”



https://192.168.1.60/ - QQ PASSWORD INFORMATION - Windows Internet Explorer

No.	ID	FileName
1.	318624984	318624984_20061106105106
2.	318624984	318624984_20061106105404

⏮ ◀ 1 ▶ ⏭ Total 2 Total Page 1 Current Page 1



File Download

Do you want to open or save this file?

Name: setup.zip
Type: WinRAR ZIP archive, 1.25MB
From: 192.168.1.60

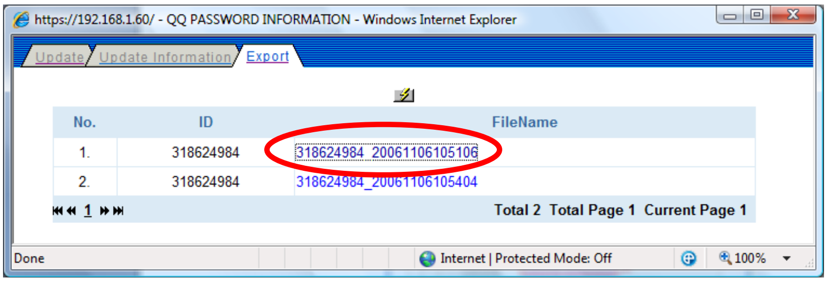
☑ Always ask before opening this type of file

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Step 2 – Install QQ cracker into computer

- Unzip the file and install the QQ cracker tool “setup.exe.”
- Click [Next] to continue.
- Click [Next] to continue. You may want to change to different directory to install the QQ Cracker Tool.
- Click [Next] to continue and the system will create a Desktop icon on your computer. The
- QQ cracker will then be ready to be installed in your PC system.
- Click [Next] to complete the Installation.
- Click [Finish] and Launch the QQ Cracker 2 Tool.

Step 3 – Decrypt the conversation.
At Information Export page, download the conversation file.



https://192.168.1.60/ - QQ PASSWORD INFORMATION - Windows Internet Explorer

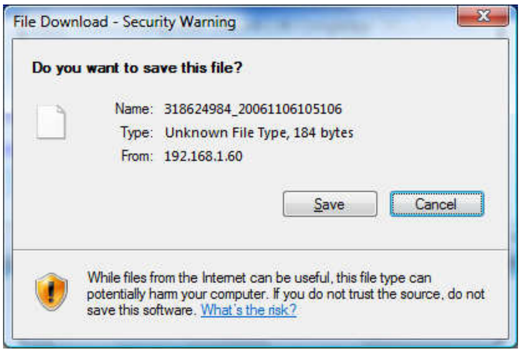
No.	ID	FileName
1.	318624984	318624984_20061106105106
2.	318624984	318624984_20061106105404

Total 2 Total Page 1 Current Page 1

Done

Internet | Protected Mode: Off

100%



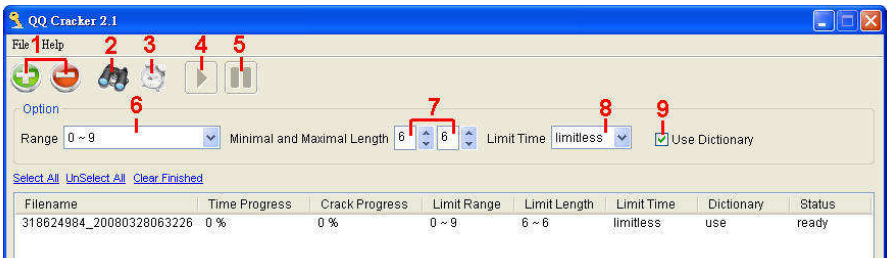
File Download - Security Warning

Do you want to save this file?

Name: 318624984_20061106105106
Type: Unknown File Type, 184 bytes
From: 192.168.1.60

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not save this software. What's the risk?

Launched QQ Cracker 2 Tool



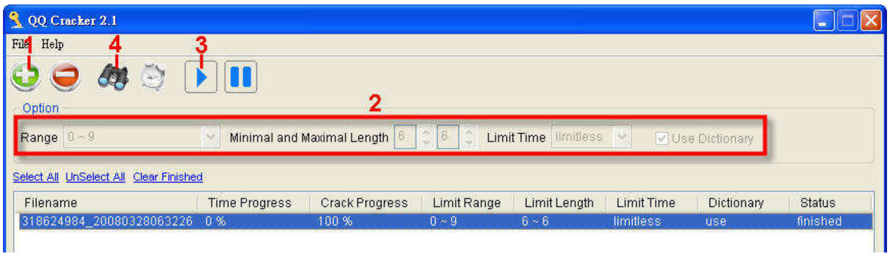
Range 0 ~ 9 Minimal and Maximal Length 6 6 Limit Time limitless ☑ Use Dictionary

Filename	Time Progress	Crack Progress	Limit Range	Limit Length	Limit Time	Dictionary	Status
318624984_20080328063226	0 %	0 %	0 ~ 9	6 ~ 6	limitless	use	ready

Function		Function Description
1	Import Encrypted File	+ and – signs. + means import, - means delete.
2	QQ ID List	QQ decrypted password information.
3	Speed Test	Password cracking capability (number per second).
4	START	Start the process to decrypt.
5	PAUSE	Pause the process to decrypt.
6	Range	Password character range.
7	Password Length	Password length.
8	Limit Time	Set time limitation.
9	Use Dictionary	Whether to use dictionary attack method.

Process of Decryption:

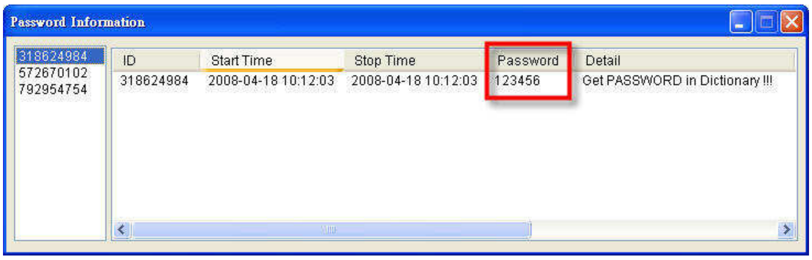
1. Import QQ conversation files to decrypt.
2. Select all configurations.
3. Start to decrypt.
4. Look for the decrypted information at QQ ID List.



Range 0 ~ 9 Minimal and Maximal Length 6 6 Limit Time limitless ☑ Use Dictionary

Filename	Time Progress	Crack Progress	Limit Range	Limit Length	Limit Time	Dictionary	Status
318624984_20080328063226	0 %	100 %	0 ~ 9	6 ~ 6	limitless	use	finished

Information in QQ ID List with password cracked:

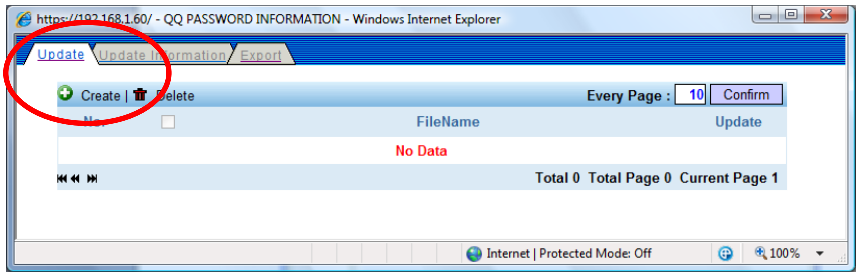


318624984
572670102
792954754

ID	Start Time	Stop Time	Password	Detail
318624984	2008-04-18 10:12:03	2008-04-18 10:12:03	123456	Get PASSWORD in Dictionary !!!

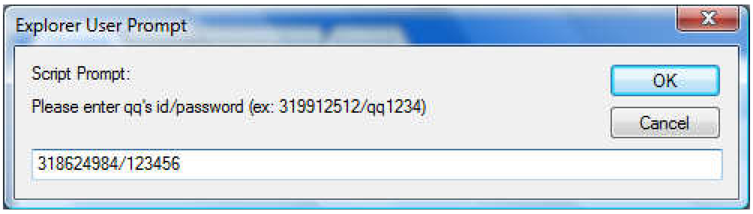
QQ Database Update

Click on Information – Update – Create. A Window will pop out and click [OK] to continue.


https://192.168.1.60/ - QQ PASSWORD INFORMATION - Windows Internet Explorer
Update
Update Information
Export
Create | Delete
Every Page : 10 Confirm
Internet | Protected Mode: Off
100%

No.	□	FileName	Update
		No Data	

Total 0 Total Page 0 Current Page 1

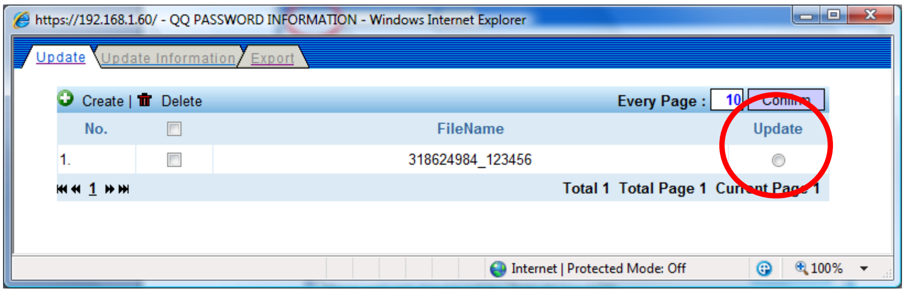


Script Prompt:

Please enter qq's id/password (ex: 319912512/qq1234)

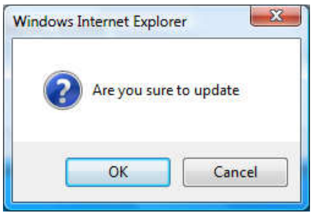
318624984/123456

Then click on the radio button [Update]


https://192.168.1.60/ - QQ PASSWORD INFORMATION - Windows Internet Explorer
Update
Update Information
Export
Create | Delete
Every Page : 10
Confirm
Internet | Protected Mode: Off
100%

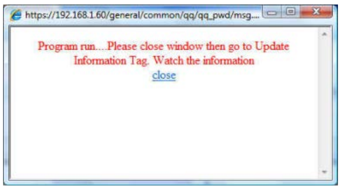
No.	□	FileName	Update
1.	□	318624984_123456	○

⏮ ⏪ 1 ⏩ ⏭ Total 1 Total Page 1 Current Page 1



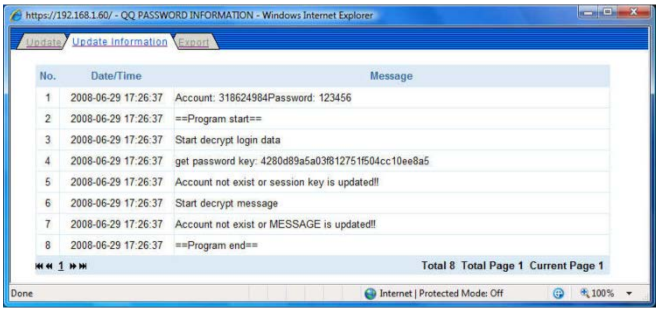
Are you sure to update

Click [OK] to continue and the following Window will pop out.



Program run....Please close window then go to Update Information Tag. Watch the information
close

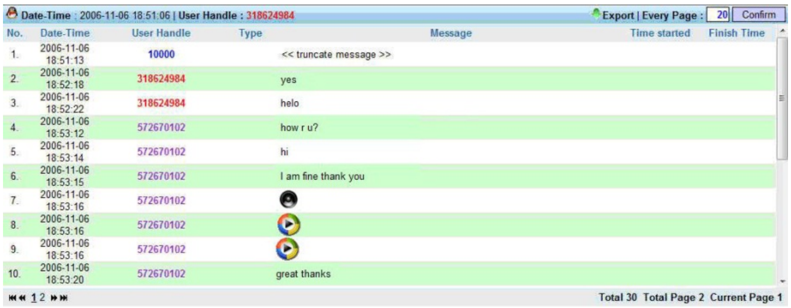
Close the Window and go to Update Information page. This page will show the information of QQ Database being update.


https://192.168.1.60/ - QQ PASSWORD INFORMATION - Windows Internet Explorer
Update
Update Information
Export
Done
Internet | Protected Mode: Off
100%

No.	Date/Time	Message
1	2008-06-29 17:26:37	Account: 318624984Password: 123456
2	2008-06-29 17:26:37	==Program start==
3	2008-06-29 17:26:37	Start decrypt login data
4	2008-06-29 17:26:37	get password key: 4280d89a5a03f812751f504cc10ee8a5
5	2008-06-29 17:26:37	Account not exist or session key is updated!!
6	2008-06-29 17:26:37	Start decrypt message
7	2008-06-29 17:26:37	Account not exist or MESSAGE is updated!!
8	2008-06-29 17:26:37	==Program end==

⏮ ⏪ 1 ⏩ ⏭ Total 8 Total Page 1 Current Page 1

You may now return to the QQ page and click on the [Conversation]. It will display the content of the conversation.



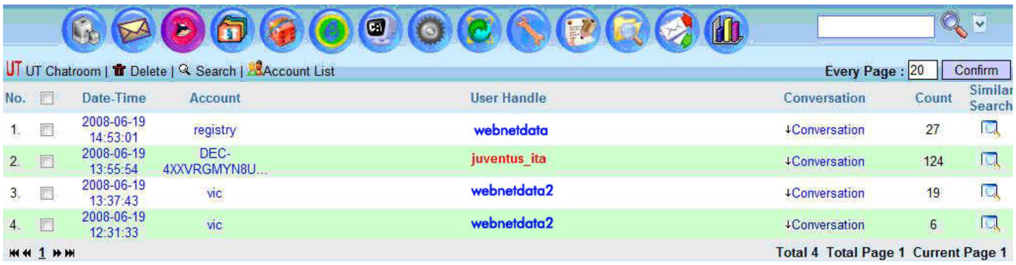
Date-Time : 2006-11-06 18:51:06 | User Handle : 318624984

No.	Date-Time	User Handle	Type	Message	Time started	Finish Time
1.	2006-11-06 18:51:13	10000		<< truncate message >>		
2.	2006-11-06 18:52:18	318624984		yes		
3.	2006-11-06 18:52:22	318624984		helo		
4.	2006-11-06 18:53:12	572670102		how r u?		
5.	2006-11-06 18:53:14	572670102		hi		
6.	2006-11-06 18:53:15	572670102		I am fine thank you		
7.	2006-11-06 18:53:16	572670102		●		
8.	2006-11-06 18:53:16	572670102		▶		
9.	2006-11-06 18:53:16	572670102		▶		
10.	2006-11-06 18:53:20	572670102		great thanks		

⏮ ⏪ 1 2 ⏩ ⏭ Total 30 Total Page 2 Current Page 1

UT Chat Room

UT Chat Room is popular chat room in Taiwan. UT Chat Room retrievable information includes Date-Time, Account, User Handle, Conversation (with content) and count.



UT Chatroom | Delete | Search | Account List   Every Page : 20 Confirm

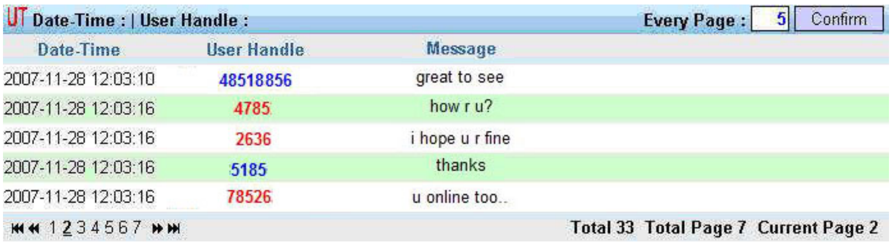
No.	□	Date-Time	Account	User Handle	Conversation	Count	Similar Search
1.	□	2008-06-19 14:53:01	registry	webnetdata	↓Conversation	27	🔍
2.	□	2008-06-19 13:55:54	DEC- 4XXVRGMYN8U...	juventus_ita	↓Conversation	124	🔍
3.	□	2008-06-19 13:37:43	vic	webnetdata2	↓Conversation	19	🔍
4.	□	2008-06-19 12:31:33	vic	webnetdata2	↓Conversation	6	🔍

⏮◀ 1 ▶⏭   Total 4 Total Page 1 Current Page 1

Features in this UT Chat Room GUI:

- UT Chat room: Refresh the page content.
- Delete: Delete the UT Chat Room chat record (that has been checked or ticked).
- Account List: This section shows UT Chat Room Account List. Administrator can download the monthly chat record (in Excel format) and search for the chat record as shown below
- Search: Search for UT Chat Room record based on the specified parameters such as Date, Time, IP, User Handle, Participants and Account
- Every Page 5 Confirm Display the number of record per page.
- □ Checkbox: Check or tick the checkbox for deleting.
- ↓ Download: Download the UT Chat Room chat record.
- Conversation: Click on Conversation to view the chat content.
- 🔍 Similar Search: Search for chat record with similar content.

Sample Conversation:



Date-Time : | User Handle :   Every Page : 5 Confirm

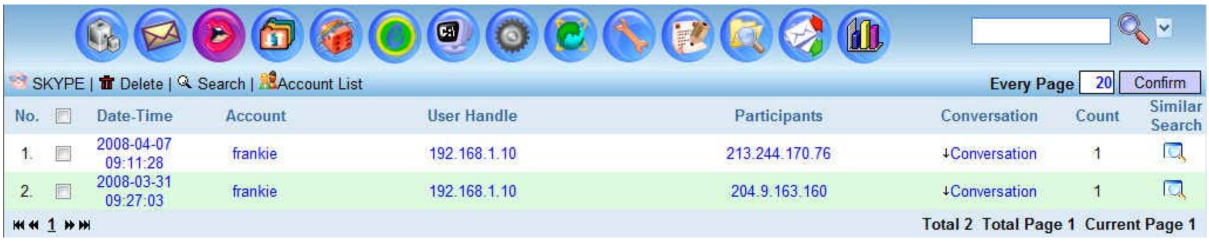
Date-Time	User Handle	Message
2007-11-28 12:03:10	48518856	great to see
2007-11-28 12:03:16	4785	how r u?
2007-11-28 12:03:16	2636	i hope u r fine
2007-11-28 12:03:16	5185	thanks
2007-11-28 12:03:16	78526	u online too..

⏮◀ 1 2 3 4 5 6 7 ▶⏭   Total 33 Total Page 7 Current Page 2

Skype *

Skype (Voice Call Log) obtainable information includes Date-Time, account (with IP/MAC), User Handle (user IP), Participants (peer IP), Conversation (with Voice Call Duration Information) and count. User can also purchase optional Skype Text Chat Message and Voice Recording Module (Skype Sniffer Agent for Skype version 4.2 and below). This add on module can record Skype Text Chat Message by manually installing an Agent software on targeted user PC.

* Skype Sniffer Agent for Content Capturing License sold separately



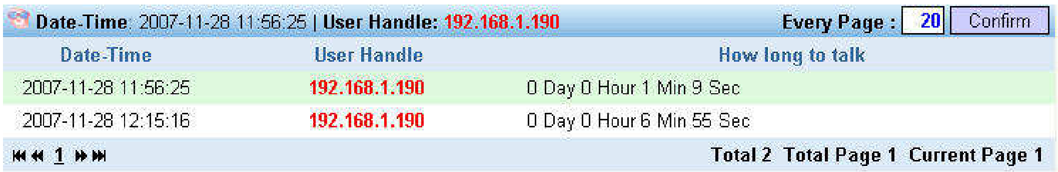
No.	☐	Date-Time	Account	User Handle	Participants	Conversation	Count	Similar Search
1.	☐	2008-04-07 09:11:28	frankie	192.168.1.10	213.244.170.76	↓Conversation	1	🔍
2.	☐	2008-03-31 09:27:03	frankie	192.168.1.10	204.9.163.160	↓Conversation	1	🔍

⏮⏪ 1 ⏩⏭ Total 2 Total Page 1 Current Page 1

Features in this Skype GUI:

- Skype: Refresh the page content.
- Delete: Delete the Skype chat record (that has been checked or ticked).
- Account List: This section shows Skype Account List. Administrator can download the monthly chat record (in Excel format) and search for the chat record as shown below
- Search: Search for QQ record based on the specified parameters such as Date, Time, IP, User Handle, Participants and Account
- Every Page 5 Confirm Display the number of record per page.
- ☐ Checkbox: Check or tick the checkbox for deleting.
- ↓ Download: Download the Skype chat record
- Conversation: Click on Conversation to view the Skype Voice Call details
- 🔍 Similar Search: Search for chat record with similar content.

Conversation Sample:



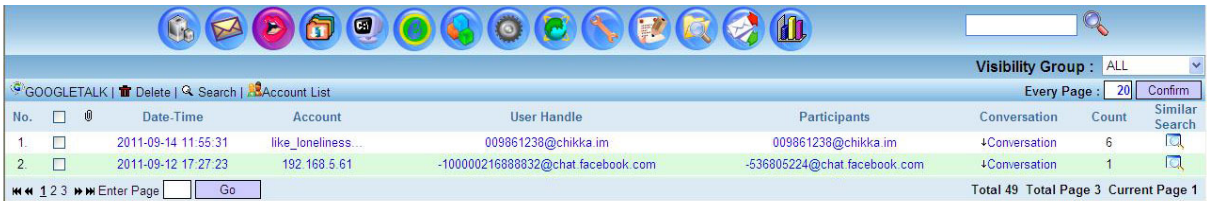
Date-Time: 2007-11-28 11:56:25 | User Handle: 192.168.1.190

Date-Time	User Handle	How long to talk
2007-11-28 11:56:25	192.168.1.190	0 Day 0 Hour 1 Min 9 Sec
2007-11-28 12:15:16	192.168.1.190	0 Day 0 Hour 6 Min 55 Sec

⏮⏪ 1 ⏩⏭ Total 2 Total Page 1 Current Page 1

Gtalk (in HTTP Gmail)

Gtalk obtainable information includes Date-Time, Account (with IP/MAC), User Handle (user account), Participant Account, Conversation with content (text and voice call) and count.



Visibility Group : ALL

GOOGLETALK | Delete | Search | Account List — Every Page : 20 Confirm

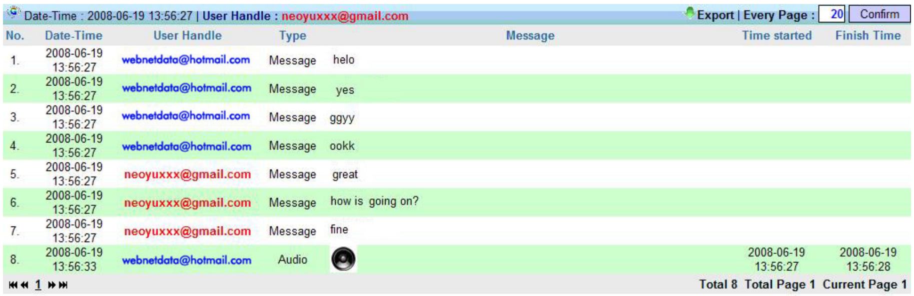
No.	□	📎	Date-Time	Account	User Handle	Participants	Conversation	Count	Similar Search
1.	□		2011-09-14 11:55:31	like_loneliness...	009861238@chikka.im	009861238@chikka.im	↓Conversation	6	🔍
2.	□		2011-09-12 17:27:23	192.168.5.61	-100000216888832@chat.facebook.com	-536805224@chat.facebook.com	↓Conversation	1	🔍

⏮ ⏪ 1 2 3 ⏩ ⏭ Enter Page Go — Total 49 Total Page 3 Current Page 1

Features in this Gtalk GUI:

- GOOGLETALK: Refresh the page content.
- Delete: Delete the Gtalk chat record (that has been checked or ticked).
- Account List: This section shows the Gtalk Account List. Admin can download the monthly chat record (in Excel format) and search for the chat record as shown below
- Search: Search for Gtalk record based on the specified parameters such as Date, Time, IP, User Handle, Participants and Account
- Every Page 5 Confirm Display the number of record per page.
- □ Checkbox: Check or tick the checkbox for deleting.
- 📎 File Transferred: This symbol shows there is file transferred over the Gtalk.
- Friend List: This will show all the friend list for the particular Gtalk account
- ↓ Download: Download the Gtalk chat record.
- Conversation: Click on Conversation to view the chat content.
- 🔍 Similar Search: Search for chat record with similar content

Conversation Sample:



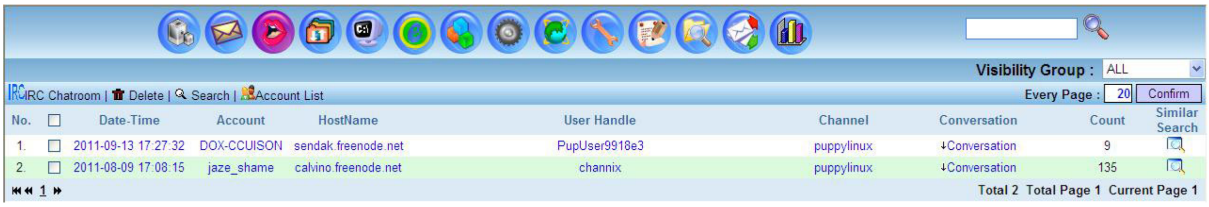
Date-Time : 2008-06-19 13:56:27 | User Handle : neoyuxxx@gmail.com — Export | Every Page : 20 Confirm

No.	Date-Time	User Handle	Type	Message	Time started	Finish Time
1.	2008-06-19 13:56:27	webnetdata@hotmail.com	Message	helo		
2.	2008-06-19 13:56:27	webnetdata@hotmail.com	Message	yes		
3.	2008-06-19 13:56:27	webnetdata@hotmail.com	Message	ggyy		
4.	2008-06-19 13:56:27	webnetdata@hotmail.com	Message	ookk		
5.	2008-06-19 13:56:27	neoyuxxx@gmail.com	Message	great		
6.	2008-06-19 13:56:27	neoyuxxx@gmail.com	Message	how is going on?		
7.	2008-06-19 13:56:27	neoyuxxx@gmail.com	Message	fine		
8.	2008-06-19 13:56:33	webnetdata@hotmail.com	Audio	🔊	2008-06-19 13:56:27	2008-06-19 13:56:28

⏮ ⏪ 1 ⏩ ⏭ — Total 8 Total Page 1 Current Page 1

Internet Relay Chat – IRC

IRC obtainable information includes date-time, account (with IP/MAC), user handle (user account), conversation with content and count.



Visibility Group : ALL

IRC Chatroom | Delete | Search | Account List

Every Page : 20 Confirm

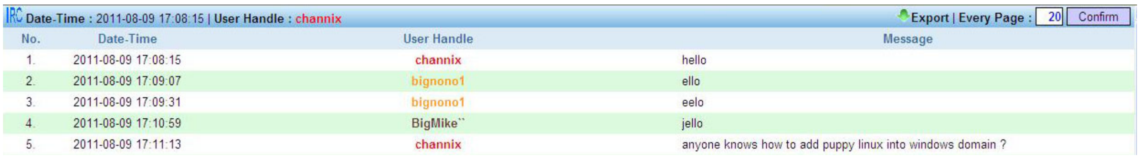
No.	□	Date-Time	Account	HostName	User Handle	Channel	Conversation	Count	Similar Search
1.	□	2011-09-13 17:27:32	DOX-CCUISON	sendak.freenode.net	PupUser9918e3	puppylinux	↓Conversation	9	🔍
2.	□	2011-08-09 17:08:15	jaze_shame	calvino.freenode.net	channix	puppylinux	↓Conversation	135	🔍

⏮ ⏪ 1 ⏩ Total 2 Total Page 1 Current Page 1

Features in this IRC GUI:

- IRC: Refresh the page content.
- Delete: Delete the IRC chat record (that has been checked or ticked)
- Account List: This section shows the IRC Account List. Administrator can download the monthly chat record (in Excel format) and search for the chat record as shown below
- Search: Search for IRC record based on the specified parameters such as Date, Time, IP, User Handle, Participants and Account
- Every Page 5 Confirm Display the number of record per page.
- □ Checkbox: Check or tick the checkbox for deleting.
- ↓ Download: Download the IRC chat record.
- Conversation: Click on Conversation to view the chat content.
- 🔍 Similar Search: Search for chat record with similar content

Sample Conversation:



IRC Date-Time : 2011-08-09 17:08:15 | User Handle : channix

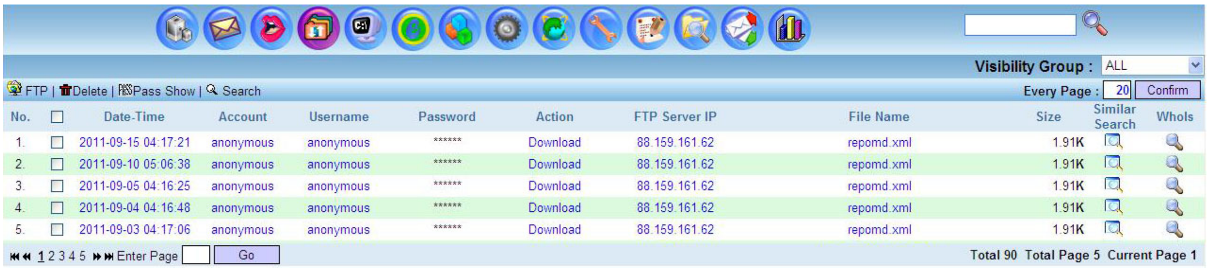
Export | Every Page : 20 Confirm

No.	Date-Time	User Handle	Message
1.	2011-08-09 17:08:15	channix	hello
2.	2011-08-09 17:09:07	bignono1	ello
3.	2011-08-09 17:09:31	bignono1	eelo
4.	2011-08-09 17:10:59	BigMike``	jello
5.	2011-08-09 17:11:13	channix	anyone knows how to add puppy linux into windows domain ?

File Transfer

File Transfer Protocol - FTP

FTP obtainable information includes Date-Time, Account (with IP/MAC), Username, Password, Action (Upload/Download), FTP Server IP, File Name with File Transferred and Whois.



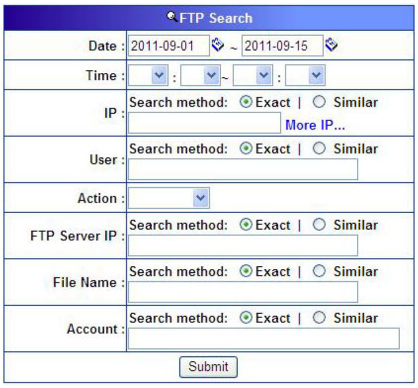
Visibility Group : ALL

FTP | Delete | Pass Show | Search — Every Page : 20 Confirm

No.	□	Date-Time	Account	Username	Password	Action	FTP Server IP	File Name	Size	Similar Search	WhoIs
1.	□	2011-09-15 04:17:21	anonymous	anonymous	******	Download	88.159.161.62	repomd.xml	1.91K		
2.	□	2011-09-10 05:06:38	anonymous	anonymous	******	Download	88.159.161.62	repomd.xml	1.91K		
3.	□	2011-09-05 04:16:25	anonymous	anonymous	******	Download	88.159.161.62	repomd.xml	1.91K		
4.	□	2011-09-04 04:16:48	anonymous	anonymous	******	Download	88.159.161.62	repomd.xml	1.91K		
5.	□	2011-09-03 04:17:06	anonymous	anonymous	******	Download	88.159.161.62	repomd.xml	1.91K		

1 2 3 4 5 Enter Page Go — Total 90 Total Page 5 Current Page 1

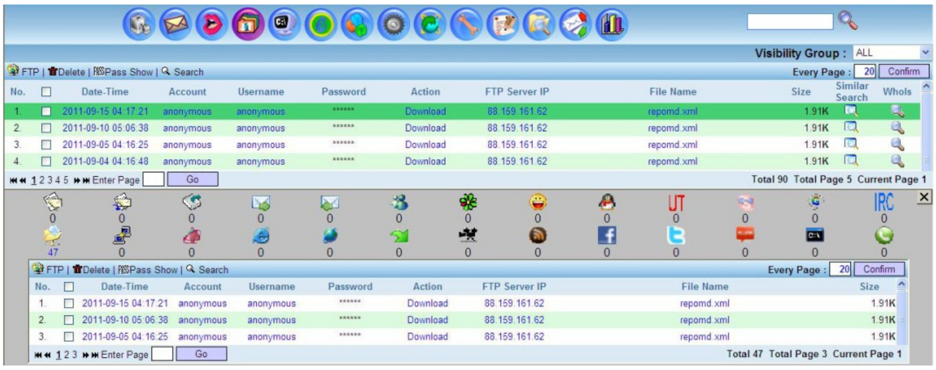
- Features in this FTP GUI:
- FTP: Refresh the page record List.
- Delete: Delete the Email (that has been checked or ticked).
- Pass Show: Display FTP account password.
- Search: Search for FTP record based on the specified parameters such as Date, Time, IP, User, Action, FTP Server IP, File Name and Account.



FTP Search

Date :	2011-09-01 ~ 2011-09-15
Time :	: ~ :
IP :	Search method: ● Exact | ○ Similar More IP...
User :	Search method: ● Exact | ○ Similar
Action :	
FTP Server IP :	Search method: ● Exact | ○ Similar
File Name :	Search method: ● Exact | ○ Similar
Account :	Search method: ● Exact | ○ Similar
	Submit

- Every Page 5 Confirm Display the number of record per page.
- □ Checkbox: Check or tick the checkbox for deleting.
- Similar Search: Search for FTP record with similar content.



Visibility Group : ALL

FTP | Delete | Pass Show | Search — Every Page : 20 Confirm

No.	□	Date-Time	Account	Username	Password	Action	FTP Server IP	File Name	Size	Similar Search	WhoIs
1.	□	2011-09-15 04:17:21	anonymous	anonymous	******	Download	88.159.161.62	repomd.xml	1.91K		
2.	□	2011-09-10 05:06:38	anonymous	anonymous	******	Download	88.159.161.62	repomd.xml	1.91K		
3.	□	2011-09-05 04:16:25	anonymous	anonymous	******	Download	88.159.161.62	repomd.xml	1.91K		
4.	□	2011-09-04 04:16:48	anonymous	anonymous	******	Download	88.159.161.62	repomd.xml	1.91K		

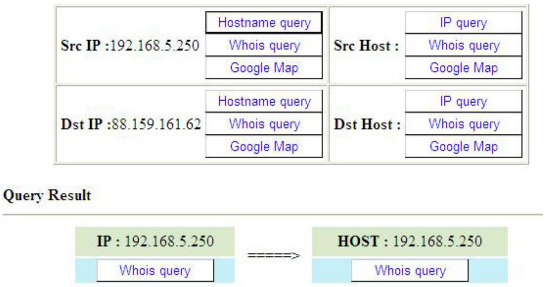
1 2 3 4 5 Enter Page Go — Total 90 Total Page 5 Current Page 1

FTP | Delete | Pass Show | Search — Every Page : 20 Confirm

No.	□	Date-Time	Account	Username	Password	Action	FTP Server IP	File Name	Size
1.	□	2011-09-15 04:17:21	anonymous	anonymous	******	Download	88.159.161.62	repomd.xml	1.91K
2.	□	2011-09-10 05:06:38	anonymous	anonymous	******	Download	88.159.161.62	repomd.xml	1.91K
3.	□	2011-09-05 04:16:25	anonymous	anonymous	******	Download	88.159.161.62	repomd.xml	1.91K

1 2 3 Enter Page Go — Total 47 Total Page 3 Current Page 1

- Whois: Provide information of Source and Destination IP and Hostname. It allows you to search for the IP Address information through the Internet.



Src IP :192.168.5.250

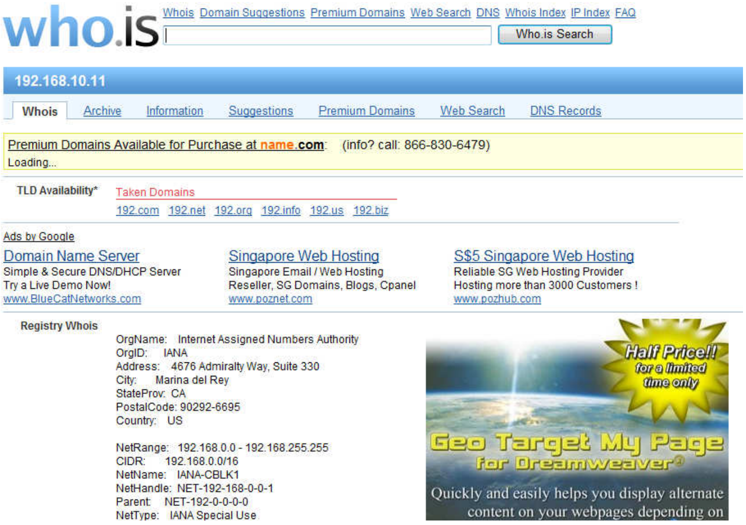
Src Host :

Dst IP :88.159.161.62

Dst Host :

Query Result

IP : 192.168.5.250 =====> HOST : 192.168.5.250



who.is
Whois Domain Suggestions Premium Domains Web Search DNS Whois Index IP Index FAQ
Who.is Search
Whois
Archive
Information
Suggestions
Premium Domains
Web Search
DNS Records
Half Price!! for a limited time only
Geo Target My Page for Dreamweaver®
Quickly and easily helps you display alternate content on your webpages depending on

192.168.10.11

Premium Domains Available for Purchase at name.com: (info? call: 866-830-6479)
Loading...

TLD Availability* Taken Domains
192.com 192.net 192.org 192.info 192.us 192.biz

Ads by Google

Domain Name Server
Simple & Secure DNS/DHCP Server
Try a Live Demo Now!
www.BlueCatNetworks.com

Singapore Web Hosting
Singapore Email / Web Hosting
Reseller, SG Domains, Blogs, Cpanel
www.poznet.com

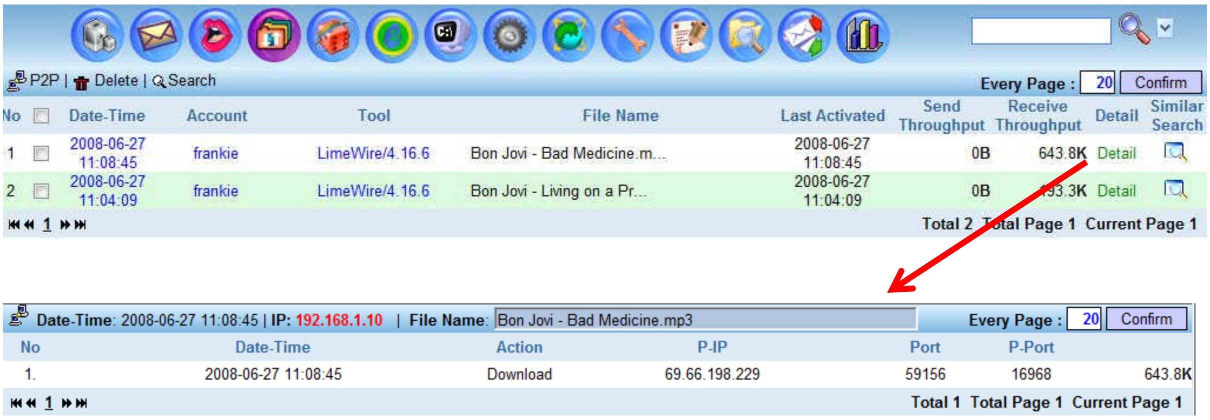
S$5 Singapore Web Hosting
Reliable SG Web Hosting Provider
Hosting more than 3000 Customers !
www.pozhub.com

Registry Whois

```
OrgName:    Internet Assigned Numbers Authority
OrgID:      IANA
Address:    4676 Admiralty Way, Suite 330
City:       Marina del Rey
StateProv:  CA
PostalCode: 90292-6695
Country:    US

NetRange:   192.168.0.0 - 192.168.255.255
CIDR:       192.168.0.0/16
NetName:    IANA-CBLK1
NetHandle:  NET-192-168-0-0-1
Parent:     NET-192-0-0-0-0
NetType:    IANA Special Use
```

Peer to Peer File Sharing – P2P

P2P File Sharing obtainable information includes Date-Time, Account (with IP/MAC), P2P Tool Used, File Name, Last Activated Date-Time, Send Throughput, Received Throughput, Detail (Each Connection Session, Peer IP, Port Used, Peer Port etc.). P2P protocols supported are Bittorent, eMule/eDonkey, Gnutella and Fast track.



P2P | Delete | Search — Every Page : 20 Confirm

No	☐	Date-Time	Account	Tool	File Name	Last Activated	Send Throughput	Receive Throughput	Detail	Similar Search
1	☐	2008-06-27 11:08:45	frankie	LimeWire/4.16.6	Bon Jovi - Bad Medicine.m...	2008-06-27 11:08:45	0B	643.8K	Detail	🔍
2	☐	2008-06-27 11:04:09	frankie	LimeWire/4.16.6	Bon Jovi - Living on a Pr...	2008-06-27 11:04:09	0B	493.3K	Detail	🔍

⏮ ◀ 1 ▶ ⏭ Total 2 Total Page 1 Current Page 1

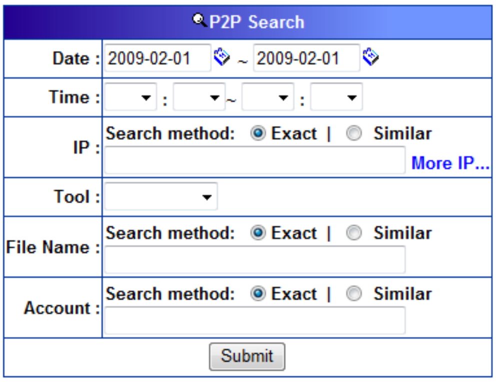
Date-Time: 2008-06-27 11:08:45 | IP: 192.168.1.10 | File Name: Bon Jovi - Bad Medicine.mp3 — Every Page : 20 Confirm

No	Date-Time	Action	P-IP	Port	P-Port	
1.	2008-06-27 11:08:45	Download	69.66.198.229	59156	16968	643.8K

⏮ ◀ 1 ▶ ⏭ Total 1 Total Page 1 Current Page 1

Features in this P2P GUI:

- P2P: Refresh the page content List.
- Delete: Delete the record that is checked (by clicking the Checkbox and Delete button).
- Search: Search the P2P record based on the specified parameters such as Date, Time, IP, Tool, File Name and Account.



P2P Search

Date :	2009-02-01 ~ 2009-02-01
Time :	▾ : ▾ ~ ▾ : ▾
IP :	Search method: ● Exact | ○ Similar More IP...
Tool :	▾
File Name :	Search method: ● Exact | ○ Similar
Account :	Search method: ● Exact | ○ Similar
	Submit

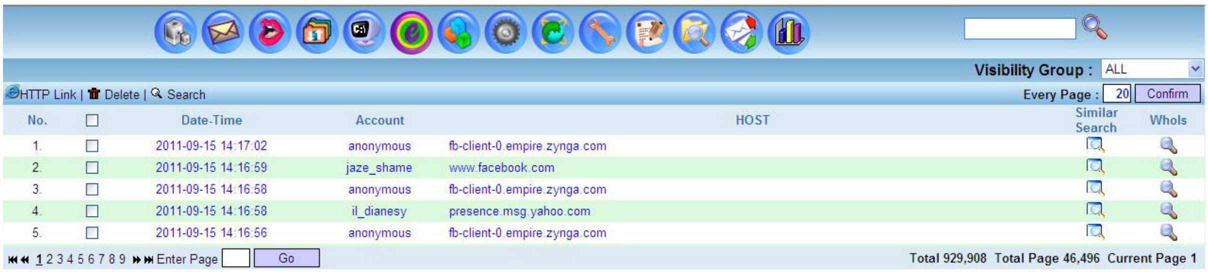
- Every Page 5 Confirm Display the number of record per page.
- ☐ Checkbox: Records can be deleted by checking the Checkbox and Delete button.
- 🔍 Similar Search: Search for P2P record with similar content.

HTTP

When the targeted user surfs the Internet (World Wide Web), ICI system will capture and reconstruct the Web page contents which include HTTP URL Link, HTTP Content and HTTP Reconstruct. ICI system will also reconstruct files upload/download (HTTP Upload/Download) as well as video steam (HTTP Video Stream) such as YouTube, Google Video, Metacafe etc.

HTTP Link

HTTP Link provides information of Web Sites accessed which includes Date-Time, Account (with IP/MAC) and Host (URL/Web Sites Tag). The Web Sites can be accessible by clicking on the URL/Web Sites Tag with connection to the Internet.



Visibility Group : ALL

HTTP Link | Delete | Search

Every Page : 20 Confirm

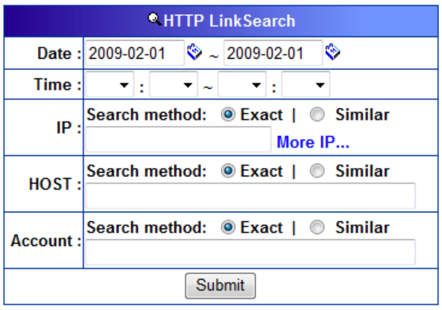
No.	□	Date-Time	Account	HOST	Similar Search	WhoIs
1.	□	2011-09-15 14:17:02	anonymous	fb-client-0.empire.zynga.com	🔍	🔍
2.	□	2011-09-15 14:16:59	jaze_shame	www.facebook.com	🔍	🔍
3.	□	2011-09-15 14:16:58	anonymous	fb-client-0.empire.zynga.com	🔍	🔍
4.	□	2011-09-15 14:16:58	il_dianesy	presence.msg.yahoo.com	🔍	🔍
5.	□	2011-09-15 14:16:56	anonymous	fb-client-0.empire.zynga.com	🔍	🔍

⏮ ◀◀ 1 2 3 4 5 6 7 8 9 ▶▶ ⏭ Enter Page Go

Total 929,908 Total Page 46,496 Current Page 1

Features in this HTTP GUI:

- HTTP Link: Refresh this page content List.
- Delete: Delete the record that is checked.
- Search: Search the HTTP record based on the specified parameters such as Date, Time, IP, Host and Account.



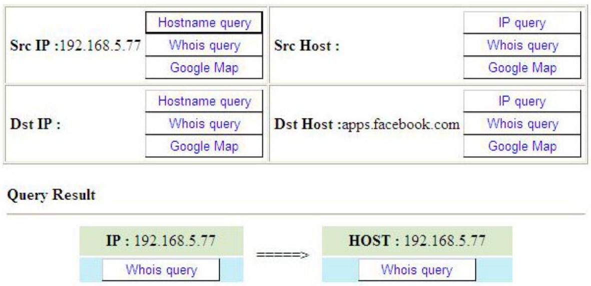
HTTP LinkSearch

Date :	2009-02-01 ~ 2009-02-01
Time :	: ~ :
IP :	Search method: ● Exact | ○ Similar More IP...
HOST :	Search method: ● Exact | ○ Similar
Account :	Search method: ● Exact | ○ Similar

Submit

- Every Page 5 Confirm Display the number of record per page.
- □ Checkbox: Records can be deleted by checking the checkbox.
- 🔍 Similar Search: Search for HTTP Link with similar content.

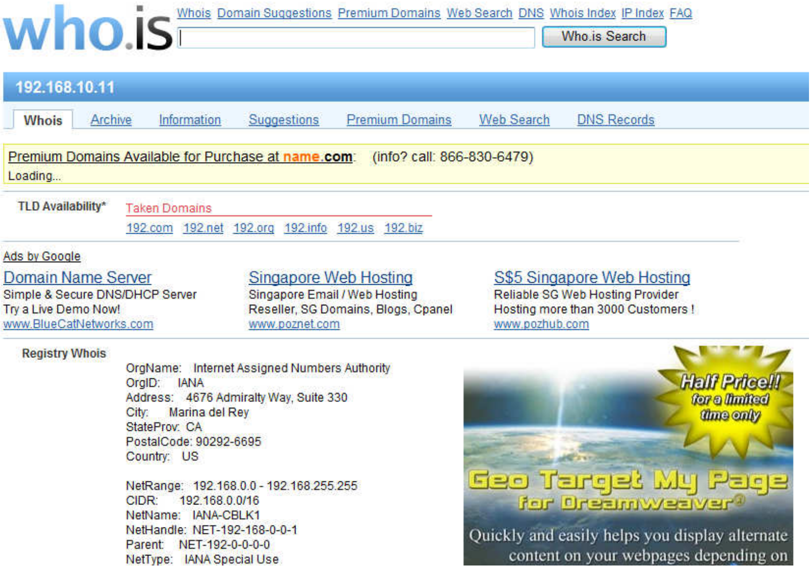
- Whois: Provide information of Source and Destination IP and Hostname. Allows you to search for the IP Address information through the Internet.



Src IP : 192.168.5.77	Hostname query Whois query Google Map	**Src Host :**	IP query Whois query Google Map
Dst IP :	Hostname query Whois query Google Map	**Dst Host :** apps.facebook.com	IP query Whois query Google Map

Query Result

IP : 192.168.5.77 =====> **HOST :** 192.168.5.77



who.is
Whois Domain Suggestions Premium Domains Web Search DNS Whois Index IP Index FAQ
Who.is Search

192.168.10.11

Whois Archive Information Suggestions Premium Domains Web Search DNS Records

Premium Domains Available for Purchase at name.com: (info? call: 866-830-6479)
Loading...

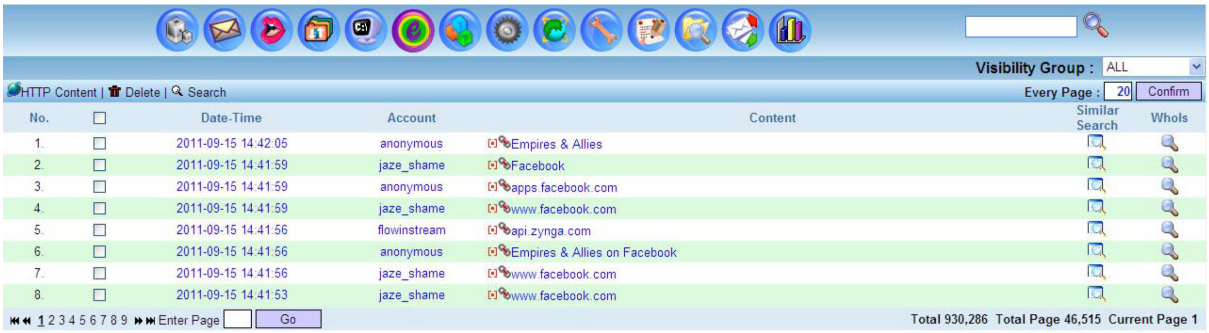
TLD Availability* Taken Domains
192.com 192.net 192.org 192.info 192.us 192.biz

Registry Whois

```
OrgName:    Internet Assigned Numbers Authority
OrgID:      IANA
Address:    4676 Admiralty Way, Suite 330
City:       Marina del Rey
StateProv:  CA
PostalCode: 90292-6695
Country:    US

NetRange:   192.168.0.0 - 192.168.255.255
CIDR:       192.168.0.0/16
NetName:    IANA-CBLK1
NetHandle:  NET-192-168-0-0-1
Parent:     NET-192-0-0-0-0
NetType:    IANA Special Use
```

HTTP Content

HTTP Content obtainable information includes Date-Time, Account (with IP/MAC), URL/Web Sites Tag with Web Pages Content (consists of html text, java script, flash etc. of the web sites browsed).



Visibility Group : ALL

HTTP Content | Delete | Search

Every Page : 20 Confirm

No.	□	Date-Time	Account	Content	Similar Search	WhoIs
1.	□	2011-09-15 14:42:05	anonymous	[•] Empires & Allies		
2.	□	2011-09-15 14:41:59	jaze_shame	[•] Facebook		
3.	□	2011-09-15 14:41:59	anonymous	[•] apps.facebook.com		
4.	□	2011-09-15 14:41:59	jaze_shame	[•] www.facebook.com		
5.	□	2011-09-15 14:41:56	flowinstream	[•] api.zynga.com		
6.	□	2011-09-15 14:41:56	anonymous	[•] Empires & Allies on Facebook		
7.	□	2011-09-15 14:41:56	jaze_shame	[•] www.facebook.com		
8.	□	2011-09-15 14:41:53	jaze_shame	[•] www.facebook.com		

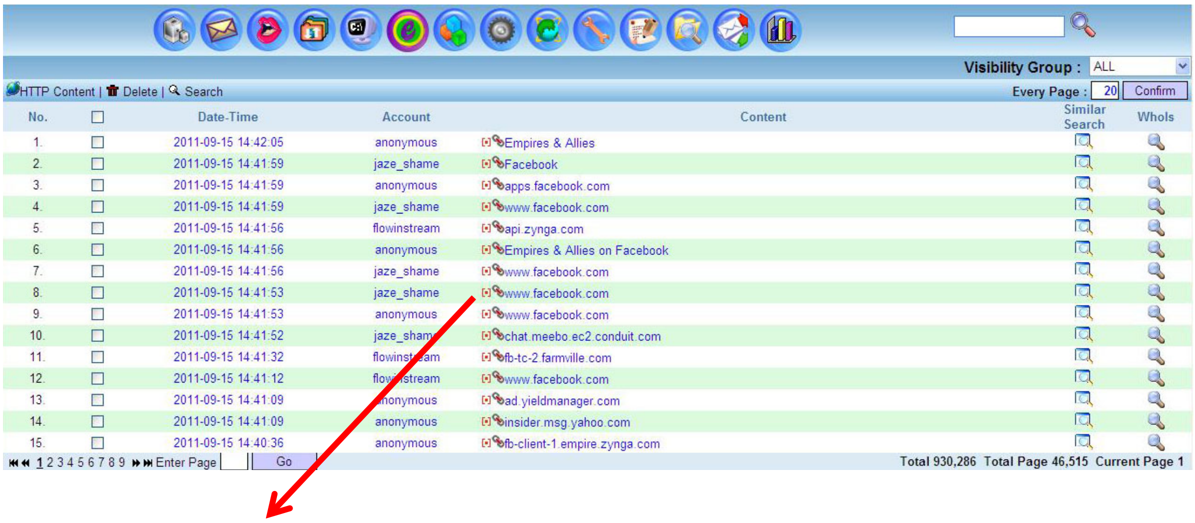
1 2 3 4 5 6 7 8 9 Enter Page Go

Total 930,286 Total Page 46,515 Current Page 1

Features in this HTTP Content GUI:

- HTTP Content: Click on to refresh the content List.
- Delete: Delete record which is checked.
- Search: Search HTTP Content record based on the specified parameters such as Date, Time, IP, Content and Account
- Every Page 5 Confirm Display the number of record per page.
- □ Checkbox: Records can be deleted by checking the Checkbox.
- [•] Source Code: Click on the red icon to view the source codes.
- Link: Open the URL link and access the Website.
- Similar Search: Search for HTTP Link with similar content
- Whois: Provide information of Source and Destination IP and Hostname. It allows you to search for the IP Address information through the Internet

Source Code: **[•]**
When click on , the following UI will pop up to display the source code of webpage.



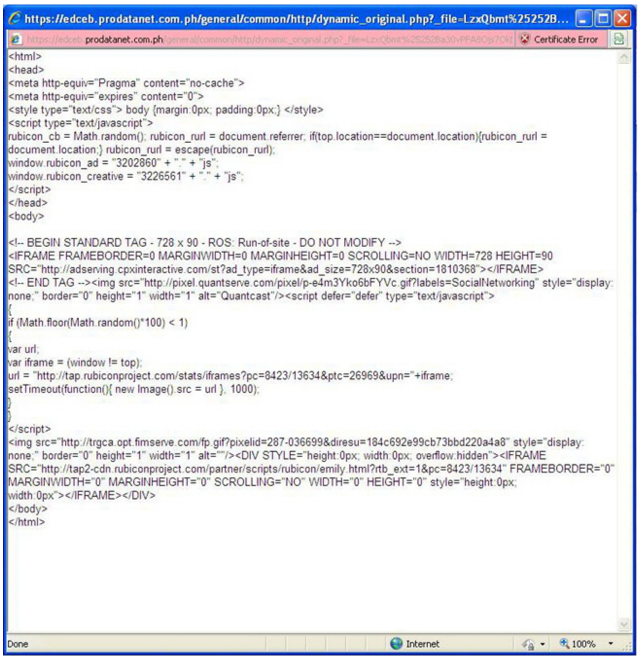
Visibility Group : ALL

Every Page : 20

No.	□	Date-Time	Account	Content	Similar Search	WhoIs
1.	□	2011-09-15 14:42:05	anonymous	Empires & Allies		
2.	□	2011-09-15 14:41:59	jaze_shame	Facebook		
3.	□	2011-09-15 14:41:59	anonymous	apps.facebook.com		
4.	□	2011-09-15 14:41:59	jaze_shame	www.facebook.com		
5.	□	2011-09-15 14:41:56	flowinstream	api.zynga.com		
6.	□	2011-09-15 14:41:56	anonymous	Empires & Allies on Facebook		
7.	□	2011-09-15 14:41:56	jaze_shame	www.facebook.com		
8.	□	2011-09-15 14:41:53	jaze_shame	www.facebook.com		
9.	□	2011-09-15 14:41:53	anonymous	www.facebook.com		
10.	□	2011-09-15 14:41:52	jaze_shame	chat.meebo.ec2.conduit.com		
11.	□	2011-09-15 14:41:32	flowinstream	fb-tc-2.farmville.com		
12.	□	2011-09-15 14:41:12	flowinstream	www.facebook.com		
13.	□	2011-09-15 14:41:09	anonymous	ad.yieldmanager.com		
14.	□	2011-09-15 14:41:09	anonymous	insider.msg.yahoo.com		
15.	□	2011-09-15 14:40:36	anonymous	fb-client-1.empire.zynga.com		

1 2 3 4 5 6 7 8 9 Enter Page

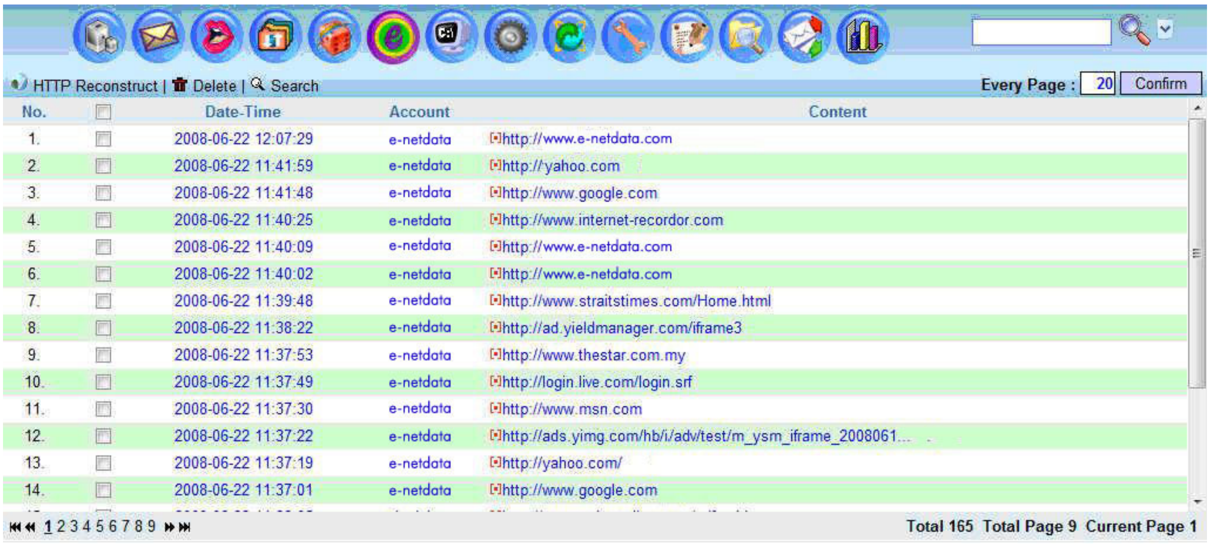
Total 930,286 Total Page 46,515 Current Page 1


https://edceb.prodatanet.com.ph/general/common/http/dynamic_original.php?_file=LzxQbmt%25252B...
https://edceb.prodatanet.com.ph/general/common/http/dynamic_original.php?_file=LzxQbmt%25252Ba30vPFA8Ojs7Ok
Certificate Error
Done
Internet
100%

```
<html>
<head>
<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="expires" content="0">
<style type="text/css"> body {margin:0px; padding:0px;} </style>
<script type="text/javascript">
rubicon_cb = Math.random(); rubicon_rurl = document.referrer; if(top.location==document.location){rubicon_rurl =
document.location;} rubicon_rurl = escape(rubicon_rurl);
window.rubicon_ad = "3202860" + "." + "js";
window.rubicon_creative = "3226561" + "." + "js";
</script>
</head>
<body>

<!-- BEGIN STANDARD TAG - 728 x 90 - ROS: Run-of-site - DO NOT MODIFY -->
<IFRAME FRAMEBORDER=0 MARGINWIDTH=0 MARGINHEIGHT=0 SCROLLING=NO WIDTH=728 HEIGHT=90
SRC="http://adserving.cpxinteractive.com/st?ad_type=iframe&ad_size=728x90&section=1810368"></IFRAME>
<!-- END TAG --><img src="http://pixel.quantserve.com/pixel/p-e4m3Yko6bFYVc.gif?labels=SocialNetworking" style="display:
none;" border="0" height="1" width="1" alt="Quantcast"/><script defer="defer" type="text/javascript">
{
if (Math.floor(Math.random()*100) < 1)
{
var url;
var iframe = (window != top);
url = "http://tap.rubiconproject.com/stats/iframes?pc=8423/13634&ptc=26969&upn="+iframe;
setTimeout(function(){ new Image().src = url }, 1000);
}
}
</script>
<img src="http://trgca.opt.fimserve.com/fp.gif?pixelid=287-036699&diresu=184c692e99cb73bbd220a4a8" style="display:
none;" border="0" height="1" width="1" alt=""/><DIV STYLE="height:0px; width:0px; overflow:hidden"><IFRAME
SRC="http://tap2-cdn.rubiconproject.com/partner/scripts/rubicon/emily.html?rtb_ext=1&pc=8423/13634" FRAMEBORDER="0"
MARGINWIDTH="0" MARGINHEIGHT="0" SCROLLING="NO" WIDTH="0" HEIGHT="0" style="height:0px;
width:0px"></IFRAME></DIV>
</body>
</html>
```

HTTP Reconstruct

HTTP Reconstruct function will rebuild/reconstruct the entire web page that has been browsed by users. The obtainable information includes Date-Time, Account (with IP/MAC) and HTTP Web Page reconstructed content.



HTTP Reconstruct | Delete | Search

Every Page : 20 Confirm

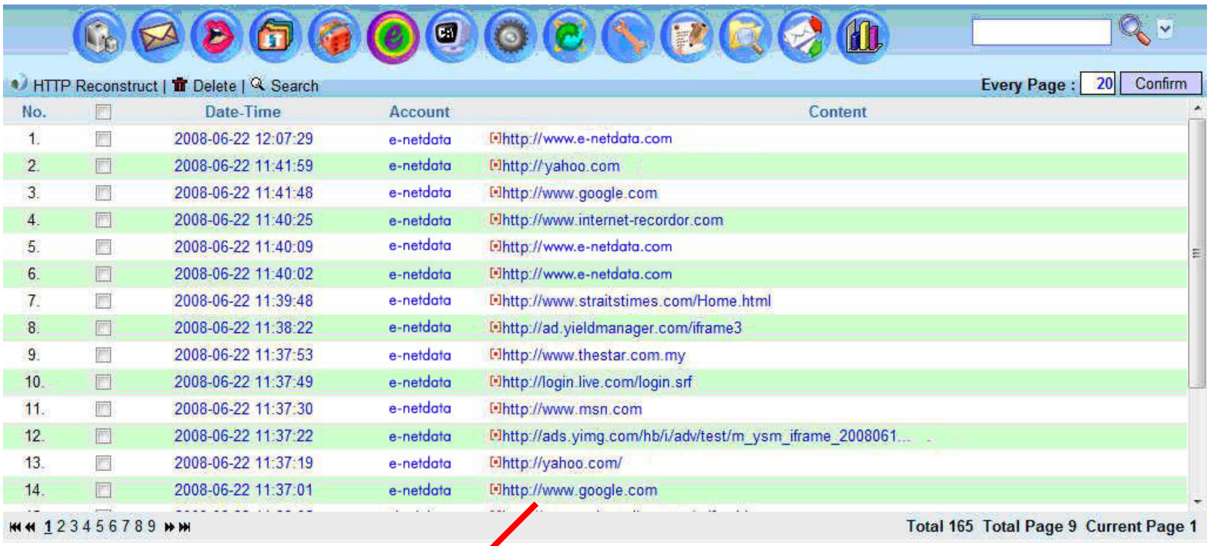
No.	□	Date-Time	Account	Content
1.	□	2008-06-22 12:07:29	e-netdata	[•]http://www.e-netdata.com
2.	□	2008-06-22 11:41:59	e-netdata	[•]http://yahoo.com
3.	□	2008-06-22 11:41:48	e-netdata	[•]http://www.google.com
4.	□	2008-06-22 11:40:25	e-netdata	[•]http://www.internet-recordor.com
5.	□	2008-06-22 11:40:09	e-netdata	[•]http://www.e-netdata.com
6.	□	2008-06-22 11:40:02	e-netdata	[•]http://www.e-netdata.com
7.	□	2008-06-22 11:39:48	e-netdata	[•]http://www.straitstimes.com/Home.html
8.	□	2008-06-22 11:38:22	e-netdata	[•]http://ad.yieldmanager.com/iframe3
9.	□	2008-06-22 11:37:53	e-netdata	[•]http://www.thestar.com.my
10.	□	2008-06-22 11:37:49	e-netdata	[•]http://login.live.com/login.srf
11.	□	2008-06-22 11:37:30	e-netdata	[•]http://www.msn.com
12.	□	2008-06-22 11:37:22	e-netdata	[•]http://ads.yimg.com/hb/i/adv/test/m_ysm_iframe_2008061...
13.	□	2008-06-22 11:37:19	e-netdata	[•]http://yahoo.com/
14.	□	2008-06-22 11:37:01	e-netdata	[•]http://www.google.com

⏮ ⏪ 1 2 3 4 5 6 7 8 9 ⏩ ⏭ Total 165 Total Page 9 Current Page 1

Features in this HTTP Reconstruct GUI:

- HTTP Reconstruct: Click on to refresh the page content List
- Delete: Delete record which is checked
- Search: Search the particular records based on the specified parameters such as Date, Time, IP, URL and ID
- Display Mode: Display either IP or computer (PC) name on this UI
- Every Page 5 Confirm Display records per page. Input the number and click on the confirm button to set up
- □ Checkbox: Records can be deleted by checking the Checkbox.
- [•] Source Code: Click on the red icon to view the source codes.

Sample Reconstructed Web Page

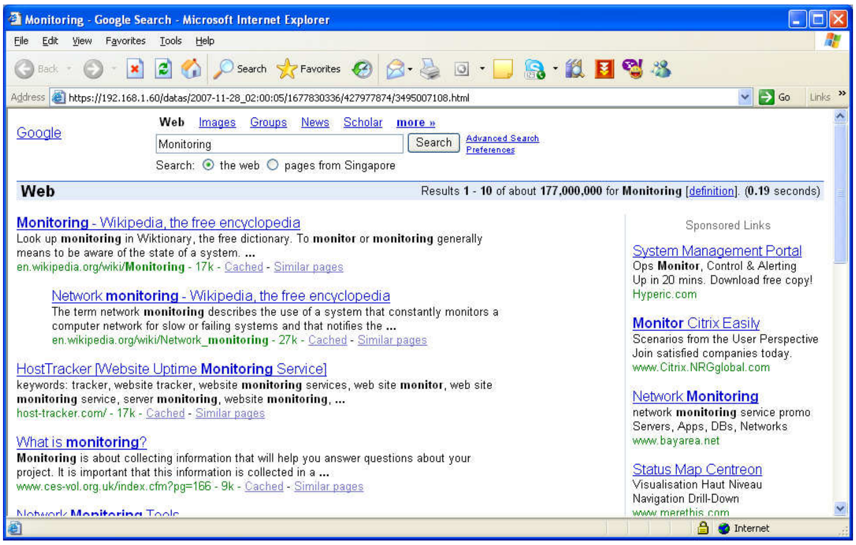


HTTP Reconstruct | Delete | Search

Every Page : 20 Confirm

No.	□	Date-Time	Account	Content
1.	□	2008-06-22 12:07:29	e-netdata	http://www.e-netdata.com
2.	□	2008-06-22 11:41:59	e-netdata	http://yahoo.com
3.	□	2008-06-22 11:41:48	e-netdata	http://www.google.com
4.	□	2008-06-22 11:40:25	e-netdata	http://www.internet-recordor.com
5.	□	2008-06-22 11:40:09	e-netdata	http://www.e-netdata.com
6.	□	2008-06-22 11:40:02	e-netdata	http://www.e-netdata.com
7.	□	2008-06-22 11:39:48	e-netdata	http://www.straitstimes.com/Home.html
8.	□	2008-06-22 11:38:22	e-netdata	http://ad.yieldmanager.com/iframe3
9.	□	2008-06-22 11:37:53	e-netdata	http://www.thestar.com.my
10.	□	2008-06-22 11:37:49	e-netdata	http://login.live.com/login.srf
11.	□	2008-06-22 11:37:30	e-netdata	http://www.msn.com
12.	□	2008-06-22 11:37:22	e-netdata	http://ads.yimg.com/hb/i/adv/test/m_ysm_iframe_2008061...
13.	□	2008-06-22 11:37:19	e-netdata	http://yahoo.com/
14.	□	2008-06-22 11:37:01	e-netdata	http://www.google.com

1 2 3 4 5 6 7 8 9 Total 165 Total Page 9 Current Page 1



Monitoring - Google Search - Microsoft Internet Explorer

Address https://192.168.1.60/datas/2007-11-28_02:00:05/1677830336/427977874/3495007108.html

File Edit View Favorites Tools Help
Back
Search
Favorites
Go
Links
Google
Web Images Groups News Scholar more »
Search
Advanced Search
Preferences

Monitoring

Search: ● the web ○ pages from Singapore

Web Results **1** - **10** of about **177,000,000** for **Monitoring** [definition]. (**0.19** seconds)

Monitoring - Wikipedia, the free encyclopedia
Look up **monitoring** in Wiktionary, the free dictionary. To **monitor** or **monitoring** generally means to be aware of the state of a system. **...**
en.wikipedia.org/wiki/**Monitoring** - 17k - Cached - Similar pages

Network **monitoring** - Wikipedia, the free encyclopedia
The term network **monitoring** describes the use of a system that constantly monitors a computer network for slow or failing systems and that notifies the **...**
en.wikipedia.org/wiki/Network_**monitoring** - 27k - Cached - Similar pages

HostTracker [Website Uptime **Monitoring** Service]
keywords: tracker, website tracker, website **monitoring** services, web site **monitor**, web site **monitoring** service, server **monitoring**, website **monitoring**, **...**
host-tracker.com/ - 17k - Cached - Similar pages

What is **monitoring**?
Monitoring is about collecting information that will help you answer questions about your project. It is important that this information is collected in a **...**
www.ces-vol.org.uk/index.cfm?pg=166 - 9k - Cached - Similar pages

Network **Monitoring** Tools

Sponsored Links

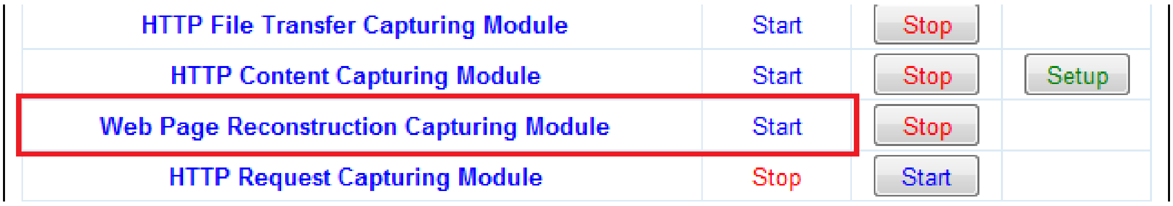
System Management Portal
Ops **Monitor**, Control & Alerting
Up in 20 mins. Download free copy!
Hyperic.com

Monitor Citrix Easily
Scenarios from the User Perspective
Join satisfied companies today.
www.Citrix.NRGglobal.com

Network **Monitoring**
network **monitoring** service promo
Servers, Apps, DBs, Networks
www.bayarea.net

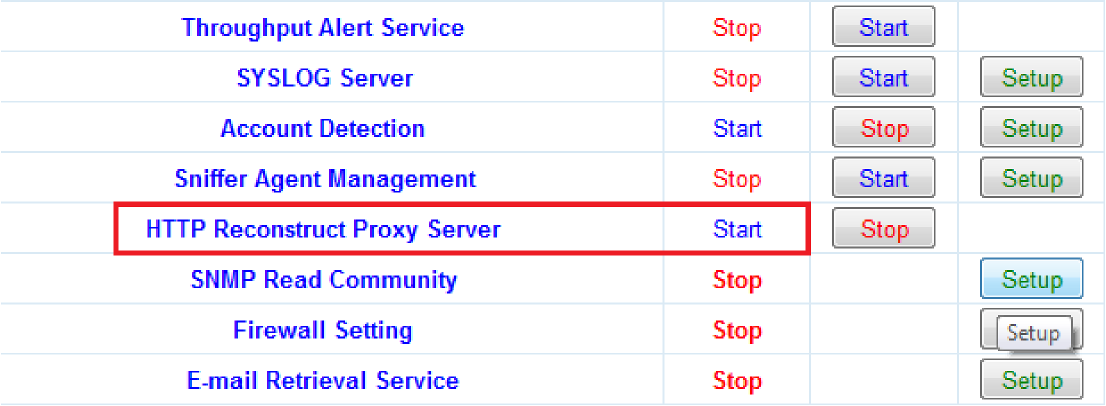
Status Map Centreon
Visualisation Haut Niveau
Navigation Drill-Down
www.merethis.com

Note:
To view the reconstructed content, firstly, you are required to turn on Web Page Reconstruction Capturing Module.



HTTP File Transfer Capturing Module	Start	Stop	
HTTP Content Capturing Module	Start	Stop	Setup
Web Page Reconstruction Capturing Module	Start	Stop	
HTTP Request Capturing Module	Stop	Start	

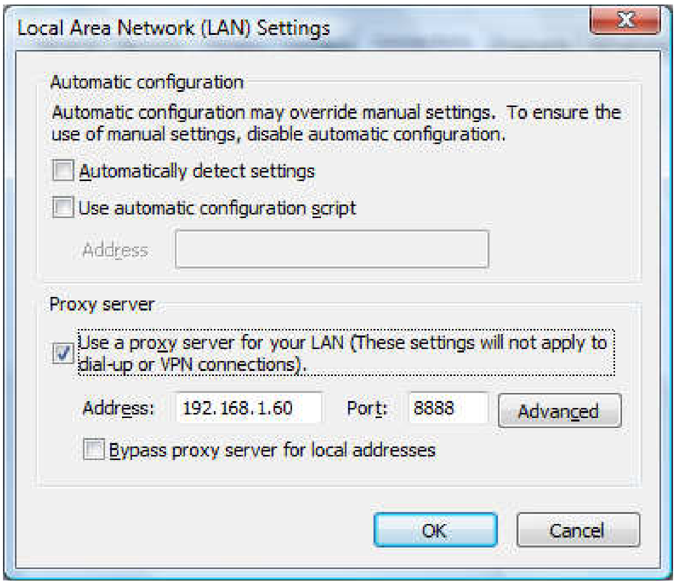
Then, you are required to start HTTP Reconstruct Proxy Server as the HTTP Reconstruct in ED2-1.15.0 has been upgraded to use Proxy Service.



Throughput Alert Service	Stop	Start	
SYSLOG Server	Stop	Start	Setup
Account Detection	Start	Stop	Setup
Sniffer Agent Management	Stop	Start	Setup
HTTP Reconstruct Proxy Server	Start	Stop	
SNMP Read Community	Stop		Setup
Firewall Setting	Stop		Setup
E-mail Retrieval Service	Stop		Setup

You are also required to set your web browser configuration to access from by following proxy setting:

- Proxy Address: IP Address of the ICI system, ex: 192.168.1.60
- Port: 8888



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

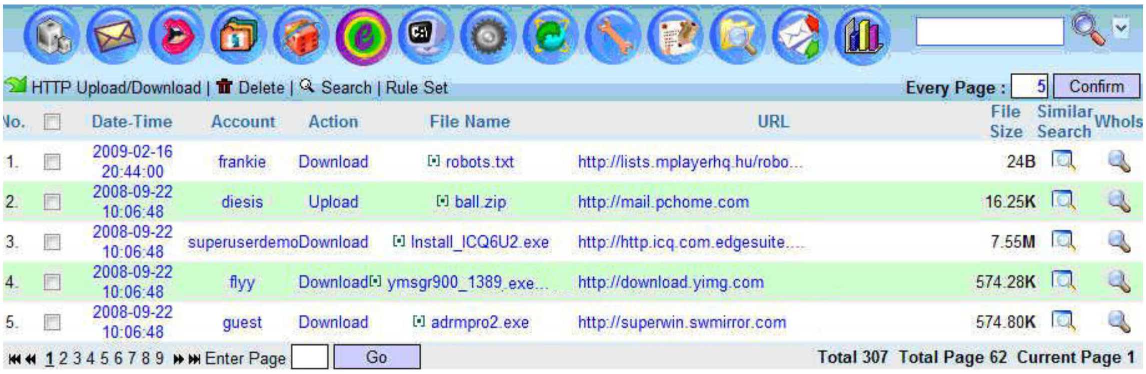
Address: 192.168.1.60 Port: 8888

□ Bypass proxy server for local addresses

With the above setting, you will be able to click on the link on the HTTP Reconstruct and view the reconstructed web page content.

HTTP Upload/Download

HTTP Upload/Download obtainable information includes Date-Time, Account (with IP/MAC), Action (Upload/Download), File Name (with actual file content) and Upload/Download URL Link, Whois etc.



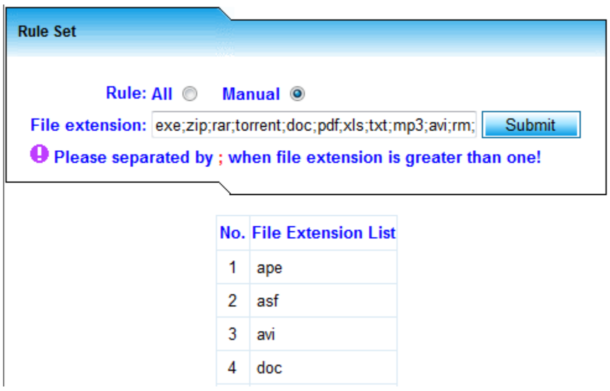
HTTP Upload/Download | Delete | Search | Rule Set   Every Page : 5 Confirm

No.	□	Date-Time	Account	Action	File Name	URL	File Size	Similar Search	WhoIs
1.	□	2009-02-16 20:44:00	frankie	Download	robots.txt	http://lists.mplayerhq.hu/robo...	24B	🔍	🔍
2.	□	2008-09-22 10:06:48	diesis	Upload	ball.zip	http://mail.pchome.com	16.25K	🔍	🔍
3.	□	2008-09-22 10:06:48	superuserdemo	Download	Install_ICQ6U2.exe	http://http.icq.com.edgesuite....	7.55M	🔍	🔍
4.	□	2008-09-22 10:06:48	flyy	Download	ymsgr900_1389.exe...	http://download.yimg.com	574.28K	🔍	🔍
5.	□	2008-09-22 10:06:48	guest	Download	adrmpro2.exe	http://superwin.swmirror.com	574.80K	🔍	🔍

1 2 3 4 5 6 7 8 9 Enter Page Go   Total 307 Total Page 62 Current Page 1

Features in this HTTP Upload/Download GUI

- HTTP Download/Upload: Click on to refresh the page content List
- Delete: Delete record which is checked and ticked
- Search: Search the particular records based on the specified parameters such as Date, Time, IP, File Name and Account
- Rule Set: Define the file extension which the system reconstructs. There are two settings: Reconstruct All or Set Manually. Administrator can opt to enter the specific file extension by select Manual option.



Rule Set

Rule: All ○ Manual ●

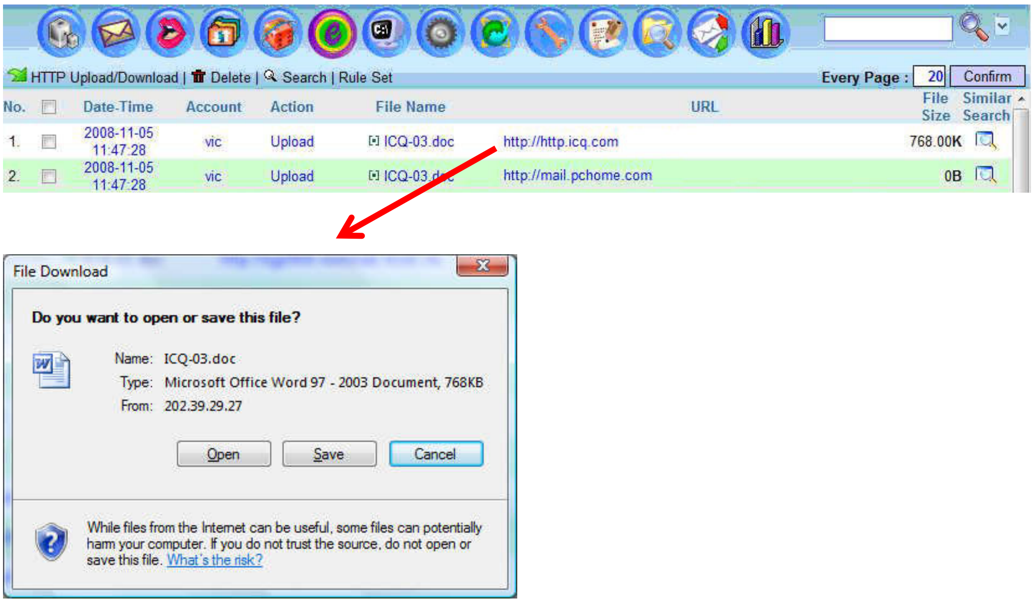
File extension: exe;zip;rar;torrent;doc;pdf;xls;txt;mp3;avi;rm; Submit

Please separated by ; when file extension is greater than one!

No.	File Extension List
1	ape
2	asf
3	avi
4	doc

- Every Page 5 Confirm Display records per page. Input the number and click on the confirm button to set up
- □ Checkbox: Records can be deleted by checking the Checkbox
- 🔍 Similar Search: Search for HTTP Link with similar file name or link
- 🔍 Whois: Provide information of Source and Destination IP and Hostname. It allows you to search for the IP Address information through the Internet

Sample HTTP Upload/Download



HTTP Upload/Download | Delete | Search | Rule Set

Every Page : 20 Confirm

No.	□	Date-Time	Account	Action	File Name	URL	File Size	Similar Search
1.	□	2008-11-05 11:47:28	vic	Upload	ICQ-03.doc	http://http.icq.com	768.00K	
2.	□	2008-11-05 11:47:28	vic	Upload	ICQ-03.doc	http://mail.pchome.com	0B	

File Download

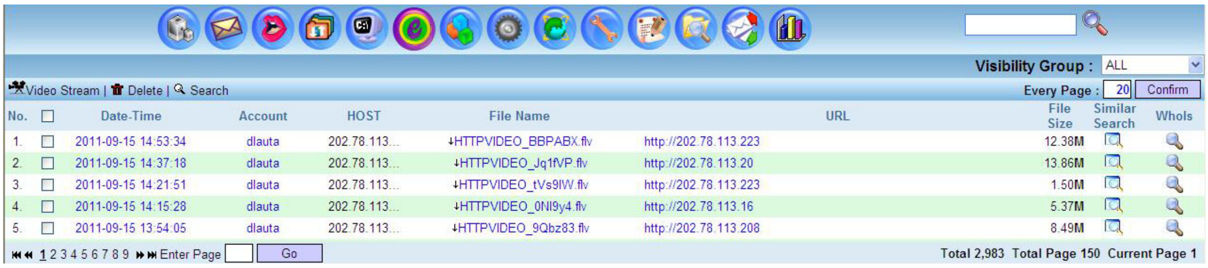
Do you want to open or save this file?

Name: ICQ-03.doc
Type: Microsoft Office Word 97 - 2003 Document, 768KB
From: 202.39.29.27

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

HTTP Video Streaming (FLV Video)

HTTP Video Streaming (FLV Video Format) obtainable information includes Date-Time, Account, Host, File Name, URL link of the video stream and file size. Video Stream supported includes YouTube, Metacafe etc.



Visibility Group : ALL

Every Page : 20 Confirm

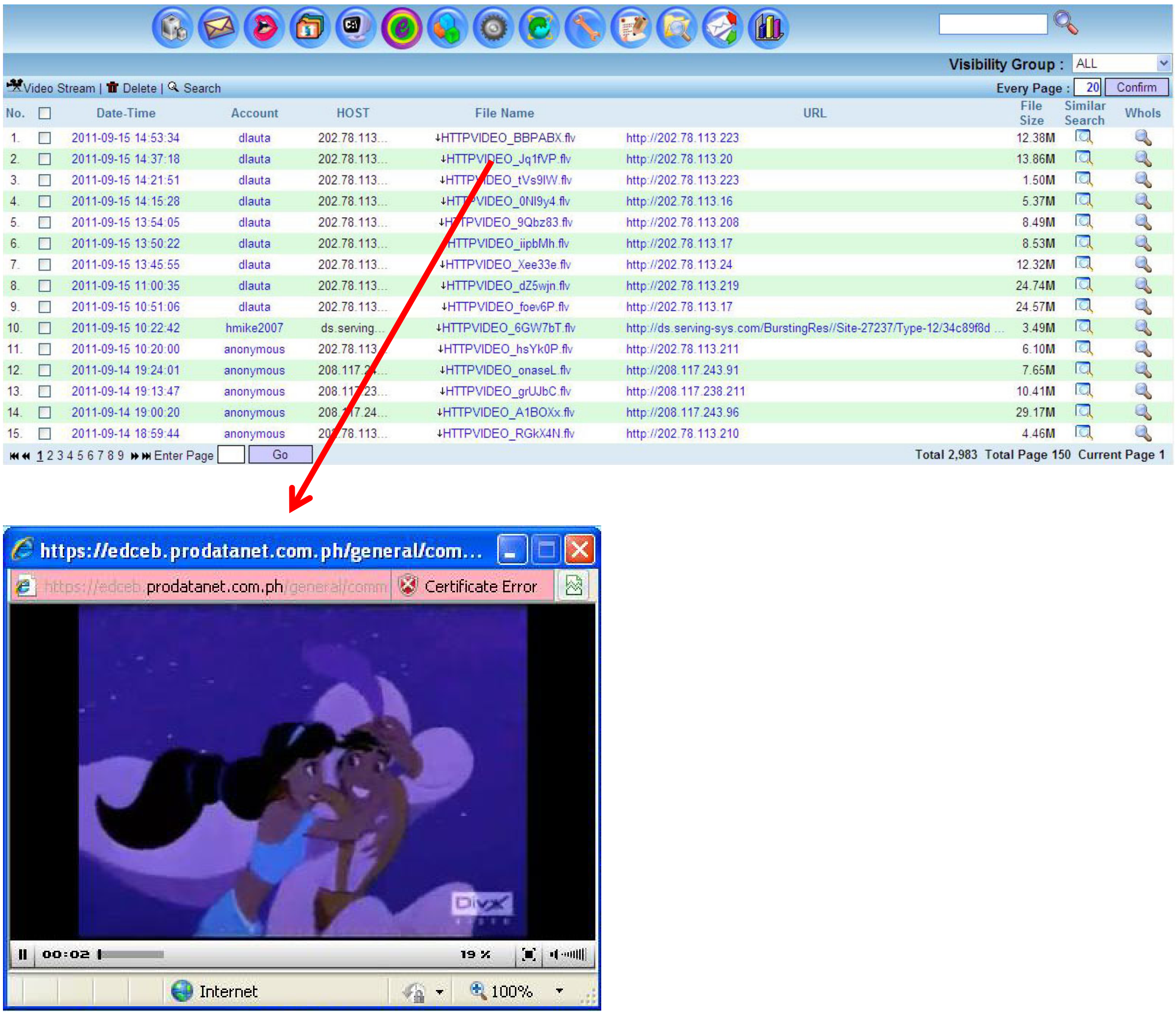
No.	□	Date-Time	Account	HOST	File Name	URL	File Size	Similar Search	WhoIs
1.	□	2011-09-15 14:53:34	dlauta	202.78.113...	↓HTTPVIDEO_BBPABX.flv	http://202.78.113.223	12.38M	🔍	🔍
2.	□	2011-09-15 14:37:18	dlauta	202.78.113...	↓HTTPVIDEO_Jq1fVP.flv	http://202.78.113.20	13.86M	🔍	🔍
3.	□	2011-09-15 14:21:51	dlauta	202.78.113...	↓HTTPVIDEO_tVs9IW.flv	http://202.78.113.223	1.50M	🔍	🔍
4.	□	2011-09-15 14:15:28	dlauta	202.78.113...	↓HTTPVIDEO_0NI9y4.flv	http://202.78.113.16	5.37M	🔍	🔍
5.	□	2011-09-15 13:54:05	dlauta	202.78.113...	↓HTTPVIDEO_9Qbz83.flv	http://202.78.113.208	8.49M	🔍	🔍

Total 2,983 Total Page 150 Current Page 1

Features in this HTTP Video Streaming GUI:

- Video Stream: Click on to refresh the page content List.
- Delete: Delete record which is checked.
- Search: Search the particular records based on the specified parameters such as Date, Time, IP, File Name and Account
- Every Page 5 Confirm Display records per page. Input the number and click on the confirm button to set up
- □ Checkbox: Records can be deleted by checking the Checkbox
- 🔍 Similar Search: Search for HTTP Video with similar file name or link
- 🔍 Whois: Provide information of Source and Destination IP and Hostname. It allows you to search for the IP Address information through the Internet

Sample HTTP Video Stream

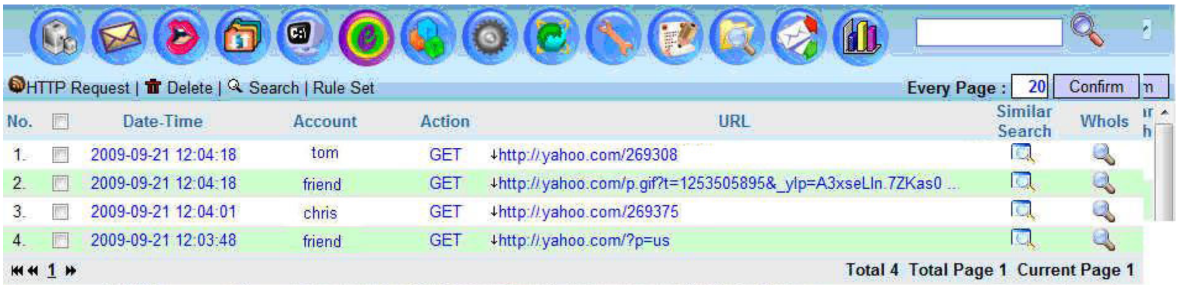


No.	□	Date-Time	Account	HOST	File Name	URL	File Size	Similar Search	WhoIs
1.	□	2011-09-15 14:53:34	dlauta	202.78.113...	↓HTTPVIDEO_BBPABX.flv	http://202.78.113.223	12.38M	🔍	🔍
2.	□	2011-09-15 14:37:18	dlauta	202.78.113...	↓HTTPVIDEO_Jq1fVP.flv	http://202.78.113.20	13.86M	🔍	🔍
3.	□	2011-09-15 14:21:51	dlauta	202.78.113...	↓HTTPVIDEO_tVs9IW.flv	http://202.78.113.223	1.50M	🔍	🔍
4.	□	2011-09-15 14:15:28	dlauta	202.78.113...	↓HTTPVIDEO_0NI9y4.flv	http://202.78.113.16	5.37M	🔍	🔍
5.	□	2011-09-15 13:54:05	dlauta	202.78.113...	↓HTTPVIDEO_9Qbz83.flv	http://202.78.113.208	8.49M	🔍	🔍
6.	□	2011-09-15 13:50:22	dlauta	202.78.113...	↓HTTPVIDEO_iipbMh.flv	http://202.78.113.17	8.53M	🔍	🔍
7.	□	2011-09-15 13:45:55	dlauta	202.78.113...	↓HTTPVIDEO_Xee33e.flv	http://202.78.113.24	12.32M	🔍	🔍
8.	□	2011-09-15 11:00:35	dlauta	202.78.113...	↓HTTPVIDEO_dZ5wjn.flv	http://202.78.113.219	24.74M	🔍	🔍
9.	□	2011-09-15 10:51:06	dlauta	202.78.113...	↓HTTPVIDEO_foev6P.flv	http://202.78.113.17	24.57M	🔍	🔍
10.	□	2011-09-15 10:22:42	hmike2007	ds.serving...	↓HTTPVIDEO_6GW7bT.flv	http://ds.serving-sys.com/BurstingRes//Site-27237/Type-12/34c89f8d ...	3.49M	🔍	🔍
11.	□	2011-09-15 10:20:00	anonymous	202.78.113...	↓HTTPVIDEO_hsYk0P.flv	http://202.78.113.211	6.10M	🔍	🔍
12.	□	2011-09-14 19:24:01	anonymous	208.117.24...	↓HTTPVIDEO_onaseL.flv	http://208.117.243.91	7.65M	🔍	🔍
13.	□	2011-09-14 19:13:47	anonymous	208.117.23...	↓HTTPVIDEO_grUJbC.flv	http://208.117.238.211	10.41M	🔍	🔍
14.	□	2011-09-14 19:00:20	anonymous	208.117.24...	↓HTTPVIDEO_A1BOXx.flv	http://208.117.243.96	29.17M	🔍	🔍
15.	□	2011-09-14 18:59:44	anonymous	202.78.113...	↓HTTPVIDEO_RGkX4N.flv	http://202.78.113.210	4.46M	🔍	🔍

1 2 3 4 5 6 7 8 9 Enter Page Go
Total 2,983 Total Page 150 Current Page 1
https://edceb.prodatanet.com.ph/general/com...
https://edceb.prodatanet.com.ph/general/comm
Certificate Error
00:02
19 %
Internet
100%

HTTP Request

HTTP Request captures pre-defined web pages record such as Host, Content Type, Referrer and other defined Rules or Definitions. The obtainable information includes Date-Time, Account, Action and HTTP Link (URL).



HTTP Request | Delete | Search | Rule Set   Every Page : 20 Confirm

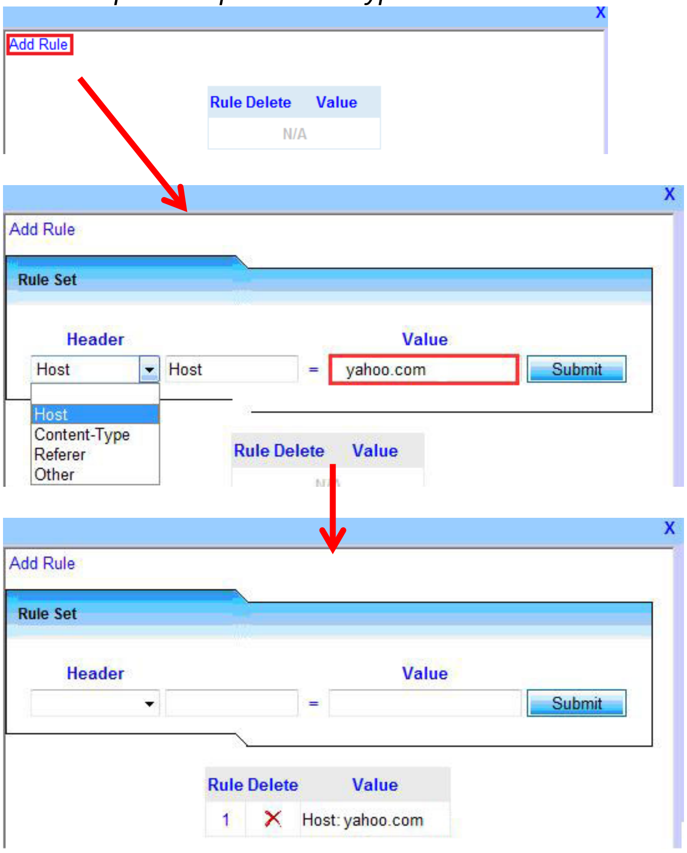
No.	□	Date-Time	Account	Action	URL	Similar Search	WhoIs
1.	□	2009-09-21 12:04:18	tom	GET	↓http://yahoo.com/269308		
2.	□	2009-09-21 12:04:18	friend	GET	↓http://yahoo.com/p.gif?t=1253505895&_ylp=A3xseLln.7ZKas0 ...		
3.	□	2009-09-21 12:04:01	chris	GET	↓http://yahoo.com/269375		
4.	□	2009-09-21 12:03:48	friend	GET	↓http://yahoo.com/?p=us		

1   Total 4 Total Page 1 Current Page 1

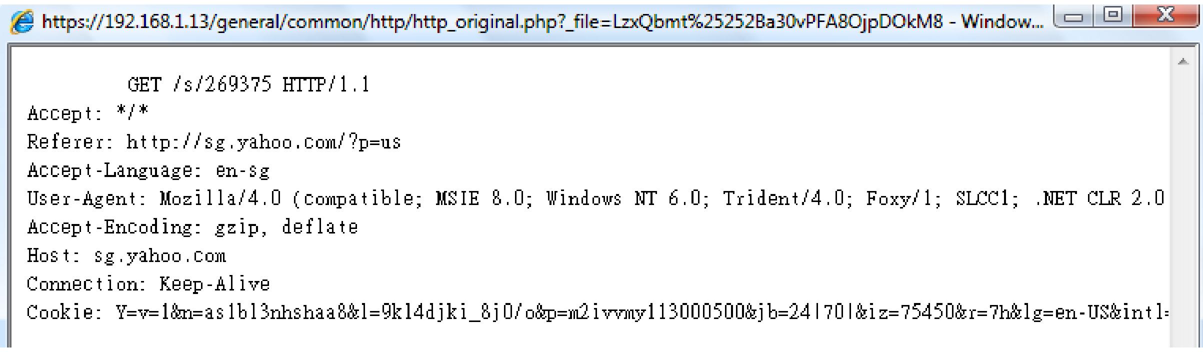
Features in this HTTP Request GUI:

- HTTP Request: Click on to refresh the page content List
- Delete: Delete record which is checked
- Search: Search the particular records based on the specified parameters such as Date, Time, IP and Account
- Every Page : 5 Confirm Display records per page. Input the number and click on the confirm button to set up
- □ Checkbox: Records can be deleted by checking the Checkbox
- Similar Search: Search for HTTP Video Stream with similar file name or link
- Whois: Provide information of Source and Destination IP and Hostname
- Rule Set: Setup and Define HTTP Request Capture Rules and Configuration

For example: Setup the Host Type Value.



Sample HTTP Request Content:

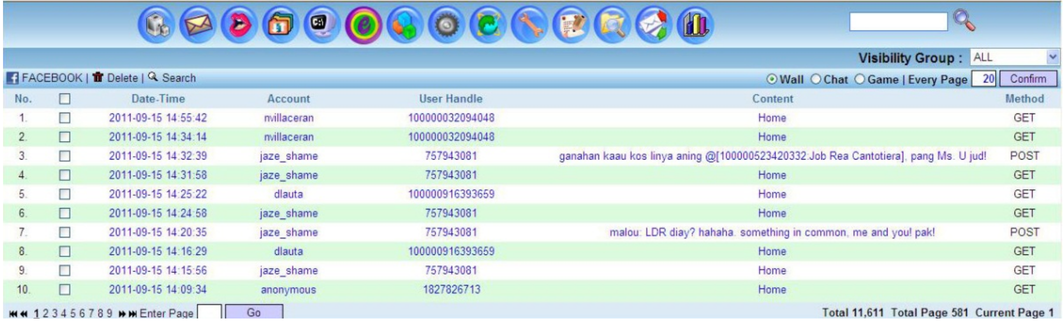

https://192.168.1.13/general/common/http/http_original.php?_file=LzxQbmt%25252Ba30vPFA8OjpDOkM8 - Window...

```
         GET /s/269375 HTTP/1.1
Accept: */*
Referer: http://sg.yahoo.com/?p=us
Accept-Language: en-sg
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; Foxy/1; SLCC1; .NET CLR 2.0
Accept-Encoding: gzip, deflate
Host: sg.yahoo.com
Connection: Keep-Alive
Cookie: Y=v=1&n=as1bl3nhshaa8&l=9kl4djki_8j0/o&p=m2ivvmy113000500&jb=24|70|&iz=75450&r=7h&lg=en-US&intl=
```

HTTP Social Network Sites

Facebook (Wall, Chat and Games)

Facebook obtainable information includes Facebook Wall, Chat and Games Records. The obtainable information includes the POST and GET content of Facebook Wall. The GET contents would consist of the user’s Facebook Homepage content. The POST contents would consist of the users’ Facebook Posting content.



Visibility Group : ALL

FACEBOOK | Delete | Search

● Wall ○ Chat ○ Game | Every Page 20 Confirm

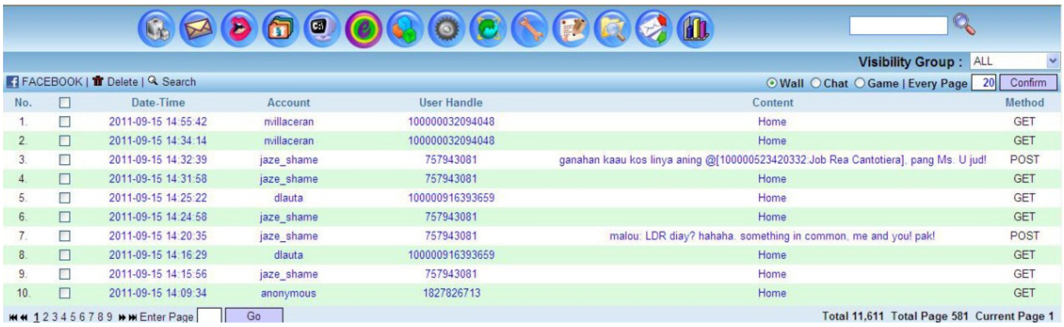
No.	□	Date-Time	Account	User Handle	Content	Method
1.	□	2011-09-15 14:55:42	nvillaceran	100000032094048	Home	GET
2.	□	2011-09-15 14:34:14	nvillaceran	100000032094048	Home	GET
3.	□	2011-09-15 14:32:39	jaze_shame	757943081	ganahan kaau kos linya aning @[100000523420332:Job Rea Cantotiera], pang Ms. U jud!	POST
4.	□	2011-09-15 14:31:58	jaze_shame	757943081	Home	GET
5.	□	2011-09-15 14:25:22	dlauta	100000916393659	Home	GET
6.	□	2011-09-15 14:24:58	jaze_shame	757943081	Home	GET
7.	□	2011-09-15 14:20:35	jaze_shame	757943081	malou: LDR diay? hahaha. something in common, me and you! pak!	POST
8.	□	2011-09-15 14:16:29	dlauta	100000916393659	Home	GET
9.	□	2011-09-15 14:15:56	jaze_shame	757943081	Home	GET
10.	□	2011-09-15 14:09:34	anonymous	1827826713	Home	GET

1 2 3 4 5 6 7 8 9 Enter Page Go Total 11,611 Total Page 581 Current Page 1

Facebook (Chat) will show the reconstructed results of chat content between the user and the friend List in his/her Facebook account. Facebook (Games) will show game played and the reconstructed Games pages accessed by the users.

HTTP Social Network Sites - Twitter

Twitter obtainable information includes date-time, account, user handle and content. The content consists of POST and GET data.



Visibility Group : ALL

FACEBOOK | Delete | Search

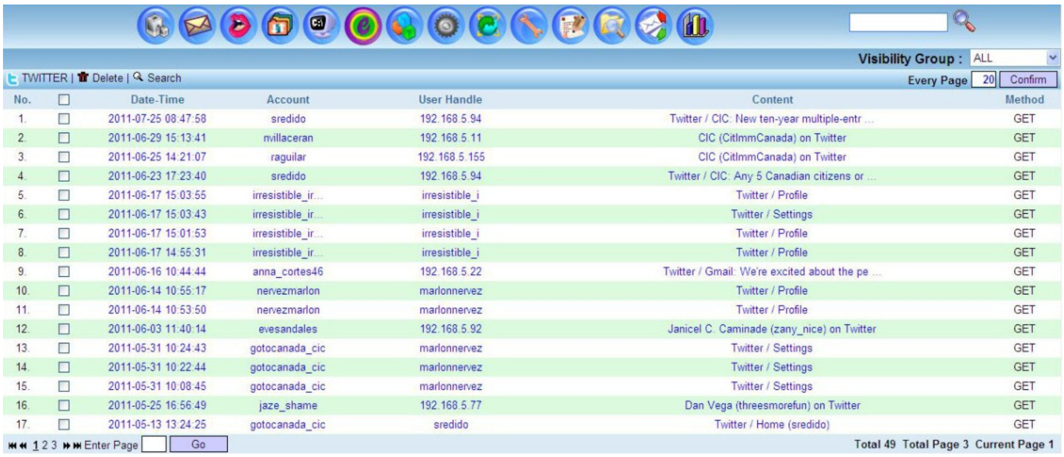
● Wall ○ Chat ○ Game | Every Page 20 Confirm

No.	□	Date-Time	Account	User Handle	Content	Method
1.	□	2011-09-15 14:55:42	nvillaceran	100000032094048	Home	GET
2.	□	2011-09-15 14:34:14	nvillaceran	100000032094048	Home	GET
3.	□	2011-09-15 14:32:39	jaze_shame	757943081	ganahan kaau kos linya aning @[100000523420332:Job Rea Cantotiera], pang Ms. U jud!	POST
4.	□	2011-09-15 14:31:58	jaze_shame	757943081	Home	GET
5.	□	2011-09-15 14:25:22	dlauta	100000916393659	Home	GET
6.	□	2011-09-15 14:24:58	jaze_shame	757943081	Home	GET
7.	□	2011-09-15 14:20:35	jaze_shame	757943081	malou: LDR diay? hahaha. something in common, me and you! pak!	POST
8.	□	2011-09-15 14:16:29	dlauta	100000916393659	Home	GET
9.	□	2011-09-15 14:15:56	jaze_shame	757943081	Home	GET
10.	□	2011-09-15 14:09:34	anonymous	1827826713	Home	GET

1 2 3 4 5 6 7 8 9 Enter Page Go Total 11,611 Total Page 581 Current Page 1

HTTP Social Network Sites - Plurk

Plurk obtainable information includes date-time, account, user handle and content. The content consists of POST and GET data.



Visibility Group : ALL

TWITTER | Delete | Search

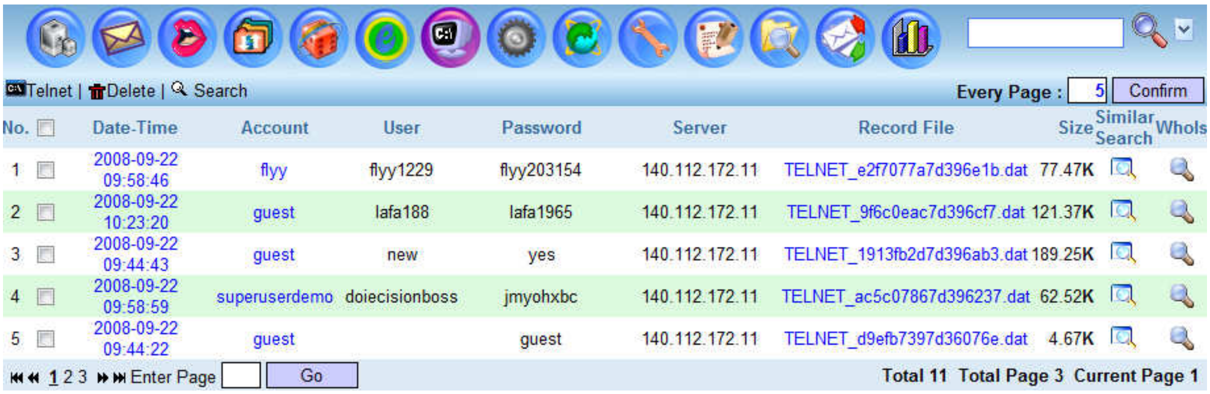
Every Page 20 Confirm

No.	□	Date-Time	Account	User Handle	Content	Method
1.	□	2011-07-25 08:47:58	sredido	192.168.5.94	Twitter / CIC: New ten-year multiple-entr ...	GET
2.	□	2011-06-29 15:13:41	nvillaceran	192.168.5.11	CIC (CitImmCanada) on Twitter	GET
3.	□	2011-06-25 14:21:07	raguilar	192.168.5.155	CIC (CitImmCanada) on Twitter	GET
4.	□	2011-06-23 17:23:40	sredido	192.168.5.94	Twitter / CIC: Any 5 Canadian citizens or ...	GET
5.	□	2011-06-17 15:03:55	irresistible_ir...	irresistible_i	Twitter / Profile	GET
6.	□	2011-06-17 15:03:43	irresistible_ir...	irresistible_i	Twitter / Settings	GET
7.	□	2011-06-17 15:01:53	irresistible_ir...	irresistible_i	Twitter / Profile	GET
8.	□	2011-06-17 14:55:31	irresistible_ir...	irresistible_i	Twitter / Profile	GET
9.	□	2011-06-16 10:44:44	anna_cortes46	192.168.5.22	Twitter / Gmail: We're excited about the pe ...	GET
10.	□	2011-06-14 10:55:17	nervezmarlon	marlonnervez	Twitter / Profile	GET
11.	□	2011-06-14 10:53:50	nervezmarlon	marlonnervez	Twitter / Profile	GET
12.	□	2011-06-03 11:40:14	evesandales	192.168.5.92	Janicel C. Caminade (zany_nice) on Twitter	GET
13.	□	2011-05-31 10:24:43	gotocanada_cic	marlonnervez	Twitter / Settings	GET
14.	□	2011-05-31 10:22:44	gotocanada_cic	marlonnervez	Twitter / Settings	GET
15.	□	2011-05-31 10:08:45	gotocanada_cic	marlonnervez	Twitter / Settings	GET
16.	□	2011-05-25 16:56:49	jaze_shame	192.168.5.77	Dan Vega (threesmorefun) on Twitter	GET
17.	□	2011-05-13 13:24:25	gotocanada_cic	sredido	Twitter / Home (sredido)	GET

1 2 3 Enter Page Go Total 49 Total Page 3 Current Page 1

Telnet

Telnet is an Internet protocol use on Internet and LAN. Telnet clients have been available on most Unix systems and are available for all platforms. Most network equipment (router, switches etc.) and OSs with a TCP/IP stack support some kind of Telnet service server for their remote configuration. Telnet obtainable information in ICI system includes date-time, account (with IP/MAC), username, password, server IP and session play back.



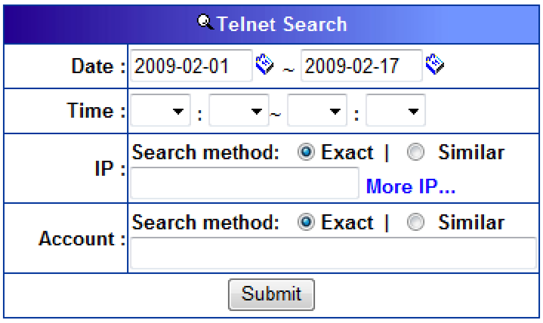
Telnet | Delete | Search   Every Page : 5 Confirm

No.	□	Date-Time	Account	User	Password	Server	Record File	Size	Similar Search	WhoIs
1	□	2008-09-22 09:58:46	flyy	flyy1229	flyy203154	140.112.172.11	TELNET_e2f7077a7d396e1b.dat	77.47K	🔍	🔍
2	□	2008-09-22 10:23:20	guest	lafa188	lafa1965	140.112.172.11	TELNET_9f6c0eac7d396cf7.dat	121.37K	🔍	🔍
3	□	2008-09-22 09:44:43	guest	new	yes	140.112.172.11	TELNET_1913fb2d7d396ab3.dat	189.25K	🔍	🔍
4	□	2008-09-22 09:58:59	superuserdemo	doiecisionboss	jmyohxbc	140.112.172.11	TELNET_ac5c07867d396237.dat	62.52K	🔍	🔍
5	□	2008-09-22 09:44:22	guest		guest	140.112.172.11	TELNET_d9efb7397d36076e.dat	4.67K	🔍	🔍

⏮ ⏪ 1 2 3 ⏩ ⏭ Enter Page [ ] Go   Total 11 Total Page 3 Current Page 1

Features in this Telnet GUI:

- Telnet: Click on to refresh the page content List.
- Delete: Delete record which is checked
- Search: Search the particular records based on the specified parameters such as Date, Time, IP, File Name and Account



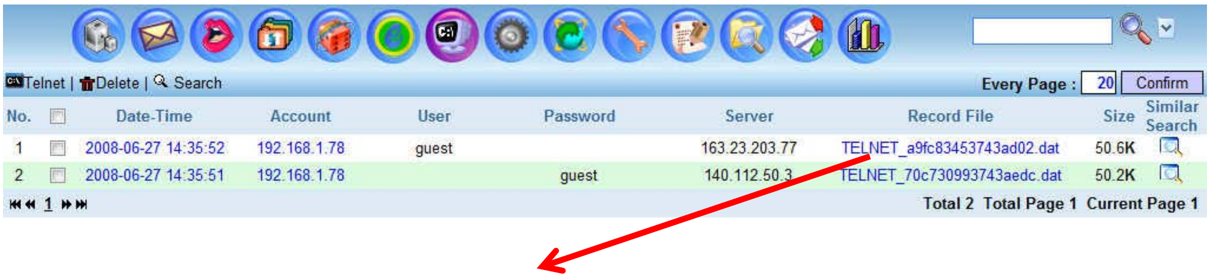
Telnet Search

Date :	2009-02-01 ~ 2009-02-17
Time :	▾ : ▾ ~ ▾ : ▾
IP :	Search method: ● Exact | ○ Similar More IP...
Account :	Search method: ● Exact | ○ Similar

Submit

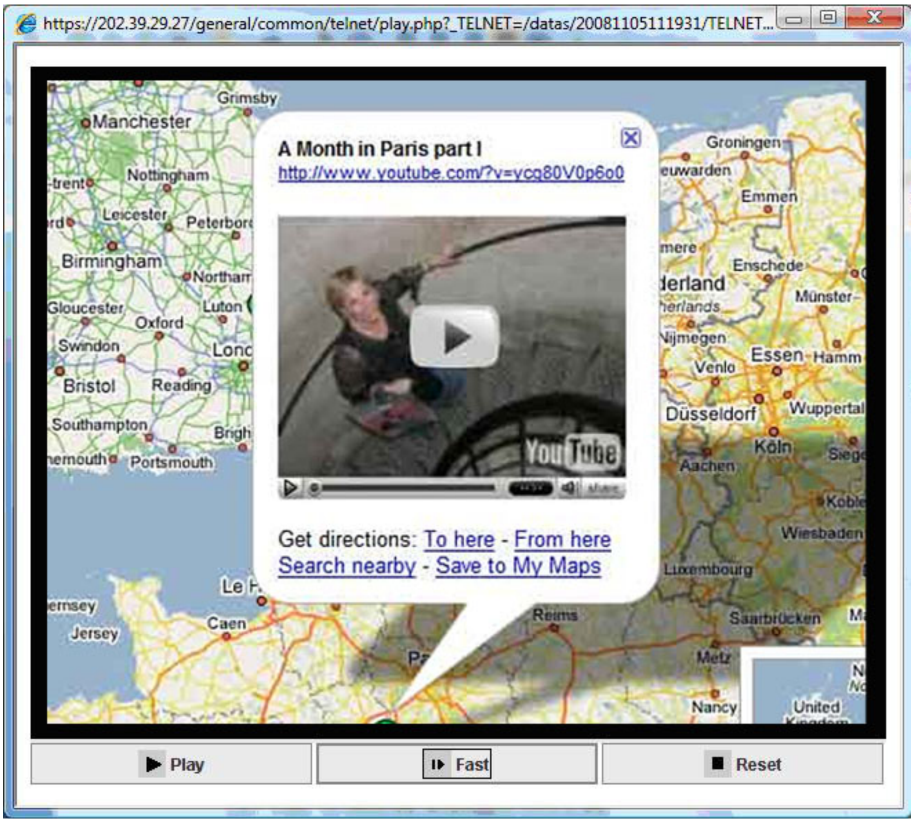
- Every Page : 5 Confirm Display records per page. Input the number and click on the confirm button to set up
- □ Checkbox: Records can be deleted by checking the Checkbox
- 🔍 Similar Search: Search for Telnet session with similar Telnet server etc
- 🔍 Whois: Provide information of Source and Destination IP and Hostname

View the Telnet Session
The following GUI will be popped up when Administrator click the link [Record File]. This GUI acts as a video player. Administrator can view the process step by step.



No.	□	Date-Time	Account	User	Password	Server	Record File	Size	Similar Search
1	□	2008-06-27 14:35:52	192.168.1.78	guest		163.23.203.77	TELNET_a9fc83453743ad02.dat	50.6K	
2	□	2008-06-27 14:35:51	192.168.1.78		guest	140.112.50.3	TELNET_70c730993743aedc.dat	50.2K	

1 Total 2 Total Page 1 Current Page 1


https://202.39.29.27/general/common/telnet/play.php?_TELNET=/datas/20081105111931/TELNET...

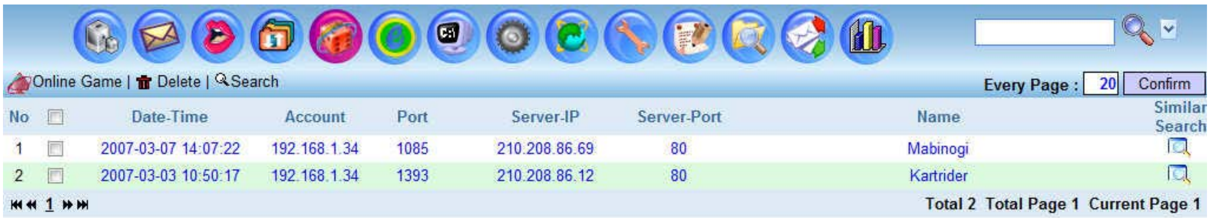
A Month in Paris part I
http://www.youtube.com/?v=ycg80V0p6o0

Get directions: To here - From here
Search nearby - Save to My Maps

Others

Online Games

Online Game log obtainable information includes Date-Time, Account (with IP/MAC), Port, Game Server IP, Server Port and Game Name.



Online Game | Delete | Search

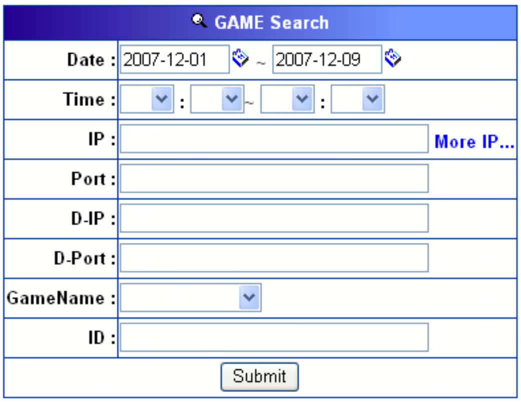
Every Page : 20 Confirm

No	□	Date-Time	Account	Port	Server-IP	Server-Port	Name	Similar Search
1	□	2007-03-07 14:07:22	192.168.1.34	1085	210.208.86.69	80	Mabinogi	
2	□	2007-03-03 10:50:17	192.168.1.34	1393	210.208.86.12	80	Kartrider	

⏮ ⏪ 1 ⏩ ⏭ Total 2 Total Page 1 Current Page 1

Features in this Online Game GUI:

- Online Game: Refresh the page content List.
- Delete: Delete the record that is checked (by clicking the Checkbox and Delete button).
- Search: Search the Online Game record based on the specified parameters such as
- Date, Time, IP, Port, Game Server IP, Game Server Port, Game Name and ID.



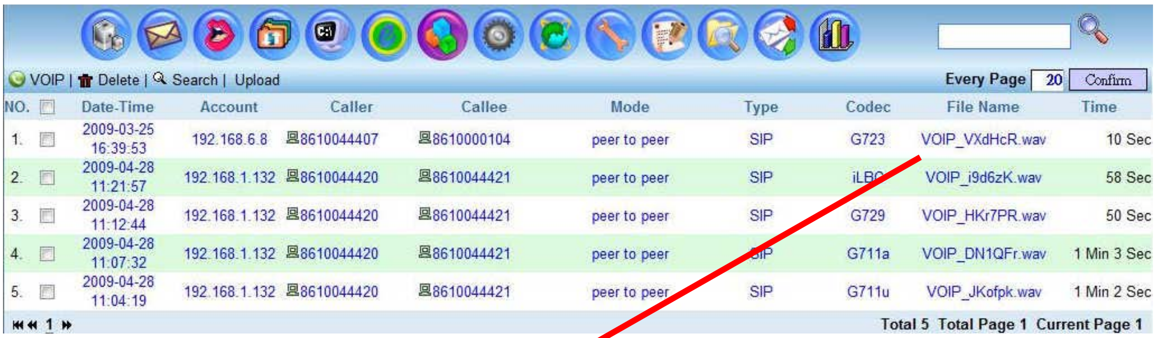
GAME Search

Date :	2007-12-01 ~ 2007-12-09
Time :	: ~ :
IP :	More IP...
Port :	
D-IP :	
D-Port :	
GameName :	
ID :	
	Submit

- Every Page : 5 Confirm Display records per page. Input the number and click on the confirm button to set up
- □ Checkbox: Records can be deleted by checking the Checkbox
- Similar Search: Search for Online Game record with similar content

VoIP (Optional Purchase License)

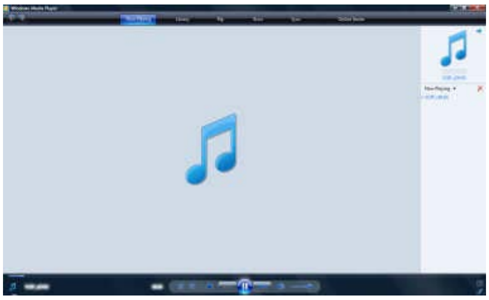
VoIP Capture and Reconstruction Module is able to capture, decode and reconstruct VoIP sessions (RTP sessions). It allows the play back of voice calls on network. The supported protocols include SIP (technology that is most commonly used) and H.323. The supported CODECs include G.729, G.711-a law and G.711-u law, G.723, G.726 and ILBC. Obtainable information includes Date-Time, Account, Caller Number, Called Number, Mode of VoIP, VoIP Protocol Type, Codec and VoIP Audio File with play back capability. **Note** that this is additional license module.



VOIP | Delete | Search | Upload   Every Page 20 Confirm

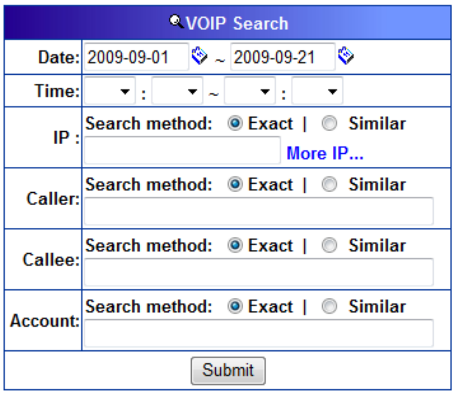
NO.	□	Date-Time	Account	Caller	Callee	Mode	Type	Codec	File Name	Time
1.	□	2009-03-25 16:39:53	192.168.6.8	8610044407	8610000104	peer to peer	SIP	G723	VOIP_VXdHcR.wav	10 Sec
2.	□	2009-04-28 11:21:57	192.168.1.132	8610044420	8610044421	peer to peer	SIP	iLBC	VOIP_i9d6zK.wav	58 Sec
3.	□	2009-04-28 11:12:44	192.168.1.132	8610044420	8610044421	peer to peer	SIP	G729	VOIP_HKr7PR.wav	50 Sec
4.	□	2009-04-28 11:07:32	192.168.1.132	8610044420	8610044421	peer to peer	SIP	G711a	VOIP_DN1QFr.wav	1 Min 3 Sec
5.	□	2009-04-28 11:04:19	192.168.1.132	8610044420	8610044421	peer to peer	SIP	G711u	VOIP_JKofpk.wav	1 Min 2 Sec

⏮ ◀ 1 ▶   Total 5 Total Page 1 Current Page 1



Features in this VoIP GUI:

- VoIP: Refresh the page content List.
- Delete: Delete the record that is checked (by clicking the Checkbox and Delete button).
- Search: Search the VoIP record based on the specified parameters such as Date, Time, IP, Caller, Called Number and Account.

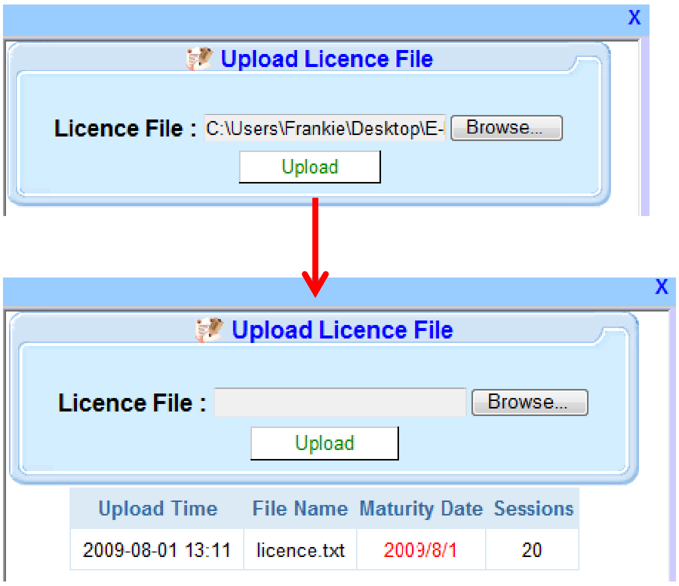


VOIP Search

Date:	2009-09-01 ~ 2009-09-21
Time:	▾ : ▾ ~ ▾ : ▾
IP :	Search method: ● Exact | ○ Similar More IP...
Caller:	Search method: ● Exact | ○ Similar
Callee:	Search method: ● Exact | ○ Similar
Account:	Search method: ● Exact | ○ Similar
	Submit

- Every Page : 5 Confirm Display records per page. Input the number and click on the confirm button to set up
- □ Checkbox: Records can be deleted by checking the Checkbox

- Upload VoIP License: Please ensure that you have activated the VoIP license (which is optional purchase). Upload the VoIP license at Registration GUI. Browse for the VoIP License, licence.txt and upload for activation. Ensure that you have also started the VoIP Reconstruction Module at System Setting – Service – System Services GUI.



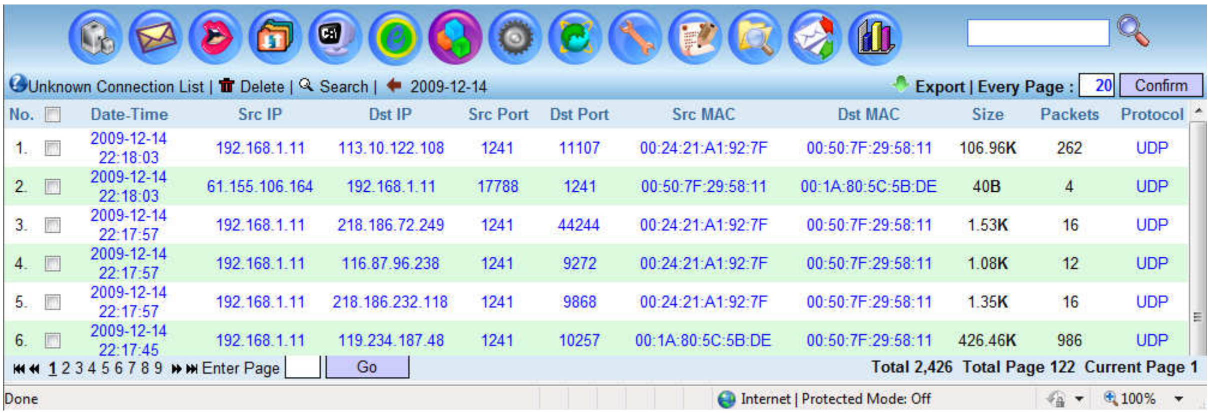
Licence File : C:\Users\Frankie\Desktop\E-

Licence File :

Upload Time	File Name	Maturity Date	Sessions
2009-08-01 13:11	licence.txt	2009/8/1	20

Unknown Connection

This section will List out the Unknown connections information like source IP, destination IP, source port, destination port, source MAC, destination MAC, connection size, packets and protocol (TCP/UDP). This information can be useful for network Administrator to detection unusual connections.



Unknown Connection List | Delete | Search | 2009-12-14 Export | Every Page : 20 Confirm

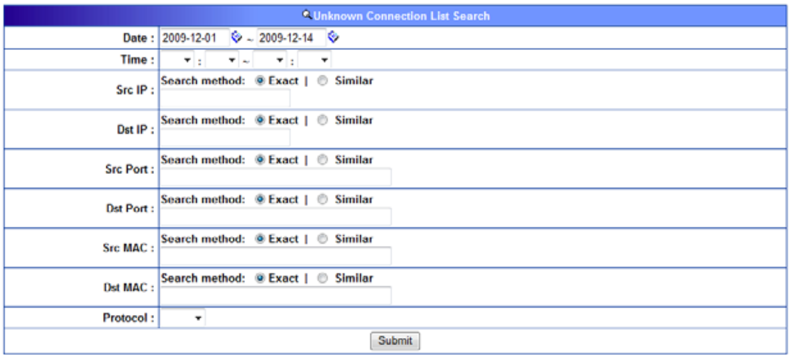
No.	□	Date-Time	Src IP	Dst IP	Src Port	Dst Port	Src MAC	Dst MAC	Size	Packets	Protocol
1.	□	2009-12-14 22:18:03	192.168.1.11	113.10.122.108	1241	11107	00:24:21:A1:92:7F	00:50:7F:29:58:11	106.96K	262	UDP
2.	□	2009-12-14 22:18:03	61.155.106.164	192.168.1.11	17788	1241	00:50:7F:29:58:11	00:1A:80:5C:5B:DE	40B	4	UDP
3.	□	2009-12-14 22:17:57	192.168.1.11	218.186.72.249	1241	44244	00:24:21:A1:92:7F	00:50:7F:29:58:11	1.53K	16	UDP
4.	□	2009-12-14 22:17:57	192.168.1.11	116.87.96.238	1241	9272	00:24:21:A1:92:7F	00:50:7F:29:58:11	1.08K	12	UDP
5.	□	2009-12-14 22:17:57	192.168.1.11	218.186.232.118	1241	9868	00:24:21:A1:92:7F	00:50:7F:29:58:11	1.35K	16	UDP
6.	□	2009-12-14 22:17:45	192.168.1.11	119.234.187.48	1241	10257	00:1A:80:5C:5B:DE	00:50:7F:29:58:11	426.46K	986	UDP

1 2 3 4 5 6 7 8 9 Enter Page Go Total 2,426 Total Page 122 Current Page 1

Done Internet | Protected Mode: Off 100%

Features in this Unknown Connection GUI:

- Unknown Connection Lists: Refresh the page content List.
- Delete: Delete record checked (by clicking the Checkbox and Delete button).
- Search: Search the Unknown Connection record based on the specified parameters such as Date, Time, Source IP, Destination IP, Source Port, Destination Port, Source MAC, Destination MAC and Protocol.



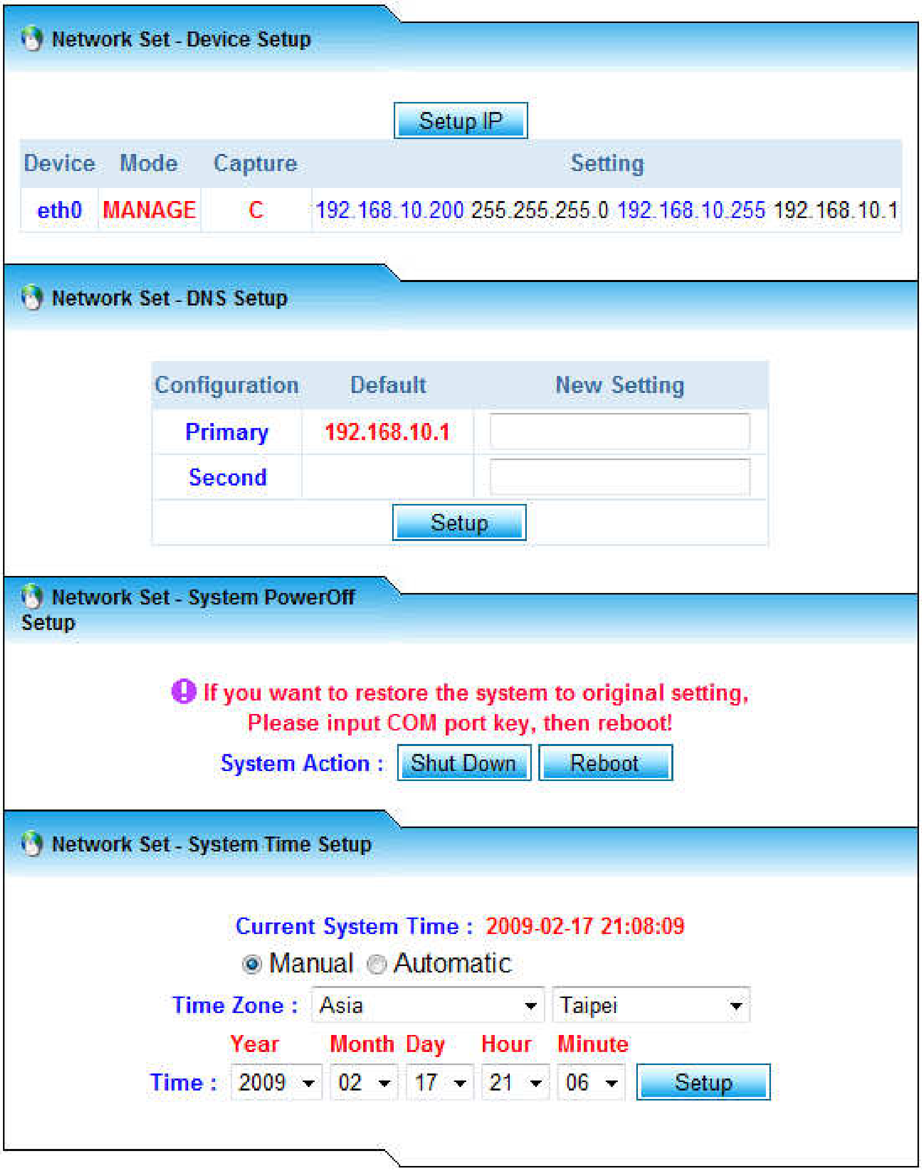
Unknown Connection List Search

Date :	2009-12-01 ~ 2009-12-14
Time :	: ~ :
Src IP :	Search method: ● Exact | ○ Similar
Dst IP :	Search method: ● Exact | ○ Similar
Src Port :	Search method: ● Exact | ○ Similar
Dst Port :	Search method: ● Exact | ○ Similar
Src MAC :	Search method: ● Exact | ○ Similar
Dst MAC :	Search method: ● Exact | ○ Similar
Protocol :	
	Submit

- Every Page : 5 Confirm Display records per page. Input the number and click on the confirm button to set up
- □ Checkbox: Records can be deleted by checking the Checkbox

System Setting

Network Setting



Network Set - Device Setup

Device	Mode	Capture	Setting
eth0	MANAGE	C	192.168.10.200 255.255.255.0 192.168.10.255 192.168.10.1

Network Set - DNS Setup

Configuration	Default	New Setting
Primary	192.168.10.1	
Second		

Network Set - System PowerOff Setup

If you want to restore the system to original setting, Please input COM port key, then reboot!

System Action :

Network Set - System Time Setup

Current System Time : 2009-02-17 21:08:09

● Manual ○ Automatic

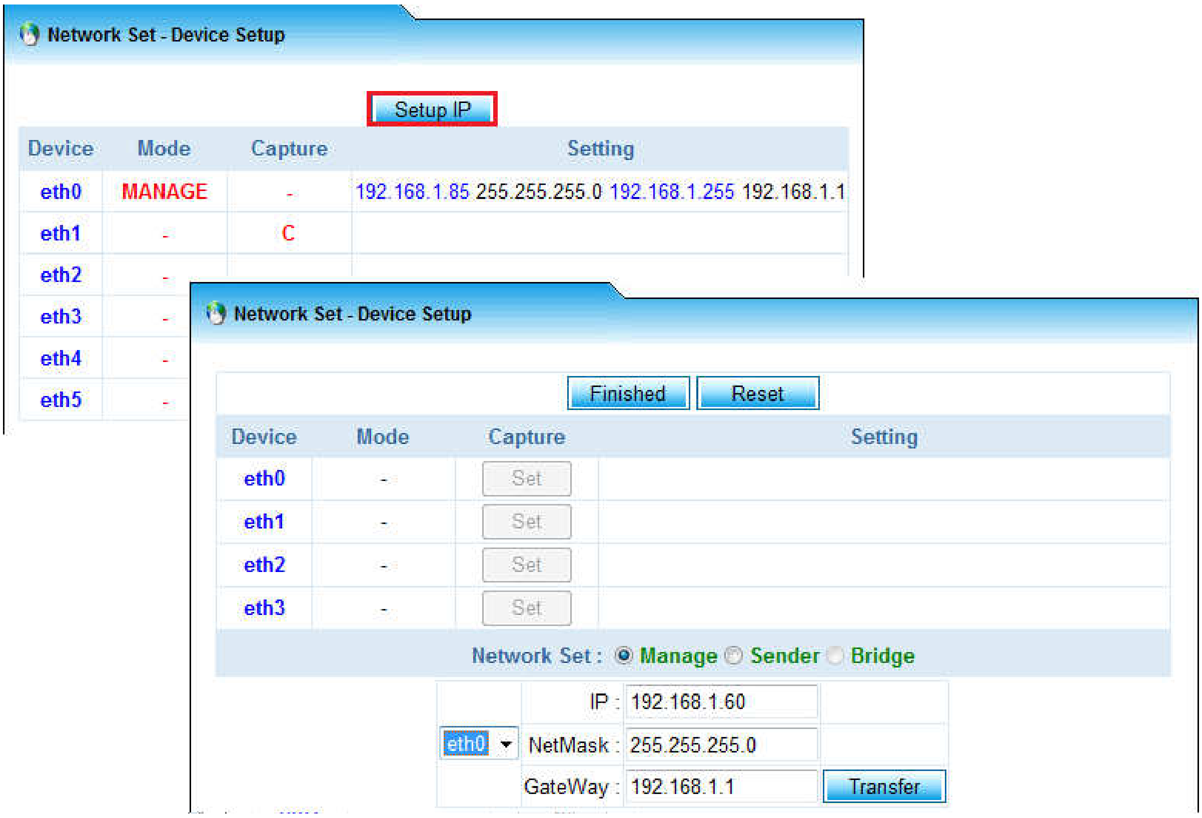
Time Zone : Asia Taipei

	Year	Month	Day	Hour	Minute
Time :	2009	02	17	21	06

- **Device Setup**: Setup the system operation mode. The next section will give more detail regarding the operation modes and how to setup the operation mode properly.
- **DNS Setup**: Setup the Domain Name Server (DNS) IP. The IP can be obtained from your ISP providers.
- **System Power off Setup**: Reboot or shut down the system.
- **System Time Setup**: Defining the system date-time.

Network Setup

This section allows the Administrator to setup different modes of operation for the ICI system.



Device	Mode	Capture	Setting
eth0	MANAGE	-	192.168.1.85 255.255.255.0 192.168.1.255 192.168.1.1
eth1	-	C	
eth2	-		
eth3	-		
eth4	-		
eth5	-		

Device	Mode	Capture	Setting
eth0	-	Set	
eth1	-	Set	
eth2	-	Set	
eth3	-	Set	

Network Set : ● Manage ○ Sender ○ Bridge

eth0
IP : 192.168.1.60
NetMask : 255.255.255.0
GateWay : 192.168.1.1

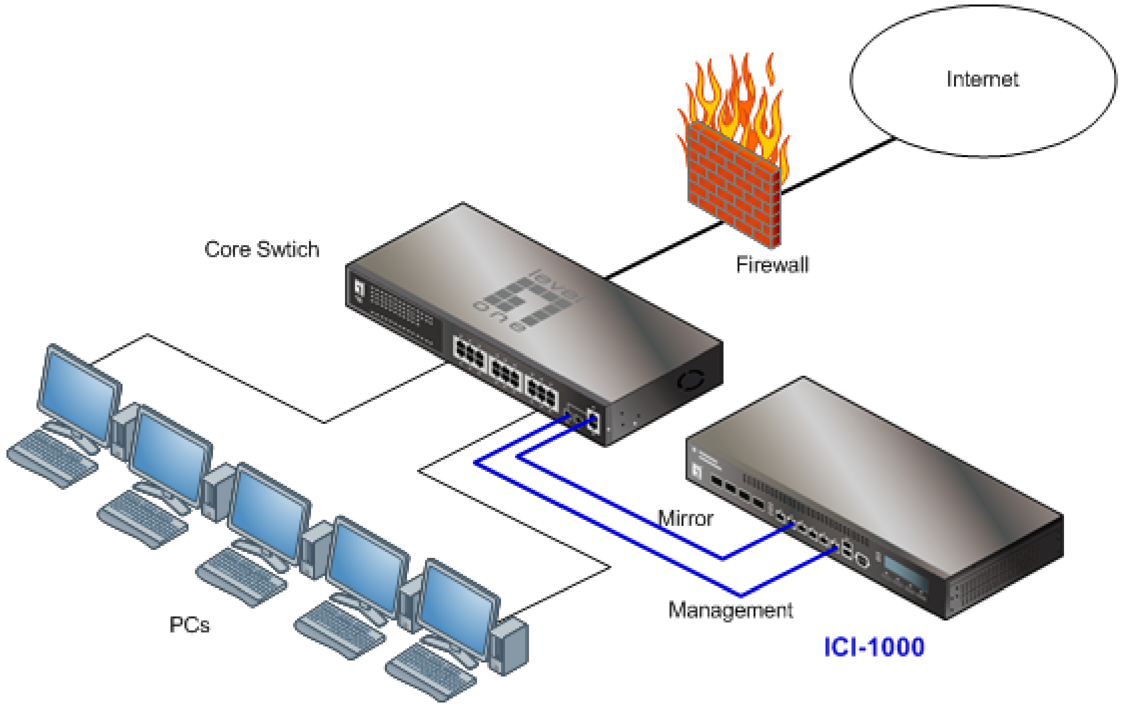
There are basically two parts need to be configured for the network setting. One is the configuration of management port and the other is configuration of the capture port. These two configurations can operate together in one NIC card or separately operate in different NIC cards.

There are two operation modes can be configured for the ICI System, however, Mirror Mode is highly recommended for best performance result.

A. Mirror Mode
B. Bridge Mode (Inline Mode)

A. Mirror Mode

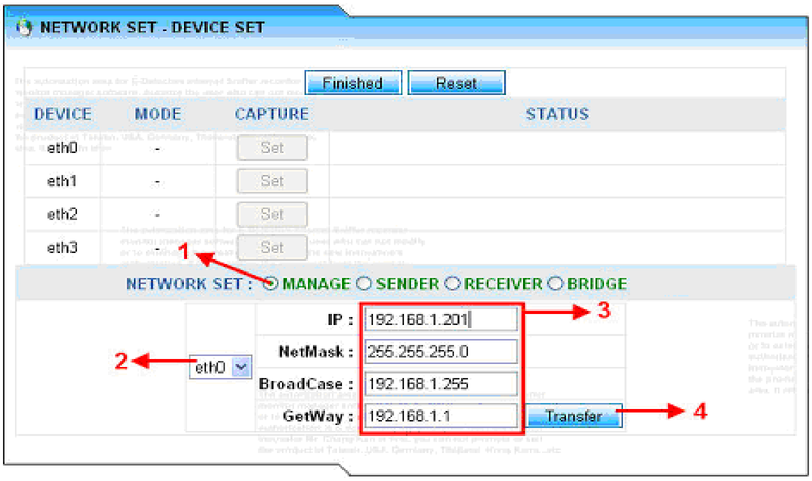
In terms of Mirror Mode, it uses two NIC cards to operate. One is for data capturing, and the other is for system management. The following diagram shows the concept of how this mode is operated. The NIC card (labelled Number 1) with port “eth0” is connected to the top HUB/Switch to capture the data. The NIC card (labelled Number 2) with port “eth1” for management (system web/telnet access) can be connected to the HUB or Switch.



This section illustrates the way of how to set up the Mirror Mode with the following diagrams step by step:

Step 1: Management Port Setup

1. Select and tick the option “MANAGE”
2. Select the NIC card called “eth0”.
3. Setup the information of IP, Mask IP, Broadcast IP and Gateway IP. Please check with your network Administrators if you are not sure the IP setting.
4. Click on the button [Transfer] to submit.



DEVICE	MODE	CAPTURE	STATUS
eth0	-	Set	
eth1	-	Set	
eth2	-	Set	
eth3	-	Set	

NETWORK SET : ● MANAGE ○ SENDER ○ RECEIVER ○ BRIDGE

eth0

IP : 192.168.1.201

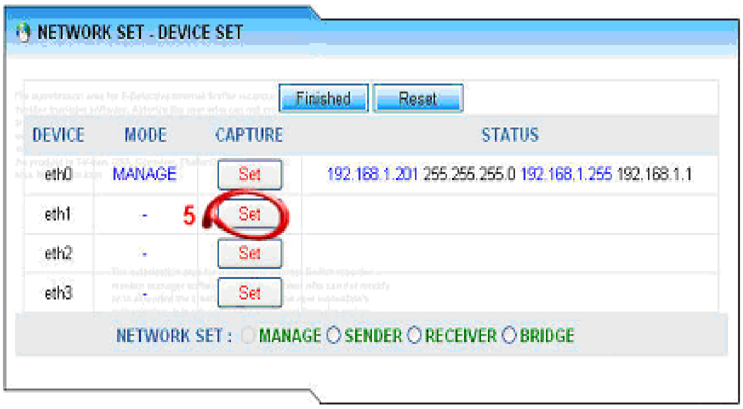
NetMask : 255.255.255.0

BroadCase : 192.168.1.255

GetWay : 192.168.1.1

Set 2: Capture Port Setup

5. Click on the button [Set] on Device eth1 or eth2 or eth3. Only one Ethernet port can be set to capture the data.

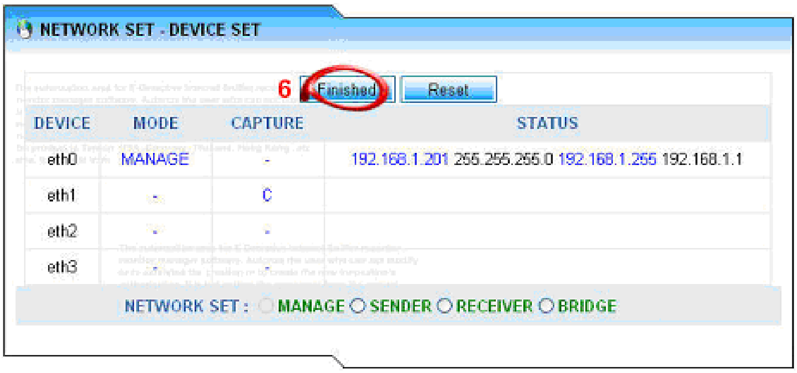


DEVICE	MODE	CAPTURE	STATUS
eth0	MANAGE	Set	192.168.1.201 255.255.255.0 192.168.1.255 192.168.1.1
eth1	-	Set	
eth2	-	Set	
eth3	-	Set	

NETWORK SET : ○ MANAGE ○ SENDER ○ RECEIVER ○ BRIDGE

Set 3: Finish Setup

6. Click on the button [Finished], the system will reboot and the network setup is completed.

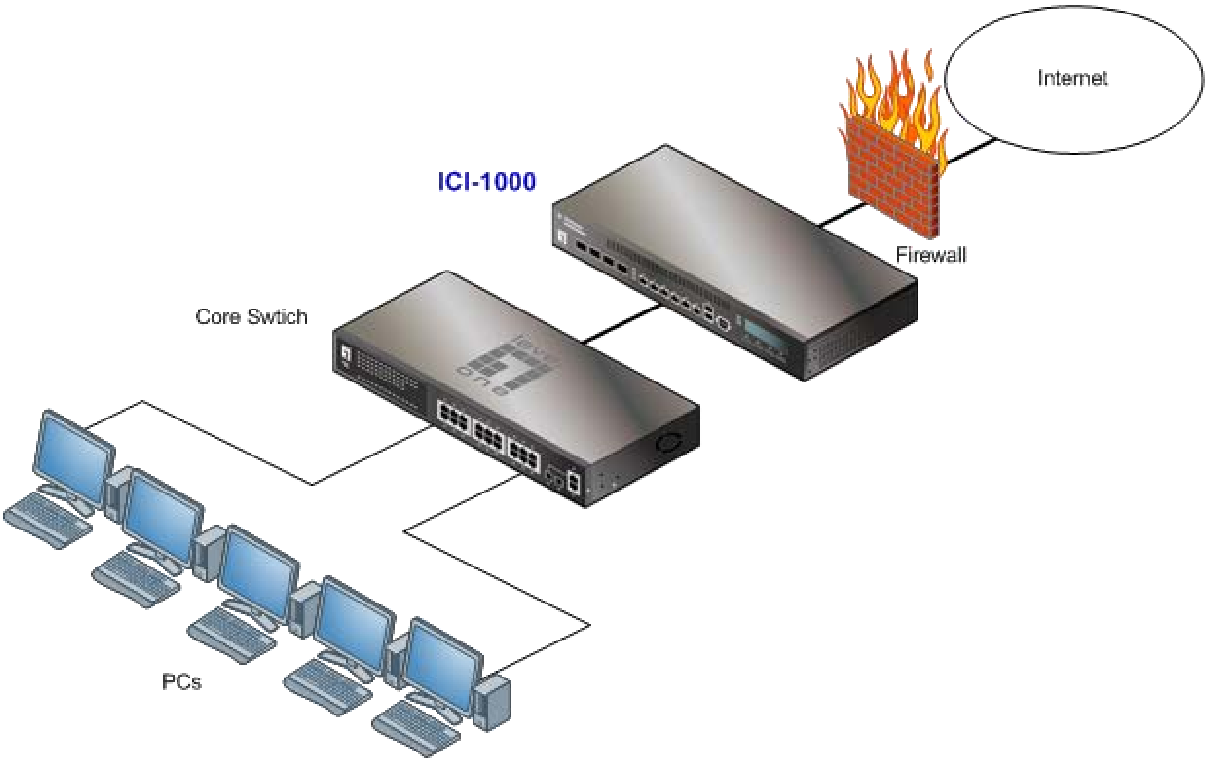


DEVICE	MODE	CAPTURE	STATUS
eth0	MANAGE	-	192.168.1.201 255.255.255.0 192.168.1.255 192.168.1.1
eth1	-	C	
eth2	-	-	
eth3	-	-	

NETWORK SET : ○ MANAGE ○ SENDER ○ RECEIVER ○ BRIDGE

B. Bridge Mode (Inline Mode)

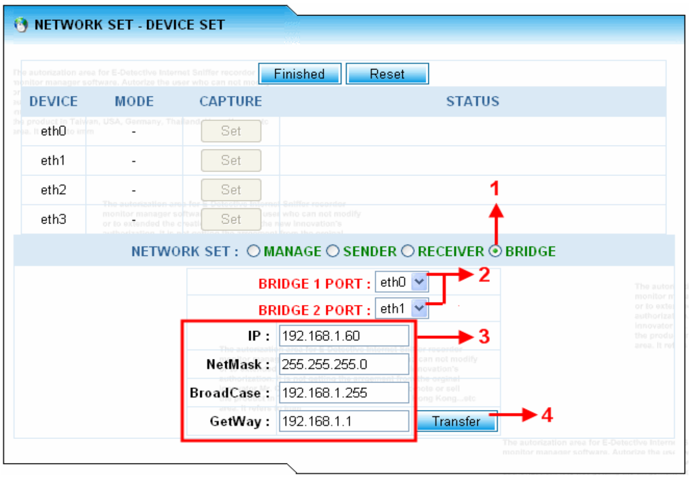
This mode uses two NIC cards to operate in the ICI system. The following diagram shows the concept of how this mode is operated.



This section illustrates the way to set up the Bridge Mode with the following diagrams step by step:

Step 1: Bridge Setup

1. Select and tick the option “BRIDGE”
2. Select Bridge port 1 and 2 (two NIC cards) as shown on the following diagram.
3. Setup the information of IP, Mask IP, Broadcast IP and Gateway IP. Please check with your network Administrators if you are not sure about IPs.
4. Click on the button [Transfer] to submit.


NETWORK SET - DEVICE SET

DEVICE	MODE	CAPTURE	STATUS
eth0	-	Set	
eth1	-	Set	
eth2	-	Set	
eth3	-	Set	

NETWORK SET : ○ MANAGE ○ SENDER ○ RECEIVER ● BRIDGE

BRIDGE 1 PORT : eth0

BRIDGE 2 PORT : eth1

IP : 192.168.1.60

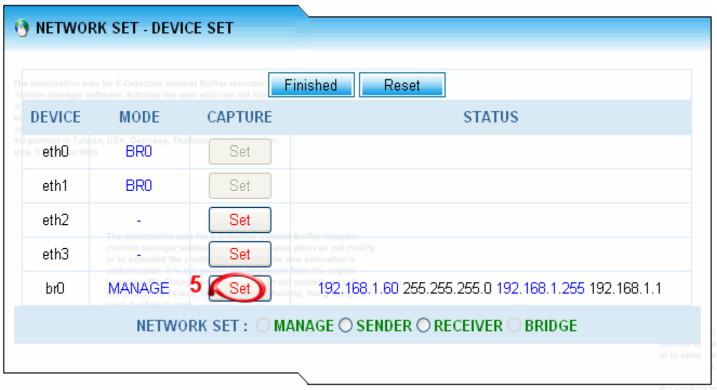
NetMask : 255.255.255.0

BroadCase : 192.168.1.255

GetWay : 192.168.1.1

Set 2: Capture Setup

5. This step produces one visual device called “br0” to manage the data. It is suggested that Administrator to choose this visual device “br0” to capture the data as well.



NETWORK SET - DEVICE SET

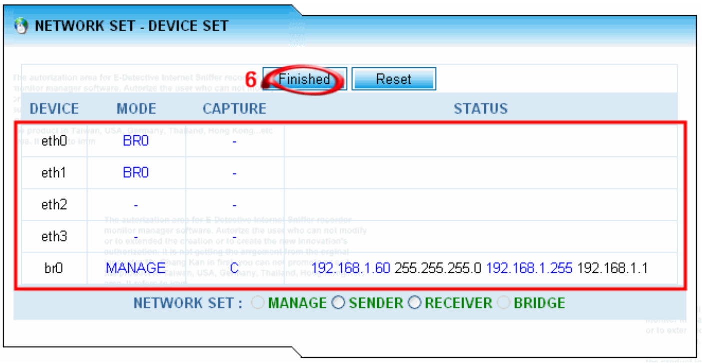
Finished Reset

DEVICE	MODE	CAPTURE	STATUS
eth0	BR0	Set	
eth1	BR0	Set	
eth2	-	Set	
eth3	-	Set	
br0	MANAGE	5 Set	192.168.1.60 255.255.255.0 192.168.1.255 192.168.1.1

NETWORK SET : ○ MANAGE ○ SENDER ○ RECEIVER ○ BRIDGE

Set 3: Finish Setup

6. Click on the button [Finished], the system will reboot and setup the Bridge mode.



NETWORK SET - DEVICE SET

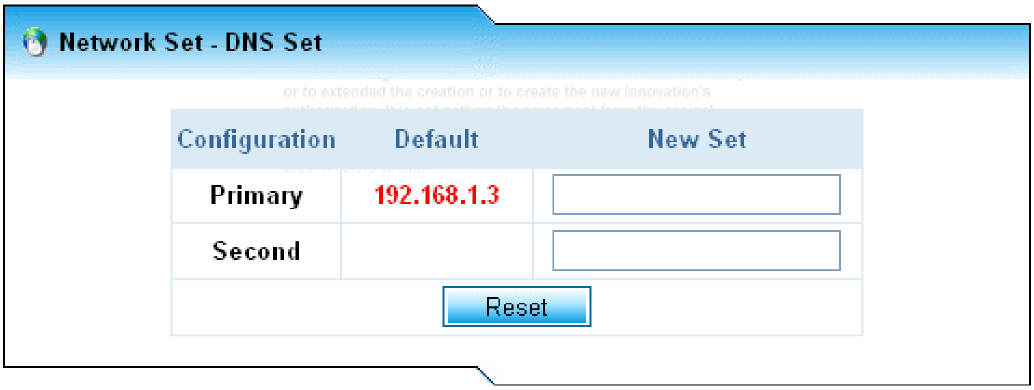
6 Finished Reset

DEVICE	MODE	CAPTURE	STATUS
eth0	BR0	-	
eth1	BR0	-	
eth2	-	-	
eth3	-	-	
br0	MANAGE	C	192.168.1.60 255.255.255.0 192.168.1.255 192.168.1.1

NETWORK SET : ○ MANAGE ○ SENDER ○ RECEIVER ○ BRIDGE

DNS Setup

Input the primary and secondary DNS provided from your ISP provider; click on the button [Reset] to set up.

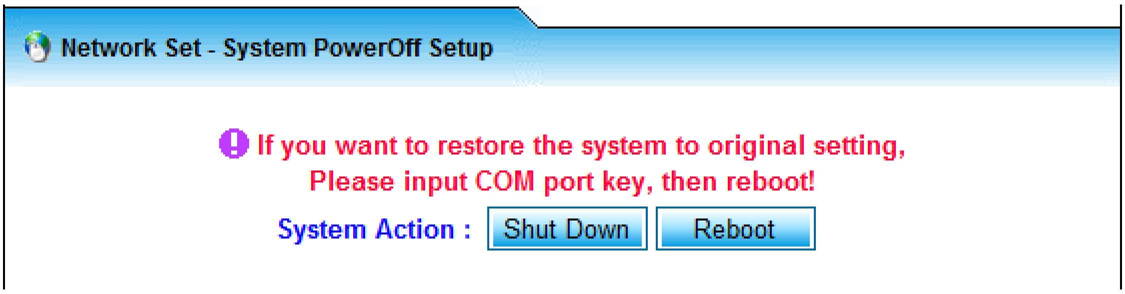


Network Set - DNS Set

Configuration	Default	New Set
Primary	192.168.1.3	
Second		

Shutdown and Reboot

Administrator can shut down or reboot the system through this GUI.



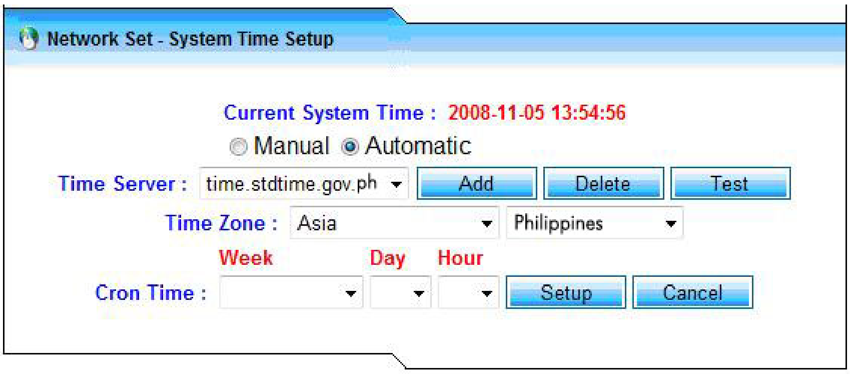
Network Set - System PowerOff Setup

If you want to restore the system to original setting,
Please input COM port key, then reboot!

System Action :

System Time Setup

Administrator can select Manual or Automatic setup for system time.



Network Set - System Time Setup

Current System Time : 2008-11-05 13:54:56

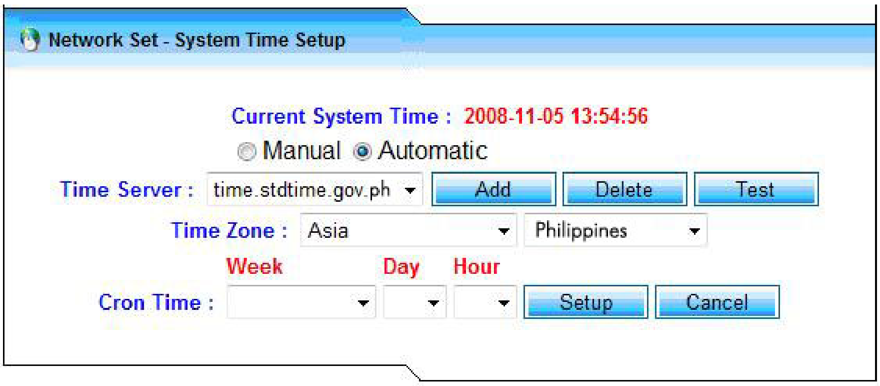
○ Manual ● Automatic

Time Server : time.stdtime.gov.ph

Time Zone : Asia | Philippines

Cron Time : Week | Day | Hour

Manual setup allows Administrator to setup the time zone and system time.



Network Set - System Time Setup

Current System Time : 2008-11-05 13:54:56

○ Manual ● Automatic

Time Server : time.stdtime.gov.ph

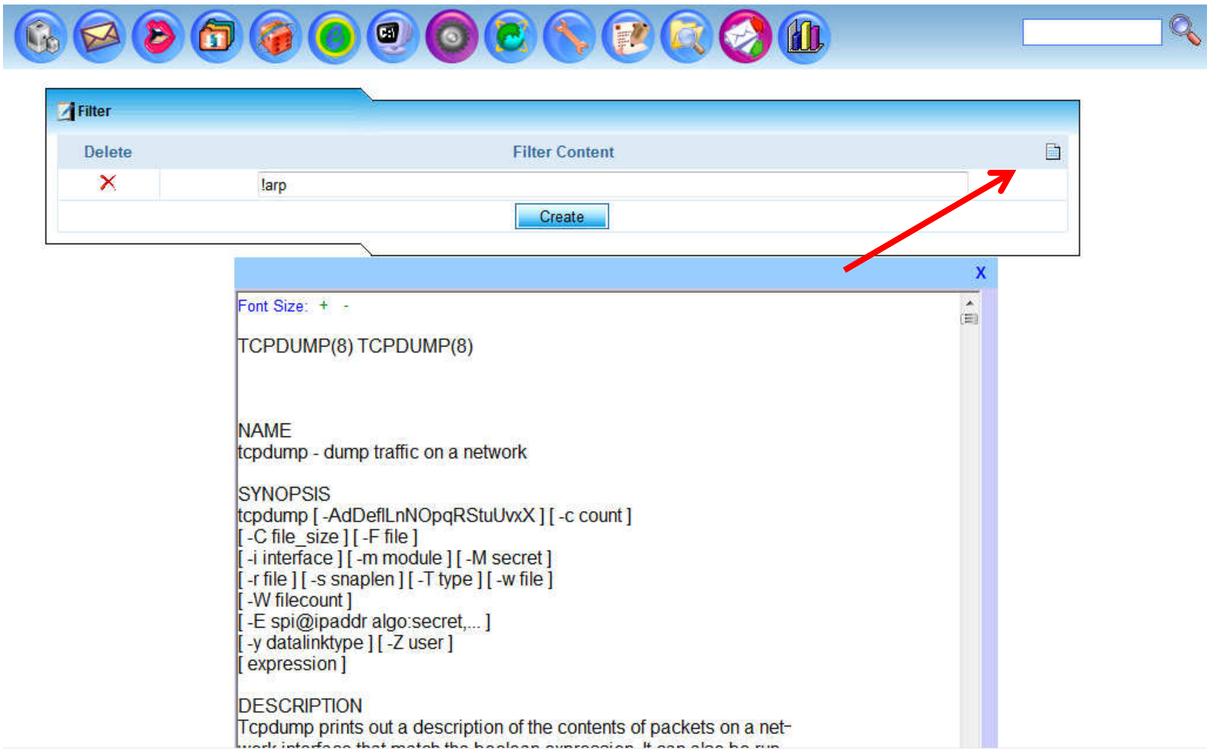
Time Zone : Asia | Philippines

Cron Time : Week | Day | Hour

Automatic setup allows Administrator to add additional time server for time synchronization. It also allows Administrator to setup the time zone. Besides, it allows Administrator to setup the synchronization time (week, day or hour).

Filter Setup

It allows the Administrator to define the List of IPs or Protocols to be captured and stored into the ICI system database base on tcpdump format.



```
TCPDUMP(8) TCPDUMP(8)


NAME
tcpdump - dump traffic on a network

SYNOPSIS
tcpdump [ -AdDeflLnNOpqRStuUvxX ] [ -c count ]
[ -C file_size ] [ -F file ]
[ -i interface ] [ -m module ] [ -M secret ]
[ -r file ] [ -s snaplen ] [ -T type ] [ -w file ]
[ -W filecount ]
[ -E spi@ipaddr algo:secret,... ]
[ -y datalinktype ] [ -Z user ]
[ expression ]

DESCRIPTION
Tcpdump prints out a description of the contents of packets on a net-
```

Some Samples Setup:

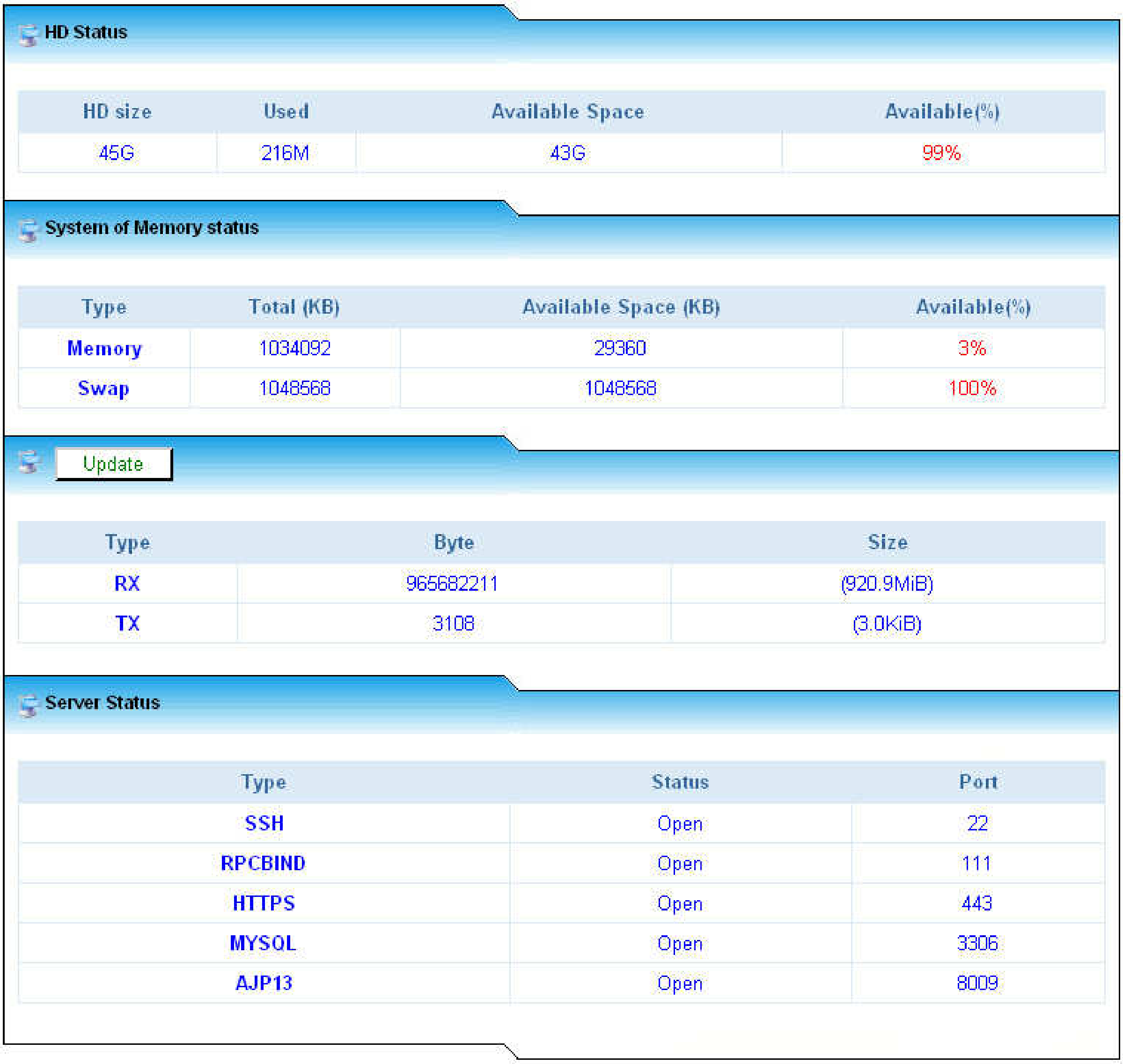
Sample 1:
Record all information captured from IP 192.168.1.10
Key in: host 192.168.1.10

Sample 2:
Records all information captured from IP 192.168.1.10 and 192.168.1.20 or 192.168.1.30. Key in: host 192.168.1.10 and (192.168.1.20 or 192.168.1.30)

Sample 3:
Records all Telnet sessions of 192.168.1.10
Key in: tcp port 23 host 192.168.1.10

Storage

It shows the hard disk utilization information which includes hard disk capacity, utilization, and available space (size in Gbytes and %) left. Warning message can be configured to be issued to Administrator when utilization reaches the threshold. The system memory status and system server status is also provided here.



HD Status

HD size	Used	Available Space	Available(%)
45G	216M	43G	99%

System of Memory status

Type	Total (KB)	Available Space (KB)	Available(%)
Memory	1034092	29360	3%
Swap	1048568	1048568	100%

Update

Type	Byte	Size
RX	965682211	(920.9MiB)
TX	3108	(3.0KiB)

Server Status

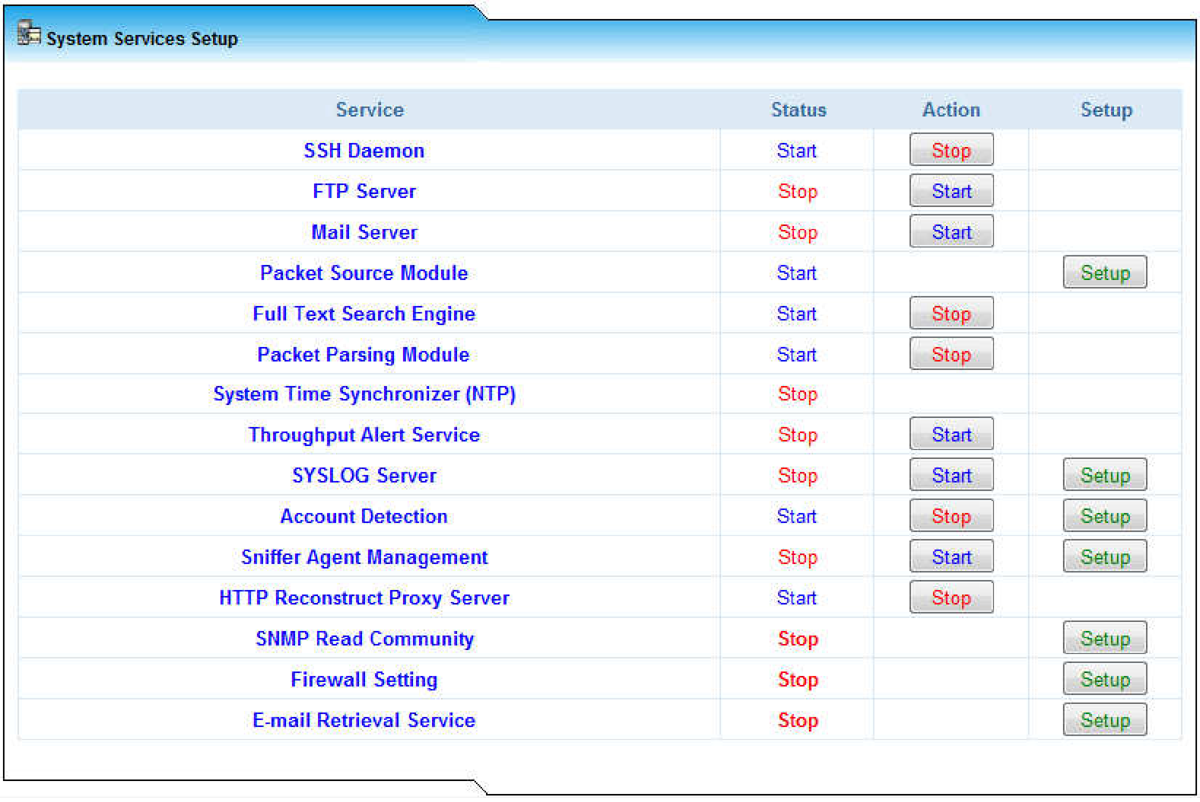
Type	Status	Port
SSH	Open	22
RPCBIND	Open	111
HTTPS	Open	443
MYSQL	Open	3306
AJP13	Open	8009

Services

It consists of 4 sub sections: System Services, Logger Services, Set Logger File Size and Sniffer Agent Management.

System Services

This section allows the Administrator to setup the system services such as FTP server, packet source module, syslog server, auto Email retrieval service etc.



System Services Setup

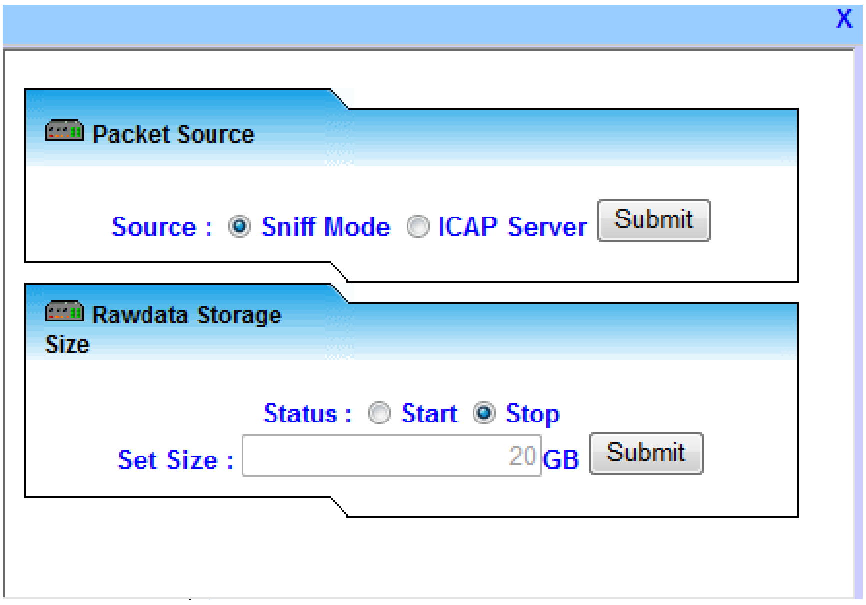
Service	Status	Action	Setup
SSH Daemon	Start	Stop	
FTP Server	Stop	Start	
Mail Server	Stop	Start	
Packet Source Module	Start		Setup
Full Text Search Engine	Start	Stop	
Packet Parsing Module	Start	Stop	
System Time Synchronizer (NTP)	Stop		
Throughput Alert Service	Stop	Start	
SYSLOG Server	Stop	Start	Setup
Account Detection	Start	Stop	Setup
Sniffer Agent Management	Stop	Start	Setup
HTTP Reconstruct Proxy Server	Start	Stop	
SNMP Read Community	Stop		Setup
Firewall Setting	Stop		Setup
E-mail Retrieval Service	Stop		Setup

Service	Function Description
SSH Daemon	Allow SSH Secure Shell Client or File Transfer access.
FTP Server	Start the FTP server service for downloading of reserved raw data files, backup ISO file or syslog message.
Mail Server	System Mail delivery service.
Packet Source Module	Allow Administrator to switch between Sniffer Mode and ICAP Server Mode (proxy server mode). Allow system to capture raw data packets through the mirror mode. Allow Administrator to setup in order to reserve (keep) raw data files collected. Setup can be configured to allow the raw data reserving function.
Full Text Service Engine	Allow full text search function, search by key word.
Packet Parsing Module	Packets parsing function
System Time Synchronizer (NTP)	Allow system time synchronization with the NTP server.
Throughput Alert Service	Allow throughput alert function.
Account Detection	Auto capture AD account name.
Syslog Server	Syslog server – syslog message collection
Sniffer Agent Management	Skype Agent Port Management
HTTP Reconstruct Proxy Server	Start this service for using Proxy service for HTTP Web Page Reconstruction
SNMP Read Community	SNMP service.
Firewall Setting	Firewall service to allow only specified IP to access the system.
Email Retrieval Service	Retrieving Emails from a specific Email Account through POP3 or IMAP service.

Packet Source Module

This section allows Administrator to setup the packet source which could be Sniffer Mode (system default) or ICAP Server Mode (Internet Content Adaption Protocol). Sniffer mode means the system will utilize the mirror/sniffer mode to capture traffic from the network (port-mirror capable switch or hub). ICAP mode allows the data to be provided by the ICAP proxy server from the network users which are connecting to the Internet through the ICAP proxy server. It requires the ICAP proxy server to be properly configured to send the data to the ICI system for reconstruction.

Besides, this section also allows Administrator to setup raw data reserving function. It allows Administrator to keep or store the captured raw data in the size of 100MB per raw data files basis. It also allows the Administrator to define storage size of raw data files. The raw data file reserved is stored in first in first out basis. New raw data file will replace the old raw data file. These raw data files reserved can be downloaded by using FTP client (with Console username/password set). The raw data files are automatically hashed with MD5 checksum to protect the raw data files integrity.



Packet Source

Source : ● Sniff Mode ○ ICAP Server

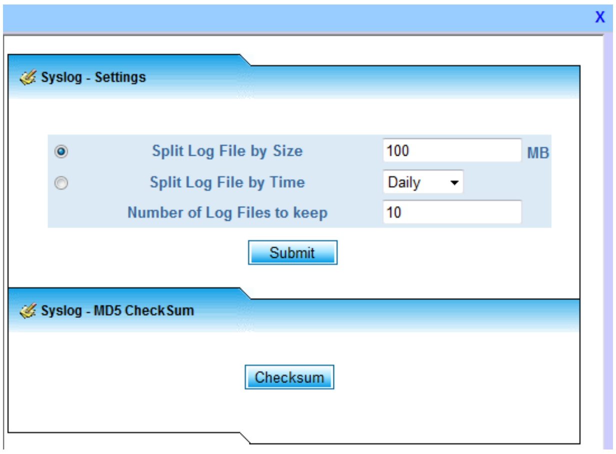
Rawdata Storage Size

Status : ○ Start ● Stop

Set Size : 20 GB

Syslog Server Service

This function allows the system to be a syslog message collector. Syslog messages collected from router, switches, servers and network equipment can be stored inside the ICI system. Administrator can export or download these syslog messages by using FTP client (with Console username/password set). Administrator needs to manually calculate the MD5 hashed value from this GUI before exporting or downloading the syslog message to protect the syslog message integrity.



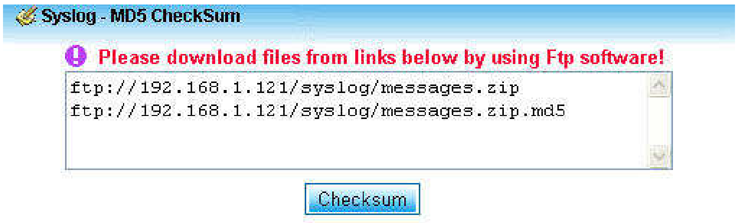
Syslog - Settings

● Split Log File by Size: 100 MB

○ Split Log File by Time: Daily

Number of Log Files to keep: 10

Syslog - MD5 CheckSum



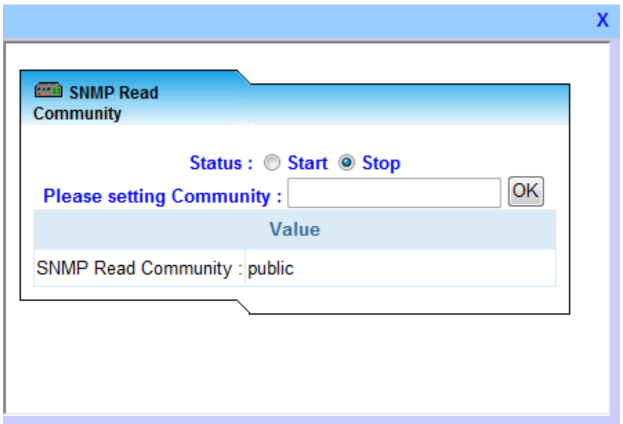
Syslog - MD5 CheckSum

Please download files from links below by using Ftp software!

```
ftp://192.168.1.121/syslog/messages.zip
ftp://192.168.1.121/syslog/messages.zip.md5
```

SNMP Read Community

This section allows the Administrator to set the SNMP Read Community.



SNMP Read Community

Status : ○ Start ● Stop

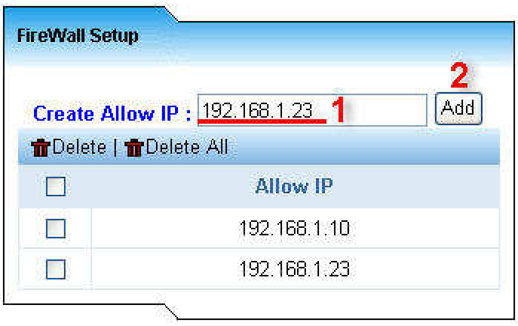
Please setting Community :

Value	
SNMP Read Community :	public

Firewall Setting

This service allows Administrator to specify the IP address or subnet that has the permission to access the ICI system.

1. Allow Access by Specific IP Address

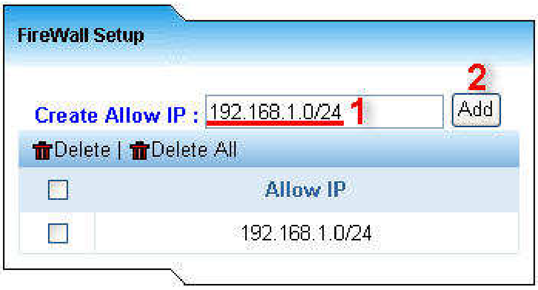


FireWall Setup

Create Allow IP : 192.168.1.23 Add

□	Allow IP
□	192.168.1.10
□	192.168.1.23

2. Allow Access by Subnet



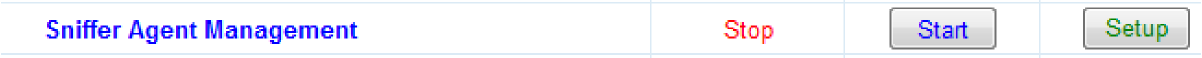
FireWall Setup

Create Allow IP : 192.168.1.0/24 Add

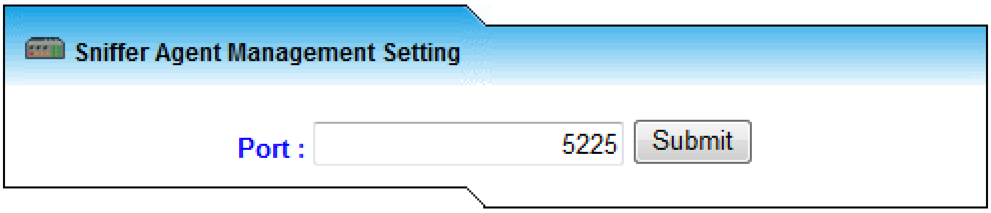
□	Allow IP
□	192.168.1.0/24

Sniffer Agent Management

If Administrator needs to change the default sniffer agent port, please click the setup button and input the port to submit.



Sniffer Agent Management Stop



Sniffer Agent Management Setting

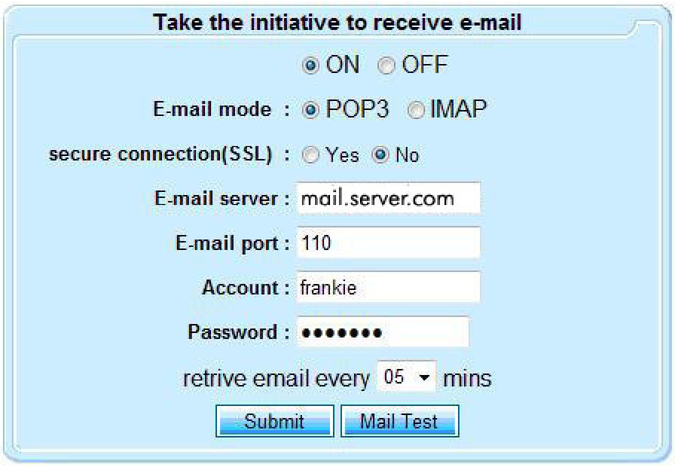
Port : 5225

Email Retrieval Service

This section allows the system to retrieve Email from a specific account from an Email Server. This function will solve the issue on the Email protocols not supported by ICI, such as MAPI/RPC of Microsoft Exchange Server etc.

Sample Implementation

Administrator setup a specific Email account on the Email server where all the Emails received (by all Email accounts) will be forwarded to. Then, Administrator can setup the following services where ICI system will retrieve the Emails (as scheduled) from the specific Email account of Email server.



Take the initiative to receive e-mail

● ON ○ OFF

E-mail mode : ● POP3 ○ IMAP

secure connection(SSL) : ○ Yes ● No

E-mail server : mail.server.com

E-mail port : 110

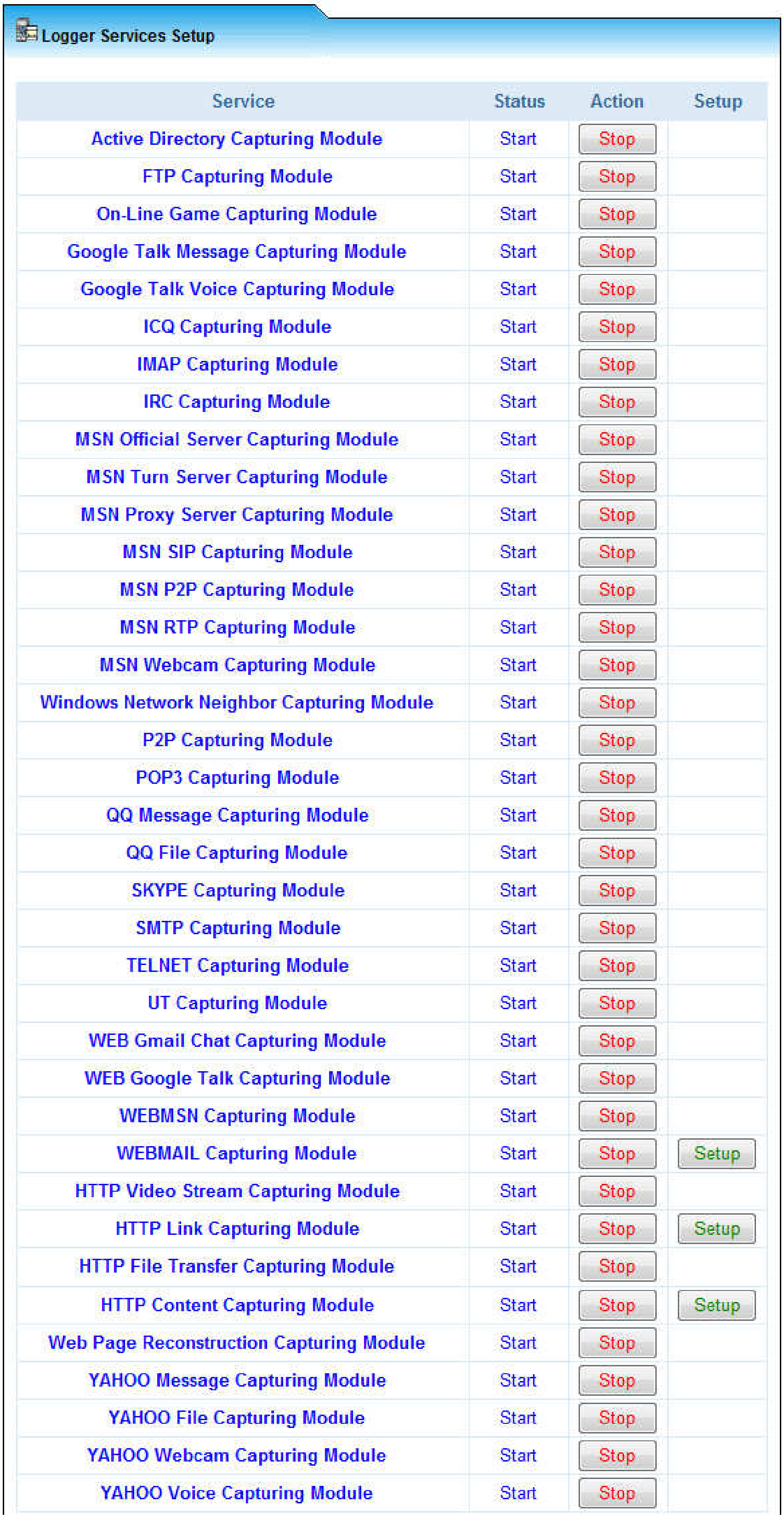
Account : frankie

Password : •••••••

retrive email every 05 mins

Logger Services

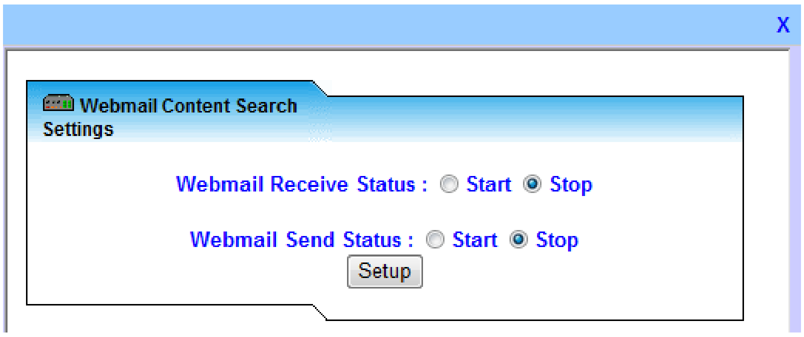
This section allows the Administrator to start or stop the logger services – protocols decoding and reconstruction.



Logger Services Setup

Service	Status	Action	Setup
Active Directory Capturing Module	Start	Stop	
FTP Capturing Module	Start	Stop	
On-Line Game Capturing Module	Start	Stop	
Google Talk Message Capturing Module	Start	Stop	
Google Talk Voice Capturing Module	Start	Stop	
ICQ Capturing Module	Start	Stop	
IMAP Capturing Module	Start	Stop	
IRC Capturing Module	Start	Stop	
MSN Official Server Capturing Module	Start	Stop	
MSN Turn Server Capturing Module	Start	Stop	
MSN Proxy Server Capturing Module	Start	Stop	
MSN SIP Capturing Module	Start	Stop	
MSN P2P Capturing Module	Start	Stop	
MSN RTP Capturing Module	Start	Stop	
MSN Webcam Capturing Module	Start	Stop	
Windows Network Neighbor Capturing Module	Start	Stop	
P2P Capturing Module	Start	Stop	
POP3 Capturing Module	Start	Stop	
QQ Message Capturing Module	Start	Stop	
QQ File Capturing Module	Start	Stop	
SKYPE Capturing Module	Start	Stop	
SMTP Capturing Module	Start	Stop	
TELNET Capturing Module	Start	Stop	
UT Capturing Module	Start	Stop	
WEB Gmail Chat Capturing Module	Start	Stop	
WEB Google Talk Capturing Module	Start	Stop	
WEBMSN Capturing Module	Start	Stop	
WEBMAIL Capturing Module	Start	Stop	Setup
HTTP Video Stream Capturing Module	Start	Stop	
HTTP Link Capturing Module	Start	Stop	Setup
HTTP File Transfer Capturing Module	Start	Stop	
HTTP Content Capturing Module	Start	Stop	Setup
Web Page Reconstruction Capturing Module	Start	Stop	
YAHOO Message Capturing Module	Start	Stop	
YAHOO File Capturing Module	Start	Stop	
YAHOO Webcam Capturing Module	Start	Stop	
YAHOO Voice Capturing Module	Start	Stop	

Webmail Capturing Module
This section allows the Administrator to activate or de-activate Webmail (Read and Send) content search function.



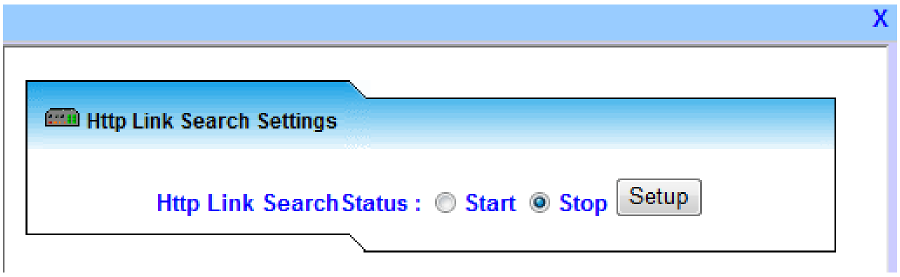
X

Webmail Content Search Settings

Webmail Receive Status : ○ Start ● Stop

Webmail Send Status : ○ Start ● Stop

HTTP Link Module
This section allows the Administrator to activate or de-active HTTP Link search function.

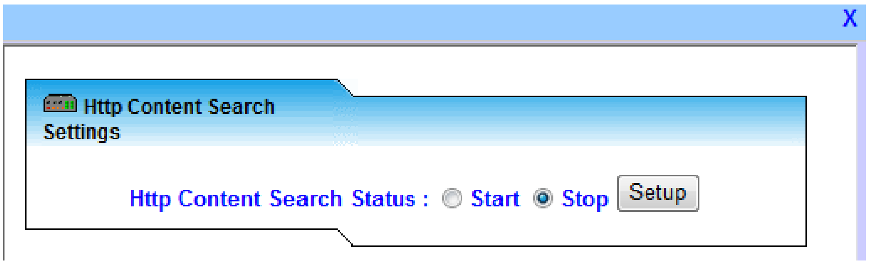


X

Http Link Search Settings

Http Link Search Status : ○ Start ● Stop

HTTP Content Module
This section allows the Administrator to activate or de-activate HTTP Content search function.



X

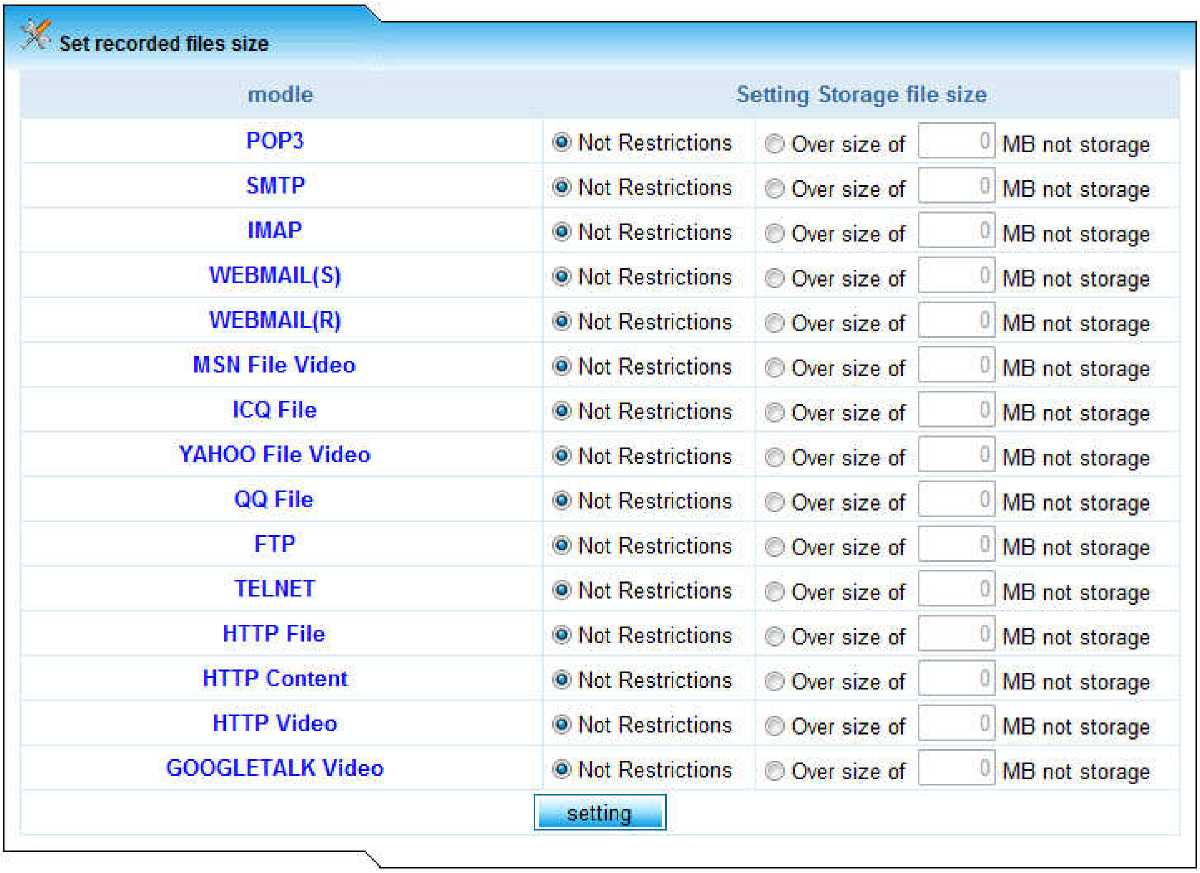
Http Content Search Settings

Http Content Search Status : ○ Start ● Stop

Note: Without activating this setup, the system by default will not provide the search function for Webmail and HTTP Content.

Set Logger File Size

This section allows the Administrator to set the file size limit for different Internet services which the system will reconstruct and stored.

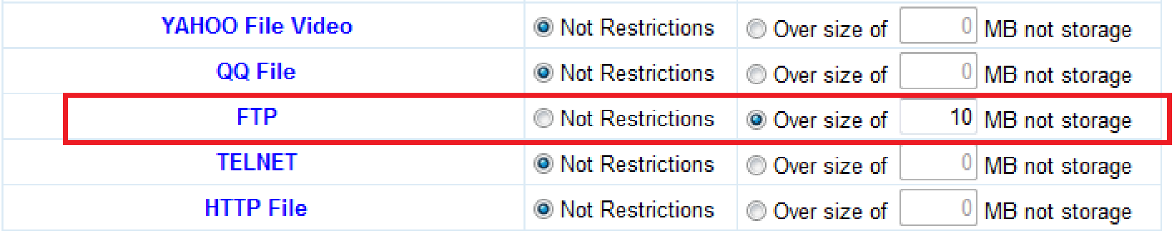


Set recorded files size

modle	Setting Storage file size			
POP3	● Not Restrictions	○ Over size of	0	MB not storage
SMTP	● Not Restrictions	○ Over size of	0	MB not storage
IMAP	● Not Restrictions	○ Over size of	0	MB not storage
WEBMAIL(S)	● Not Restrictions	○ Over size of	0	MB not storage
WEBMAIL(R)	● Not Restrictions	○ Over size of	0	MB not storage
MSN File Video	● Not Restrictions	○ Over size of	0	MB not storage
ICQ File	● Not Restrictions	○ Over size of	0	MB not storage
YAHOO File Video	● Not Restrictions	○ Over size of	0	MB not storage
QQ File	● Not Restrictions	○ Over size of	0	MB not storage
FTP	● Not Restrictions	○ Over size of	0	MB not storage
TELNET	● Not Restrictions	○ Over size of	0	MB not storage
HTTP File	● Not Restrictions	○ Over size of	0	MB not storage
HTTP Content	● Not Restrictions	○ Over size of	0	MB not storage
HTTP Video	● Not Restrictions	○ Over size of	0	MB not storage
GOOGLETALK Video	● Not Restrictions	○ Over size of	0	MB not storage

Example:

Set FTP file limit to 10 MB. This means if the FTP download/upload file size is more than 10 MB, the system will not store this file in the system. However, the FTP log will still be obtained.

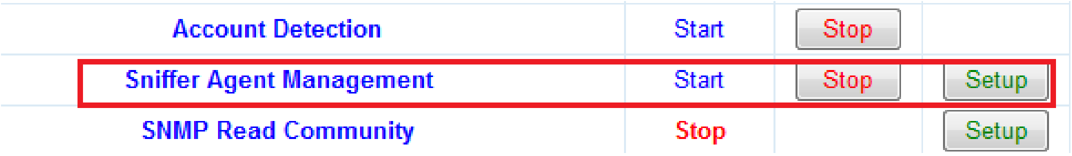


YAHOO File Video	● Not Restrictions	○ Over size of	0	MB not storage
QQ File	● Not Restrictions	○ Over size of	0	MB not storage
FTP	○ Not Restrictions	● Over size of	10	MB not storage
TELNET	● Not Restrictions	○ Over size of	0	MB not storage
HTTP File	● Not Restrictions	○ Over size of	0	MB not storage

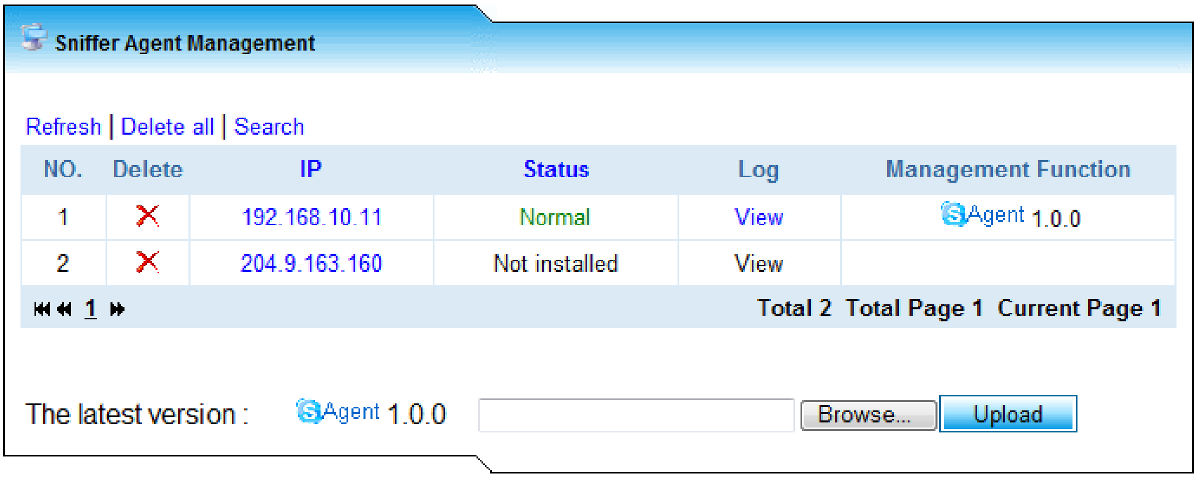
Sniffer Agent Management (Additional Paid Service)

ICI supports QQ 2010 version and Skype text message + VoIP conversation recording through the implementation of Audit/Sniffer Agent. This Audit/Sniffer Agent needs to be manually pre-installed on the targeted user's PC on the network.

Administrator needs to start the Skype Sniffer Agent service at system service setup page.



Account Detection	Start	Stop	
Sniffer Agent Management	Start	Stop	Setup
SNMP Read Community	Stop		Setup



Sniffer Agent Management

Refresh | Delete all | Search

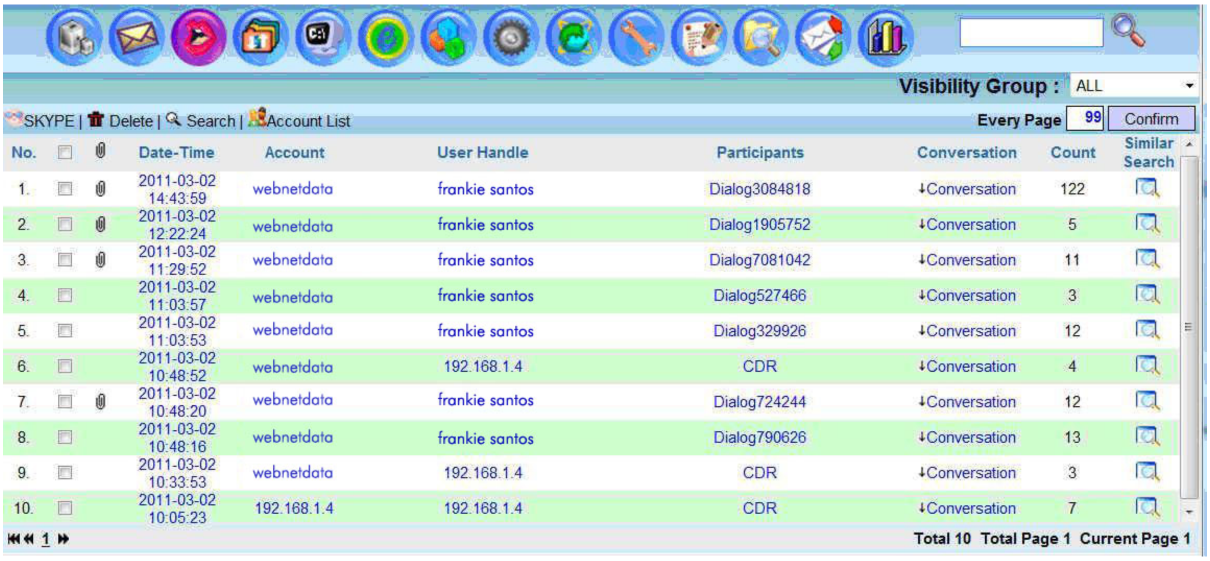
NO.	Delete	IP	Status	Log	Management Function
1	✕	192.168.10.11	Normal	View	Agent 1.0.0
2	✕	204.9.163.160	Not installed	View	

⏮ ⏪ 1 ⏩ Total 2 Total Page 1 Current Page 1

The latest version : Agent 1.0.0 Browse... Upload

The Sniffer Agent Management page will List out the local network PC (IP Address) with Skype Agent installed or not yet installed. Administrator need to select the target PC with the Audit/Sniffer Agent installed and register it on the ED system. Administrator can refresh this page, delete and search for local PC using this management GUI.

Besides, Administrator can also update the latest version of Skype Agent once through this GUI.



Visibility Group : ALL

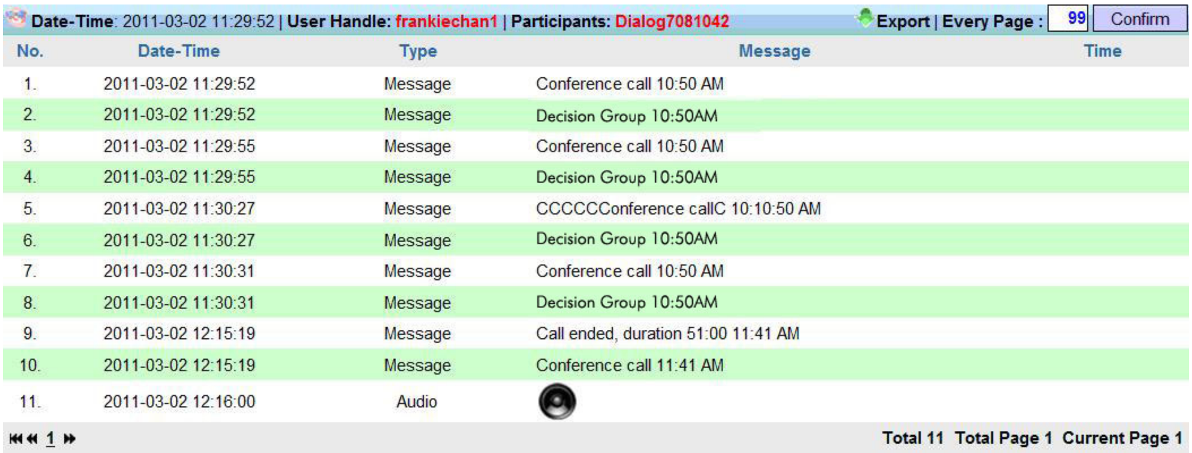
SKYPE | Delete | Search | Account List

Every Page 99 Confirm

No.	☐	📎	Date-Time	Account	User Handle	Participants	Conversation	Count	Similar Search
1.	☐	📎	2011-03-02 14:43:59	webnetdata	frankie santos	Dialog3084818	↓Conversation	122	🔍
2.	☐	📎	2011-03-02 12:22:24	webnetdata	frankie santos	Dialog1905752	↓Conversation	5	🔍
3.	☐	📎	2011-03-02 11:29:52	webnetdata	frankie santos	Dialog7081042	↓Conversation	11	🔍
4.	☐		2011-03-02 11:03:57	webnetdata	frankie santos	Dialog527466	↓Conversation	3	🔍
5.	☐		2011-03-02 11:03:53	webnetdata	frankie santos	Dialog329926	↓Conversation	12	🔍
6.	☐		2011-03-02 10:48:52	webnetdata	192.168.1.4	CDR	↓Conversation	4	🔍
7.	☐	📎	2011-03-02 10:48:20	webnetdata	frankie santos	Dialog724244	↓Conversation	12	🔍
8.	☐		2011-03-02 10:48:16	webnetdata	frankie santos	Dialog790626	↓Conversation	13	🔍
9.	☐		2011-03-02 10:33:53	webnetdata	192.168.1.4	CDR	↓Conversation	3	🔍
10.	☐		2011-03-02 10:05:23	192.168.1.4	192.168.1.4	CDR	↓Conversation	7	🔍

1 Total 10 Total Page 1 Current Page 1

Diagram: Skype Text Chat Message and Voice Call Capture by Sniffer Agent



Date-Time: 2011-03-02 11:29:52 | **User Handle: frankiechan1** | **Participants: Dialog7081042**

Export | Every Page : 99 Confirm

No.	Date-Time	Type	Message	Time
1.	2011-03-02 11:29:52	Message	Conference call 10:50 AM	
2.	2011-03-02 11:29:52	Message	Decision Group 10:50AM	
3.	2011-03-02 11:29:55	Message	Conference call 10:50 AM	
4.	2011-03-02 11:29:55	Message	Decision Group 10:50AM	
5.	2011-03-02 11:30:27	Message	CCCCCConference callC 10:10:50 AM	
6.	2011-03-02 11:30:27	Message	Decision Group 10:50AM	
7.	2011-03-02 11:30:31	Message	Conference call 10:50 AM	
8.	2011-03-02 11:30:31	Message	Decision Group 10:50AM	
9.	2011-03-02 12:15:19	Message	Call ended, duration 51:00 11:41 AM	
10.	2011-03-02 12:15:19	Message	Conference call 11:41 AM	
11.	2011-03-02 12:16:00	Audio	●	

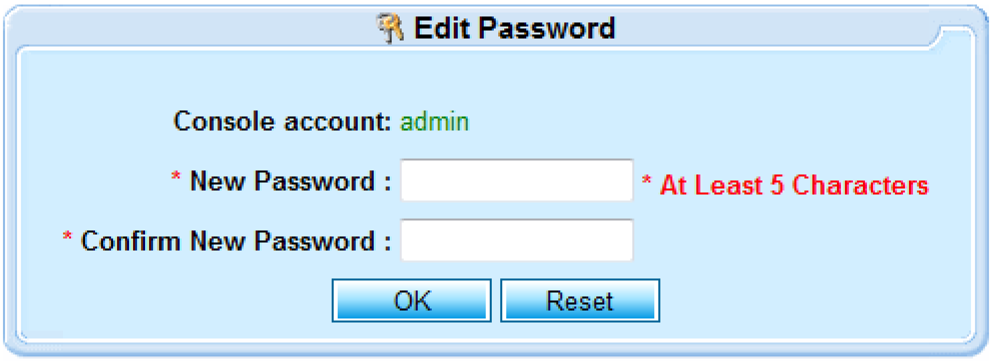
1 Total 11 Total Page 1 Current Page 1

Diagram: The conversation will contain the text chat and voice call record

Note: Please ensure the Sniffer Agent (purchased) has been installed successfully at target user PC. Go to Task Manager and verified that decage.exe and s_mo.exe are running.

Edit Password

Administrator can change the system console (client console access – by putty or monitor console) and FTP access password through this GUI. The console account name is default set as “admin” and not is editable.



Edit Password

Console account: admin

* New Password : * At Least 5 Characters

* Confirm New Password :

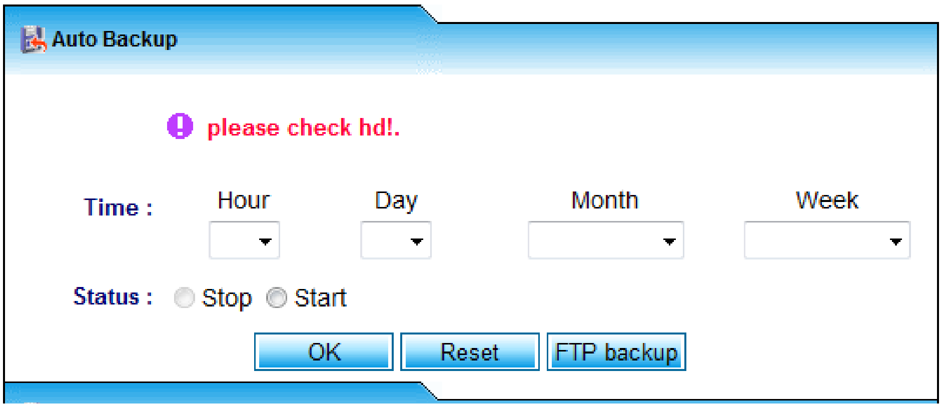
Backup Data

There are 3 configuration modes for data backup which are Auto Backup, Manual Backup and FTP Backup.

Auto Backup

Auto Backup will automatically backup the reconstructed data files (DBtag files) into ISO file. It contains 3 sections: Scheduling, Selection of Backup Modules and Notification.

Auto Backup – Schedule



Auto Backup

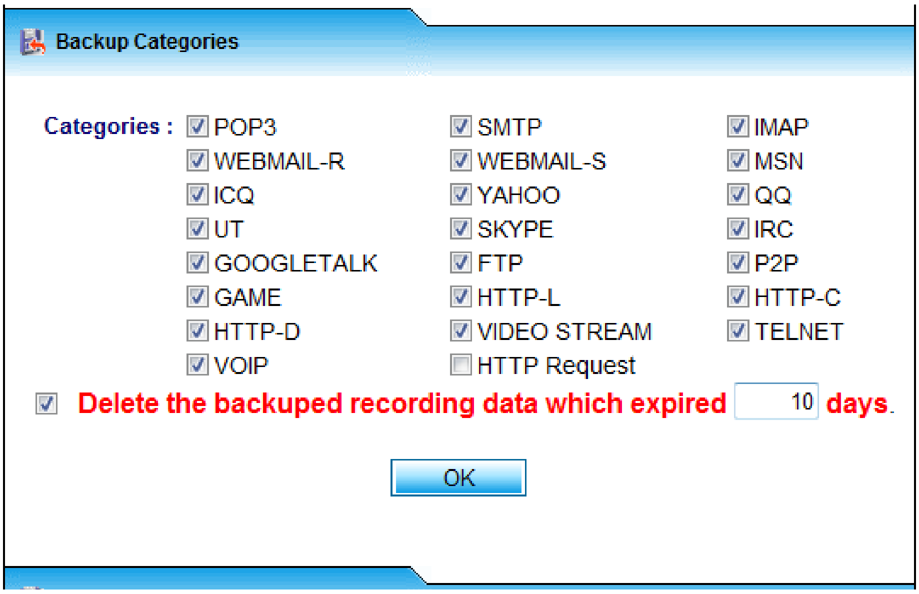
please check hd!.

Time : Hour Day Month Week

Status : ○ Stop ○ Start

On this section, the Administrator can setup the schedule to enable the system to start the backup process automatically at pre-defined date-time. It allows the Administrator to schedule the auto backup by hour (0-24 Hour of the Day), day (1-31 Day of the Month), week (Sunday-Saturday) and month (January-December). It also allows the Administrator to upload this auto backup reconstructed data to FTP server for storage.

Auto Backup - Backup Categories



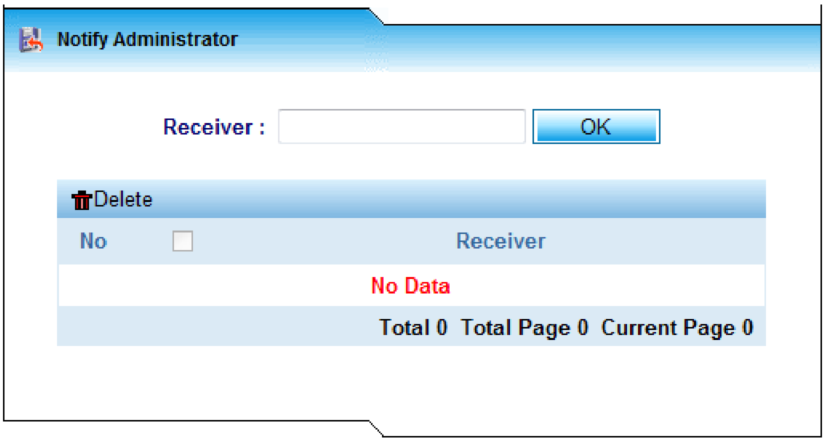
Backup Categories

Categories : ☑ POP3 ☑ SMTP ☑ IMAP
☑ WEBMAIL-R ☑ WEBMAIL-S ☑ MSN
☑ ICQ ☑ YAHOO ☑ QQ
☑ UT ☑ SKYPE ☑ IRC
☑ GOOGLETALK ☑ FTP ☑ P2P
☑ GAME ☑ HTTP-L ☑ HTTP-C
☑ HTTP-D ☑ VIDEO STREAM ☑ TELNET
☑ VOIP □ HTTP Request

☑ Delete the backuped recording data which expired 10 days.

Administrator can select the service categories for backup. Administrator can also define storage days of the reconstructed data files (DBtag file) after the backup file (in ISO format) has been created.

Auto Backup – Administrator Notification



Notify Administrator

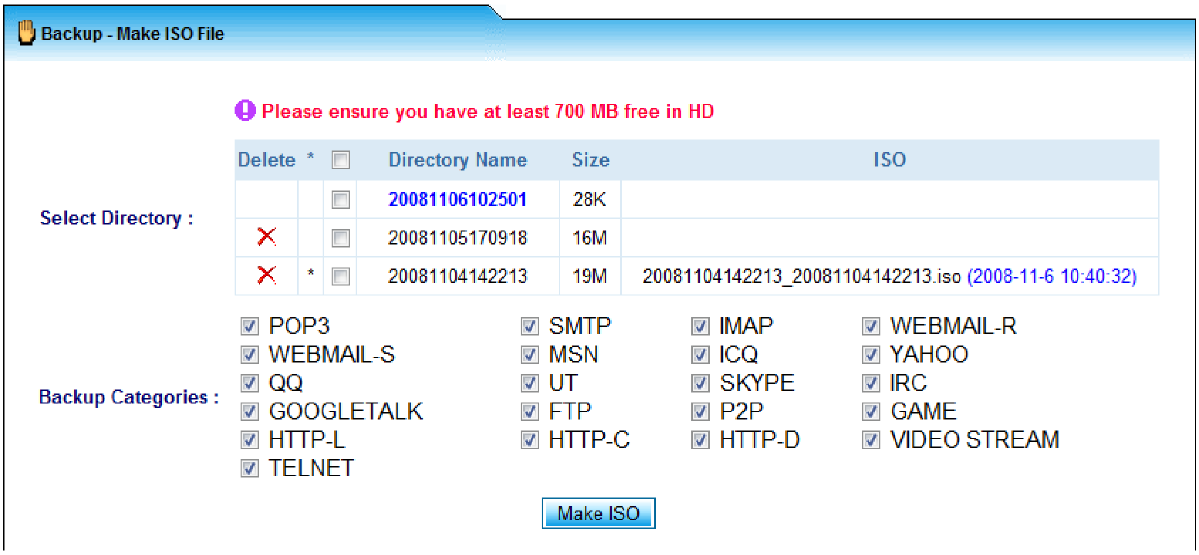
Receiver :

No	□	Receiver
	No Data	
		Total 0 Total Page 0 Current Page 0

Once the system complete the automatic backup (created the ISO file at the specified date-time), the system can send notification to the defined user Email.

Manual Backup

This section allows the Administrator to create backup ISO file manually. Administrator can select the reconstructed data files (DBtag files) and backup service categories for backup into ISO format before burning out in to CD/DVD or export into external storage.



Backup - Make ISO File

Please ensure you have at least 700 MB free in HD

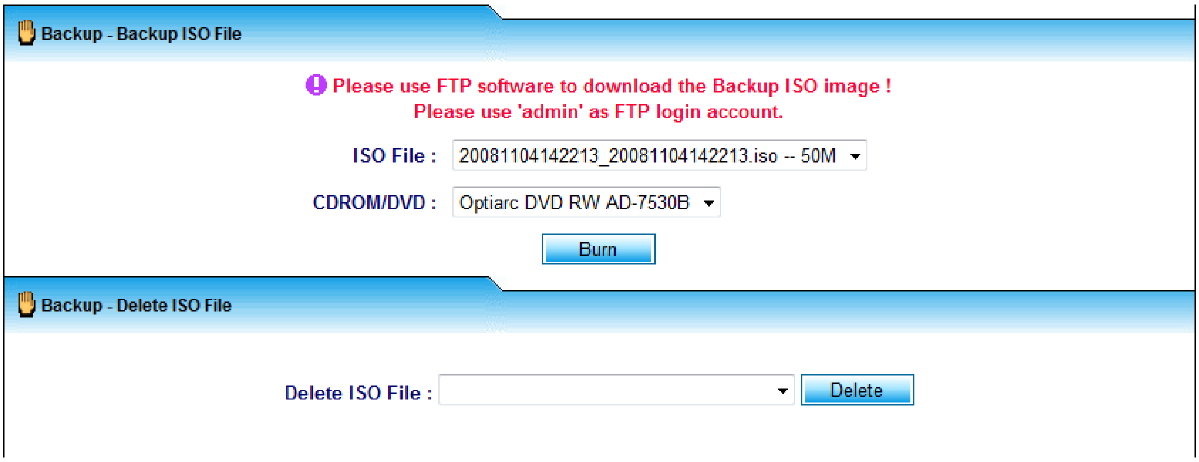
Select Directory :

Delete	*	□	Directory Name	Size	ISO
		□	20081106102501	28K	
✗		□	20081105170918	16M	
✗	*	□	20081104142213	19M	20081104142213_20081104142213.iso (2008-11-6 10:40:32)

Backup Categories :

☑ POP3
☑ WEBMAIL-S
☑ QQ
☑ GOOGLETALK
☑ HTTP-L
☑ TELNET
☑ SMTP
☑ MSN
☑ UT
☑ FTP
☑ HTTP-C
☑ IMAP
☑ ICQ
☑ SKYPE
☑ P2P
☑ HTTP-D
☑ WEBMAIL-R
☑ YAHOO
☑ IRC
☑ GAME
☑ VIDEO STREAM

Backup ISO files can be burned into CD/DVD or can be exported out or downloaded by FTP Client (with Console username/password). Backup ISO files can also be deleted.



Backup - Backup ISO File

Please use FTP software to download the Backup ISO image !
Please use 'admin' as FTP login account.

ISO File : 20081104142213_20081104142213.iso -- 50M

CDROM/DVD : Optiarc DVD RW AD-7530B

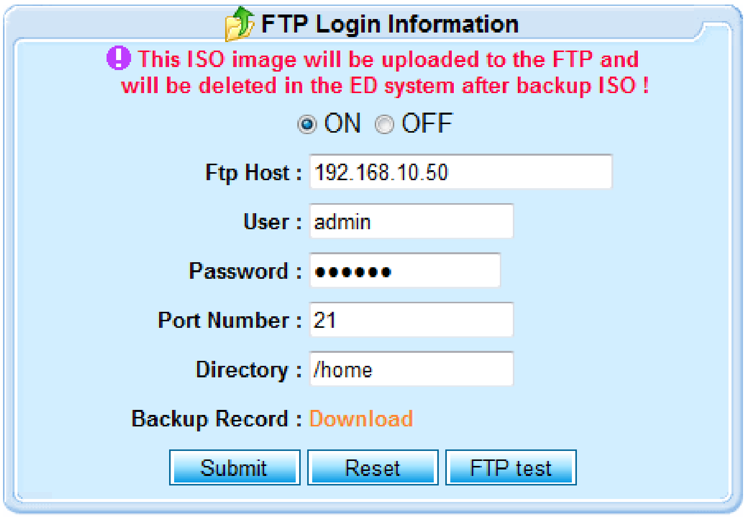
Backup - Delete ISO File

Delete ISO File :

FTP Backup

FTP Backup function allows the Administrator to upload Backup ISO file to a storage server such as NAS and SAN via FTP upload. It will upload the Backup ISO files created by Auto Backup to the FTP storage server. Please ensure that the Storage Server to support FTP upload function.

Note: User can opt to purchase Backup Server System from ICI which will allow user to store Backup ISO file and viewing the Backup ISO file.



FTP Login Information

This ISO image will be uploaded to the FTP and will be deleted in the ED system after backup ISO !

● ON ○ OFF

Ftp Host : 192.168.10.50

User : admin

Password : ●●●●●●

Port Number : 21

Directory : /home

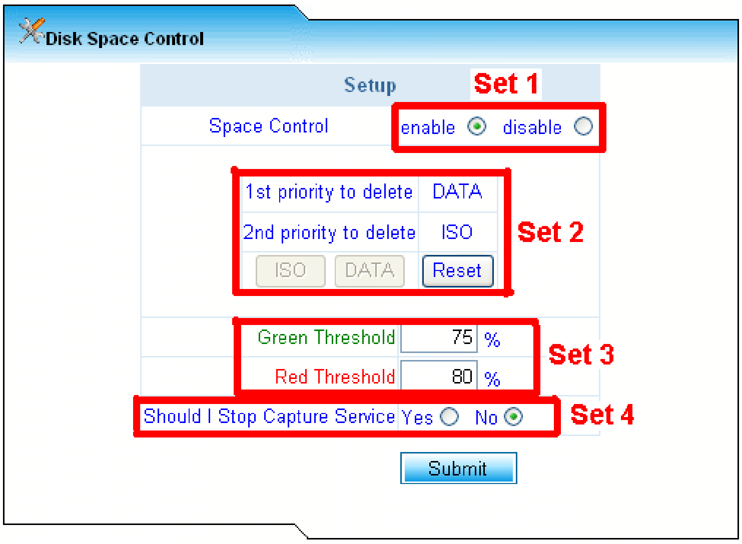
Backup Record : Download

Features in this GUI:

1) FTP Host: The FTP server IP address where the backup ISO file is to be sent to
2) User: The FTP username account.
3) Password: The FTP password.
4) Port Number: The FTP port number used to transmit the data
5) Directory: The directory where the backup ISO file is stored.
6) Backup Record: User can download the ISO file after it has been uploaded successfully to FTP server.
7) ON/OFF is to activate/de-activate the FTP backup function.
8) Click on [Submit] button to save the setting. Click on [Reset] button to clear up all values on each field.
9) FTP Test: To test the FTP server/storage connection

Disk Space Control

The Disk Space Control allows Administrator to control the data storage inside the hard disk of the ICI system with Red Threshold and Green Threshold setting.



Disk Space Control

Setup

Set 1

Space Control: enable ● disable ○

1st priority to delete	DATA
2nd priority to delete	ISO

Set 2

Green Threshold 75 %

Red Threshold 80 %

Set 3

Should I Stop Capture Service Yes ○ No ●

Set 4

Set 1: Enable or disable the disk space control function.

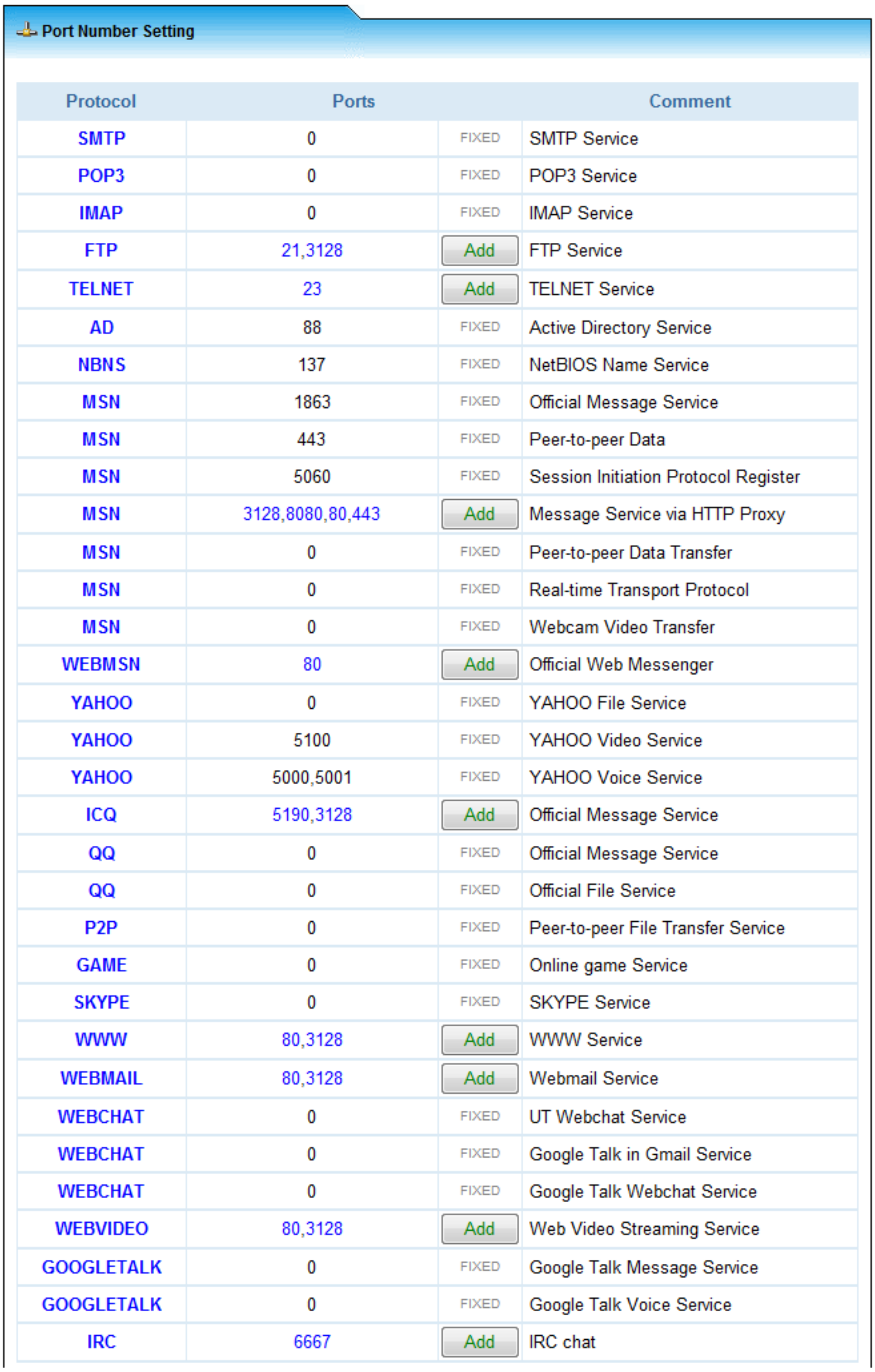
Set 2: Select either ISO Backup File as first priority or DATA file as first priority. Administrator can reset the setting by click on the [Reset] button.

Set 3: Red Threshold and Green Threshold Setting. Red Threshold is the hard disk space capacity in % where it will trigger the alert for delete off the old data (%) defined by Green Threshold. For example: Red Threshold is set at 80% and Green Threshold is set at 50%. When the hard disk space reaches 80% capacity, it will delete off 30% of the older data from the hard disk.

System Status

Port Number

This function allows the Administrator to inspect each protocol and set the port number value for those service categories where the port number is variable. Administrator can add and delete port number manually for different defined Internet protocols.

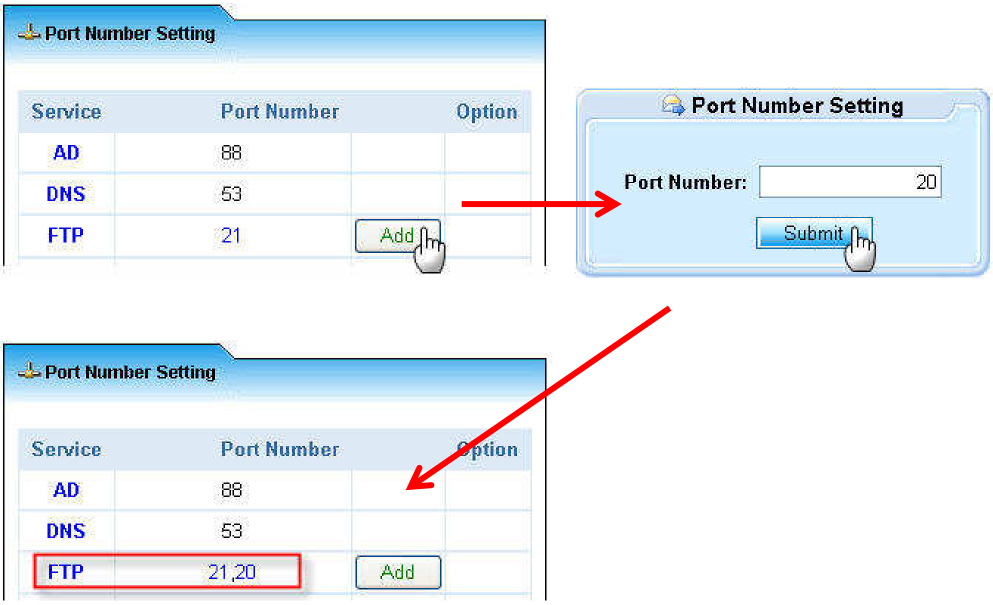


Port Number Setting

Protocol	Ports		Comment
SMTP	0	FIXED	SMTP Service
POP3	0	FIXED	POP3 Service
IMAP	0	FIXED	IMAP Service
FTP	21,3128	Add	FTP Service
TELNET	23	Add	TELNET Service
AD	88	FIXED	Active Directory Service
NBNS	137	FIXED	NetBIOS Name Service
MSN	1863	FIXED	Official Message Service
MSN	443	FIXED	Peer-to-peer Data
MSN	5060	FIXED	Session Initiation Protocol Register
MSN	3128,8080,80,443	Add	Message Service via HTTP Proxy
MSN	0	FIXED	Peer-to-peer Data Transfer
MSN	0	FIXED	Real-time Transport Protocol
MSN	0	FIXED	Webcam Video Transfer
WEBMSN	80	Add	Official Web Messenger
YAHOO	0	FIXED	YAHOO File Service
YAHOO	5100	FIXED	YAHOO Video Service
YAHOO	5000,5001	FIXED	YAHOO Voice Service
ICQ	5190,3128	Add	Official Message Service
QQ	0	FIXED	Official Message Service
QQ	0	FIXED	Official File Service
P2P	0	FIXED	Peer-to-peer File Transfer Service
GAME	0	FIXED	Online game Service
SKYPE	0	FIXED	SKYPE Service
WWW	80,3128	Add	WWW Service
WEBMAIL	80,3128	Add	Webmail Service
WEBCHAT	0	FIXED	UT Webchat Service
WEBCHAT	0	FIXED	Google Talk in Gmail Service
WEBCHAT	0	FIXED	Google Talk Webchat Service
WEBVIDEO	80,3128	Add	Web Video Streaming Service
GOOGLETALK	0	FIXED	Google Talk Message Service
GOOGLETALK	0	FIXED	Google Talk Voice Service
IRC	6667	Add	IRC chat

Add New Port

By clicking on the [Add] button, Administrator can add new port number. Click [Submit] to finalize the adding of port number.



Port Number Setting

Service	Port Number	Option
AD	88	
DNS	53	
FTP	21	Add

Port Number Setting

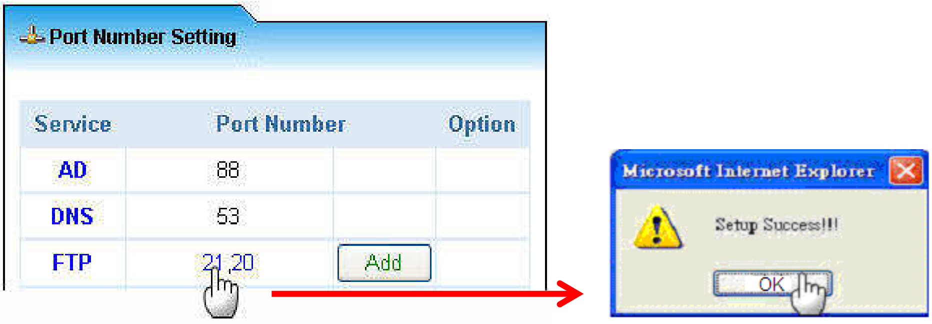
Port Number: 20

Port Number Setting

Service	Port Number	Option
AD	88	
DNS	53	
FTP	21,20	Add

Delete Port Number

By clicking on the port number, admin can delete the port number for the particular service.



Port Number Setting

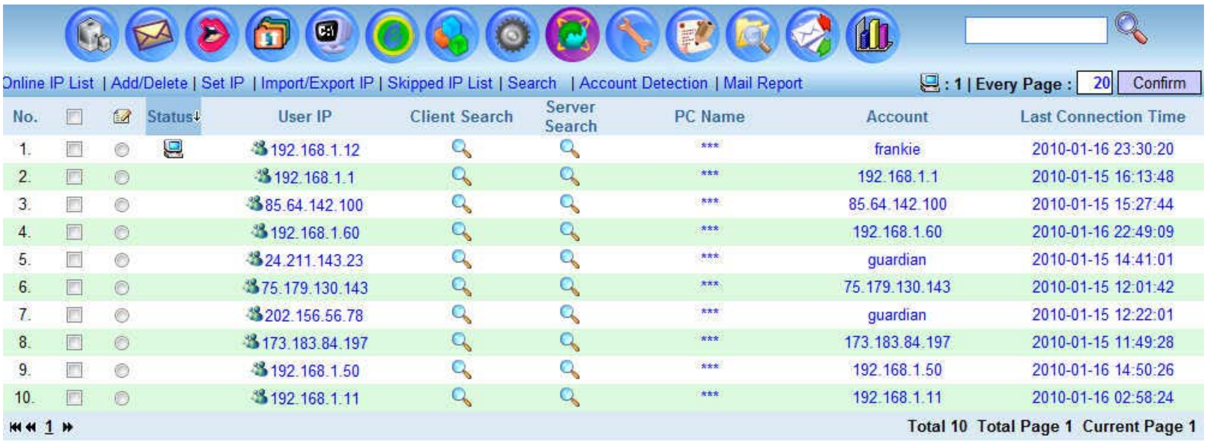
Service	Port Number	Option
AD	88	
DNS	53	
FTP	21,20	Add

Microsoft Internet Explorer

Setup Success!!!

Online IP

Online IP will List out all the IP addresses with Accounts on the targeted organization network automatically. ICI system will auto detect these online IP addresses through network packets transmitted and collected from the organization network.



Online IP List | Add/Delete | Set IP | Import/Export IP | Skipped IP List | Search | Account Detection | Mail Report

🖥 : 1 | Every Page : 20 Confirm

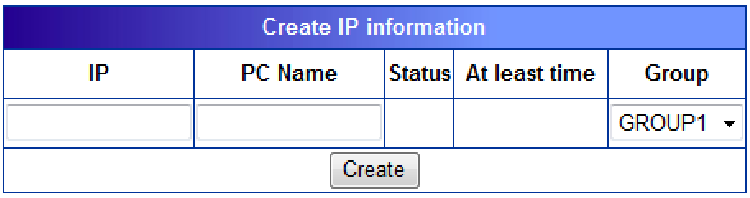
No.	□	✎	Status↓	User IP	Client Search	Server Search	PC Name	Account	Last Connection Time
1.	□	○	🖥	192.168.1.12	🔍	🔍	***	frankie	2010-01-16 23:30:20
2.	□	○		192.168.1.1	🔍	🔍	***	192.168.1.1	2010-01-15 16:13:48
3.	□	○		85.64.142.100	🔍	🔍	***	85.64.142.100	2010-01-15 15:27:44
4.	□	○		192.168.1.60	🔍	🔍	***	192.168.1.60	2010-01-16 22:49:09
5.	□	○		24.211.143.23	🔍	🔍	***	guardian	2010-01-15 14:41:01
6.	□	○		75.179.130.143	🔍	🔍	***	75.179.130.143	2010-01-15 12:01:42
7.	□	○		202.156.56.78	🔍	🔍	***	guardian	2010-01-15 12:22:01
8.	□	○		173.183.84.197	🔍	🔍	***	173.183.84.197	2010-01-15 11:49:28
9.	□	○		192.168.1.50	🔍	🔍	***	192.168.1.50	2010-01-16 14:50:26
10.	□	○		192.168.1.11	🔍	🔍	***	192.168.1.11	2010-01-16 02:58:24

⏮ ⏪ 1 ⏩ Total 10 Total Page 1 Current Page 1

Features in this Online IP GUI:

1) Online IP List: Click to refresh the Online IP List content.
2) Add/Delete: To create, delete and auto search for Online IP
3) Set IP: To hide or skip certain IP.
4) Import/Export IP: To import IP List or export the Online IP List
5) Skipped IP List: List out all IP that is not recorded.
6) Search: To search for IP or account.
7) Account Detection: Start or stop the service of Account Detection
8) Mail Report: Send online IP List report to a specific Email.

Add/Delete – Create IP
Administrator can create IP List with PC Name and Group.



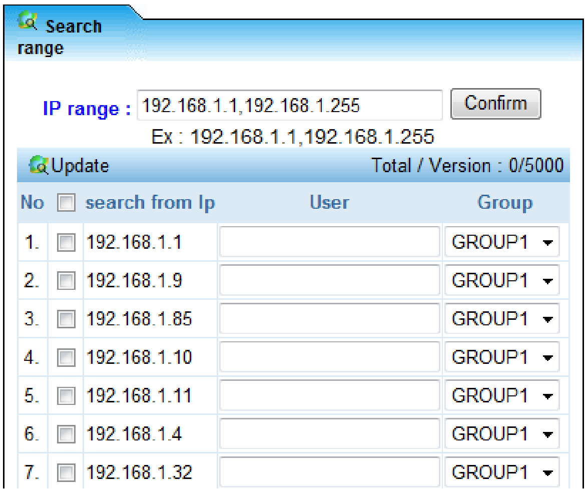
Create IP information

IP	PC Name	Status	At least time	Group
				GROUP1 ▾

Create

Add/Delete – Delete
Administrator can also delete the IP List by tick the IP check box at the Online IP List page. Then, click on Add/Delete – Delete to delete the IP record.

Add/Delete – Search
Administrator can also search for the IP in the organization network by subnet.



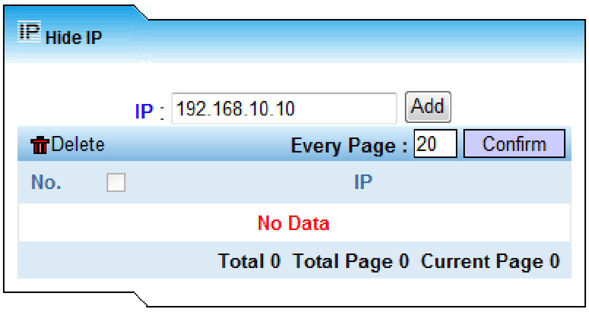
Search range

IP range : 192.168.1.1,192.168.1.255 Confirm
Ex : 192.168.1.1,192.168.1.255

Update Total / Version : 0/5000

No	□ search from Ip	User	Group
1.	□ 192.168.1.1		GROUP1 ▾
2.	□ 192.168.1.9		GROUP1 ▾
3.	□ 192.168.1.85		GROUP1 ▾
4.	□ 192.168.1.10		GROUP1 ▾
5.	□ 192.168.1.11		GROUP1 ▾
6.	□ 192.168.1.4		GROUP1 ▾
7.	□ 192.168.1.32		GROUP1 ▾

Set IP – Hide IP
Administrator can hide the IP record so that the specific IP information related to the particular IP will not be displayed.



Hide IP

IP : 192.168.10.10 Add

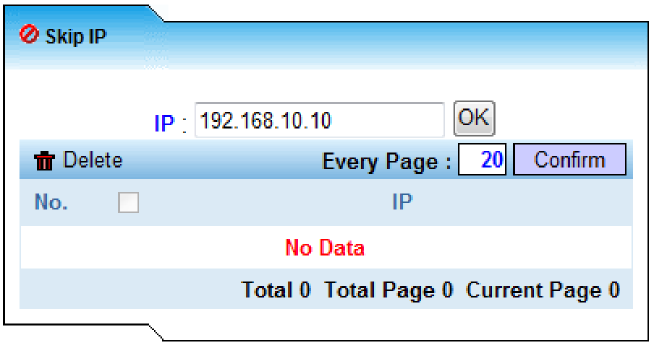
Delete Every Page : 20 Confirm

No.	□	IP
	No Data	

Total 0 Total Page 0 Current Page 0

Set IP – Skip IP

Administrator can skip specific IP so that all information related to this specific IP will not be captured.



Skip IP

IP : 192.168.10.10 OK

Delete Every Page : 20 Confirm

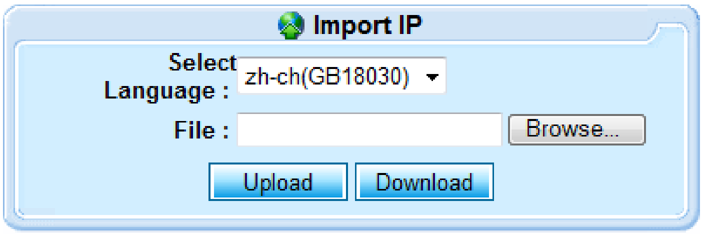
No. □ IP

No Data

Total 0 Total Page 0 Current Page 0

Import/Export IP

Administrator can import targeted IP List in Excel file format into the ICI system. Besides, Administrator can also download the IP List. Format: IP, PC NAME, GROUP. Please save the Excel file as *.CSV



Import IP

Select Language : zh-ch(GB18030)

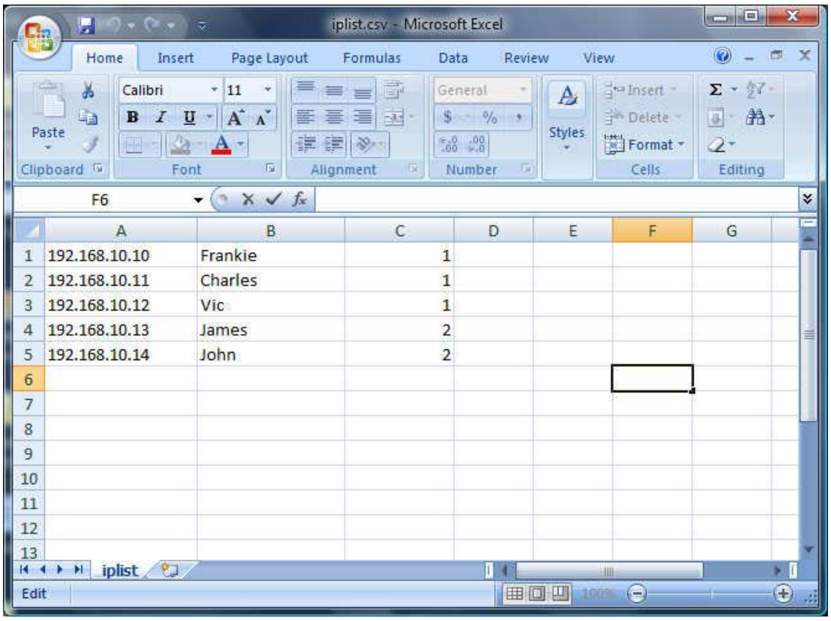
File :

Browse...

Upload

Download

Import Excel File Format



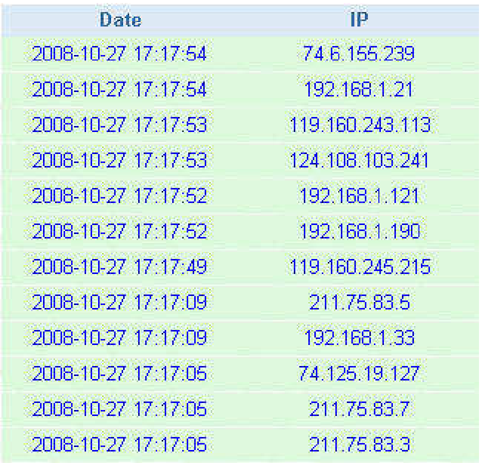
iplist.csv - Microsoft Excel

F6

	A	B	C	D	E	F	G
1	192.168.10.10	Frankie	1				
2	192.168.10.11	Charles	1				
3	192.168.10.12	Vic	1				
4	192.168.10.13	James	2				
5	192.168.10.14	John	2				
6							
7							
8							
9							
10							
11							
12							
13							

Skipped IP

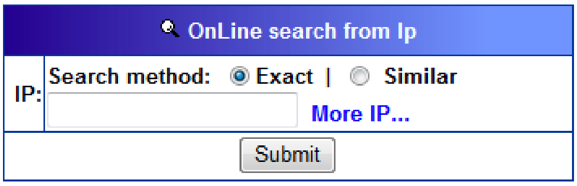
Skipped IP will display the IP addresses skipped and not captured by the system.



Date	IP
2008-10-27 17:17:54	74.6.155.239
2008-10-27 17:17:54	192.168.1.21
2008-10-27 17:17:53	119.160.243.113
2008-10-27 17:17:53	124.108.103.241
2008-10-27 17:17:52	192.168.1.121
2008-10-27 17:17:52	192.168.1.190
2008-10-27 17:17:49	119.160.245.215
2008-10-27 17:17:09	211.75.83.5
2008-10-27 17:17:09	192.168.1.33
2008-10-27 17:17:05	74.125.19.127
2008-10-27 17:17:05	211.75.83.7
2008-10-27 17:17:05	211.75.83.3

Search IP

This section allows the Administrator to search for a specific IP address.

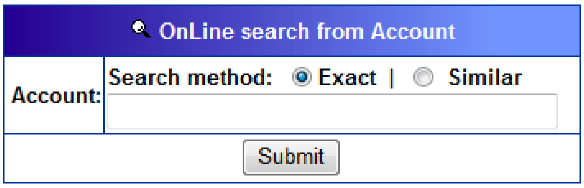


OnLine search from Ip

IP: Search method: ● Exact | ○ Similar

Search Account

This section allows the Administrator to search for a specific account.

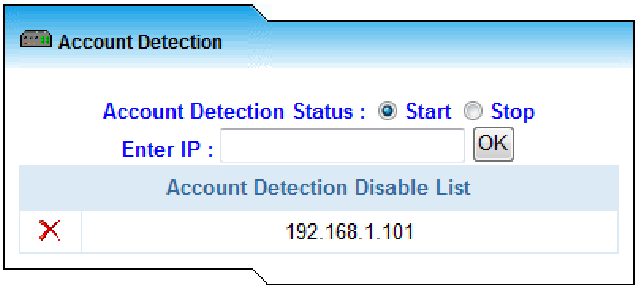


OnLine search from Account

Account: Search method: ● Exact | ○ Similar

Account Detection

This section allows the Administrator to start or stop the account detection service. Administrator can start or stop the account detection service for entire network (all online IPs) or Administrator can even specify to start or stop the account detection service for specific online IP.



Account Detection

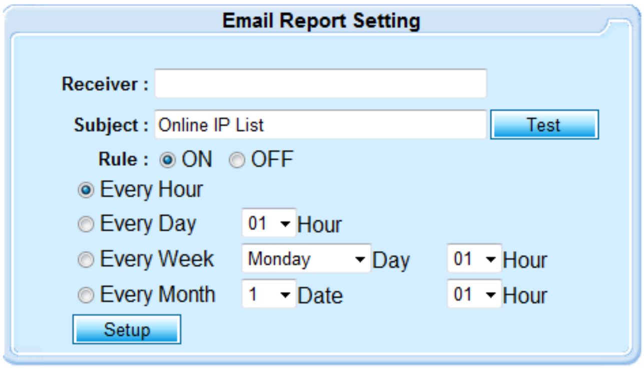
Account Detection Status : ● Start ○ Stop

Enter IP : OK

Account Detection Disable List	
✗	192.168.1.101

Mail Report

This section allows the Administrator to send Online IP List Report to Administrator through Email.



Email Report Setting

Receiver :

Subject : Online IP List

Rule : ● ON ○ OFF

● Every Hour

○ Every Day 01 Hour

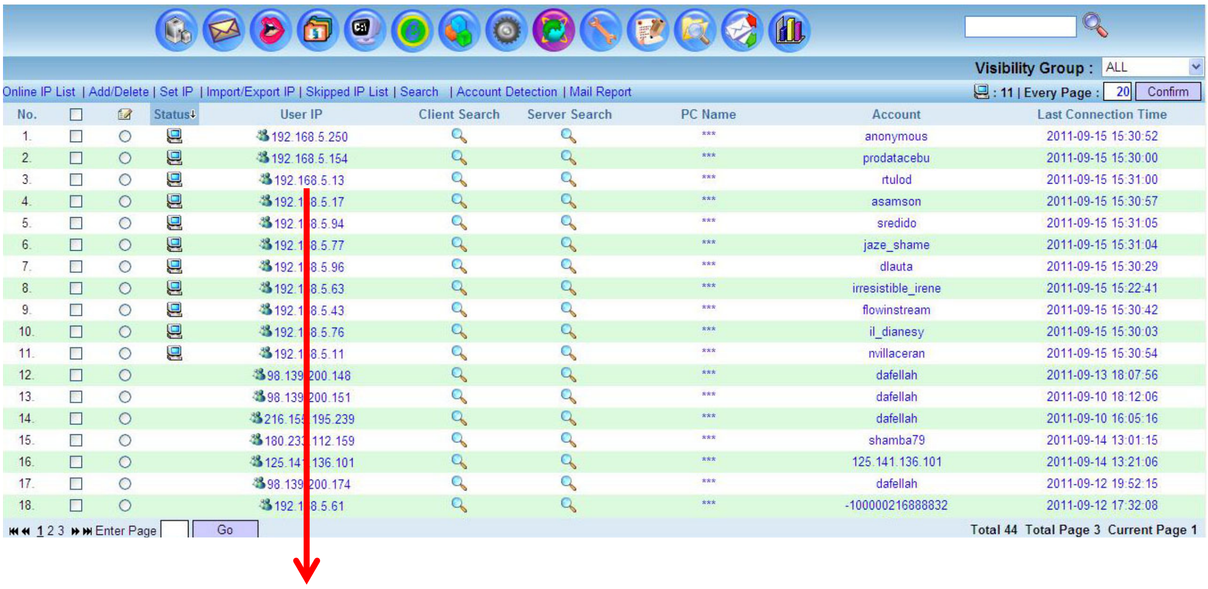
○ Every Week Monday Day 01 Hour

○ Every Month 1 Date 01 Hour

Online IP List – Traffic Statistics and Traffic Content

Online IP – User IP Statistics

When click on the User IP, Administrator can obtain the Daily Throughput Statistical Report of that particular IP.



Visibility Group : ALL

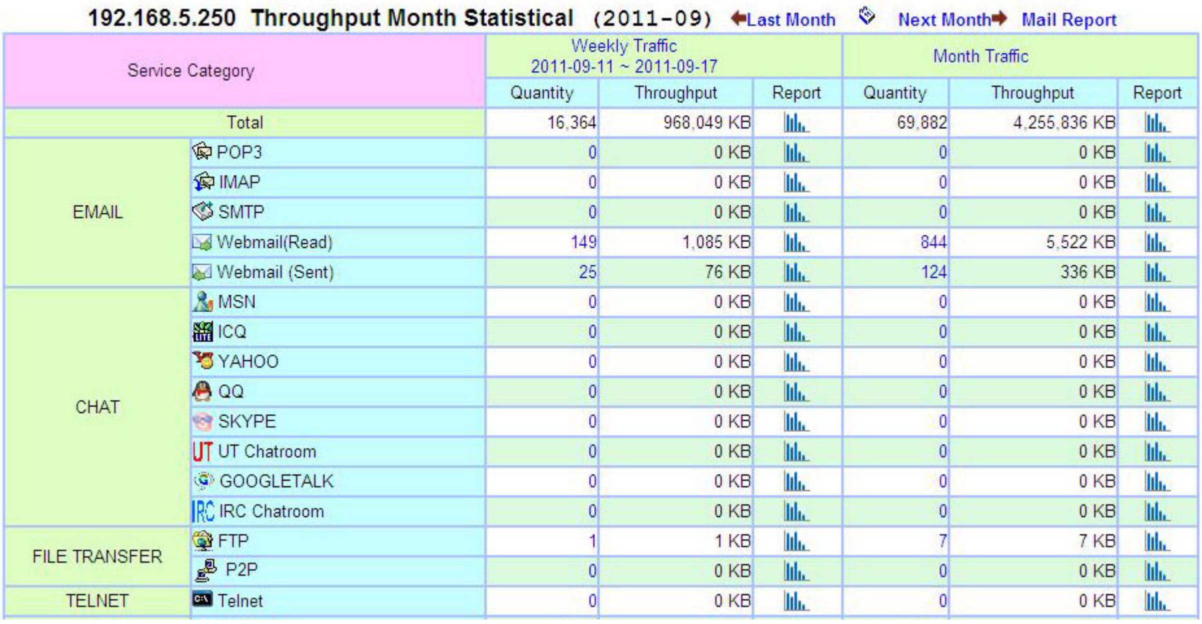
Online IP List | Add/Delete | Set IP | Import/Export IP | Skipped IP List | Search | Account Detection | Mail Report

🖥 : 11 | Every Page : 20 Confirm

No.	□		Status↓	User IP	Client Search	Server Search	PC Name	Account	Last Connection Time
1.	□	○	🖥	192.168.5.250	🔍	🔍	***	anonymous	2011-09-15 15:30:52
2.	□	○	🖥	192.168.5.154	🔍	🔍	***	prodatacebu	2011-09-15 15:30:00
3.	□	○	🖥	192.168.5.13	🔍	🔍	***	rtulod	2011-09-15 15:31:00
4.	□	○	🖥	192.1 8.5.17	🔍	🔍	***	asamson	2011-09-15 15:30:57
5.	□	○	🖥	192.1 8.5.94	🔍	🔍	***	sredido	2011-09-15 15:31:05
6.	□	○	🖥	192.1 8.5.77	🔍	🔍	***	jaze_shame	2011-09-15 15:31:04
7.	□	○	🖥	192.1 8.5.96	🔍	🔍	***	dlauta	2011-09-15 15:30:29
8.	□	○	🖥	192.1 8.5.63	🔍	🔍	***	irresistible_irene	2011-09-15 15:22:41
9.	□	○	🖥	192.1 8.5.43	🔍	🔍	***	flowinstream	2011-09-15 15:30:42
10.	□	○	🖥	192.1 8.5.76	🔍	🔍	***	il_dianesy	2011-09-15 15:30:03
11.	□	○	🖥	192.1 8.5.11	🔍	🔍	***	nvillaceran	2011-09-15 15:30:54
12.	□	○		98.139 200.148	🔍	🔍	***	dafellah	2011-09-13 18:07:56
13.	□	○		98.139 200.151	🔍	🔍	***	dafellah	2011-09-10 18:12:06
14.	□	○		216.15 195.239	🔍	🔍	***	dafellah	2011-09-10 16:05:16
15.	□	○		180.23 112.159	🔍	🔍	***	shamba79	2011-09-14 13:01:15
16.	□	○		125.14 136.101	🔍	🔍	***	125.141.136.101	2011-09-14 13:21:06
17.	□	○		98.139 200.174	🔍	🔍	***	dafellah	2011-09-12 19:52:15
18.	□	○		192.1 8.5.61	🔍	🔍	***	-100000216888832	2011-09-12 17:32:08

⏮ ⏪ 1 2 3 ⏩ ⏭ Enter Page Go

Total 44 Total Page 3 Current Page 1

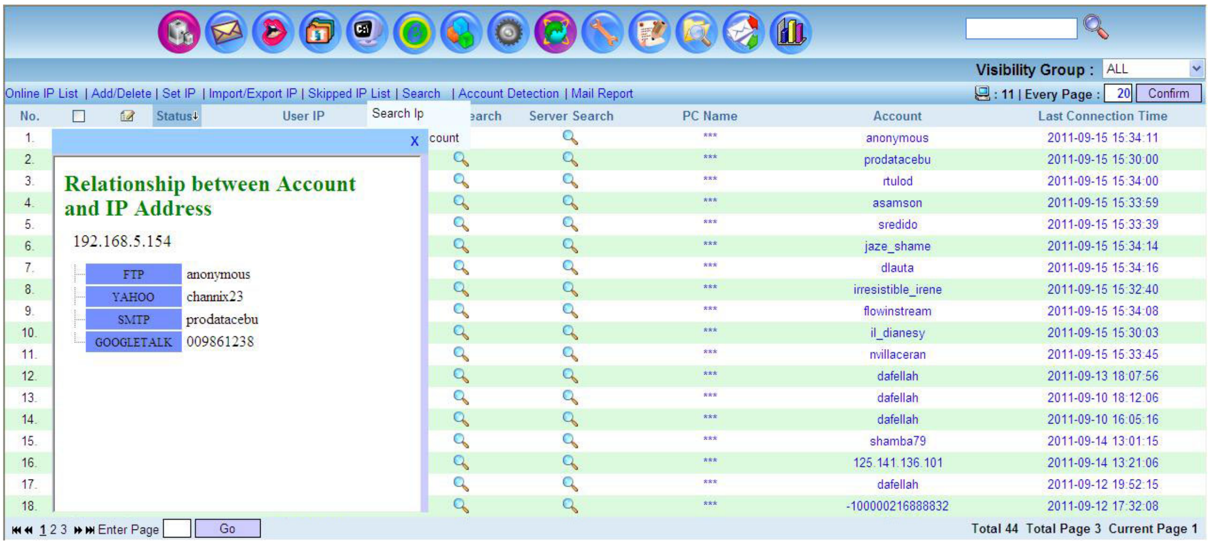


192.168.5.250 Throughput Month Statistical (2011-09) ←Last Month Next Month→ Mail Report

Service Category		Weekly Traffic 2011-09-11 ~ 2011-09-17			Month Traffic		
		Quantity	Throughput	Report	Quantity	Throughput	Report
Total		16,364	968,049 KB	📊	69,882	4,255,836 KB	📊
EMAIL	POP3	0	0 KB	📊	0	0 KB	📊
	IMAP	0	0 KB	📊	0	0 KB	📊
	SMTP	0	0 KB	📊	0	0 KB	📊
	Webmail(Read)	149	1,085 KB	📊	844	5,522 KB	📊
	Webmail (Sent)	25	76 KB	📊	124	336 KB	📊
CHAT	MSN	0	0 KB	📊	0	0 KB	📊
	ICQ	0	0 KB	📊	0	0 KB	📊
	YAHOO	0	0 KB	📊	0	0 KB	📊
	QQ	0	0 KB	📊	0	0 KB	📊
	SKYPE	0	0 KB	📊	0	0 KB	📊
	UT Chatroom	0	0 KB	📊	0	0 KB	📊
	GOOGLETALK	0	0 KB	📊	0	0 KB	📊
	IRC Chatroom	0	0 KB	📊	0	0 KB	📊
FILE TRANSFER	FTP	1	1 KB	📊	7	7 KB	📊
	P2P	0	0 KB	📊	0	0 KB	📊
TELNET	Telnet	0	0 KB	📊	0	0 KB	📊

IP Relationship

Click on the icon as shown in below diagram will provide you the List or related user accounts of various Internet services for that particular user IP.



Visibility Group : ALL

Online IP List | Add/Delete | Set IP | Import/Export IP | Skipped IP List | Search | Account Detection | Mail Report

: 11 | Every Page : 20 Confirm

Search Ip

Relationship between Account and IP Address

192.168.5.154

FTP	anonymous
YAHOO	channix23
SMTP	prodatacebu
GOOGLETALK	009861238

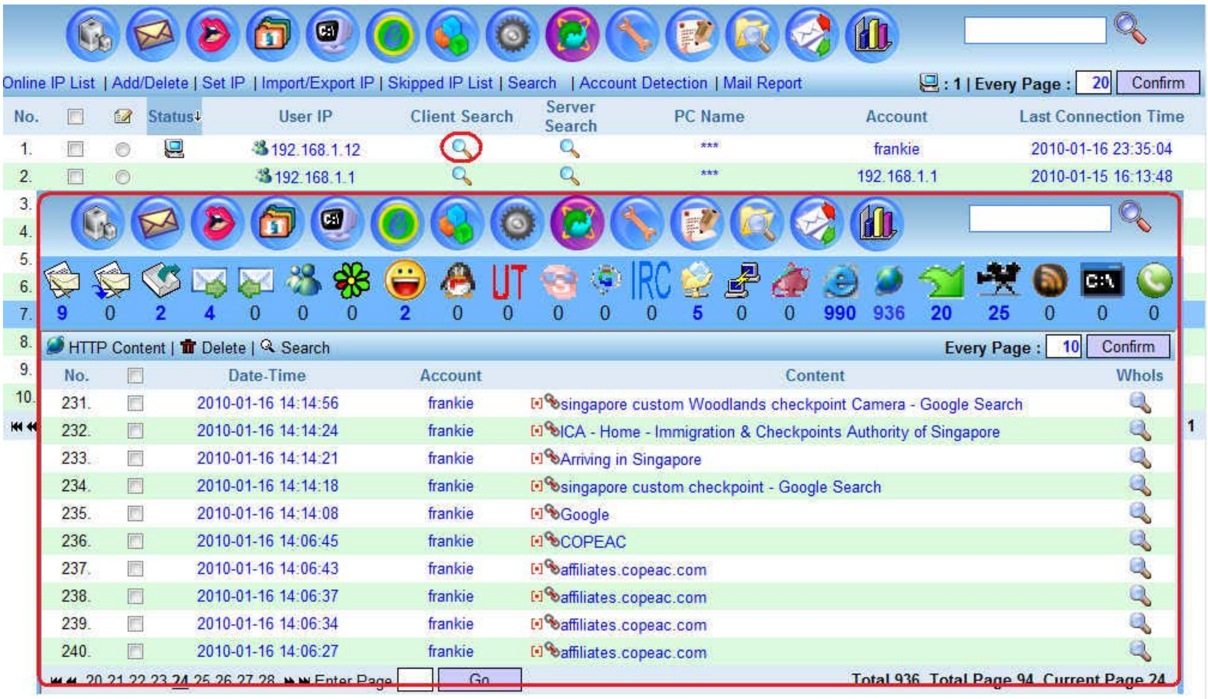
No.	Server Search	PC Name	Account	Last Connection Time
1.	🔍	***	anonymous	2011-09-15 15:34:11
2.	🔍	***	prodatacebu	2011-09-15 15:30:00
3.	🔍	***	rtulod	2011-09-15 15:34:00
4.	🔍	***	asamson	2011-09-15 15:33:59
5.	🔍	***	sredido	2011-09-15 15:33:39
6.	🔍	***	jaze_shame	2011-09-15 15:34:14
7.	🔍	***	dlauta	2011-09-15 15:34:16
8.	🔍	***	irresistible_irene	2011-09-15 15:32:40
9.	🔍	***	flowinstream	2011-09-15 15:34:08
10.	🔍	***	il_dianesy	2011-09-15 15:30:03
11.	🔍	***	nvillaceran	2011-09-15 15:33:45
12.	🔍	***	dafellah	2011-09-13 18:07:56
13.	🔍	***	dafellah	2011-09-10 18:12:06
14.	🔍	***	dafellah	2011-09-10 16:05:16
15.	🔍	***	shamba79	2011-09-14 13:01:15
16.	🔍	***	125.141.136.101	2011-09-14 13:21:06
17.	🔍	***	dafellah	2011-09-12 19:52:15
18.	🔍	***	-100000216888832	2011-09-12 17:32:08

1 2 3 Enter Page Go

Total 44 Total Page 3 Current Page 1

Client Search

Click on the following client search will provide you all the traffic content of that particular user IP – client.



Online IP List | Add/Delete | Set IP | Import/Export IP | Skipped IP List | Search | Account Detection | Mail Report

: 1 | Every Page : 20 Confirm

No.	Status	User IP	Client Search	Server Search	PC Name	Account	Last Connection Time
1.	○	192.168.1.12	🔍	🔍	***	frankie	2010-01-16 23:35:04
2.	○	192.168.1.1	🔍	🔍	***	192.168.1.1	2010-01-15 16:13:48

9 0 2 4 0 0 0 2 0 0 0 0 0 5 0 0 990 936 20 25 0 0 0

HTTP Content | Delete | Search

Every Page : 10 Confirm

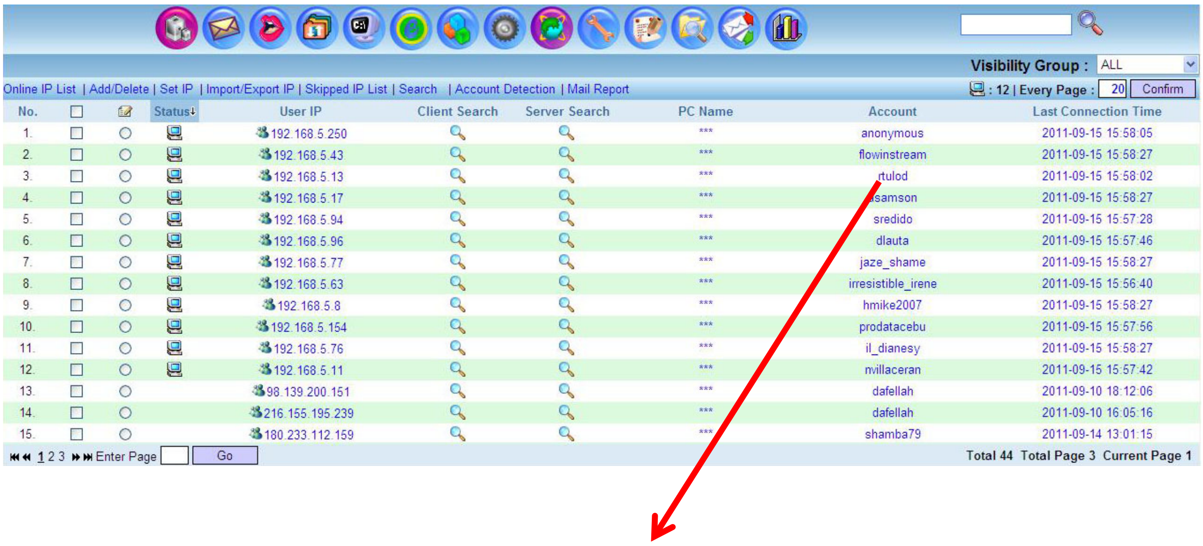
No.	□	Date-Time	Account	Content	WhoIs
231.	□	2010-01-16 14:14:56	frankie	singapore custom Woodlands checkpoint Camera - Google Search	🔍
232.	□	2010-01-16 14:14:24	frankie	ICA - Home - Immigration & Checkpoints Authority of Singapore	🔍
233.	□	2010-01-16 14:14:21	frankie	Arriving in Singapore	🔍
234.	□	2010-01-16 14:14:18	frankie	singapore custom checkpoint - Google Search	🔍
235.	□	2010-01-16 14:14:08	frankie	Google	🔍
236.	□	2010-01-16 14:06:45	frankie	COPEAC	🔍
237.	□	2010-01-16 14:06:43	frankie	affiliates.copeac.com	🔍
238.	□	2010-01-16 14:06:37	frankie	affiliates.copeac.com	🔍
239.	□	2010-01-16 14:06:34	frankie	affiliates.copeac.com	🔍
240.	□	2010-01-16 14:06:27	frankie	affiliates.copeac.com	🔍

20 21 22 23 24 25 26 27 28 Enter Page Go

Total 936 Total Page 94 Current Page 24

Online IP – Account Statistics

Account Statistics will show you the daily throughput statistics of that particular user account.



Visibility Group : ALL

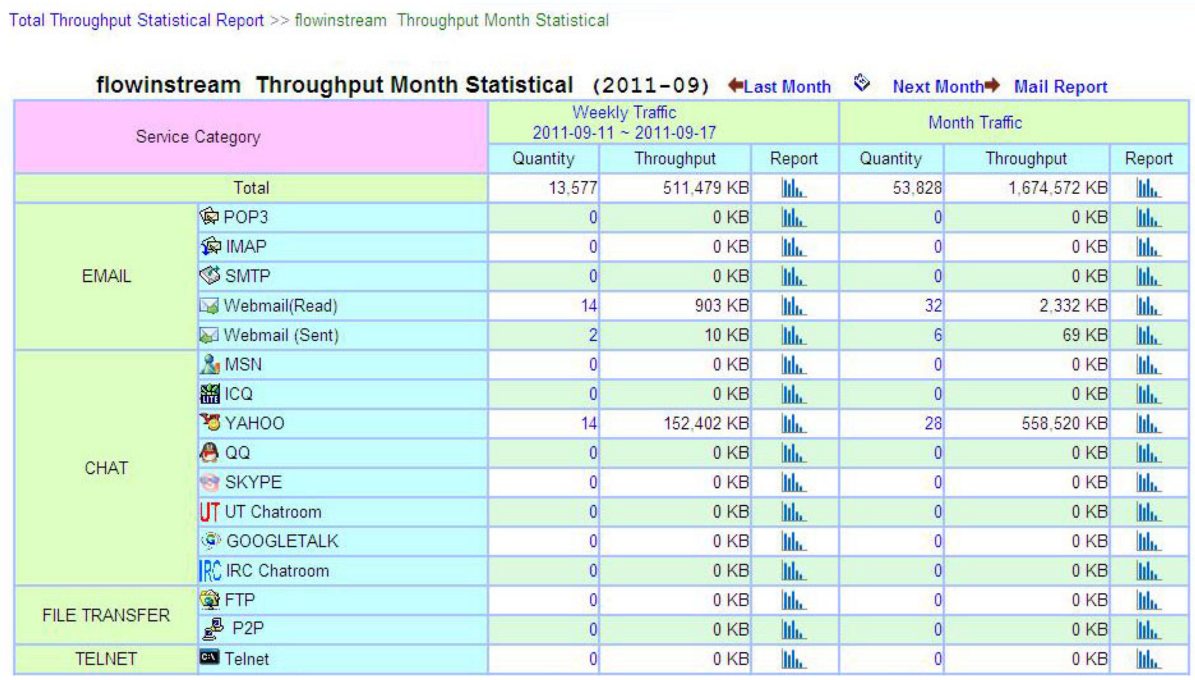
Online IP List | Add/Delete | Set IP | Import/Export IP | Skipped IP List | Search | Account Detection | Mail Report

: 12 | Every Page : 20 Confirm

No.	□		Status↓	User IP	Client Search	Server Search	PC Name	Account	Last Connection Time
1.	□	○		192.168.5.250			***	anonymous	2011-09-15 15:58:05
2.	□	○		192.168.5.43			***	flowinstream	2011-09-15 15:58:27
3.	□	○		192.168.5.13			***	rtulod	2011-09-15 15:58:02
4.	□	○		192.168.5.17			***	samson	2011-09-15 15:58:27
5.	□	○		192.168.5.94			***	sredido	2011-09-15 15:57:28
6.	□	○		192.168.5.96			***	dlauta	2011-09-15 15:57:46
7.	□	○		192.168.5.77			***	jaze_shame	2011-09-15 15:58:27
8.	□	○		192.168.5.63			***	irresistible_irene	2011-09-15 15:56:40
9.	□	○		192.168.5.8			***	hmike2007	2011-09-15 15:58:27
10.	□	○		192.168.5.154			***	prodatacebu	2011-09-15 15:57:56
11.	□	○		192.168.5.76			***	il_dianesy	2011-09-15 15:58:27
12.	□	○		192.168.5.11			***	nvillaceran	2011-09-15 15:57:42
13.	□	○		98.139.200.151			***	dafellah	2011-09-10 18:12:06
14.	□	○		216.155.195.239			***	dafellah	2011-09-10 16:05:16
15.	□	○		180.233.112.159			***	shamba79	2011-09-14 13:01:15

1 2 3 Enter Page Go

Total 44 Total Page 3 Current Page 1



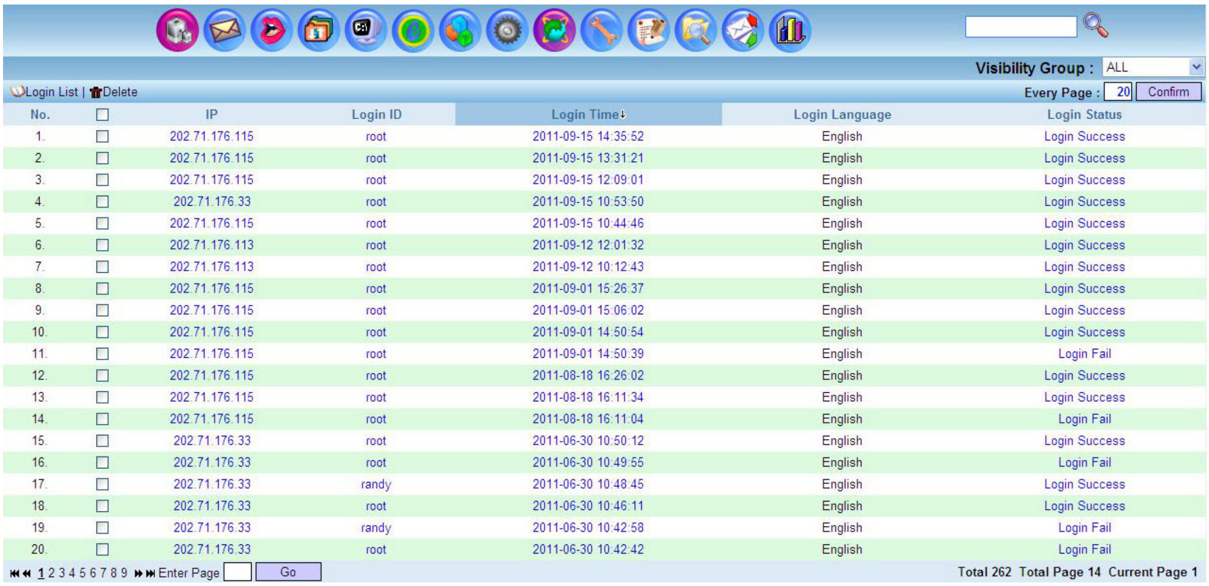
Total Throughput Statistical Report >> flowinstream Throughput Month Statistical

flowinstream Throughput Month Statistical (2011-09) Last Month Next Month Mail Report

Service Category		Weekly Traffic 2011-09-11 ~ 2011-09-17			Month Traffic		
		Quantity	Throughput	Report	Quantity	Throughput	Report
Total		13,577	511,479 KB	📊	53,828	1,674,572 KB	📊
EMAIL	POP3	0	0 KB	📊	0	0 KB	📊
	IMAP	0	0 KB	📊	0	0 KB	📊
	SMTP	0	0 KB	📊	0	0 KB	📊
	Webmail(Read)	14	903 KB	📊	32	2,332 KB	📊
	Webmail (Sent)	2	10 KB	📊	6	69 KB	📊
CHAT	MSN	0	0 KB	📊	0	0 KB	📊
	ICQ	0	0 KB	📊	0	0 KB	📊
	YAHOO	14	152,402 KB	📊	28	558,520 KB	📊
	QQ	0	0 KB	📊	0	0 KB	📊
	SKYPE	0	0 KB	📊	0	0 KB	📊
	UT Chatroom	0	0 KB	📊	0	0 KB	📊
	GOOGLETALK	0	0 KB	📊	0	0 KB	📊
	IRC Chatroom	0	0 KB	📊	0	0 KB	📊
FILE TRANSFER	FTP	0	0 KB	📊	0	0 KB	📊
	P2P	0	0 KB	📊	0	0 KB	📊
TELNET	Telnet	0	0 KB	📊	0	0 KB	📊

Login List

It shows all login attempts to the ICI system (whether it is a successfully login or a failed login). Information obtainable includes IP, Login ID, Login Date-Time and Login Language.



Visibility Group : ALL

Login List | Delete

Every Page : 20 Confirm

No.	□	IP	Login ID	Login Time↓	Login Language	Login Status
1.	□	202.71.176.115	root	2011-09-15 14:35:52	English	Login Success
2.	□	202.71.176.115	root	2011-09-15 13:31:21	English	Login Success
3.	□	202.71.176.115	root	2011-09-15 12:09:01	English	Login Success
4.	□	202.71.176.33	root	2011-09-15 10:53:50	English	Login Success
5.	□	202.71.176.115	root	2011-09-15 10:44:46	English	Login Success
6.	□	202.71.176.113	root	2011-09-12 12:01:32	English	Login Success
7.	□	202.71.176.113	root	2011-09-12 10:12:43	English	Login Success
8.	□	202.71.176.115	root	2011-09-01 15:26:37	English	Login Success
9.	□	202.71.176.115	root	2011-09-01 15:06:02	English	Login Success
10.	□	202.71.176.115	root	2011-09-01 14:50:54	English	Login Success
11.	□	202.71.176.115	root	2011-09-01 14:50:39	English	Login Fail
12.	□	202.71.176.115	root	2011-08-18 16:26:02	English	Login Success
13.	□	202.71.176.115	root	2011-08-18 16:11:34	English	Login Success
14.	□	202.71.176.115	root	2011-08-18 16:11:04	English	Login Fail
15.	□	202.71.176.33	root	2011-06-30 10:50:12	English	Login Success
16.	□	202.71.176.33	root	2011-06-30 10:49:55	English	Login Fail
17.	□	202.71.176.33	randy	2011-06-30 10:48:45	English	Login Success
18.	□	202.71.176.33	root	2011-06-30 10:46:11	English	Login Success
19.	□	202.71.176.33	randy	2011-06-30 10:42:58	English	Login Fail
20.	□	202.71.176.33	root	2011-06-30 10:42:42	English	Login Fail

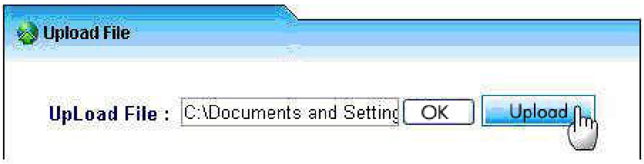
⏮ ⏪ 1 2 3 4 5 6 7 8 9 ⏩ ⏭ Enter Page ▭ Go

Total 262 Total Page 14 Current Page 1

Update

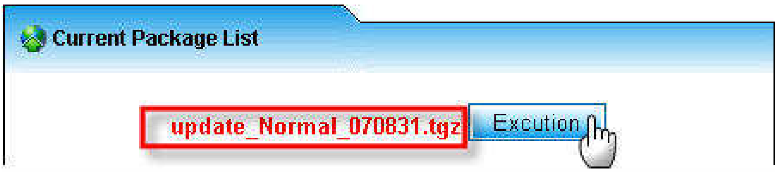
Update section allows the Administrator to upload update patch released to update and upgrade the system.

Step 1: Administrator browses for the update patch (file) and upload the file to the system.



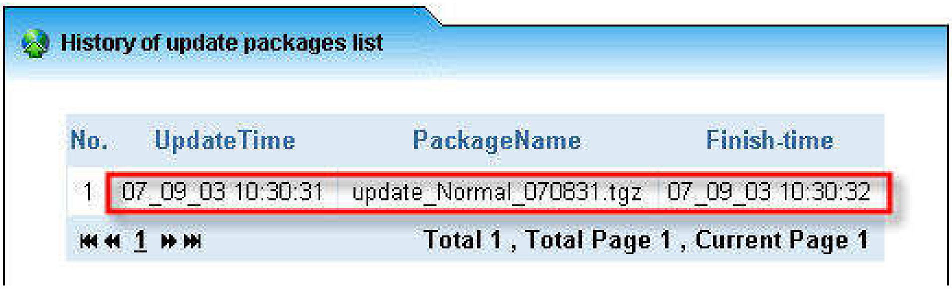
UpLoad File : C:\Documents and Setting

Step 2: If upload is successful, click on [Execution] to run the Update process.



update_Normal_070831.tgz

Step 3: Check on the Update Detail Files and History of update packages List for successful update of the system.

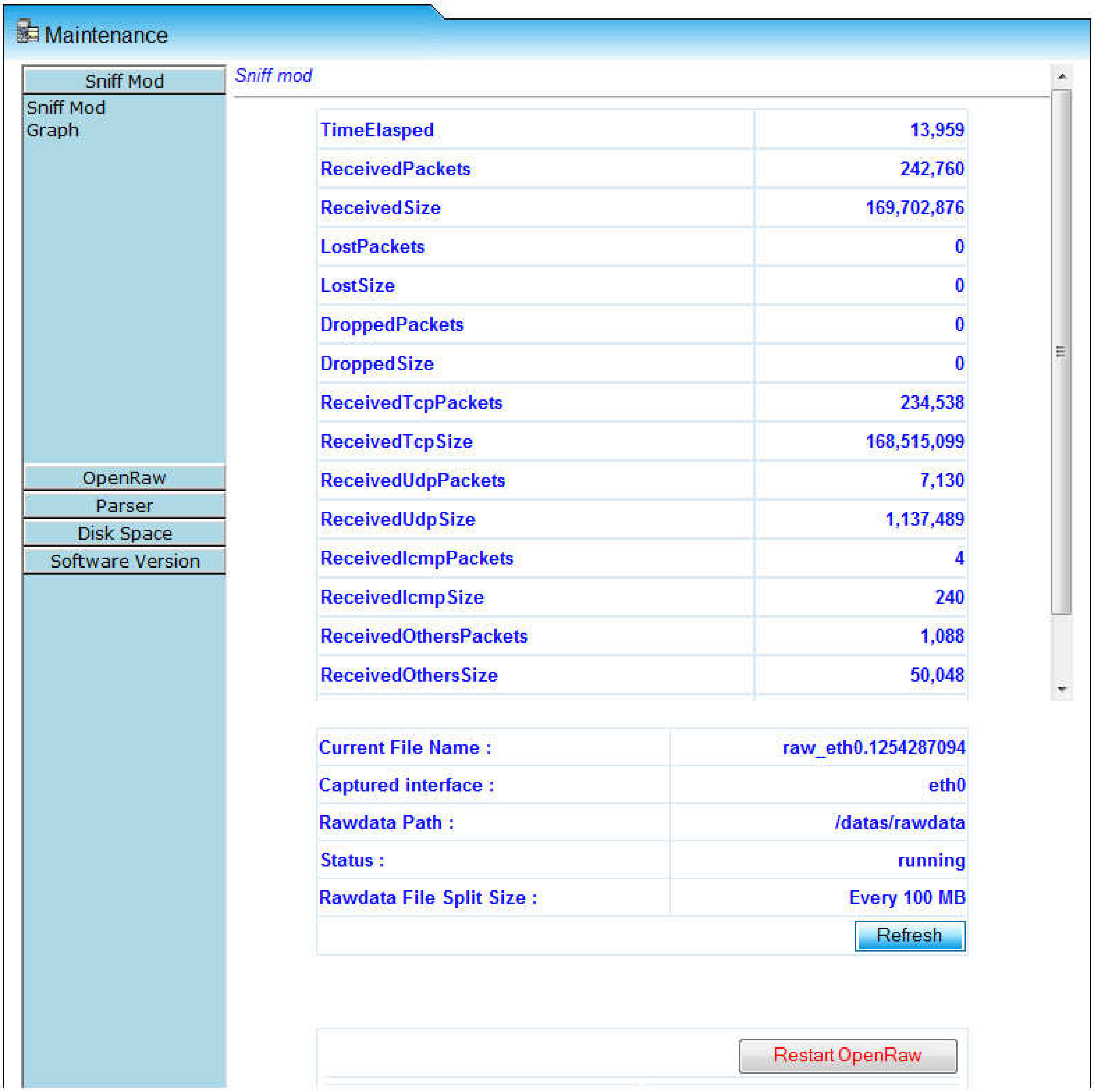


No.	UpdateTime	PackageName	Finish-time
1	07_09_03 10:30:31	update_Normal_070831.tgz	07_09_03 10:30:32

⏮ ⏪ 1 ⏩ ⏭ Total 1 , Total Page 1 , Current Page 1

Maintenance

This feature allows the Administrator to check on the system main processes status or health condition which includes Sniff Mod, OpenRaw, Parser, Disk Space and Software Version. You may refresh or restart the services if necessary.

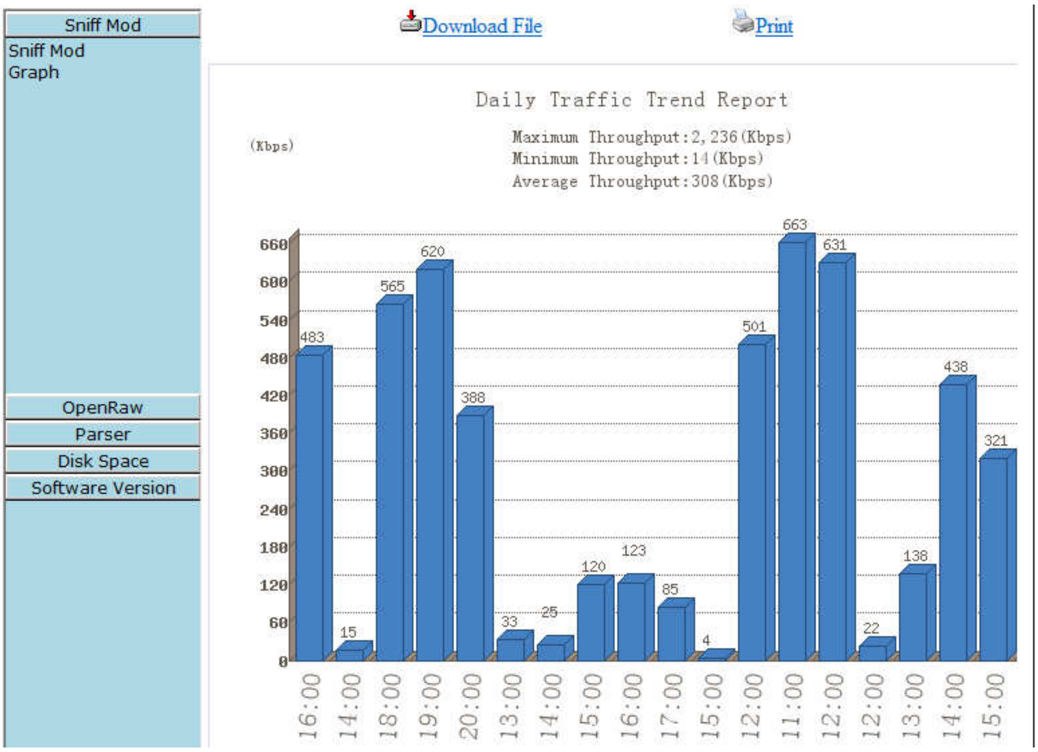


TimeElasped	13,959
ReceivedPackets	242,760
ReceivedSize	169,702,876
LostPackets	0
LostSize	0
DroppedPackets	0
DroppedSize	0
ReceivedTcpPackets	234,538
ReceivedTcpSize	168,515,099
ReceivedUdpPackets	7,130
ReceivedUdpSize	1,137,489
ReceivedIcmpPackets	4
ReceivedIcmpSize	240
ReceivedOthersPackets	1,088
ReceivedOthersSize	50,048

Current File Name :	raw_eth0.1254287094
Captured interface :	eth0
Rawdata Path :	/datas/rawdata
Status :	running
Rawdata File Split Size :	Every 100 MB

Sniff Mod: Packet capturing process. This process is responsible for collecting raw data from the Capturing Network Card Interface. Click on [Refresh] button to view the increment of raw data collected and to check whether raw data is being captured using mode of operation like Mirror Mode. You can also check on the network throughput by clicking on Graph.

Sniff Mode Graph showing the maximum throughput, minimum throughput and average throughput of the targeted network (point of interception).



Open Raw: Raw data packets service categorization process. This process is responsible to categorize raw data according to different services/applications/protocols.

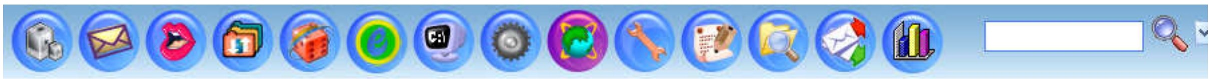
Parser: Raw data decoding and reconstruction process. This process is responsible to reconstruct the raw data which has been captured and categorized. Administrator may check on incremental of the session in the different parser processes. If the certain parser process/service does not show the result, you may press the [Restart] button to restart the process.

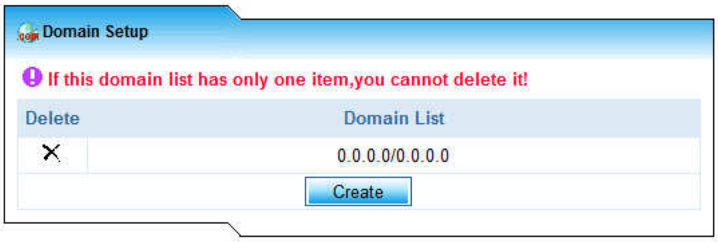
Disk Space: Displays the system drives and file system information (size, available space, used space etc.)

Software Version: Displays the version of different parser function/service.

Domain

This section allows the Administrator to set the domain or subnet. If domain is set, ICI will only capture and reconstruct Internet traffic from that particular domain set. By default, ICI captures and reconstructs Internet traffic from all domains.

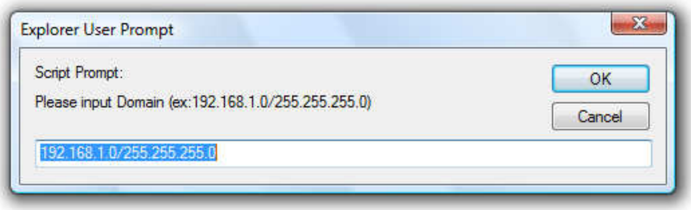




Domain Setup

If this domain list has only one item,you cannot delete it!

Delete	Domain List
✕	0.0.0.0/0.0.0.0



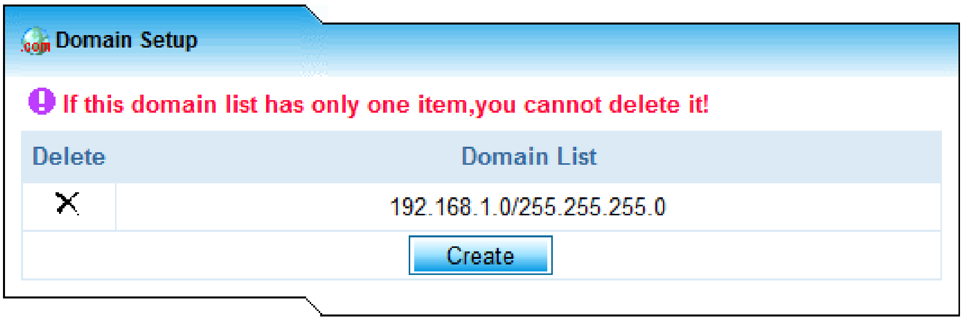
Explorer User Prompt

Script Prompt:

Please input Domain (ex:192.168.1.0/255.255.255.0)

192.168.1.0/255.255.255.0

Create a new domain by clicking on [Create] and the Domain Setting Windows will pop up. Input domain by ex: 192.168.1.0/255.255.255.0. Click [OK] to complete.



Domain Setup

If this domain list has only one item,you cannot delete it!

Delete	Domain List
✕	192.168.1.0/255.255.255.0

Implementation sample:

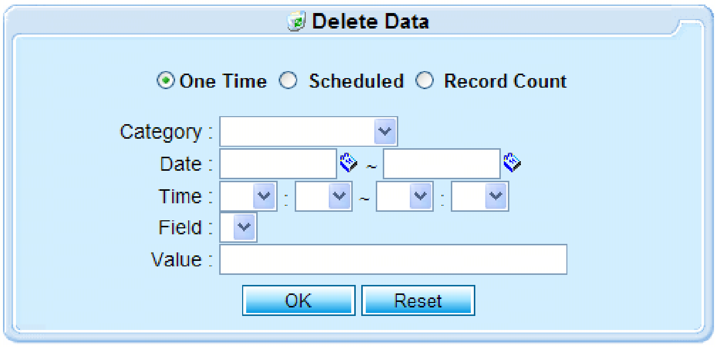
You may have a network with 1000 users with 5 subnets or domains. However, you may only want to include one domain users for monitoring. For instant, you only want to include 192.168.1.0/255.255.255.0 domain for monitoring.

System Tools

Delete Data

A. Delete Data by Category

One Time Delete
Administrator can delete data based on specific category or protocol such as Email, FTP, Chat, HTTP, Webmail, and Telnet in the category List.



Delete Data

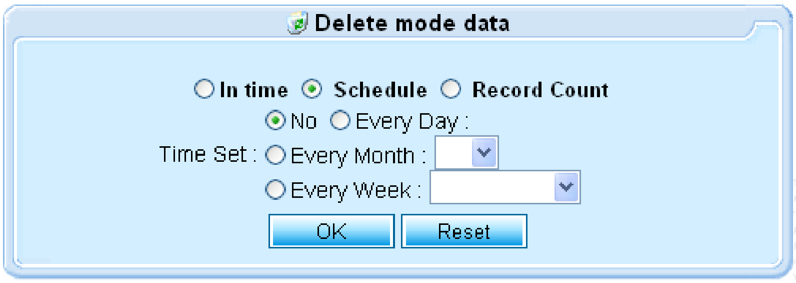
● One Time ○ Scheduled ○ Record Count

Category :
Date : ~
Time : : ~ :
Field :
Value :

Features in this GUI:

1) Mode: choose what data type you want to delete, e.g. POP3
2) Date & Time: Delete the data within the period specified
3) Field: Specify the record such as IP, sender, receiver
4) Value: The value of the item of record

Scheduled Delete
Administrator can delete all data records at specific scheduled time.



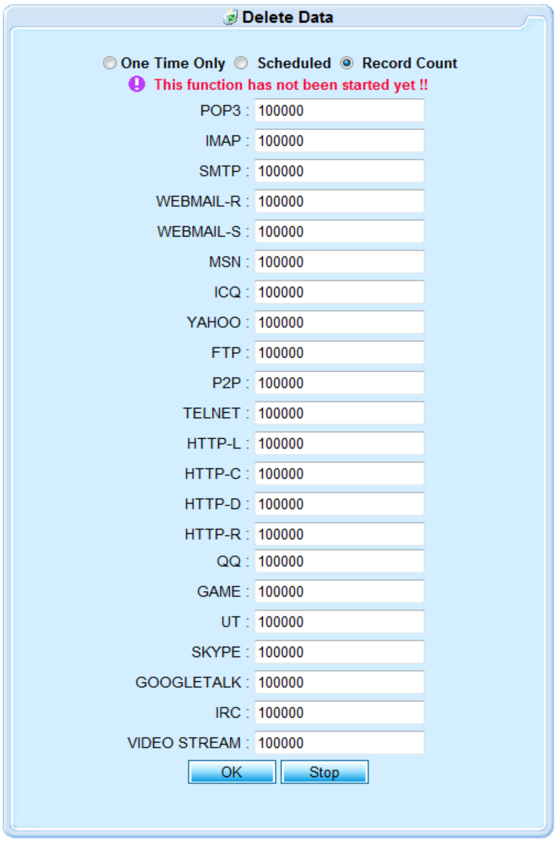
Delete mode data

○ In time ● Schedule ○ Record Count

Time Set : ● No ○ Every Day :
○ Every Month :
○ Every Week :

Record Count

Administrator can specify the threshold record for each service category. The Administrator can specify a number which the system can keep the record. Only the latest number of records is left if the actual number of record exceed the threshold specified (FIFO theory apply). For example: The threshold number for the data type POP3 is 50. The actual number of records for POP3 is 55. ED system will delete the first 5 oldest records in the POP3 and keep the latest 50 records.



○ One Time Only ○ Scheduled ● Record Count

This function has not been started yet !!

POP3 :	100000
IMAP :	100000
SMTP :	100000
WEBMAIL-R :	100000
WEBMAIL-S :	100000
MSN :	100000
ICQ :	100000
YAHOO :	100000
FTP :	100000
P2P :	100000
TELNET :	100000
HTTP-L :	100000
HTTP-C :	100000
HTTP-D :	100000
HTTP-R :	100000
QQ :	100000
GAME :	100000
UT :	100000
SKYPE :	100000
GOOGLETALK :	100000
IRC :	100000
VIDEO STREAM :	100000

B. Delete All Data

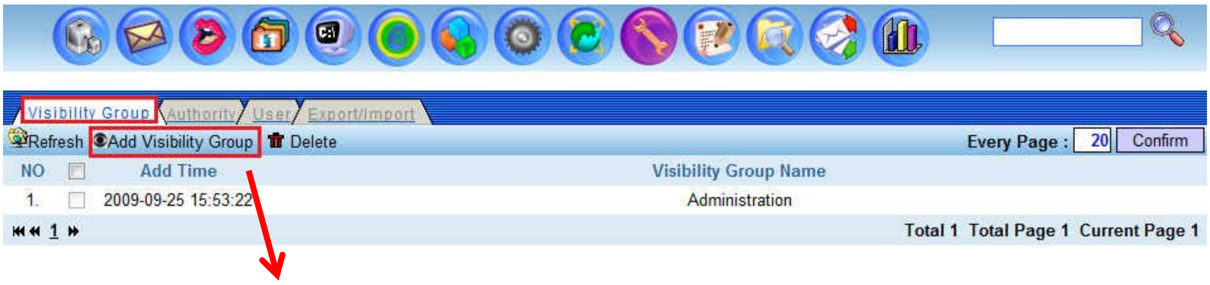
Administrator can select to delete all data with or without configuration through this Delete All Data section.

Authority

This section allows the Master System Administrator to assign different levels of authority for users to login to the ICI system for viewing or configuring the system.

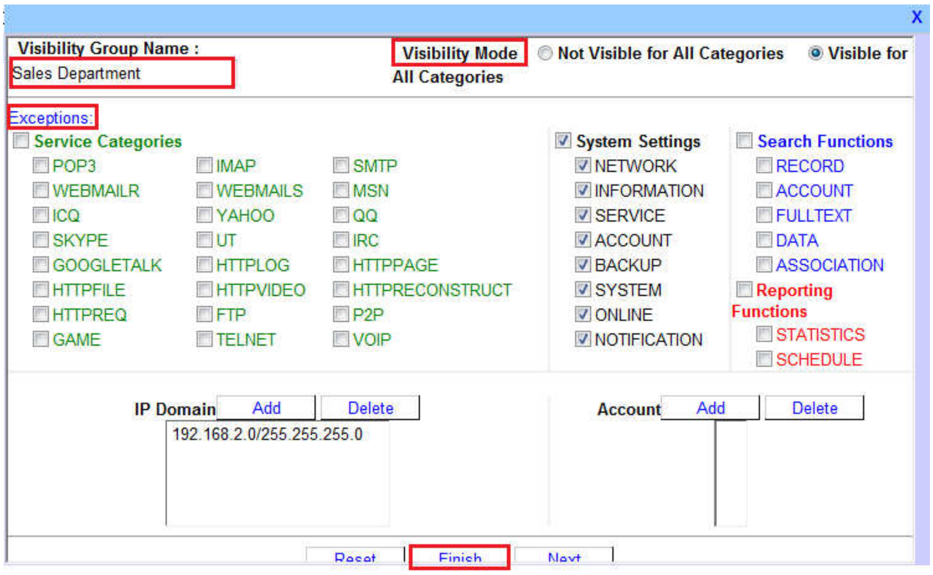
Visibility Group

This section allows the Administrator to setup Group of Users with different visibilities. For example, the Administrator can create a Group known as Sales Department Visible Group. Then, the Administrator can define what this Group can view (view all or view none or view with selected exceptions) as shown in diagram below. Please refer to screen shot below for setting up the Visibility Group. The Administrator can select Finish then complete this Visibility Group setting or click next to go to next Authority configuration.



NO	□	Add Time	Visibility Group Name
1.	□	2009-09-25 15:53:22	Administration

Total 1 Total Page 1 Current Page 1



Visibility Group Name : Sales Department

Visibility Mode ○ Not Visible for All Categories ● Visible for All Categories

Exceptions:

□ Service Categories

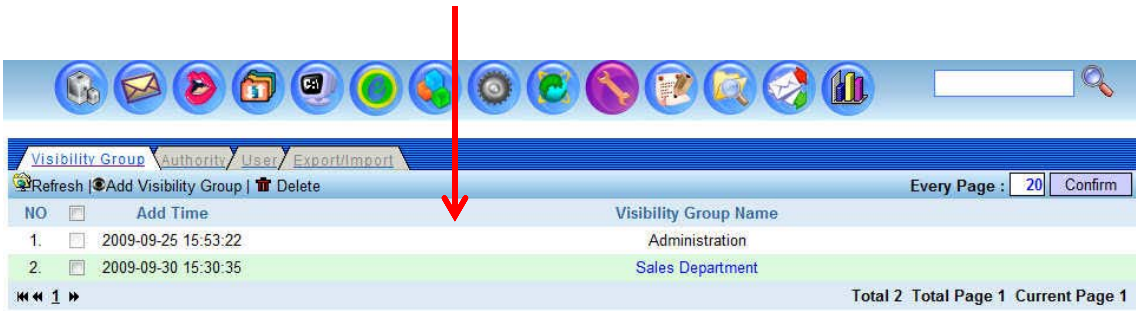
□ POP3	□ IMAP	□ SMTP
□ WEBMAILR	□ WEBMAILS	□ MSN
□ ICQ	□ YAHOO	□ QQ
□ SKYPE	□ UT	□ IRC
□ GOOGLETALK	□ HTTPLOG	□ HTTPPAGE
□ HTTPFILE	□ HTTPVIDEO	□ HTTPRECONSTRUCT
□ HTTPREQ	□ FTP	□ P2P
□ GAME	□ TELNET	□ VOIP

☑ System Settings
- ☑ NETWORK
- ☑ INFORMATION
- ☑ SERVICE
- ☑ ACCOUNT
- ☑ BACKUP
- ☑ SYSTEM
- ☑ ONLINE
- ☑ NOTIFICATION

□ Search Functions
- □ RECORD
- □ ACCOUNT
- □ FULLTEXT
- □ DATA
- □ ASSOCIATION

□ Reporting Functions
- □ STATISTICS
- □ SCHEDULE

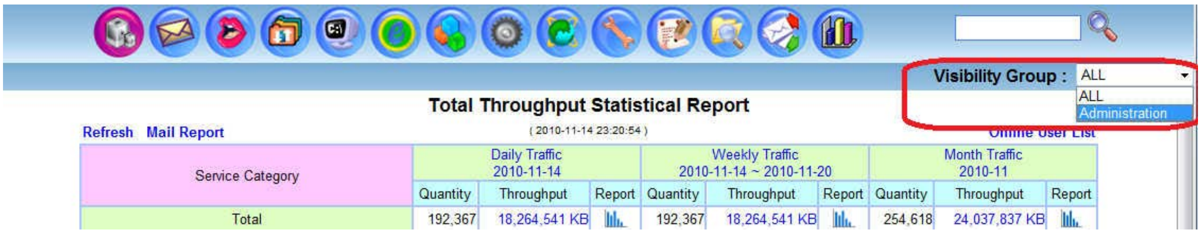
IP Domain: 192.168.2.0/255.255.255.0



NO	□	Add Time	Visibility Group Name
1.	□	2009-09-25 15:53:22	Administration
2.	□	2009-09-30 15:30:35	Sales Department

Total 2 Total Page 1 Current Page 1

Viewing by Visibility Group at ED Management GUI



Visibility Group : ALL

ALL
Administration

Total Throughput Statistical Report

Refresh Mail Report

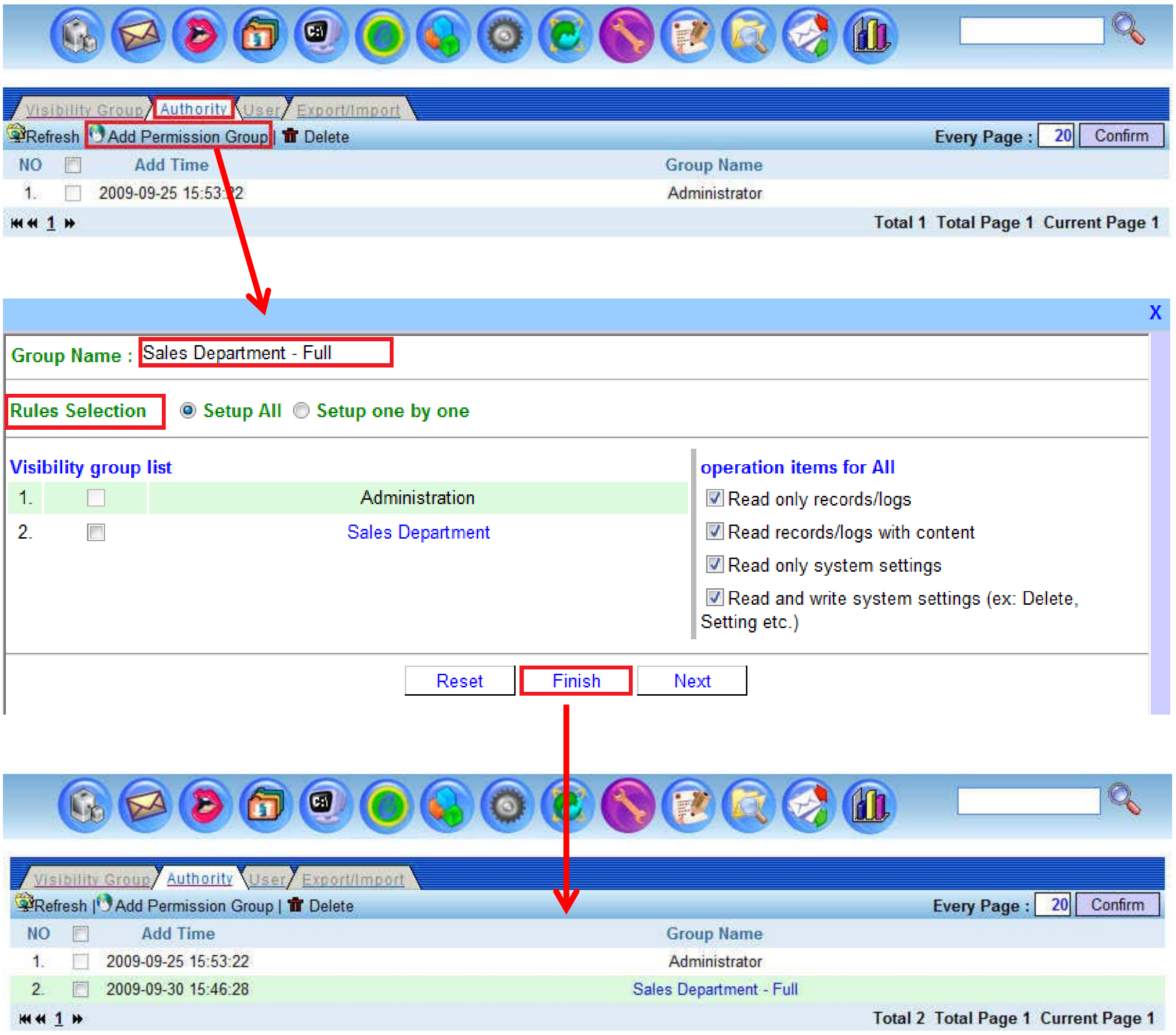
(2010-11-14 23:20:54)

Online User List

Service Category	Daily Traffic 2010-11-14			Weekly Traffic 2010-11-14 ~ 2010-11-20			Month Traffic 2010-11		
	Quantity	Throughput	Report	Quantity	Throughput	Report	Quantity	Throughput	Report
Total	192,367	18,264,541 KB		192,367	18,264,541 KB		254,618	24,037,837 KB	

Authority

This section allows the Administrator to setup the visibility group with different operating authorities (by setting up 4 different rules: read only recorded record, read recorded content, read and set the content, read and write capabilities). Please refer to screen shot below for setting up this Authority.



NO	□	Add Time	Group Name
1.	□	2009-09-25 15:53:22	Administrator

Total 1 Total Page 1 Current Page 1

Group Name : Sales Department - Full

Rules Selection ● Setup All ○ Setup one by one

Visibility group list

1.	□	Administration
2.	□	Sales Department

operation items for All

☑ Read only records/logs

☑ Read records/logs with content

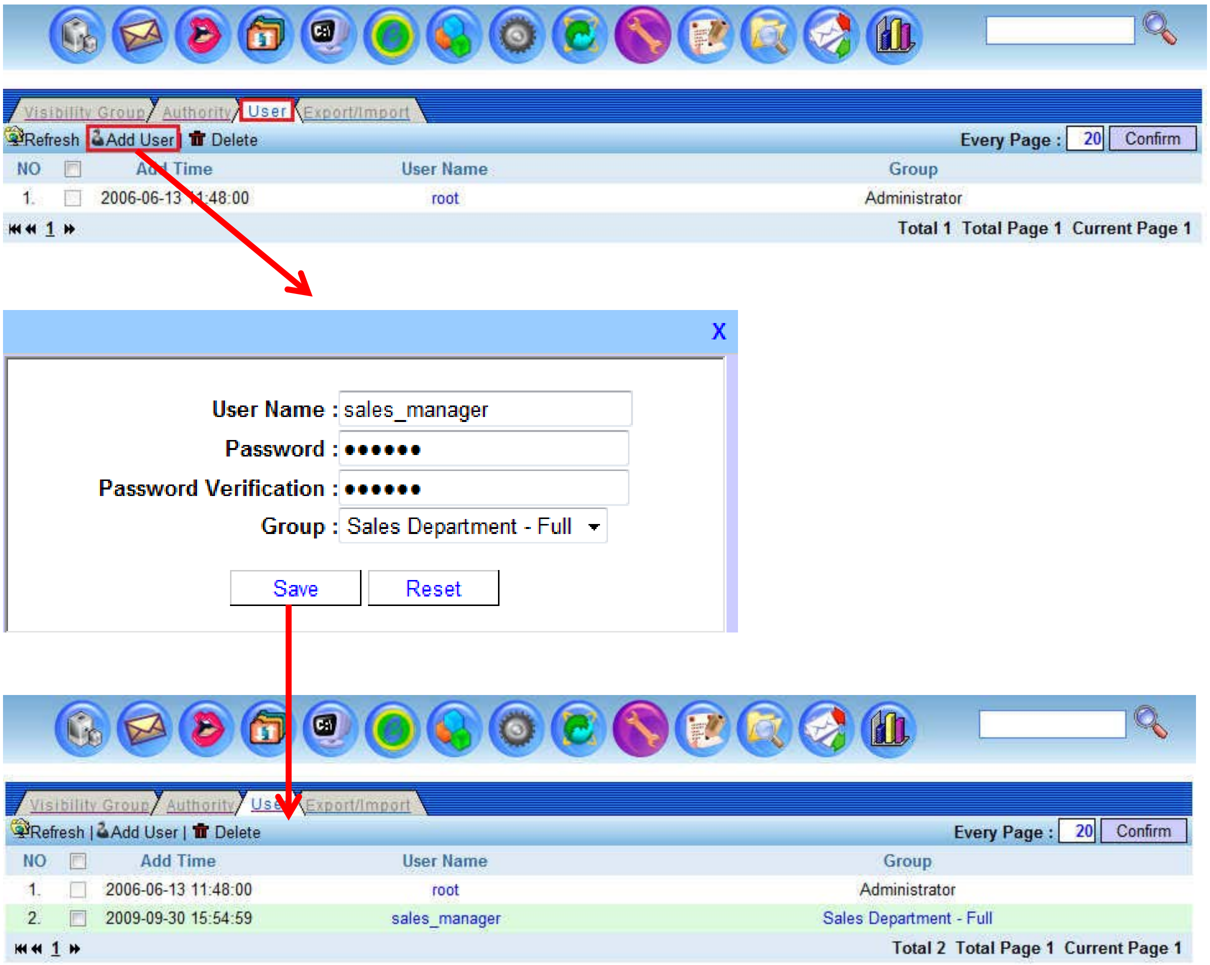
☑ Read only system settings

☑ Read and write system settings (ex: Delete, Setting etc.)

NO	□	Add Time	Group Name
1.	□	2009-09-25 15:53:22	Administrator
2.	□	2009-09-30 15:46:28	Sales Department - Full

Total 2 Total Page 1 Current Page 1

User
This section allows the Administrator to create the users. It also allows the Administrator to assign the Group to the specific user created. Please refer to screen shot below for the setup of the User Group.



NO	☐	Add Time	User Name	Group
1.	☐	2006-06-13 11:48:00	root	Administrator

Total 1 Total Page 1 Current Page 1

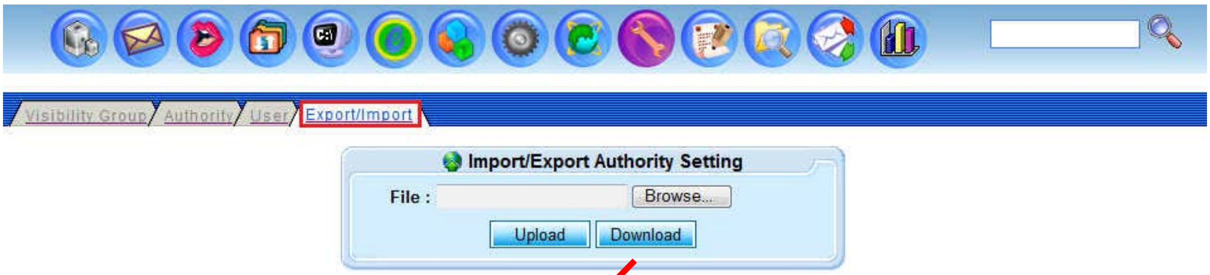
User Name : sales_manager
Password : ●●●●●●
Password Verification : ●●●●●●
Group : Sales Department - Full

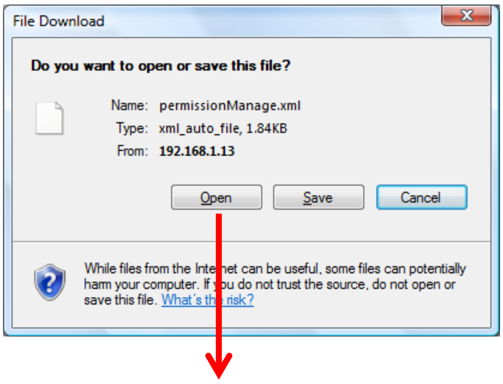
NO	☐	Add Time	User Name	Group
1.	☐	2006-06-13 11:48:00	root	Administrator
2.	☐	2009-09-30 15:54:59	sales_manager	Sales Department - Full

Total 2 Total Page 1 Current Page 1

Import/Export

This section allows the Administrator to import or export the users with pre-defined setup. The template (XML format) can be downloaded for editing.





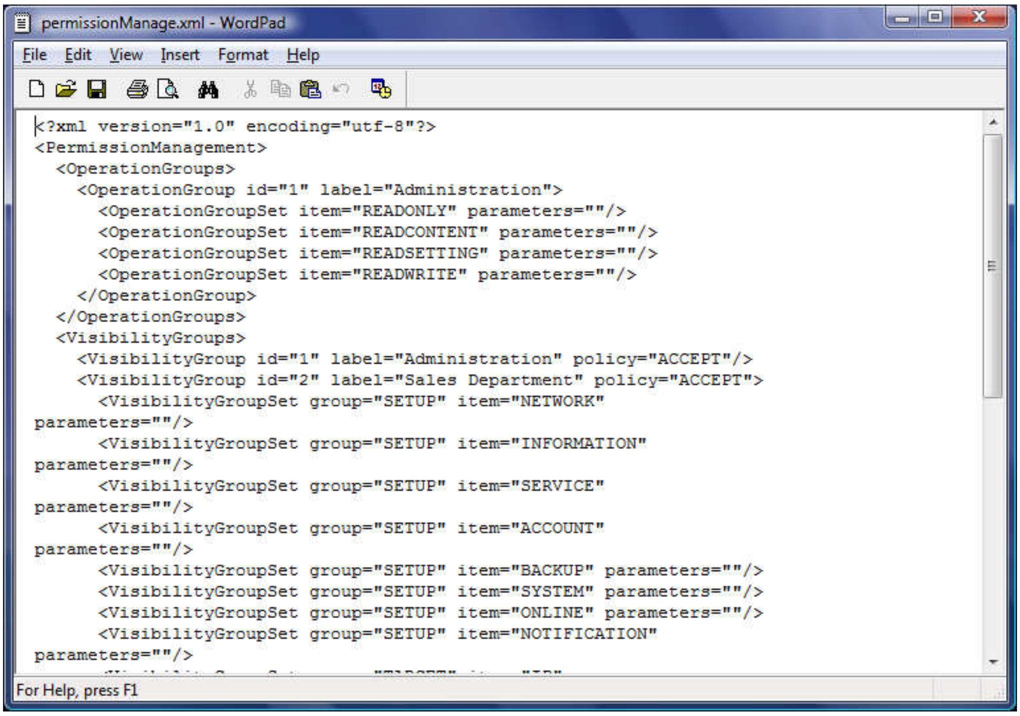
Do you want to open or save this file?

Name: permissionManage.xml

Type: xml_auto_file, 1.84KB

From: 192.168.1.13

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

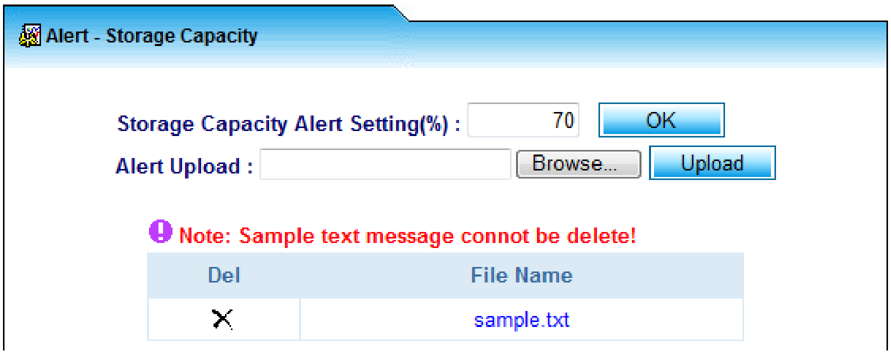


```
<?xml version="1.0" encoding="utf-8"?>
<PermissionManagement>
  <OperationGroups>
    <OperationGroup id="1" label="Administration">
      <OperationGroupSet item="READONLY" parameters=""/>
      <OperationGroupSet item="READCONTENT" parameters=""/>
      <OperationGroupSet item="READSETTING" parameters=""/>
      <OperationGroupSet item="READWRITE" parameters=""/>
    </OperationGroup>
  </OperationGroups>
  <VisibilityGroups>
    <VisibilityGroup id="1" label="Administration" policy="ACCEPT"/>
    <VisibilityGroup id="2" label="Sales Department" policy="ACCEPT">
      <VisibilityGroupSet group="SETUP" item="NETWORK"
parameters=""/>
      <VisibilityGroupSet group="SETUP" item="INFORMATION"
parameters=""/>
      <VisibilityGroupSet group="SETUP" item="SERVICE"
parameters=""/>
      <VisibilityGroupSet group="SETUP" item="ACCOUNT"
parameters=""/>
      <VisibilityGroupSet group="SETUP" item="BACKUP" parameters=""/>
      <VisibilityGroupSet group="SETUP" item="SYSTEM" parameters=""/>
      <VisibilityGroupSet group="SETUP" item="ONLINE" parameters=""/>
      <VisibilityGroupSet group="SETUP" item="NOTIFICATION"
parameters=""/>
```

Storage Alert

Storage Alert consists of the follow: Alert – Storage Capacity, Alert – Notification Parameters and Alert – Daily System Status Report.

Storage Capacity



Alert - Storage Capacity

Storage Capacity Alert Setting(%) : 70

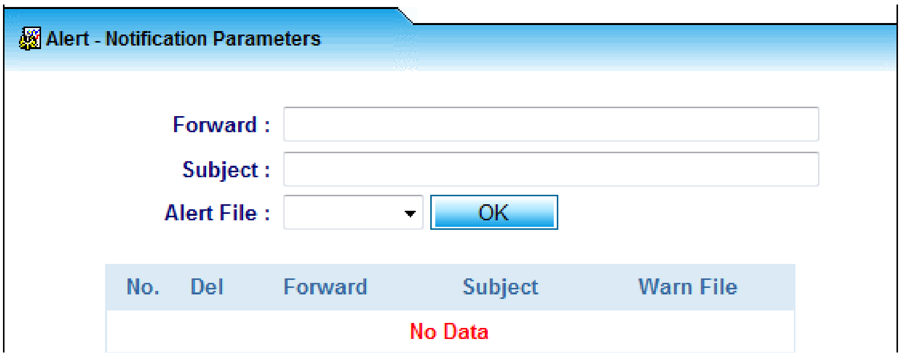
Alert Upload :

Note: Sample text message connot be delete!

Del	File Name
✕	sample.txt

Administrator can define the storage capacity alert. When the system storage has approach certain %, the system can send alert Email to the Administrator. Administrator can upload the sample alert Email to the system.

Notification Parameters



Alert - Notification Parameters

Forward :

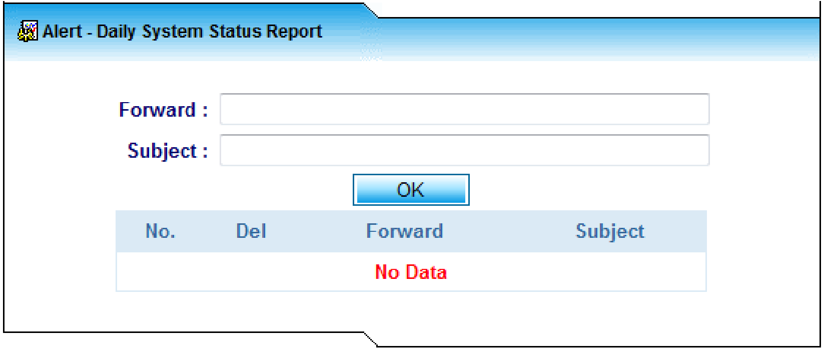
Subject :

Alert File :

No.	Del	Forward	Subject	Warn File
No Data				

Administrator can specify the Email account that the alert message can be send to in Forward field. Besides, Administrator can define the subject and the alert file.

Daily System Status Report



Alert - Daily System Status Report

Forward :

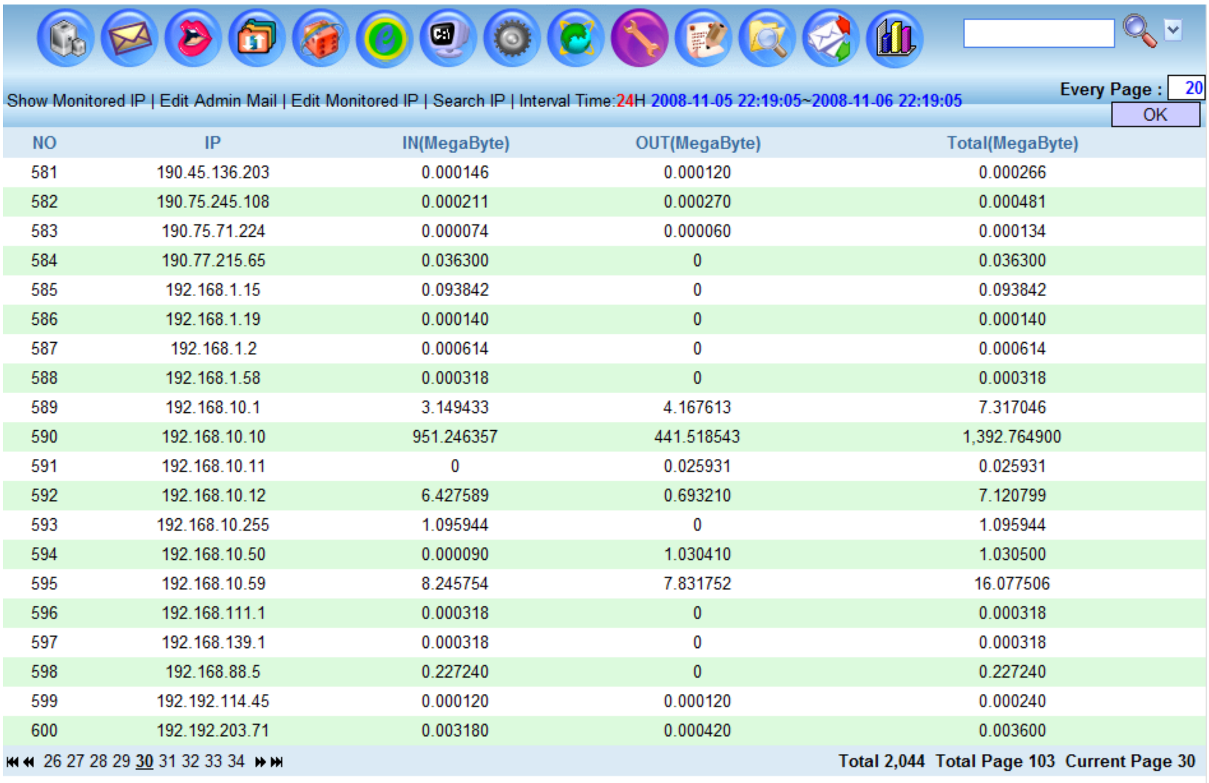
Subject :

No.	Del	Forward	Subject
No Data			

Administrator can also setup the system to automatically send a system storage status to the Administrator Email daily.

Throughput Alert

Throughput Alert function allows Alert Email to be sent to the Administrator when the pre-defined IP has consumed and reached the throughput threshold defined.



Show Monitored IP | Edit Admin Mail | Edit Monitored IP | Search IP | Interval Time:24H 2008-11-05 22:19:05~2008-11-06 22:19:05

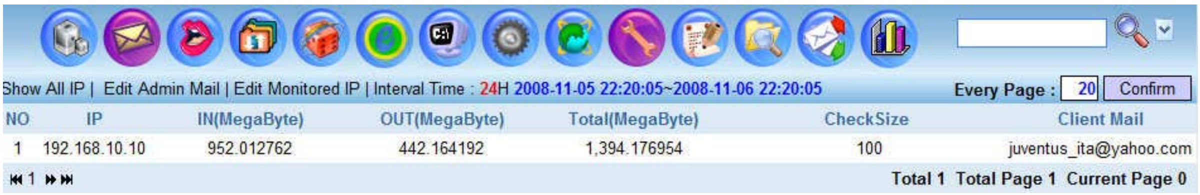
Every Page : 20 OK

NO	IP	IN(MegaByte)	OUT(MegaByte)	Total(MegaByte)
581	190.45.136.203	0.000146	0.000120	0.000266
582	190.75.245.108	0.000211	0.000270	0.000481
583	190.75.71.224	0.000074	0.000060	0.000134
584	190.77.215.65	0.036300	0	0.036300
585	192.168.1.15	0.093842	0	0.093842
586	192.168.1.19	0.000140	0	0.000140
587	192.168.1.2	0.000614	0	0.000614
588	192.168.1.58	0.000318	0	0.000318
589	192.168.10.1	3.149433	4.167613	7.317046
590	192.168.10.10	951.246357	441.518543	1,392.764900
591	192.168.10.11	0	0.025931	0.025931
592	192.168.10.12	6.427589	0.693210	7.120799
593	192.168.10.255	1.095944	0	1.095944
594	192.168.10.50	0.000090	1.030410	1.030500
595	192.168.10.59	8.245754	7.831752	16.077506
596	192.168.111.1	0.000318	0	0.000318
597	192.168.139.1	0.000318	0	0.000318
598	192.168.88.5	0.227240	0	0.227240
599	192.192.114.45	0.000120	0.000120	0.000240
600	192.192.203.71	0.003180	0.000420	0.003600

⏮ ◀ 26 27 28 29 30 31 32 33 34 ▶ ⏭ Total 2,044 Total Page 103 Current Page 30

Show Monitored IP

Click on the [Show Monitored IP] link and targets which are being monitored will be displayed. The information for each target is shown as the following diagram.



Show All IP | Edit Admin Mail | Edit Monitored IP | Interval Time : 24H 2008-11-05 22:20:05~2008-11-06 22:20:05

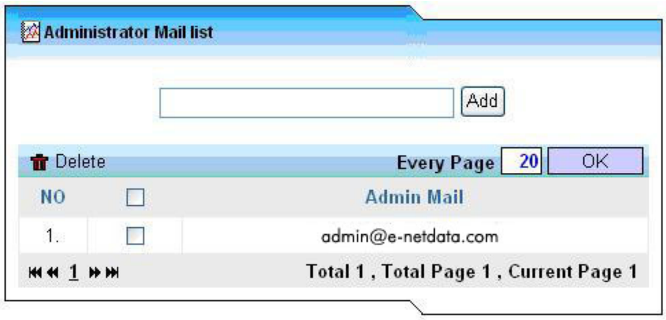
Every Page : 20 Confirm

NO	IP	IN(MegaByte)	OUT(MegaByte)	Total(MegaByte)	CheckSize	Client Mail
1	192.168.10.10	952.012762	442.164192	1,394.176954	100	juventus_ita@yahoo.com

⏮ 1 ▶ ⏭ Total 1 Total Page 1 Current Page 0

Edit Admin Mail

The following window will pop up if the link [Edit Admin Mail] is clicked. Administrator can add the admin Email account here. The alert/warning message will be sent to these Email accounts specified if there is any monitored target exceeds the bandwidth quota.

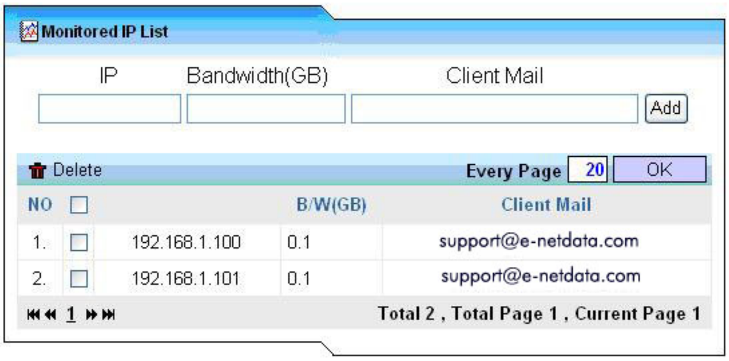


NO	□	Admin Mail
1.	□	admin@e-netdata.com

⏮ ⏪ 1 ⏩ ⏭ Total 1 , Total Page 1 , Current Page 1

Edit Monitored IP

Admin can edit the monitored IP/PC parameters such as Bandwidth (GB), Client Mail etc.

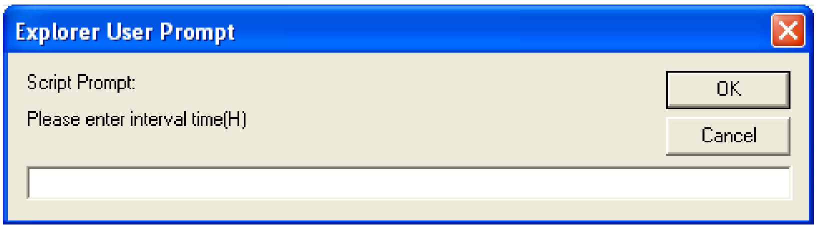


NO	□		B/W(GB)	Client Mail
1.	□	192.168.1.100	0.1	support@e-netdata.com
2.	□	192.168.1.101	0.1	support@e-netdata.com

⏮ ⏪ 1 ⏩ ⏭ Total 2 , Total Page 1 , Current Page 1

Interval Time (H)

The interval time specify the duration that the target IP/PC is to be monitored for the throughput usage. For example: The interval time is 5 hours. ICI system time is currently at 12:00 on 12/Dec/2007. ICI system will then count the total size of information occurred between 12:00 of 12/Dec/2007 and 17:00 of 12/Dec/2007 for each target (monitored IP).



Script Prompt:

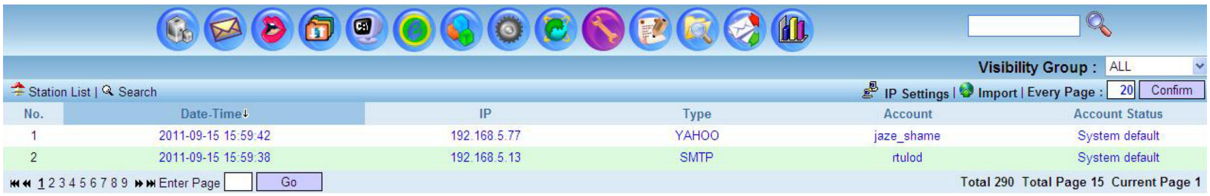
Please enter interval time(H)

AD Import

This section provides the targeted PC or station information. It includes station List, NetBIOS PC List and AD List.

A.Station List

The section List out the Date-Time, IP Addresses, Traffic Type and Account detected.



Visibility Group : ALL

Station List | Search

IP Settings | Import | Every Page : 20 Confirm

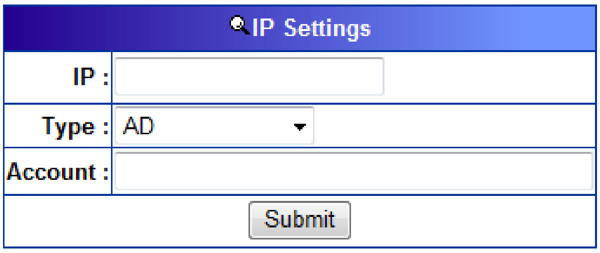
No.	Date-Time↓	IP	Type	Account	Account Status
1	2011-09-15 15:59:42	192.168.5.77	YAHOO	jaze_shame	System default
2	2011-09-15 15:59:38	192.168.5.13	SMTP	rtulod	System default

⏮⏪ 1 2 3 4 5 6 7 8 9 ⏩⏭ Enter Page Go

Total 290 Total Page 15 Current Page 1

It also includes function that allows the Administrator to manually import IP Address, Type and Account List into the system and allows retrieval or accessing of reconstructed data based on the List. Administrator can use Excel/csv file which contains the input of user account and MAC to upload to the system.

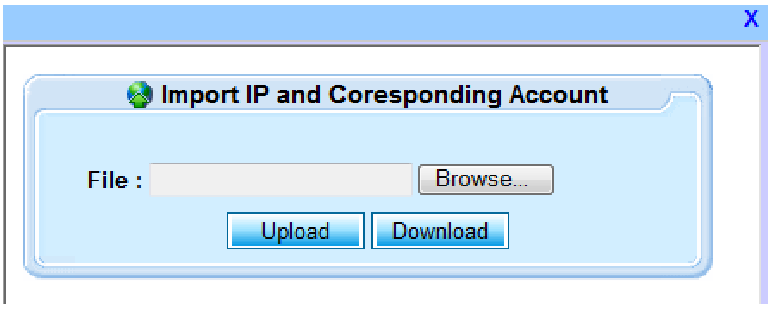
By clicking on the [IP Settings] Administrator can edit the IP Setting by manually input IP and match with Type of Services and Account Name.



IP Settings

IP :	
Type :	AD
Account :	

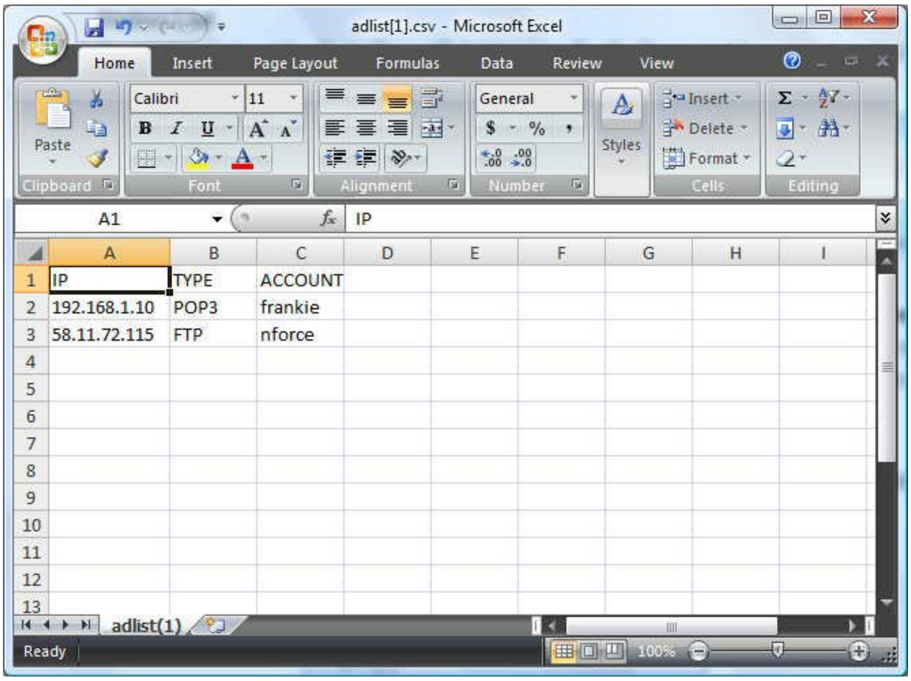
By clicking on [Import] icon, the following window will appear and user can upload the Excel/csv file containing the pre-defined IP-Type-Account to the system.



Import IP and Coresponding Account

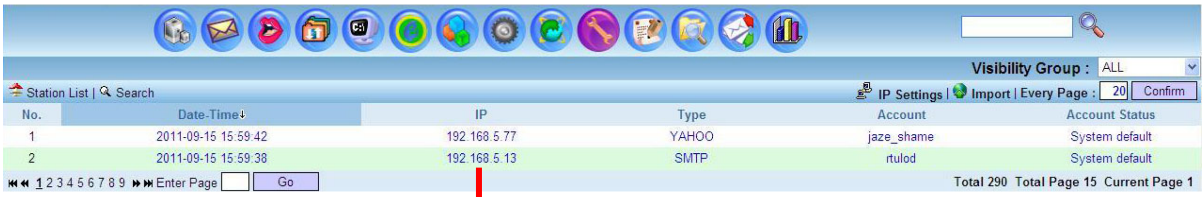
File :

Excel/csv file that can the Administrator can pre-defined the IP Address, Type and Account.



	A	B	C
1	IP	TYPE	ACCOUNT
2	192.168.1.10	POP3	frankie
3	58.11.72.115	FTP	nforce

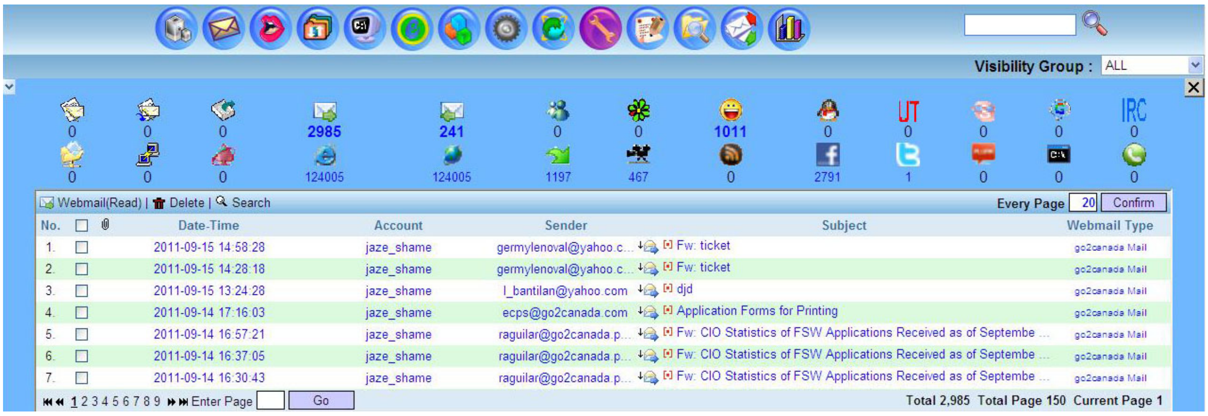
Search by IP Address or Account
The Administrator can click on the IP Address or Account to find the data related to that particular IP Address or Account.


Visibility Group : ALL
Station List | Search
IP Settings | Import | Every Page : 20 Confirm

No.	Date-Time↓	IP	Type	Account	Account Status
1	2011-09-15 15:59:42	192.168.5.77	YAHOO	jaze_shame	System default
2	2011-09-15 15:59:38	192.168.5.13	SMTP	rtulod	System default

⏮ ⏪ 1 2 3 4 5 6 7 8 9 ⏩ ⏭ Enter Page Go

Total 290 Total Page 15 Current Page 1



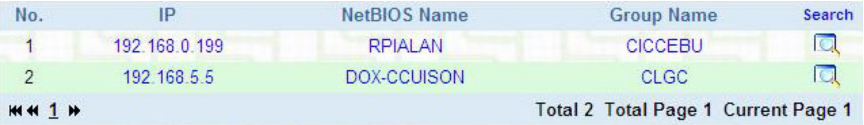
0	0	0	2985	241	0	0	1011	0	0	0	0	0
0	0	0	124005	124005	1197	467	0	2791	1	0	0	0

No.	□		Date-Time	Account	Sender	Subject	Webmail Type
1.	□		2011-09-15 14:58:28	jaze_shame	germylenoval@yahoo.c...	Fw: ticket	go2canada Mail
2.	□		2011-09-15 14:28:18	jaze_shame	germylenoval@yahoo.c...	Fw: ticket	go2canada Mail
3.	□		2011-09-15 13:24:28	jaze_shame	l_bantilan@yahoo.com	djd	go2canada Mail
4.	□		2011-09-14 17:16:03	jaze_shame	ecps@go2canada.com	Application Forms for Printing	go2canada Mail
5.	□		2011-09-14 16:57:21	jaze_shame	raguilar@go2canada.p...	Fw: CIO Statistics of FSW Applications Received as of Septembe ...	go2canada Mail
6.	□		2011-09-14 16:37:05	jaze_shame	raguilar@go2canada.p...	Fw: CIO Statistics of FSW Applications Received as of Septembe ...	go2canada Mail
7.	□		2011-09-14 16:30:43	jaze_shame	raguilar@go2canada.p...	Fw: CIO Statistics of FSW Applications Received as of Septembe ...	go2canada Mail

Total 2,985 Total Page 150 Current Page 1

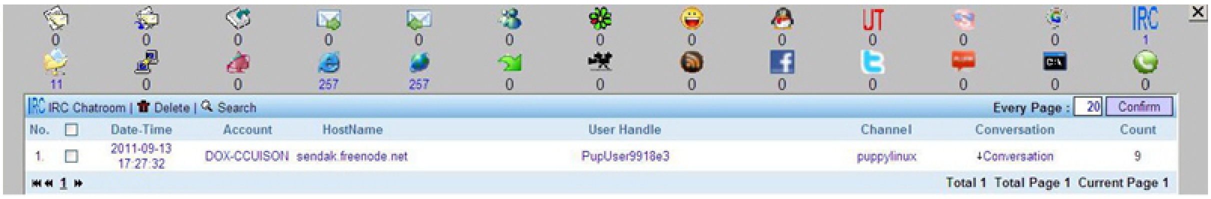
B. NetBIOS PC List

NetBIOS (Network Basic Input/Output System) normally runs over TCP/IP, gives each computer or PC in the network both a NetBIOS name and an IP address corresponding to a (possibly different) host name. ICI system can display the NetBIOS PC List on the network and Administrator can search the related reconstructed data based on this List as shown in diagram below.



No.	IP	NetBIOS Name	Group Name	Search
1	192.168.0.199	RPIALAN	CICCEBU	🔍
2	192.168.5.5	DOX-CCUISON	CLGC	🔍

⏮ ⏪ 1 ⏩ Total 2 Total Page 1 Current Page 1



IRC IRC Chatroom | Delete | Search Every Page : 20 Confirm

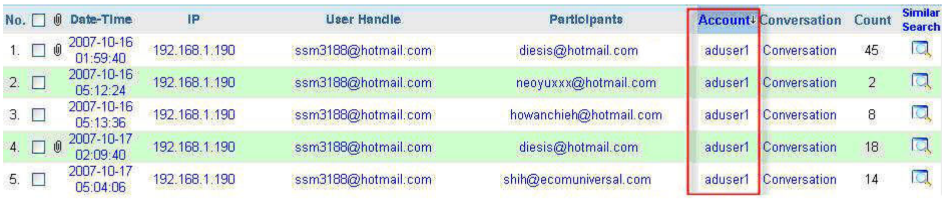
No.	□	Date-Time	Account	HostName	User Handle	Channel	Conversation	Count
1.	□	2011-09-13 17:27:32	DOX-CCUISON	sendak.freenode.net	PupUser9918e3	puppylinux	↓Conversation	9

⏮ ⏪ 1 ⏩ Total 1 Total Page 1 Current Page 1

C. Active Directory Account List

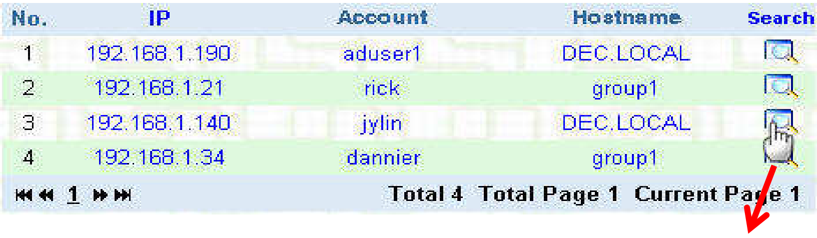
When there is Active Directory (AD) server running on the network, Administrator can start the AD Server service at SETTING – SERVICES. Therefore, the system will auto retrieve and show the IP and AD Account for all categories of data reconstructed as shown diagram below. Administrator can also search the related information from particular AD account.

Besides this automatic AD account retrieval function (which might not work in some network environment due to network implementation architecture), we also provide an AD Probe tool which allows AD server to manually send this AD account information to ICI system.



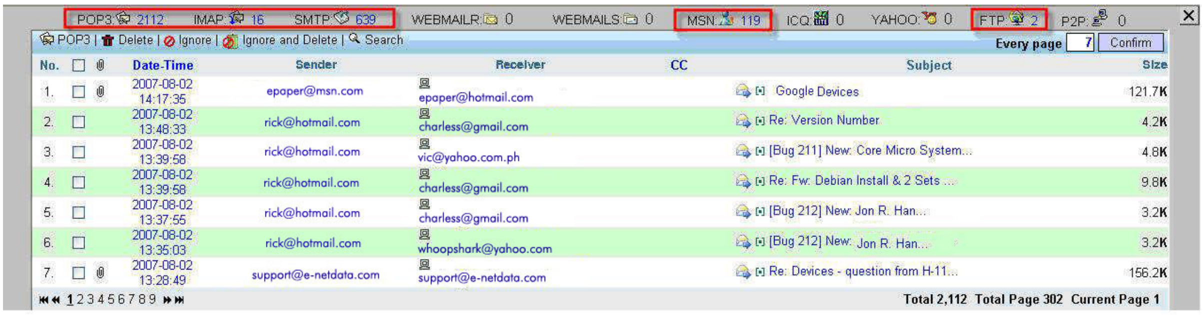
No.	□	📎	Date-Time	IP	User Handle	Participants	Account↓	Conversation	Count	Similar Search
1.	□	📎	2007-10-16 01:59:40	192.168.1.190	ssm3188@hotmail.com	diesis@hotmail.com	aduser1	Conversation	45	🔍
2.	□		2007-10-16 05:12:24	192.168.1.190	ssm3188@hotmail.com	neoyuxxx@hotmail.com	aduser1	Conversation	2	🔍
3.	□		2007-10-16 05:13:36	192.168.1.190	ssm3188@hotmail.com	howanchieh@hotmail.com	aduser1	Conversation	8	🔍
4.	□	📎	2007-10-17 02:09:40	192.168.1.190	ssm3188@hotmail.com	diesis@hotmail.com	aduser1	Conversation	18	🔍
5.	□		2007-10-17 05:04:06	192.168.1.190	ssm3188@hotmail.com	shih@ecomuniversal.com	aduser1	Conversation	14	🔍

Similar Search for Particular AD Account



No.	IP	Account	Hostname	Search
1	192.168.1.190	aduser1	DEC.LOCAL	🔍
2	192.168.1.21	rick	group1	🔍
3	192.168.1.140	jylin	DEC.LOCAL	🔍
4	192.168.1.34	dannier	group1	🔍

⏮ ⏪ 1 ⏩ ⏭ Total 4 Total Page 1 Current Page 1



POP3 | Delete | Ignore | Ignore and Delete | Search Every page 7 Confirm

No.	□	📎	Date-Time	Sender	Receiver	CC	Subject	Size
1.	□	📎	2007-08-02 14:17:35	epaper@msn.com	epaper@hotmail.com		Google Devices	121.7K
2.	□		2007-08-02 13:48:33	rick@hotmail.com	charless@gmail.com		Re: Version Number	4.2K
3.	□		2007-08-02 13:39:58	rick@hotmail.com	vic@yahoo.com.ph		[Bug 211] New: Core Micro System...	4.8K
4.	□		2007-08-02 13:39:58	rick@hotmail.com	charless@gmail.com		Re: Fw: Debian Install & 2 Sets ...	9.8K
5.	□		2007-08-02 13:37:55	rick@hotmail.com	charless@gmail.com		[Bug 212] New: Jon R. Han...	3.2K
6.	□		2007-08-02 13:35:03	rick@hotmail.com	whoopshark@yahoo.com		[Bug 212] New: Jon R. Han...	3.2K
7.	□	📎	2007-08-02 13:28:49	support@e-netdata.com	support@e-netdata.com		Re: Devices - question from H-11...	156.2K

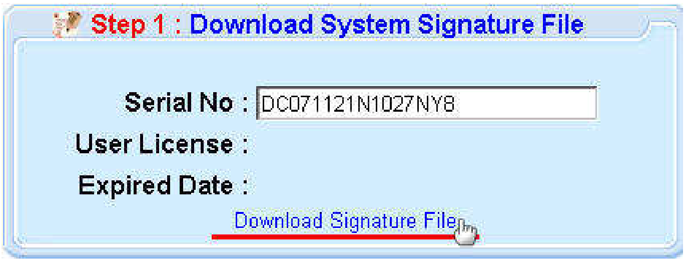
⏮ ⏪ 1 2 3 4 5 6 7 8 9 ⏩ ⏭ Total 2,112 Total Page 302 Current Page 1

Registration

This page shows the system registration information. For system registration and activation, please follow the below steps.

Signature File

Step 1: Enter the Serial Number and click on [Download Signature File] to download the Signature File. Sample format of the Signature File is signature_file_DC071121N1027NY8.



Step 1 : Download System Signature File

Serial No : DC071121N1027NY8

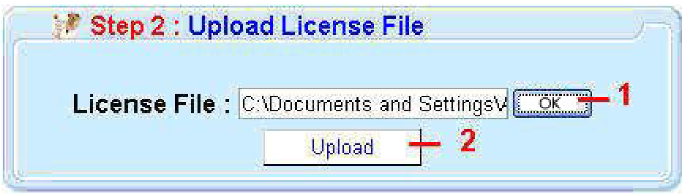
User License :

Expired Date :

Step 2: Please send the Signature File by email to support@level1.com with the subject : **ICI License File Request**.

Step 3 : After Registry has been verified the details, it will send the user the license file with the format like license_file_DC071121N1027NY8.

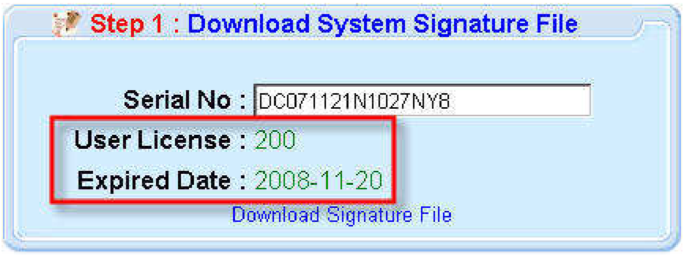
Step 4 : Upload this license file to ICI system for service activation.



Step 2 : Upload License File

License File : C:\Documents and Settings\

Step 5: Successful registration will show the user license and expiry date as shown below.



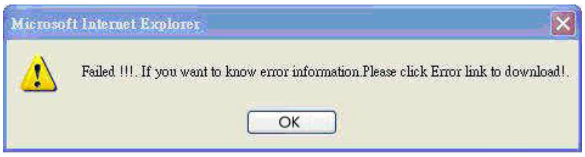
Step 1 : Download System Signature File

Serial No : DC071121N1027NY8

User License : 200

Expired Date : 2008-11-20

If the registration process fails (shown by Error message), please download register_import.log and send it to support@level1.com

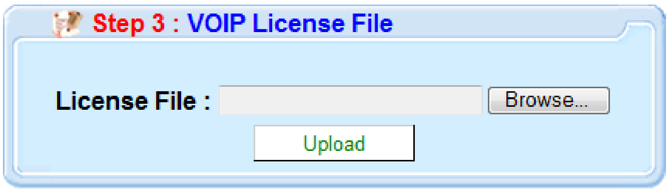


Microsoft Internet Explorer

Failed !!!. If you want to know error information.Please click Error link to download!.

VoIP License

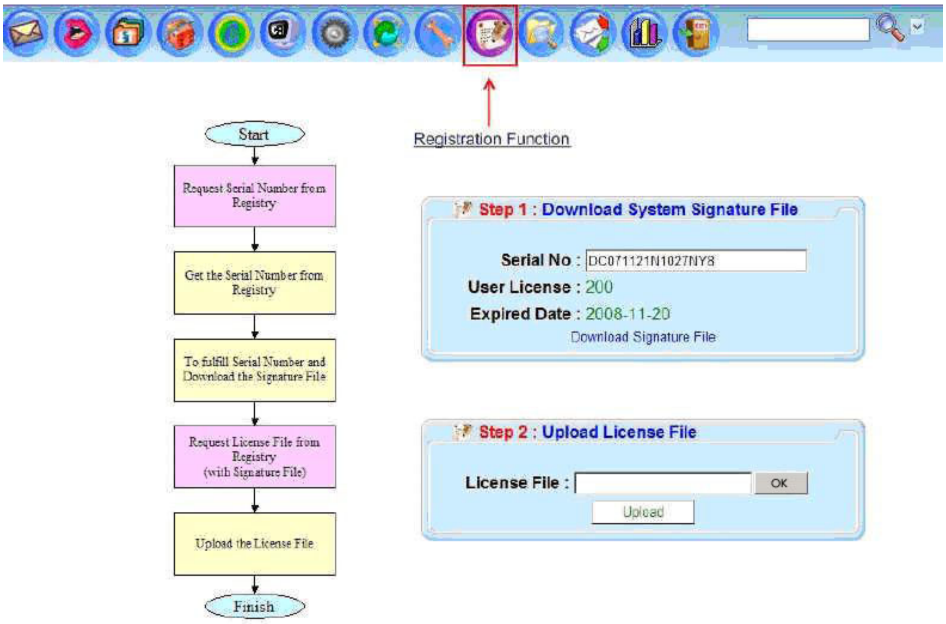
Voice over IP License (Optional Purchase) is to be uploaded at this Registration GUI as well. The license file will be named “licence.txt.”



Step 3 : VOIP License File

License File :

By default, the ICI system (appliance based) shipped out is already pre-registered. Please check by clicking the registration page. You will be able to see the following diagram with the serial no, user license and license expiry date.



Registration Function
Start
Request Serial Number from Registry
Get the Serial Number from Registry
To fulfill Serial Number and Download the Signature File
Request License File from Registry (with Signature File)
Upload the License File
Finish

Step 1 : Download System Signature File

Serial No : DC071121N1027NY8

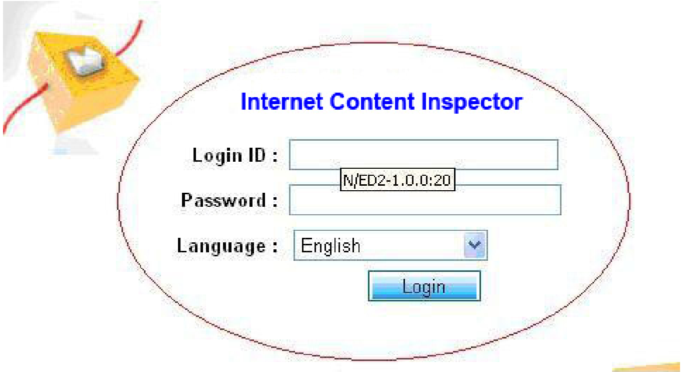
User License : 200

Expired Date : 2008-11-20

Step 2 : Upload License File

License File :

You can also check from the login page. Information like N/ED2-1.0.0:20 (ED version 2-1.0.0 and this system supports a maximum of 20 concurrent users) will be shown when the pointer is placed at the ICI system, Login ID or Password.



Internet Content Inspector

Login ID :

N/ED2-1.0.0:20

Password :

Language : English

Data Search

Full Text Search

Full Text Search provides the capability of searching into the database content of Email (such as POP3, SMTP, IMAP, Web Mail, IM Text Chat etc with the key word(s) inputted by the user. It is even capable to search in to attachment, file transfer, zipped file etc. and Listed the output result that contains the matching search criteria.

Key word(s) search supports full Boolean Algebra concept. For full details of Full Text Search, please refer to Appendix in this guide.

string	up to 32 words, 128 bytes per word
& AND	
OR	
NOT	
NEAR	
Logic Application " "	
@ : . - _	These 5 symbols, cannot be at the end of a word, such as "love@", system will filter out automatically
Alphabet	A, B, C,…
Number	
? *	Wildcard search ? represent one alphabet * represent multiple alphabet First search character cannot be wildcard character

For example:

li?e => to find out similar words like => live, life

li *e => to find out similar words like => live, life, license, little

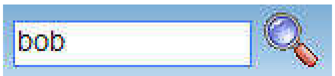
Following are the limitation of Full Text Search:
Natural language. Some of the words as follow will be automatically neglected by Full Text Search engine as it would have appeared too many times in the database content. Therefore for accuracy and performance, we neglect these words which we have known in as “Stop Words”.

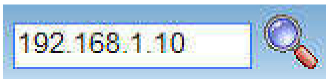
For example: "and", "are", "as", "at", "be", "but", "by", "for", "if", "in", "into", "is", "it", "no", "not", "of", "on", "or", "such", "that", "the", "their", "then", "there", "these", "they", "this", "to", "was", "will", "with"

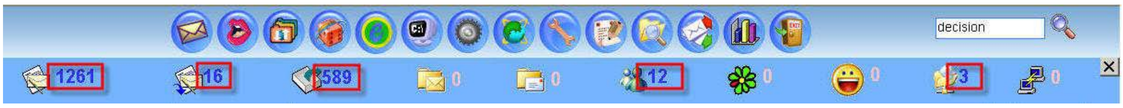
Does not support a single English alphabet search. Same concept as “Stop Words”

For example: "a" ,"b"

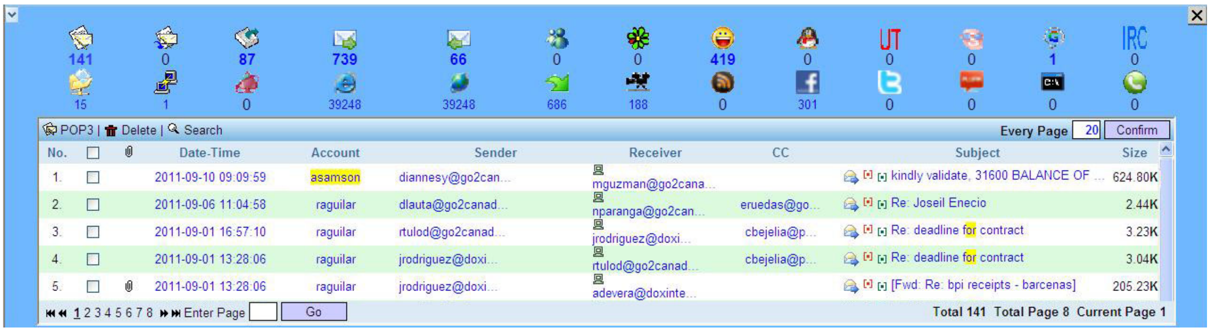
User can input key word or IP and press on 🔍 and the system will query and List out the content that match the search criteria as shown below.







Select and click on the application List (with the relevant number of hit), system will then List out all the record of that application.

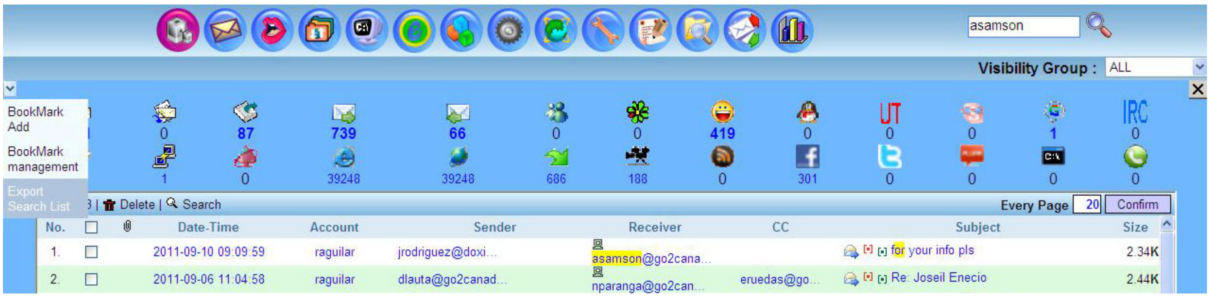


POP3 | Delete | Search — Every Page 20 Confirm

No.	□		Date-Time	Account	Sender	Receiver	CC	Subject	Size
1.	□		2011-09-10 09:09:59	asamson	diannesy@go2can...	mguzman@go2cana...		kindly validate, 31600 BALANCE OF ...	624.80K
2.	□		2011-09-06 11:04:58	raguilar	dlauta@go2canad...	nparanga@go2can...	eruedas@go...	Re: Joseil Enecio	2.44K
3.	□		2011-09-01 16:57:10	raguilar	rtulod@go2canad...	jrodriguez@doxi...	cbejelia@p...	Re: deadline for contract	3.23K
4.	□		2011-09-01 13:28:06	raguilar	jrodriguez@doxi...	rtulod@go2canad...	cbejelia@p...	Re: deadline for contract	3.04K
5.	□	📎	2011-09-01 13:28:06	raguilar	jrodriguez@doxi...	adevera@doxinte...		[Fwd: Re: bpi receipts - barcenas]	205.23K

1 2 3 4 5 6 7 8 Enter Page Go — Total 141 Total Page 8 Current Page 1

Export Search Records
Export the query result as Excel .csv file.



3 | Delete | Search — Every Page 20 Confirm

No.	□		Date-Time	Account	Sender	Receiver	CC	Subject	Size
1.	□		2011-09-10 09:09:59	raguilar	jrodriguez@doxi...	asamson@go2cana...		for your info pls	2.34K
2.	□		2011-09-06 11:04:58	raguilar	dlauta@go2canad...	nparanga@go2can...	eruedas@go...	Re: Joseil Enecio	2.44K

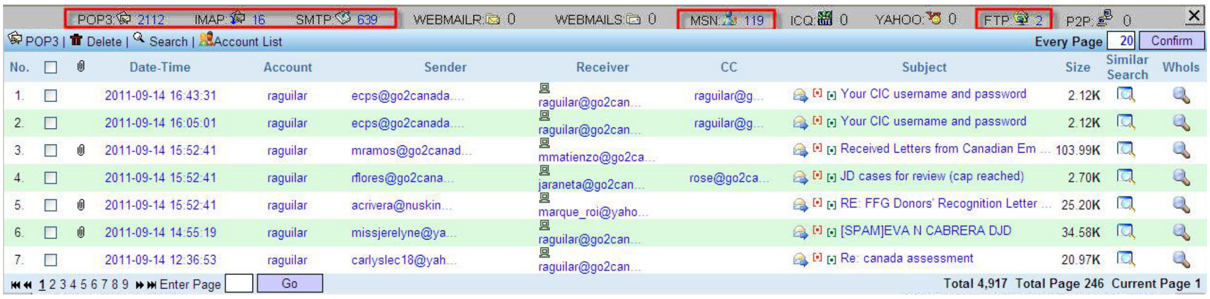
Similar Search

It provides relative search function which search for similar words, account names etc. in the database and display them according to application.

The key source of search is from:

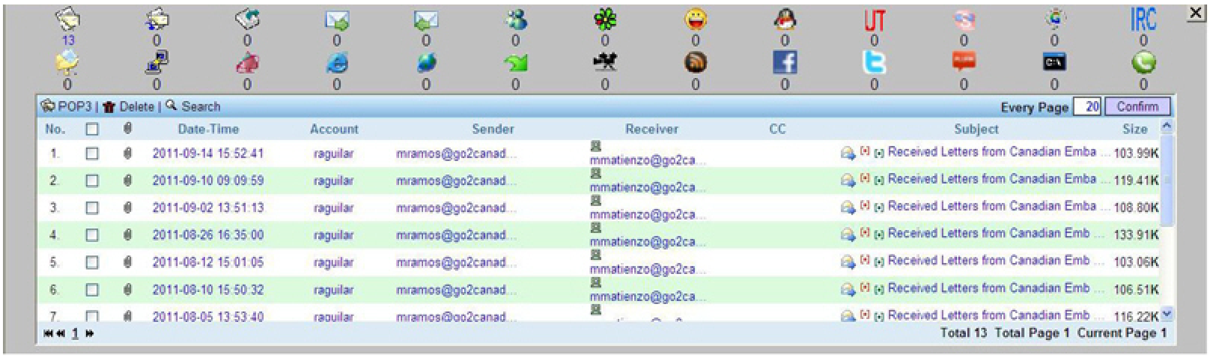
Similar Group	Words Source
SMTP, POP3, IMAP, WEBMAIL	subject from to cc bcc attachments content
ICQ, MSN, QQ, YAHOO	sender receiver messages
P2P, FTP	account filename

Click on 🔍 and the Similar Search function will show the results in subsequent diagram.



No.	□	📎	Date-Time	Account	Sender	Receiver	CC	Subject	Size	Similar Search	WhoIs
1.	□		2011-09-14 16:43:31	raguilar	ecps@go2canada....	raguilar@go2can...	raguilar@g...	Your CIC username and password	2.12K	🔍	🔍
2.	□		2011-09-14 16:05:01	raguilar	ecps@go2canada....	raguilar@go2can...	raguilar@g...	Your CIC username and password	2.12K	🔍	🔍
3.	□	📎	2011-09-14 15:52:41	raguilar	mramos@go2canad...	mmatienzo@go2ca...		Received Letters from Canadian Em ...	103.99K	🔍	🔍
4.	□		2011-09-14 15:52:41	raguilar	rflores@go2cana...	jaraneta@go2can...	rose@go2ca...	JD cases for review (cap reached)	2.70K	🔍	🔍
5.	□	📎	2011-09-14 15:52:41	raguilar	acrivera@nuskin...	marque_roi@yaho...		RE: FFG Donors' Recognition Letter ...	25.20K	🔍	🔍
6.	□	📎	2011-09-14 14:55:19	raguilar	missjerelyne@ya...	raguilar@go2can...		[SPAM]EVA N CABRERA DJD	34.58K	🔍	🔍
7.	□		2011-09-14 12:36:53	raguilar	carlyslec18@yah...	raguilar@go2can...		Re: canada assessment	20.97K	🔍	🔍

⏮ ⏪ 1 2 3 4 5 6 7 8 9 ⏩ ⏭ Enter Page [ ] Go   Total 4,917 Total Page 246 Current Page 1

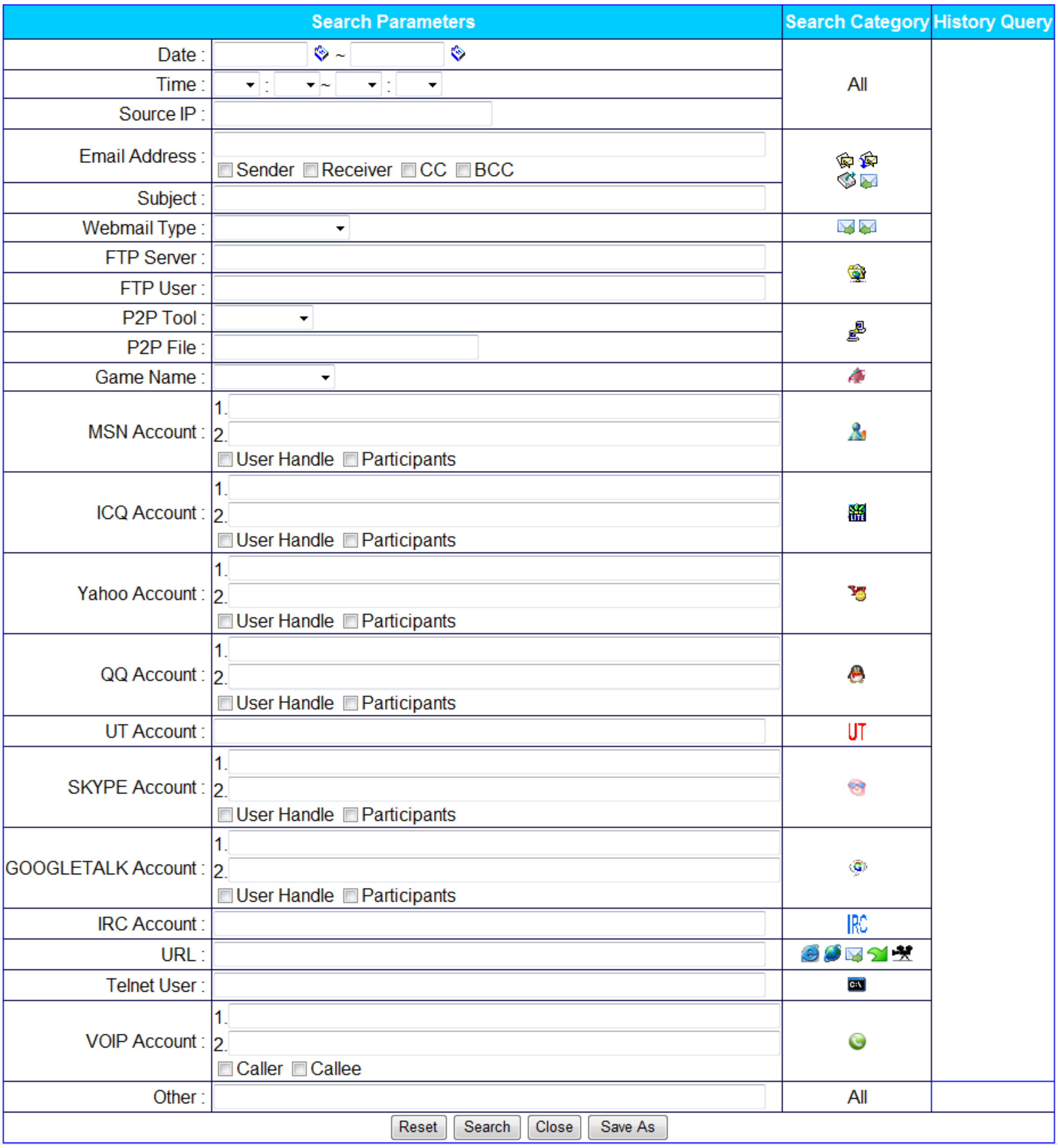


No.	□	📎	Date-Time	Account	Sender	Receiver	CC	Subject	Size
1.	□	📎	2011-09-14 15:52:41	raguilar	mramos@go2canad...	mmatienzo@go2ca...		Received Letters from Canadian Emba ...	103.99K
2.	□	📎	2011-09-10 09:09:59	raguilar	mramos@go2canad...	mmatienzo@go2ca...		Received Letters from Canadian Emba ...	119.41K
3.	□	📎	2011-09-02 13:51:13	raguilar	mramos@go2canad...	mmatienzo@go2ca...		Received Letters from Canadian Emba ...	108.80K
4.	□	📎	2011-08-26 16:35:00	raguilar	mramos@go2canad...	mmatienzo@go2ca...		Received Letters from Canadian Emb ...	133.91K
5.	□	📎	2011-08-12 15:01:05	raguilar	mramos@go2canad...	mmatienzo@go2ca...		Received Letters from Canadian Emb ...	103.06K
6.	□	📎	2011-08-10 15:50:32	raguilar	mramos@go2canad...	mmatienzo@go2ca...		Received Letters from Canadian Emb ...	106.51K
7.	□	📎	2011-08-05 13:53:40	raguilar	mramos@go2canad...			Received Letters from Canadian Emb ...	116.22K

⏮ ⏪ 1 ⏩   Total 13 Total Page 1 Current Page 1

Data Search – Conditional or Parameter Search

The system provides advanced Data Search (Conditional or Parameters Search) function. Information or data recorded can be searched based on different applications and parameters set.



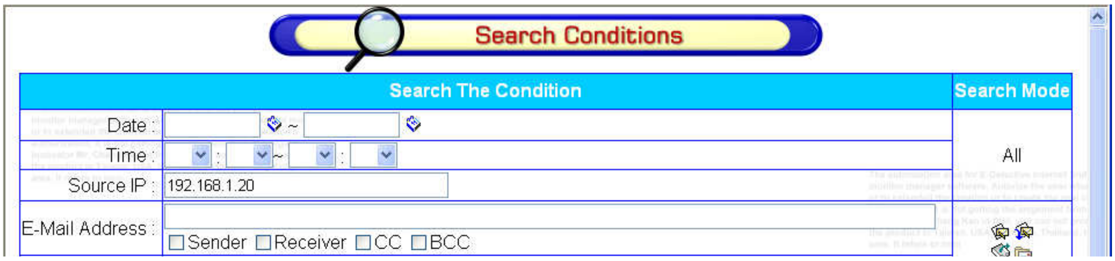
Search Parameters		Search Category	History Query
Date :	~	All	
Time :	▾ : ▾ ~ ▾ : ▾		
Source IP :			
Email Address :	□ Sender □ Receiver □ CC □ BCC		
Subject :			
Webmail Type :	▾		
FTP Server :			
FTP User :			
P2P Tool :	▾		
P2P File :			
Game Name :	▾		
MSN Account :	1. 2. □ User Handle □ Participants		
ICQ Account :	1. 2. □ User Handle □ Participants		
Yahoo Account :	1. 2. □ User Handle □ Participants		
QQ Account :	1. 2. □ User Handle □ Participants		
UT Account :		UT	
SKYPE Account :	1. 2. □ User Handle □ Participants		
GOOGLETALK Account :	1. 2. □ User Handle □ Participants		
IRC Account :		IRC	
URL :			
Telnet User :			
VOIP Account :	1. 2. □ Caller □ Callee		
Other :		All	

Search Parameters by Application or Service Category

Item	Description	Example
Date	From X to X: Format Date (Year/Month/Day)	2007-11-10
Time	From X to X: Format Time (Hour: Minute)	23:11
Source IP	The IP address to search	192.168.1.100
Email Address	The Email address in Sender, Receiver, CC or BCC	frankie@abc.com
Subject	The subject or title keywords	Hello ...
Webmail Type	The webmail type	Yahoo
FTP Server	The FTP IP address	192.168.1.249
FTP User	The FTP user account	admin
P2P Tool	The P2P tool use	LimeWire
P2P File	The P2P file name	Abc.mp3
Game Name	The name of the online game	Kartrider
MSN Account	The account of MSN (User Handle/Participant)	abc@hotmail.com
ICQ Account	The account of ICQ (User Handle/Participant)	11244567
Yahoo Account	The account of YAHOO (User Handle/Participant)	abc@yahoo.com
QQ Account	The account of QQ (User Handle/Participant)	23456995
HTTP	URL Link	www.yahoo.com.au
Telnet User	The user account	
VoIP Account	SIP Caller and Called Number	
Other	Searching the related information from all data type by the keyword	Movie, Carlos, Tom

Example: Search the records of specific source IP

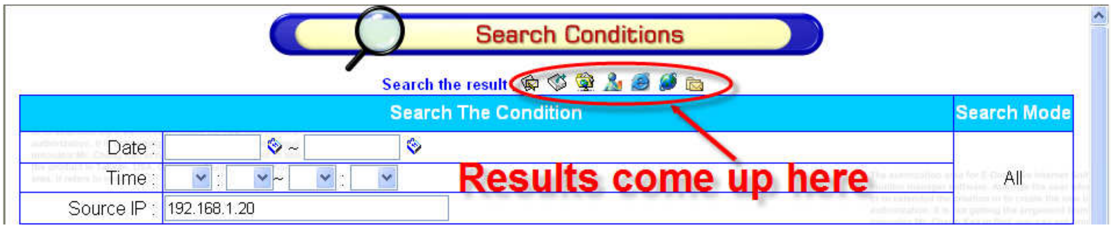
Step 1: Type the Source IP “192.168.1.20” and click on the button [search].



Search Conditions

Search The Condition		Search Mode
Date :	~	All
Time :	: ~ :	
Source IP :	192.168.1.20	
E-Mail Address :	□Sender □Receiver □CC □BCC	

Step 2: Result will be shown.



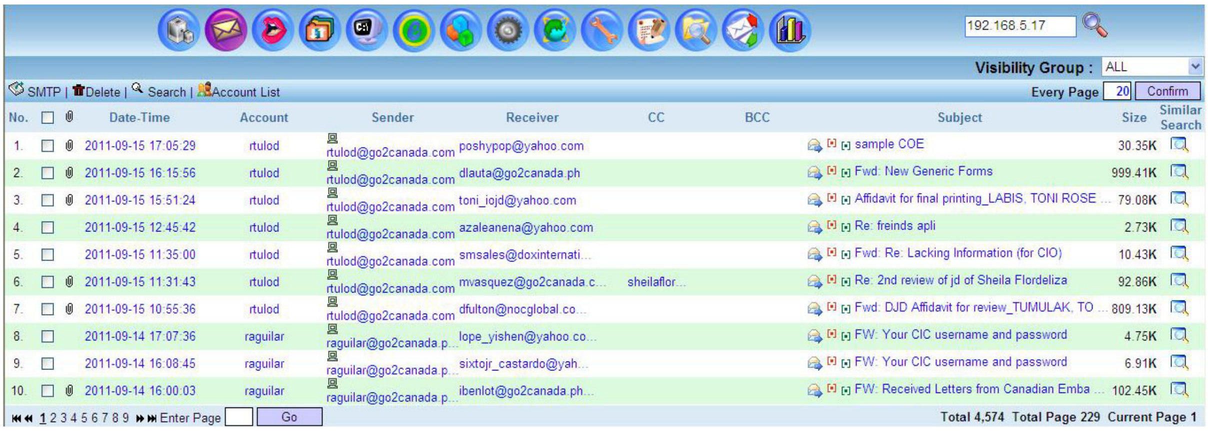
Search Conditions

Search the result

Search The Condition		Search Mode
Date :	~	All
Time :	: ~ :	
Source IP :	192.168.1.20	

Results come up here

Step 3: Click on the SMTP icon above, the records will be shown as the following diagram.



192.168.5.17

Visibility Group : ALL

SMTP | Delete | Search | Account List

Every Page 20 Confirm

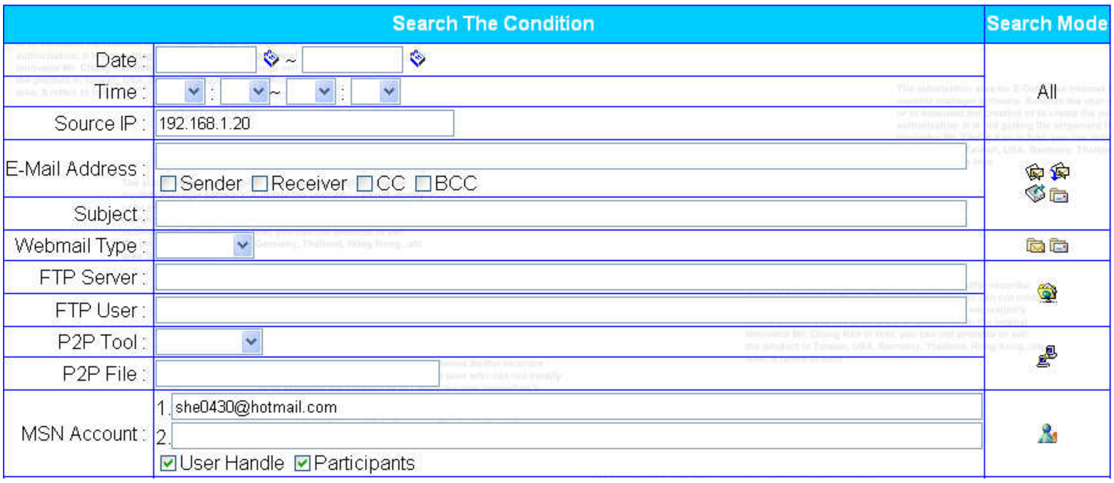
No.	□	📎	Date-Time	Account	Sender	Receiver	CC	BCC	Subject	Size	Similar Search
1.	□	📎	2011-09-15 17:05:29	rtulod	rtulod@go2canada.com	poshypop@yahoo.com			sample COE	30.35K	🔍
2.	□	📎	2011-09-15 16:15:56	rtulod	rtulod@go2canada.com	dlauta@go2canada.ph			Fwd: New Generic Forms	999.41K	🔍
3.	□	📎	2011-09-15 15:51:24	rtulod	rtulod@go2canada.com	toni_iojd@yahoo.com			Affidavit for final printing_LABIS, TONI ROSE ...	79.08K	🔍
4.	□		2011-09-15 12:45:42	rtulod	rtulod@go2canada.com	azaleanena@yahoo.com			Re: freinds apli	2.73K	🔍
5.	□		2011-09-15 11:35:00	rtulod	rtulod@go2canada.com	smsales@doxinternati...			Fwd: Re: Lacking Information (for CIO)	10.43K	🔍
6.	□	📎	2011-09-15 11:31:43	rtulod	rtulod@go2canada.com	mvasquez@go2canada.c...	sheilaflor...		Re: 2nd review of jd of Sheila Flordeliza	92.86K	🔍
7.	□	📎	2011-09-15 10:55:36	rtulod	rtulod@go2canada.com	dfulton@nocglobal.co...			Fwd: DJD Affidavit for review_TUMULAK, TO ...	809.13K	🔍
8.	□		2011-09-14 17:07:36	raguilar	raguilar@go2canada.p...	lope_yishen@yahoo.co...			FW: Your CIC username and password	4.75K	🔍
9.	□		2011-09-14 16:08:45	raguilar	raguilar@go2canada.p...	sixtojr_castardo@yah...			FW: Your CIC username and password	6.91K	🔍
10.	□	📎	2011-09-14 16:00:03	raguilar	raguilar@go2canada.p...	ibenlot@go2canada.ph...			FW: Received Letters from Canadian Emba ...	102.45K	🔍

1 2 3 4 5 6 7 8 9 Enter Page Go

Total 4,574 Total Page 229 Current Page 1

Example: Search the records of specific source IP and MSN account.

Step1: Type the Source IP “192.168.1.20”, Msn account “she0430@hotmail.com” and click on the button [search].



Search The Condition | Search Mode

Date : ~

Time : : ~ :

Source IP : 192.168.1.20

E-Mail Address : □Sender □Receiver □CC □BCC

Subject :

Webmail Type :

FTP Server :

FTP User :

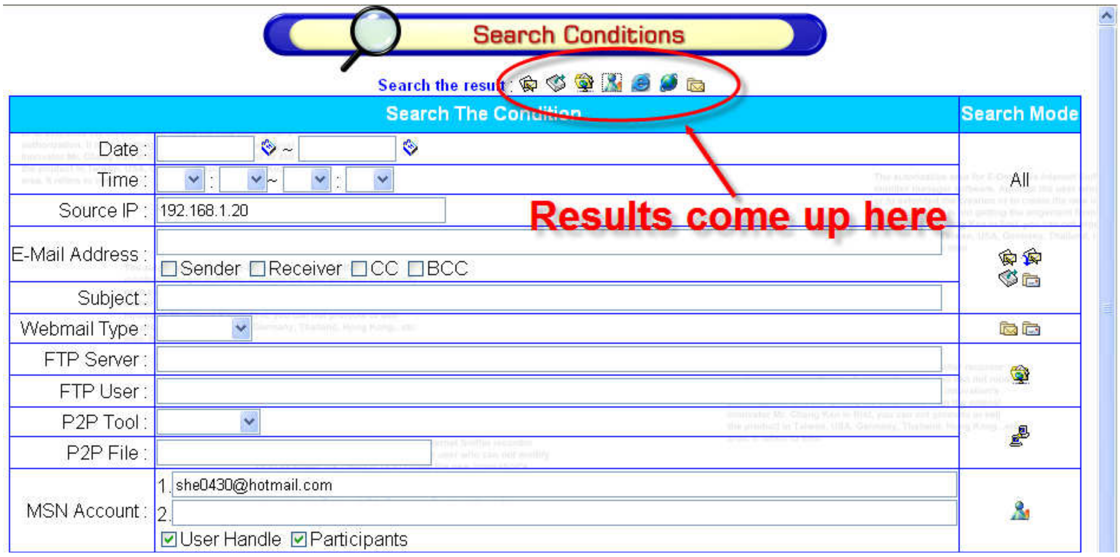
P2P Tool :

P2P File :

MSN Account : 1. she0430@hotmail.com
2.
☑User Handle ☑Participants

All

Step 2: Result will be shown.



Search The Condition | Search Mode

Date : ~

Time : : ~ :

Source IP : 192.168.1.20

E-Mail Address : □Sender □Receiver □CC □BCC

Subject :

Webmail Type :

FTP Server :

FTP User :

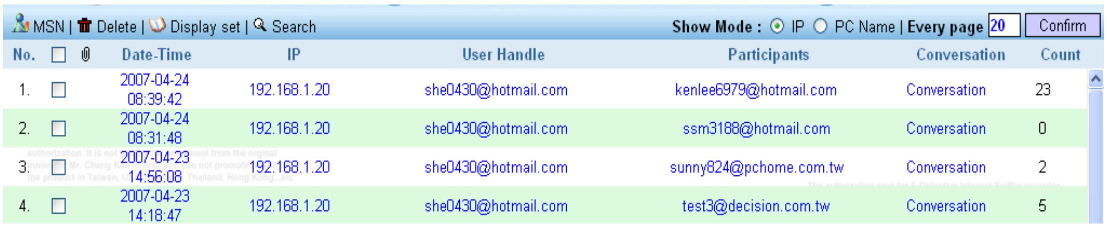
P2P Tool :

P2P File :

MSN Account : 1. she0430@hotmail.com
2.
☑User Handle ☑Participants

All

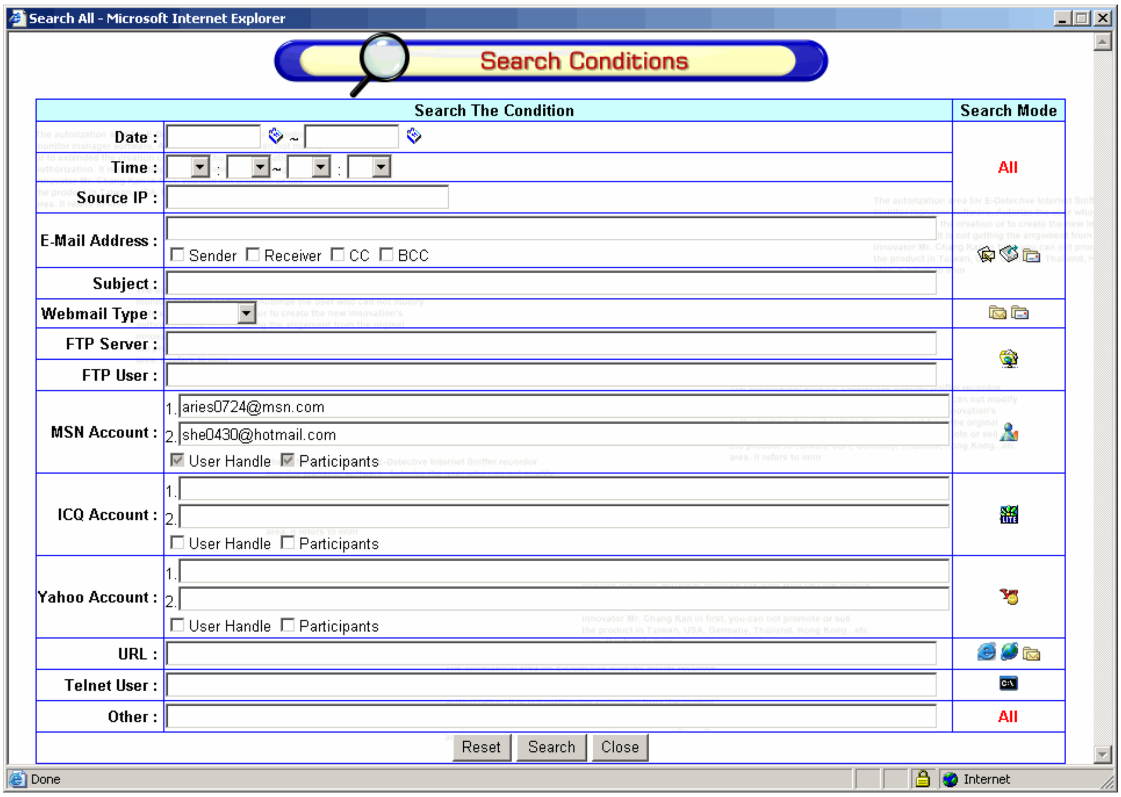
Step 3: Click on the MSN icon above, the records will be shown as the following diagram.



MSN | Delete | Display set | Search   Show Mode : ◉ IP ○ PC Name | Every page 20 Confirm

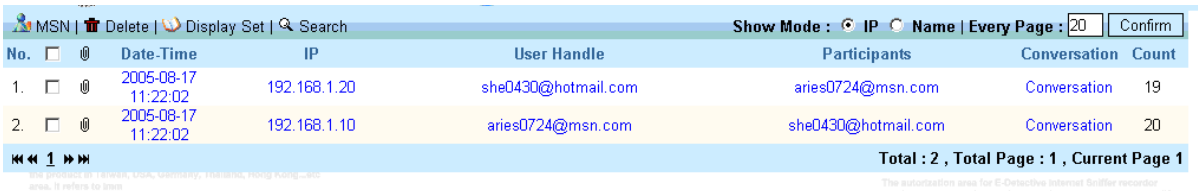
No.	□		Date-Time	IP	User Handle	Participants	Conversation	Count
1.	□		2007-04-24 08:39:42	192.168.1.20	she0430@hotmail.com	kenlee6979@hotmail.com	Conversation	23
2.	□		2007-04-24 08:31:48	192.168.1.20	she0430@hotmail.com	ssm3188@hotmail.com	Conversation	0
3.	□		2007-04-23 14:56:08	192.168.1.20	she0430@hotmail.com	sunny824@pchome.com.tw	Conversation	2
4.	□		2007-04-23 14:18:47	192.168.1.20	she0430@hotmail.com	test3@decision.com.tw	Conversation	5

Example: Search the records of the specific MSN account.



MSN Account :
1. aries0724@msn.com
2. she0430@hotmail.com
☑ User Handle ☑ Participants

The data search based on the search parameters of user reference account (user handle) and participant reference account. User reference account as [aries0724@msn.com] and participant reference account [she0343@hotmail.com].



MSN | Delete | Display Set | Search
Show Mode : ● IP ○ Name | Every Page : 20 Confirm

No.	□		Date-Time	IP	User Handle	Participants	Conversation	Count
1.	□		2005-08-17 11:22:02	192.168.1.20	she0430@hotmail.com	aries0724@msn.com	Conversation	19
2.	□		2005-08-17 11:22:02	192.168.1.10	aries0724@msn.com	she0430@hotmail.com	Conversation	20

⏮ ⏪ 1 ⏩ ⏭ Total : 2 , Total Page : 1 , Current Page 1

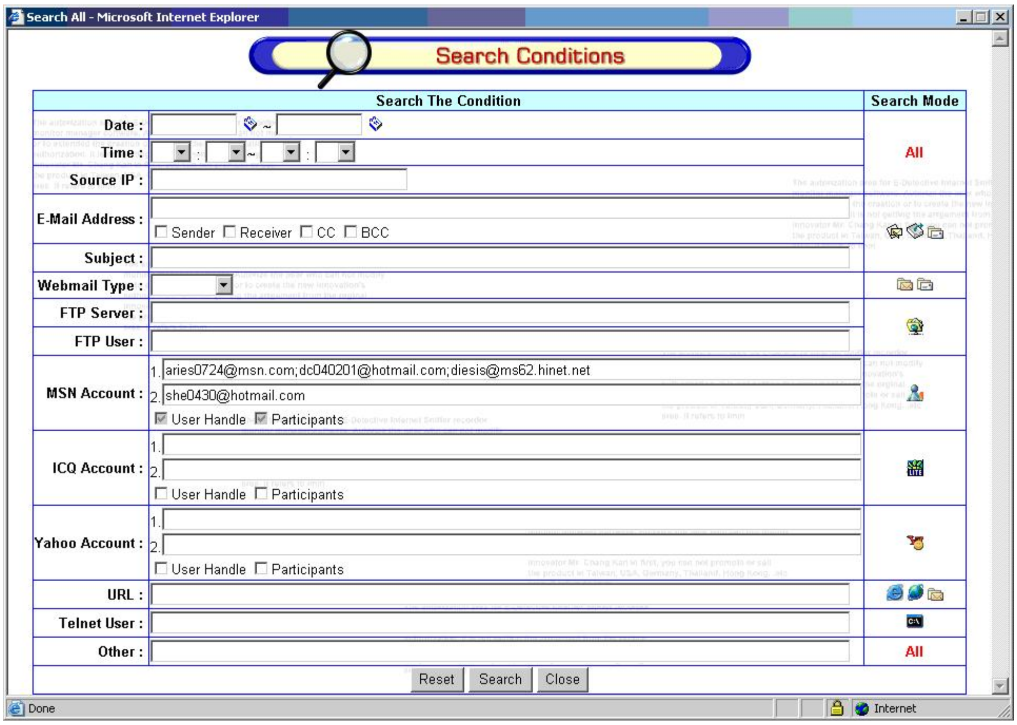
So it can be categorized as two combined groups:

1. User reference account as [aries0724@msn.com] and participant reference account [she0343@hotmail.com].
2. User reference account as [she0343@hotmail.com] and participant reference account [aries0724@msn.com].

Instruction:
When you key in two textbox column, the first textbox column is as single account [dc@level1.com], the second textbox column is as single account [web@level1.com], then checkbox column will be enabled.

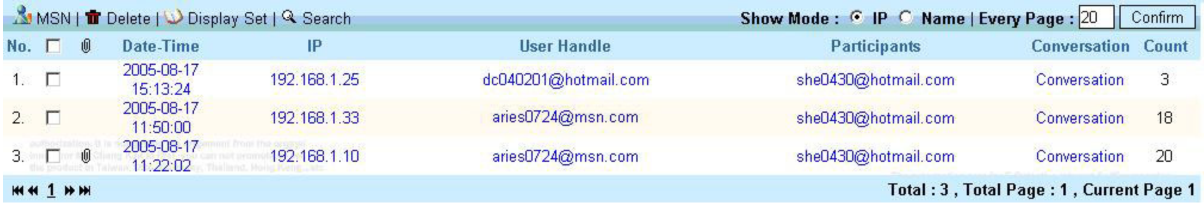
It is not allowed to modify and search the data as below:
[(user reference account = dc@level1.com and participant reference account = web@level1.com) or (participant reference account = web@level1.com and user reference account = dc@level1.com)], then use "and" combining the other search row with other application.

Example: Input two or three user reference accounts and one participant reference account at MSN/ ICQ/YAHOO



Search The Condition		Search Mode
Date :	~	All
Time :	: ~ :	
Source IP :		
E-Mail Address :	□ Sender □ Receiver □ CC □ BCC	
Subject :		
Webmail Type :		
FTP Server :		
FTP User :		
MSN Account :	1. aries0724@msn.com;dc040201@hotmail.com;diesis@ms62.hinet.net 2. she0430@hotmail.com ☑ User Handle ☑ Participants	
ICQ Account :	1. 2. □ User Handle □ Participants	
Yahoo Account :	1. 2. □ User Handle □ Participants	
URL :		
Telnet User :		
Other :		All

The data search based on the search parameters of user reference account aries0724@msn.com or dc040201@hotmail.com or diesis@ms62.hinte.net] and participant reference account aries0724@msn.com



MSN | Delete | Display Set | Search
Show Mode : ● IP ○ Name | Every Page : 20 Confirm

No.	□		Date-Time	IP	User Handle	Participants	Conversation	Count
1.	□		2005-08-17 15:13:24	192.168.1.25	dc040201@hotmail.com	she0430@hotmail.com	Conversation	3
2.	□		2005-08-17 11:50:00	192.168.1.33	aries0724@msn.com	she0430@hotmail.com	Conversation	18
3.	□	📎	2005-08-17 11:22:02	192.168.1.10	aries0724@msn.com	she0430@hotmail.com	Conversation	20

Total : 3 , Total Page : 1 , Current Page 1

So it can be categorized as three combined groups:

1. User reference account as [aries0724@msn.com] and participant reference account [she0343@hotmail.com].
2. User reference account as [dc040201@hotmail.com] and participant reference account [she0430@hotmail.com].
3. User reference account as [diesis@ms62.hinet.net] and participant reference account [she0430@hotmail.com].

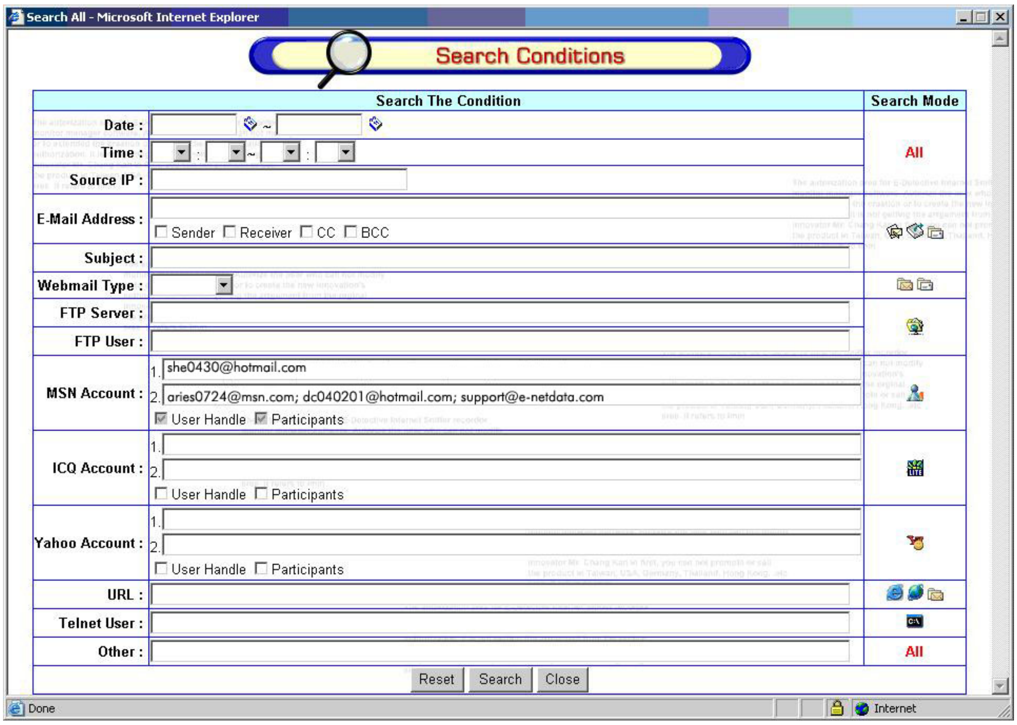
Instruction:

When you key in two textbox column, the first textbox column is as [web@level1.com ; ken@level1.com] for multi-account (maximum only 3 multi-account), the second textbox column is as single account [web@level1.com], then checkbox column will be enabled.

It is not allowed to modify and search the data as below：

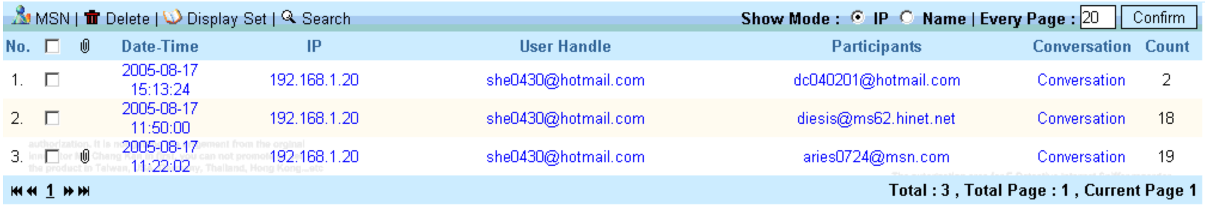
[(Participant reference account = dc@Level1.com and user reference account = web@Level1.com) or (user reference account = Ken@Level1.com)], then use "and" combining the search of other row or application.

Example: Input one user reference account and two or three participant reference accounts at MSN/ ICQ/ YAHOO.



MSN Account :
1. she0430@hotmail.com
2. aries0724@msn.com; dc040201@hotmail.com; support@e-netdata.com
☑ User Handle ☑ Participants

The data search based on the search parameters of user reference account she0430@hotmail.com and participant reference account aries0724@msn.com or dc040201@hotmail.com or diesis@ms62.hinet.net


MSN | Delete | Display Set | Search
Show Mode : ● IP ○ Name | Every Page : 20 Confirm
⏮ ⏪ 1 ⏩ ⏭

No.	□	📎	Date-Time	IP	User Handle	Participants	Conversation	Count
1.	□		2005-08-17 15:13:24	192.168.1.20	she0430@hotmail.com	dc040201@hotmail.com	Conversation	2
2.	□		2005-08-17 11:50:00	192.168.1.20	she0430@hotmail.com	diesis@ms62.hinet.net	Conversation	18
3.	□	📎	2005-08-17 11:22:02	192.168.1.20	she0430@hotmail.com	aries0724@msn.com	Conversation	19

Total : 3 , Total Page : 1 , Current Page 1

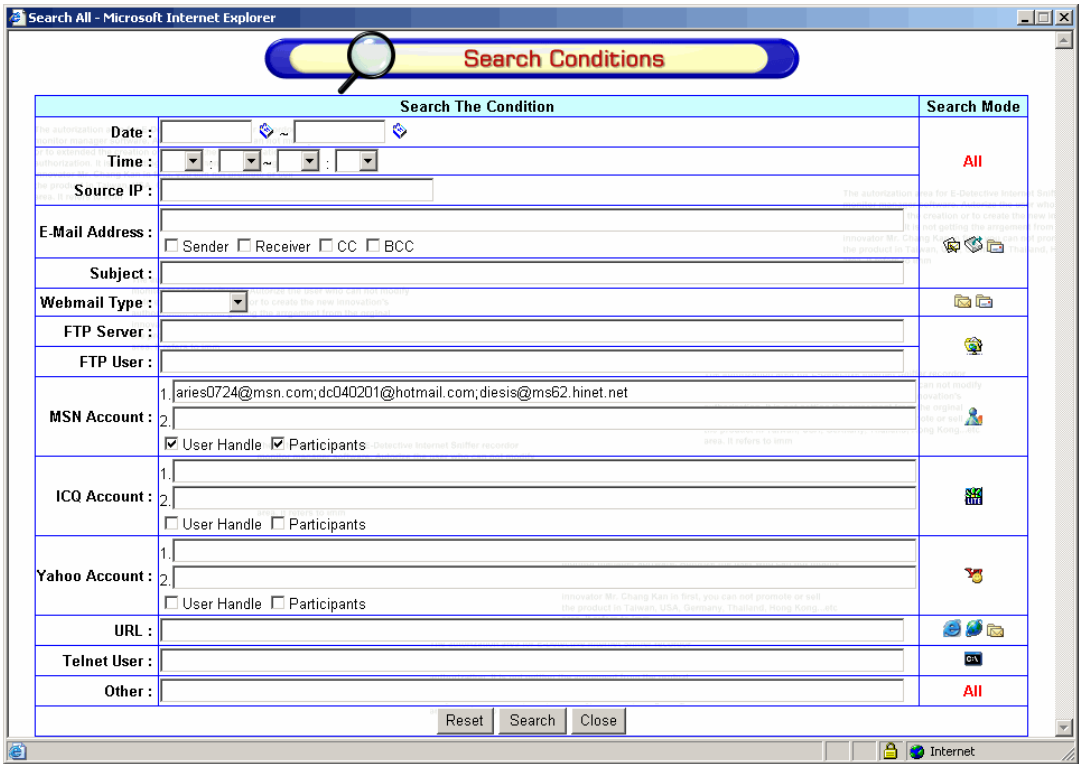
So it can be categorized as three combined groups:

1. User reference account as [she0343@hotmail.com] and participant reference account [aries0724@msn.com]
2. User reference account as [she0430@hotmail.com] and participant reference account [dc040201@hotmail.com]
3. User reference account as [she0430@hotmail.com]and participant reference account [diesis@ms62.hinet.net]

Instruction:
When you key in two textbox column, the first textbox column is as single account dc@Level1.com , the second textbox column is as multi-account [web@Level1.com]; ken@Level1.com (maximum only 3 multi-account), then checkbox column will be enabled.

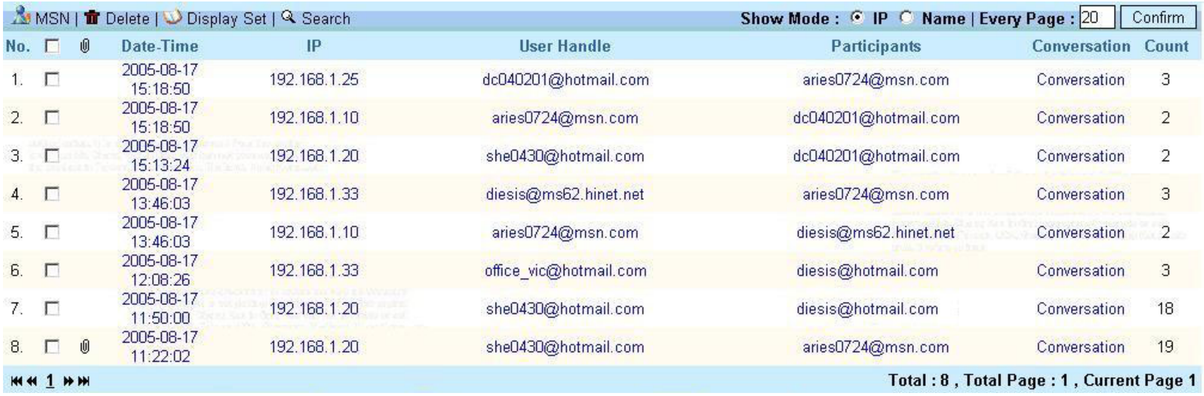
It is not allowed to modify and search the data as below：
User reference account = dc@Level1.com and participant reference account = web@Level1.com or participant reference account = ken@Level1.com, then use "and" combining the other search row and application.

Example: Input two or three user reference accounts without key in participant reference accounts at MSN/ ICQ/ YAHOO.



Search The Condition		Search Mode
Date :	~	All
Time :	: ~ :	
Source IP :		
E-Mail Address :	□ Sender □ Receiver □ CC □ BCC	
Subject :		
Webmail Type :		
FTP Server :		
FTP User :		
MSN Account :	1. aries0724@msn.com;dc040201@hotmail.com;diesis@ms62.hinet.net 2. ☑ User Handle ☑ Participants	
ICQ Account :	1. 2. □ User Handle □ Participants	
Yahoo Account :	1. 2. □ User Handle □ Participants	
URL :		
Telnet User :		
Other :		All

The data search based on the search parameters of user reference account or participant reference account aries0724@msn.com or dc040201@hotmail.com or diesis@ms62.hinet.net



MSN | Delete | Display Set | Search
Show Mode : ● IP ○ Name | Every Page : 20 Confirm

No.	□		Date-Time	IP	User Handle	Participants	Conversation	Count
1.	□		2005-08-17 15:18:50	192.168.1.25	dc040201@hotmail.com	aries0724@msn.com	Conversation	3
2.	□		2005-08-17 15:18:50	192.168.1.10	aries0724@msn.com	dc040201@hotmail.com	Conversation	2
3.	□		2005-08-17 15:13:24	192.168.1.20	she0430@hotmail.com	dc040201@hotmail.com	Conversation	2
4.	□		2005-08-17 13:46:03	192.168.1.33	diesis@ms62.hinet.net	aries0724@msn.com	Conversation	3
5.	□		2005-08-17 13:46:03	192.168.1.10	aries0724@msn.com	diesis@ms62.hinet.net	Conversation	2
6.	□		2005-08-17 12:08:26	192.168.1.33	office_vic@hotmail.com	diesis@hotmail.com	Conversation	3
7.	□		2005-08-17 11:50:00	192.168.1.20	she0430@hotmail.com	diesis@hotmail.com	Conversation	18
8.	□	📎	2005-08-17 11:22:02	192.168.1.20	she0430@hotmail.com	aries0724@msn.com	Conversation	19

Total : 8 , Total Page : 1 , Current Page 1

So it can be categorized as six combined groups:

1. User reference account as [aries0724@msn.com] and participant reference account will be as any account.
2. User reference account as [dc040201@hotmail.com] and participant reference account will be as any account.
3. User reference account as [diesis@ms62.hinet.net] and participant reference account will be as any account.
4. User reference account will be as any account and participant reference account as [aries0724@msn.com]
5. User reference account will be as any account and participant reference account as [dc040201@hotmail.com]
6. User reference account will be as any account and participant reference account as [diesis@ms62.hinet.net]

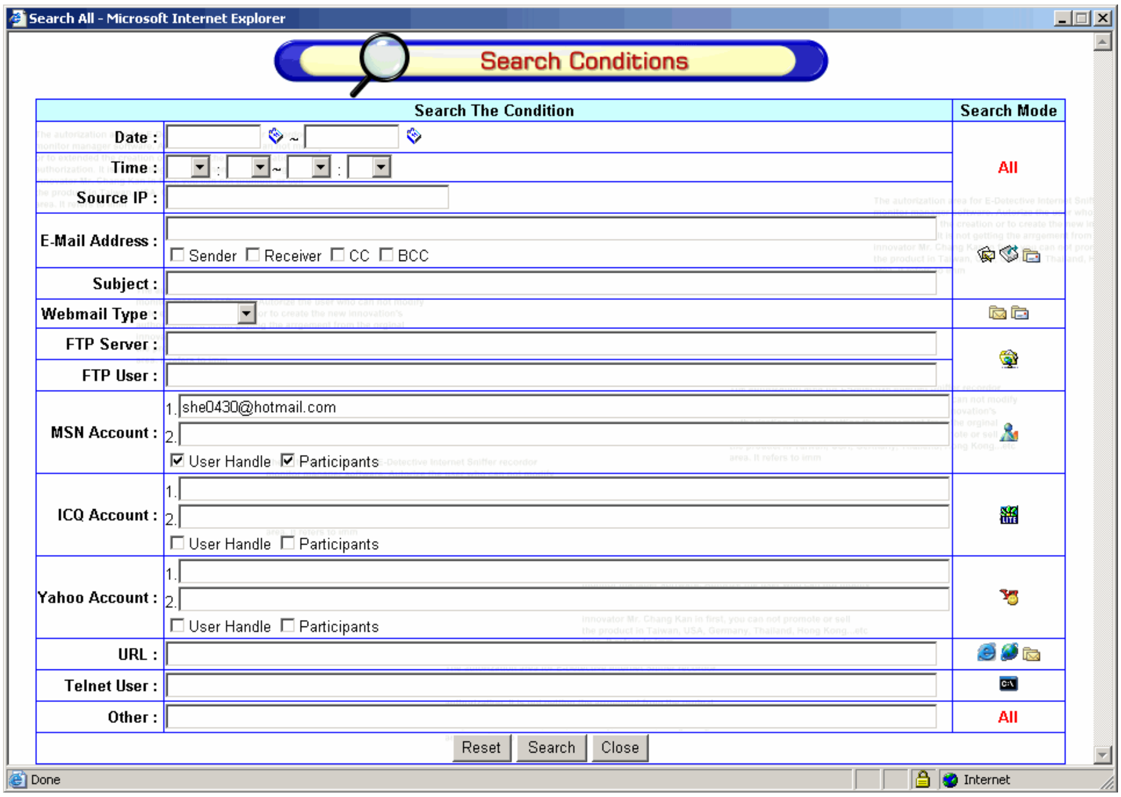
Instruction:

1. When you key in the first textbox column as multi-account [dc@Level1.com, web@Level1.com] (maximum only 3 multi-account), then checkbox column will be enabled, the data will be searched like as below:
   user reference account = dc@Level1.com or user reference account = web@Level1.com , then use "and" combining the other searching column.

2. When you key in the first textbox column as multi-account dc@Level1.com , web@Level1.com (3 multi-account maximum), then only select the participant account at checkbox column, the data will be searched like as below: (participant reference account = dc@Level1.com or participant reference account = web@Level1.com) , then use "and" combining the other searching column.

3. When you key in the first textbox column as multi-account dc@Level1.com , web@Level1.com (3 multi-account maximum), then select the participant account and user reference account at check box column, the data will be searched as below:
   (user reference account = dc@Level1.com or participant reference account = web@Level1.com or participant reference account = dc@Level1.com or user reference account = web@Level1.com).

Example: Input one user reference account without key in participant reference account at MSN/ ICQ/ YAHOO.

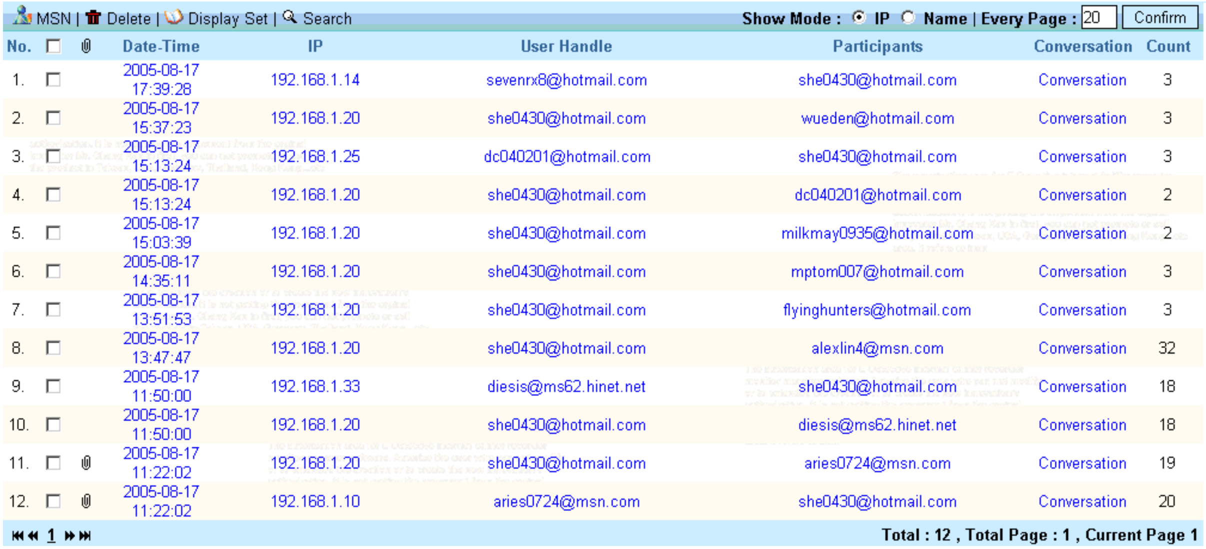


Search All - Microsoft Internet Explorer

Search Conditions

Search The Condition		Search Mode
Date :	~	All
Time :	: ~ :	
Source IP :		
E-Mail Address :	□ Sender □ Receiver □ CC □ BCC	
Subject :		
Webmail Type :		
FTP Server :		
FTP User :		
MSN Account :	1. she0430@hotmail.com 2. ☑ User Handle ☑ Participants	
ICQ Account :	1. 2. □ User Handle □ Participants	
Yahoo Account :	1. 2. □ User Handle □ Participants	
URL :		
Telnet User :		
Other :		All

The data search based on the search parameters of user reference account or participant reference account she0430@hotmail.com



Show Mode : ● IP ○ Name | Every Page : 20 Confirm

No.	□	📎	Date-Time	IP	User Handle	Participants	Conversation	Count
1.	□		2005-08-17 17:39:28	192.168.1.14	sevenrx8@hotmail.com	she0430@hotmail.com	Conversation	3
2.	□		2005-08-17 15:37:23	192.168.1.20	she0430@hotmail.com	wueden@hotmail.com	Conversation	3
3.	□		2005-08-17 15:13:24	192.168.1.25	dc040201@hotmail.com	she0430@hotmail.com	Conversation	3
4.	□		2005-08-17 15:13:24	192.168.1.20	she0430@hotmail.com	dc040201@hotmail.com	Conversation	2
5.	□		2005-08-17 15:03:39	192.168.1.20	she0430@hotmail.com	milkmay0935@hotmail.com	Conversation	2
6.	□		2005-08-17 14:35:11	192.168.1.20	she0430@hotmail.com	mptom007@hotmail.com	Conversation	3
7.	□		2005-08-17 13:51:53	192.168.1.20	she0430@hotmail.com	flyinghunters@hotmail.com	Conversation	3
8.	□		2005-08-17 13:47:47	192.168.1.20	she0430@hotmail.com	alexlin4@msn.com	Conversation	32
9.	□		2005-08-17 11:50:00	192.168.1.33	diesis@ms62.hinet.net	she0430@hotmail.com	Conversation	18
10.	□		2005-08-17 11:50:00	192.168.1.20	she0430@hotmail.com	diesis@ms62.hinet.net	Conversation	18
11.	□	📎	2005-08-17 11:22:02	192.168.1.20	she0430@hotmail.com	aries0724@msn.com	Conversation	19
12.	□	📎	2005-08-17 11:22:02	192.168.1.10	aries0724@msn.com	she0430@hotmail.com	Conversation	20

Total : 12 , Total Page : 1 , Current Page 1

So it can categorize as two combined groups:

1. User reference account as [she0430@hotmail.com] and participant reference account will be as any account.
2. User reference account will be any account and participant reference account is as [she0430@hotmail.com]

Instruction:

1. When you key in the first textbox column as single account dc@Level1.com , then checkbox column will be selected only user reference account and searched the data like as below:
   (user reference account = dc@Level1.com) then use "and" combining the other searching column.

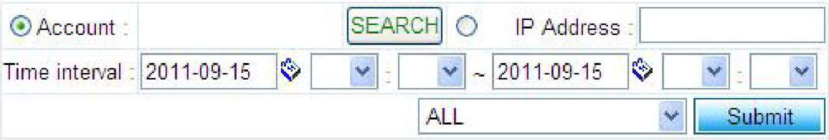
2. When you key in the first textbox column as single account dc@Level1.com , then checkbox column will be selected only participant reference account and searched the data like as below:
   (participant reference account = dc@Level1.com) then use "and" combining the other searching column.

3. When you key in the first textbox column as single account dc@Level1.com , then checkbox column will be selected both user reference account and participant reference account, then the data will be searched like as below:
   (user reference account = dc@Level1.com or participant reference account = dc@Level1.com) , then use "and" combining the other searching column.

Association Search

It allows the association search by Account or by IP Address.

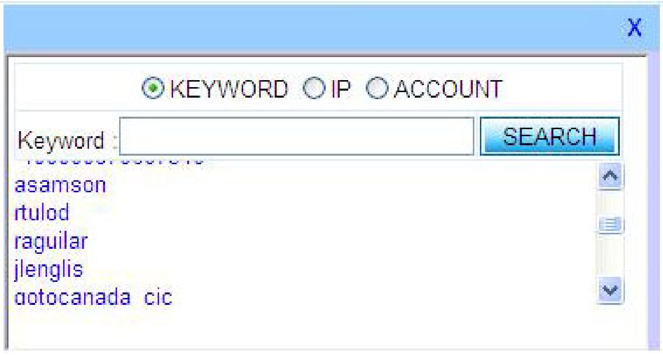
For instance, click on Account – [SEARCH] button and a Window will pop out. You may key in to search for KEYWORD/IP/ACCOUNT. After select the search condition and input the information to search, click on [SEARCH] and the system will look up the related information in the database and List them down. You may select and click on the item Listed. It will direct you to back to the original Window and you may then select Time Interval and Protocol/Service to Search for the information you want. By clicking on [Submit], the system will search for the related information and Listed them down.



● Account : [SEARCH] ○ IP Address :

Time interval : 2011-09-15 : ~ 2011-09-15 :

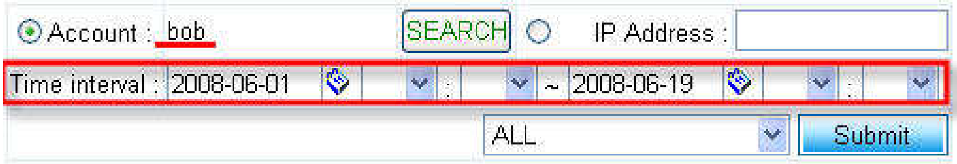
ALL [Submit]



● KEYWORD ○ IP ○ ACCOUNT

Keyword : [SEARCH]

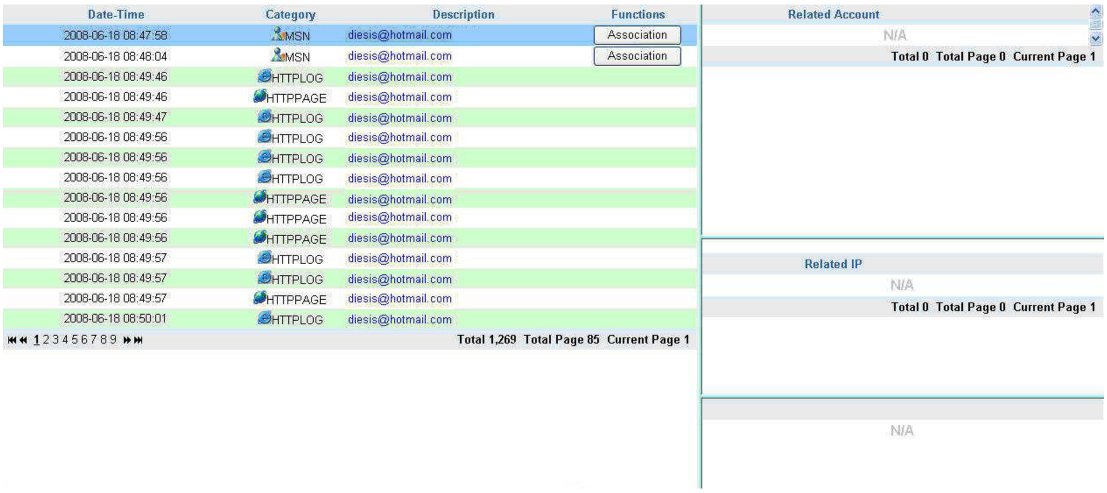
asamson
rtulod
raguilar
jlenglis
aotocanada_cic



● Account : bob [SEARCH] ○ IP Address :

Time interval : 2008-06-01 : ~ 2008-06-19 :

ALL [Submit]



Date-Time	Category	Description	Functions
2008-06-18 08:47:58	MSN	diesis@hotmail.com	Association
2008-06-18 08:48:04	MSN	diesis@hotmail.com	Association
2008-06-18 08:49:46	HTTPLOG	diesis@hotmail.com	
2008-06-18 08:49:46	HTTPPAGE	diesis@hotmail.com	
2008-06-18 08:49:47	HTTPLOG	diesis@hotmail.com	
2008-06-18 08:49:56	HTTPLOG	diesis@hotmail.com	
2008-06-18 08:49:56	HTTPLOG	diesis@hotmail.com	
2008-06-18 08:49:56	HTTPLOG	diesis@hotmail.com	
2008-06-18 08:49:56	HTTPPAGE	diesis@hotmail.com	
2008-06-18 08:49:56	HTTPPAGE	diesis@hotmail.com	
2008-06-18 08:49:56	HTTPPAGE	diesis@hotmail.com	
2008-06-18 08:49:57	HTTPLOG	diesis@hotmail.com	
2008-06-18 08:49:57	HTTPLOG	diesis@hotmail.com	
2008-06-18 08:49:57	HTTPPAGE	diesis@hotmail.com	
2008-06-18 08:50:01	HTTPLOG	diesis@hotmail.com	

⏮ ⏪ 1 2 3 4 5 6 7 8 9 ⏩ ⏭ Total 1,269 Total Page 85 Current Page 1

Related Account

N/A

Total 0 Total Page 0 Current Page 1

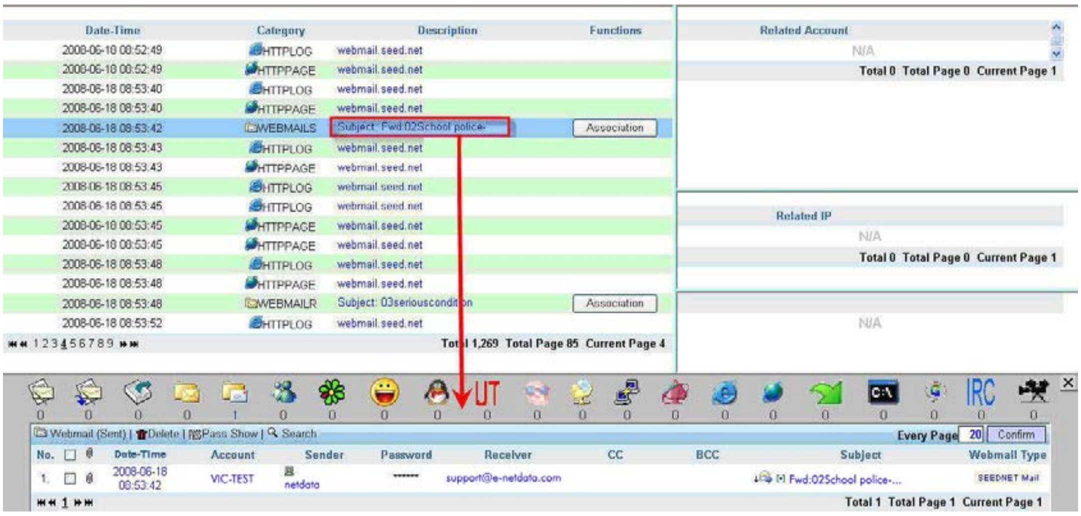
Related IP

N/A

Total 0 Total Page 0 Current Page 1

N/A

You may click on the description Listed to search for the particular record and content information as shown in diagram below.



Date-Time	Category	Description	Functions
2008-06-18 08:52:49	HTTPLOG	webmail.seed.net	
2008-06-18 08:52:49	HTTPPAGE	webmail.seed.net	
2008-06-18 08:53:40	HTTPLOG	webmail.seed.net	
2008-06-18 08:53:40	HTTPPAGE	webmail.seed.net	
2008-06-18 08:53:42	WEBMAILS	Subject: Fwd:02School police-	Association
2008-06-18 08:53:43	HTTPLOG	webmail.seed.net	
2008-06-18 08:53:43	HTTPPAGE	webmail.seed.net	
2008-06-18 08:53:45	HTTPLOG	webmail.seed.net	
2008-06-18 08:53:45	HTTPLOG	webmail.seed.net	
2008-06-18 08:53:45	HTTPPAGE	webmail.seed.net	
2008-06-18 08:53:45	HTTPPAGE	webmail.seed.net	
2008-06-18 08:53:48	HTTPLOG	webmail.seed.net	
2008-06-18 08:53:48	HTTPPAGE	webmail.seed.net	
2008-06-18 08:53:48	WEBMAILR	Subject: 03seriouscondition	Association
2008-06-18 08:53:52	HTTPLOG	webmail.seed.net	

⏮ ⏪ 1 2 3 4 5 6 7 8 9 ⏩ ⏭ Total 1,269 Total Page 85 Current Page 4

Related Account
N/A
Total 0 Total Page 0 Current Page 1

Related IP
N/A
Total 0 Total Page 0 Current Page 1

N/A

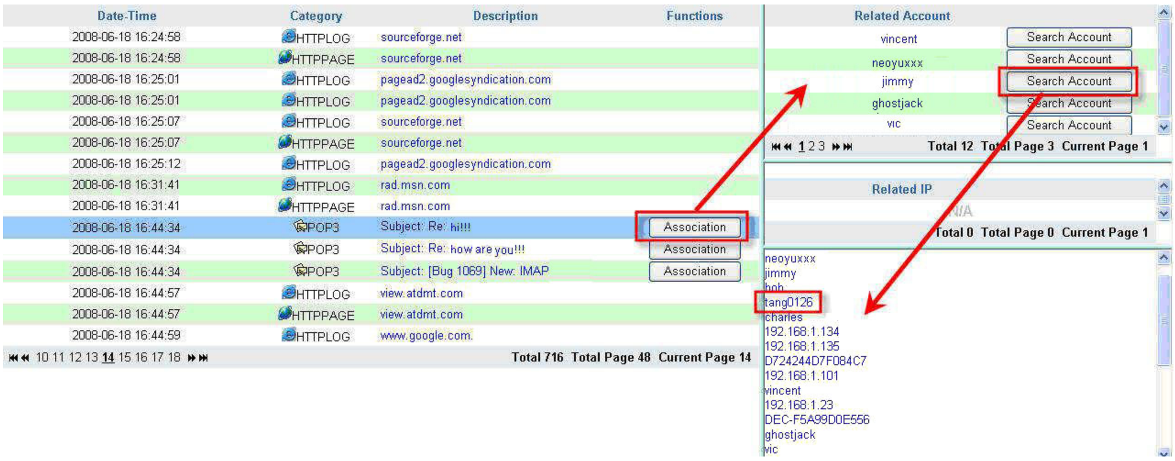
Webmail (Sent) | Delete | Pass Show | Search Every Page 20 Confirm

No.	□		Date-Time	Account	Sender	Password	Receiver	CC	BCC	Subject	Webmail Type
1.	□		2008-06-18 08:53:42	VIC-TEST	netdata	******	support@e-netdata.com			Fwd:02School police-...	SEEDNET Mail

⏮ ⏪ 1 ⏩ ⏭ Total 1 Total Page 1 Current Page 1

Searching for Association or Relationship

By clicking on the [Association] at the Function column of the Listed information, you may search for account that is related to this interaction (chat/email etc.). The account related will be Listed. You may also click on the [Search Account] to List down the account that is related this account.



Date-Time	Category	Description	Functions
2008-06-18 16:24:58	HTTPLOG	sourceforge.net	
2008-06-18 16:24:58	HTTPPAGE	sourceforge.net	
2008-06-18 16:25:01	HTTPLOG	pagead2.googlesyndication.com	
2008-06-18 16:25:01	HTTPLOG	pagead2.googlesyndication.com	
2008-06-18 16:25:07	HTTPLOG	sourceforge.net	
2008-06-18 16:25:07	HTTPPAGE	sourceforge.net	
2008-06-18 16:25:12	HTTPLOG	pagead2.googlesyndication.com	
2008-06-18 16:31:41	HTTPLOG	rad.msn.com	
2008-06-18 16:31:41	HTTPPAGE	rad.msn.com	
2008-06-18 16:44:34	POP3	Subject: Re: hi!!!	Association
2008-06-18 16:44:34	POP3	Subject: Re: how are you!!!	Association
2008-06-18 16:44:34	POP3	Subject: [Bug 1069] New: IMAP	Association
2008-06-18 16:44:57	HTTPLOG	view.atdmt.com	
2008-06-18 16:44:57	HTTPPAGE	view.atdmt.com	
2008-06-18 16:44:59	HTTPLOG	www.google.com.	

⏮ ⏪ 10 11 12 13 14 15 16 17 18 ⏩ ⏭ Total 716 Total Page 48 Current Page 14

Related Account	
vincent	Search Account
neoyuxxx	Search Account
jimmy	Search Account
ghostjack	Search Account
vic	Search Account

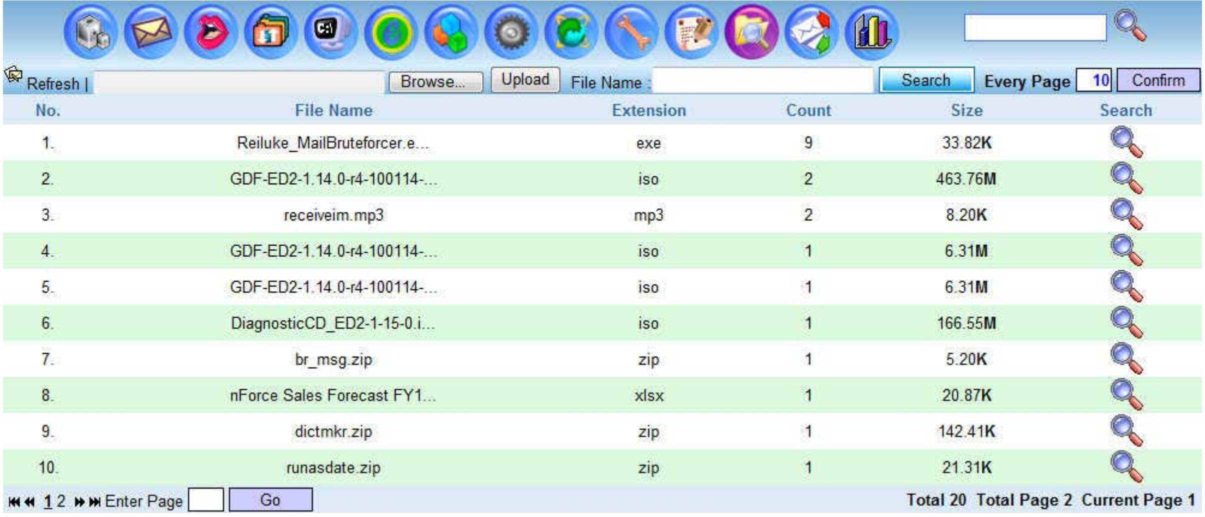
⏮ ⏪ 1 2 3 ⏩ ⏭ Total 12 Total Page 3 Current Page 1

Related IP
N/A
Total 0 Total Page 0 Current Page 1

neoyuxxx
jimmy
bob
tang0126
charles
192.168.1.134
192.168.1.135
D724244D7F084C7
192.168.1.101
vincent
192.168.1.23
DEC-F5A99D0E556
ghostjack
vic

Captured File List

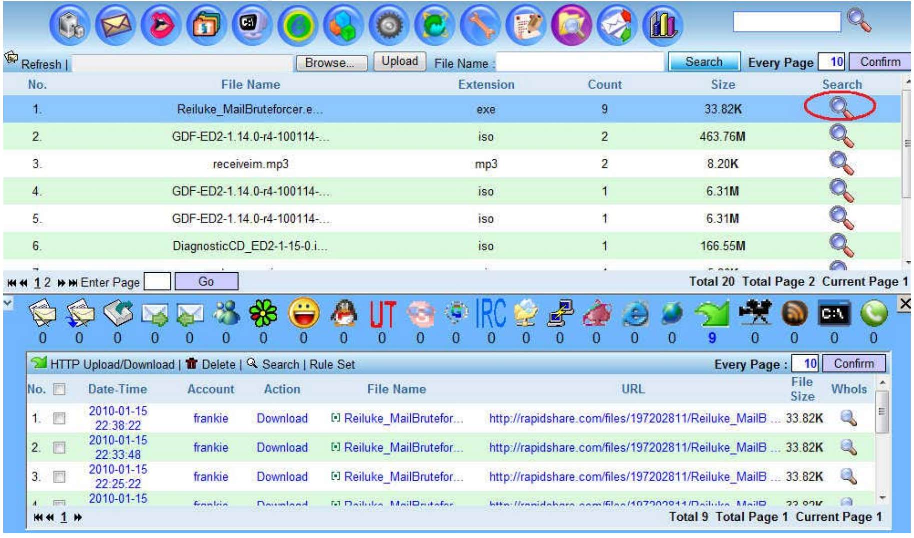
This section will List out all the files that have been reconstructed by ICI system with information such as file name, file extension, count (number of time this file has been appeared in the captured record) and file size. It also allows the Administrator to search for the file using the search function.



No.	File Name	Extension	Count	Size	Search
1.	Reiluke_MailBruteforcer.e...	exe	9	33.82K	🔍
2.	GDF-ED2-1.14.0-r4-100114-...	iso	2	463.76M	🔍
3.	receiveim.mp3	mp3	2	8.20K	🔍
4.	GDF-ED2-1.14.0-r4-100114-...	iso	1	6.31M	🔍
5.	GDF-ED2-1.14.0-r4-100114-...	iso	1	6.31M	🔍
6.	DiagnosticCD_ED2-1-15-0.i...	iso	1	166.55M	🔍
7.	br_msg.zip	zip	1	5.20K	🔍
8.	nForce Sales Forecast FY1...	xlsx	1	20.87K	🔍
9.	dictmkr.zip	zip	1	142.41K	🔍
10.	runasdate.zip	zip	1	21.31K	🔍

⏮ ⏪ 1 2 ⏩ ⏭ Enter Page Go Total 20 Total Page 2 Current Page 1

Search for the Captured File



No.	File Name	Extension	Count	Size	Search
1.	Reiluke_MailBruteforcer.e...	exe	9	33.82K	🔍
2.	GDF-ED2-1.14.0-r4-100114-...	iso	2	463.76M	🔍
3.	receiveim.mp3	mp3	2	8.20K	🔍
4.	GDF-ED2-1.14.0-r4-100114-...	iso	1	6.31M	🔍
5.	GDF-ED2-1.14.0-r4-100114-...	iso	1	6.31M	🔍
6.	DiagnosticCD_ED2-1-15-0.i...	iso	1	166.55M	🔍

⏮ ⏪ 1 2 ⏩ ⏭ Enter Page Go Total 20 Total Page 2 Current Page 1

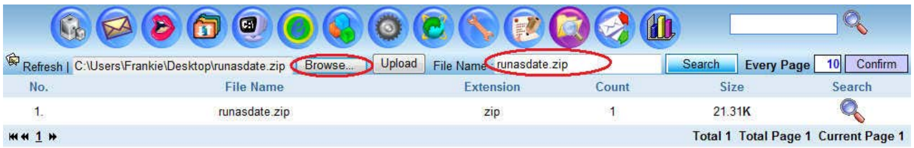
HTTP Upload/Download | Delete | Search | Rule Set Every Page : 10 Confirm

No.	□	Date-Time	Account	Action	File Name	URL	File Size	WhoIs
1.	□	2010-01-15 22:38:22	frankie	Download	Reiluke_MailBrutefor...	http://rapidshare.com/files/197202811/Reiluke_MailB ...	33.82K	🔍
2.	□	2010-01-15 22:33:48	frankie	Download	Reiluke_MailBrutefor...	http://rapidshare.com/files/197202811/Reiluke_MailB ...	33.82K	🔍
3.	□	2010-01-15 22:25:22	frankie	Download	Reiluke_MailBrutefor...	http://rapidshare.com/files/197202811/Reiluke_MailB ...	33.82K	🔍

⏮ ⏪ 1 ⏩ Total 9 Total Page 1 Current Page 1

Search for a file (with the similar content)

Administrator can also upload a file and try to find whether this file is found within the captured file List. In this case, the Administrator can know whether such file has been send out by anyone in the organization even the file name has been changed by the user.



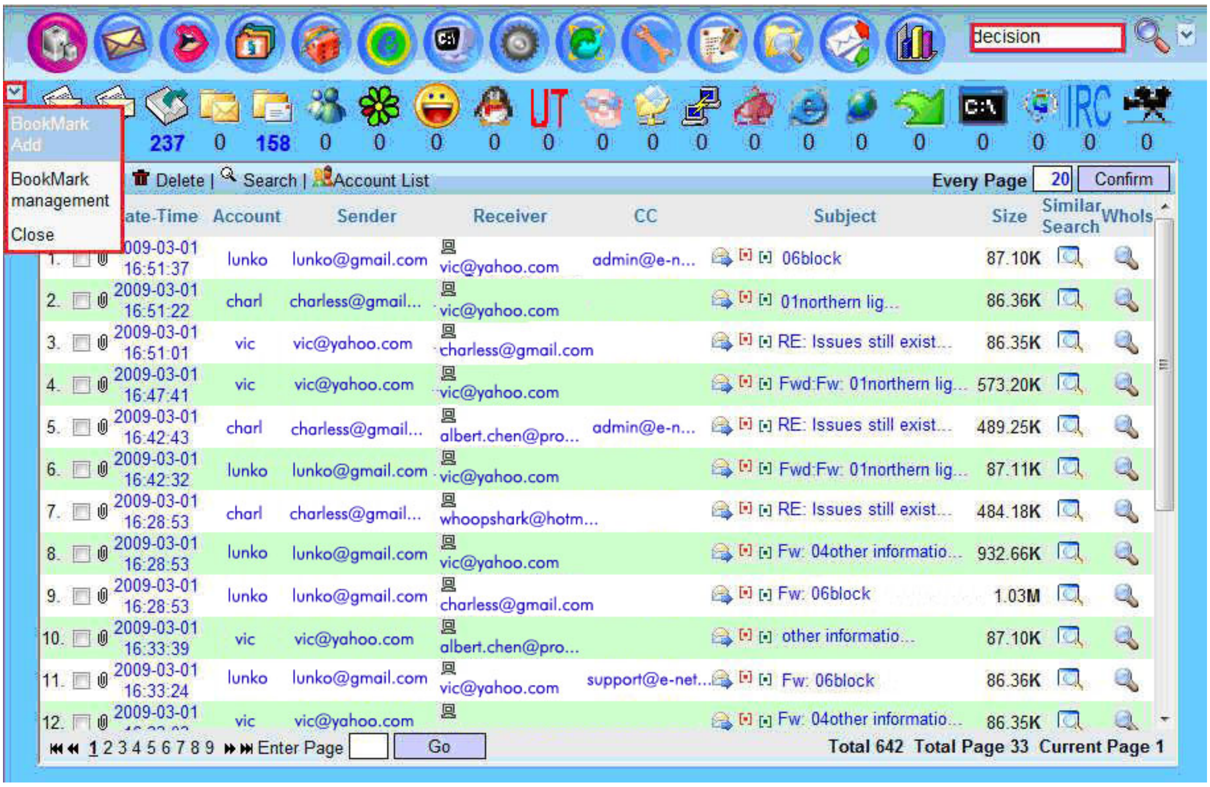
No.	File Name	Extension	Count	Size	Search
1.	runasdate.zip	zip	1	21.31K	🔍

⏮ ⏪ 1 ⏩ Total 1 Total Page 1 Current Page 1

Bookmark

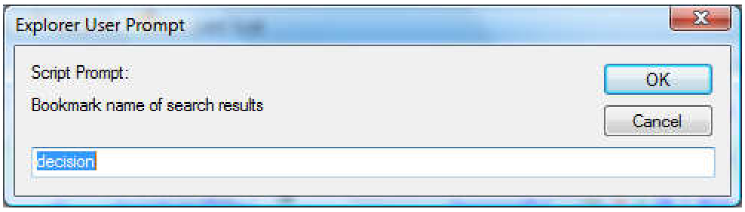
This function allows the Administrator to make a bookmark or record whenever he searches with the Free Text Search function. This will allow him to view back all the items that he has searched before and with the original search result.

Whenever the Administrator does a Free Text Search, he can bookmark it by clicking the icon on the left hand corner of the List of result. Select [Bookmark Add] to add the record into bookmark. A Window will pop up for you to name the bookmark record.



			ate-Time	Account	Sender	Receiver	CC	Subject	Size	Similar Search	WhoIs
1.	□		009-03-01 16:51:37	lunko	lunko@gmail.com	vic@yahoo.com	admin@e-n...	06block	87.10K		
2.	□		2009-03-01 16:51:22	charl	charless@gmail...	vic@yahoo.com		01northern lig...	86.36K		
3.	□		2009-03-01 16:51:01	vic	vic@yahoo.com	charless@gmail.com		RE: Issues still exist...	86.35K		
4.	□		2009-03-01 16:47:41	vic	vic@yahoo.com	vic@yahoo.com		Fwd:Fw: 01northern lig...	573.20K		
5.	□		2009-03-01 16:42:43	charl	charless@gmail...	albert.chen@pro...	admin@e-n...	RE: Issues still exist...	489.25K		
6.	□		2009-03-01 16:42:32	lunko	lunko@gmail.com	vic@yahoo.com		Fwd:Fw: 01northern lig...	87.11K		
7.	□		2009-03-01 16:28:53	charl	charless@gmail...	whoopshark@hotm...		RE: Issues still exist...	484.18K		
8.	□		2009-03-01 16:28:53	lunko	lunko@gmail.com	vic@yahoo.com		Fw: 04other informatio...	932.66K		
9.	□		2009-03-01 16:28:53	lunko	lunko@gmail.com	charless@gmail.com		Fw: 06block	1.03M		
10.	□		2009-03-01 16:33:39	vic	vic@yahoo.com	albert.chen@pro...		other informatio...	87.10K		
11.	□		2009-03-01 16:33:24	lunko	lunko@gmail.com	vic@yahoo.com	support@e-net...	Fw: 06block	86.36K		
12.	□		2009-03-01	vic	vic@yahoo.com			Fw: 04other informatio...	86.35K		

Total 642 Total Page 33 Current Page 1



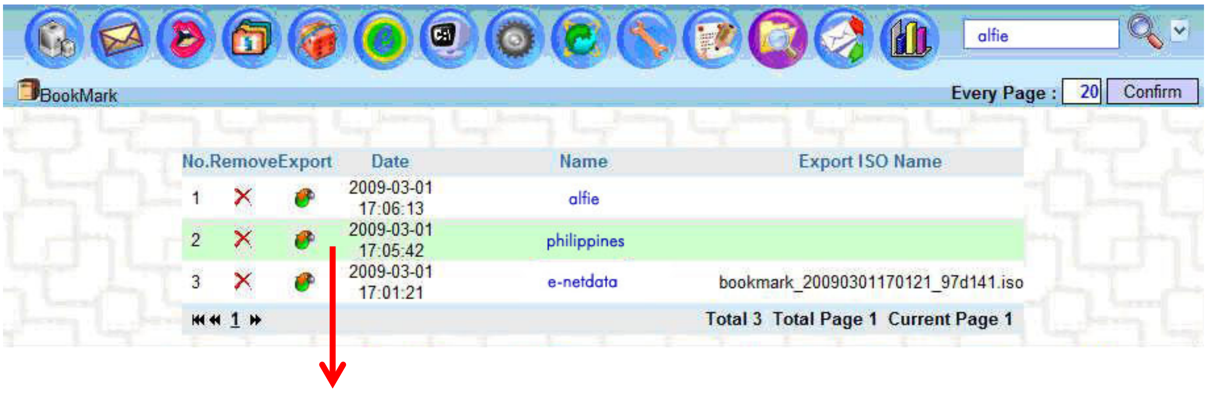
Script Prompt:

Bookmark name of search results

decision

Bookmark Management

The Administrator can delete the bookmark as well as export the bookmark (in ISO format).



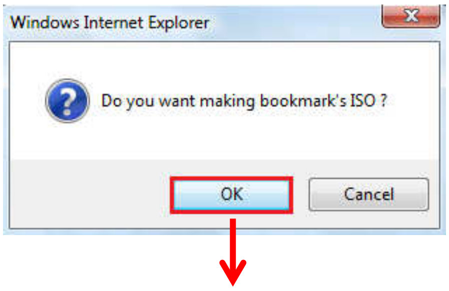
alfie

BookMark

Every Page : 20 Confirm

No.	Remove	Export	Date	Name	Export ISO Name
1	✗	●	2009-03-01 17:06:13	alfie	
2	✗	●	2009-03-01 17:05:42	philippines	
3	✗	●	2009-03-01 17:01:21	e-netdata	bookmark_20090301170121_97d141.iso

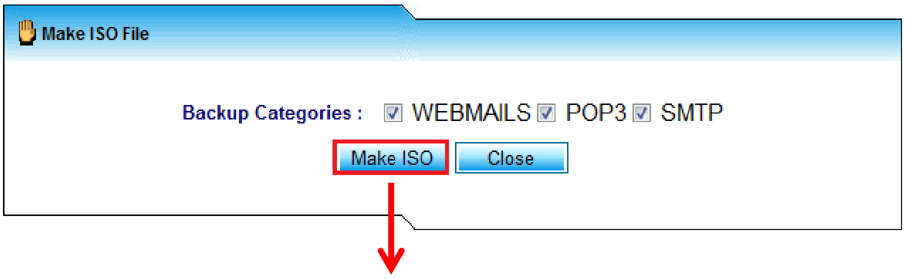
⏮ ⏪ 1 ⏩ Total 3 Total Page 1 Current Page 1



Windows Internet Explorer

Do you want making bookmark's ISO ?

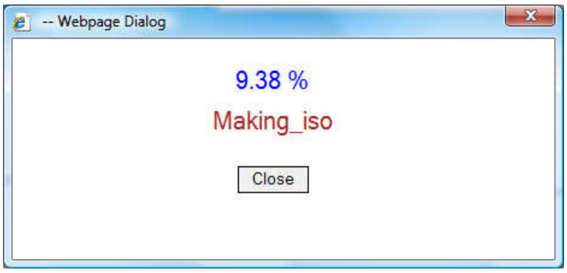
OK Cancel



Make ISO File

Backup Categories : ☑ WEBMAILS ☑ POP3 ☑ SMTP

Make ISO Close



-- Webpage Dialog

9.38 %

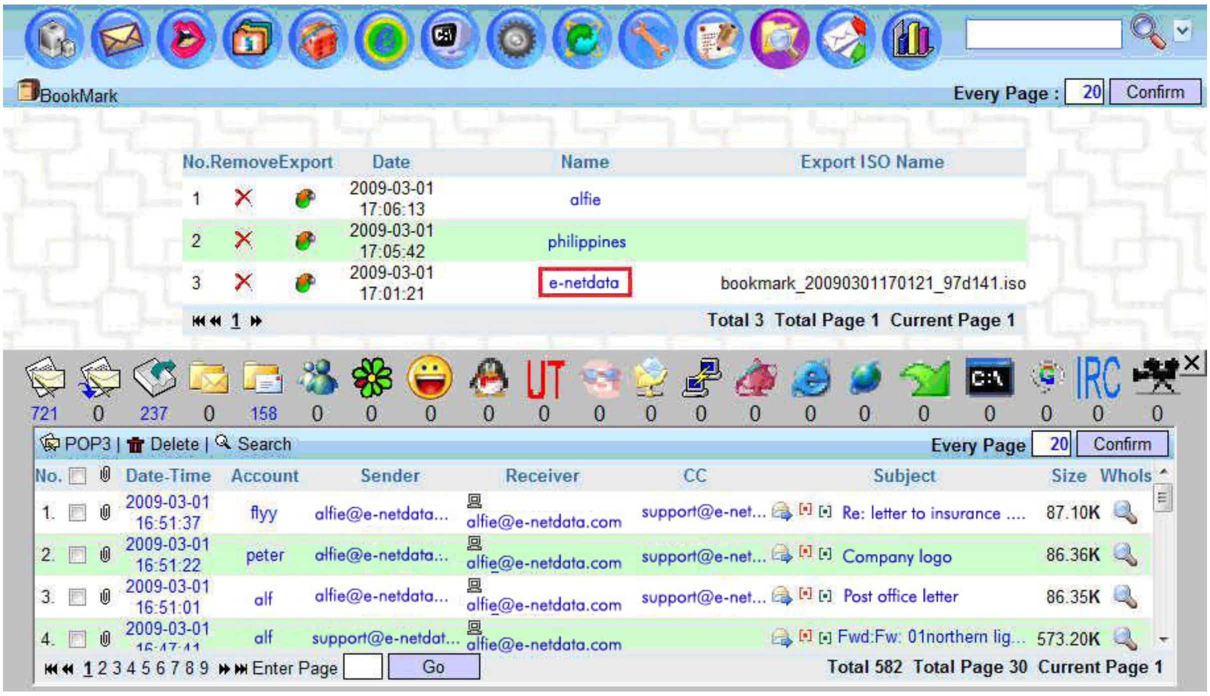
Making_iso

Close

The Administrator can use FTP client to access and download the ISO file from the system. The Administrator can login to the system by using FTP client with the Console/FTP username and password with port 21 or port 22.

Search for Bookmark Item

The Administrator can search for the bookmark item. This will show the previously searched and bookmarked record.



Every Page : 20 Confirm

No.	Remove	Export	Date	Name	Export ISO Name
1	✕		2009-03-01 17:06:13	alfie	
2	✕		2009-03-01 17:05:42	philippines	
3	✕		2009-03-01 17:01:21	e-netdata	bookmark_20090301170121_97d141.iso

⏮ ⏪ 1 ⏩ Total 3 Total Page 1 Current Page 1

Every Page 20 Confirm

No.	□		Date-Time	Account	Sender	Receiver	CC	Subject	Size	WhoIs
1.	□		2009-03-01 16:51:37	flyy	alfie@e-netdata...	alfie@e-netdata.com	support@e-net...	Re: letter to insurance	87.10K	
2.	□		2009-03-01 16:51:22	peter	alfie@e-netdata.:.	alfie@e-netdata.com	support@e-net...	Company logo	86.36K	
3.	□		2009-03-01 16:51:01	alf	alfie@e-netdata...	alfie@e-netdata.com	support@e-net...	Post office letter	86.35K	
4.	□		2009-03-01 16:47:41	alf	support@e-netdat...	alfie@e-netdata.com		Fwd:Fw: 01northern lig...	573.20K	

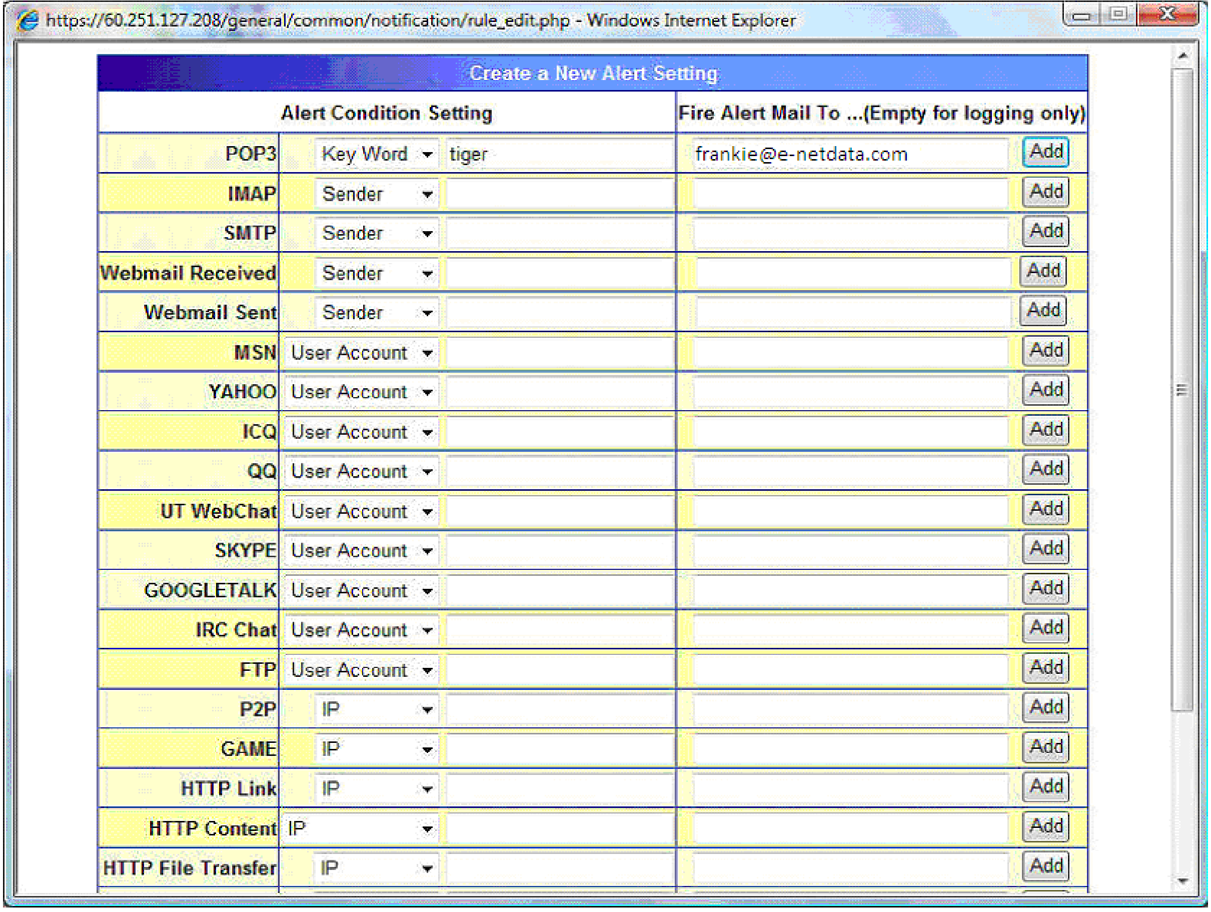
⏮ ⏪ 1 2 3 4 5 6 7 8 9 ⏩ ⏭ Enter Page Go Total 582 Total Page 30 Current Page 1

Send Mail Service

Administrator can be alerted or notified by Email (with content) if the alert condition met the parameter set. In Alert with content, Email (POP3, SMTP, IMAP and Webmail) and Chat (MSN, YAHOO, ICQ, QQ, AOL) content can be sent to the Administrator through Email if the pre-set parameters (sender account, receiver account, IP and key words) met or triggered. For example, administrator can forward all emails (POP3, SMTP, IMAP or Webmail) from account abc@xyz.com to himself/herself at admin@level1.com

Alert with Content

Administrator can set up the alert parameters based on the different service categories. Alert parameters such as sender account, receiver account and key word can be configured in each service category. The alert can be send to the specific email account(s) defined by the Administrator.

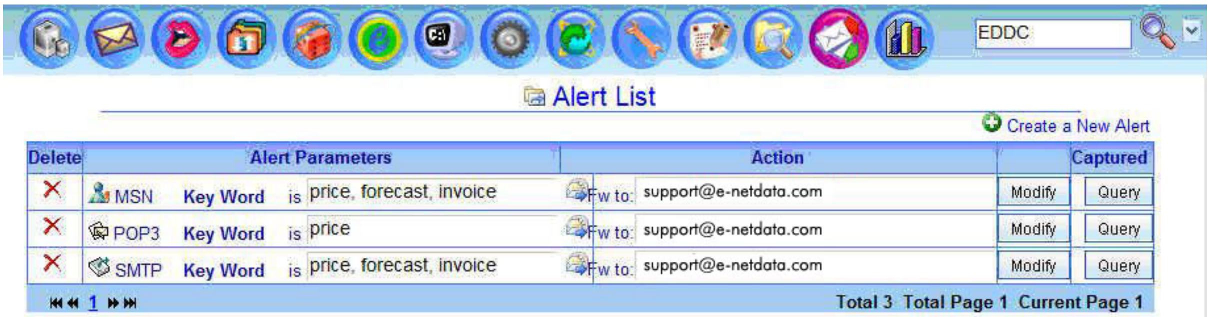


https://60.251.127.208/general/common/notification/rule_edit.php - Windows Internet Explorer

Create a New Alert Setting

Alert Condition Setting			Fire Alert Mail To ...(Empty for logging only)	
POP3	Key Word	tiger	frankie@e-netdata.com	Add
IMAP	Sender			Add
SMTP	Sender			Add
Webmail Received	Sender			Add
Webmail Sent	Sender			Add
MSN	User Account			Add
YAHOO	User Account			Add
ICQ	User Account			Add
QQ	User Account			Add
UT WebChat	User Account			Add
SKYPE	User Account			Add
GOOGLETALK	User Account			Add
IRC Chat	User Account			Add
FTP	User Account			Add
P2P	IP			Add
GAME	IP			Add
HTTP Link	IP			Add
HTTP Content	IP			Add
HTTP File Transfer	IP			Add

Administrator can check the alert List as well as modifying the alert rule through the alert List GUI. Besides, the Administrator can also query for the defined alert parameter through this GUI.



EDDC

Alert List

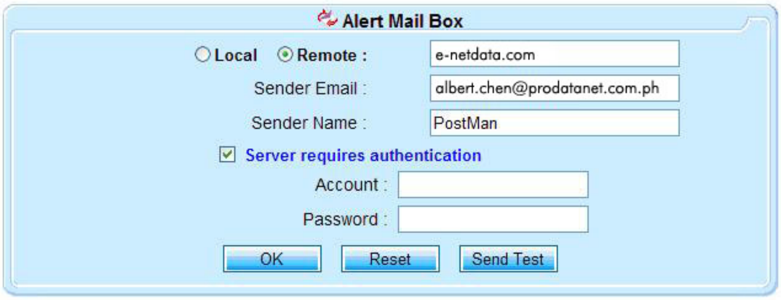
Create a New Alert

Delete	Alert Parameters				Action			Captured
✕	MSN	Key Word	is	price, forecast, invoice	Fw to:	support@e-netdata.com	Modify	Query
✕	POP3	Key Word	is	price	Fw to:	support@e-netdata.com	Modify	Query
✕	SMTP	Key Word	is	price, forecast, invoice	Fw to:	support@e-netdata.com	Modify	Query

⏮ ◀ 1 ▶ ⏭ Total 3 Total Page 1 Current Page 1

Alert Mail Box

Administrator needs to setup the Alert Mail Box so that all notification and alert Emails can be sent out by the system.



Alert Mail Box

○ Local ● Remote : e-netdata.com

Sender Email : albert.chen@prodatanet.com.ph

Sender Name : PostMan

☑ Server requires authentication

Account :

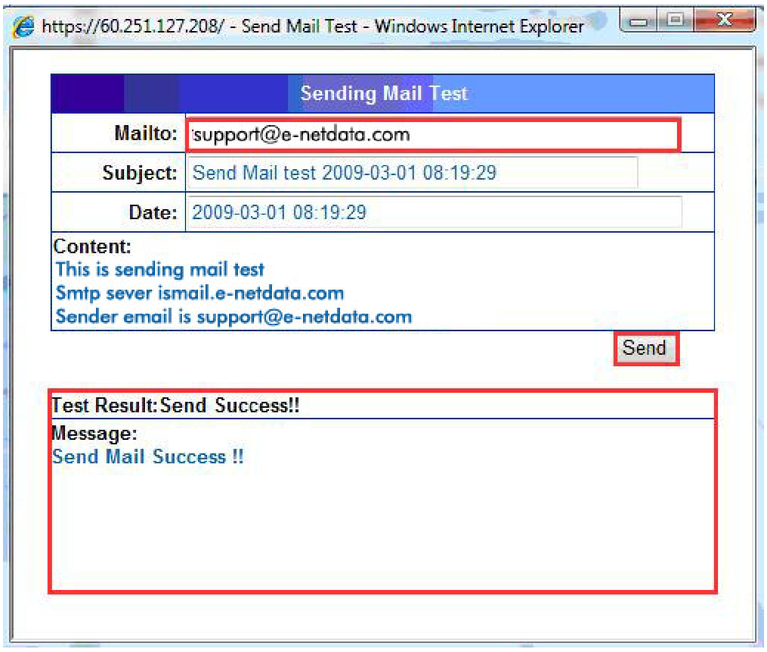
Password :

Features in this Alert Mail Box GUI:

1) Local/Remote: The SMTP domain name. Administrator ticks the local one if you have set up the mail server locally
2) Sender Email: Administrator provides one Email account for ED system for sending out the system Emails
3) Server requires authentication: Tick this option if the mail server used requires authentication
4) Account and Password: Provides the account name and its password here for authentication
5) The button [OK] is to submit the setting
6) The button [Reset] is to clear up the setting
7) The button [Send Test] is to test this function based on the given conditions

Testing of Mail Server Setup

The following GUI will pop up when Administrator click on the button [Send Test]. Fill in the information required to test the Mail Server setup.



https://60.251.127.208/ - Send Mail Test - Windows Internet Explorer

Sending Mail Test

Mailto: 'support@e-netdata.com

Subject: Send Mail test 2009-03-01 08:19:29

Date: 2009-03-01 08:19:29

Content:
This is sending mail test
Smtp sever ismail.e-netdata.com
Sender email is support@e-netdata.com

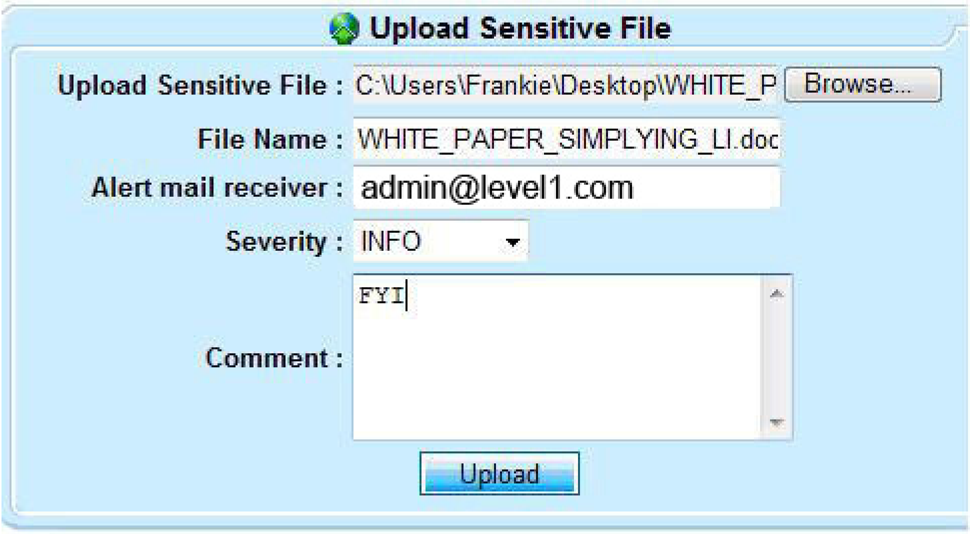
Test Result:Send Success!!

Message:
Send Mail Success !!

Send Mail Success means that the Email can been successfully sent out. Send Mail Failed means that the system failed with send out the Email. Therefore, please recheck your Email server and username/password.

Alert Sensitive File

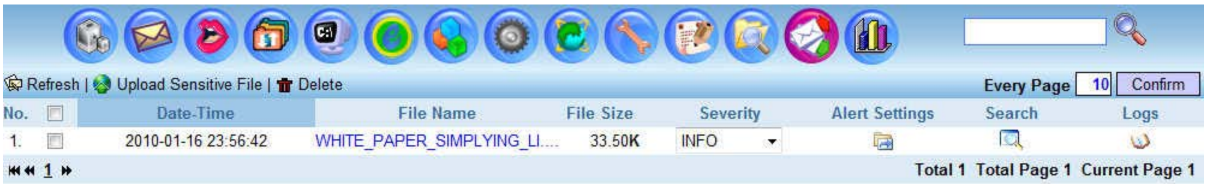
Administrator can upload certain files to the system. If these files are found in any of the Internet content communications, alert email can be sent to the Administrator.



Upload Sensitive File

Upload Sensitive File :	C:\Users\Frankie\Desktop\WHITE_P [Browse...]
File Name :	WHITE_PAPER_SIMPLYING_LI.doc
Alert mail receiver :	admin@level1.com
Severity :	INFO
Comment :	FYI

[Upload]



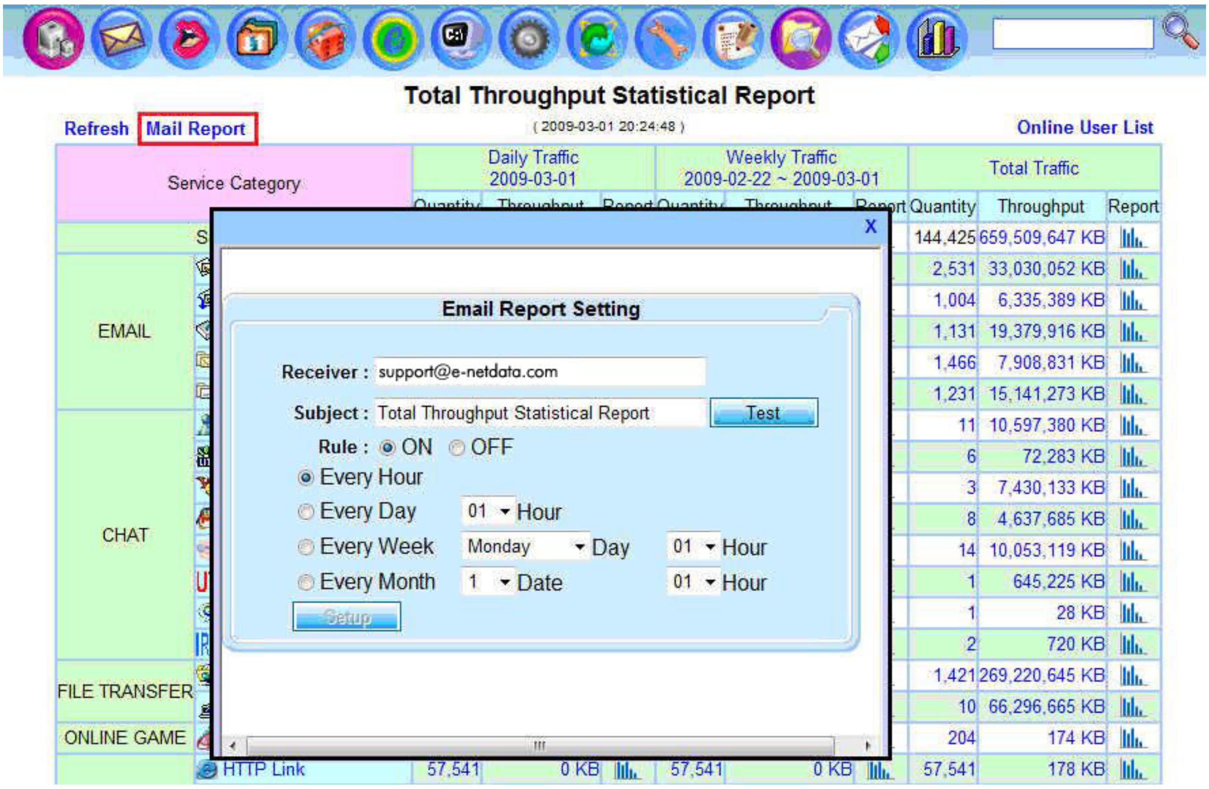
Refresh | Upload Sensitive File | Delete — Every Page 10 [Confirm]

No.	□	Date-Time	File Name	File Size	Severity	Alert Settings	Search	Logs
1.	□	2010-01-16 23:56:42	WHITE_PAPER_SIMPLYING_LI....	33.50K	INFO			

⏮ ◀ 1 ▶ Total 1 Total Page 1 Current Page 1

Report Management

This section will List out all the scheduled reports setup by the Administrator. The Administrator can delete this schedule report delivery setup.



Total Throughput Statistical Report

Refresh | Mail Report | (2009-03-01 20:24:48) | Online User List

Service Category		Daily Traffic 2009-03-01			Weekly Traffic 2009-02-22 ~ 2009-03-01			Total Traffic		
		Quantity	Throughput	Report	Quantity	Throughput	Report	Quantity	Throughput	Report
	S							144,425	659,509,647 KB	
EMAIL								2,531	33,030,052 KB	
								1,004	6,335,389 KB	
								1,131	19,379,916 KB	
								1,466	7,908,831 KB	
								1,231	15,141,273 KB	
CHAT								11	10,597,380 KB	
								6	72,283 KB	
								3	7,430,133 KB	
								8	4,637,685 KB	
								14	10,053,119 KB	
	U							1	645,225 KB	
								1	28 KB	
	IR							2	720 KB	
FILE TRANSFER								1,421	269,220,645 KB	
								10	66,296,665 KB	
ONLINE GAME								204	174 KB	
	HTTP Link	57,541	0 KB		57,541	0 KB		57,541	178 KB	

Email Report Setting

Receiver : support@e-netdata.com

Subject : Total Throughput Statistical Report [Test]

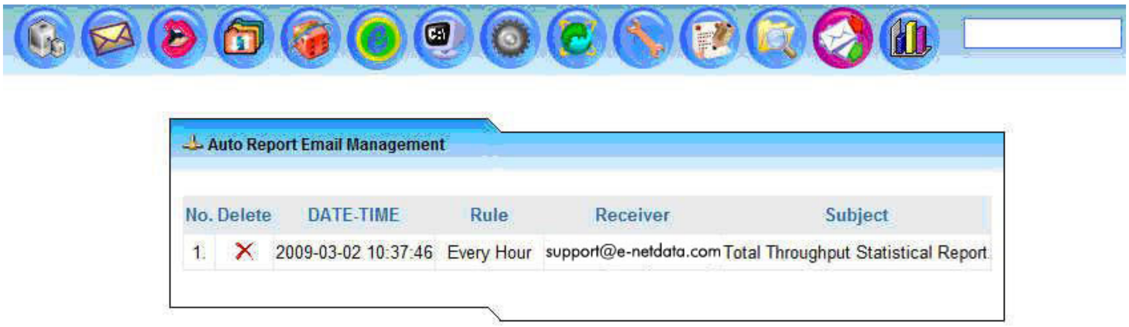
Rule : ● ON ○ OFF

● Every Hour

○ Every Day 01 Hour

○ Every Week Monday Day 01 Hour

○ Every Month 1 Date 01 Hour

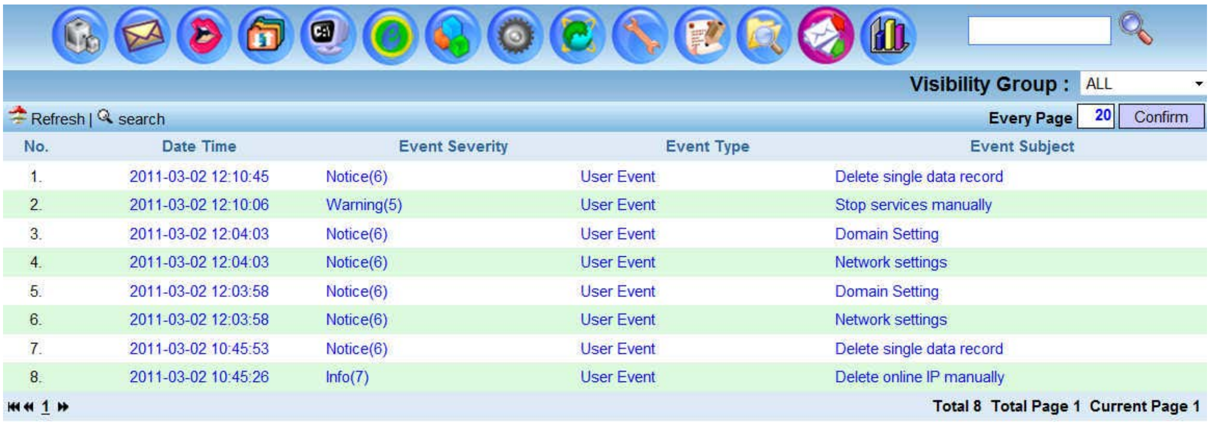


Auto Report Email Management

No.	Delete	DATE-TIME	Rule	Receiver	Subject
1.	✕	2009-03-02 10:37:46	Every Hour	support@e-netdata.com	Total Throughput Statistical Report

Event Management

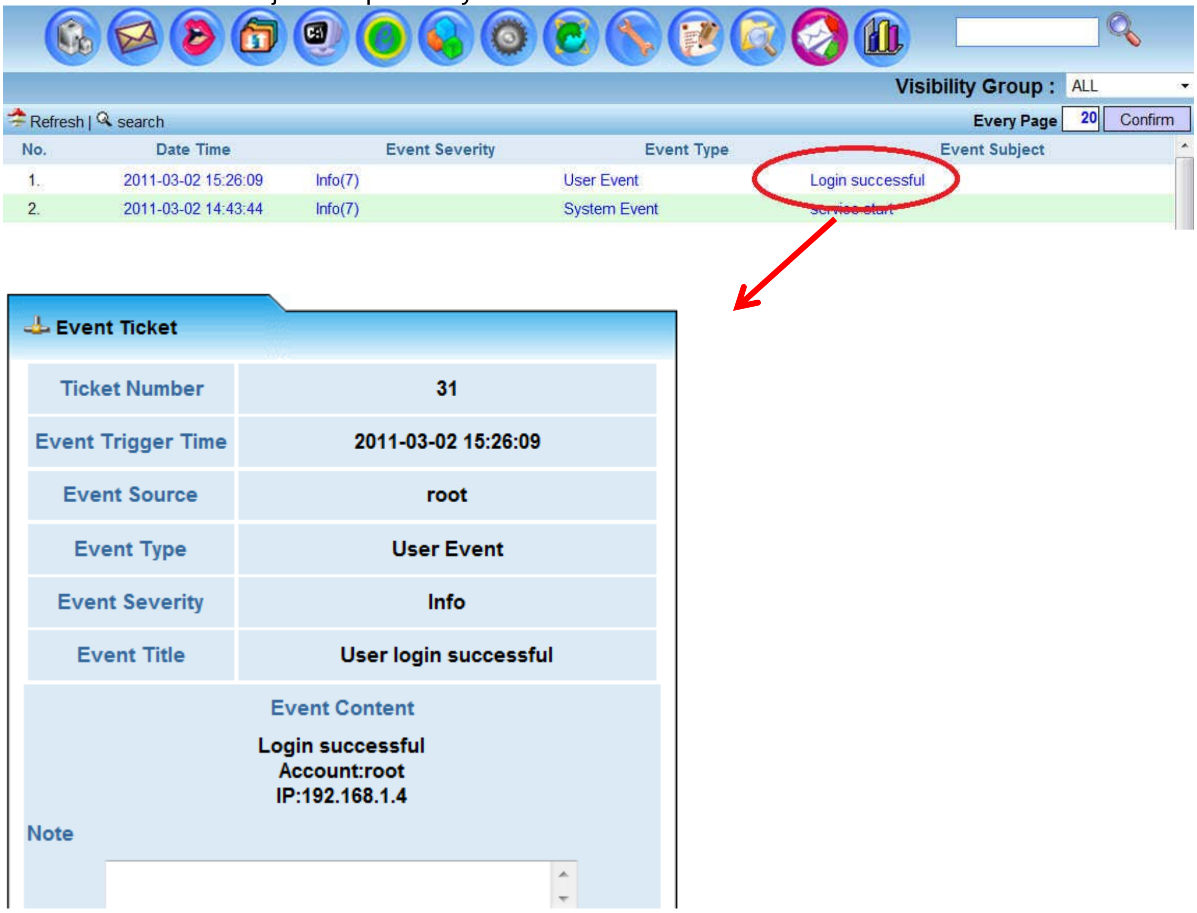
Event Management provides logging of users' action on ICI system such as delete of record, stop of services, change of network settings etc. It provides information of Date-Time event occurred, Event Severity (Warning-5, Notice-6 and Info-7), Event Type (System Event or User Even) and Event Subject.



No.	Date Time	Event Severity	Event Type	Event Subject
1.	2011-03-02 12:10:45	Notice(6)	User Event	Delete single data record
2.	2011-03-02 12:10:06	Warning(5)	User Event	Stop services manually
3.	2011-03-02 12:04:03	Notice(6)	User Event	Domain Setting
4.	2011-03-02 12:04:03	Notice(6)	User Event	Network settings
5.	2011-03-02 12:03:58	Notice(6)	User Event	Domain Setting
6.	2011-03-02 12:03:58	Notice(6)	User Event	Network settings
7.	2011-03-02 10:45:53	Notice(6)	User Event	Delete single data record
8.	2011-03-02 10:45:26	Info(7)	User Event	Delete online IP manually

Total 8 Total Page 1 Current Page 1

Click on the Event Subject will provide you details of the event.



No.	Date Time	Event Severity	Event Type	Event Subject
1.	2011-03-02 15:26:09	Info(7)	User Event	Login successful
2.	2011-03-02 14:43:44	Info(7)	System Event	Service start

Event Ticket

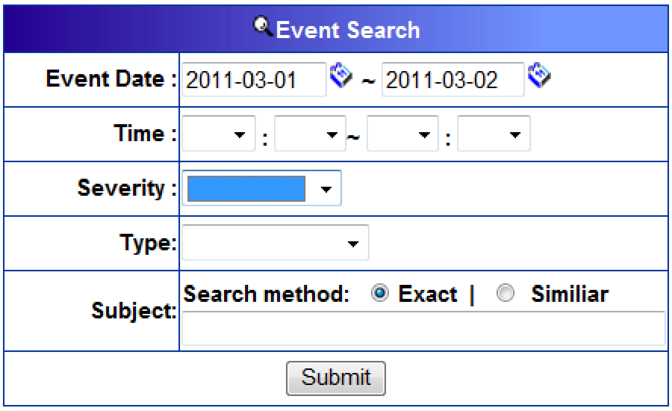
Ticket Number	31
Event Trigger Time	2011-03-02 15:26:09
Event Source	root
Event Type	User Event
Event Severity	Info
Event Title	User login successful

Event Content

Login successful
Account:root
IP:192.168.1.4

Note

Event Management Search function allow you to search for particular event according to Event occur Date, Time, Severity, Type of Event and Event Subject.



Event Search

Event Date : 2011-03-01 ~ 2011-03-02

Time : : ~ :

Severity :

Type:

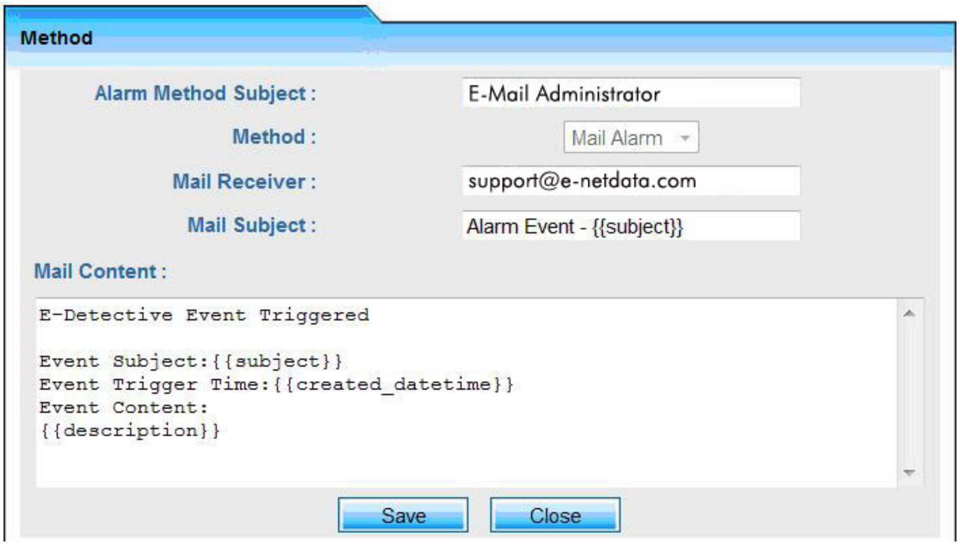
Subject: Search method: ● Exact | ○ Similiar

Note: Do ensure that you turn on Event Log service at System Settings – Services – System Services to enable this function.

Event Trigger Management

Event trigger management allows user to alert email to be sent to Administrator whenever the specified condition met.

Step 1: Setup Alarm Report Management
Click on [Alarm Report Management] and the following Windows will appear. Input the Alarm Method Subject, Mail Receiver, Mail Subject and Mail Content and Save. Then, go to Step 2.



Method

Alarm Method Subject : E-Mail Administrator

Method : Mail Alarm

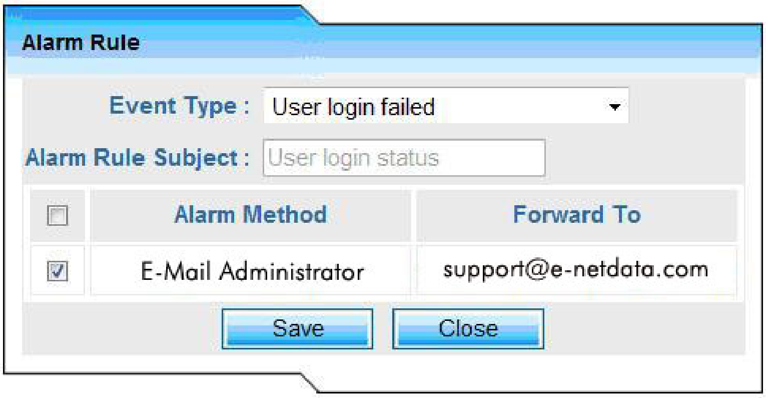
Mail Receiver : support@e-netdata.com

Mail Subject : Alarm Event - {{subject}}

Mail Content :

```
E-Detective Event Triggered

Event Subject:{{subject}}
Event Trigger Time:{{created_datetime}}
Event Content:
{{description}}
```

Step 2: Setup Create Alarm Rule
Click on [Create Alarm Rule] and the following Windows will appear. Select the Event Type that you want alert email to be sent and save it.

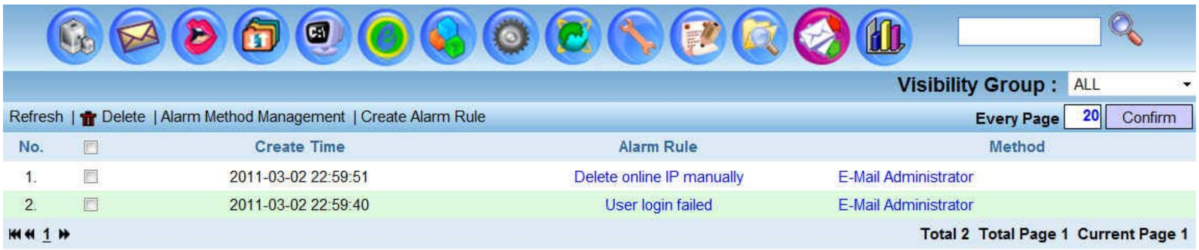


Alarm Rule

Event Type : User login failed

Alarm Rule Subject : User login status

□	Alarm Method	Forward To
☑	E-Mail Administrator	support@e-netdata.com



Visibility Group : ALL

Refresh | Delete | Alarm Method Management | Create Alarm Rule

Every Page 20

No.	□	Create Time	Alarm Rule	Method
1.	□	2011-03-02 22:59:51	Delete online IP manually	E-Mail Administrator
2.	□	2011-03-02 22:59:40	User login failed	E-Mail Administrator

1

Total 2 Total Page 1 Current Page 1

Diagram: Alarm Rules created.

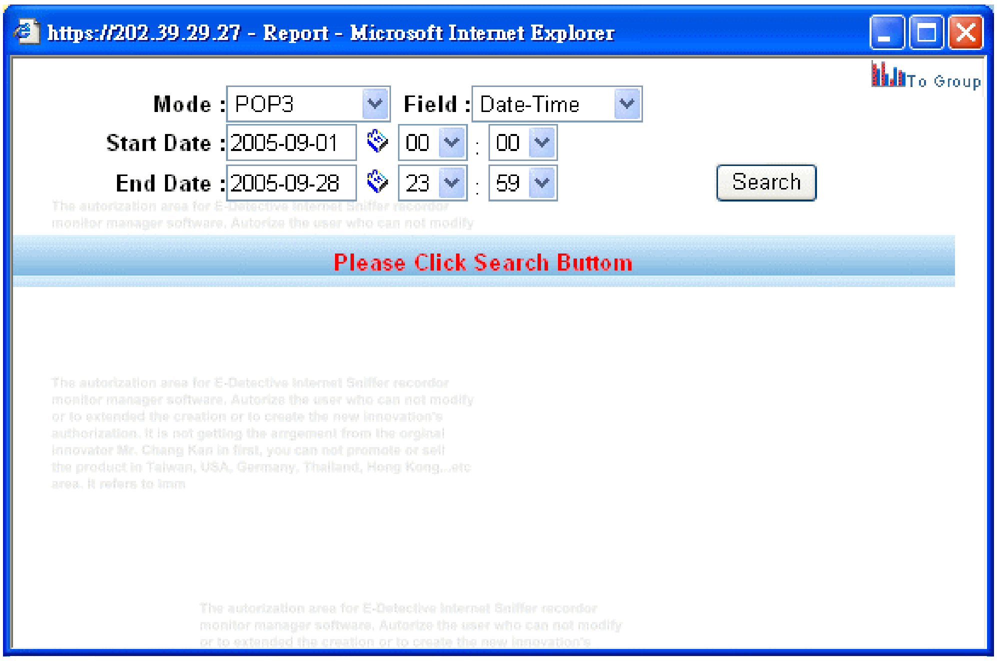
Statistical Reports

ICI system provides comprehensive statistical reporting function. It can generate different types of reports based on single application or protocol, group of users' different online activities as well as various statistical reports.

Conditional Reports (Single Report)

Step 1

Identify the period that the specific category (protocol) to be displayed in the report. Category: POP3, SMTP, FTP, P2P, MSN, ICQ, YAHOO, HTTP Link, HTTP Content, WEBMAIL-R, WEBMAIL-S, TELNET etc.



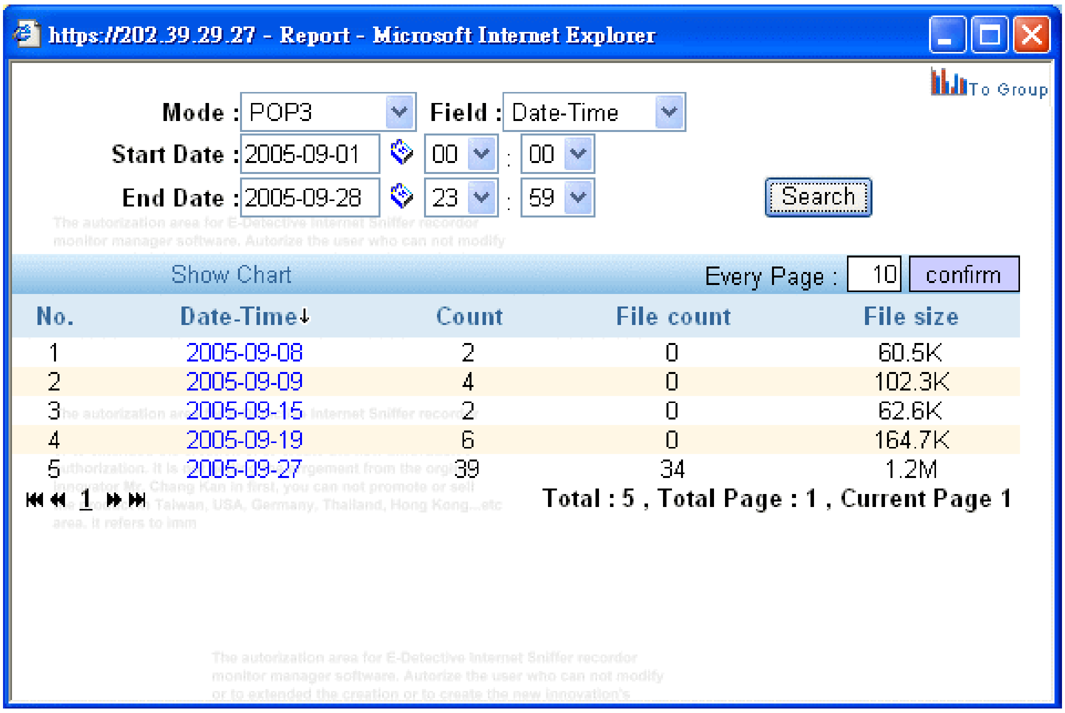
https://202.39.29.27 - Report - Microsoft Internet Explorer

Mode : POP3 Field : Date-Time

Start Date : 2005-09-01 00 : 00

End Date : 2005-09-28 23 : 59

Please Click Search Buttom



https://202.39.29.27 - Report - Microsoft Internet Explorer

Mode : POP3 Field : Date-Time

Start Date : 2005-09-01 00 : 00

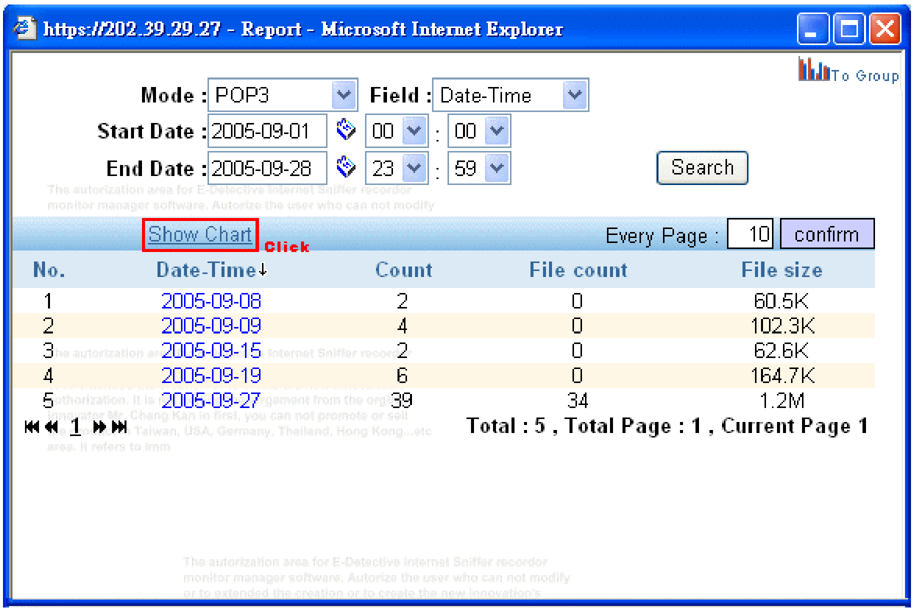
End Date : 2005-09-28 23 : 59

Every Page : 10 confirm

No.	Date-Time↓	Count	File count	File size
1	2005-09-08	2	0	60.5K
2	2005-09-09	4	0	102.3K
3	2005-09-15	2	0	62.6K
4	2005-09-19	6	0	164.7K
5	2005-09-27	39	34	1.2M

⏮ ◀◀ 1 ▶▶ ⏭ Total : 5 , Total Page : 1 , Current Page 1

Step 2
Click Show Chart.



https://202.39.29.27 - Report - Microsoft Internet Explorer

To Group

Mode : POP3 Field : Date-Time

Start Date : 2005-09-01 00 : 00

End Date : 2005-09-28 23 : 59 Search

Show Chart Click

Every Page : 10 confirm

No.	Date-Time↓	Count	File count	File size
1	2005-09-08	2	0	60.5K
2	2005-09-09	4	0	102.3K
3	2005-09-15	2	0	62.6K
4	2005-09-19	6	0	164.7K
5	2005-09-27	39	34	1.2M

⏮ ⏪ 1 ⏩ ⏭ Total : 5 , Total Page : 1 , Current Page 1

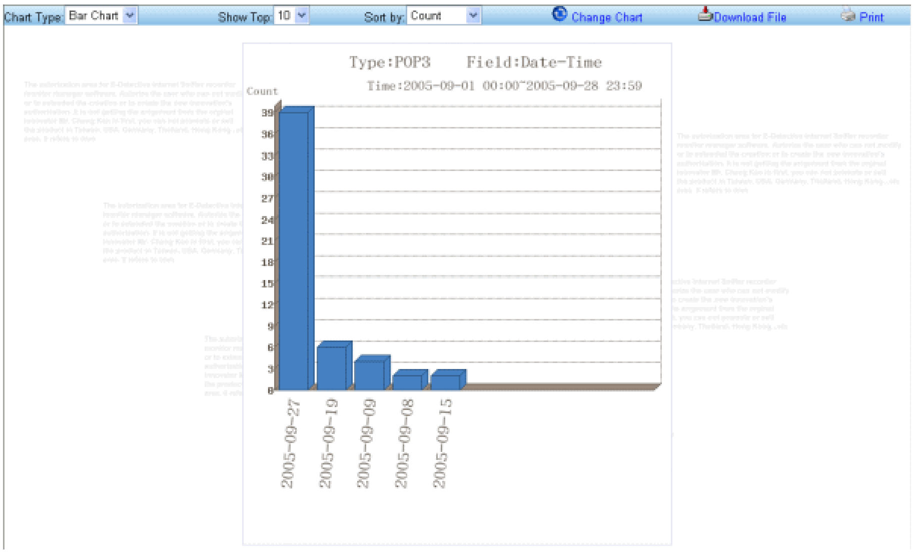


Chart Type: Bar Chart Show Top: 10 Sort by: Count

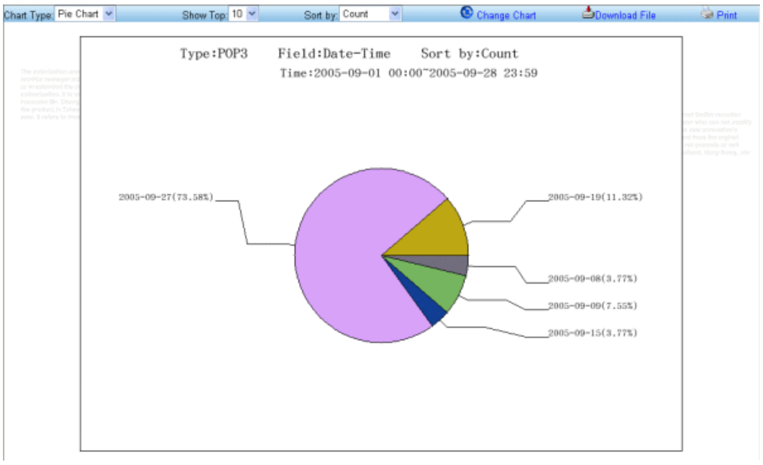


Chart Type: Pie Chart
Show Top: 10
Sort by: Count

Chart Type:

Bar Chart
Pie Chart

Show Top: Select to display the first 10, 20, 30 data row.

Sort by:

Count: total data.
File count: all included attached file data.
File size: all included attached file size.

Change Chart

Select Chart Type, Show Top, Sort by. Clip Change Chart then can display you the type you would like to display.

Download File

The report can be downloaded in chart figure (.png) format.

Print

The report can be printed.

Note：Because the charset of sender and receiver of POP3, SMTP, Web Mail, and the user handle and participant of YAHOO is not saved by Unicode. When showing the chart, you can choose the correct charset (unicode, big5, gb2312).

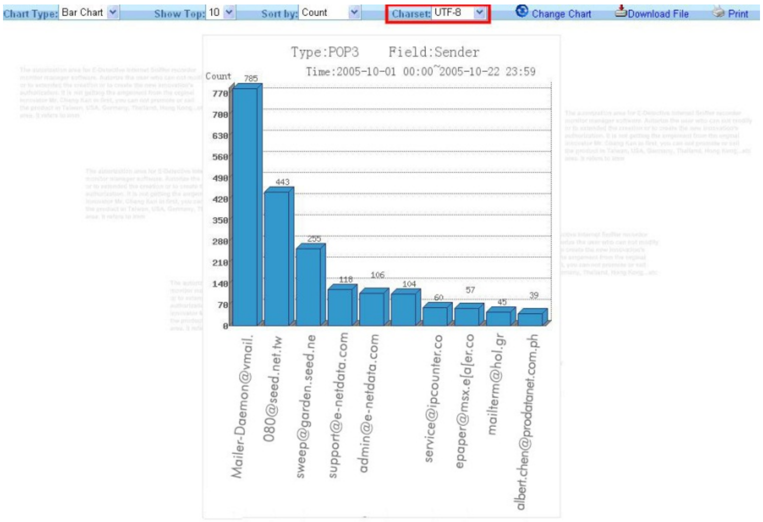
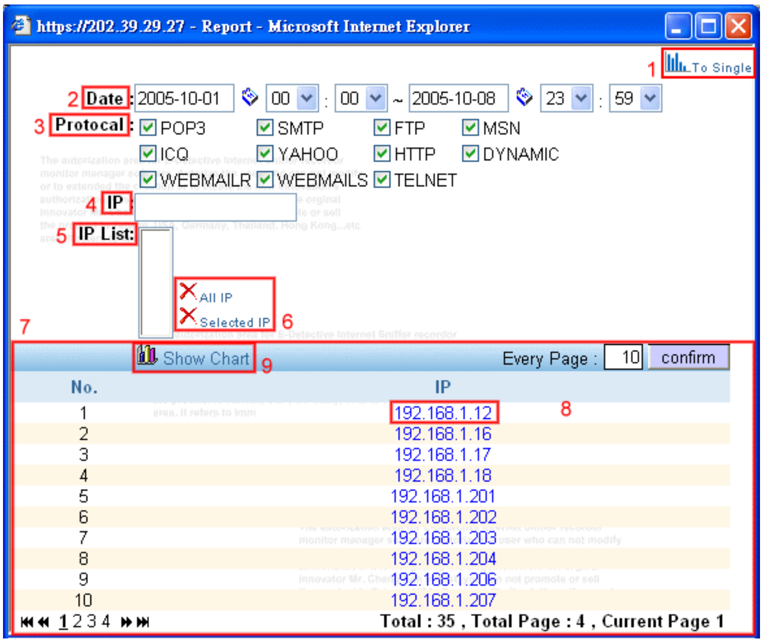


Chart Type: Bar Chart
Show Top: 10
Sort by: Count
Charset: UTF-8

Conditional Report (Group Report)



https://202.39.29.27 - Report - Microsoft Internet Explorer

1 To Single

2 Date : 2005-10-01 00 : 00 ~ 2005-10-08 23 : 59

3 Protocal : ☑ POP3 ☑ SMTP ☑ FTP ☑ MSN ☑ ICQ ☑ YAHOO ☑ HTTP ☑ DYNAMIC ☑ WEBMAILR ☑ WEBMAILS ☑ TELNET

4 IP :

5 IP List:

6 ✕ All IP ✕ Selected IP

7

9 Show Chart

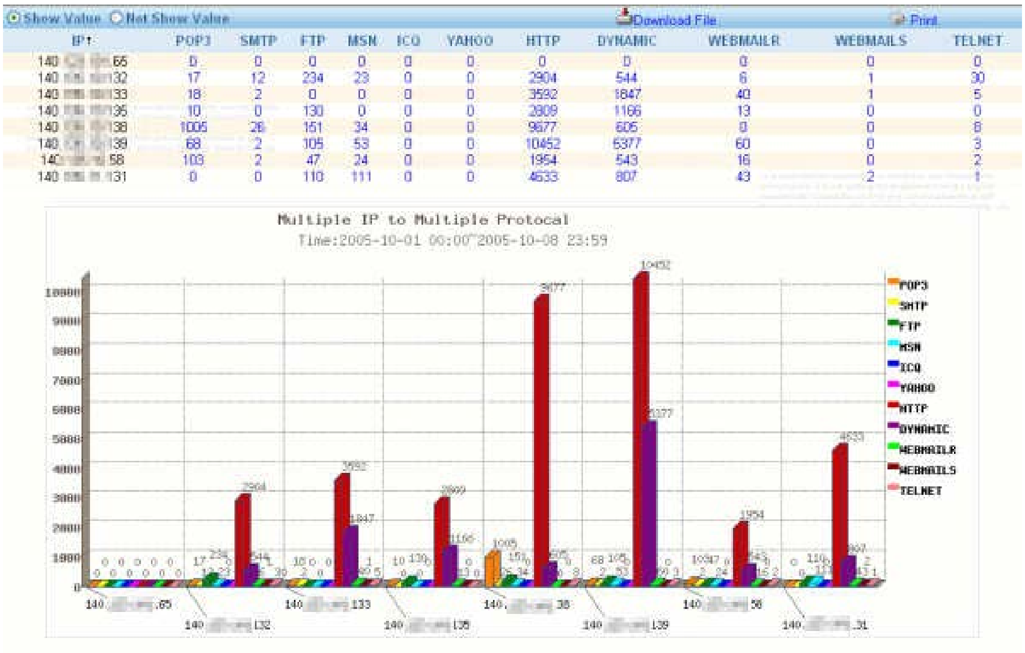
Every Page : 10 confirm

No.	IP
1	192.168.1.12
2	192.168.1.16
3	192.168.1.17
4	192.168.1.18
5	192.168.1.201
6	192.168.1.202
7	192.168.1.203
8	192.168.1.204
9	192.168.1.206
10	192.168.1.207

⏮ ◀ 1 2 3 4 ▶ ⏭ Total : 35 , Total Page : 4 , Current Page 1

After select the Group Report, it will display the Group Report List (see above diagram)

1) To Single: Select the icon to link to Single Report.
2) Date: Date and time setting.
3) Protocol/Category: Selection or Protocol/Category of different Internet applications such as POP3, SMTP, FTP, MSN etc.
4) IP: Key in IP address manually.
5) IP List: Administrator can select the IP addresses based on the List of IP displayed.
6) Delete All/Delete Selected: Administrator can delete all IPs or just the selected IPs.
7) The record IP List that have Listed in the present ICI system
8) By using the mouse to select any IP, it can be added the IP to the new IP List, the maximum can be selected 10 IP.
9) Show Chart: Display the chart report.

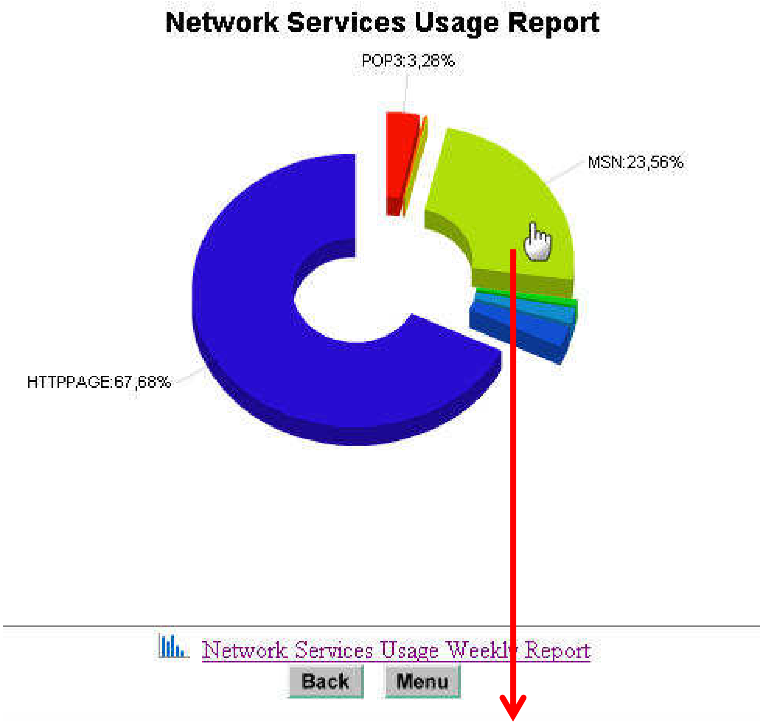


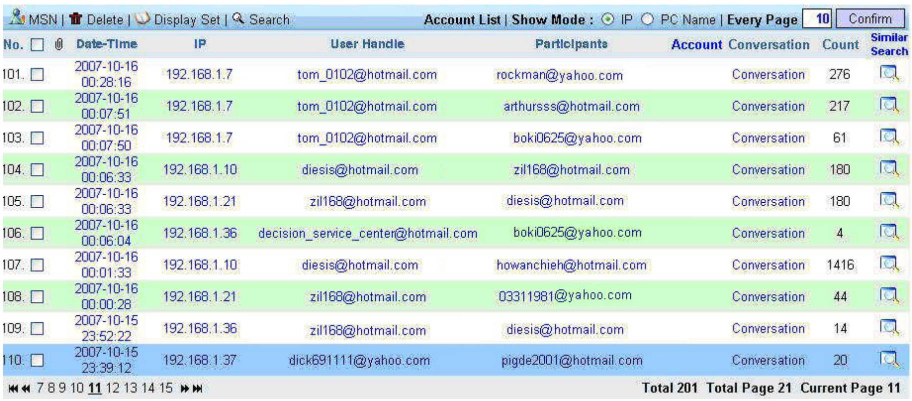
● Show Value ○ Not Show Value Download File Print

IP↑	POP3	SMTP	FTP	MSN	ICQ	YAHOO	HTTP	DYNAMIC	WEBMAILR	WEBMAILS	TELNET
140 [redacted] 65	0	0	0	0	0	0	0	0	0	0	0
140 [redacted] 132	17	12	234	23	0	0	2904	544	6	1	30
140 [redacted] 133	18	2	0	0	0	0	3592	1847	40	1	5
140 [redacted] 135	10	0	130	0	0	0	2809	1166	13	0	0
140 [redacted] 138	1005	26	151	34	0	0	9677	605	0	0	8
140 [redacted] 139	68	2	105	53	0	0	10452	6377	60	0	3
140 [redacted] 58	103	2	47	24	0	0	1954	543	16	0	2
140 [redacted] 131	0	0	110	111	0	0	4633	807	43	2	1

Network Services Usage Report

It shows the number and percentages of different services (protocols) usage on the network. By clicking on the service on the pie chart, it will link to List out all the related service as shown below.



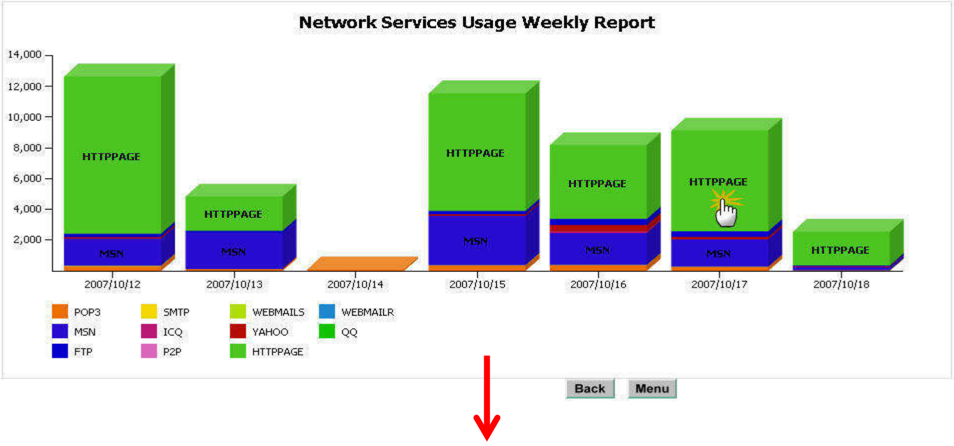

MSN | Delete | Display Set | Search
Account List | Show Mode : ● IP ○ PC Name | Every Page 10 Confirm

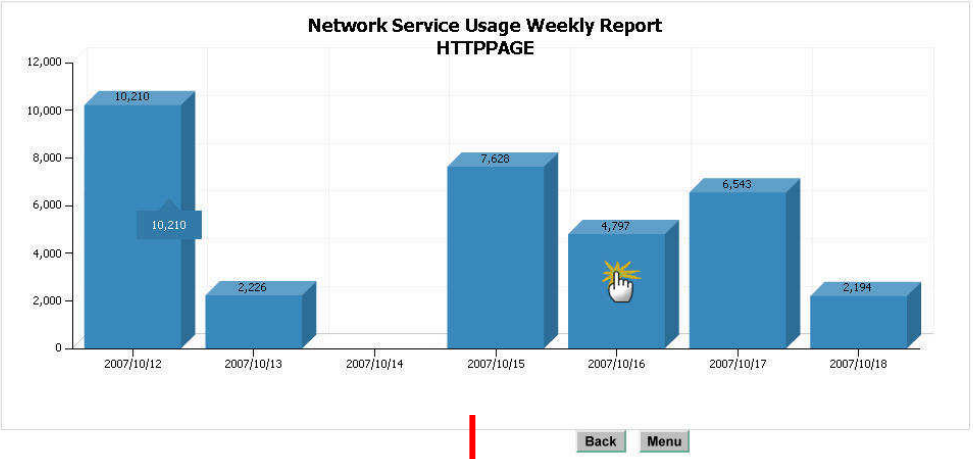
No.	□		Date-Time	IP	User Handle	Participants	Account	Conversation	Count	Similar Search
101.	□		2007-10-16 00:28:16	192.168.1.7	tom_0102@hotmail.com	rockman@yahoo.com		Conversation	276	🔍
102.	□		2007-10-16 00:07:51	192.168.1.7	tom_0102@hotmail.com	arthursss@hotmail.com		Conversation	217	🔍
103.	□		2007-10-16 00:07:50	192.168.1.7	tom_0102@hotmail.com	boki0625@yahoo.com		Conversation	61	🔍
104.	□		2007-10-16 00:06:33	192.168.1.10	diesis@hotmail.com	zil168@hotmail.com		Conversation	180	🔍
105.	□		2007-10-16 00:06:33	192.168.1.21	zil168@hotmail.com	diesis@hotmail.com		Conversation	180	🔍
106.	□		2007-10-16 00:06:04	192.168.1.36	decision_service_center@hotmail.com	boki0625@yahoo.com		Conversation	4	🔍
107.	□		2007-10-16 00:01:33	192.168.1.10	diesis@hotmail.com	howanchieh@hotmail.com		Conversation	1416	🔍
108.	□		2007-10-16 00:00:28	192.168.1.21	zil168@hotmail.com	03311981@yahoo.com		Conversation	44	🔍
109.	□		2007-10-15 23:52:22	192.168.1.36	zil168@hotmail.com	diesis@hotmail.com		Conversation	14	🔍
110.	□		2007-10-15 23:39:12	192.168.1.37	dick691111@yahoo.com	pigde2001@hotmail.com		Conversation	20	🔍

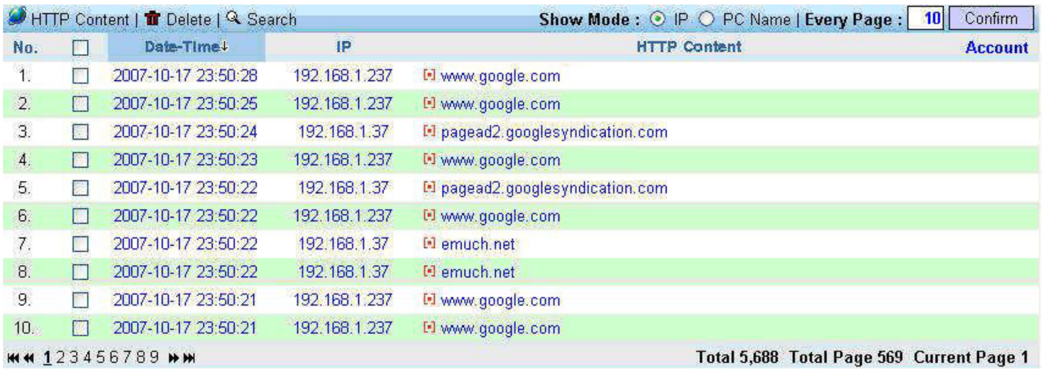
⏮ ⏪ 7 8 9 10 **11** 12 13 14 15 ⏩ ⏭ Total 201 Total Page 21 Current Page 11

Network Services Usage Weekly Report

It shows the weekly (last 7 days) different network services count. By clicking on particular service such as HTTP Page, it will direct you to the bar chart of HTTP Page report for last 7 days. By clicking on the specific day bar chart for HTTP Page, it will List out the entire HTTP Page (URL) visited by the network users.





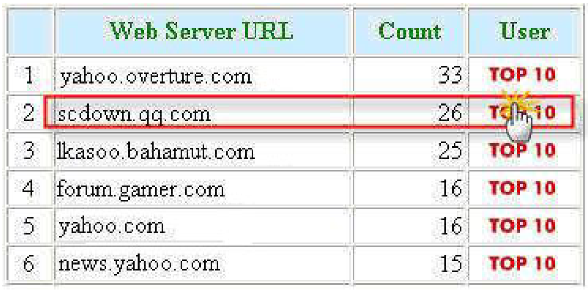

HTTP Content | Delete | Search
Show Mode : ● IP ○ PC Name | Every Page : 10 Confirm

No.	□	Date-Time↓	IP	HTTP Content	Account
1.	□	2007-10-17 23:50:28	192.168.1.237	www.google.com	
2.	□	2007-10-17 23:50:25	192.168.1.237	www.google.com	
3.	□	2007-10-17 23:50:24	192.168.1.37	pagead2.googlesyndication.com	
4.	□	2007-10-17 23:50:23	192.168.1.237	www.google.com	
5.	□	2007-10-17 23:50:22	192.168.1.37	pagead2.googlesyndication.com	
6.	□	2007-10-17 23:50:22	192.168.1.237	www.google.com	
7.	□	2007-10-17 23:50:22	192.168.1.37	emuch.net	
8.	□	2007-10-17 23:50:22	192.168.1.37	emuch.net	
9.	□	2007-10-17 23:50:21	192.168.1.237	www.google.com	
10.	□	2007-10-17 23:50:21	192.168.1.237	www.google.com	

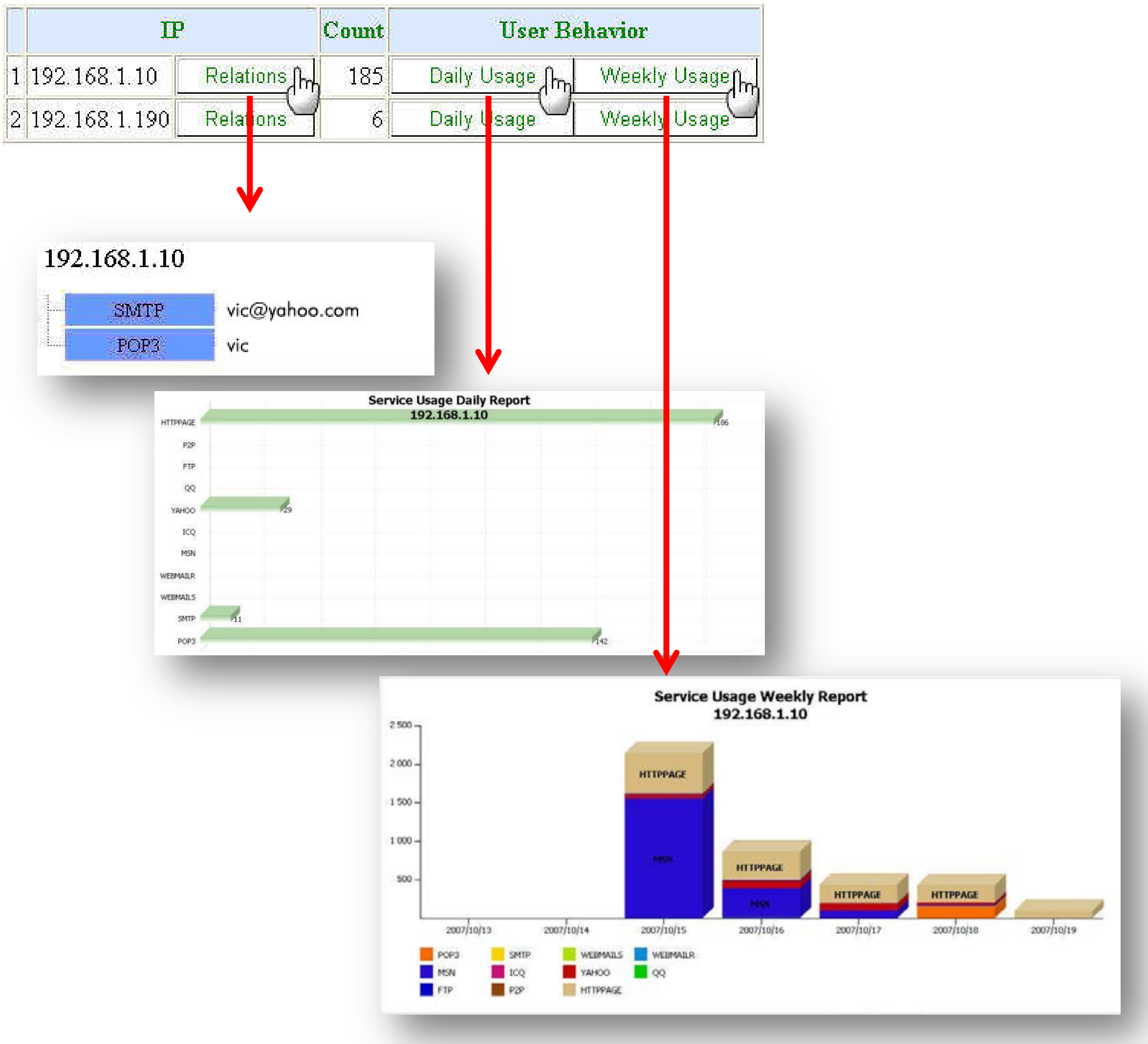
⏮ ◀ 1 2 3 4 5 6 7 8 9 ▶ ⏭ Total 5,688 Total Page 569 Current Page 1

Top Websites Report

It shows the top web sites visited by users on the network. By clicking on the TOP 10 of each Listed URL, it will direct to the page which shows the IP List that visited the website (URL) most often. From there, admin can click on Relations, Daily Usage or Weekly Usage Report as shown in diagrams below.



	Web Server URL	Count	User
1	yahoo.overture.com	33	TOP 10
2	scdown.qq.com	26	TOP 10
3	lkasoo.bahamut.com	25	TOP 10
4	forum.gamer.com	16	TOP 10
5	yahoo.com	16	TOP 10
6	news.yahoo.com	15	TOP 10



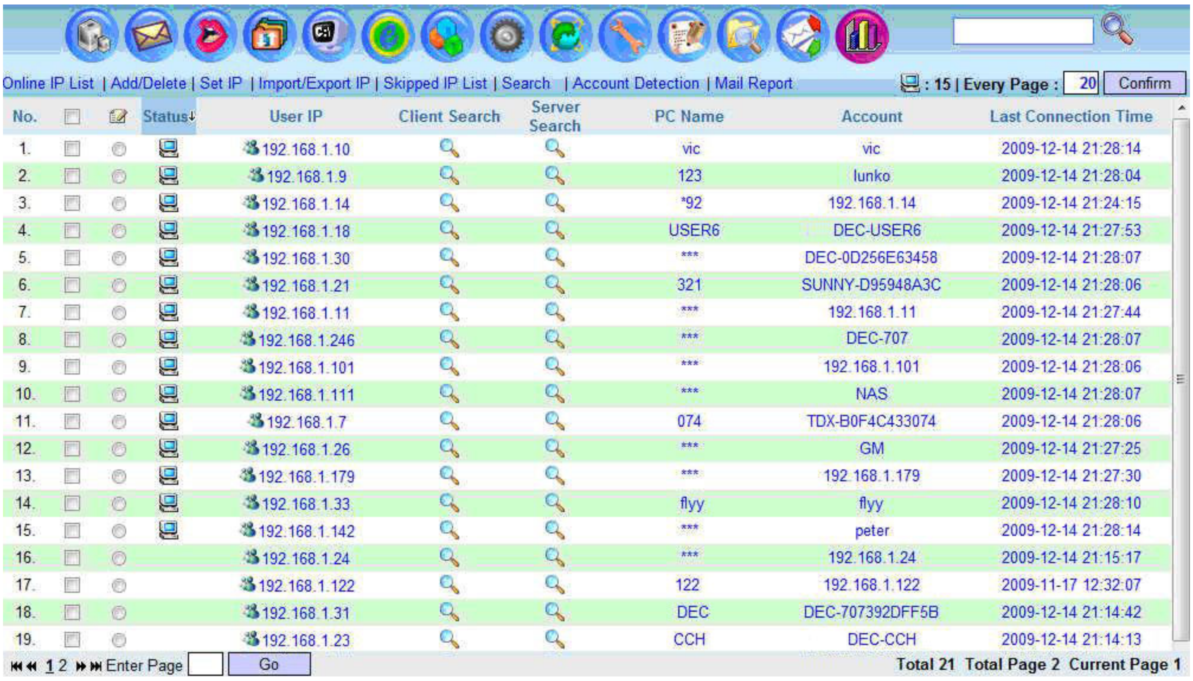
	IP		Count	User Behavior	
1	192.168.1.10	Relations	185	Daily Usage	Weekly Usage
2	192.168.1.190	Relations	6	Daily Usage	Weekly Usage

192.168.1.10

SMTP	vic@yahoo.com
POP3	vic

Online Users Report

It shows the Online IP List and Account with throughput statistics.



Online IP List | Add/Delete | Set IP | Import/Export IP | Skipped IP List | Search | Account Detection | Mail Report

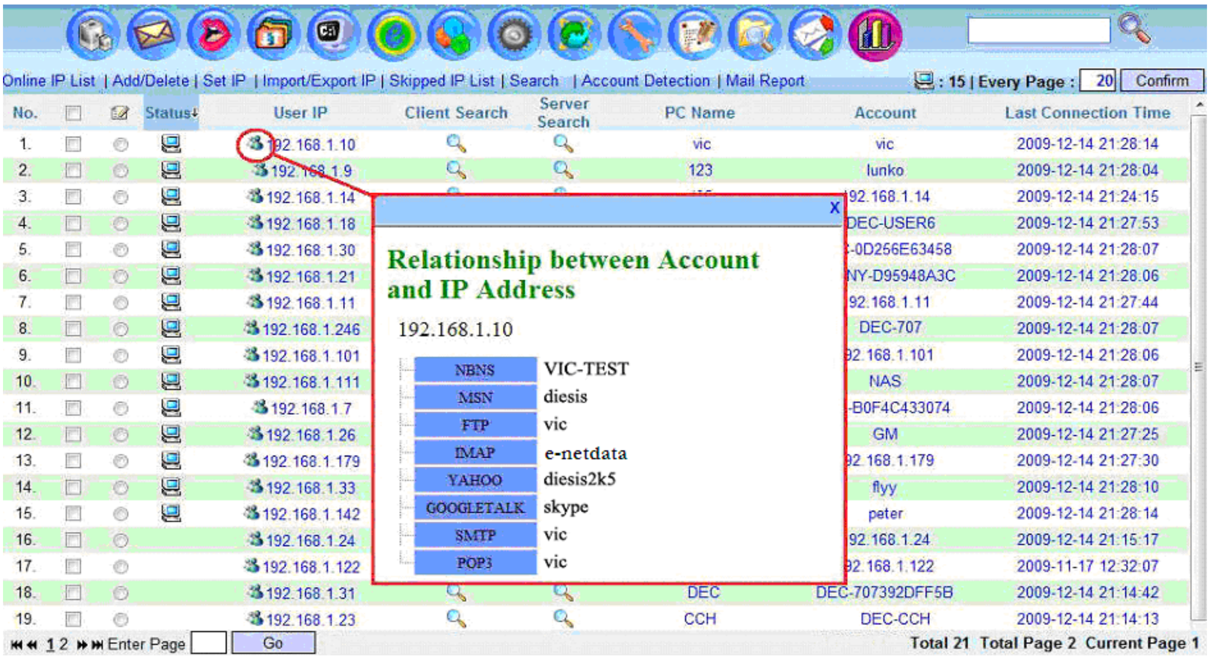
🖥 : 15 | Every Page : 20 Confirm

No.	□		Status↓	User IP	Client Search	Server Search	PC Name	Account	Last Connection Time
1.	□	○	🖥	192.168.1.10	🔍	🔍	vic	vic	2009-12-14 21:28:14
2.	□	○	🖥	192.168.1.9	🔍	🔍	123	lunko	2009-12-14 21:28:04
3.	□	○	🖥	192.168.1.14	🔍	🔍	*92	192.168.1.14	2009-12-14 21:24:15
4.	□	○	🖥	192.168.1.18	🔍	🔍	USER6	DEC-USER6	2009-12-14 21:27:53
5.	□	○	🖥	192.168.1.30	🔍	🔍	***	DEC-0D256E63458	2009-12-14 21:28:07
6.	□	○	🖥	192.168.1.21	🔍	🔍	321	SUNNY-D95948A3C	2009-12-14 21:28:06
7.	□	○	🖥	192.168.1.11	🔍	🔍	***	192.168.1.11	2009-12-14 21:27:44
8.	□	○	🖥	192.168.1.246	🔍	🔍	***	DEC-707	2009-12-14 21:28:07
9.	□	○	🖥	192.168.1.101	🔍	🔍	***	192.168.1.101	2009-12-14 21:28:06
10.	□	○	🖥	192.168.1.111	🔍	🔍	***	NAS	2009-12-14 21:28:07
11.	□	○	🖥	192.168.1.7	🔍	🔍	074	TDX-B0F4C433074	2009-12-14 21:28:06
12.	□	○	🖥	192.168.1.26	🔍	🔍	***	GM	2009-12-14 21:27:25
13.	□	○	🖥	192.168.1.179	🔍	🔍	***	192.168.1.179	2009-12-14 21:27:30
14.	□	○	🖥	192.168.1.33	🔍	🔍	flyy	flyy	2009-12-14 21:28:10
15.	□	○	🖥	192.168.1.142	🔍	🔍	***	peter	2009-12-14 21:28:14
16.	□	○		192.168.1.24	🔍	🔍	***	192.168.1.24	2009-12-14 21:15:17
17.	□	○		192.168.1.122	🔍	🔍	122	192.168.1.122	2009-11-17 12:32:07
18.	□	○		192.168.1.31	🔍	🔍	DEC	DEC-707392DFF5B	2009-12-14 21:14:42
19.	□	○		192.168.1.23	🔍	🔍	CCH	DEC-CCH	2009-12-14 21:14:13

⏮ ⏪ 1 2 ⏩ ⏭ Enter Page Go

Total 21 Total Page 2 Current Page 1

Click on the icon beside the User IP, it will show you the relationship of this IP with the accounts or usernames captured from different services.



Online IP List | Add/Delete | Set IP | Import/Export IP | Skipped IP List | Search | Account Detection | Mail Report

🖥 : 15 | Every Page : 20 Confirm

No.	□		Status↓	User IP	Client Search	Server Search	PC Name	Account	Last Connection Time
1.	□	○	🖥	92.168.1.10	🔍	🔍	vic	vic	2009-12-14 21:28:14
2.	□	○	🖥	192.168.1.9	🔍	🔍	123	lunko	2009-12-14 21:28:04
3.	□	○	🖥	192.168.1.14				92.168.1.14	2009-12-14 21:24:15
4.	□	○	🖥	192.168.1.18				DEC-USER6	2009-12-14 21:27:53
5.	□	○	🖥	192.168.1.30				-0D256E63458	2009-12-14 21:28:07
6.	□	○	🖥	192.168.1.21				NY-D95948A3C	2009-12-14 21:28:06
7.	□	○	🖥	192.168.1.11				92.168.1.11	2009-12-14 21:27:44
8.	□	○	🖥	192.168.1.246				DEC-707	2009-12-14 21:28:07
9.	□	○	🖥	192.168.1.101				92.168.1.101	2009-12-14 21:28:06
10.	□	○	🖥	192.168.1.111				NAS	2009-12-14 21:28:07
11.	□	○	🖥	192.168.1.7				-B0F4C433074	2009-12-14 21:28:06
12.	□	○	🖥	192.168.1.26				GM	2009-12-14 21:27:25
13.	□	○	🖥	192.168.1.179				92.168.1.179	2009-12-14 21:27:30
14.	□	○	🖥	192.168.1.33				flyy	2009-12-14 21:28:10
15.	□	○	🖥	192.168.1.142				peter	2009-12-14 21:28:14
16.	□	○		192.168.1.24				92.168.1.24	2009-12-14 21:15:17
17.	□	○		192.168.1.122				92.168.1.122	2009-11-17 12:32:07
18.	□	○		192.168.1.31	🔍	🔍	DEC	DEC-707392DFF5B	2009-12-14 21:14:42
19.	□	○		192.168.1.23	🔍	🔍	CCH	DEC-CCH	2009-12-14 21:14:13

⏮ ⏪ 1 2 ⏩ ⏭ Enter Page Go

Total 21 Total Page 2 Current Page 1

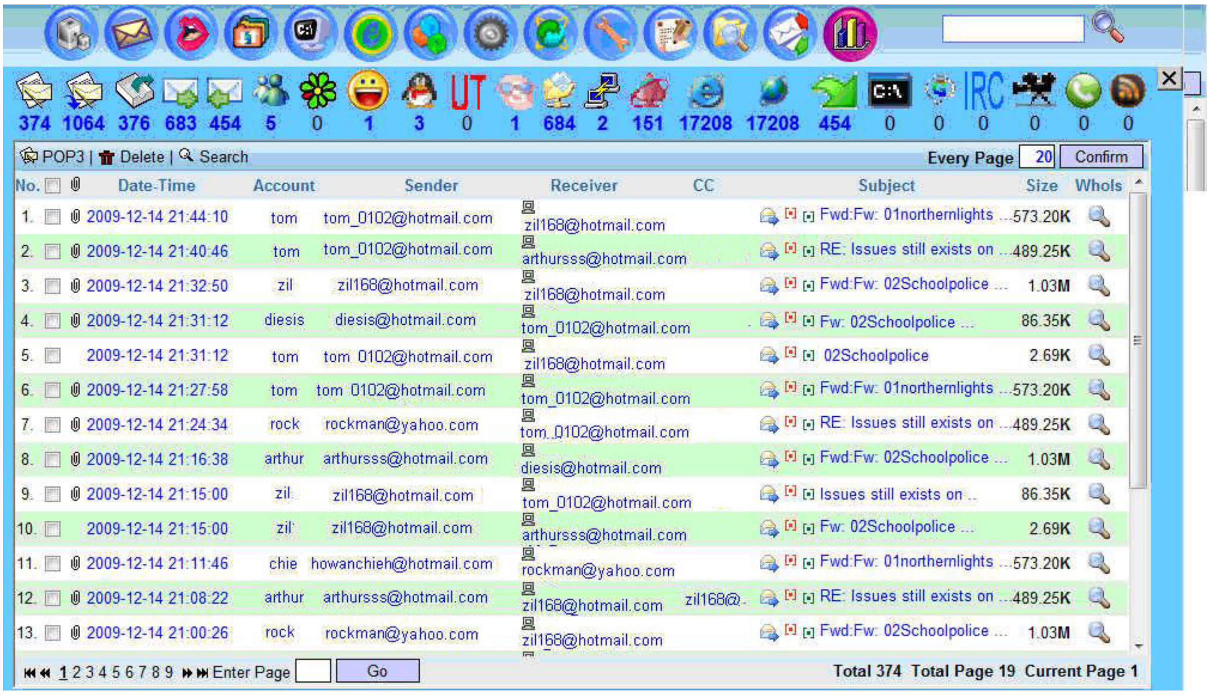
X

Relationship between Account and IP Address

192.168.1.10

NBNS	VIC-TEST
MSN	diesis
FTP	vic
IMAP	e-netdata
YAHOO	diesis2k5
GOOGLETALK	skype
SMTP	vic
POP3	vic

Click on search client will provide you all the data reconstructed for the particular client or IP Address.



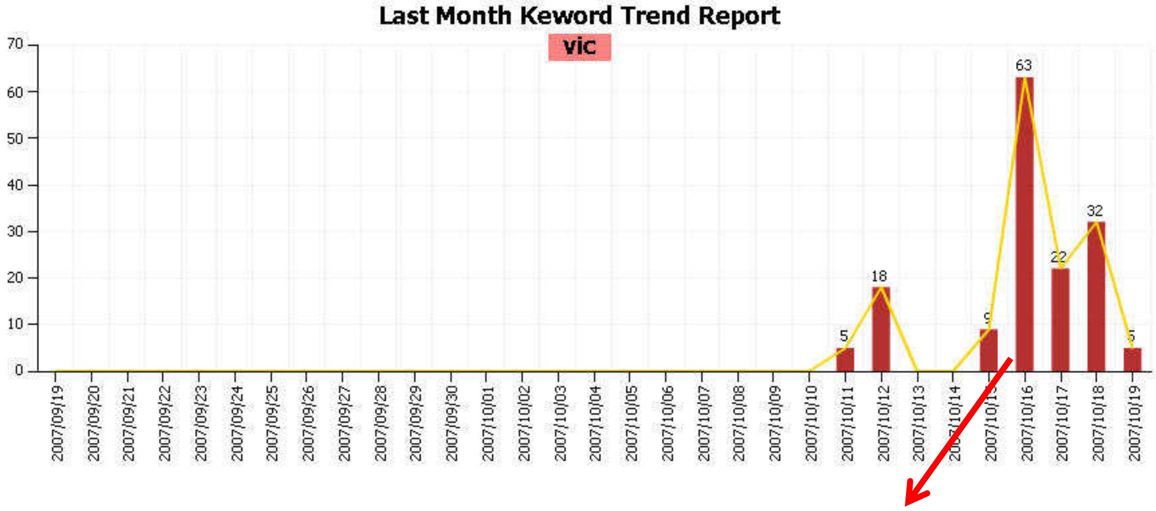
No.	□		Date-Time	Account	Sender	Receiver	CC	Subject	Size	WhoIs
1.	□		2009-12-14 21:44:10	tom	tom_0102@hotmail.com	zil168@hotmail.com		Fwd:Fw: 01northernlights ...	573.20K	
2.	□		2009-12-14 21:40:46	tom	tom_0102@hotmail.com	arthursss@hotmail.com		RE: Issues still exists on ...	489.25K	
3.	□		2009-12-14 21:32:50	zil	zil168@hotmail.com	zil168@hotmail.com		Fwd:Fw: 02Schoolpolice ...	1.03M	
4.	□		2009-12-14 21:31:12	diesis	diesis@hotmail.com	tom_0102@hotmail.com		Fw: 02Schoolpolice ...	86.35K	
5.	□		2009-12-14 21:31:12	tom	tom_0102@hotmail.com	zil168@hotmail.com		02Schoolpolice	2.69K	
6.	□		2009-12-14 21:27:58	tom	tom_0102@hotmail.com	tom_0102@hotmail.com		Fwd:Fw: 01northernlights ...	573.20K	
7.	□		2009-12-14 21:24:34	rock	rockman@yahoo.com	tom_0102@hotmail.com		RE: Issues still exists on ...	489.25K	
8.	□		2009-12-14 21:16:38	arthur	arthursss@hotmail.com	diesis@hotmail.com		Fwd:Fw: 02Schoolpolice ...	1.03M	
9.	□		2009-12-14 21:15:00	zil	zil168@hotmail.com	tom_0102@hotmail.com		Issues still exists on ..	86.35K	
10.	□		2009-12-14 21:15:00	zil	zil168@hotmail.com	arthursss@hotmail.com		Fw: 02Schoolpolice ...	2.69K	
11.	□		2009-12-14 21:11:46	chie	howanchieh@hotmail.com	rockman@yahoo.com		Fwd:Fw: 01northernlights ...	573.20K	
12.	□		2009-12-14 21:08:22	arthur	arthursss@hotmail.com	zil168@hotmail.com	zil168@..	RE: Issues still exists on ...	489.25K	
13.	□		2009-12-14 21:00:26	rock	rockman@yahoo.com	zil168@hotmail.com		Fwd:Fw: 02Schoolpolice ...	1.03M	

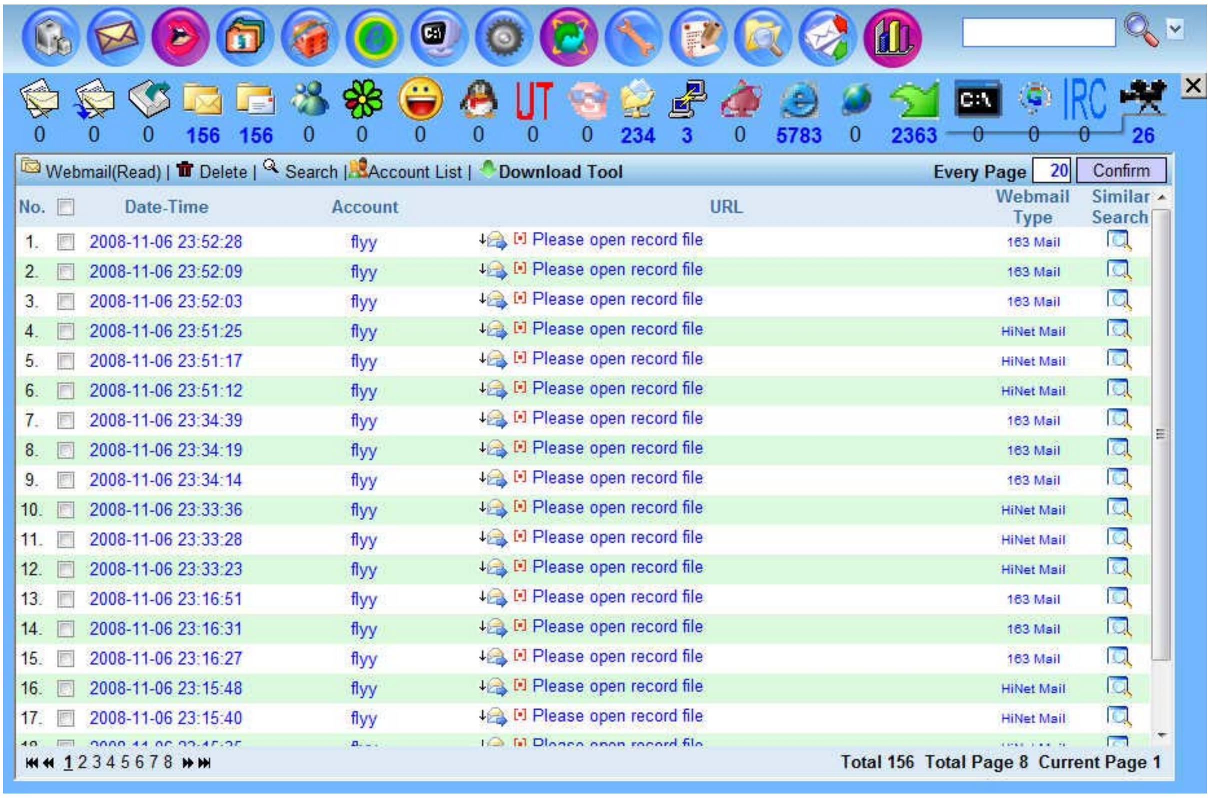
Total 374 Total Page 19 Current Page 1

Last Month Key Word Trend Report

Admin can search particular keyword on the database and the report can display the number of time (count) the keyword appears daily for the last one month. For example, by key in the keywords “vic” and search for it in database. The report obtained is as follow.

vic



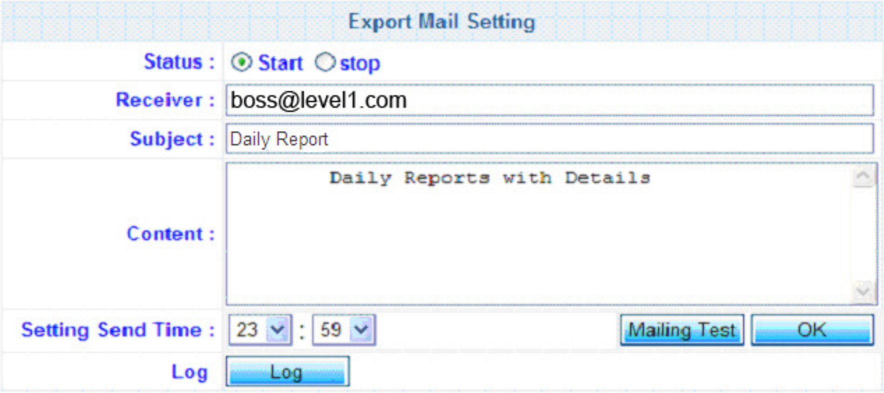


No.	□	Date-Time	Account	URL	Webmail Type	Similar Search
1.	□	2008-11-06 23:52:28	flyy	Please open record file	163 Mail	
2.	□	2008-11-06 23:52:09	flyy	Please open record file	163 Mail	
3.	□	2008-11-06 23:52:03	flyy	Please open record file	163 Mail	
4.	□	2008-11-06 23:51:25	flyy	Please open record file	HiNet Mail	
5.	□	2008-11-06 23:51:17	flyy	Please open record file	HiNet Mail	
6.	□	2008-11-06 23:51:12	flyy	Please open record file	HiNet Mail	
7.	□	2008-11-06 23:34:39	flyy	Please open record file	163 Mail	
8.	□	2008-11-06 23:34:19	flyy	Please open record file	163 Mail	
9.	□	2008-11-06 23:34:14	flyy	Please open record file	163 Mail	
10.	□	2008-11-06 23:33:36	flyy	Please open record file	HiNet Mail	
11.	□	2008-11-06 23:33:28	flyy	Please open record file	HiNet Mail	
12.	□	2008-11-06 23:33:23	flyy	Please open record file	HiNet Mail	
13.	□	2008-11-06 23:16:51	flyy	Please open record file	163 Mail	
14.	□	2008-11-06 23:16:31	flyy	Please open record file	163 Mail	
15.	□	2008-11-06 23:16:27	flyy	Please open record file	163 Mail	
16.	□	2008-11-06 23:15:48	flyy	Please open record file	HiNet Mail	
17.	□	2008-11-06 23:15:40	flyy	Please open record file	HiNet Mail	
18.	□	2008-11-06 23:15:35	flyy	Please open record file	HiNet Mail	

Total 156 Total Page 8 Current Page 1

Daily Report (Excel Log Report)

This function allows Administrator to schedule report generation in Excel format. The Daily Report can be configured to be sent to the Administrator every day at specific time. Click on Start at the Status and fill the information such as receiver, subject, content, send time and click [OK] to activate this service.

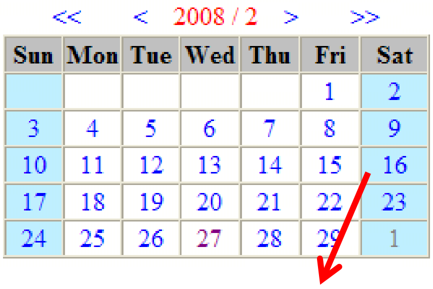


Export Mail Setting

Status :	● Start ○ stop
Receiver :	boss@level1.com
Subject :	Daily Report
Content :	Daily Reports with Details
Setting Send Time :	23 : 59
Log	

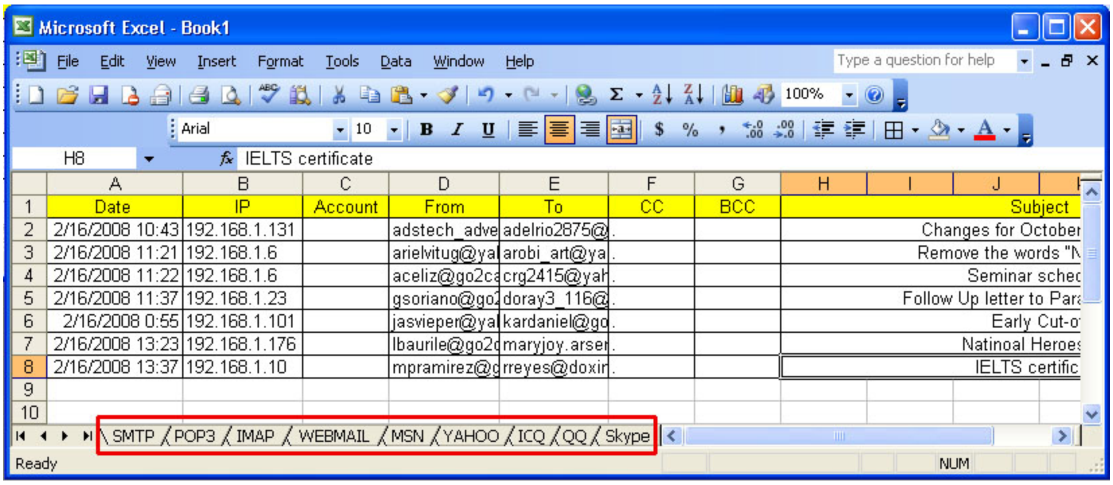
Download Daily Report

Administrator can download the daily report (in excel format) manually.



<< < 2008 / 2 > >>

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	1



Microsoft Excel - Book1

H8 IELTS certificate

	A	B	C	D	E	F	G	H
1	Date	IP	Account	From	To	CC	BCC	Subject
2	2/16/2008 10:43	192.168.1.131		adstech_adve	adelrio2875@	.		Changes for October
3	2/16/2008 11:21	192.168.1.6		arielvitug@yal	arobi_art@ya	.		Remove the words "N
4	2/16/2008 11:22	192.168.1.6		aceliz@go2ca	crg2415@yah	.		Seminar schec
5	2/16/2008 11:37	192.168.1.23		gsoriano@go2	doray3_116@	.		Follow Up letter to Para
6	2/16/2008 0:55	192.168.1.101		jasvieper@yal	kardaniel@go	.		Early Cut-o
7	2/16/2008 13:23	192.168.1.176		lbaurile@go2d	maryjoy.arser	.		Natinoal Heroes
8	2/16/2008 13:37	192.168.1.10		mpramirez@g	rreyes@doxin	.		IELTS certific
9								
10								

Appendix A: P2P Supported

Bittorrent Protocol	BitCometdz	uTorrent	BitSpirit
BitTornado	BitLord	BitBuddy	Flashget 1.81
Azureus	BitTorrent	BitTyrant	ezpeer+
Gnutella Protocol	Foxy	LimeWare	BearShare
eDonkey/eMule	eDonkey	eMule	Fasttrack Protocol
Kazaa			

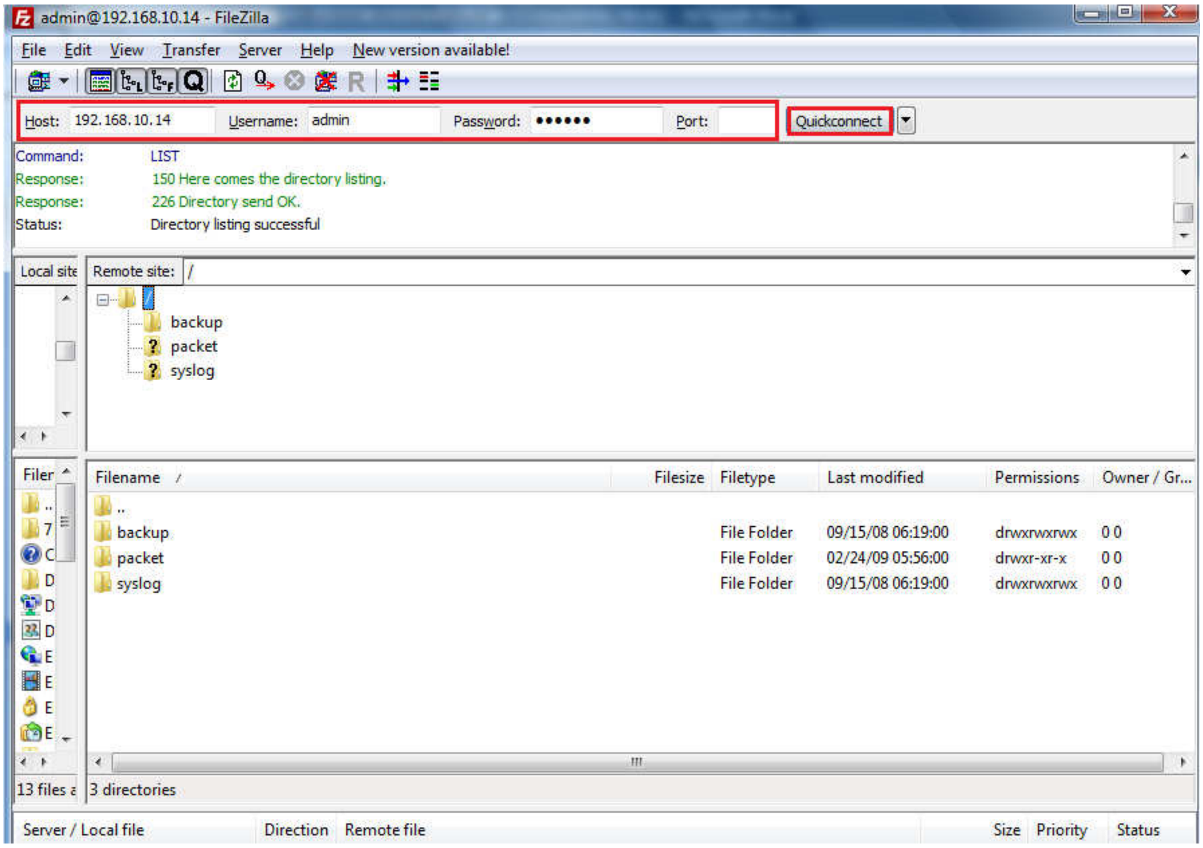
Appendix B: Online Games Supported

Maplestory	HE	Nobol	Metin
Kartrider	ZU	FDO	MS
BnB	Cabala	GHOSTSOUL	SUN
Mabinogi	JY1	AL	Stoneage
Hotdance	JY2	CPW	A3
Getamped	WonderLand	GVO	Hero
GrandChase	SA	CG	HB
Pangya	TS	DOMO	Mystina
Heatproject	LoveBox	BO	ZT
DTG	SANGO	SWDOL	FairyLand
Superrich	Dekaron	DOMOFREE	King of king 2
OO2jam	WOW	RICHOL	WE5
Seal	Cabal	RO	FongShen
COCOCAN	Rohan	Mir3	FongShen2
Nage	1003b	JX	Q3baby
Gersang	9D	JX2	FongShen2
Laghaim	EverQuestII	TTH	Q3baby
Hot	Nostale	RF Online	SHE
3P	Flyff	SOL	Megaten
SF	Silkroad2	Elysium	12q
Noritel			

Appendix C: Retrieve Data Log via FTP

System admin can retrieve the ICI system data log via ftp. Please make sure that you have configured the FTP/Console Username and Password, also make sure that you have started the FTP service at Services section

Login Name: **admin**
Password: **000000** (six zero)



admin@192.168.10.14 - FileZilla

Host: 192.168.10.14 Username: admin Password: •••••• Port:

```
Command:    LIST
Response:   150 Here comes the directory listing.
Response:   226 Directory send OK.
Status:     Directory listing successful
```

Local site | Remote site: /

```
/
  backup
  packet
  syslog
```

Filename /	Filesize	Filetype	Last modified	Permissions	Owner / Gr...
..					
backup		File Folder	09/15/08 06:19:00	drwxrwxrwx	0 0
packet		File Folder	02/24/09 05:56:00	drwxr-xr-x	0 0
syslog		File Folder	09/15/08 06:19:00	drwxrwxrwx	0 0

13 files a | 3 directories

Appendix D: Field Definition of Full-Text Search Function

Full-Text Search function not only supports the keyword search but also supports data search by the specified fields of record. For example, if I want to query the sent mail records from rick@Level1.com on 2008/09/16, I can give a query statement as below:

type:SMTP AND date:20080916 AND from:rick@Level1.com

The wild card searching is also supported in Full-Text Search Function. For example, if I want to get all the mail records sent from 'rick', I can give a query statement as below:

*type:SMTP AND from:rick**

The detail document of supported query syntax is Listed in the extension chapter. What kinds of fields searching you can apply for each decoding record are defined as below:

[SMTP Mail Sending] (type:SMTP)
account - The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is 'YYYYMMDD'. Ex. 20080916 time - Syntax format is 'HHMMSS'. Ex. 231020
subject - Mail subject
from - Sender to - Recipients
cc - Carbon copy
bcc - Blind carbon copy
ext - File name extension. Ex. doc, txt, exe, ...

[POP3 Mail Retrieving] (type:POP3)
account - The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is 'YYYYMMDD'. Ex. 20080916 time - Syntax format is 'HHMMSS'. Ex. 231020
subject - Mail subject
from - Sender
to - Recipients
cc - Carbon copy
bcc - Blind carbon copy
ext - File name extension. Ex. doc, txt, exe, ... login - Mail server login account

[IMAP Mail Retrieving] (type:IMAP)
account - The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is 'YYYYMMDD'. Ex. 20080916 time - Syntax format is 'HHMMSS'. Ex. 231020
subject - Mail subject
from - Sender to - Recipients
cc - Carbon copy
bcc - Blind carbon copy
ext - File name extension. Ex. doc, txt, exe, ... login- Mail server login account

[Web Mail Sending] (type:WEBMAILS)
account- The target account of record srcIp - Source IP address of record
mac - Source MAC address of record

date - Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 231020
subject- Mail subject
from- Sender to - Recipients
cc - Carbon copy
bcc - Blind carbon copy
service - Webmail service. Ex. YAHOO, GMAIL, HINET, ...

[Web Mail Retrieving] (type:WEBMAILR)
account- The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 231020
subject- Mail subject from- Sender
to- Recipients
cc- Carbon copy
bcc - Blind carbon copy
service- Webmail service. Ex. YAHOO, GMAIL, HINET, ...

[MSN Messenger] (type:MSN)
account- The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date- Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 231020
msnOwner- Initiator of message communication msnWhom- Participant of message communication

[ICQ] (type:ICQ)
account- The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 231020
icqOwner - Initiator of message communication icqWhom - Participant of message communication

[Yahoo Messenger] (type:YAHOO)
account- The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 231020
yahooOwner- Initiator of message communication yahooWhom- Participant of message communication

[QQ] (type:QQ)
account- The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is ‘YYYYMMDD’. Ex. 20080916
time - Syntax format is ‘HHMMSS’. Ex. 231020 qqOwner - Initiator of message communication
qqWhom - Participant of message communication

[SKYPE] (type:SKYPE)
account- The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 231020

[UT Webchat] (type:UT)
account- The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 231020
utOwner - Initiator of message communication utWhom - Participant of message communication

[IRC Messenger] (type:IRC)
account- The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 231020
ircOwner - Initiator of message communication ircWhom - Participant of message communication

[Google Talk Messenger] (type:GOOGLETALK)
account- The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 231020
googletalkOwner- Initiator of message communication googletalkWhom- Participant of message communication

[HTTP URL Record] (type:HTTPLOG)
account- The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 231020
host - Web Site hostname. Ex. www.google.com.tw

[Web Page Record] (type:HTTPPAGE)
account- The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 231020
host - Web Site hostname. Ex. www.google.com.tw

[HTTP File Download/Upload] (type:HTTPFILE)
account- The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 231020
host - Web Site hostname. Ex. www.google.com.tw filename - Transferred file name. Ex. test.doc
ext- File name extension. Ex. doc, txt, exe, ...

[HTTP Video Clip] (type:HTTPVIDEO)
account- The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 231020
host - Web Site hostname. Ex. www.google.com.tw filename - Transferred file name. Ex. test.doc
ext- File name extension. Ex. doc, txt, exe, ...

[FTP File Transfer] (type:FTP)
account- The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 23102
server- FTP Server IP Address user - FTP login account
filename - Transferred file name. Ex. test.doc ext- File name extension. Ex. doc, txt, exe, ...

[P2P File Transfer] (type:P2P)
account- The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 23102
tool - P2P toolkit. Ex. BitTorrent, Foxy, ...

ext- File name extension. Ex. doc, txt, exe, ...

[On-line GAME Record] (type:GAME)
account - The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 23102
tool - Name of on-line game. Ex. WOW, ...

[Telnet Communication] (type:TELNET)
account - The target account of record srcIp - Source IP address of record
mac - Source MAC address of record
date - Syntax format is ‘YYYYMMDD’. Ex. 20080916 time - Syntax format is ‘HHMMSS’. Ex. 23102
server- Telnet Server IP Address user - Telnet login account

Extension – Query Syntax Definition

Overview

This page provides the Query syntax in ICI Inner Search Engine. Before choosing to use the provided Query, please consider the following:

1. If you are programmatically generating a query string and then parsing it with the query parser then you should seriously consider building your queries directly with the query API. In other words, the query parser is designed for human-entered text, not for program-generated text.

2. Untokenized fields are best added directly to queries, and not through the query parser. If a field's values are generated programmatically by the application, then so should query clauses for this field. An analyzer, which the query parser uses, is designed to convert human-entered text to terms. Program-generated values, like dates, keywords, etc., should be consistently program-generated.

3. In a query form, fields which are general text should use the query parser. All others, such as date ranges, keywords, etc. are better added directly through the query API. A field with a limit set of values, that can be specified with a pull-down menu should not be added to a query string which is subsequently parsed, but rather added as a TermQuery clause.

Terms

A query is broken up into terms and operators. There are two types of terms: Single Terms and Phrases.

A Single Term is a single word such as "test" or "hello".

A Phrase is a group of words surrounded by double quotes such as "hello dolly".

Multiple terms can be combined together with Boolean operators to form a more complex query (see below).

Note: The analyzer used to create the index will be used on the terms and phrases in the query string. So it is important to choose an analyzer that will not interfere with the terms used in the query string.

Fields

Inner Search Engine supports fielded data. When performing a search you can either specify a field, or use the default field. The field names and default field is implementation specific.

You can search any field by typing the field name followed by a colon ":" and then the term you are looking for.

As an example, let's assume an Inner Search Engine index contains two fields, title and text and text is the default field. If you want to find the document entitled "The Right Way" which contains the text "don't go this way", you can enter:

title:"The Right Way" AND text:go

or

title:"Do it right" AND right

Since text is the default field, the field indicator is not required.

Note: The field is only valid for the term that it directly precedes, so the query

title:Do it right

Will only find "Do" in the title field. It will find "it" and "right" in the default field (in this case the text field).

Term Modifiers

Inner Search Engine supports modifying query terms to provide a wide range of searching options.

Wildcard Searches

Inner Search Engine supports single and multiple character wildcard searches.
To perform a single character wildcard search use the "?" symbol.
To perform a multiple character wildcard search use the "*" symbol.

The single character wildcard search looks for terms that match that with the single character replaced. For example, to search for "text" or "test" you can use the search:

te?t

Multiple character wildcard searches looks for 0 or more characters. For example, to search for test, tests or tester, you can use the search:

*test**

You can also use the wildcard searches in the middle of a term.

*te*t*

Note: You cannot use a * or ? symbol as the first character of a search.

Fuzzy Searches

Inner Search Engine supports fuzzy searches based on the Levenshtein Distance, or Edit Distance algorithm. To do a fuzzy search use the tilde, "~", symbol at the end of a Single word Term. For example to search for a term similar in spelling to "roam" use the fuzzy search:

roam~

This search will find terms like foam and roams.

Starting with ICI Inner Search Engine 1.9 an additional (optional) parameter can specify the required similarity. The value is between 0 and 1, with a value closer to 1 only
terms with a higher similarity will be matched. For example:

roam~0.8

The default that is used if the parameter is not given is 0.5.

Proximity Searches

Inner Search Engine supports finding words are within a specific distance away. To do a proximity search use the tilde, "~", symbol at the end of a Phrase. For example to search for "apache" and "jakarta" within 10 words of each other in a document use the search:

"jakarta apache"~10

Range Searches

Range Queries allow one to match documents whose field(s) values are between the lower and upper bound specified by the Range Query. Range Queries can be inclusive or exclusive of the upper and lower bounds. Sorting is done lexicographically.

mod_date:[20020101 TO 20030101]

This will find documents whose mod_date fields have values between 20020101 and 20030101, inclusive. Note that Range Queries are not reserved for date fields. You could also use range queries with non-date fields:

title:{Aida TO Carmen}

This will find all documents whose titles are between Aida and Carmen, but not including Aida and Carmen.

Inclusive range queries are denoted by square brackets. Exclusive range queries are denoted by curly brackets.

Boosting a Term

Inner Search Engine provides the relevance level of matching documents based on the terms found. To boost a term use the caret, "^", symbol with a boost factor (a number) at the end of the term you are searching. The higher the boost factor, the more relevant the term will be.

Boosting allows you to control the relevance of a document by boosting its term. For example, if you are searching for

jakarta apache

and you want the term "jakarta" to be more relevant boost it using the ^ symbol along with the boost factor next to the term. You would type:

jakarta^4 apache

This will make documents with the term jakarta appear more relevant. You can also boost Phrase Terms as in the example:

"jakarta apache"^4 "Apache ICI Inner Search Engine"

By default, the boost factor is 1. Although the boost factor must be positive, it can be less than 1 (e.g. 0.2)

Boolean Operators

Boolean operators allow terms to be combined through logic operators. ICI Inner Search Engine supports AND, "+", OR, NOT and "-" as Boolean operators(Note: Boolean operators must be ALL CAPS).

The OR operator is the default conjunction operator. This means that if there is no Boolean operator between two terms, the OR operator is used. The OR operator links two terms and finds a matching document if either of the terms exist in a document. This is equivalent to a union using sets. The symbol || can be used in place of the word OR.

To search for documents that contain either "jakarta apache" or just "jakarta" use the query:

"jakarta apache" jakarta

or

"jakarta apache" OR jakarta

AND

The AND operator matches documents where both terms exist anywhere in the text of a single document. This is equivalent to an intersection using sets. The symbol && can be used in place of the word AND.

To search for documents that contain "jakarta apache" and "Apache ICI Inner Search Engine" use the query:

"jakarta apache" AND "Apache ICI Inner Search Engine"

+

The "+" or required operator requires that the term after the "+" symbol exist somewhere in a the field of a single document.

To search for documents that must contain "jakarta" and may contain "ICI Inner Search Engine" use the query:

+jakarta apache

NOT

The NOT operator excludes documents that contain the term after NOT. This is equivalent to a difference using sets. The symbol ! can be used in place of the word NOT.

To search for documents that contain "jakarta apache" but not "Apache ICI Inner Search Engine" use the query:

"jakarta apache" NOT "Apache ICI Inner Search Engine"

Note: The NOT operator cannot be used with just one term. For example, the following search will return no results:

NOT "jakarta apache"

-

The "-" or prohibit operator excludes documents that contain the term after the "-" symbol. To search for documents that contain "jakarta apache" but not "Apache ICI Inner Search Engine" use the query:

"jakarta apache" -"Apache ICI Inner Search Engine"

Grouping

Inner Search Engine supports using parentheses to group clauses to form sub queries. This can be very useful if you want to control the boolean logic for a query.

To search for either "jakarta" or "apache" and "website" use the query:

(jakarta OR apache) AND website

This eliminates any confusion and makes sure you that website must exist and either term jakarta or apache may exist.

Field Grouping

Inner Search Engine supports using parentheses to group multiple clauses to a single field.

To search for a title that contains both the word "return" and the phrase "pink panther" use the query:

title:(+return +"pink panther")

Escaping Special Characters

Inner Search Engine supports escaping special characters that are part of the query syntax. The current List special characters are

+ - *&& || ! ( ) { } [ ] ^ " ~ * ? : *

To escape these character use the \ before the character. For example to search for (1+1):2 use the query:

\(1\+1\)\:2

Technical Support Email:

support@level1.com

levelone