NG Trace User Manual

December 2009

Table of Contents

1. IN	NTRODUCTION	4
1.1	Overview	4
2. S	YSTEM OVERVIEW	4
2.1	About the System	4
2.2	FEATURE	4
2.3	System Requirement	4
3. U	JSER MANAGEMENT	5
3.1	User Log In	5
3.2	USER MANAGEMENT	6
3.3	User Privilege	
4. R	REPORT AND ANALYSIS	11
4. R 4.1	REPORT AND ANALYSIS	11
4. R 4.1 <i>4</i> .	REPORT AND ANALYSIS Logs and Audits	11
 4. R 4.1 4. 4. 	REPORT AND ANALYSIS LOGS AND AUDITS .1.1 Whole .1.2	11
 4. R 4.1 4. 4. 4. 4. 	REPORT AND ANALYSIS LOGS AND AUDITS 1.1 Whole 1.2 ICMP 1.3 E-mail	
 4. R 4.1 4. 4. 4. 4. 4. 4. 	REPORT AND ANALYSIS LOGS AND AUDITS 1.1 Whole 1.2 ICMP 1.3 E-mail 1.4 IM	11
 4. R 4.1 4. 4. 4. 4. 4. 4. 4. 	REPORT AND ANALYSIS LOGS AND AUDITS 1.1 Whole 1.2 ICMP 1.3 E-mail 1.4 IM 1.5 HTTP	11 11 11 14 14 16 19 20
 4. R 4.1 4. 4. 4. 4. 4. 4. 4. 4. 	REPORT AND ANALYSIS LOGS AND AUDITS 1.1 Whole 1.2 ICMP 1.3 E-mail 1.4 IM 1.5 HTTP 1.6 FTP	11 11 11 11 14 16 19 20 22
 4. R 4.1 4. 4. 4. 4. 4. 4. 4.2 	REPORT AND ANALYSIS LOGS AND AUDITS 1.1 Whole 1.2 ICMP 1.3 E-mail 1.4 IM 1.5 HTTP 1.6 FTP SEARCH	11 11 11 11 14 16 19 20 22 25
 4. R 4.1 4. 4. 4. 4. 4. 4. 4.2 4.3 	REPORT AND ANALYSIS LOGS AND AUDITS 1.1 Whole 1.2 ICMP 1.3 E-mail 1.4 IM 1.5 HTTP 1.6 FTP SEARCH DATABASE	11 11 11 11 14 16 19 20 22 25 25

Table of Figures

FIGURE 1. USER LOG IN	5
Figure 2. User Management Tab	6
FIGURE 3. ADD USER	7
FIGURE 4. SHOW USER INFORMATION	8
FIGURE 5. EDIT USER	9
FIGURE 6. SET NEW PASSWORD	10
Figure 7. Whole Log List	12
FIGURE 8. RESULT FILTER OF WHOLE LOG LIST	12
Figure 9. Date – Time Filter	13
FIGURE 10. PROTOCOL FILTER	13
Figure 11. Target Filter	13
Figure 12. Host Filter	14
FIGURE 13. PAGE FILTER	14
Figure 14. ICMP Log List	15
FIGURE 15. RESULT FILTER OF ICMP LOG	15
Figure 16. Export message	16
Figure 17. ICMP Detail	16
Figure 18. E-mail Log List	17
FIGURE 19. RESULT FILTER OF E-MAIL LOG	17
Figure 20. Export message	18
Figure 21. E-mail Detail	18
Figure 22. IM Log List	19
FIGURE 23. RESULT FILTER OF IM LOG	20
Figure 24. Export message	20
FIGURE 25. HTTP LOG LIST	21
FIGURE 26. RESULT FILTER OF HTTP LOG	21
Figure 27. Export message	22
FIGURE 28. HTTP DETAIL	22
FIGURE 29. FTP LOG LIST	23
FIGURE 30. RESULT FILTER OF FTP LOG	23
FIGURE 31. EXPORT MESSAGE.	24
FIGURE 32. FTP DETAIL	24
FIGURE 33. SEARCH	25

FIGURE	34. Select	DATABASE	26
FIGURE	35. Whole	Log List Of RECENTDB	27
FIGURE	36. Export	TABLE LIST	28

1. Introduction

1.1 Overview

This document describes information on the usage of the system from the user point of view.

It explains about the different user account and their privileges, t he options for exporting the result as CSV file, using the different reports and analysis pages, searching and filtering the results.

2. System Overview

2.1 About the System

NG Trace is a corporate security which is capable of monitoring the network traffic and taking action on the occurrence of suspi cious or potentially dangerous events.

NG Trace as any modern security system is with flexible, multil ayered and easily configurable architecture and software design.

It has intuitive user-friendly interface and lots of functionalities. It can apply both set of predefined rules following suspicious us ers' behavior and it can accept new targets of interest defined by newly inserted rule sets.

2.2 Feature

- ✓ Capturing network traffic, transferring it to readable look and connecting of communication sessions.
- \checkmark Saving the decoded traffic into database.
- \checkmark Indexing of the decoded traffic into database.
- \checkmark Exporting the data of database.
- \checkmark Archiving of the database on hardware device.
- \checkmark Sending e-mails in case of the emerging of difference event.

2.3 System Requirement

OS : Cent OS 5.3 recommended.

The system's components run on Intel based, GNU / Linux com patible server machines, equipped with at least one network card, a CD / DVD drive, enough hard-disk space and RAM. If all the system's components are deployed on a single server; Dual Core 2.4GHz Pentium CPU, 4GB RAM system memory, 80GB available disk space or more 100Mbit/s Network card or more

3. User Management

3.1 User Log In

User with user account enters Username and Password to log in.

NG TRACE ^{®0}
Enterprise Security System Username
LOGIN Remember me
© 2008-2009 NGTraceManager. All Rights Reserved NG Trace v1.0 b100 Rails 2.3.2 Env development

Figure 1. User Log In

3.2 User Management

User management section provides functionalities such as adding and deleting of user, displaying and modifying user's information.

NG TRACE ^{©©} Enterprise Security System	SYSTEM ADMINISTRATION	REPORT AND ANALYSIS	USER MANAGEMENT	
USERS Users Roles	List Users ADD SHOW EDIT DELET	E	10 Per Page	Show All Roles
	Login ID Full Name ngadmin Administrator NGTrace	Email ngadmin@example.com	Login Roles logon Administer NGTrace	Receive Rpt Host Groups

© 2008-2009 NGTraceManager. All Rights Reserved NG Trace v1.0 b100 Rails 2.3.2 Env production

Figure 2. User Management Tab

User information contains user login ID, user name, e-mail address, phone nu mber, registered date, modified date, option whether or not to receive notify i nformation from notifier, login status, login date/time, user role, manageable host groups, description and etc.

• [ADD] :

Register new user.

Enter user information of new user.

Login ID and e-mail address should not be same as the ones of already registered users.

Symbol "*" indicates mandatory fields. If mandatory field is left blank, user registration is not processed.

If user role "Administer NG Trace" is selected, other user role options become disabled. "Groups" item becomes activated only if user role "Group Part Admin" or "Group Part Viewer" is selected.

					Logouτ Logouτ
NG TRACE	SYSTEM ADMINI	STRATION	REPORT AND ANALYSIS	USER MANAGEMENT	
USERS Users Roles	New User Listall users				
	Isername				
	Email				
	Last llame				
	Phone II umber	NO RE			
	Report Receiver Password				
	Confirm Pessword				
	Description				
	Poles	Ad mit Analy Analy Syste Syste Iser Grou Grou	ninister IIGT moe yas Adıministnator yas Newer am Adıministnator am Viewer -Adıministnator -Vewer up Part Adımin up Part Viewer		
	Groups(This user can	manage host	groups as below) p1 p2		
		SAVE			

Figure 3. Add User

• [SHOW]

We can view selected User's information.

User's Information includes the Login ID, Name, Email Addre ss, phone number, creation date/time, update date/time, Logon Status, Roles, Host Groups, and Description.

"Create at" indicates created time and "Update at" represents u pdated time.

Logon Status shows login state if user is login.

USERS USer S Show User Information Of Ngadmin Roles LIST ALL USERS Login ID: ngadmin Name: Administrator NGTrace Email Address: ngadmin@example.com Phone Number: 0415235634433 Created at: 2009-08-15 02:42:38 UTC Updated at: 2009-11-20 18:00:50 UTC Report Receiver: true Logon Status: Logon Logon Time: 2009-11-20 18:00:50 UTC Roles: Administer NGTrace Description default admininstrator	NG TRACE ^{©©} Enterprise Security System	SYSTEM ADMINISTRATION	REPORT AND ANALYSIS USER MANAGEMENT
Roles LIST ALL USERS Login ID : ngadmin Name : Administrator NGTrace Email Address : ngadmin@example.com Phone Number : 0415236534433 Created at : 2009-08-15 02:42:38 UTC Updated at : 2009-11-20 18:00:50 UTC Report Receiver : true Logon Status : Logon Logon Time : 2009-11-20 18:00:50 UTC Roles : Administer NGTrace Description default administrator	JSERS Jsers O	Show User Information Of Ng	jadmin
Login ID :ngadminName :Administrator NGTraceEmail Address :ngadmin@example.comPhone Number :0415235634433Created at :2009-08-15 02:42:38 UTCUpdated at :2009-11-20 18:00:50 UTCReport Receiver :trueLogon Status :LogonLogon Time :2009-11-20 18:00:50 UTCRoles :Administer NGTraceDescriptiondefault administrator	Roles O	LIST ALL USERS	
Name :Administrator NGTraceEmail Address :ngadmin@example.comPhone Number :0415235634433Created at :2009-08-15 02:42:38 UTCUpdated at :2009-11-20 18:00:50 UTCReport Receiver :trueLogon Status :LogonLogon Time :2009-11-20 18:00:50 UTCRoles :Administer NGTraceDescriptiondefault administrator		Login ID :	ngadmin
Email Address :ngadmin@example.comPhone Number :0415235634433Created at :2009-08-15 02:42:38 UTCUpdated at :2009-11-20 18:00:50 UTCReport Receiver :trueLogon Status :LogonLogon Time :2009-11-20 18:00:50 UTCRoles :Administer NGTraceDescriptiondefault admininstrator		Name :	Administrator NGTrace
Phone Number :0415236634433Created at :2009-08-15 02:42:38 UTCUpdated at :2009-11-20 18:00:50 UTCReport Receiver :trueLogon Status :LogonLogon Time :2009-11-20 18:00:50 UTCRoles :Administer NGTraceDescriptiondefault admininstrator		Email Address :	ngadmin@example.com
Created at : 2009-08-15 02:42:38 UTC Updated at : 2009-11-20 18:00:50 UTC Report Receiver : true Logon Status : Logon Logon Time : 2009-11-20 18:00:50 UTC Roles : Administer NGTrace Description default admininstrator		Phone Number :	0415235634433
Updated at : 2009-11-20 18:00:50 UTC Report Receiver : true Logon Status : Logon Logon Time : 2009-11-20 18:00:50 UTC Roles : Administer NGTrace Description default admininstrator		Created at :	2009-08-15 02:42:38 UTC
Report Receiver : true Logon Status : Logon Logon Time : 2009-11-20 18:00:50 UTC Roles : Administer NGTrace Description default admininstrator		Updated at :	2009-11-20 18:00:50 UTC
Logon Status : Logon Logon Time : 2009-11-20 18:00:50 UTC Roles : Administer NGTrace Description default administrator		Report Receiver :	true
Logon Time : 2009-11-20 18:00:50 UTC Roles : Administer NGTrace Description default administrator		Logon Status :	Logon
Roles : Administer NGTrace Description default adminingtrator		Logon Time :	2009-11-20 18:00:50 UTC
Description default administrator		Roles :	Administer NGTrace
		Description	default admininstrator

Figure 4. Show User Information

• [EDIT]

You can edit information and password of registered user here. If user role "Administer NG Trace" is selected, other user role options become disabled. "Groups" item becomes activated only if user role "Group Part Admin" or "Group Part Viewer" is selected.

Enterprise Security system	SYSTEM ADM	NISTRATION REPORT AND ANALYSIS USER MANAGEMENT	
HOEDO			
Users D	Edit User 'Ngad		
Roles O	LIST ALL USERS	CHANGE PASSWORD	
	Isemame	ngadmin	
	Emeti	nqadmin@example.com	
	First llame	Administrator	
	Last llame	NGTrace	
	Die ee Humber	0415235634433	
	Phone Rumber		
	Report Receiver		
	Description	default admininstrator	
	Roles	Administer IIGTinoce Analysis Administrator Analysis Viewer System Administrator System Viewer Iser Administrator Iser Wewer Group Part Admin Group Part Viewer	
	Groups(This user ca	in manage host groups as below) ვიადი I ვიადი 2	
		SAVE	

Figure 5. Edit User

To change the Password, input new Password and Confirm Pas sword, press [SAVE].

NG TRACE ^{©©} Enterprise Security System	SYSTEM ADMINISTRATION REPORT AND ANALYSIS USER MANAGEMENT	ngadmin Logout
USERS Users O Roles O	Set New Password LIST ALL USER EDIT USER	
	Password Confirm Password SAVE	
	© 2008-2009 N NG Trace v	IGTraceManager. All Rights Reserved 1.0 b100 Rails 2.3.2 Env development

Figure 6. Set New Password

• [DELETE]

You can delete selected User from user list.

3.3 User Privilege

NG Trace Management Console provides several user privileges such as Adm inister NGTrace, Analysis Administrator, Analysis Viewer, System Administrat or, System, Viewer, User Administrator, User Viewer, Group Part Admin and Group Part Viewer.

- Administer NG Trace
 The user of an account with Administer NG Trace privilege has all
 privilege of NG Trace System.
 That is, can manage all information within SYSTEM ADMINISTRATION
 page and REPORT AND ANALYSIS page and USER MANAGEMENT.
- Analysis Administrator

The user with this privilege has access to all functionalities of REPORT AND ANALYSIS page.

• Analysis Viewer

The user with this privilege can only view information of REPORT AND ANALYSIS page.

- System Administrator The user with this privilege has access to all functionalities of SYSTEM ADMINISTRATION page.
- System viewer

The user with this privilege can only view information of SYSTEM ADMINISTRATION page.

- User Administrator
 The user with this privilege has access to all functionalities of USER MANAGEMENT page.
- User Viewer The user with this privilege can only view information of USER MANAGEMENT page.
- Group Part Admin
- Group Part Viewer

4. Report and Analysis

4.1 Logs and Audits

4.1.1 Whole

Show list of stored Logs and audits in selected DB.

LOGS AND AUDITS Whole Log List Of STOREDDB ICMP 2009-11-13 00:00 All Types All Target Enter host ip or name 10 Per Page E-mail Date-Time Source Destination Type Protocol Rule Info M O Date-Time Source Destination Type Protocol Rule Info ITTP O Oug-11-17 09:21:24 166.172:11 24 224.00.2 ICMP Audit Rotorescilotation view mu SEARCH O09-11-16 12:06:40 192.168.1.1 192.168.7.88 ICMP IOMP Audit Echo (ping) request view mu Select Database 009-11-18 12:06:40 192.168.7.88 192.168.1.1 ICMP Audit Echo (ping) request view mu Select Database 009-11-18 12:06:39 192.168.7.88 192.168.1.1 ICMP Audit Echo (ping) request view mu Select Database 009-11-18 12:06:39 192.168.7.88 ISCMP ICMP Audit Echo (ping) request view mu									
Whole Wildle Cog List of of of clocob ICMP 2009-11-13 00:00 All Types All Target Enter host ip or name 10 Per Page Email Date-Time Source Destination Type Protocol Rule Info IM O Date-Time Source Destination Type Protocol Rule Info IM O Date-Time Source Destination Type Protocol Rule Info IM O Date-Time Source Destination Type Protocol Rule Info IM O Date-Time Source Destination Type Protocol Rule Info IM O Date-Time Source Destination Type Protocol Rule Roder solidation: wiew multication: Standard 192:168.1.1 192:168.7.8 ICMP ICMP Audt Echo (ping) reply: N wiew multication: Select Database 192:168.7.8 192:16	LOGS AND AUDITS		Whole Log List		۱R				
ICMP 2009-11-13 00:00 All Types All Target Enter hostip or name 10 Per Page E-mail Date-Time Source Destination Type Protocol Rule Info IM O 2009-11-17 09:21:24 166.172.11.24 224.0.0 ICMP Audt Roder solicitation: view mu File Transfer 009-11-16 12.06.40 192.168.1.1 192.168.7.88 ICMP ICMP Audt Redrect Redrect f view mu SEARCH 2009-11-16 12.06.40 192.168.1.1 192.168.1.4 ICMP ICMP Audt Redrect Redrect f view mu Search 009-11-16 12.06.40 192.168.7.88 192.168.1.4 ICMP ICMP Audt Echo (ping) request view mu Search 009-11-16 12.06.39 192.168.7.88 192.168.1.4 ICMP ICMP Audt Echo (ping) request view mu Search 009-11-16 12.06.39 192.168.7.88 192.168.7.88 ICMP ICMP Audt Echo (ping) request view mu <	Whole	0							
Email Date-Time Source Destination Type Protocol Rule Info IM 0 2003-11-17.08:21:24 186.172:11:24 224.0.0.2 ICMP ICMP Audt Router solicitation: view m File Transfer 2003-11-17.08:21:24 186.172:11:24 224.0.0.2 ICMP ICMP Audt Router solicitation: view m SEARCH 2003-11-18.12.06:40 192.168.1.1 192.168.1.1 ICMP Audt Echo (ping) request view m 2003-11-18.12.06:40 192.168.1.77 192.168.1.8 ICMP ICMP Audt Echo (ping) request view m 2003-11-18.12.06:40 192.168.1.8 192.168.1.1 ISCMP ICMP Audt Echo (ping) request view m 2003-11-18.12.06:39 192.168.7.88 ISCMP ICMP Audt Echo (ping) reply: N view m Select Database 0003-11-16.12.06:39 192.168.7.88 ISCMP ICMP Audt Echo (ping) reply: N view m 2003-11-16.12.06:39 192.168	ICMP	0	2009-11-13 00:00	All Types	\$ All	Target	Ente	er host ip	orname 10 Per Page
IM O 2009-11.17 09:21:24 186.172.11.24 224.0.0.2 ICMP ICMP Audit Router solicitation view me File Transfer 2009-11.16 12:06:40 192.168.1.1 192.168.7.88 ICMP ICMP Audit Echo (ping) request view me SEARCH 2009-11.18 12:06:40 192.168.1.77 192.168.7.88 ICMP ICMP Audit Echo (ping) request view me Search 009-11.18 12:06:40 192.168.7.88 ISCMP ICMP Audit Echo (ping) request view me 009-11.18 12:06:40 192.168.7.88 ISCMP ICMP Audit Echo (ping) request view me 009-11.18 12:06:39 192.168.7.88 ISCMP ICMP Audit Echo (ping) request view me Select Database 009-11.18 12:06:39 192.168.7.88 ISCMP ICMP Audit Echo (ping) reply: N view me 009-11.18 12:06:39 192.168.7.88 ISCMP ICMP Audit Echo (ping) reply: N view me 009-11.18 12:06:39 19	E-mail	0	Date-Time	Source	Destination	Type	Protocol	Rule	Info
HTTP Constrained Router solution With million File Transfer 2009-11-16 12.06.40 192.168.1.1 192.168.7.88 ICMP ICMP Audit Echo (ping) request wiew million SEARCH 2009-11-18 12.06.40 192.168.1.1 192.168.7.88 ICMP ICMP Audit Echo (ping) request wiew million DATABASE 2009-11-18 12.06.40 192.168.1.1 192.168.7.88 ICMP ICMP Audit Echo (ping) request wiew million DATABASE 2009-11-18 12.06.40 192.168.7.88 192.168.1.1 ICMP Audit Echo (ping) reply: N wiew million Select Database 2009-11-18 12.06.39 192.168.7.88 192.168.1.1 ICMP Audit Echo (ping) reply: N wiew million Coop-11-18 12.06.39 192.168.1.1 192.168.7.88 ICMP ICMP Audit Echo (ping) reply: N wiew million Coop-11-18 12.06.39 192.168.1.1 192.168.7.88 ICMP ICMP Audit Echo (ping) reply: N wiew million 2009-11-18 12.06.38	IM	0	2009-11-17 09:21:24	186.172.11.24	224.0.0.2	ICMP	ICMP	Audit	
File Transfer 2003-11-18 12:08:30 132:188:1.1 132:188:7.80 1CMP ICMP Audit Echo (sing) request view m SEARCH 2003-11-18 12:08:40 192:188:1.77 192:188:1.1 ICMP Audit Redirect: Redirect f view m DATABASE 2003-11-18 12:08:40 192:168:1.8 192:168:1.1 ICMP Audit Echo (sing) request view m DATABASE 2003-11-18 12:06:40 192:168:7.88 192:168:1.1 ICMP Audit Echo (sing) request view m Select Database 2003-11-18 12:06:39 192:168:7.88 192:168:1.1 ICMP Audit Echo (sing) reply: N view m CEXPORT 2003-11-18 12:06:39 192:168:1.1 192:168:7.88 ICMP ICMP Audit Echo (ping) reply: N view m 2003-11-18 12:06:39 192:168:1.1 192:168:7.88 ICMP ICMP Audit Echo (ping) reply: N view m 2003-11-18 12:06:39 192:168:1.1 192:168:7.88 ICMP ICMP Audit Echo (ping) reply: N view m <	HTTP	0	2000 14 10 12 00 10	10240244	100 400 7 00	ICHID	1010	0	Router solicitation: view m
SEARCH 2009-11-18 12.06.40 192.168.1.77 192.168.1.1 ICMP Audit Redirect. Redirect f view m Search 0 0.03-11-18 12.06.40 192.168.1.8 192.168.7.88 ICMP Audit Echo (ping) respecti view m DATABASE 009-11-18 12.06.30 192.168.7.88 192.168.1.1 ICMP Audit Echo (ping) respecti view m Select Database 009-11-18 12.06.39 192.168.7.88 192.168.1.1 ICMP Audit Echo (ping) respecti view m Coop-11-18 12.06.39 192.168.1.1 192.168.7.88 ICMP ICMP Audit Echo (ping) respecti view m 2009-11-18 12.06.39 192.168.1.1 192.168.7.88 ICMP ICMP Audit Echo (ping) respecti view m 2009-11-18 12.06.38 192.168.1.1 192.168.7.88 ICMP ICMP Audit Echo (ping) respecti view m 2009-11-18 12.06.38 192.168.7.88 IS2.168.1.1 IS2.168.1.1 IS2.168.1.1 ICMP Audit Echo (ping) respect view m <	File Transfer	0	2009-11-10 12:06:40	192.100.1.1	192.100.7.00	ICMP	ICHIP	Audit	Echo (ping) request: view m
Search 2009-11-16 12.06.40 192.168.7.88 ICMP ICMP Audt Echo (ping) request view mage DATABASE 2009-11-16 12.06.40 192.168.7.88 192.168.1.1 ICMP ICMP Audt Echo (ping) request view mage Select Database 2009-11-16 12.06.39 192.168.7.88 192.168.1.1 ICMP ICMP Audt Echo (ping) reply: N view mage Exported Tables 009-11-16 12.06.39 192.168.1.1 192.168.7.88 ICMP ICMP Audt Echo (ping) reply: N view mage 2009-11-16 12.06.39 192.168.1.1 192.168.7.88 ICMP ICMP Audt Echo (ping) reply: N view mage 2009-11-16 12.06.39 192.168.1.1 192.168.7.88 ICMP ICMP Audt Echo (ping) reply: N view mage 2009-11-16 12.06.38 192.168.7.88 192.168.7.18 IS2.168.1.1 ICMP Audt Echo (ping) reply: N view mage 2009-11-16 12.06.38 192.168.7.88 192.168.7.18 IS2.168.1.1 ICMP Audt Echo (ping) reply	SEARCH		2009-11-18 12:06:40	192.168.1.77	192.168.1.1	ICMP	ICMP	Audit	Redirect: Redirect f view m
DATABASE 2009-11-18 12:06:39 192:168.7.88 192:168.1.1 ICMP Audit Echo (ping) reply: N view m Select Database 2009-11-18 12:06:39 192:168.7.88 192:168.1.1 ICMP Audit Echo (ping) reply: N view m ExpORT 2009-11-18 12:06:39 192:168.1.1 192:168.7.88 ICMP ICMP Audit Echo (ping) reply: N view mu 2009-11-18 12:06:39 192:168.1.1 192:168.7.88 ICMP ICMP Audit Echo (ping) reply: N view mu 2009-11-18 12:06:39 192:168.1.1 192:168.7.88 ICMP ICMP Audit Echo (ping) reply: N view mu 2009-11-18 12:06:38 192:168.7.88 IS2:168.1.1 IS2:168.7.88 ICMP Audit Echo (ping) reply: N view mu 2009-11-18 12:06:38 192:168.7.88 IS2:168.1.1 ICMP Audit Echo (ping) reply: N view mu 2009-11-18 12:06:38 192:168.7.88 192:168.7.88 IS2:168.7.84 ICMP Audit Echo (ping) reply: N view mu 2009-11	Search	0	2009-11-18 12:06:40	192.168.1.1	192.168.7.88	ICMP	ICMP	Audit	Echo (ping) request: view m
Select Database 2009-11-18 12:06:39 192:168.7.88 192:168.1.1 ICMP Audit Echo (ping) reply; N view m Exported Tables 2009-11-18 12:06:39 192:168.1.1 192:168.7.88 ICMP ICMP Audit Echo (ping) reply; N view m 009-11-18 12:06:39 192:168.1.1 192:168.7.88 ICMP ICMP Audit Echo (ping) reply; N view m 009-11-18 12:06:39 192:168.1.1 192:168.7.88 ICMP ICMP Audit Echo (ping) reply; N view m 009-11-18 12:06:38 192:168.7.88 ISCMP ICMP Audit Echo (ping) reply; N view m 009-11-18 12:06:38 192:168.7.88 ISCMP ICMP Audit Echo (ping) reply; N view m 009-11-18 12:06:38 192:168.7.88 ISCMP ICMP Audit Echo (ping) reply; N view m 009-11-18 12:06:38 192:168.7.88 ISCMP ICMP Audit Echo (ping) reply; N view m	DATABASE		2009-11-18 12:06:39	192.168.7.88	192.168.1.1	ICMP	ICMP	Audit	Echo (ping) reply: N view m
EXPORT 2009-11-18 12:06:39 192:168.7.88 ICMP IOMP Audit Echo (ping) request view mage 2009-11-18 12:06:38 192:168.7.88 ISCMP IOMP Audit Echo (ping) request view mage 2009-11-18 12:06:38 192:168.7.88 ISCMP ICMP Audit Echo (ping) request view mage 2009-11-18 12:06:38 192:168.7.88 192:168.1.1 ICMP Audit Echo (ping) reply: N view mage 2009-11-18 12:06:38 192:168.7.88 192:168.1.1 ICMP Audit Echo (ping) reply: N view mage 2009-11-18 12:06:38 192:168.7.88 192:168.1.1 ICMP Audit Echo (ping) reply: N view mage	Select Database	0	2009-11-18 12:06:39	192.168.7.88	192.168.1.1	ICMP	ICMP	Audit	Echo (ping) reply: N view m
Exported Tables 2009-11.18 12.06:39 192.168.1.1 192.168.7.88 ICMP ICMP Audit Echo (ping) request view model 2009-11.18 12.06:38 192.168.7.88 192.168.1.1 ICMP ICMP Audit Echo (ping) request view model 2009-11.18 12.06:38 192.168.7.88 192.168.1.1 ICMP ICMP Audit Echo (ping) repty: N view model 2009-11.18 12.06:38 192.168.7.88 192.168.1.1 ICMP ICMP Audit Echo (ping) repty: N view model	EXPORT		2009-11-18 12:06:39	192.168.1.1	192.168.7.88	ICMP	ICMP	Audit	Echo (ping) request: view m
2009-11-18 12:06:38 192:168.7.88 192:158.1.1 ICMP ICMP Audit Echo (ping) reply: N view mu 2009-11-18 12:06:38 192:168.7.88 192:168.1.1 ICMP Audit Echo (ping) reply: N view mu	Exported Tables	0	2009-11-18 12:06:39	192.168.1.1	192.168.7.88	ICMP	ICMP	Audit	Echo (ping) request: view m
2009-11-18 12:06:38 192:168:7.88 192:168:1.1 ICMP ICMP Audit Echo (ping) reply; N view mo			2009-11-18 12:06:38	192.168.7.88	192.168.1.1	ICMP	ICMP	Audit	Echo (ping) reply: N view m
			2009-11-18 12:06:38	192.168.7.88	192.168.1.1	ICMP	ICMP	Audit	Echo (ping) reply: N view m
Displaying 1 - 10 of 9704 K ≤ Page 1 of 971 ≥ 34			Displaving 1 - 10 of 9704		i< <	Page 1	of 971 ≥ >I		

Figure 7. Whole Log List

The following information displays contents of recorded whole log.

- Date Time: Captured time.
- Source: IP Address of Source.
- Destination: IP Address of Destination.
- Type: Type of communication protocol.
- Protocol: Type of sub protocol.
- Rule: Target information.
- Info: Summarize information of carried contents. [view more]: Can see detail information of carried contents.

User can filter Whole Log List by Date-Time, Protocol, Target, Host, and Page.

2009-11-13.00:00 🔍	All Types	\$ All Target	٥.	Enter host ip or name	10 Per Page	4 *	
					and the second se	_	187

Figure 8. Result Filter of Whole Log List

- Date - Time Filter



Figure 9. Date – Time Filter

Filter whole Log List by date - time.

It shows all logs recorded since specified date/time to current date/time.

- Type filter

All Types	-
All Types	
ICMP	natio
E-Mail	1.103
IM	
HTTP	1.103
File Transfer	1.103

Figure 10. Protocol Filter

It allows filtering whole Log List by Protocol. It shows searched result by selected protocol.

For example, if selected E-mail protocol, user can see only E-mail communication log.

- Target Filter



Figure 11. Target Filter

It allows filtering Whole Log List by Target.

It shows searched result by selected target.

For example, if "Log" is selected, user can see only logs.

- Host Filter

102 168 1 103	
132.100.1.103	

Figure 12. Host Filter

Allow filtering Whole Log List by name or address of host. It shows searched result by selected host.

For example, if you enter 192.168.1.103, logs and audits containing 192.168.1.103 as its source or target IP address are filtered.

Or you can specify host name "powercom" instead of its IP address.

- Page Filter



Figure 13. Page Filter

Filter Whole Log List by Page.

User can see only log as much as selected number. For example, if selected 10 per Page, you can see 10 logs in one page.

4.1.2 ICMP

Show list of stored ICMP Communication Logs in selected DB.

LOGS AND AUDITS	ICMP Log List Of S					
Whole				1993 1		
ICMP (EXPORT DETAIL		2009-11-13 (00:00 🖸 Enter ho	stip or name 10 F	Per Page 😂
E-mail (Date-Time	Source	Destination	Message Type	Message Code	Size
IM (2009-11-19 19:10:59	192.168.1.1	192.168.1.77	0: Echo (ping) reply	0: No code	56
HTTP File Transfer	2009-11-19 19:10:59	192.168.1.77	192.168.1.1	8: Echo (ping) request	0: No code	56
CEADOU	2009-11-19 19:10:58	192.168.1.1	192.168.1.77	0: Echo (ping) reply	0: No code	56
Search (2009-11-19 19:10:58	192.168.1.77	192.168.1.1	8: Echo (ping) request	0: No code	56
DATABASE	2009-11-19 19:10:57	192.168.1.77	192.168.1.1	8: Echo (ping) request	0: No code	56
Select Database	2009-11-19 19:10:57	192.168.1.1	192.168.1.77	0: Echo (ping) reply	0: No code	56
EXPORT	2009-11-19 19:10:56	192.168.1.1	192.168.1.77	0: Echo (ping) reply	0: No code	56
Exported Tables	2009-11-19 19:10:56	192.168.1.77	192.168.1.1	8: Echo (ping) request	0: No code	56
	2009-11-19 19:10:55	192.168.1.77	192.168.1.1	8: Echo (ping) request	0: No code	56
	2009-11-19 19:10:55	192.168.1.1	192.168.1.77	0: Echo (ping) reply	0: No code	56
	Displaying 1 - 10 of 9206		K < Page	of 921 💙 🔰		

Figure 14. ICMP Log List

The following information indicates contents of recorded ICMP log.

- Date Time: Captured time.
- Source: IP Address of Source.
- Destination: IP Address of Destination.
- Message Type: ICMP message type.
- Message Code: Message code information.
- Size: ICMP packet length.

Can filter ICMP Log List by Date-Time, Host, Page.

2009-11-13 00:00 🖸 Enter host ip or name 10. Per Page 🗘

Figure 15. Result Filter of ICMP Log

• [EXPORT]

Export the ICMP Log as CSV file.

When receiving the following message, click OK, then ICMP Log is exported as CSV file.



Figure 16. Export message.

• [DETAIL]

View detailed information of ICMP Log.

NG TRAC	E ®©					ngadmin Logout
Enterprise Security	System	SYSTEM ADMIN	ISTRATION	REPORT AND ANALYSIS	USER MANAGEMENT	
	_	_	_			
LOGS AND AUDITS		ICMP Detail				
Whole	0					
ICMP	0	BACK				
E-mail	0	Classific	Contents	3		
IM	0	Date-Time:	2009-11-19	19:10:59		
нттр	0	Source Address:	10016911			
File Transfer	0		102.100.1.1			
SEADCH		Destination Address:	192.168.1.7	7		
Search	0	Message Type:	0: Echo (pin	ng) reply		
Search		Message Code:	0: No code			
DATABASE		Size:	56			
Select Database	0	Information:	Echo (ping)	reply: No code		
EXPORT						
Exported Tables	0					
	- 1					
	- 1					
	- 1					
	L					
					© 2008-2009	NGTraceManager. All Rights Reserved

Figure 17. ICMP Detail

4.1.3 E-mail

Display list of stored E-mail Communication Logs in selected DB.

LOGS AND AUDITS		12000 2001							
Whole	0	E-mail Log Li	st Of STOR	EDDB					
ICMP	0	EXPORT DET	AIL		2009-11-	-13 00:00 🔍	Enter host ip o	orname 10 Per P	age 🔅
E-mail	0	Date-Time	Source	Destination	Protocol	subject	sender	receiver	Attachs
IM	0	2000 11 12	103 169 1 77	102.169.1.99	1101000	HUCHULM	root	nek@meil.koc.com	2
нттр	0	16:43:30	132,100.1.77	132,100,1.00	pops	2	root	ракадианское.com	2
File Transfer	0	2009-11-18 16:43:25	192.168.1.77	192.168.1.88	smtp	너어디어나어 ?	root	pak@mail.kcc.com	2
SEARCH		2009-11-18	192.168.1.77	192.168.1.88	smtp	fjkldsfja;lflkajdl;	root	pak@mail.kcc.com	3
Search	0	2009-11-18	192.168.1.77	192.168.1.88	smtp	test mail (pop3)	root	pak@mail.kcc.com	0
DATABASE Select Database	0	2009-11-18 16:27:09	192.168.1.77	192.168.1.88	imap	welcome test mail	root	pak@mail.kcc.com	2
EXPORT		2009-11-18 16:26:40	192.168.1.77	192.168.1.88	smtp	welcome test mail	root	pak@mail.kcc.com	2
Exported Tables	0	2009-11-18 16:24:45	192.168.1.77	192.168.1.88	imap	123345	pak	ri@mail.kcc.com	0
		2009-11-18 16:24:09	192.168.1.77	192.168.1.88	smtp	123345	pak	ri@mail.kcc.com	0

Figure 18. E-mail Log List

The following information indicates contents of recorded E-mail log.

- Date Time: Captured time.
- Source: IP Address of Source.
- Destination: IP Address of Destination.
- Protocol: Type of E-mail.
- Subject: E-mail's subject.
- Sender: E-mail Sender.
- Receiver: E-mail Receiver.
- Attaches: Attached files.

Filter E-mail Log List by Date-Time, Host, and Page.



Figure 19. Result Filter of E-mail Log

• [EXPORT]

Export the E-mail Log as CSV file.

When receiving the following message, click OK, then ICMP Log is exported as CSV file.



Figure 20. Export message.

• [DETAIL]

View detailed information of E-mail Log.

G TRAC	E ®C	í.				
terprise Security	System	SYSTE	M ADMINISTRATION	REPORT AND ANALYSIS	USER MANAGEMENT	
OGS AND AUDITS						
hole	0	E-mail Deta	ail			
MP	0	BACK				
mail	0	Date-Time:	2009-11-18 16:26:40			
1	0	Source Address:	192.168.1.77			
TTP	0	Destination Addre	ss:192.168.1.88			
lo Transfor	0	To:	pak@mail.kcc.com	1>		
le manstel	0	Subject:	welcome test mail			
EARCH	-	Attachs:	2 files test soan server rhii	nstall log		
earch	0	pongpang test ma	il computer numeric	control		
ATABASE						
elect Database	0	1				
KPORT	_					
xported Tables	0	1				
		1				

Figure 21. E-mail Detail.

4.1.4 IM

Display list of stored IM Communication Logs in selected DB.

NG TRAC	CE ^{®©}						8	ngadmin Log
Enterprise Security	System	SYSTEM ADM	IINISTRATION	REPORT AND ANALYS	IS USI	ER MANAGEMEN	IT	
	_					_	_	
LOGS AND AUDITS		IM Log List Of S	TOREDDB					
Whole	0			0000.00	02.00.00	All Lie ste	÷ 10	
ICMP	0	EXPORT		2008-05	-03 00:00	All Hosts	- 10	Per Page
E-mail		Date-Time	Source	Destination	Туре	Server	Up/Down	Contents
IM	0	2009-06-09 00:00:00	192.168.1.103	192.168.1.106	Skype	skype	Down	? ? ??? ???
нпр	0	2009-08-12 11:15:03	192.168.1.107	192.168.1.101	JABBER	hahaha	Up	mt.exe
Select Database	0							
Exported Tables	0							

Figure 22. IM Log List

The following information indicates contents of recorded IM log.

- Date Time: Captured time.
- Source: IP Address of Source.
- Destination: IP Address of Destination.
- Type: Sub type of IM protocol.
- Server: Name of Server.
- Up/Down: Upload/Download.
- Contents: Message text, file name.

Filter IM Log List by Date-Time, Host, and Page.

2009-11-13 00:00	2	Enter host ip or name	10 Per Page	\$

Figure 23. Result Filter of IM Log

• [EXPORT]

Export the IM Log as CSV file.

When receiving the following message, click OK, then ICMP Log is exported as CSV file.



Figure 24. Export message.

4.1.5 HTTP

Display list of stored HTTP Communication Logs in selected DB.

LOGS AND AUDITS						
Whole	0	HTTP Log Lis	I OF RECEN	NTDB- 192.16	8.1.144	
ICMP	0	EXPORT DETA	L		2009-11-13	00:00 🤦 Enter host ip or name 10 Per Page 🗘
E-mail	0	Data-Tima	Qource	Destination	Method	1101
IM	0	Dates Inne	3001C8	Destination	Wethou	
нттр	0	2009-11-20 15:06:47	192.168.1.88	192.168.1.144	GET	http://192.168.1.144/ts/file/index.php?img=favicon
File Transfer	0	2009-11-20 15:06:37	192.168.1.88	192.168.1.144	GET	http://192.168.1.144#s/file/view?path=%27ngt_lelxKkfilePh
SEARCH		2009-11-20	192.168.1.88	192.168.1.202	GET	http://192.168.1.202/report/Report/contents?proto=4&id=9745
Search	0	13.00.22				
	_	2009-11-20 15:04:40	192.168.1.88	192.168.1.34	GET	http://192.168.1.34/mysois
DATABASE Select Database	0	2009-11-20 15:03:51	192.168.1.88	192.168.1.202	GET	http://192.168.1.202/report/report/?proto=4
EXPORT		2009-11-20 15:03:39	192.168.1.88	192.168.1.34	GET	http://192.168.1.34/mysois/
Exported Tables	0	2009-11-20 15:03:38	192.168.1.88	192.168.1.34	GET	http://192.168.1.34/index.html
		2009-11-20 15:03:11	192.168.1.88	192.168.1.202	GET	http://192.168.1.202/networkadmin/exe_components

Figure 25. HTTP Log List

The following information indicates contents of recorded IM log.

- Date Time: Captured time.
- Source: IP Address of Source.
- Destination: IP Address of Destination.
- Method: HTTP method.
- URL: URL of visit web site.
- Cookie: Cookie information.

Filter HTTP Log List by Date-Time, Host, and Page.

2009-11-13 00:00 🖸 Enter host ip or name 10. Per Page 📫

Figure 26. Result Filter of HTTP Log

• [EXPORT]

Export the HTTP Log as CSV file.

When receiving the following message, click OK, then ICMP Log is exported as CSV file.



Figure 27. Export message.

• [DETAIL] View detailed information of HTTP Log.

NG TRAC	System	SYSTEM ADM	INISTRATION	REPORT AND ANALYSIS	USER MANAGEMENT
	_				
LOGS AND AUDITS	-	HTTP Detail			
Whole	0				
ICMP	0	BACK			
E-mail	0	Classific	Contents		
IM	0	Date-Time:	2009-11-20 15:0	13:11	
нттр	0	Carriera da la la caraci	402.400.4.00		
File Transfer	0	Source Address:	192.168.1.88		
		Destination Address:	192.168.1.202		
SEARCH		Method:	GET		
Search	0	Cookie:	_source_sessio aVV9uc3sHOg1v bml0b3JfaVVQvv	n=BAh7DDoPc2Vzc2lvbl9pZCllOTRiOT vZXJfcGFnZTA6CXBhZ2UwOhhoaVVd 0qxvX3Byb3RvMDslMDoLb19uYVV1	3ZGFJY2MxY2NjNzViNzRIYTMyMTZjNzAwNDE6FG1vbml0b3.fb3B0 ox2ZpbHRicl9vcHRpb25zexA7BzA6DW9fdGFyZ2V0MDoMb19jcml0aTA6D21v
DATABASE Select Database	0	Content Type:	text/html; charse	st=utf-8	
Select Database		1101	http://403.469.4	202/patworkadmin/ova_aomnana	nto.
EXPORT		one.	11(1)	.zoznictworkddminieke_compone	
Exported Tables	0	Information:	HTTP///ebdav/O	ther: The client host <192.168.1.88> w	as tried to connect to or get . Result code: http/1.0 1.1 200:OK Response.
					© 2008-2009 NGTraceManager. All Rights Resen NG Trace v1.0 b100 Rails 2.3.2 Env product

Figure 28. HTTP Detail

4.1.6 FTP

Display list of stored FTP Communication Logs in selected DB.

interprise Security	System	SY	STEM ADMINIST	RATION REP	Port and an	ILYSIS USE	R MANAGEMENT	
OGS AND AUDITS	_				_	_	_	_
Whole	0	FTP Log	J List Of ST	OREDDB				
CMP	0	EXPORT	DETAIL		1902-0	11-08 00:00	Enter host ip or name	10 Per Page 😂
-mail	0	Date-	Source	Destination	Protocol	LIRI	Comma	and Arguments
Л	0	Time		beetination	, 1010001	0.112	J	ing ingenetic
ттр	0	2009-11-19 18:53:58	192.168.1.77	192.168.1.103	NFS	nfs://192.168.1.103	ACCESS	/osi-utils.c
ile Transfer	0	2009-11-19 18:53:37	192.168.1.77	192.168.1.103	NFS	nfs://192.168.1.103	ACCESS	∏ ℓ
EARCH		2009-11-19 18:53:37	192.168.1.77	192.168.1.103	NFS	nfs://192.168.1.103	ACCESS	/centos5.1 server setup.pdf
earch	0	2009-11-19 18:52:04	192.168.1.77	192.168.1.103	NFS	nfs://192.168.1.103	ACCESS	/system-config-bin 4.0.3-4.el
DATABASE		2009-11-19 18:52:02	192.168.1.77	192.168.1.103	NFS	nfs://192.168.1.103	ACCESS	
elect Database	0	2009-11-19 18:51:03	192.168.1.77	192.168.1.103	NFS	nfs://192.168.1.103	ACCESS	/test0
XPORT		2009-11-19 18:51:03	192.168.1.77	192.168.1.103	NFS	nfs://192.168.1.103	READDIRPL	.US /test0
xported Tables		2009-11-19 18:50:57	192.168.1.77	192.168.1.103	NFS	nfs://192.168.1.103	ACCESS	/test1/test00/New Folder/saa/a
		2009-11-19 18:50:56	192.168.1.77	192.168.1.103	NFS	nfs://192.168.1.103	ACCESS	/test1/test00/New Folder/saa
		2009-11-19 18:50:55	192.168.1.77	192.168.1.103	NFS	nfs://192.168.1.103	ACCESS	/test1/test00/New Folder/aa
		Displaying 31	- 40 of 407		K ≮ P	age 4 of 41 >	×	

Figure 29. FTP Log List

The following information indicates contents of recorded FTP log.

- Date Time: Captured time.
- Source: IP Address of Source.
- Destination: IP Address of Destination.
- Protocol: Type of file transfer protocol such as FTP and SMB
- URL: URL of visited web site
- Command: Request command.
- Arguments: Information of communication file.

Filter FTP Log List by Date-Time, Host, and Page.

2009-11-13 00:00 🖸 Enter host ip or name 10 Per Page 🗘

Figure 30. Result Filter of FTP Log

• [EXPORT]

Export the FTP Log as CSV file.

When receiving the following message, click OK, then ICMP Log is exported as CSV file.



Figure 31. Export message.

• [DETAIL]

View detailed information of FTP Log.

	orean -	SYSTEM ADMIN	IISTRATION REPORT AND ANALYSIS USER MANAGEMENT
LOGS AND AUDITS			
Whole	0	FTP Detail	
ICMP	0	ВАСК	
E-mail	0	Classific	Contents
IM	0	Protocol:	SMB
HTTP	0	Date-Time:	2009-11-20 15:44:54
File Transfer	0	Source Address:	192.168.1.88
SEARCH		Destination Address:	192.168.1.33
Search	0	URL:	smb://192.168.1.33/Test_Plan/test_file.txt
DATABASE		Command:	File Read/Copy
Select Database	0	Arguments:	/test_file.txt
EXPORT		Information:	File Read, FID : 4000
Exported Tables	0		

Figure 32. FTP Detail

Console log could be shown slowly about large file.

4.2 Search

Search the audit data stored in stored Database by keyword and prot ocol.

LOGS AND AUDITS									
Whole	0	Searc	ch Audits						
ICMP	0	mail				Q A	ll Types	🗘 🚺 10 Per Page	\$
E-mail	0	ID	Time	Source	Destination	Protocol	Rule	Info	
M	0	9421	2009-11-18 16:24:09	192.168.1.77	192,168,1,88	E-mail	Audit		
нттр	0							"pak " send a mail to "ri@mail.kcc	.com" view more
File Transfer	0	9422	2009-11-18 16:24:45	192.168.1.77	192.168.1.88	E-mail	Audit	"pak " send a mail to "ri@mail.kcc	.com" view more
SEARCH Search	0	9423	2009-11-18 16:26:40	192.168.1.77	192.168.1.88	E-mail	Audit	"root " send a mail to "pak@mail.k	cc.com" view more
DATABASE		9424	2009-11-18 16:27:09	192.168.1.77	192.168.1.88	E-mail	Audit	"" send a mail to ""	view more
EXPORT Exported Tables	0								

Figure 33. Search

Input the keyword, or select the protocol and press

4.3 Database

Display Database list that connect to System.

NG TRAC	E ®©	SYSTEM ADMI	NISTRATION REPORT	FAND ANALYSIS	USER MANAGEMENT	ngadmin	Logout
	_						_
LOGS AND AUDITS		Select Database					
Whole	0						
ICMP E-mail	0	SELECT					
	0	Database Type	Database Name	IP Address			
		RECENTDB	ngtracerecent_dev	192.168.1.104			
ni i P	0	STOREDDB	ngtracestored_dev	192.168.1.104			
rtp		ARCHIVEDB	ngtracearchive_dev	192.168.1.104			
SEARCH							
Search	0						
DATABASE	_						
Select Database	0						
EXPORT							
Exported Tables	0						
	- 1						
	- 1						
	- 1						
	- 1						
	- 1						
					© 2008-2009 I	NGTraceManager. All Righ	s

Figure 34. Select Database

• [SELECT]

From database list, select specific database to view stored log in it. If you select the RECENTDB and press the [SELECT], user can see Whole Log List stored in Recent DB.

		GTOTEMPLE				outrinin	toement.		
LOGS AND AUDITS		Whele Log Lie		DB 402 469 4	104				
Whole	0		UNRECENT	DD- 132.100.1	1.104				
СМР	0	2008-09-03 00:00	All Protocol	s 🌲 All 1	Farget	\$ All Ho	sts	10 Per Page	\$
E-mail	0	Date-Time	Source	Destination	Protocol	Sub Type	Rule	Info	
N	0	2009-03-15 00:00:00	192.168.1.105	192.168.1.1	E-mail	SMTP	Audit	???, ??	view mo
TTP	0	2009-03-15 00:00:00	192.168.1.108	192,168,1,101	E-mail	POP3	Log	?? ?? ????	
tp	0	2009-04-21 00:00:00	192,168,1,106	192 168 1 101	FTP	FTP	Audit	stacraft.exe	view mo
EARCH		2009-05-23 00:00:00	192 168 1 107	192 168 1 101	нттр	HTTP	Audit	Download Flash Player	view mo
earch	0	2009-06-09-00-00-00	192 168 1 103	192.168.1.106	IM	100	Audit	22 22 22	
ATADASE		2009-06-09 00:00:00	100 169 1 107	102 469 4 404	ETD	ETD	Audit	22.22.2222	
elect Database	0	2009-06-09 00.00.00	192.100.1.107	192.100.1.101	FIP	FIF	Log	22.22.2222	
		2009-06-09 00:00:00	192.168.1.107	192.168.1.101	FIP	FIP	Log	22.22.2222	
XPORT		2009-06-09 00:00:00	192.168.1.107	192.168.1.101	FIP	FIP	Log		
xported Tables	0	2009-06-09 00:00:00	192.168.1.107	192.168.1.101	FTP	FTP	Log	aaaa	
		2009-06-09 00:00:00	192.168.1.107	192.168.1.101	FTP	FTP	Log	?? ?? ????	
		Displaying 1 - 10 of 23		14	Page 1 of 3	> >1			

Figure 35. Whole Log List Of RECENTDB

4.4 EXPORT

Display exported file's list.

NG TRACE	80			ngadmin Logou
Enterprise Security Syst	tem	SYSTEM ADMINISTRATION	REPORT AND ANALY:	YSIS USER MANAGEMENT
	_			
LOGS AND AUDITS		Exported Table List		
ICMP	0	DOWNLOAD DELETE DELETE	A11	
E-mail	0			
IM	0	File Name	Exported Date	Filter Condition
нттр	0	export-ftplogs-20090903213306-1.csv	2009-09-03 21:33:06	Protocol:FTP, From Time: 2008-09-03 00:00
Ftp	0	export-ftplogs-20090903213328-1.csv	2009-09-03 21:33:28	Protocol:FTP, From Time: 2008-09-03 00:00
		export-ftplogs-20090903213348-1.csv	2009-09-03 21:33:48	Protocol:FTP, From Time: 2008-09-03 00:00
SEARCH				
Search	0			
DATABASE				
Select Database	0			
	_			
EXPORT	0			
Exported rables				
	1			
				© 2008-2009 NGTraceManager. All Rights Reserve

Figure 36. Export Table List

The following information indicates contents of exported file.

- File Name: Name of exported file.
- Exported Date: Exported date.
- Filter Condition: Filter condition of exported file.
- [DOWNLOAD] Download selected file.
- [DELETE] Delete selected file.
- [DELETE ALL] Delete all file.