

ContentReporter™ 3.0

System Administration Guide

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Information email: info@netapp.com
Information Web: <http://www.netapp.com>

Part number 210-00066
December 2001

Copyright and trademark information

Copyright information

Copyright © 1994–2001 Network Appliance, Inc. All rights reserved. Printed in the U.S.A.

No part of this book covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Portions of this product are derived from the Berkeley Net2 release and the 4.4-Lite-2 release, which are copyrighted and publicly distributed by The Regents of the University of California.

Copyright © 1980–1995 The Regents of the University of California. All rights reserved.

Portions of this product are derived from NetBSD, which is copyrighted by Carnegie Mellon University.

Copyright © 1994, 1995 Carnegie Mellon University. All rights reserved. Author Chris G. Demetriou.

Permission to use, copy, modify, and distribute this software and its documentation is hereby granted, provided that both the copyright notice and its permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.

CARNEGIE MELLON ALLOWS FREE USE OF THIS SOFTWARE IN ITS “AS IS” CONDITION. CARNEGIE MELLON DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.

Software derived from copyrighted material of The Regents of the University of California and Carnegie Mellon University is subject to the following license and disclaimer:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notices, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER

IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Software contains materials from third parties licensed to Network Appliance Inc. which is sublicensed, and not sold, and title to such material is not passed to the end user. All rights reserved by the licensors. You shall not sublicense or permit timesharing, rental, facility management or service bureau usage of the Software.

Portions developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright © 1999 The Apache Software Foundation.

Portions Copyright © 1995-1998, Jean-loup Gailly and Mark Adler

Portions Copyright © 2001, Sitraka Inc.

Portions Copyright © 2001, iAnywhere Solutions

Portions Copyright © 2001, i-net software GmbH

Software derived from copyrighted material of Network Appliance, Inc. is subject to the following license and disclaimer:

Network Appliance reserves the right to change any products described herein at any time, and without notice. Network Appliance assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Network Appliance. The use and purchase of this product do not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Network Appliance.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp and the Network Appliance design are registered trademarks of Network Appliance, Inc. in the United States, Canada, and the European Union. Network Appliance is a registered trademark of Network Appliance, Inc. in Monaco and a trademark of Network Appliance, Inc. in the United States and Canada. FAServer is a registered trademark of Network Appliance, Inc. in the United States and the European Union. NetCache is a registered trademark of Network Appliance, Inc. in the European Union and Japan, and a trademark of Network Appliance, Inc. in the United States. SnapCopy is a registered trademark of Network Appliance, Inc. in the European Union and a trademark of Network Appliance, Inc. in the United States. WAFL is a registered trademark of Network Appliance, Inc. in the European Union and a trademark of Network Appliance, Inc. in the United States and Canada. FilerView and SecureShare are registered trademarks of Network Appliance, Inc. in the United States. Data ONTAP is a trademark of Network Appliance, Inc. in the United States and Canada. Snapshot is a trademark of Network Appliance, Inc. in the United States and the European Union. ApplianceWatch, BareMetal, NetApp—The Network Appliance Company, SecureAdmin, Serving Data by Design, Smart SAN, SnapManager, SnapMirror, SnapRestore, and Web Filer are trademarks of Network Appliance, Inc. in the United States.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

Table of Contents

	Preface	ix
Chapter 1	Installing ContentReporter	1
	Planning the installation	2
	Minimum system requirements.	4
	Installing the ContentReporter server	6
	Uninstalling ContentReporter	9
	Repairing ContentReporter	10
Chapter 2	Initial Configuration Tasks	11
	Logging in the first time	12
	Installing the Java Runtime Environment	14
	Learning about the demonstration database	15
	Configuring your enterprise database	17
	Configuring an MS SQL database	18
	Configuring an Oracle database	24
	Configuring multiple ContentReporter servers.	29
Chapter 3	Navigating the ContentReporter User Interface	31
	ContentReporter header.	32
	ContentReporter Home page	33
	Administration page	34
	Cache Group tab	36
	User Groups tab	39
	Authentication tab	41
	DB Admin tab	46
	Billing tab	48
	Licensing tab	50
	Logging tab.	52
	Import Log Files page	54
	Scheduled Events page	56
	Details tab	59

Schedule tab	61
Security Tab	63

Chapter 4

Using ContentReporter	65
Step one: Defining a cache group	66
Step two: Adding caches to the cache group	71
Cache properties	74
Adding a cache to collect from a directory.	76
Adding a cache to collect from NetCache appliances	78
Adding a cache to collect from an FTP server	91
Step three: Scheduling log file collection	93
Scheduling log file collection and processing	94
Examining information about scheduled events	97
Modifying cache groups and caches	102
Modifying a cache group.	103
Deleting a cache group	105
Modifying a cache's settings	107
Removing a cache from a cache group.	109
Importing saved log files	111

Chapter 5

Setting Access Control	115
Learning about authentication, permissions, and security	116
Authentication in ContentReporter.	117
Page permissions in ContentReporter	119
Web site name restrictions	121
Security in ContentReporter	123
Configuring LDAP and NTLM authentication	125
Configuring ContentReporter for LDAP authentication	126
Configuring ContentReporter for NTLM authentication	129
Adding user groups and setting user group permissions	131
Adding Local users and setting Local user permissions	134
Modifying user and user group permissions	138
Modifying a user group's permissions	139
Deleting an LDAP or NTLM user group.	141
Modifying a Local user's permissions	142
Deleting a Local user.	144

Chapter 6	Additional Configurations	.145
	Examining and upgrading your license information	.146
	Configuring ContentReporter server logging.	.149
	Examining the ContentReporter server log file.	.152
	Understanding the “cs-comment” field return codes.	.154
	Examining the log file	.158
	Configuring database rollups	.159
	Configuring Billing aggregation	.163
	Adding logo images to ContentReporter for XHTML Reports	.168
 Appendix A	 Quick-Start Instructions	 .169
	Quick-start: Setting up log file collection	.170
	Quick-start: Adding a Local user and setting the user’s permissions	.174
 Appendix B	 Assigning a Login to ContentReporter Service	 .177
	Learning about the login user account	.178
	Configuring a Windows NT system	.179
	Configuring a Windows 2000 system	.181
 Appendix C	 Configuring NetCaches for ContentReporter	 .183
	Enabling NetCache appliance Web Access logging	.184
	Enabling NetCache appliance Streaming Access logging	.185
	Configuring a NetCache appliance for SmartFilter reports	.186
	Configuring NetCache appliance log file collection	.188
	Gathering NetCache appliance information	.189
	Synchronizing logging rotation and log file collection	.191
	Enabling SNMP and using Auto Discovery	.194
	 Glossary	 .195
	 Index	 .201

Preface

Introduction

Welcome to the NetApp® *ContentReporter™ 3.0 System Administration Guide*, a product from NetApp—The Network Appliance Company™, which is Serving Data By Design™.

This guide contains the information you need to install and configure the ContentReporter server, to configure your database and caches, and to set up and schedule log file collection and processing. After you have installed and configured the ContentReporter server and set up log file collection and processing, you can create and generate reports on the cache log files. See the *ContentReporter 3.0 Reporting Guide* for instructions on creating, scheduling and generating reports on NetCache™ appliance, Web server, and streaming server log files.

Audience

This guide is for system administrators and others who will install, configure, and use ContentReporter to collect and process log files with an enterprise database. It assumes you are familiar with your operating system, database, network, caches, and servers. This guide does not cover basic system or network administration topics, such as IP addressing, routing, and network topology.

Terminology and conventions

This guide uses the term “type” to mean pressing one or more keys on the keyboard. It uses the term “enter” to mean pressing one or more keys, and then pressing the Enter key.

Keyboard conventions

When describing key combinations, this guide uses the hyphen (-) to separate individual keys. For example, “Ctrl-D” means pressing the “Control” and “D” keys simultaneously. Also, this guide uses the term “Enter” to refer to the key that generates a carriage return, although the key is named “Return” on some keyboards.

Typographic conventions

The following table describes typographic conventions used in this guide.

Convention	Type of information
<i>Italic type</i>	Words or characters that require special attention. File names. Placeholders for information you must supply. For example, <i>IP=12.34.56.78</i> Book titles in cross-references.
Monospaced font	Command names. Information displayed on the system console or other computer monitors. The contents of files.
Bold monospaced font	Words or characters you type. What you type is always shown in lowercase letters, unless you must type it in uppercase letters.

Special messages

This guide contains the following special messages:

Note

A note contains important information that helps you install or operate the system efficiently.

Caution

A caution contains instructions that you must follow to avoid loss of data.

About this chapter

This chapter gives you the information you need to install, uninstall, and repair the ContentReporter server.

Topics covered in this chapter

This chapter covers the following topics:

- ◆ “[Planning the installation](#)” on page 2
- ◆ “[Minimum system requirements](#)” on page 4
- ◆ “[Installing the ContentReporter server](#)” on page 6
- ◆ “[Uninstalling ContentReporter](#)” on page 9
- ◆ “[Repairing ContentReporter](#)” on page 10

Planning the installation

About ContentReporter

The ContentReporter application enables you to analyze content usage, performance, and infrastructure load across your entire content delivery network. The ContentReporter server collects and processes log files from NetCache appliances, directories, and FTP servers throughout a network, and outputs the results of the log file processing to your enterprise database. You log into ContentReporter with a Web browser (the ContentReporter user interface) on your network, and schedule and generate customized reports on the log file data in your database.

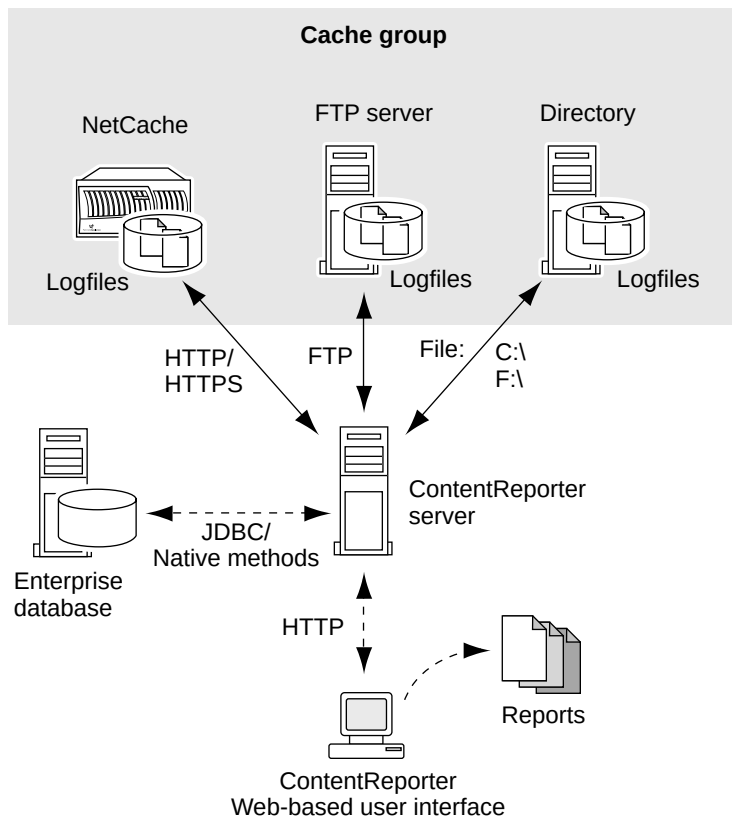
Major components of ContentReporter

The following table describes the major components of ContentReporter.

Component	Description
ContentReporter server	The ContentReporter server is the program that receives and fulfills HTTP requests from client browsers on the same or other computers. The computer on which you install ContentReporter is the ContentReporter server machine.
ContentReporter Web-based user interface	The ContentReporter user interface is a Web browser with HTTP access to the ContentReporter server. You make requests to, and receive fulfilled requests from, the ContentReporter server through a Web browser.
Database	Your enterprise database is a crucial part of the ContentReporter application. The ContentReporter server stores its settings and all aggregated log file records for each cache device in the database. All reports in ContentReporter are based on the records for each cache in the database.
Cache	In ContentReporter, a “cache” represents a particular device that generates the log files that the ContentReporter server collects and processes. ContentReporter can collect and process NetCache™ appliance log files, Web server log files, and streaming server log files.

Illustration of ContentReporter

The following diagram illustrates the major components of ContentReporter.



Minimum system requirements

Minimum requirements

The following table lists the minimum requirements for a ContentReporter configuration.

Note

To learn more about specific sizing requirements and recommendations for your environment, contact a Network Appliance Systems Engineer.

Component	Minimum requirement
System for the ContentReporter server	Pentium III, 800 MHz, 1 GB RAM 20 GB disk space (Disk space should be sufficient for the number and size of the collected and stored log files.) Internet connection
Platform	Windows NT SP 5 Windows 2000 (Server, Advanced Server)
Database	Oracle 8.1.7 MS SQL 7.0 (with Service Pack 2) ASA 7.0.1
Node devices	NetCache appliance Web server Streaming server
Log formats	HTTP: Web Access, Common, Netscape Extended, Squid, Web Access Custom, W3C Streaming: Streaming Access, Custom, Real, WMS, QuickTime
NetCache appliance release	NetCache 5.x or later NetCache 5.1D4 or later required for SmartFilter reports NetCache 5.2 R1 or later required for log file compression

Component	Minimum requirement
Web browser	Internet Explorer 5.0 or 5.5, or Netscape Navigator 6.1 Java 2 Runtime Environment 1.3.1 Plug-in enabled (Internet Explorer Security Settings: Enable “Run ActiveX controls and plug-ins”) JavaScript and Java Applet enabled Browser set to check for new content each visit to a stored page

Installing the ContentReporter server

Guidelines for installing

Follow these guidelines when installing ContentReporter:

- ◆ The user who installs ContentReporter must have Administrator privileges on the machine in order for the installation program to make the necessary system changes. Otherwise, ContentReporter does not function properly.
- ◆ If you are setting up a multiple ContentReporter server environment, see [“Configuring multiple ContentReporter servers”](#) on page 29.
- ◆ If you want to access network resources, you can assign a login user account to the ContentReporter service. See Appendix B, [“Learning about the login user account,”](#) on page 178.

Space requirements for the installation

The ContentReporter server installation has the following disk space requirements:

- ◆ 60 MB of space during the installation on the drive with the Temp directory for temporary installation files
- ◆ 60 MB of space on the drive with the operating system for the permanent InstallShield™ information files
- ◆ 150 MB of space on the drive on which you install the ContentReporter server

Installing ContentReporter

To install ContentReporter, complete the following steps.

Step	Action
1	Ensure that your configuration meets the minimum requirements.
2	Log into the system with a user account that has Administrator privileges.
3	From the Windows interface, click Start > Settings > Control Panel

Step	Action	
4	If installing...	Then...
	On a Windows 2000 system	1. Click Add/Remove Programs. 2. Double-click Add/Remove Programs. 3. Click Add New Programs. 4. Click CD or Floppy, then click Next.
	On a Windows NT system	1. Double-click the Add/Remove Programs icon. 2. Click Install. 3. Click Next.
5	Click Browse, browse to and select the ContentReporter.exe file, and click Open.	
6	Click Finish.	
7	In the Welcome screen of the InstallShield Wizard, click Next. Result: The InstallShield Wizard extracts the files needed to install ContentReporter, and then the InstallShield window appears.	
8	In the InstallShield window, click Next.	
9	Read and accept the License Agreement.	
10	In the Customer Information window, enter your user name and your company name, and then click Next.	
11	In the Choose Destination Location window, accept the default location or select a different location by clicking Browse, and then click Next.	
12	In the Select Program Folder window, accept the default name of the Program folder, enter a new name in the Program Folders field, or select an existing name from the Existing Folders list, and then click Next. Result: The Start Copying Files window appears.	

Step	Action
13	Review the settings in the Start Copying Files window, clicking Back to change any of them, and then click Next. Result: The InstallShield wizard installs ContentReporter. When the installation is complete, the ContentReporter service (“ContentReporter”) begins initializing and the Setup Complete window appears.
14	Click Finish to exit the Installation program. Result: A message box appears.
15	Click OK to launch your Web browser, and to log into ContentReporter after the ContentReporter database initializes. After ContentReporter initializes, the License Login window appears, and you can log into ContentReporter for the first time. See “Logging in the first time” on page 12 Note _____ Do not stop the ContentReporter service or restart the computer while the ContentReporter service initializes. _____

Uninstalling ContentReporter

Uninstalling ContentReporter

To uninstall ContentReporter, complete the following steps.

Step	Action	
1	From the Windows user interface, click Start > Settings > Control Panel.	
2	Double-click Add/Remove Programs.	
3	If uninstalling...	Then...
	On a Windows 2000 system	Select Network Appliance ContentReporter 3.0 from the list of installed programs, and click Change/Remove.
	On a Windows NT system	Select Network Appliance ContentReporter 3.0, and click Add/Remove.
4	Select the Remove button, and click Next.	
5	Click OK.	
6	Click Finish to complete the uninstallation process.	

Repairing ContentReporter

About repairing ContentReporter

If you accidentally delete a ContentReporter program file, you can repair the ContentReporter installation.

Note _____
Repairing ContentReporter does not repair a partially uninstalled copy of ContentReporter, nor restore enterprise database settings.

Repairing ContentReporter

To repair a ContentReporter installation, complete the following steps.

Step	Action	
1	From the Windows user interface, click Start > Settings > Control Panel.	
2	Double-click the Add/Remove Programs icon.	
3	If repairing...	Then...
	On a Windows 2000 system	Select Network Appliance ContentReporter 3.0 from the list of installed programs, and click Change/Remove.
	On a Windows NT system	Select Network Appliance ContentReporter 3.0, and click Add/Remove.
4	Select the Repair/Upgrade button, and click Next. Result: The InstallShield Wizard repairs your ContentReporter installation.	
5	Click Finish to complete the repair process.	

About this chapter

This chapter gives you the information you need to complete initial configuration tasks in ContentReporter.

Topics in this chapter

This chapter discusses the following topics:

- ◆ [“Logging in the first time”](#) on page 12
- ◆ [“Installing the Java Runtime Environment”](#) on page 14
- ◆ [“Learning about the demonstration database”](#) on page 15
- ◆ [“Configuring your enterprise database”](#) on page 17
- ◆ [“Configuring multiple ContentReporter servers”](#) on page 29

Logging in the first time

Logging in the first time

To log into ContentReporter the first time, complete the following steps.

Note—————
If you purchased ContentReporter, you will find your License Key listed in the Software License Key letter in your ContentReporter kit.

Step	Action	
1	If...	Then...
	You have opened the License Login window as part of the installation process	Go to step 2.
	You are logging in from the ContentReporter server machine	Double-click the ContentReporter startup icon on your desktop, or click Start > Programs > Network Appliance > ContentReporter > ContentReporter Login.
	You are logging in from a machine with HTTP access to the ContentReporter server machine	Launch your Web browser and browse to the following URL: http://servername:7777/ContentReporter/index.html servername is the server name or IP address of the ContentReporter machine. 7777 is the ContentReporter-specific port.
2	In the License Login window, enter your License Key or select the Evaluation check box, then click Submit.	

Step	Action
3	In the ContentReporter Login page, enter “admin” in the Username field, enter “admin” in the Password field, and then click Enter. Result: You open the ContentReporter home page, and are successfully logged into ContentReporter.

Note

If you log into ContentReporter from the ContentReporter server machine, you see an IP address of 127.0.0.1 in the Web browser’s URL field. This is the machine’s local host IP address.

Installing the Java Runtime Environment

Installing Java Runtime

If ContentReporter prompts you to install the Java 2 Runtime Environment 1.3.1, complete the following steps.

Step	Action
1	In the Security Warning window, click Yes. Result: The Select Java Plug-in Installation window appears.
2	In the Select Java Plug-in Installation window, select U.S. English from the Locale drop-down list, and click Install. Note_____ If you want to select a Locale other than U.S. English, exit this installation program and go to the www.sun.com Web site to select a non-English version. _____
3	Read and accept the License Agreement.
4	In the Choose Destination Location window, click Next to complete the installation process. Result: You can begin using ContentReporter.

Learning about the demonstration database

About the embedded database

The embedded Sybase Adaptive Server Anywhere (ASA) 7.0.1 database is for evaluation situations only. When you first install ContentReporter, the ASA is your default database. You can use this database to collect and process small log files, and to generate reports on these log files. After logging into ContentReporter the first time, you can examine the ASA database settings on the Administration DB Admin tab.

Caution

Only use the embedded ASA database for demonstration purposes. You cannot transfer data from the ASA database to an enterprise database.

The DB Admin tab with ASA settings

The following screen shows the Administration DB Admin tab with ASA settings.

The screenshot displays the 'DB Admin' tab within a configuration window. The window has a tabbed interface with 'Cache Group', 'User Groups', 'Authentication', 'DB Admin', 'Billing', 'Licensing', and 'Logging'. The 'DB Admin' tab is active. It contains several input fields and buttons. The 'Database' field is a dropdown menu showing 'Adaptive Serv...'. To its right are 'Reset' and 'Test...' buttons. Below 'Database' is the 'Username' field with 'cr_admin'. To its right is the 'Db Name' field with 'crsettings'. Below 'Username' is the 'Password' field with '*****'. Below 'Password' is the 'Hostname' field with 'bills-nt'. Below 'Hostname' is the 'Port' field with '2630'. Below 'Port' is the 'DatabaseHome' field with 'C:\MSSQL7\'. To the right of 'DatabaseHome' is a 'Browse...' button.

Cache Group	User Groups	Authentication	DB Admin	Billing	Licensing	Logging
Database: Adaptive Serv... Reset Test... Username: cr_admin Db Name: crsettings Password: ***** Hostname: bills-nt Port: 2630 DatabaseHome: C:\MSSQL7\ Browse...						

List of ASA database settings

The following table describes the embedded ASA database settings.

Caution

Do not modify the Username, Password, Port, or DB Name settings. Otherwise, you cannot log back into ContentReporter after restarting the service. Only modify the Hostname setting if you must connect to an ASA database on another machine.

ASA setting	Value	Description
Username	cr_admin	The account user name of the built-in ASA crsetting database.
Password	admin	The account password of the built-in ASA crsetting database.
Hostname	machine name	The machine name of the system on which you installed the ASA database. In most cases, this is the machine on which you installed ContentReporter. Example: If the machine name is “smith-nt.domainname.com,” the host name is either “smith-nt,” or “smith-nt.domainname.com.”
Port	2630	The ContentReporter server connection port to the ASA database.
DB Name	crsettings	The name of the embedded database.

Configuring your enterprise database

About the database

Your enterprise database is a crucial part of the ContentReporter application. Once you connect ContentReporter to your database, all of the ContentReporter server settings are stored on your database. If your database service stops or the ContentReporter server loses network connectivity to your database, you will receive an error message in your Web browser and will not be able to log into ContentReporter. The ContentReporter server also stores all parsed log file records for each cache in your database. Finally, all reports in ContentReporter are based on the records for each cache in your database.

For detailed information

For details about configuring your enterprise database, see the following topics:

- ◆ [“Configuring an MS SQL database”](#) on page 18
- ◆ [“Configuring an Oracle database”](#) on page 24

Configuring your enterprise database

Configuring an MS SQL database

Where you can install the database

You can install an MS SQL 7.0 (with Service Pack 2) database and the ContentReporter server on the same machine or on different machines. If you install them on different machines, you must install an MS SQL client on the ContentReporter server machine.

Required configuration procedures

- You must perform the following procedures to configure an MS SQL database:
- ◆ Create or identify a database (“crsettings” is the default name) and a login (either the “sa” login or a some other login granted the Server Administrator role) for the ContentReporter server
 - ◆ Configure ContentReporter to use the MS SQL database

The DB Admin tab with MS SQL settings

The following screen shows the DB Admin tab with MS SQL settings.

The screenshot displays the 'DB Admin' tab of a configuration window. The window has a tabbed interface with the following tabs: 'Cache Group', 'User Groups', 'Authentication', 'DB Admin' (selected), 'Billing', 'Licensing', and 'Logging'. The 'DB Admin' tab contains the following fields and controls:

- Database:** A dropdown menu set to 'SQL Server'. To its right are 'Reset' and 'Test ...' buttons.
- Username:** A text box containing 'sa'.
- Password:** A text box containing '*****'.
- Hostname:** A text box containing 'bills-nt'.
- Port:** A text box containing '1433'.
- DatabaseName:** A text box containing 'crsettings'.
- DatabaseHome:** A text box containing 'C:\MSSQL7\'. To its right is a 'Browse...' button.

Database settings

The following table describes the MS SQL database settings in ContentReporter.

Setting	Description
User name	The username of the MS SQL login that ContentReporter uses to access the database listed in the DB Name field. The default is the “sa” login. ContentReporter can also use a login that meets the following three requirements: ◆ granted only the Server Administrator role ◆ has only “Public” and “db_ddladmin” privileges for the ContentReporter database (listed in the DB Name field) ◆ defaults to the ContentReporter database (listed in the DB Name field)
Password	The password of the MS SQL login that ContentReporter uses to access the database listed in the DB Name field. The default is no password.
Hostname	The MS SQL server machine name. Example: If the machine name is “bills-nt.domainname.com,” the host name is either “bills-nt” or “bills-nt.domainname.com.”
Port	The port through which the ContentReporter server connects to an MS SQL database. The default port is 1433.
Database Home	The root directory of the MS SQL server, or of the MS SQL client installation on the ContentReporter server machine. The typical directory is C:\MSSQL7\ (or the directory in which MS SQL is installed).
DB Name	The name of the database you created in MS SQL for ContentReporter. The default database name is “crsettings.”

Configuring a database and login

To configure an MS SQL database and a login for ContentReporter, complete the following steps.

Step	Action	
1	To create a database for ContentReporter in the MS SQL Manager console, expand the database server in the left-hand console tree (under Console Root Microsoft SQL Servers SQL Server Group), right-click Databases, and then click New Database.	
2	In the Database Properties window, enter a name (the default is “crsettings”), set any other file properties, and click OK.	
3	Right-click the new database in the console tree (under the database server), and click Properties.	
4	In the Properties window, click the Options tab, ensure that the “Select into/bulk copy” check box is selected, and click OK.	
5	If...	Then...
	You want ContentReporter to use the “sa” System Administrator SQL login	1. Expand Security in the console tree, click Logins, right-click the “sa” login, and click Properties. 2. Identify or enter a password for the “sa” login, click OK, and go to Step 7.
	You want to create a new SQL login for ContentReporter	Go to Step 6.

Step	Action	
6	To create a new SQL Server Administrator login for ContentReporter, complete the following steps: 1. Expand Security in the console tree, right-click Logins, and click New Login. 2. Enter a name for the login, click the SQL Server Authentication button, enter a password for the login, select the new ContentReporter database from the lower default Database drop-down list, and then click the Server Roles tab. 3. Select only the Server Administrators role check box, and click the Database Access tab. 4. Select the Permit box next to the database in the upper panel, select only the “public” and the “db_ddladmin” check boxes in the lower panel, and click OK. 5. Enter the password, and click OK.	
7	If...	Then...
	The ContentReporter server and the MS SQL database are on different machines	Install an MS SQL client on the ContentReporter server machine.
	The ContentReporter server and the MS SQL database are on the same machine	Go to step 8.
8	Go to “ Configuring ContentReporter to use MS SQL ” on page 21.	

Configuring ContentReporter to use MS SQL

To configure ContentReporter to use an MS SQL database, complete the following steps.

Step	Action
1	Log into ContentReporter, and click the Administration tab.
2	Click the Admin button.

Step	Action	
3	From the Cache Groups tab, click the DB Admin tab. Note _____ At any point, you can click Reset to reset the database settings on this tab to their current (actual) state.	
4	Select SQL Server from the Database drop-down list.	
5	Enter the MS SQL login user name (or leave “sa”) in the Username field, and then enter the login password in the Password field.	
6	Enter the MS SQL server machine name in the Hostname field.	
7	Ensure that port 1433 (or the appropriate port) appears in the Port field.	
8	Enter (or click Browse, browse to, and select) the root directory of the MS SQL server or client installation in the Database Home field.	
9	Enter the name of the SQL database (the default is “crsettings”) you created or identified for ContentReporter.	
10	Test the ContentReporter server’s connection to the SQL database by clicking Test DB Connection.	
11	If...	Then...
	A successful connection exists between ContentReporter and the SQL database	1. Click OK. 2. Click OK again.
	The database connection test failed	1. Click OK. 2. Verify the information you entered and check network connectivity between the ContentReporter server and the SQL server. 3. Repeat Step 9.
12	From the Administration page, log out of ContentReporter.	

Step	Action
13	Stop and restart the ContentReporter service. (In Windows NT: Click Start > Settings > Control Panel > Services. Then stop and start the ContentReporter service. In Windows 2000: Right-click My Computer > Manage > expand Services and Applications > double-click Services. Then stop and start the ContentReporter service.) Note_____ Any time you modify database settings, you must stop and restart the ContentReporter service for the new settings to take affect. You might need to wait a moment for ContentReporter to start running. Result: You successfully configured ContentReporter to use an SQL database.

Configuring your enterprise database

Configuring an Oracle database

Where you can install the database

You can install an Oracle 8.1.7 database and the ContentReporter server on the same machine or on different machines. If you install them on different machines, you must install an Oracle 8.1.7 client on the ContentReporter server machine.

Required configuration procedures

You must perform the following procedures to configure an Oracle database:

- ◆ Configure the database to work with ContentReporter
- ◆ Configure ContentReporter to use the Oracle database

The DB Admin tab with Oracle settings

The following screen shows the DB Admin tab with Oracle settings.

The screenshot displays the 'DB Admin' tab of a configuration window. The window has a tabbed interface with the following tabs: 'Cache Group', 'User Groups', 'Authentication', 'DB Admin' (selected), 'Billing', 'Licensing', and 'Logging'. The 'DB Admin' tab contains the following fields and controls:

- Database:** A dropdown menu set to 'Oracle'. To its right are 'Reset' and 'Test ...' buttons.
- Username:** A text field containing 'scott'. To its right is a label 'SID' and a text field containing 'T11'.
- Password:** A text field containing '*****'.
- Hostname:** A text field containing 'bills-nt'.
- Port:** A text field containing '1521'.
- DatabaseHome:** A text field containing 'f:\oracle\ora817\'. To its right is a 'Browse...' button.

Database settings

The following table describes the Oracle database settings in ContentReporter.

Database setting	Description
User name	The Oracle user name of the account that ContentReporter uses to access the database.
Password	The password for the Oracle user account that ContentReporter uses to access the database.
Hostname	The Oracle server machine name. Example: If the machine name is “bills-nt.domainname.com,” the host name is either “bills-nt” or “bills-nt.domainname.com.”
Port	The port through which the ContentReporter server connects to an Oracle database. The default port is 1521.
Database Home	The Home directory of the Oracle database server or Oracle client.
SID	The Oracle Service Name or SID of the database instance used with ContentReporter.

Client requirements

The following table lists the ContentReporter server’s Oracle client requirements.

Characteristic	Requirement
Version	The Oracle client’s version (8.1.7) must match the Oracle database server’s version.
Installed utilities	JDBC Drivers and SQL Loader utilities installed. These are part of the “Typical” client installation.

Configuring the database

To configure the database for ContentReporter, complete the following steps.

Step	Action	
1	If you installed...	Then...
	The ContentReporter server and Oracle server on different machines	1. Install an Oracle 8.1.7 client on the ContentReporter server machine. 2. Ensure that the SQL Loader utilities for the client are installed. These are included in the “Typical” installation.
	The ContentReporter server and Oracle server on the same machine	Ensure that the JDBC Drivers and SQL Loader utilities for the Oracle server are installed.
2	Create a user account for ContentReporter.	
3	Go to “ Configuring ContentReporter ” on page 26.	

Configuring ContentReporter

To configure ContentReporter for the database, complete the following steps.

Step	Action
1	Log into ContentReporter, and click the Administration tab.
2	Click Admin.
3	From the Cache Groups tab, click the DB Admin tab. Note _____ At any point, you can click Reset to reset the database settings on this tab to their current (actual) state.
4	Select Oracle from the Database drop-down list.
5	Enter the Oracle account user name in the Username field, and enter the account password in the Password field.
6	Enter the Oracle server machine name in the Hostname field.

Step	Action	
7	Ensure that port 1521 (or the appropriate port) appears in the Port field.	
8	Click Browse to browse to and select the Oracle Home directory path, or enter the Home directory path manually. Example: F:\\oracle\\ora817\\	
9	In the SID field, enter the Oracle Service Name or SID of the database instance used with ContentReporter.	
10	Test ContentReporter server's connection to the Oracle database by clicking Test DB Connection.	
11	If...	Then...
	A successful connection exists between ContentReporter and the Oracle database	1. Click OK. 2. Click OK again.
	The database connection test failed	1. Click OK. 2. Verify the information you entered and check network connectivity between the ContentReporter server and the SQL server. 3. Repeat Step 10.
12	From the Administration page, log out of ContentReporter.	

Step	Action
13	Stop and restart the ContentReporter service. (In Windows NT: Click Start > Settings > Control Panel > Services. Then stop and start the ContentReporter service. In Windows 2000: Right-click My Computer > Manage > expand Services and Applications > double-click Services. Then stop and start the ContentReporter service.) Note_____ Any time you modify database settings, you must stop and restart the ContentReporter service for the new settings to take affect. You might need to wait a moment for ContentReporter to start running. Result: You successfully configured ContentReporter to use an Oracle database.

Configuring multiple ContentReporter servers

About configuring multiple servers

If you collect log files for a large number of caches, you can configure a multiple ContentReporter server environment. In a multiple ContentReporter server environment, each ContentReporter server can collect and process log files and update the database for some of the caches in your environment.

After each ContentReporter server updates the database, you can log into any ContentReporter server to create and generate reports based on any or all of the caches in your environment. You can also import log files for any of the caches in your environment.

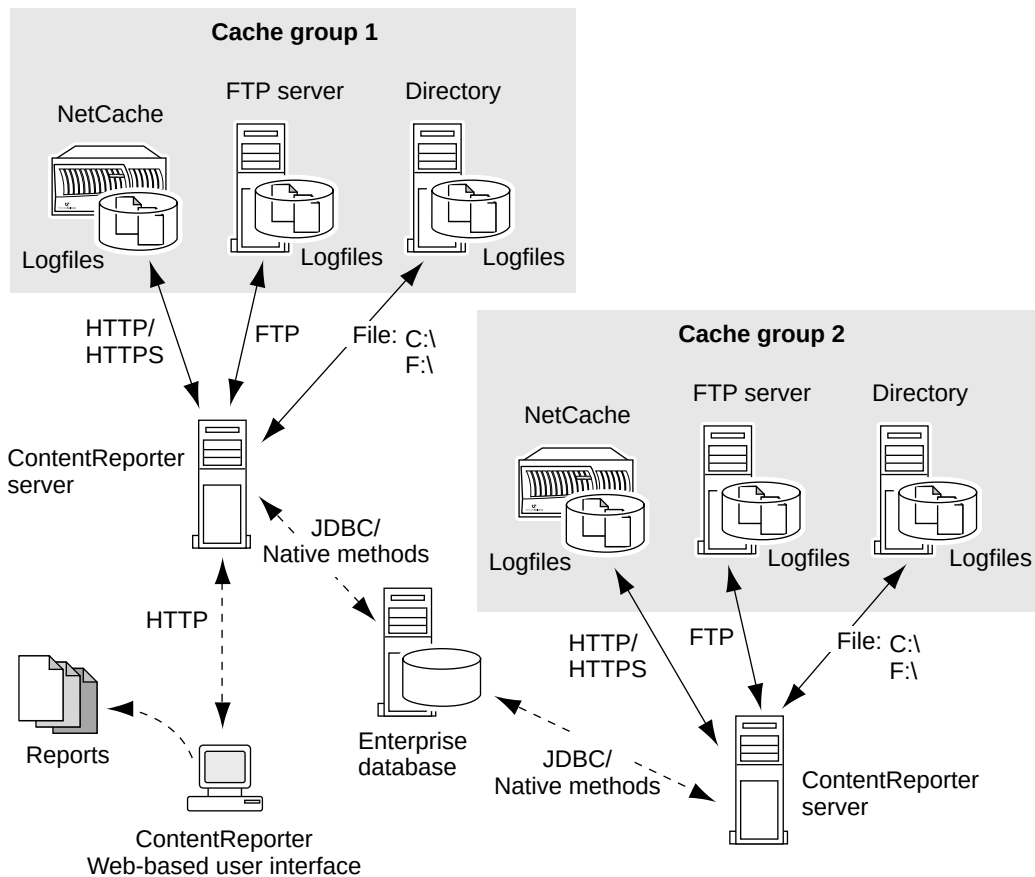
Configuring multiple ContentReporter servers

To set up a multiple ContentReporter server environment, complete the following steps.

Step	Action
1	Install each copy of ContentReporter. See “ Installing the ContentReporter server ” on page 6
2	Connect each ContentReporter server to the same database. See “ Configuring your enterprise database ” on page 17.

Multiple ContentReporter server configuration

The following diagram illustrates a multiple ContentReporter server environment.



About this chapter

This chapter gives you an overview of the main ContentReporter pages and tabs you use to complete the administrative tasks described in this guide.

To learn about the pages and tabs you use to complete reporting tasks, see the *ContentReporter 3.0 Reporting Guide*.

Topics in this chapter

This chapter provides information about the following topics:

- ◆ “[ContentReporter header](#)” on page 32
- ◆ “[ContentReporter Home page](#)” on page 33
- ◆ “[Administration page](#)” on page 34
- ◆ “[Scheduled Events page](#)” on page 56

ContentReporter header

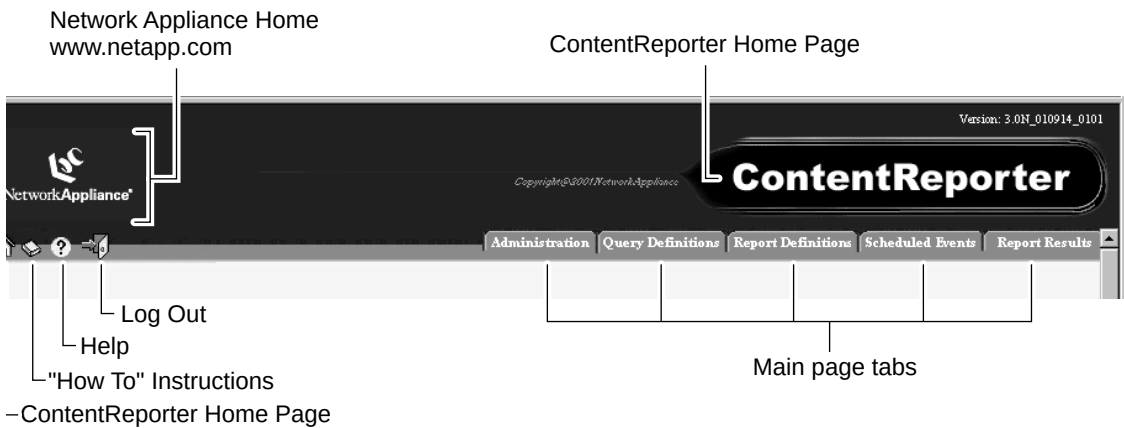
What it provides

The ContentReporter header, which you can access from any of the main pages in ContentReporter, provides the following features and functions:

- ◆ Two links to the ContentReporter Home page
- ◆ Tab links to the main pages
- ◆ Two links to the online Help system
- ◆ A logout icon
- ◆ A link to the Network Appliance Web site

What it looks like

The following screen shows the ContentReporter header.



ContentReporter Home page

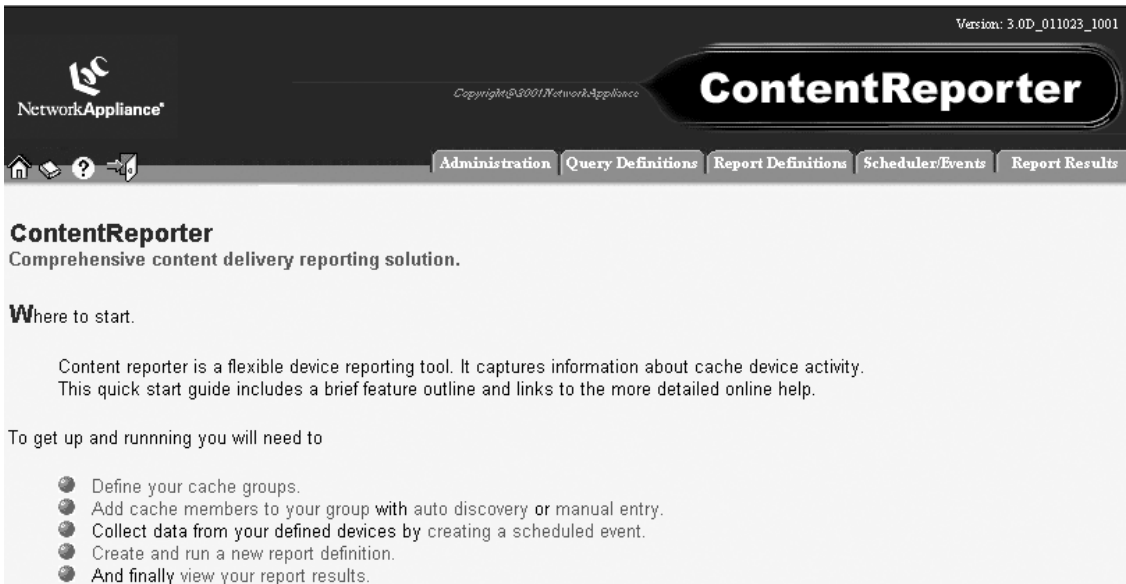
What it provides

The ContentReporter Home page, which you open when you log into ContentReporter, contains links to online Help instructions that explain how to do the following:

- ◆ Define a cache group
- ◆ Add cache group members
- ◆ Schedule log file collection
- ◆ Create and run reports
- ◆ View report results.

What it looks like

The following screen shows the ContentReporter Home page.



Administration page

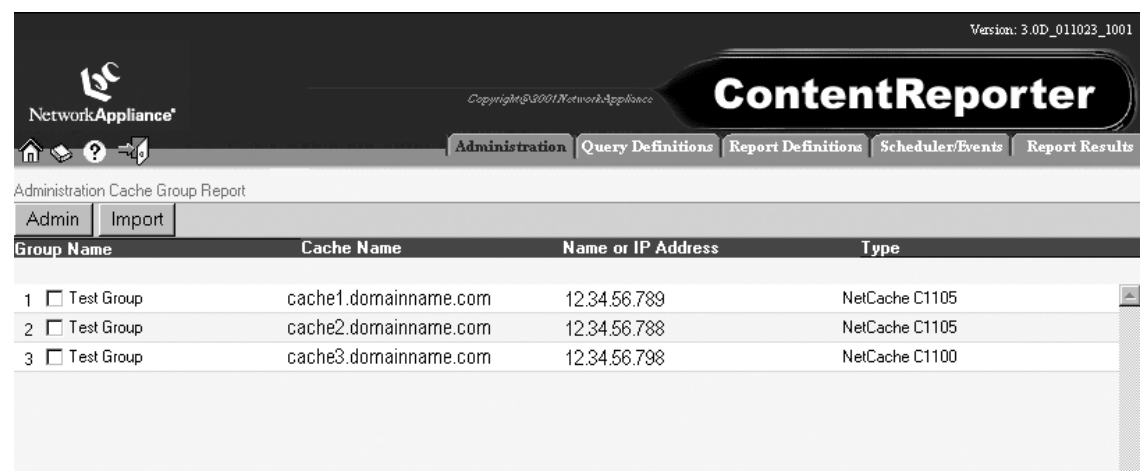
What it provides

The Administration page enables you to complete all administrative tasks in ContentReporter:

- ◆ Create and manage cache groups
- ◆ Import log files
- ◆ Manage users and groups
- ◆ Configure authentication
- ◆ Configure database settings
- ◆ Configure billing aggregation
- ◆ Configure ContentReporter logging
- ◆ Enter license information

What it looks like

The following screen shows the Administration page.



Administration page components

The following table describes the Administration page components and their functions.

Component	Function
Admin button	Clicking the Admin button launches the tabs for all administrative tasks in ContentReporter.
Import button	Clicking the Import button launches the Import Log File page. The Import Log File page enables you to process log files for a new or an existing cache device without creating a scheduled event. This means you can process log files that were not collected or processed by a scheduled event and output the result to your database for an existing cache. For example, you can import and process old log files for a particular cache.
Group Name column	Lists the name of each cache device's cache group.
Cache Name column	Lists the name of each cache device. Note _____ After you add a NetCache appliance to a cache group, you can access its management console from the Administration page by clicking its name in the Cache Name column. _____
IP Address column	Lists the IP address or name of each cache device.
Type column	Lists the type of NetCache appliance, such as C6100 and C1100.

For detailed information

For details about the Administration page tabs and the Import Log Files page, see the following topics.

- ◆ [“Cache Group tab”](#) on page 36
- ◆ [“User Groups tab”](#) on page 39
- ◆ [“Authentication tab”](#) on page 41
- ◆ [“DB Admin tab”](#) on page 46
- ◆ [“Billing tab”](#) on page 48
- ◆ [“Licensing tab”](#) on page 50
- ◆ [“Logging tab”](#) on page 52
- ◆ [“Import Log Files page”](#) on page 54

Cache Group tab

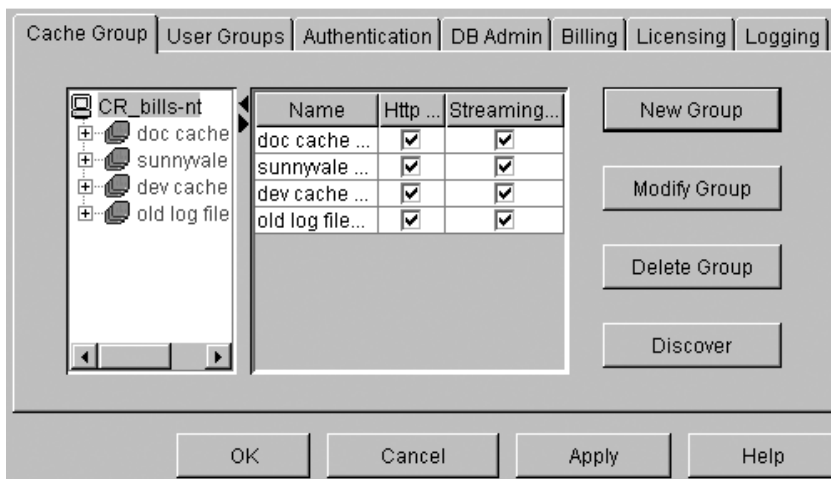
What it provides

The Cache Group tab enables you to create, configure, and manage cache groups for log file collection.

To learn more about adding caches to cache groups, see “[Step two: Adding caches to the cache group](#)” on page 71

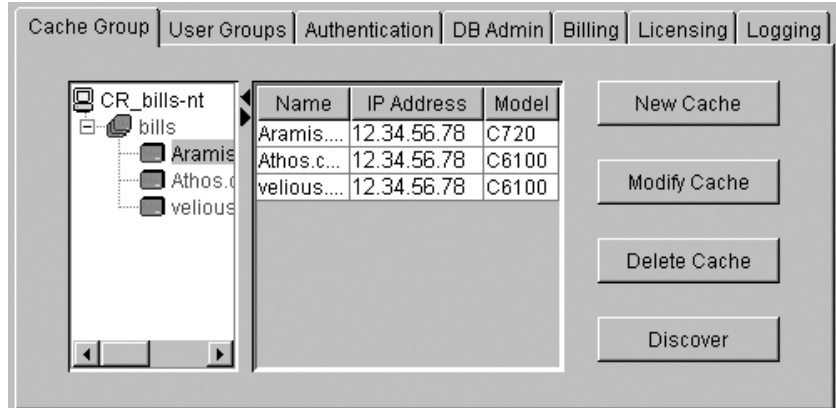
Cache Group tab

The following screen highlights cache group settings on the Cache Group tab.



Cache Group tab

The following screen highlights cache settings on the Cache Group tab.



Cache Group tab components

The following table describes the Cache Group tab components.

Component	Function
Left-hand explorer panel	Lists each cache group under the ContentReporter server you used to create it, and each cache device under its group. When you select a ContentReporter server, the central contents panel displays the server's cache groups and type of analysis (HTTP and/or Streaming) performed for each group. When you select a particular cache group, the central contents panel displays the names, IP addresses, and model numbers of the group's cache devices.
Central contents panel	Displays the contents of the selected item in the left-hand explorer panel.
New Group button	Creates a new cache group.
Modify Group button	Modifies the type of analysis (HTTP and/or Streaming) performed for the group selected in the left-hand explorer panel.
Delete Group button	Deletes the cache group selected in the left-hand explorer panel.
New Cache button	Adds a new cache device to the cache group selected in the left-hand explorer panel.
Discover button	Enables you to use the Auto Discovery feature to add NetCache appliances to a group.

Component	Function
Modify Cache button	Modifies the settings of the cache selected in the left-hand explorer panel.
Delete Cache button	Removes the cache selected in the left-hand explorer panel from its group.
Apply and OK buttons	Enables you to save changes to the ContentReporter server. If you click OK, you return to the Administration page. If you click Apply, you remain on this tab. If you want to make multiple, interdependent changes to settings on this tab, you must click Apply after each interdependent change. For example, if you delete a cache from a cache group, you must click Apply before you can add the cache to another group.

Administration page

User Groups tab

What it provides

The User Groups tab enables you to set page permissions for the three Local user groups, as well as, LDAP and NTLM user groups.

To learn more about setting user group permissions, see “[Adding user groups and setting user group permissions](#)” on page 131.

What it looks like

The following screen shows the User Groups tab.

Name	Events	Reports	Query D...	Report ...	Admini...
Admin	rwed	rwed	rwed	rwed	rwed
Guest	rwed	rwed	rwed	rwed	rwed
User	rwed	rwed	rwed	rwed	rwed

Buttons: Add, Edit, Delete

Buttons: OK, Cancel, Apply, Help

User Groups tab components

The following table describes the User Groups tab components.

Component(s)	Function(s)
Name column	Lists the user group names.
Add	Sets permissions for a particular LDAP or NTLM user group.
Edit	Modifies permissions of a particular Local, LDAP, or NTLM user group.
Delete	Removes permissions settings for a particular LDAP or NTLM user group.
Page permissions columns	List the user group's page permissions (read, write, execute, delete) for the Scheduled Events, Report Definitions, Query Definitions, Report Results, and Administration pages.
Read (r) permissions	Enables group members to open the Scheduled Events, Report Definitions, Query Definitions, Report Results, or Administration page.
Write (w) permissions	Enables group members to modify objects on the Scheduled Events, Report Definitions, Query Definitions, Report Results, or Administration page.
Execute (e) permissions	Enables group members to run or execute objects on the Scheduled Events, Report Definitions, Query Definitions, Report Results, or Administration page.
Delete (d) permissions	Enables groups members to delete objects on the Scheduled Events, Report Definitions, Query Definitions, Report Results, or Administration page.
Apply and OK buttons	Enables you to save changes to the ContentReporter server. If you click OK, you return to the Administration page. If you click Apply, you remain on this tab. If you want to make multiple, interdependent changes to settings on this tab, you must click Apply after each interdependent change. For example, if you delete a user group, you must click Apply before you can add another user group with the same name.

Authentication tab

What it provides

The Authentication tab enables you to add, delete, set, and modify page permissions for Local users, as well as configure ContentReporter for either LDAP or NTLM Authentication.

To learn more about setting permissions for Local users, see [“Adding Local users and setting Local user permissions”](#) on page 134.

To learn more about configuring authentication, see [“Configuring LDAP and NTLM authentication”](#) on page 125.

What it looks like

The following screen shows Local Authentication settings on the Authentication tab.

Cache Group User Groups **Authentication** DB Admin Billing Licensing Logging

Authentication Method: Local

Local

UserName	Group	Email
admin	Admin	
guest	Guest	
nonadmin	User	
george	Admin	

New Modify Delete

OK Cancel Apply Help

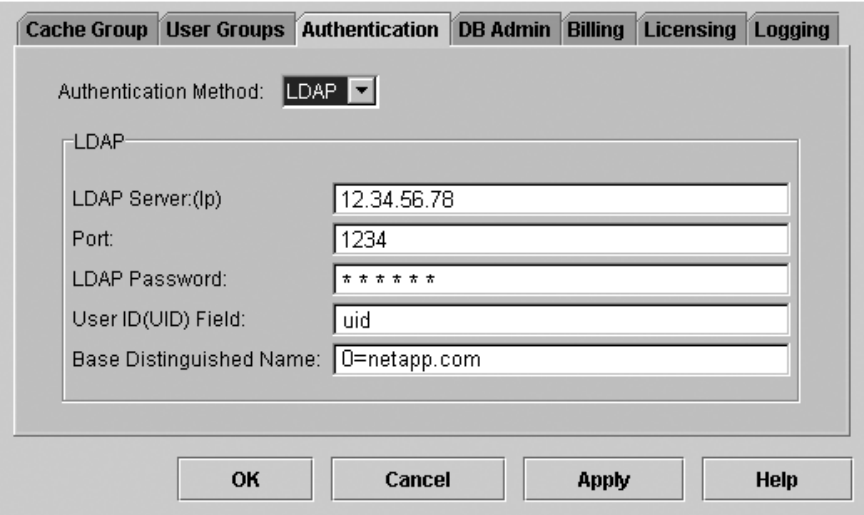
Local Authentication tab components

The following table describes the Local Authentication tab components.

Component(s)	Function(s)
UserName column	Lists the Local group user names.
Group column	Lists the Local user's group.
E-mail column	Lists the Local user's (optional) e-mail address.
New button	Creates and sets page permissions and site name report restrictions for a new Local user.
Modify button	Modifies page permissions and site name report restrictions for a Local user.
Delete button	Removes a Local user from ContentReporter.
Apply and OK buttons	Enables you to save changes to the ContentReporter server. If you click OK, you return to the Administration page. If you click Apply, you remain on this tab. If you want to make multiple, interdependent changes to settings on this tab, you must click Apply after each interdependent change.

**LDAP
Authentication
settings**

The following screen shows LDAP Authentication settings.

A screenshot of a software interface showing the 'Authentication' tab. The 'Authentication Method' is set to 'LDAP'. Below this, there are five input fields: 'LDAP Server:(lp)' with the value '12.34.56.78', 'Port' with '1234', 'LDAP Password' with masked characters '*****', 'User ID(UID) Field' with 'uid', and 'Base Distinguished Name' with 'O=netapp.com'. At the bottom are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

**LDAP
Authentication tab
components**

The following table describes the LDAP Authentication tab components.

Component	Function
LDAP Server IP field	The IP Address of the LDAP server.
Port field	The port through which ContentReporter accesses the LDAP server.
LDAP Password field	The password ContentReporter uses to gain access to the bind distinguished name. This password authorizes ContentReporter to access and query the LDAP directory.
User ID (UID) field	The name (often “uid”) of the attribute in the LDAP directory that contains user login names that ContentReporter authenticates.
Base Distinguished Name field	The Base Distinguished Name of the directory on the LDAP server where ContentReporter begins its authentication search.

Component	Function
Apply and OK buttons	Enables you to save changes to the ContentReporter server. If you click OK, you return to the Administration page. If you click Apply, you remain on this tab. If you want to make multiple, interdependent changes to settings on this tab, you must click Apply after each interdependent change.

**NTLM
Authentication
settings**

The following screen shows the NTLM Authentication settings.

A screenshot of a software configuration window titled 'Authentication'. The window has several tabs at the top: 'Cache Group', 'User Groups', 'Authentication' (which is selected), 'DB Admin', 'Billing', 'Licensing', and 'Logging'. Inside the 'Authentication' tab, there is a label 'Authentication Method:' followed by a dropdown menu showing 'NTLM'. Below this, there is a large rectangular area with the text 'NTLM' at the top. Inside this area, there is a label 'Windows Domain Name :' followed by a text input field containing the value 'netapp'. At the bottom of the window, there are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

**NTLM
Authentication tab
components**

The following table describes the NTLM Authentication tab components.

Component	Function
Windows Domain Name field	The name of the domain in which the ContentReporter server resides. For example, if the ContentReporter server machine is in the “netapp” domain, enter “netapp” in this field.
Apply and OK buttons	Enables you to save changes to the ContentReporter server. If you click OK, you return to the Administration page. If you click Apply, you remain on this tab. If you want to make multiple, interdependent changes to settings on this tab, you must click Apply after each interdependent change.

What it provides

The DB Admin tab enables you to connect ContentReporter to your database, and to configure database rollups.

To learn more about configuring database rollups, see “[Configuring database rollups](#)” on page 159.

Illustration of database rollup properties

The following screen shows the database rollup properties on the DB Admin tab.

Database Rollups:

☒ Use database rollups.

Rollup Frequency:

monthly

Set Schedule...

33

 number of days of hourly data to keep.

6

 number of months of monthly data to keep.

3

 number of days of billing data to keep.

3

 number of days of streaming data to keep.

Database rollup properties

The following table describes the database rollup properties.

Property	Description
Rollup Frequency	The frequency (Daily, Weekly, Monthly) of database rollups. You can specify in the Number of Days to Keep Hourly Data field how often all hourly data in the database is converted into monthly data. The Set Schedule button launches the Rollup Scheduled window to specify the rollup frequency.

Property	Description
Number of days of hourly data to keep	The minimum number of days of hourly data to keep available for reports in your database. Immediately after a database rollup, you have exactly this many days of hourly data in the database. After a rollup, the hourly data in the database increases by one day each day until the next rollup. For example, if you schedule database rollups for the 1st and 15th of the month and specify to keep 33 days of hourly data in your database, you have 33 days of hourly data immediately after the rollup on the 1st of the month, 46 days of hourly data on the 14th day of the month, and then 33 days of hourly data immediately after the rollup on the 15th day of the month.
Number of months of monthly data to keep	The number of months of monthly data to keep available for reports in your database. Immediately after a database rollup, you have exactly this many months of monthly data in the database. For example, if you set this number to six months and schedule a rollup to occur on October 1st, you will have monthly data available in your database for reports for the months of April through September.
Number of days of billing data to keep	The minimum number of days of billing data to keep available for reports in your database. Immediately after a database rollup, you have exactly this many days of billing data in the database. After a rollup, the billing data in the database increases by one day each day until the next rollup.
Number of days of Streaming data to keep	The minimum number of days of streaming data to keep available for reports in your database. Immediately after a database rollup, you have exactly this many days of streaming data in the database. After a rollup, the amount of streaming data in the database increases by one day each day until the next rollup.
Apply and OK buttons	Enables you to save changes to the ContentReporter server. If you click OK, you return to the Administration page. If you click Apply, you remain on this tab. If you want to make multiple, interdependent changes to settings on this tab, you must click Apply after each interdependent change.

Billing tab

What it provides

The Billing tab enables you to configure billing aggregation for Billing reports. You can select three of twelve fields (such as Hits and Bytes Dropped), the action taken on the data (such as calculating the average or total), and the number of minutes over which to measure the data.

To learn more about configuring billing aggregation, see [“Configuring Billing aggregation”](#) on page 163.

What it looks like

The following screen shows the Billing tab.

The screenshot shows a web-based configuration interface for the Billing tab. At the top, there is a horizontal menu with tabs: Cache Group, User Groups, Authentication, DB Admin, Billing (selected), Licensing, and Logging. Below the menu, the main configuration area is titled "Billing Aggregation Interval (minutes):". It contains a dropdown menu set to "5" and a checkbox labeled "Enable billing processing" which is checked. Below this, there are three rows of configuration for fields and actions. Each row has a label (Field 1, Field 2, Field 3) and an action label (Action 1, Action 2, Action 3). Field 1 is set to "Bytes", Action 1 is set to "Total". Field 2 is set to "Hits", Action 2 is set to "Max". Field 3 is set to "Packets Served", Action 3 is set to "Average". At the bottom left, there is a "Reset" button.

Field	Action
Field 1: Bytes	Action 1: Total
Field 2: Hits	Action 2: Max
Field 3: Packets Served	Action 3: Average

Reset

Billing aggregation settings The following table describes Billing tab settings.

Setting	Description
Enable billing processing check box	Enables and disables billing processing.
Time Interval	The number of minutes over which the billing data is aggregated. The shorter you set the interval, the finer the level of detail (or “granularity”) of the data you generate.
Available fields (Billing Statistics)	Hits, Bytes, Bytes Dropped, Packets Requested, Packets Served, Packets Resent, Packets Dropped, Streaming Connect Time, Play Time, Response Time, Streaming Transfer Time, and Streaming Average Bit Rate
Action taken on field data	Minimum, Maximum, Average, or Total
Apply and OK buttons	Enables you to save changes to the ContentReporter server. If you click OK, you return to the Administration page. If you click Apply, you remain on this tab. If you want to make multiple, interdependent changes to settings on this tab, you must click Apply after each interdependent change.

Administration page

Licensing tab

What it provides

The Licensing tab enables you to examine your current license information and upgrade your license.

To learn more about entering license information, see “[Examining and upgrading your license information](#)” on page 146.

What it looks like

The following screen shows the Licensing tab.

Cache Group	User Groups	Authentication	DB Admin	Billing	Licensing	Logging
Product License Key:		12345				
Serial No:		12345				
License Type:		Primary				
Number of caches:		5				
Expiration:		None				
Upgrade License:						Upgrade

Licensing tab fields The following table describes the Licensing tab fields.

Field	Function
Product License Key	Lists your current License Key.
Serial No. field	Lists your current serial number.
License Type field	Lists your current type of license.
Number of caches	Lists the maximum number of node devices you can add to cache groups with your current License Key.
Expiration field	Lists either an expiration date (if you are using an Evaluation copy of ContentReporter), or no date (if you are using a purchased copy of ContentReporter).
Upgrade License field	Enables you to enter a new License Key to upgrade from an Evaluation copy of ContentReporter, or to increase the maximum number of node devices or ContentReporter servers.
Apply and OK buttons	Enables you to save changes to the ContentReporter server. If you click OK, you return to the Administration page. If you click Apply, you remain on this tab. If you want to make multiple, interdependent changes to settings on this tab, you must click Apply after each interdependent change.

Logging tab

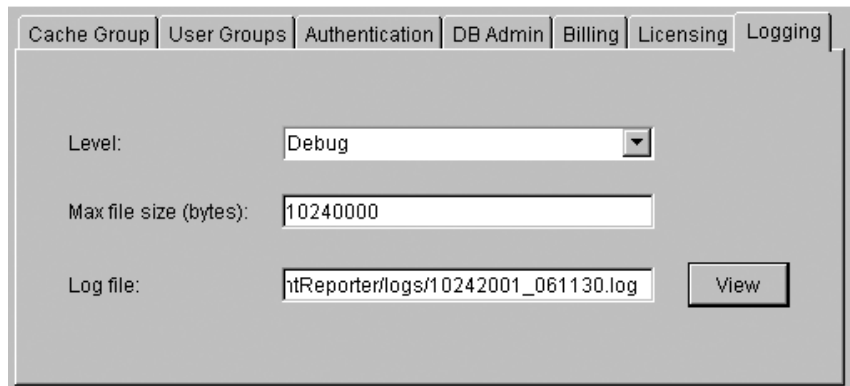
What it provides

The Logging tab enables you to configure the ContentReporter server logging and examine the current ContentReporter log file.

To learn more about configuring the ContentReporter log file, see “[Configuring ContentReporter server logging](#)” on page 149.

What it looks like

The following screen shows the Logging tab.



The screenshot shows a web interface with a tabbed menu at the top. The tabs are: Cache Group, User Groups, Authentication, DB Admin, Billing, Licensing, and Logging. The 'Logging' tab is selected. Below the tabs, there are three configuration fields: 'Level:' with a dropdown menu set to 'Debug', 'Max file size (bytes):' with a text input field containing '10240000', and 'Log file:' with a text input field containing 'htReporter/logs/10242001_061130.log'. To the right of the 'Log file:' field is a 'View' button.

Logging tab components

The following table describes the Logging tab components.

Component	Function(s)
Level field drop-down list	Specifies one of five levels of information (Debug, Info, Status, Warning, or Terminal) you want to record in the ContentReporter log file. Debug generates log files with the most comprehensive information about ContentReporter, and Terminal generates log files with the least comprehensive information about ContentReporter.
Max file size field	Lists the log file size at which ContentReporter begins generating a new log file. The default size is 10.24 MB. You can accept the default size or enter a different value.
Log file field	Lists the name of the current ContentReporter log file.
View button	Enables you to view the current ContentReporter log file in Notepad or a similar text file editor.
Apply and OK buttons	Enables you to save changes to the ContentReporter server. If you click OK, you return to the Administration page. If you click Apply, you remain on this tab. If you want to make multiple, interdependent changes to settings on this tab, you must click Apply after each interdependent change.

Import Log Files page

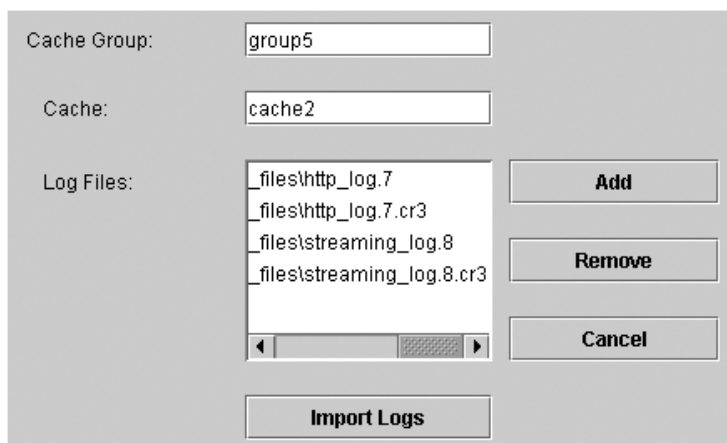
What it provides

The Import Log File page give you the ability to process log files for a cache device without creating a scheduled event. This feature enables you to process log files that were not collected or processed by a scheduled event and output the result to your database for a new or existing cache device.

To learn more about importing log files, see “[Importing saved log files](#)” on page 111.

What it looks like

The following screen shows the Import Log Files page.



The screenshot displays the 'Import Log Files' page interface. It features a light gray background with several input fields and buttons. On the left, there are labels for 'Cache Group:', 'Cache:', and 'Log Files:'. The 'Cache Group:' field contains the text 'group5'. The 'Cache:' field contains the text 'cache2'. The 'Log Files:' field is a list box containing four entries: '_files\http_log.7', '_files\http_log.7.cr3', '_files\streaming_log.8', and '_files\streaming_log.8.cr3'. To the right of the list box are three buttons: 'Add', 'Remove', and 'Cancel'. Below the list box is a horizontal scrollbar. At the bottom center of the form is a large button labeled 'Import Logs'.

Import Log File page components

The following table describes the Import Log File page components.

Component	Function
Cache Group field	Lists the name of the cache group of the cache device that generated the log file or file. If you selected the check box adjacent to a cache on the Administration page before opening the Import Log Files page, this field displays the cache's cache group.
Cache field	Lists the name of the cache device that generated the log file. If you selected the check box adjacent to a cache on the Administration page before opening the Import Log Files page, this field displays the cache's name.
Log Files panel	Lists the log files you selected to be imported.
Add button	Enables you to browse to the folder that contains the log files, and to select one or more log files.
Remove button	Deselects one or more log files for importing.
Import Logs button	Launches the process of importing and process the selected log files.

Scheduled Events page

What it provides

The Scheduled Events page enables you to create and manage scheduled log file collection events and scheduled report generation events. The Scheduled Event tabs give you the ability to specify the type of event, the time and frequency of an event, and any security settings to apply to an event.

To learn more about scheduling log file collection, see “[Scheduling log file collection and processing](#)” on page 94.

To learn more about scheduling reports, see the *ContentReporter 3.0 Reporting Guide*.

What it looks like

The following screen shows the Scheduled Events page.

Version: 3.0D_011023_1001



NetworkAppliance®

Copyright © 2001 Network Appliance

ContentReporter

Administration

Query Definitions

Report Definitions

Scheduler/Events

Report Results

Scheduled Events

New

Copy

Edit

Run

Delete

Check All

History

Find

refresh sec 0

Start

Stop

Task Name	Created Date	State	Status Condition	Schedule	Next Run Date	Type
1 ☐ techpubs11272001_163906	11/27/01	Expired		One Time Only	Never	Manual File Import
2 ☐ Collect from ts caches.	10/29/01	Completed		hourly	Tue @ 4:07 PM 10/30/01	Collect and or import logs
3 ☐ X4 report	10/29/01	Completed Successful		one time only	Mon @ 10:43 AM 10/29/01	Reporting

Scheduled Events page components

The following table describes the Scheduled Events page components and their functions.

Component	Function
Task Name column	Lists the name of each scheduled event.
Created Date column	Lists the creation date of each scheduled event.
State column	Lists the state, such as Running, Idle, or Completed, of each scheduled event.
Status Condition column	Provides feedback, such as “Aggregating hourly data” and “Successful,” about each scheduled event as it occurs.
Schedule column	Lists the frequency, such as “one time only,” “hourly,” and “weekly,” of each scheduled event.
Next Run Date column	Lists the date of each scheduled event’s next (or only) occurrence.
Type column	Lists the type (either “Collect and or import logs,” “Manual File Import,” or “Reporting”) of each scheduled event.
New button	Creates a new scheduled event.
Copy button	Creates a new scheduled event with the configuration of an existing one.
Edit button	Edits a scheduled event’s configuration.
Run button	Immediately runs a scheduled event.
Delete button	Deletes a scheduled event.
Check All/UnCheck All button	Selects or deselects all scheduled events.
History button	Enables you to view scheduled event information, such as the Start Time, Finish Time, Duration, Status, and Type. Also enables you to open the following pages: Logs page: Lists the log files collected for an occurrence of a scheduled event. Details page: Lists the ContentReporter server’s actions, such as “Collecting from” or “Getting file,” and status, such as “Completed” and “Successful,” for each occurrence of a scheduled event.

Component	Function
Task Display Filter field	Specifies a filter value for the list of scheduled events.
Find button	Filters the display of scheduled events with the Task Display Filter field value (by executing a “find” of the filter value). Displays all scheduled events if the Task Display Filter field is blank.
Refresh sec field	Specifies the automatic refresh (reload) rate, in seconds, of the Scheduled Events page.
Start/Stop button	Starts or stops the automatic refresh (reload) of the Scheduled Events page.

For detailed information

For details about the Scheduled Events page tabs, see the following sections:

- ◆ “[Details tab](#)” on page 59
- ◆ “[Schedule tab](#)” on page 61
- ◆ “[Security Tab](#)” on page 63

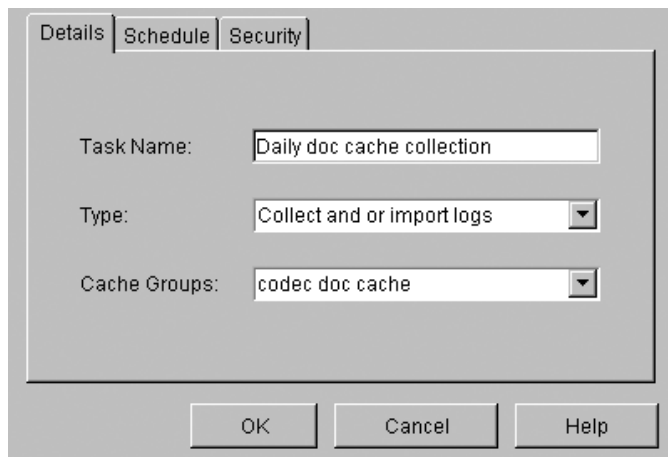
Details tab

What it provides

The Scheduled Events Details tab enables you to specify a name for a new scheduled event, and the type and (cache group or report definition) for a new or existing scheduled event.

What it looks like

The following screen shows the Details tab.



The screenshot shows a dialog box with three tabs: 'Details', 'Schedule', and 'Security'. The 'Details' tab is selected. Inside the dialog, there are three input fields: 'Task Name' with the text 'Daily doc cache collection', 'Type' with a dropdown menu showing 'Collect and or import logs', and 'Cache Groups' with a dropdown menu showing 'codec doc cache'. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

Details tab components

The following table describes the Details tab components.

Component	Function
Task Name field	Lists the name of a new or existing scheduled event.
Type drop-down list	Enables you to select the scheduled event's type. When you select "Collect and/or import logs" from the Type drop-down list, the lower field is the Cache Groups drop-down list. When you select "Reporting" from the Type drop-down list, the lower field is the Definitions drop-down list.
Cache Groups drop-down list	Enables you to select a cache group from which to collect and process log files for this scheduled event.
Definitions drop-down list	Enables you to select a report definition with which to generate a report for this scheduled event.

Schedule tab

What it provides

The Scheduled Events Schedule tab enables you to specify the time and frequency of a new or existing scheduled event.

What it looks like

The following screen shows the Scheduled Events Schedule tab.

The screenshot shows a dialog box with three tabs: 'Details', 'Schedule', and 'Security'. The 'Schedule' tab is selected. The dialog contains the following fields and controls:

- Execute this task:** A dropdown menu set to 'weekly'.
- Start time:** A text box containing '1:05 AM'.
- Start date:** A date picker showing '11 / 5 / 2001'.
- End date:** A date picker showing '11 / 6 / 2001'.
- Ignore end date:** A checked checkbox.
- Select day(s) of the week:** A group box containing seven checkboxes:
 - ☐ Sun
 - ☒ Mon
 - ☒ Tues
 - ☒ Weds
 - ☒ Thurs
 - ☒ Fri
 - ☐ Sat

At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

Schedule tab components

The following table describes the Schedule tab components.

Component	Function
Execute This Task field drop-down list	Specifies a scheduled event's frequency. As you select different frequencies, the Schedule tab changes dynamically.
Start Date field	Specifies the first day this scheduled event's Schedule tab settings take effect.
End Date field	Specifies the last day this scheduled event's Schedule tab settings take effect.
Ignore End Date check box	Configures the scheduled event to ignore the end date. If you leave this check box selected, ContentReporter continues to run this scheduled event at the scheduled intervals for an indefinite period of time.
Start Time field	Lists the first time this scheduled event runs. You can leave the default time or enter a different time.

Security Tab

What it provides

The Security tab enables you to set permissions on Local users and user groups for a particular scheduled event, query definition, or report definition. The Security tab enables you to prevent certain users or groups from seeing, modifying, running, selecting, or deleting an event or definition.

What it looks like

The following screen shows the Security tab.

The screenshot shows a dialog box with three tabs: 'Details', 'Schedule', and 'Security'. The 'Security' tab is selected. Inside the dialog, there are two sections: 'Users' and 'Groups'. Each section has a 'Names:' label followed by a text input field. Below each input field are four checkboxes: 'Read', 'Write', 'Execute', and 'Delete'. In the 'Users' section, the input field contains 'Steve', and all four checkboxes are checked. In the 'Groups' section, the input field contains 'Guest', and the 'Read' and 'Execute' checkboxes are checked, while 'Write' and 'Delete' are unchecked. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

Entity	Read	Write	Execute	Delete
Users: Steve	☒	☒	☒	☐
Groups: Guest	☒	☐	☒	☐

Security tab components

The following table describes the Security tab components.

Component	Function
Users Names field	Specifies the user name or names on which you want to set security settings for the event or definition.
Groups Names	Specifies the group name or group names on which you want to set security settings for the event or definition.
Read check box	Specifies whether a user or group has permission to see a particular event or definition.
Write check box	Specifies whether a user or group has permission to examine or modify a particular event or definition.
Execute check box	Specifies whether a user or group has permission to run a particular event or select a particular definition.
Delete check box	Specifies whether a user or group has permission to delete a particular event or definition.

About this chapter

This chapter discusses the three-step process of setting up log file collection:

- ◆ Defining a cache group
- ◆ Adding one or more caches to the cache group
- ◆ Scheduling collection of the cache group's log files

It also discusses the ways you can modify cache groups and caches and import log files for a cache device without creating a scheduled event. After you set up log file collection and the ContentReporter server processes the log files, you can generate reports on the caches.

Note

To set up and schedule log file collection by following “Quick-Start” instructions, see Appendix A, “[Quick-start: Setting up log file collection](#),” on page 170.

Topics in this chapter

This chapter covers the following topics:

- ◆ “[Step one: Defining a cache group](#)” on page 66
- ◆ “[Step two: Adding caches to the cache group](#)” on page 71
- ◆ “[Step three: Scheduling log file collection](#)” on page 93
- ◆ “[Modifying cache groups and caches](#)” on page 102
- ◆ “[Importing saved log files](#)” on page 111

Step one: Defining a cache group

What a cache group is

A cache group is a logically defined group of one or more caches. Caches, in ContentReporter, are the devices that generate the log files that the ContentReporter server collects and processes. A cache group is a management tool that enables you to specify the time and frequency of log file collection, and the type of log file analysis for a number of caches. Defining a cache group is the first step in the process of setting up log file collection.

Note

You can only create scheduled events to collect and process log files from cache groups, not individual caches. If you want to create a scheduled event to collect and process one cache's log files, you need to place it in its own cache group.

Where you access cache group information

You can access cache group information from the following sources:

- ◆ Administration page—The Administration page lists all cache groups and caches for which one or more ContentReporter servers are outputting data to your database.
- ◆ Administration Cache Group tab—You manage and modify cache groups through the Cache Group tab. You see cache groups listed under ContentReporter servers.

The Administration page

The following screen shows cache groups on the Administration page.

Administration | Query De

Administration Cache Group Report

Admin | Import

	Group Name	Cache Name	IP Address	Type
1	☐ cachegroup1	c3.domainname.com	12.34.56.78	NetCache C720
2	☐ cachegroup1	c5.domainname.com	12.34.56.78	NetCache C6100
1	☐ cachegroup2	c1.domainname.com	12.34.56.78	NetCache C1105
1	☐ QAcachegroup	c2.domainname.com	12.34.56.78	NetCache C760
2	☐ QAcachegroup	c6.domainname.com	12.34.56.78	NetCache C720
3	☐ QAcachegroup	c4.domainname.com	12.34.56.78	NetCache C6100

The Cache Group tab

The following screen shows cache groups created with the ContentReporter server on the “bills-nt” machine on the Cache Group tab.

Cache Group

CR_bills-nt

cachegroup1

c6.domainname

c2.domainname

cachegroup2

c3.domainname

Name	Http Analysis	Streaming Anal...
cachegroup1	☒	☒
cachegroup2	☒	☒

Cache group information you can define

You can define the type of log files to collect and process for each cache group:

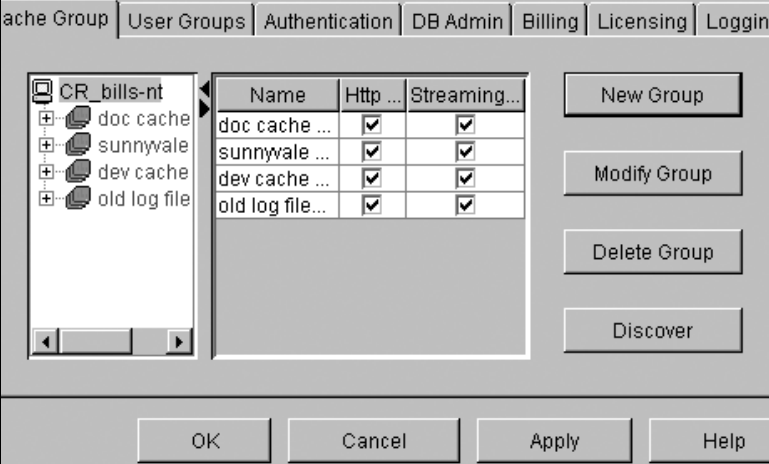
- ◆ HTTP analysis—HTTP (or Web Access) log files are helpful for tracking the types of objects that are cache hits and misses. They are also helpful for evaluating the load on a NetCache appliance (for example, peak performance and which content is requested at peak times).
- ◆ Streaming analysis—Streaming Access log files record client and server information for streaming media connections. Each log entry contains specific connection information that you can use to diagnose and solve problems, optimize performance, and track usage patterns.
- ◆ Both

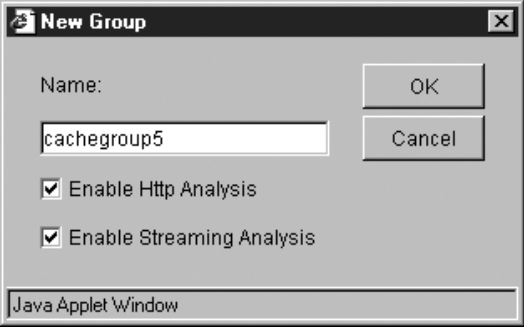
To learn more about configuring a NetCache for Web Access logging, see Appendix C, “[Enabling NetCache appliance Web Access logging](#),” on page 184.

To learn more about configuring a NetCache for Streaming Access logging, see Appendix C, “[Enabling NetCache appliance Streaming Access logging](#),” on page 185.

Defining a cache group

To define a cache group, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab.
2	From the Administration page, click the Admin button.
3	From the Cache Group tab, click New Group. Result: The New Group window appears. 
4	Enter a unique name for the cache group, select the type of log file analysis to perform, and then click OK. Result: You return to the Cache Group tab, and this cache group appears in the cache group listing.

Step	Action
5	Click OK or Apply to save the changes. Result: You successfully defined the cache group. 

Step two: Adding caches to the cache group

What a cache is

In ContentReporter, a cache is a device that generates the log files that the ContentReporter server collects/imports and processes. ContentReporter can collect/import and process NetCache™ appliance log files, Web server log files, and streaming server log files. Adding one or more caches to a cache group is the second step in the process of setting up log file collection.

Rules for adding caches

You must follow these rules when adding caches to a cache group:

- ◆ Each cache must have a unique name in ContentReporter. If you attempt to add a cache with the name of another cache, ContentReporter prompts you to enter a different name.
- ◆ For every 1 GB of log data you collect and process, ContentReporter needs 2 GB of temporary space in the stored log file directory during the collection and processing event.

Where you add caches

You can add caches from the New Cache window and from the Auto Discovery window.

New Cache window The following screen shows the New Cache window.

New Cache

Name:

Log file location:

☒ Collect from NetCache

☐ Collect from FTP Server

☐ Collect from imported directory

Store collected files here:

Log file format:

☐ Log file contains no header field.

☐ Web Access log format

☐ Common log format

☐ Netscape Extended log format

☐ Squid

☐ Streaming Access

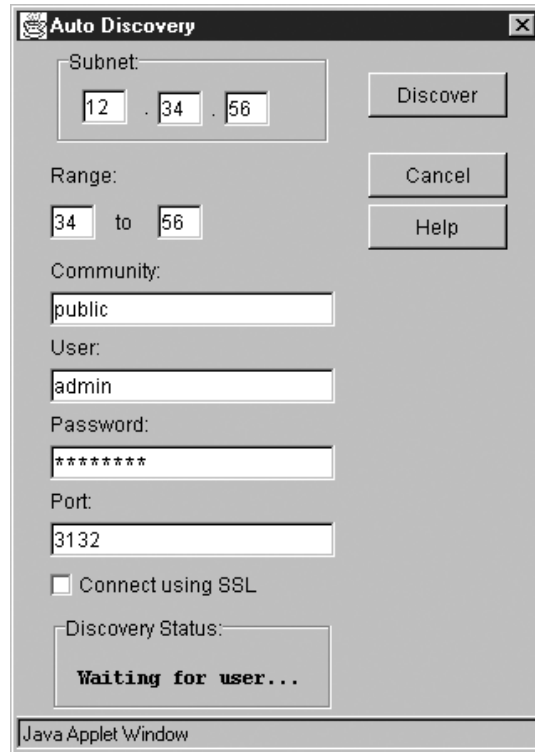
☐ Real

☐ Delete log files after parsing.

Stop parsing when error lines exceed:

The Auto Discovery window

The following screen shows the Auto Discovery window.



The screenshot shows a Java Applet Window titled "Auto Discovery". It contains several input fields and buttons. The "Subnet:" field has three boxes containing "12", "34", and "56". The "Range:" field has two boxes containing "34" and "56" with the word "to" between them. The "Community:" field contains the text "public". The "User:" field contains the text "admin". The "Password:" field contains seven asterisks "*****". The "Port:" field contains the text "3132". There is a checkbox labeled "Connect using SSL" which is currently unchecked. The "Discovery Status:" field contains the text "Waiting for user...". On the right side, there are three buttons: "Discover", "Cancel", and "Help".

For detailed information

For details about adding caches, see the following topics:

- ◆ [“Cache properties”](#) on page 74
- ◆ [“Adding a cache to collect from a directory”](#) on page 76
- ◆ [“Adding a cache to collect from NetCache appliances”](#) on page 78
- ◆ [“Adding a cache to collect from an FTP server”](#) on page 91

Cache properties

Stored log files directory

When ContentReporter collects log files from a NetCache or an FTP server, it copies (stores) the log files into the location specified to store the log files and then processes the log files. This directory is the ContentReporter server's "work area" for the cache. After processing, the ContentReporter server either leaves the log files in the folder or deletes them. By default, ContentReporter stores a cache's collected log files in the ContentReporter server directory:

```
..\Network Appliance\ContentReporter\jakarta-  
tomcat\webapps\ContentReporter\cache group\cache\
```

You can change this directory to a location that better suits your space requirements.

Temporary space requirements: While ContentReporter processes log files, it stores log files and creates temporary files in the stored log file directory. ContentReporter requires 2 GB of temporary space for every 1 GB of log data you collect and process during collection and processing.

Examples of space requirements: The following table lists the amount of temporary space you need during various collection and processing events.

Scheduled events to collect twenty 100-MB log files per cache	Temporary space needed during collection and processing
A scheduled event to process logs for a cache group with one cache	4 GB
A scheduled event to process logs for a cache group with five caches	20 GB
Two concurrent scheduled events to process logs for two cache groups with five caches	40 GB

Note

If ContentReporter stops processing a log file, it saves the log file in the stored log files directory even if you configured ContentReporter to delete the log file after processing. For example, if ContentReporter stops processing a log file with an unacceptable number of error lines, it save the log file in this directory. You should monitor the directories you select to store collected log files to ensure adequate disk space and to identify any unprocessed log files.

Headerless log file format

ContentReporter automatically recognizes NetCache appliance log files (as well as WMS and QuickTime log files) when it processes them because they contain identifying headers. However, some log files contain no headers by which they can be identified. If you add a cache to process headerless Web server or streaming server log files, you must specify the log file type when you set the cache properties in the New Cache window.

Note

If you attempt to process a headerless log file without specifying the format, the ContentReporter parser does not process the log file; it returns the invalid log file header error code (- 4) to the ContentReporter log file.

Delete log files after parsing

ContentReporter enables you to either leave the collected log files in the stored log files directories from which the log files were collected, or to delete them after processing. If you configure ContentReporter to collect a cache's log files at scheduled intervals and choose to leave the log files in the stored log files directory, you should monitor these locations to ensure disk space availability.

Stop parsing when error lines exceed maximum

By default, ContentReporter stops processing a log file if it records 200 error lines in a log file. You can change this value to a number that better suits your needs. To have no limit, set the number of error lines to 0. If the ContentReporter server stops processing a log file because number of error lines has exceeded the maximum, the error code (- 11) is written to the ContentReporter log file.

Adding a cache to collect from a directory

About collecting from a directory

You can configure ContentReporter to collect log files from a directory, such as a local or mapped drive folder, that is accessible to the ContentReporter service's login user account.

By default, the ContentReporter service uses the Local System Account, and automatically starts when the system starts up. If you want to access network resources such as mapped drives, you can assign a login user account to the ContentReporter service. See Appendix B, "[Learning about the login user account](#)," on page 178.

Collecting from a directory

To add a cache to collect and process log files from a directory, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab.
2	From the Administration page, click the Admin button.
3	From the Cache Group tab, select a cache group in the left-hand panel, then click New Cache.
4	From the New Cache window, enter a name for the log file source, click the "Collect from imported directory" button, and click Browse.
5	Browse to the location of the saved log files, then double-click the directory. Result: You return to the New Cache window, and the location of the saved log files appears in the Import log files directory field.
6	If the log files contain no header, select the check box and click the radio button for the log file's format.
7	If you want to delete the log files after processing, select the appropriate check box.

Step	Action
8	Accept the default number of error lines (200), or enter another number. If you do not want the number of error lines in a log file to stop the ContentReporter server from processing, enter the number 0.
9	Click OK. Result: You return to the Cache Group tab and the cache appears under the cache group in the left-hand panel.
10	Click Apply or OK to save the changes to the ContentReporter server. Result: You successfully added a cache to collect and process log files from a directory.
11	Go to “ Step three: Scheduling log file collection ” on page 93 to create a scheduled event to collect and process this cache group’s log files.

Adding a cache to collect from NetCache appliances

About collecting from NetCache appliances

You can configure ContentReporter to use HTTP or HTTPS to collect log files from one or more NetCache appliances at scheduled intervals.

Note

When you configure ContentReporter to collect NetCache appliance log files, you must synchronize NetCache appliance logging and ContentReporter log file collection to ensure data integrity. If you do not want to synchronize NetCache logging and ContentReporter log file collection, configure your NetCache to push its log files to either a directory or an FTP server. To learn about synchronizing NetCache logging and ContentReporter collection, see Appendix C, “[Synchronizing logging rotation and log file collection](#),” on page 191.

Methods of adding caches

ContentReporter provides two methods of adding caches to collect and process NetCache appliance log files:

- ◆ “[Manually adding a NetCache appliance](#)” on page 82
- ◆ “[Using Auto Discovery](#)” on page 85

Potential prerequisite for collecting log files

If you installed SecureAdmin™ software on a NetCache appliance, you can configure ContentReporter to use the Secure Sockets Layer (SSL) protocol to securely collect log files from the NetCache. SSL configuration is discussed in “[Configuring ContentReporter for SSL](#)” on page 80. You must complete this configuration process before you add a cache to collect and process NetCache appliance log files.

Using the SSL protocol

SSL provides an encrypted administrative exchange between a NetCache and a client browser. By default, the ContentReporter server uses port 443 to access the NetCache log files when using SSL. When the ContentReporter server accesses the NetCache appliance log files through SSL, it uses the SSL certificate that you copied to the ContentReporter machine during this configuration process. You can use a self-signed certificate generated by the NetCache appliance, or a CA-signed certificate signed by a trusted authority for secure Web services, such as Verisign, Inc., SecureIT Enterprise, and Thawte Consulting.

Note

For ContentReporter to collect a NetCache appliance's log files using the SSL protocol, you must ensure that you configured the DNS settings of the machine on which you installed ContentReporter so that the ContentReporter server can resolve the fully qualified domain name of the NetCache appliance.

Cache Name for SSL

If ContentReporter will collect NetCache log files using the SSL protocol, you must copy the NetCache SSL certificate into the ContentReporter server folder:

```
..\Network Appliance\ContentReporter\jakarta-  
tomcat\webapps\ContentReporter\
```

and save the certificate file as *cachename.cer* (where *cachename* is the name you will enter for the cache in the Name field of the New Cache window if you manually add the cache to a cache group and *.cer* is the required file extension).

See step 8 of [“Configuring ContentReporter for SSL”](#) on page 80 and step 4 of [“Manually adding a NetCache appliance”](#) on page 82.

Note

If you add a cache using the Auto Discovery feature to collect from a NetCache with SSL, save the certificate file as *cachename.cer* (where *cachename* is the NetCache appliance's fully qualified domain name and *.cer* is the required file extension).

NetCache Name or IP Address for SSL

The name you enter (when generating the SSL certificate) in the Common Name field in Step 4 (Generate the SSL Certificate) of the Software - SecureAdmin page of the Maintenance tab of the NetCache management console must match the name you specify for the NetCache in the Name or IP Address field of ContentReporter's NetCache Settings window. If these names do not match, the certificate will not be accepted and the log file collection will fail.

See step 5 of [“Manually adding a NetCache appliance”](#) on page 82.

Note

By default, the Auto Discovery feature of ContentReporter uses the NetCache appliance's IP address in the Name or IP Address field of the NetCache Settings window. If you add a cache using the Auto Discovery feature to collect from a NetCache with SSL, modify the Name or IP Address field value for the cache after adding the cache with Auto Discovery to match the name you entered in the NetCache management console Common Name field.

Configuring ContentReporter for SSL

To configure ContentReporter to collect a NetCache appliance's log files using the SSL protocol, complete the following steps.

Note

Complete the following configuration steps for each NetCache appliance that will have its log files collected by ContentReporter using SSL.

Note

The following instructions explain how to import a self-signed certificate for Internet Explorer 5.0. Some of these steps will vary for other browsers.

Step	Action
1	Enable SSL on the NetCache appliance.
2	To test whether the ContentReporter server can resolve the fully qualified domain name of the NetCache, enter the following at the command line of the ContentReporter server machine: <pre>> nslookup cachename</pre> <i>cachename</i> is the fully qualified domain name of the NetCache. Result: Your system displays the results of the <code>nslookup</code> command. If your system found the NetCache, continue with Step 3. If your system did not find the NetCache, ask your IT Administrator to correct this problem, and then continue with Step 3.
3	Browse to the NetCache using HTTPS.
4	From the Security Alert window, click View Certificate.
5	From the Certificate window, click the Details tab, and then click Copy to File.

Step	Action
6	From the Certificate Manager Export Wizard, click Next.
7	From the Certificate Export File window, select the Base64 Encoded X.509 (.CER) button, and click Next. Result: The Export File Name window appears.
8	On the ContentReporter server machine, browse to the ..\Network Appliance\ContentReporter\jakarta-tomcat\webapps\ContentReporter\ directory and enter <i>cachename.cer</i> for the file name. <i>cachename</i> is the name you will enter for the cache in the Name field of the New Cache window if you manually add the cache to a cache group, or the NetCache's fully qualified domain name if you will use Auto Discovery to add the cache to a cache group <i>.cer</i> is the required file extension To learn more about the certificate name, see “Cache Name for SSL” on page 79.
9	Click Next to copy the NetCache's certificate into the directory.
10	Click Finish to return to the Certificate window.
11	Click OK to return to the Security window.
12	Click Yes to confirm that you can open the NetCache Manager using the SSL protocol.
13	Close the NetCache Manager.
14	Repeat Steps 1-13 for each NetCache you want to add to a cache group.
15	Add caches to a cache group ◆ “Using Auto Discovery” on page 85. ◆ “Manually adding a NetCache appliance” on page 82.

Manually adding a NetCache appliance

If you prefer to add a NetCache appliance to a group without using the Auto Discovery feature, you can manually add one NetCache at a time to a cache group.

To manually add a NetCache appliance to a cache group, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab.
2	From the Administration page, click the Admin button.
3	From the Cache Group tab, select a cache group in the left-hand panel, and click New Cache.
4	In the New Cache window, enter a name for the NetCache, select the Collect from NetCache button, and then click Settings. Note If ContentReporter will collect from this NetCache using the SSL protocol, this name must match the SSL certificate file name (without the <i>.cer</i> extension). To learn more about naming the SSL certificate, see “Cache Name for SSL” on page 79.
5	In the NetCache Settings window, enter the NetCache’s IP address or fully qualified domain name. Note If ContentReporter will collect from this NetCache using the SSL protocol, this value must match the NetCache’s Common Name field value you entered when generating the SSL certificate. To learn more about the NetCache Name or IP Address field value, see “NetCache Name or IP Address for SSL” on page 79.
6	Enter the NetCache user name and password.
7	Ensure that the port field displays 3132 if NetCache allows HTTP collection of log files, or select the SSL check box and ensure that the port field displays 443 to allow SSL protocol collection.

Step	Action	
8	To test connectivity between ContentReporter and the NetCache, click Test. Result: The Test Cache Connectivity window appears. When ContentReporter completes the test, displays a status of either “available” or “not available.”	
9	If...	Then...
	The NetCache has an “available” status	Click OK to return to the NetCache Settings window.
	The NetCache has a “not available” status	1. Click OK to return to the NetCache Settings window. 2. Verify that you entered the correct IP Address or a fully qualified domain name that can be resolved by the machine on which you installed ContentReporter. 3. Verify that a network connection exists between the NetCache and the ContentReporter server machine. 4. If using SSL, verify that the Cache Name matches the certificate name, that the certificate is in the proper directory, and that the NetCache Name or IP Address matches the NetCache’s “Common Name” field value. 5. Repeat Step 8.
10	If you want, enter the NetCache model, such as C720, and the NetCache OS version, such as 5.1R2D5.	

Step	Action
11	Click OK to return to the New Cache window.
12	Accept the default location to store this cache's log files, or click Browse, select an appropriate directory, and click OK. Note— The ContentReporter server copies the log files to this location before processing them. If it fails to process a particular log file, it leaves the log file in this directory.
13	To delete the log files after processing, select the appropriate check box.
14	Accept the default number of error lines (200), or enter another number. If you do not want the number of error lines in a log file to stop the ContentReporter server from processing, enter the number 0.
15	After you enter all the required information, click OK. Result: You return to the Cache Group tab and the cache appears under the cache group in the left-hand panel.
16	Click Apply or OK to save the changes to the ContentReporter server. Result: You successfully added the NetCache to a cache group.
17	Go to “ Step three: Scheduling log file collection ” on page 93 to create a scheduled event to collect and process this cache group's log files.

**Using Auto
Discovery**

You can use the ContentReporter Auto Discovery feature to add one or more SNMP-enabled NetCache appliances (for which you have community string names) to a cache group to collect and process log files. You can only discover NetCaches with Class C IP addresses using the Auto Discovery feature. Each NetCache appliance has an IP address consisting of four numbers separated by periods. In ContentReporter, the first three numbers represent the subnet on which the NetCache is located. You can add some or all of the NetCache appliances located on the same subnet at one time with the Auto Discovery feature.

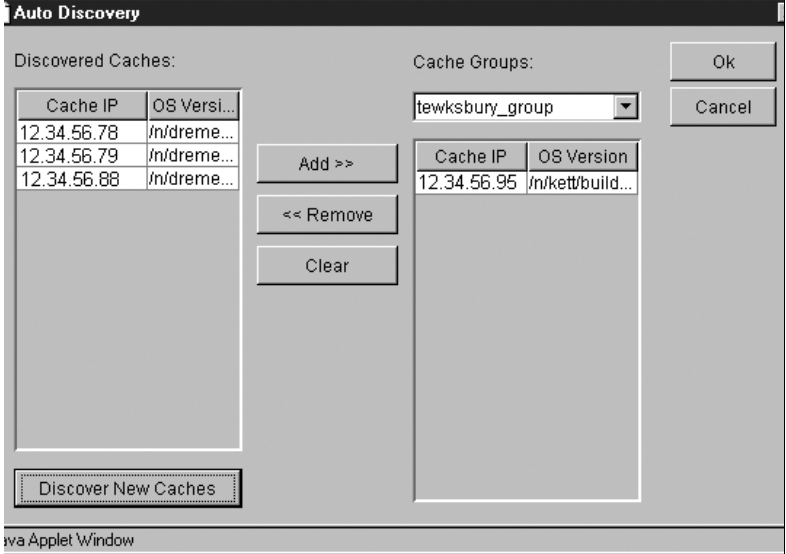
Note—————
You can only detect SNMP-enabled NetCaches for which you have a community string names with the Auto Discovery feature. For more information, see Appendix C, “[Enabling SNMP and using Auto Discovery](#),” on page 194.

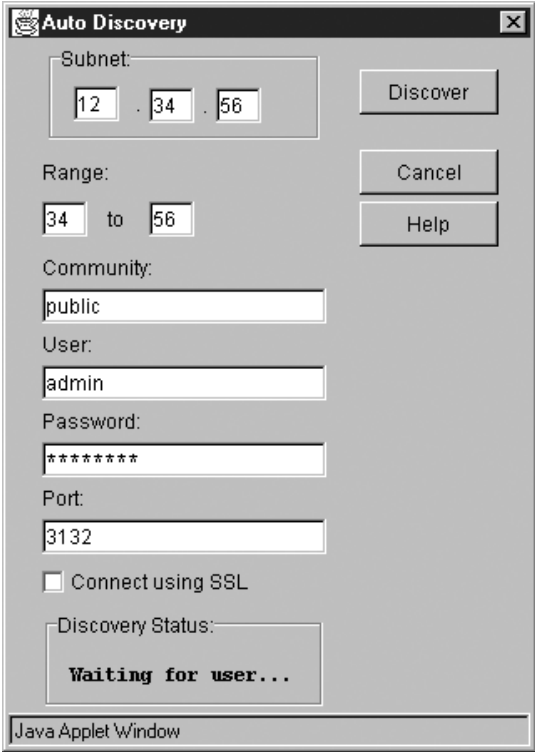
**Adding caches with
Auto Discovery**

To use Auto Discovery to add NetCache appliances to a cache group, complete the following steps.

Note—————
If you want to use Auto Discovery to discover some NetCaches that allow collection by SSL and others that do not, complete the following steps twice. The first time you complete these steps, select SSL in Step 9, and select only the NetCaches that allow collection by SSL in Step 11. The second time you complete these steps, do not select SSL in Step 9, and select only the NetCaches that do not use SSL in Step 11.

Step	Action
1	From a page in ContentReporter, click the Administration tab.
2	From the Administration page, click the Admin button.
3	From the Cache Group tab, select a cache group in the left-hand panel, and click Discover. Result: The first Auto Discovery window appears.

Step	Action
4	Ensure that the appropriate cache group appears in the upper-right Cache Groups field, then click Discover New Caches. Result: The second Auto Discovery window appears. 
5	Enter the subnet on which the NetCache appliances are located.
6	In the Range fields, enter the first and last numbers of the range you want to search for NetCache appliances. Any range between the numbers 1 and 254 is acceptable.
7	Ensure that the correct string appears in the community field to detect the SNMP-enabled NetCaches. The default is “public.”
8	Enter the NetCache user name and password.

Step	Action
9	Ensure that the port field displays 3132 for caches allowing HTTP collection of log files or, check the SSL box, and ensure that the port field displays 443 for caches allowing SSL protocol collection. 

Step	Action	
10	After you enter all required information, click Discover.	
	Note _____	
	Auto Discovery takes approximately one second for each number in a range.	
	Result: ContentReporter searches for all SNMP-enabled NetCache appliances in the range of the subnet that are recognized with the selected community string.	
	If...	Then...
	ContentReporter discovers any NetCache appliances in the subnet range, you return to the first Auto Discovery window, and the discovered NetCaches appear in the left-hand Discovered Caches panel.	Proceed to step 11 to select the NetCache appliances for this cache group.
	The No Caches Discovered dialog box appears	1. Click OK to return to the first Auto Discovery window. 2. Verify that the NetCaches are SNMP-enabled, and that the community string, User name, Password, and port numbers are correct. 3. Repeat steps 4 through 10.
11	Select the NetCaches in the left-hand Discovered Caches panel, and click Add.	
	Result: The NetCaches appear in the right-hand panel.	
12	To test connectivity between ContentReporter and the selected NetCaches, click Test Connection.	
	Result: The Test Cache Connectivity window appears, and, when ContentReporter completes the test, displays a status of either “available” or “not available” for each NetCache.	

Step	Action	
13	If...	Then...
	All the NetCaches have an “available” status	Click OK to return to the first Auto Discovery window.
	Some or all of the NetCaches have a “not available” status	1. Click OK to return to the first Auto Discovery window. 2. Verify that the ContentReporter server can resolve the fully qualified domain name of each NetCache that had a “not available” status. 3. If using SSL, verify each certificate is in the proper directory. 4. In the right-hand panel, select each NetCache that had a “not available” status and click Remove. 5. Repeat Steps 4 through 12.
14	Click OK. Result: You return to the Cache Group tab, and the NetCaches discovered with the Auto Discovery feature appear under the cache group in the left-hand panel.	
15	Click OK to return to the Cache Group tab.	
16	Click Apply or OK to save your changes.	

Step	Action
17	Go to “Step three: Scheduling log file collection” on page 93 to create a scheduled event to collect and process this cache group’s log files. Note The Auto Discovery feature does not give you the ability to specify a folder to store the collected log files. If you accept the Auto Discovery default location, ContentReporter stores collected log files for each cache added with Auto Discovery in the ContentReporter server machine’s folder: ..\Network Appliance\ContentReporter\jakarta-tomcat\webapps\ContentReporter\cache group name\cache name\. To specify a different location to store a particular cache’s log files, you must modify the cache’s settings. See step 4 of “Modifying a cache’s settings” on page 107. Note By default, the Auto Discovery feature uses each NetCache’s IP Address for the NetCache Settings window Name or IP Address field value. If ContentReporter will use SSL to collect from a NetCache added with Auto Discovery, the Name or IP Address field value must match the NetCache’s Common Name. If the cache’s NetCache Management console Common Name field value is not its IP Address, you must modify the NetCache settings in ContentReporter to specify the correct name in the Name or IP Address field of the NetCache Settings window. See step 6 of “Modifying a cache’s settings” on page 107. To learn about the NetCache Common Name field, see “NetCache Name or IP Address for SSL” on page 79.

Adding a cache to collect from an FTP server

About collecting log files from an FTP server

You can configure ContentReporter to collect and process log files saved on a File Transfer Protocol (FTP) server. To schedule the collection and processing of these log files, you first add a NetCache appliance to a cache group with which to associate these log files. At each collection event, ContentReporter collects all log files in the specified directory that have more recent time stamps than the newest log file collected during the previous collection event.

Note

ContentReporter only uses standard FTP to collect log files from an FTP server. You cannot use passive mode enabled FTP. As a result, you cannot collect from an FTP server behind a fire wall or Network Address Translation (NAT) box.

Note

ContentReporter can only collect log files from an FTP server that supports UNIX-style file lists. This is the FTP LIST command format. To collect log files from an IIS server, you must configure the FTP server to use the UNIX format. The FTP server cannot use the MS-DOS format.

Adding a cache to collect from an FTP server

To add a cache to collect and process log files from an FTP server, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab.
2	From the Administration page, click the Admin button.
3	From the Cache Group tab, select a cache group in the left-hand panel, and click New Cache.
4	In the New Cache window, enter a name for the log file source, click the Collect from FTP Server button, and then click Settings.

Step	Action
5	In the FTP Settings window, enter the name of the FTP server in the Server field, ensure that the correct port number (such as 21) appears in the Port field, enter the FTP user name and password, enter the name of the folder on the FTP server that contains the log files (such as “/users/jsmith/logs”) in the File location field, and then click OK.
6	If the log files contain no header, select the appropriate check box, and then click the button for the log file’s format.
7	Accept the default location to store this cache’s log files, or click Browse, select an appropriate directory, and click OK.
8	To delete the log files after processing, select the appropriate box.
9	Accept the default number of error lines (200), or enter another number. If you do not want the number of error lines in a log file to stop the ContentReporter server from processing, enter the number 0.
10	After you enter all the required information, click OK. Result: You return to the Cache Group tab and the cache appears under the cache group in the left-hand panel.
11	Click Apply or OK to save your changes. Result: You successfully added a cache to collect and process log files from an FTP server.
12	Go to “ Step three: Scheduling log file collection ” on page 93 to create a scheduled event to collect and process this cache group’s log files.

Step three: Scheduling log file collection

About collection events

Scheduling the collection of a cache group's log files is the third and final step of setting up log file collection. Once ContentReporter collects and processes a cache group's log files, you can examine information about the collection event.

For detailed information

For details about scheduling and examining log file collection events, see the following topics:

- ◆ [“Scheduling log file collection and processing”](#) on page 94
- ◆ [“Examining information about scheduled events”](#) on page 97

Scheduling log file collection and processing

About scheduling log file collection

Once you create a cache group and add one or more caches to the group, you can create a scheduled event to collect and process the group’s log files one time or at regular intervals. You create scheduled events on the Scheduled Events page.

Note

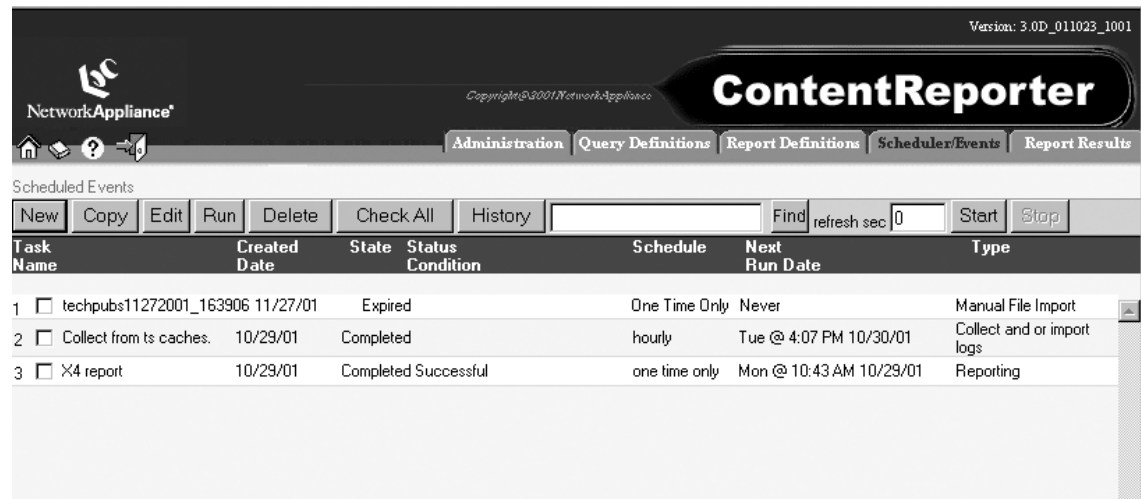
You can only create scheduled events to collect and process log files from cache groups, not individual caches. If you want to create a scheduled event to collect and process one cache’s log files, place it in its own cache group.

Which log files ContentReporter collects

If you create a scheduled event to collect and process the log files from a directory, a NetCache appliance, or an FTP server at scheduled intervals, ContentReporter will process all log files (in the directory, on the NetCache, or on the FTP server) that have more recent time-stamps than the newest log file processed during the previous collection and processing event.

The Scheduled Events page

The following screen shows the Scheduled Events page.



Scheduling log file collection and processing

To schedule log file collection and processing, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Scheduled Events tab. Result: The Scheduled Events page appears.
2	Click the New button. Result: The Details tab appears. Note _____ To learn more about the Details tab, see “Details tab” on page 59.
3	Enter a name (such as “Cache Group 1 Collection”) in the Task Name field.
4	Select “Collect and or import logs” from the Type drop-down selection list.
5	Select the cache group from the Cache Groups drop-down list.
6	Click the Schedule tab. Result: The Schedule tab appears. Note _____ To learn more about the Schedule tab, see “Schedule tab” on page 61.
7	Schedule the collection and processing of this group’s log files one time or at regular intervals. (If you want the first occurrence of a recurring collection event to begin as soon as possible, schedule it to begin in one or two minutes.) Note _____ The lower half of the Schedule tab dynamically changes as you select different frequencies from the “Execute this task” drop-down list.

Step	Action
8	Click the Security tab. Result: The Security tab appears. Note_____ To learn more about the Security tab, see “Security Tab” on page 63.
9	Accept the default security settings for this scheduled event, or change them as needed.
10	Click OK. Result: You return to the Scheduled Events page, the new scheduled event appears on the page, and you have successfully scheduled the collection and processing of this cache group’s log files. After ContentReporter has collected and processed this cache group’s log files, you can view information about the scheduled event, and information about the log files. To learn more about examining a scheduled collection event’s history, see “Examining information about scheduled events” on page 97. Note_____ You can force the ContentReporter server to immediately run a log file collection and processing event by checking its box in the Task Name column and clicking Run on the Scheduled Events page.

Examining information about scheduled events

About examining an event's information

ContentReporter gives you the ability to examine detailed information about each scheduled log file collection and processing event while it occurs and after it completes.

The Scheduled Events page

The Scheduled Events page provides feedback about each collection event as it occurs. You can monitor a scheduled event's current state (such as "Running," "Idle," or "Completed") and its status or condition ("Successful" or "Failed") on the Scheduled Events page.

Scheduled Events page

The follow screen is the Scheduled Events page.

Version: 3.0D_011023_1001



NetworkAppliance®

Copyright © 2001 Network Appliance

ContentReporter

AdministrationQuery DefinitionsReport DefinitionsScheduler/EventsReport Results

Scheduled Events

NewCopyEditRunDeleteCheck AllHistory

Find refresh sec 0

StartStop

Task Name	Created Date	State	Status Condition	Schedule	Next Run Date	Type
1 ☐ techpubs11272001_163906	11/27/01	Expired		One Time Only	Never	Manual File Import
2 ☐ Collect from ts caches.	10/29/01	Completed		hourly	Tue @ 4:07 PM 10/30/01	Collect and or import logs
3 ☐ X4 report	10/29/01	Completed	Successful	one time only	Mon @ 10:43 AM 10/29/01	Reporting

Event states, statuses, and conditions

The following table describes the possible states, statuses, and conditions of scheduled events.

Event Property	Value	Meaning
State	Pending	An occurrence of the scheduled event will begin when some other process completes.
	Running	An occurrence of the scheduled event is currently running.
	Completed	An occurrence of the scheduled event has just completed.
	Idle	The scheduled event is scheduled to occur sometime in the future.
Status Condition	Pending	The scheduled event will begin when some other process completes.
	Successful	The scheduled event was successful.
	With Errors	The scheduled event completed, but had one or more errors. It did not completely fail nor completely succeed.
	Failed	The scheduled event failed.

The History, Details, and Logs pages

ContentReporter also creates a “History” page, a “Details” page, and a “Logs” page for each scheduled collection event after it completes. You can open these three pages to examine information about a scheduled log file collection and processing event. The following table describes these three pages.

Scheduled event page	Function
History page	Enables you to: ◆ View information (such as the Start Time, Finish Time, Duration, Status, and Type) about each occurrence of a scheduled event. ◆ Open the Logs page and Details page.
Logs page	Lists the log files collected for an occurrence of a scheduled event.
Details page	Lists the ContentReporter server’s actions (such as “Collecting from” or “Getting file”) and status (such as “Completed” and “Successful”) for each occurrence of a scheduled event.

The Scheduled Event History page

The following screen shows the Scheduled Event History page.

Version: 3.0D_011023_1001

NetworkAppliance® Copyright © 2001 NetworkAppliance

ContentReporter

Administration Query Definitions Report Definitions Scheduler/Events Report Results

Scheduled Events History

Close Check All Logs Details

Task Name	Start Time	Finish Time	Duration	Status	Type
1 ☐ Collect from ts caches.	Mon Oct 29 10:07:01 EST 2001	Mon Oct 29 10:12:14 EST 2001	5 minutes 14 seconds	SUCCESSFUL	COLLECT AND OR IMPORT LOGS
2 ☐ Collect from ts caches.	Mon Oct 29 11:07:01 EST 2001	Mon Oct 29 11:08:16 EST 2001	1 minutes 16 seconds	SUCCESSFUL	COLLECT AND OR IMPORT LOGS
3 ☐ Collect from ts caches.	Mon Oct 29 12:07:00 EST 2001	Mon Oct 29 12:08:15 EST 2001	1 minutes 15 seconds	SUCCESSFUL	COLLECT AND OR IMPORT LOGS
4 ☐ Collect from ts caches.	Mon Oct 29 13:07:01 EST 2001	Mon Oct 29 13:08:16 EST 2001	1 minutes 16 seconds	SUCCESSFUL	COLLECT AND OR IMPORT LOGS
5 ☐ Collect from ts caches.	Mon Oct 29 14:07:01 EST 2001	Mon Oct 29 14:08:16 EST 2001	1 minutes 16 seconds	SUCCESSFUL	COLLECT AND OR IMPORT LOGS

The Events History Log Files page

The following screen shows the Log Files page.

Version: 3.0D_011023_1001

NetworkAppliance® Copyright © 2001 NetworkAppliance

ContentReporter

Administration Query Definitions Report Definitions Scheduler/Events Report Results

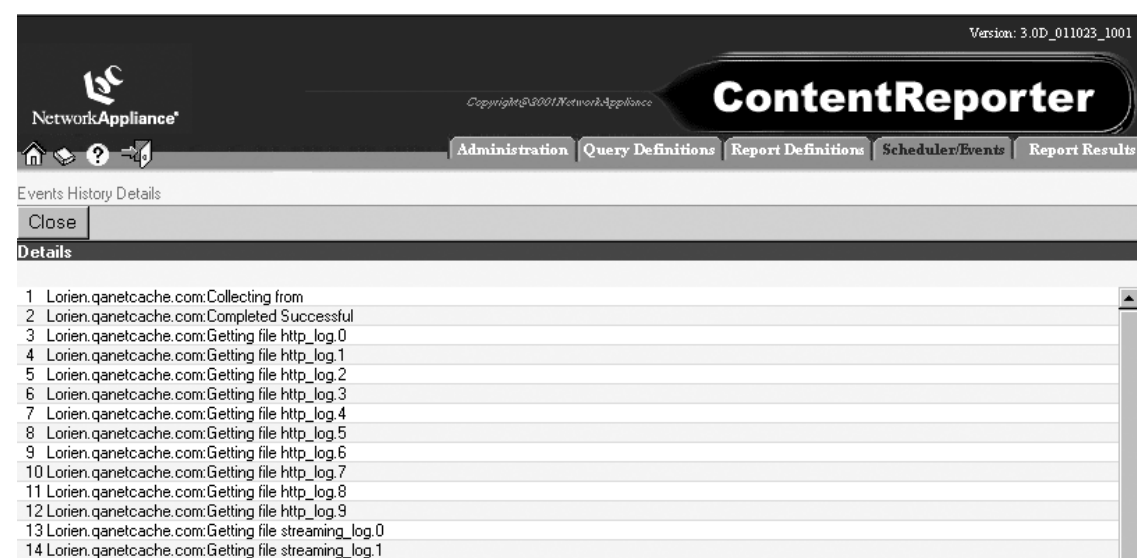
Events History Log Files

Close

Task Name	Log File Name
1 Collect from ts caches.10292001_101214	Lorien.qanetcache.com http_log.0:245.0:1002902646
2 Collect from ts caches.10292001_101214	Lorien.qanetcache.com http_log.1:245.0:1002904442
3 Collect from ts caches.10292001_101214	Lorien.qanetcache.com http_log.2:245.0:1002904447
4 Collect from ts caches.10292001_101214	Lorien.qanetcache.com http_log.3:245.0:1002906241
5 Collect from ts caches.10292001_101214	Lorien.qanetcache.com http_log.4:245.0:1002906246

The Events History
Details page

The following screen shows the Details page.



Note—
You can also learn more about a particular collection event by examining the ContentReporter log file. To learn more about the ContentReporter log file, see [“Examining the ContentReporter server log file”](#) on page 152.

Examining the
history of a
scheduled event

To examine the history of a completed scheduled log file collection and processing event, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Scheduled Events tab. Result: The Scheduled Events page appears, and a completed log file collection events appear on the page. A collection event’s name is composed of the cache group’s name and a time-stamp.

Step	Action
2	To examine more detailed information about this log file collection and processing event, check the box adjacent to this event, and click History. Result: The scheduled event's History page appears.
3	To examine the names and locations or sources of log files, check the box adjacent to an occurrence of this event, and click Logs. Result: The Log Files page for this occurrence of the event appears, and lists the names and locations or sources of the log files.
4	After examining the log files, click Close to return to the Scheduled Events History page for this event,
5	To examine the ContentReporter server's actions for an occurrence of the scheduled event, check the box adjacent to an occurrence of the event, and click Details. Result: The Details page for this occurrence of the scheduled event appears.
6	After examining the details, click Close to return to the Scheduled Events History page for this event,
7	When you have finished examining the history of the scheduled collection event, click Close. Result: You return to the Scheduled Events page, and have successfully examined the history of the scheduled log file collection and processing event.

Modifying cache groups and caches

About modifying cache groups and caches

In certain situations, you need to modify some cache or cache group settings and properties. For example, you may need to add or remove a particular cache from a group or change the type of analysis (HTTP, Streaming, or both) performed on a cache group's log files. You may also need to change the number of acceptable error lines in a cache's log files or change the location to store a cache's collected log files.

For detailed information

The following sections describe how to modify cache groups and caches:

- ◆ [“Modifying a cache group”](#) on page 103
- ◆ [“Deleting a cache group”](#) on page 105
- ◆ [“Modifying a cache's settings”](#) on page 107
- ◆ [“Removing a cache from a cache group”](#) on page 109

Modifying a cache group

About modifying a cache group

You can change the type of log file analysis (HTTP, Streaming, or both) performed for an existing cache group's, and can add or remove caches from an existing cache group.

Modifying a cache group

To modify a cache group, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	To change the type of log file analysis performed on a cache groups log files, select a cache group in the left-hand panel, and click Modify Group. Result: The Modify Group window appears.
4	Change the type of log file analysis (HTTP, Streaming, or both), by checking or unchecking the appropriate boxes, and click OK. Result: You return to the Cache Group tab, and have successfully changed the type of analysis.
5	To add one or more caches to the cache group, select the cache group in the left-hand panel, click either New Cache or Discover, and complete the required steps.
6	To remove a cache from a cache group, select the cache in the left-hand panel, and click Delete Cache. Result: A confirmation message dialog box appears.

Step	Action
7	Click OK. Result: The cache no longer appears under the cache group in the left-hand panel, you return to the Cache Group tab, and you have successfully removed the cache from the cache group.
8	Click Apply or OK to save the changes to the ContentReporter server. Result: You have successfully modified the cache group.

Deleting a cache group

About deleting a cache group

When you no longer need a particular cache group, you can easily delete it. Since you cannot restore a deleted cache group, make sure you will no longer need it. When you delete a cache group, you must also delete or modify any scheduled collection events based upon this cache group.

To learn more about scheduled events, see “[Scheduling log file collection and processing](#)” on page 94.

Note

ContentReporter stores records in your database on a per cache basis. It does not store records for cache groups. If you delete a cache group, and then create a new cache group with the same name, the new cache group has no relation to the deleted group with the same name. However, records for deleted caches remain in the database. A report on a deleted cache will be based on the cache’s database records. In addition, if you delete a cache, and add a new cache with the same name to a cache group, ContentReporter will associate the new cache with the database records of the old cache.

Deleting a cache group

To delete a cache group, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	Select a cache group in the left-hand panel, and click Delete Group. Result: A confirmation message dialog box appears.

Step	Action
4	Click OK. Result: You return to the Cache Groups tab, and have successfully deleted the cache group.
5	Click Apply or OK to save the changes to the ContentReporter server. Result: You have successfully deleted the cache group.

Modifying a cache's settings

About modifying a cache's settings

You can change several cache settings, including the:

- ◆ Log file location (NetCache, FTP server, or Directory)
- ◆ Stored log files directory
- ◆ Log file format
- ◆ Number of acceptable error lines
- ◆ State of the “Delete log files after parsing” check box

Modifying a cache's settings

To modify a cache's settings, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	Select a cache in the left-hand panel, and click Modify Cache. Result: The Modify Cache window appears.
4	Modify the cache's settings on the Modify Cache window.
5	To modify NetCache Settings (or FTP settings), click Settings. Result: The NetCache Settings (or FTP Settings) window appears.
6	Modify the settings on the NetCache Settings (or FTP Settings) window, and click OK.
7	In the Modify Cache window, click OK. Result: You return to the Cache Group tab.

Step	Action
8	Click Apply or OK to save the changes to the ContentReporter server. Result: You have successfully modified the cache.

Removing a cache from a cache group

About removing a cache from a cache group

You can remove a cache from a cache group to add it to another group, or to completely stop collecting and processing its log files.

Note

ContentReporter stores records in your database on a per cache basis. It does not store records for cache groups. If you delete a cache group, and then create a new cache group with the same name, the new cache group has no relation to the deleted group with the same name. However, records for deleted caches remain in the database. A report on a deleted cache will be based on the cache's database records. In addition, if you delete a cache, and add a new cache with the same name to a cache group, ContentReporter will associate the new cache with the database records of the old cache.

Removing a cache from a cache group

To remove a cache from a cache group, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	Select a cache in the left-hand panel, and click Delete Cache. Result: A confirmation dialog box appears.
4	Click OK. Result: You return to the Cache Groups tab, and have successfully deleted the cache.

Step	Action
5	Click Apply or OK to save the changes to the ContentReporter server. Result: You have successfully deleted the cache.

Importing saved log files

About importing log files

The Import Log File page give you the ability to process log files for a cache device without creating a scheduled event. This feature enables you to process log files that were not collected or processed by a scheduled event and output the result to your database for a new or existing cache device.

Import Log Files page

The following screen shows the Import Log Files page.

Cache Group: group5

Cache: cache2

Log Files:

- files\http_log.7
- files\http_log.7.cr3
- files\streaming_log.8
- files\streaming_log.8.cr3

Add

Remove

Cancel

Import Logs

Import Log Files page components

The following table describes the Import Log Files page components and their functions.

Component	Function
Cache Group field	Lists the name of the cache group of the cache device that generated the log file or file. If you selected the check box next to a cache on the Administration page before opening the Import Log Files page, this field displays the cache group of the cache.

Component	Function
Cache field	Lists the name of the cache device that generated the log file. If you selected the check box next to a cache on the Administration page before opening the Import Log Files page, this field displays the cache name.
Log Files panel	Lists the log files you selected to be imported.
Add button	Enables you to browse to the folder that contains the log files, and to select one or more log files.
Remove button	Enables you to deselect one or more log files for importing.
Import Logs button	Enables you to launch the process of importing and process the selected log file or files.

Importing log files

To import one or more log files, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab.
2	From the Administration page, click the Import button.
3	If you did not select the check box next to a cache on the Administration page before opening the Import Log Files page, enter the name of a new or existing cache group.
4	If you did not select the check box next to a cache on the Administration page before opening the Import Log Files page, enter the name of a new or existing cache. If you enter the name of an existing cache, you must enter its current cache group in the Cache Group field.
5	Click Add.

Step	Action
6	Browse to the location of the log files, select the log files you want to import using the Ctrl+Shift keys to select multiple files, and then click OK. Result: You return to the Import Log File page, and the log file or log files appear in the Log Files panel.
7	To select additional log files to import, repeat Steps 5 and 6.
8	After you select the log files you want, click Import Logs. Result: ContentReporter processes the log files and updates the database for this cache group and cache.
9	To view general information about this importing event, click the Scheduled Events tab. Result: The Scheduled Events page appears with a Manual File Import event for this cache group. The event's name is comprised of the cache group name and a time/date stamp.
10	To view detailed information about this manual file import, select the check box next to this event, then click History.
11	To view the names and locations of the imported log files, select the check box next to this event, then click Logs.
12	After viewing the log files, click Close to return to the Scheduled Events History page for this event, then click Close again.

About this chapter

This chapter gives you the information you need to configure authentication and permissions for users and groups in ContentReporter.

Note

To add a Local user and set permissions by following “Quick-Start” instructions, see Appendix A, “[Quick-start: Adding a Local user and setting the user’s permissions](#),” on page 174.

Topics covered in this chapter

This chapter covers the following topics:

- ◆ “[Learning about authentication, permissions, and security](#)” on page 116
- ◆ “[Configuring LDAP and NTLM authentication](#)” on page 125
- ◆ “[Adding user groups and setting user group permissions](#)” on page 131
- ◆ “[Adding Local users and setting Local user permissions](#)” on page 134
- ◆ “[Modifying user and user group permissions](#)” on page 138

Learning about authentication, permissions, and security

About access control

The combination of authentication, permissions, security, and Web site name restrictions gives you the ability to assign multiple users and groups different levels of access to pages and objects in ContentReporter.

For detailed information

The following sections explain authentication, permissions, and security in ContentReporter:

- ◆ [“Authentication in ContentReporter”](#) on page 117
- ◆ [“Page permissions in ContentReporter”](#) on page 119
- ◆ [“Web site name restrictions”](#) on page 121
- ◆ [“Security in ContentReporter”](#) on page 123

Authentication in ContentReporter

About Authentication

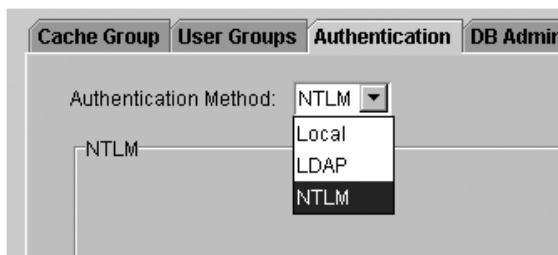
The ContentReporter server authenticates a username-password combination each time a user logs in. ContentReporter gives you the ability to simultaneously use its own built-in “Local” authentication, and either a Lightweight Directory Access Protocol (LDAP) server or an NT LAN Manager (NTLM) to authenticate users. A Local user is a login account maintained in the ContentReporter application.

Note

Adding and deleting groups to set permissions in ContentReporter for LDAP or NTLM authentication only adds or deletes them from the ContentReporter database. These actions have no effect on your organization’s LDAP or NTLM database.

Authentication methods

The following screen highlights the Authentication Method drop-down list on the Administration Authentication tab.



LDAP and NTLM failover to Local authentication

Local users (such as the initial “admin” and “guest” users) can still log into ContentReporter when you select LDAP or NTLM. When you select LDAP or NTLM as the authentication method, the ContentReporter server checks each login attempt with that method. If a login authentication fails, the ContentReporter server attempts to authenticate the user name-password combination with its Local authentication. To completely secure the ContentReporter server with LDAP or NTLM authentication, you must also set permissions for (or delete) all Local user accounts.

The relationship between user and group permissions

You can set permissions and security for groups and for Local users. You cannot set permissions or security for individual users with NTLM and LDAP authentication. If you set permissions or security on the group level, the permissions affect all users in the group. For example, if you take away all Administration privileges from the Guest group, no user in the Guest group can have Administration privileges. Each Local user you create must be a member of either the Admin, Guest, or User Local group. In its initial configuration, ContentReporter has two Local users: “admin” (password “admin”) and “guest” (password “guest”).

Note

When a user or group has two or more different permissions or security settings, the most restrictive permissions or security setting overrides the more permissive setting(s).

Page permissions in ContentReporter

About page permissions

ContentReporter gives you the ability to grant Unix-style permissions (read, write, execute, and delete) for the Administration, Query Definitions, Report Definitions, Scheduled Events, and Report Results pages. You can specify which Local users and which groups have permission to access a page, and how they can use a page’s features and objects. For example, if you set permissions so that the “Everyone” group does not have read privileges for the Administration page, members of this group cannot access this page and its features. If you take away delete privileges from the “Guest” group on the Query Definitions page, members of the group will be able to create, modify, and copy query definitions on the page, but not be able to delete them.

page permissions panel

The following screen highlights the Page permissions panel.

Type	Read	Write	Execute	Delete
Events	☒	☒	☒	☒
Reports	☒	☒	☒	☒
Query Definitions	☒	☒	☒	☒
Report Results	☒	☒	☒	☒
Administration	☒	☒	☒	☒

Page permissions descriptions

The following table describes page permissions in ContentReporter

Page	Permission	Enables a user or group to...
Administration	Read	Access the Administration page and to examine administrative settings.
	Write	Make Administrative changes (such as modifying a cache group or changing permissions).
	Execute	Does not apply.
	Delete	Does not apply.
Query Definitions	Read	Access the Query Definitions page.
	Write	Create, modify, and copy query definitions on the page.
	Execute	Does not apply.
	Delete	Delete query definitions on the page.
Report Definitions	Read	Access the Report Definitions page.
	Write	Create, modify, and copy report definitions on the page.
	Execute	Generate a report (by clicking Run) for the report definitions on the page.
	Delete	Delete report definitions on the page.
Scheduled Events	Read	Access the Scheduled Events page.
	Write	Create, modify, and copy scheduled events on the page.
	Execute	Generate new occurrences (by clicking Run) of scheduled events on the page.
	Delete	Delete scheduled events on the page.
Report Results	Read	Access the Report Results page and to view generated reports.
	Write	Does not apply.
	Execute	Does not apply.
	Delete	Delete generated reports.

Web site name restrictions

Web site restrictions

In addition to setting page permissions, you can specify the Web site names on which a user or group can generate reports. By default, a user or group can generate reports on all site names (such as “www.netapp.com”) in a cache’s database records. When you specify site names for a Local user or a group in the Add Permissions and Modify Permissions windows, the user or group can only create and run reports on these sites names.

Site Name and Host Name

In ContentReporter, a “Site Name” is the first or only domain name (with its extension) in a URL string. When one web site hosts another web site, the first domain name (with its extension) is the “Site Name,” and the last domain name (with its extension) is the “Host Name.”

Site Name and Host Name examples

The following table provides examples of Site Names and Host Names in ContentReporter.

Log file entry	Site Name	Host Name
www.netapp.com/newproducts/index.html	www.netapp.com	none
www.netapp.com/aaa/www.webmanage.com/home.htm	www.netapp.com	www.webmanage.com

The Site Names panel

The following screen illustrates the Site Names panel settings for user “SJones” on the Add Permissions window.

The "Add Permissions" dialog box shows the "Site Names" panel for user "SJones". The "Name" field contains "SJones". The "Permissions" table has the following data:

Type	Read	Write	Execute	Delete
Events	☒	☒	☒	☒
Reports	☒	☒	☒	☒
Query ...	☒	☒	☒	☒
Repor...	☒	☒	☒	☒

The "Site Names" list contains:

- www.netapp.com
- www.webmanage.com

Buttons: OK, Cancel, Clear, Add, Delete.

The Report Definitions Data tab

The following screen highlights the Report Definitions Data tab settings for user “SJones.”

The "Report Definitions Data" tab shows the following settings:

- Report Filters
 - Site Name: www.netapp.com
 - File / Clip: www.netapp.com
 - Client IP: *
- Time Filters

Security in ContentReporter

Object security

In addition to page permissions (which apply to all objects on a page), ContentReporter gives you the ability to set security for users and groups on specific objects (query definitions, report definitions, and scheduled events) on pages. You set object security on the Security tab of the particular definition or event. Object security enables you to prevent certain users or groups who have access to the Query Definitions, Report Definitions, and Scheduled Events pages from seeing, modifying, running, selecting, or deleting particular events or definitions.

Security tab

The following screen highlights the object Security tab settings.



The screenshot shows a window titled "Security" with two sections: "Users:" and "Groups:". Each section has a "Names:" text box and four checkboxes: "Read", "Write", "Execute", and "Delete".

Section	Names	Read	Write	Execute	Delete
Users:	JSmith, BJones, SBrown	☒	☒	☐	☐
Groups:	Users	☒	☒	☒	☐

Object security descriptions

The following table describes object security in ContentReporter.

Object Type	Security	Enables a user or group to...
Query Definition	Read	See the query definition on the Query Definitions page and select it for a report definition.
	Write	Modify and copy the query definition.
	Execute	Does not apply.
	Delete	Delete the query definition.
Report Definition	Read	See the report definition listed on the Report Definitions page and select it for a scheduled event.
	Write	Modify and copy the report definition.
	Execute	Generate a report with this report definition (by clicking Run) from the Report Definitions page.
	Delete	Delete the report definition.
Scheduled Event	Read	See the scheduled event on the Scheduled Events page.
	Write	Modify and copy the scheduled event.
	Execute	Run the scheduled event (by clicking Run) from the Scheduled Events page.
	Delete	Delete the scheduled event.

Configuring LDAP and NTLM authentication

About authentication

The ContentReporter server authenticates a username-password combination each time a user logs in. ContentReporter gives you the ability to simultaneously use its own built-in “Local” authentication, and either a Lightweight Directory Access Protocol (LDAP) server or an NT LAN Manager (NTLM) to authenticate users. If you configure ContentReporter for LDAP or NTLM authentication, users will be able to log into ContentReporter with their account, and you will be able to set permissions for these users on a group level. You can only set permissions for existing groups in your LDAP or NTLM database. You cannot set permissions for individual users in your LDAP or NTLM database.

Caution

When you successfully configure ContentReporter for LDAP or NTLM authentication, all users in your organization’s LDAP or NTLM database initially have full permissions, including Administration permissions, by default. To learn more about configuring permissions for groups, see “[Adding user groups and setting user group permissions](#)” on page 131.

For detailed information

The following sections describe how to configure LDAP and NTLM authentication:

- ◆ “[Configuring ContentReporter for LDAP authentication](#)” on page 126
- ◆ “[Configuring ContentReporter for NTLM authentication](#)” on page 129

Configuring ContentReporter for LDAP authentication

About LDAP authentication

ContentReporter gives you the ability to use an existing Lightweight Directory Access Protocol (LDAP) server for authentication. This includes Microsoft Active Directory. Basically, you “point” ContentReporter at an LDAP server. When users attempt to log into ContentReporter with their LDAP account, the ContentReporter server retrieves the account information from the database on an LDAP server.

LDAP settings on the Authentication tab

The following screen highlights LDAP settings on the Authentication tab.

The screenshot shows a web-based configuration interface with several tabs: Cache Group, User Groups, Authentication, DB Admin, Billing, Licensing, and Logging. The 'Authentication' tab is selected. Below the tabs, there is a section for 'Authentication Method' with a dropdown menu set to 'LDAP'. Below this, there is a sub-section titled 'LDAP' containing several input fields: 'LDAP Server:(lp)' with the value '12.34.56.78', 'Port' with the value '1234', 'LDAP Password:' with masked characters '*****', 'User ID(UID) Field:' with the value 'uid', and 'Base Distinguished Name:' with the value 'O=netapp.com'. At the bottom of the form are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

LDAP Settings

The following table describes the ContentReporter LDAP settings.

LDAP Setting	Description
LDAP Server IP	The IP Address (such as 12.34.56.78) of the LDAP server.
Port	The port through which ContentReporter will access the LDAP server.
LDAP Password	The password ContentReporter will use to gain access to the bind distinguished name. This password authorizes ContentReporter to access and query the LDAP directory.
User ID (UID)	The name (often “uid”) of the attribute in the LDAP directory that contains user login names that ContentReporter will authenticate.
Base Distinguished Name	The name of the directory on the LDAP server where ContentReporter begins its authentication search.

Configuring ContentReporter for LDAP

To configure ContentReporter for LDAP Authentication, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	Click the Authentication tab. Result: The Authentication tab appears.
4	Select LDAP from the Authentication Method drop-down list. Result: The lower portion of the Authentication tab dynamically changes and displays the LDAP setting fields.

Step	Action
5	Enter the LDAP Server IP, the Port number, the LDAP Password, the User ID (UID), and the Base Distinguished Name in the appropriate fields, and click Apply or OK to save the changes to the ContentReporter server. Result: You have successfully configured ContentReporter for LDAP authentication.

Configuring ContentReporter for NTLM authentication

About NTLM authentication

ContentReporter gives you the ability to use an NT LAN Manager (NTLM) domain controller’s user database to authenticate users. When users attempt to log into ContentReporter with their NTLM account, the ContentReporter server will retrieve the account information from the domain controller’s database.

NTLM settings on the Authentication tab

The following screen highlights the NTLM setting on the Authentication tab.

A screenshot of the ContentReporter web interface. At the top, there are several tabs: 'Cache Group', 'User Groups', 'Authentication', 'DB Admin', 'Billing', 'Licensing', and 'Logging'. The 'Authentication' tab is selected. Below the tabs, there is a section for 'Authentication Method' with a dropdown menu set to 'NTLM'. Below this, there is a large text area labeled 'NTLM'. At the bottom of this text area, there is a label 'Windows Domain Name :' followed by a text input field containing the value 'netapp'. At the very bottom of the window, there are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

Configuring ContentReporter for NTLM authentication

To configure ContentReporter for NTLM Authentication, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.

Step	Action
2	Click the Admin button. Result: The Cache Group tab appears.
3	Click the Authentication tab. Result: The Authentication tab appears.
4	Select NTLM from the Authentication Method drop-down list. Result: The lower portion of the Authentication tab dynamically changes and displays the Windows Domain Name field.
5	In the Windows Domain Name field, enter the name of the domain in which the machine on which you installed ContentReporter resides. For example, if the ContentReporter server machine is in the “netapp” domain, enter “netapp” in this field.
6	Click Apply or OK to save the changes to the ContentReporter server. Result: You have successfully configured ContentReporter for NTLM authentication.

Adding user groups and setting user group permissions

About setting group permissions

When you use the LDAP or NTLM methods of authentication, you can only set permissions on a group level. You cannot set permissions for individual users with LDAP or NTLM. When you use the ContentReporter Local authentication, you can set permissions on both the group level and the user level. If you set permissions or security settings on the group level, the permissions or security settings affect all users in the group. For example, if you take away all Administration privileges from the Guest group, no user in the Guest group can have Administration privileges.

Note Adding and deleting groups to set permissions in ContentReporter for LDAP or NTLM authentication only adds or deletes them from the ContentReporter database. These actions have no effect on your organization’s LDAP or NTLM database.

Although you cannot add new Local user groups, you can modify the permissions of the three default Local user groups. To learn more about modifying an existing group’s permissions, see “[Modifying user and user group permissions](#)” on page 138.

Adding a new LDAP or NTLM user group and configuring its permissions

To add a new LDAP or NTLM user group and configure its permissions, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	Click the Authentication tab. Result: The Authentication tab appears.

Step	Action
4	Select the method of authentication (either LDAP or NTLM) from the Authentication Method drop-down list, and click the User Groups tab. Result: The User Groups tab appears.
5	Click Add. Result: The Add Permissions window appears.
6	To modify the default permissions, check or uncheck the permissions boxes as needed.
7	To specify the site names upon which the new group can generate reports, click Add. Result: The Add Site Name window appears. Note_____ By default, group members can generate reports on all sites names. You can configure this new group's permissions in the Add Site Name window so that the group members can only generate reports on the sites names you specify. _____
8	Enter the site name (such as "www.netapp.com") and click OK. Result: You return to the Add Permissions window. Note_____ You can also use the * (asterisk) wildcard character in the Name field. For example, you can enter "*.edu" so that the group can only generate reports on sites names with the ".edu" extension. _____
9	Repeat steps 7 and 8 to specify additional site names.
10	When you have set the desired permissions, click OK. Result: You return to the User Groups tab.

Step	Action
11	To save the changes to the ContentReporter server, click Apply or OK. Result: You have successfully added the new user group and configured its permissions.

Adding Local users and setting Local user permissions

About Local users

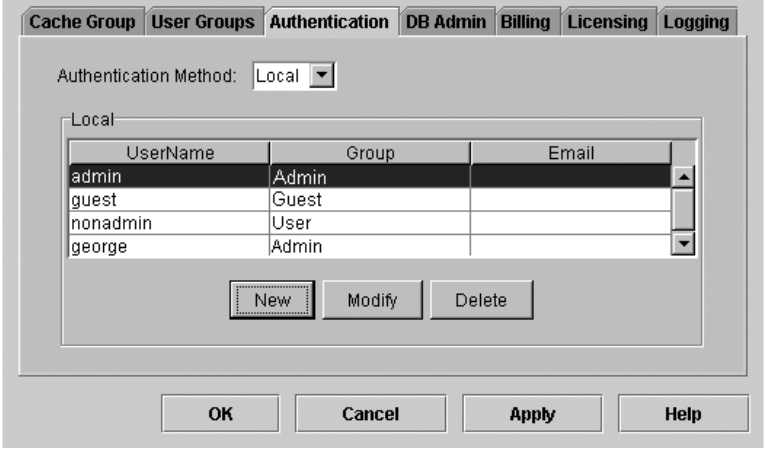
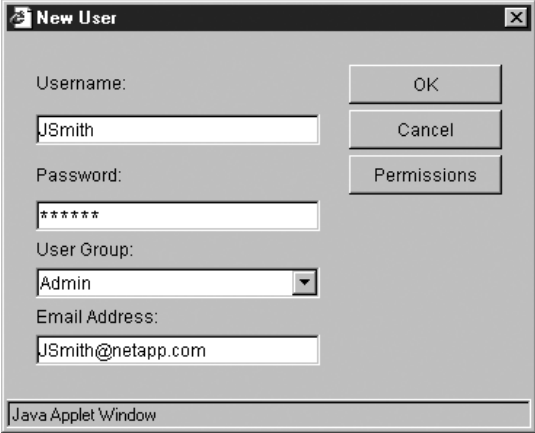
When you select the Local method of authentication, you use the “built-in” ContentReporter user and group database. You can add multiple users and set permissions with Local authentication. When adding a new user, you must add the user to one of the three Local (Admin, Guest, and User) groups. You can set permissions on both the group level and the user level with Local authentication. In its initial configuration, ContentReporter has two Local users “admin” (password “admin”) and “guest” (password “guest”).

Note — Unless you take away additional permissions or specify different Web site names when creating a new Local user account, the account starts out with its Local user group’s permissions.

Adding a Local user and setting the user’s permissions

To add a Local user and configure the user’s permissions, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	Click the Authentication tab. Result: The Authentication tab appears.

Step	Action
4	Select Local from the Authentication Method drop-down list, and click New. Result: The New User window appears. 
5	Enter a name, a password, select one of the three groups from the User Group drop down list, and, if desired, an e-mail address.
6	To set permissions for this new Local user, click Permissions. Result: The Add Permissions window appears. 

Step	Action
7	To take away particular privileges, uncheck the appropriate boxes. Note_____ If you have not granted a particular permission to the user's group, checking that permission in this window will not give the user that permission. In this window you can only take away permissions from this user that you have granted to this user's group.
8	To specify the site name on which the user can generate reports, click Add. Result: The Add Site Name window appears. Note_____ By default, users can generate reports on all site names. You can configure a user's permissions in the Add Site Name window so that they can only generate reports on the site names you specify.
9	Enter the site name (such as “www.netapp.com”) and click OK. Result: You return to the Add Permissions window. Note_____ You can also use the * (asterisk) wildcard character in the Name field. For example, you can enter “*.edu” so that the user can only generate reports on site names with the “.edu” extension.

Step	Action
10	Repeat steps 8 and 9 to specify additional site names.
11	When you have set the desired permissions, click OK. Result: You return to the New User window.
12	Click OK. Result: You return to the Authentication tab.
13	To save the changes to the ContentReporter server, click Apply or OK. Result: You have successfully added a new Local user and configured the user's permissions.

Modifying user and user group permissions

About modifying permissions

ContentReporter enables you to make the following changes:

- ◆ Modify Local, LDAP, and NTLM user group permissions
- ◆ Delete LDAP and NTLM user groups

Note

Deleting an LDAP or NTLM user group in ContentReporter only removes the user group from the ContentReporter database. This action has no effect on your LDAP or NTLM database. You cannot delete the three default Local user groups.

- ◆ Modify a Local user's permissions
- ◆ Delete Local users

For detailed information

The following sections describe how to modify user and user group permission:

- ◆ [“Modifying a user group's permissions”](#) on page 139
- ◆ [“Deleting an LDAP or NTLM user group”](#) on page 141
- ◆ [“Modifying a Local user's permissions”](#) on page 142
- ◆ [“Deleting a Local user”](#) on page 144

Modifying a user group's permissions

Modifying a user group's permissions

To modify an existing Local, LDAP, or NTLM user group's permissions, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	Click the Authentication tab. Result: The Authentication tab appears.
4	Select the user group's method of authentication (Local, LDAP or NTLM) from the Authentication Method drop-down list, and click the User Groups tab. Result: The User Groups tab appears.
5	Select the user group, and click Edit. Result: The Modify Permissions window appears.
6	To modify permissions, check or uncheck the permissions boxes as needed.

Step	Action
7	To specify a site name upon which the group can generate reports, click Add. Result: The Add Site Name window appears. Note_____ By default, group members can generate reports on all sites names. You can configure the group's permissions in the Add Site Name window so that the group members can only generate reports on the site names you specify.
8	Enter the site name (such as "www.netapp.com") and click OK. Result: You return to the Add Permissions window. Note_____ You can also use the * (asterisk) wildcard character in the Name field. For example, you can enter "*.edu" so that the group can only generate reports on site names with the ".edu" extension.
9	Repeat steps 7 and 8 to specify additional site names.
10	To delete a site name from the group's Site Names list, select the site name from the Site Names panel, and click Delete. Result: You remove the site name from the Sites Names list.
11	Once you have set the desired permissions, click OK. Result: You return to the User Groups tab.
12	To save the changes to the ContentReporter server, click Apply or OK. Result: You have successfully modified the user group's permissions.

Deleting an LDAP or NTLM user group

About deleting a user group

You can delete an existing LDAP or NTLM user group from ContentReporter at any time. You cannot delete the three default Local user groups.

Deleting an LDAP or NTLM user group

To delete an LDAP or NTLM user group, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	Click the Authentication tab. Result: The Authentication tab appears.
4	Select the method of authentication (LDAP or NTLM) from the Authentication Method drop-down list, and click the User Groups tab. Result: The User Groups tab appears.
5	Select the user group, and click Delete. Result: The Confirm Delete dialog box appears.
6	Click Yes. Result: You delete the user group and return to the User Groups tab.
7	To save the changes to the ContentReporter server, click Apply or OK.

Modifying a Local user's permissions

Modifying a Local user's permissions

To modify a Local user's permissions, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	Click the Authentication tab. Result: The Authentication tab appears.
4	Select Local from the Authentication Method drop-down list, select the user from Local panel, and click Modify. Result: The Modify User window appears.
5	Modify the Password, User Group, and Email Address as needed.
6	To modify the Local user's permissions, click Permissions. Result: The Modify Permission window appears.
7	To modify permissions, check or uncheck the permissions boxes as needed.
8	To specify a site name upon which the Local user can generate reports, click Add. Result: The Add Site Name window appears. Note _____ By default, local users can generate reports on all site names. You can configure a Local user's permissions in the Add Site Names window so that the user can only generate reports on the site names you specify. _____

Step	Action
9	Enter the site name (such as “www.netapp.com”) and click OK. Result: You return to the Modify User window. Note_____ You can also use the * (asterisk) wildcard character in the Name field. For example, you can enter “*.edu” so that the group can only generate reports on site names with the “.edu” extension. _____
10	Repeat steps 8 and 9 to specify additional site names.
11	To delete a site name from the user’s Site Names list, select the site name from the Site Names panel, and click Delete. Result: You remove the site name from the Site Names list.
12	Once you have set the desired permissions, click OK. Result: You return to the Modify User window.
13	Click OK. Result: You return to the Authentication tab.
14	To save the changes to the ContentReporter server, click Apply or OK. Result: You have successfully modified the Local user’s information and permissions.

Deleting a Local user

Deleting a Local user

To delete a Local user, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	Click the Authentication tab. Result: The Authentication tab appears.
4	Select Local from the Authentication Method drop-down list, select the user from Local panel, and click Delete. Result: The Confirm Delete dialog box appears.
5	Click Yes. Result: You delete the user and return to the Authentication tab.
6	To save the changes to the ContentReporter server, click Apply or OK. Result: You have successfully deleted the Local user.

About this chapter

This chapter gives you the information you need to complete additional ContentReporter server configuration tasks.

Topics covered in this chapter

This chapter covers the following topics:

- ◆ [“Examining and upgrading your license information”](#) on page 146
- ◆ [“Configuring ContentReporter server logging”](#) on page 149
- ◆ [“Examining the ContentReporter server log file”](#) on page 152
- ◆ [“Configuring database rollups”](#) on page 159
- ◆ [“Configuring Billing aggregation”](#) on page 163
- ◆ [“Adding logo images to ContentReporter for XHTML Reports”](#) on page 168

Examining and upgrading your license information

About examining and upgrading license information

You can examine your current license information, and upgrade your license on the Administration Licensing tab. You can examine the number of caches (NetCaches, Web servers, and streaming servers) supported by your current software license. If you obtain a license key to increase the number of caches, you enter the upgrade license key on this tab as well.

Note _____
If you purchased ContentReporter, you will find your License Key listed in the Software License Key letter in your ContentReporter kit.

The Licensing tab

The following screen shows the Licensing tab.

Cache Group	User Groups	Authentication	DB Admin	Billing	Licensing	Logging
Product License Key:		12345				
Serial No:		12345				
License Type:		Primary				
Number of caches:		5				
Expiration:		None				
Upgrade License:						Upgrade

Licensing tab fields The following table describes the Licensing tab fields.

Field	Function
Product License Key	Lists your current License Key.
Serial No. field	Lists your current serial number.
License Type field	Lists your current type of license.
Number of caches	Lists the maximum number of node devices you may add to cache groups with your current License Key.
Expiration field	Lists either an expiration date (if you are using an Evaluation copy of ContentReporter), or no date (if you are using a purchased copy of ContentReporter).
Upgrade License	Enables you to enter a new License Key to upgrade from an Evaluation copy of ContentReporter, or to increase the maximum number of node devices or ContentReporter servers.

Examining or entering license information

To examine or enter ContentReporter software license information, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	Click the Licensing tab. Result: The Licensing tab appears.
4	Examine your current license information.
5	To upgrade your license, enter the upgrade information in the appropriate fields, and click Upgrade. Result: The License Upgrade message box appears confirming your upgrade.
6	Click Apply or OK to save any changes to the ContentReporter server. Result: You have successfully examined or upgraded your ContentReporter software license information.

Configuring ContentReporter server logging

About ContentReporter logging

The ContentReporter server maintains a log file that contains a record of its activity. If you have a problem processing log files or generating reports, you might be able to discover the cause of the problem by examining the ContentReporter log file. The ContentReporter server begins generating a new date/time-stamped log file each time it starts, and each time the log file reaches its maximum file size. The ContentReporter server stores its own log files in the ContentReporter server machine folder:

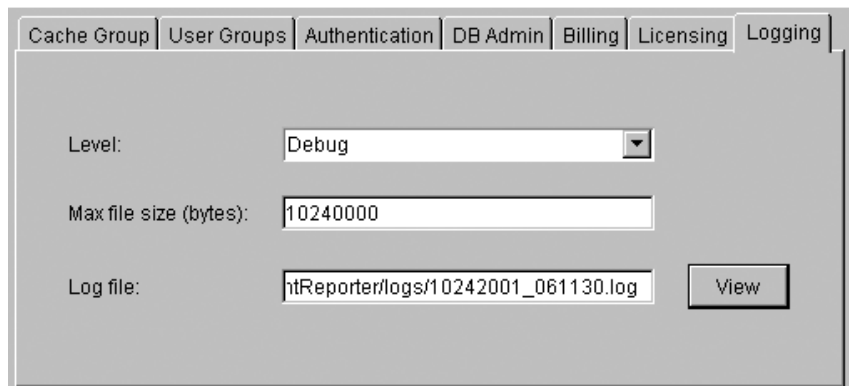
..\Network Appliance\ContentReporter\jakarta-tomcat\webapps\ContentReporter\logs\

You can specify the log file size (the default size is 10.24 MB) at which ContentReporter begins generating a new log file, and the level of information you want the ContentReporter server to record in the log file. You configure ContentReporter logging on the Administration Logging tab.

To learn about examining the ContentReporter server log file, see [“Examining the ContentReporter server log file”](#) on page 152.

The Logging tab

The following screen shows the Administration Logging tab.



The screenshot shows a web-based configuration interface for ContentReporter. At the top, there is a horizontal tab bar with the following tabs: "Cache Group", "User Groups", "Authentication", "DB Admin", "Billing", "Licensing", and "Logging". The "Logging" tab is currently selected. Below the tabs, the interface contains three configuration fields:

- Level:** A dropdown menu with "Debug" selected.
- Max file size (bytes):** A text input field containing "10240000".
- Log file:** A text input field containing "ntReporter/logs/10242001_061130.log".

To the right of the "Log file" field is a button labeled "View".

Logging levels

You can select one of five levels of information you want the ContentReporter server to record in its log file. To generate log files with the most comprehensive information about ContentReporter, select “Debug.” To generate log files with the least comprehensive information about ContentReporter, select “Terminal.” Each line of the ContentReporter server log file has a “cr-level” field value (1 - 5) that corresponds to one of the five logging levels. Each logging level includes information recorded in any less comprehensive levels. For example, the “Debug” level includes information recorded in the other four levels.

Logging level descriptions

The following table describes each ContentReporter logging level, the corresponding “cr-level” field value in the log file, and a brief description of the logging level.

Level	cr-level field	Description
Debug	1	The most comprehensive ContentReporter server logging level. The ContentReporter server records information about all its activities and all other types of information.
Info	2	The ContentReporter server records information about most of its activities.
Status	3	The ContentReporter server records information about completed events, such as a successful login.
Warning	4	The ContentReporter server records information about unsuccessful events, such as an unsuccessful log file collection.
Terminal	5	The least comprehensive ContentReporter server logging level. The ContentReporter server only records information about the most serious problems.

Configuring ContentReporter server logging

To configure the ContentReporter server logging, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	Click the Logging tab. Result: The Logging tab appears.
4	Select the level of information you want the ContentReporter server to record in the log file from the Level drop-down list.
5	Accept the default maximum log file size, or enter a different size, in the Max file size field.
6	Click Apply or OK to save any changes to the ContentReporter server. Result: You have successfully configured your ContentReporter server logging. To learn about examining the log file, see “ Examining the ContentReporter server log file ” on page 152.

Examining the ContentReporter server log file

About examining the ContentReporter log file

You can examine the current ContentReporter server log file to look for the cause of a certain problem, or to learn more about the ContentReporter server’s activities. The log file is a date/time-stamped file with a *.log* extension. The ContentReporter server log file contains six fields. You open the ContentReporter server log file on the Administration Logging tab.

To learn more about configuring the ContentReporter server logging, see [“Configuring ContentReporter server logging”](#) on page 149.

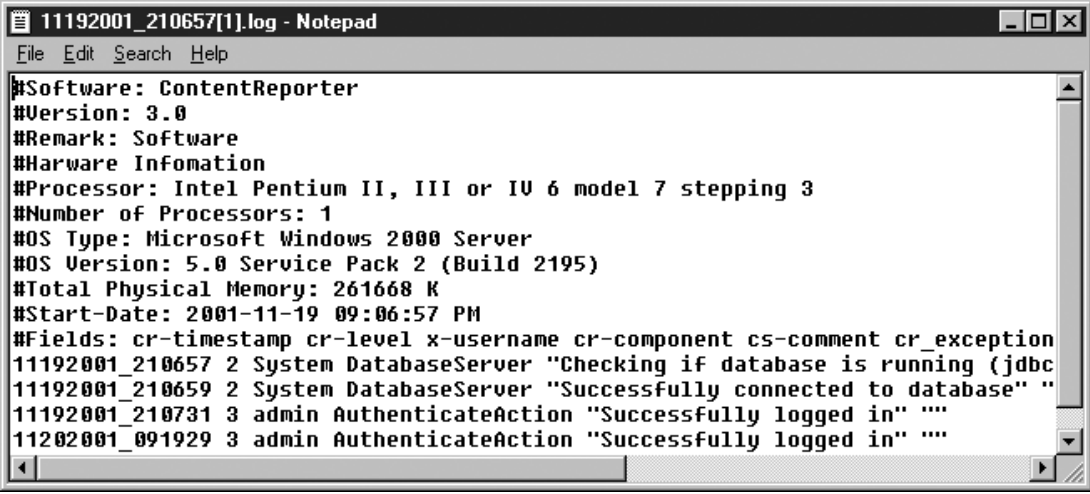
ContentReporter log file fields

The following table describes the six ContentReporter log file fields.

Field	Description
cr-timestamp	The date/time-stamp of the activity in the format: mmddyyyy_hhmmss
cr-level	The logging level of the activity: from 1 to 5
x-username	The user (or the System) related to (or responsible for) the activity
cr-component	The component of ContentReporter responsible for the activity (such as the parser or the DataCollector)
cs-comment	A brief description of the activity (such as “Successfully logged in”) This field also contains: ◆ The parser return codes ◆ The sorter return codes ◆ The SQL bulk uploader return codes
cr_exception	A brief description of a Java exception

The ContentReporter log file

The following screen shows a portion of a ContentReporter server log file.



```
11192001_210657[1].log - Notepad
File Edit Search Help
#Software: ContentReporter
#Version: 3.0
#Remark: Software
#Hardware Information
#Processor: Intel Pentium II, III or IV 6 model 7 stepping 3
#Number of Processors: 1
#OS Type: Microsoft Windows 2000 Server
#OS Version: 5.0 Service Pack 2 (Build 2195)
#Total Physical Memory: 261668 K
#Start-Date: 2001-11-19 09:06:57 PM
#Fields: cr-timestamp cr-level x-username cr-component cs-comment cr_exception
11192001_210657 2 System DatabaseServer "Checking if database is running (jdbc
11192001_210659 2 System DatabaseServer "Successfully connected to database" "
11192001_210731 3 admin AuthenticateAction "Successfully logged in" ""
11202001_091929 3 admin AuthenticateAction "Successfully logged in" ""
```

For detailed information

The following sections explain how to examine the ContentReporter server log file:

- ◆ [“Understanding the “cs-comment” field return codes”](#) on page 154
- ◆ [“Examining the log file”](#) on page 158

Understanding the “cs-comment” field return codes

About the ContentReporter return codes

Three of the ContentReporter server components (the parser, the sorter, and the SQL bulk uploader) record return codes in the “cs-comment” field of the ContentReporter server log file. The return codes help you to identify problems and to understand the ContentReporter server’s activities.

The parser return codes

The ContentReporter parser processes collected log files. The parser return codes record information about the parser’s activities. The parser return code value in the “cs-comment” field is “Parser return error code n” (where “n” is a numeric value from 0 to -12). The following table describes the parser return codes in the ContentReporter server log file.

Return Code	Description	Internal Code
0	The parser successfully parsed the log file.	SUCCESS
-1	The parser was unable to allocate enough memory to parse the log file.	ERR_MEMORY_ALLOCATION_FAILED
-2	There was a problem accessing (or related to) the stored log file folder.	ERR_COULD_NOT_OPEN_OUTPUT_FILE
-3	There was a problem accessing (or related to) the stored log file folder.	ERR_COULD_NOT_OPEN_LOG_FILE
-4	The log file contained an invalid header.	ERR_INVALID_LOG_FILE_HEADER
-5	There was a problem accessing (or related to) the stored log file folder.	ERR_COULD_NOT_OPEN_CSV_FILE
-6	The log file contained an unknown header field.	ERR_UNKNOWN_HEADER_FIELD

Return Code	Description	Internal Code
-7	There was a problem related to the datatypes.dat file in the folder: ..\Network Appliance\ContentReporter\ jakarta-tomcat\webapps\DataCollector	ERR_COULD_NOT_OPEN_DATA_FILE
-8	There was a problem accessing (or related to) the stored log file folder.	ERR_COULD_NOT_OPEN_CTL_FILE
-9	There was a problem accessing (or related to) the stored log file folder.	ERR_COULD_NOT_OPEN_SQL_FILE
-10	The log file was empty.	ERR_EMPTY_LOG_FILE
-11	The log file contained more than the maximum number of allowed error lines.	ERR_MAX_ERRORS
-12	The parser did not process the log file because the log file format changed at some point in the log file.	ERR_LOG_FMT_CHANGED_IN_LOG

The sorter return codes

The ContentReporter sorter sorts and groups the log file data it receives from the ContentReporter parser. The sorter return codes record information about the sorter's activities. The sorter return code value in the "cs-comment" field is "crsort complete, returning n" (where "n" is a numeric value from 0 to -10). The following table describes the sorter return codes in the ContentReporter server log file.

Return Code	Description
0	The sorter successfully completed the sorting task.
-1	The ContentReporter server machine did not have enough memory for the sorter to complete the task.

Return Code	Description
-2	The sorter could not open its output file (“.srt” extension). Possible causes: ◆ The file may be in use ◆ Not enough disk space to create it
-3	The sorter could not open the ContentReporter server log file. Possible causes: ◆ The file may be in use ◆ Not enough disk space to create it
-4	The sorter could not open its input CSV file generated by the parser. To learn more about this, see the parser return error code -5 in “ The parser return codes ” on page 154.
-5	The sorter could not open the format file generated by the parser. To learn more about this, see “ The parser return codes ” on page 154.
-6	The sorter could not open the “datatypes.dat” file in the ContentReporter server machine folder: ..\Network Appliance\ContentReporter\jakarta-tomcat\webapps\DataCollector
-7	The sorter could not open the format file generated by the parser. To learn more about this, see “ The parser return codes ” on page 154.
-8	The sorter received one or more incorrect command line arguments. This is caused by an internal ContentReporter problem.
-9	The sorter received one or more incorrect command line arguments. This is caused by an internal ContentReporter problem.
-10	The sorter received one or more incorrect command line arguments. This is caused by an internal ContentReporter problem.

The SQL bulk uploader return codes

The SQL bulk uploader return codes record information about the bulk updates to the database. The bulk uploader return code value in the “cs-comment” field is “Bulk load return: n” (where “n” is a numeric value from 0 to -4). The following table describes the bulk uploader return codes in the ContentReporter server log file.

Return Code	Description
0	The bulk upload is successful.
-1	There is a driver error.
-2	There is a connection error.
-3	A bulk copy program (bcp) error has occurred. The bcp may have rejected one row or may have totally failed. The user should check the log file to find out which bcp error has occurred.
-4	The bulk uploader has an error releasing its connection.

Examining the log file

Examining the ContentReporter server log file

To examine the ContentReporter server log file, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	Click the Logging tab. Result: The Logging tab appears.
4	Click View. Result: The current ContentReporter server log file appears
5	Examine the log file. When you have finished examining the log file, close the file or save it with a different file name for future reference. Note _____The ContentReporter server continues updating the log file until the ContentReporter service stops or until the log file reaches the maximum size. _____

Configuring database rollups

About database rollups

The database rollup feature gives you the ability to keep a specified number of days of hourly data available for reports in your database. You can also specify the number of days of Billing data and Streaming data to keep available for reports. Using database rollups, you can create a “sliding window” of data available for reports. In most production environments, hourly data is only needed for a week or two. Using database rollups settings, you can get rid of unwanted data on a regular basis and, at the same time, have the ContentReporter server store more information without your database continuing to grow in size. The database rollup activity is a scheduled database background task.

Note

If you disable database rollups, your database will grow in size at approximately the rate of log file processing. Also, if you disable rollups, the ContentReporter server will never update the monthly database tables.

How database rollups work

Database rollups control the size of your database by converting hourly data into monthly data. For example, before a database rollup, you could use the “Activity Level by Hour” query definition to generate a report on the number of hits per hour received by a particular NetCache appliance during the month of May. When the month of May’s data is rolled up (for example, in early July), all hourly data for the month of May is cleared from the database. If you wanted to generate a report of the number of hits the cache received in May after the rollup, you could use the “Activity Level by Month” query definition.

The Database Rollups portion of the DB Admin tab

The following screen shows the Database Rollups portion of the Administration DB Admin tab.

Database Rollups:

☒ Use database rollups.

Rollup Frequency:

monthly

Set Schedule...

33

number of days of hourly data to keep.

6

number of months of monthly data to keep.

3

number of days of billing data to keep.

3

number of days of streaming data to keep.

Database Rollups settings

The following table describes the Database Rollups properties.

Setting	Description
Rollup Frequency	The frequency of database rollups: Daily, Weekly, or Monthly. You can specify how often all hourly data in the database that is more than the specified number of days old (in the “number of days to keep hourly data” field) is converted into monthly data. Use the Set Schedule... button to launch the Rollup Scheduled window to specify the rollup frequency.
Number of days of hourly data to keep	The minimum number of days of hourly data to keep available for reports in your database. Immediately after a database rollup, you have exactly this many days of hourly data in the database. After a rollup, the amount of hourly data in the database increases by one day each day until the next rollup. For example if you schedule database rollups for the 1st and 15th days of the month, and specify to keep 33 days of hourly data in your database, you will have 33 days of hourly data immediately after the rollup on the 1st of the month, 46 days of hourly data on the 14th day of the month, and then 33 days of hourly data immediately after the rollup on the 15th day of the month.

Setting	Description
Number of months of monthly data to keep	The number of months of monthly data to keep available for reports in your database. Immediately after a database rollup, you have exactly this many months of monthly data in the database. If you set this number to six months and schedule a rollup to occur on October 1st, you will have monthly data available in your database for reports for the months of April through September.
Number of days of billing data to keep	The minimum number of days of billing data to keep available for reports in your database. Immediately after a database rollup, you have exactly this many days of billing data in the database. After a rollup, the amount of billing data in the database increases by one day each day until the next rollup. Ensure that the number of days of billing data you specify to keep is compatible with your Billing tab settings. To learn more about the Billing tab settings, see “Configuring Billing aggregation” on page 163.
Number of days of Streaming data to keep	The minimum number of days of streaming data to keep available for reports in your database. Immediately after a database rollup, you have exactly this many days of streaming data in the database. After a rollup, the amount of streaming data in the database increases by one day each day until the next rollup.

Configuring database rollups

To configure database rollups, complete the following steps.

Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	Click the DB Admin tab. Result: The DB Admin tab appears.

Step	Action
4	Ensure that the Use Database Rollups check box is checked.
5	Ensure that the number of days to keep hourly, monthly, billing, and streaming data are adequate or enter a different numbers of days in the appropriate fields.
6	To schedule database rollups at regular intervals, click Set Schedule. Result: The Rollup Scheduler window appears.
7	Select Daily, Week, or Monthly from the Execute this task drop-down list. Result: The lower portion of the window dynamically changes.
8	Select the time and dates for the rollup, and click OK. Result: You return to the DB Admin tab.
9	Click Apply or OK. Result: You have successfully configured database rollups.

Configuring Billing aggregation

About Billing aggregation

ContentReporter gives you the ability to generate Billing reports (delimited Text files) based on usage of your network resources. You can import these Billing reports into third-party billing applications. You can select three of twelve fields (such as Hits and Bytes Dropped), the action taken on the data (such as calculating the average or total), the number of minutes over which to measure the data, and the delimiter of the text file (on the Report Definitions Style tab). You configure Billing aggregation on the Administration Billing tab.

To learn more about the Report Definitions Style tab, see the *ContentReporter 3.0 Reporting Guide*.

Note

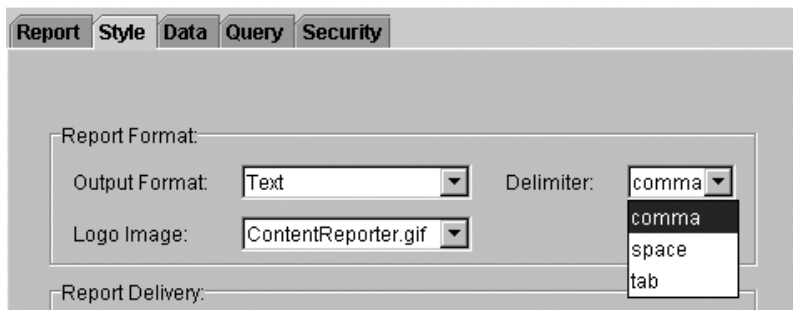
Whenever you modify Billing tab settings, you clear the database of all billing data for all ContentReporter servers connected to your database. Any pre-existing query definitions with billing statistics will no longer generate data. If you modify the Billing tab settings, delete any pre-existing query definitions based on Billing statistics, and create new query definitions based on Billing statistics.

Note

Ensure that you have set the number of days to keep billing data on the DB Admin tab high enough to generate meaningful billing reports. To learn more about database rollover, see “[Configuring database rollups](#)” on page 159.

The Report Definitions Style tab

The following screen highlights the Text file (Billing report) selection for report output on the Report Definitions Style tab.



The screenshot shows the 'Report Definitions Style' tab in the ContentReporter interface. The tab is selected, and the 'Report Format' section is visible. It contains three dropdown menus: 'Output Format' (set to 'Text'), 'Delimiter' (set to 'comma'), and 'Logo Image' (set to 'ContentReporter.gif'). The 'Report Delivery' section is partially visible at the bottom. The 'Delimiter' dropdown menu is open, showing options: 'comma', 'space', and 'tab'.

Billing Report characteristics

The following table describes Billing report characteristics

Characteristic	Description
Text File Delimiters	Comma (csv), Tab (txt), and Space (txt) You select the delimiter on the Report Definitions Style tab.
Time Interval	Minutes (from one to 60 minutes) The number of minutes over which the billing data is aggregated. The shorter you set the interval, the finer the level of detail (or “granularity”) of the data you generate.
Available fields (Billing Statistics)	Hits, Bytes, Bytes Dropped, Packets Requested, Packets Served, Packets Resent, Packets Dropped, Streaming Connect Time, Play Time, Response Time, Streaming Transfer Time, and Streaming Average Bit Rate
Action taken on field data	Minimum, Maximum, Average, or Total

Billing aggregation example

The following table contains an example of billing aggregation settings.

Aggregation settings to bill for total bytes over 30 minute intervals	
Billing tab field or box	Value
Billing aggregation interval	30
Field 1	Bytes
Action 1	Total
Enable billing processing	Checked

The relationship between Billing tab settings and available Billing Query statistics

The Administration Billing tab settings determine which three Billing statistics are available for a query definition, and determine how these statistics are calculated. For example, if you select Hits, Bytes Dropped, and Play Time on the Administration tab, these are the only Billing statistics that will be available to you for query definitions. Query definitions that use other Billing statistics do not generate data in reports. If you select to calculate the average of the three statistics on the Administration Billing tab, these statistics will be averaged in every report.

Note_____The action taken on each field (Min, Max, Ave, or Total) determines the Billing statistic value you generate in reports.

The Billing tab

The following screen shows the Administration Billing tab with settings for Total Bytes, Maximum Hits, and Average Packets Served, and a five minute billing aggregation interval.

Cache Group

User Groups

Authentication

DB Admin

Billing

Licensing

Logging

Billing Aggregation Interval (minutes):

5

☒ Enable billing processing

Field 1:

Field 2:

Field 3:

Action 1:

Action 2:

Action 3:

Bytes

Hits

Packets Served

Total

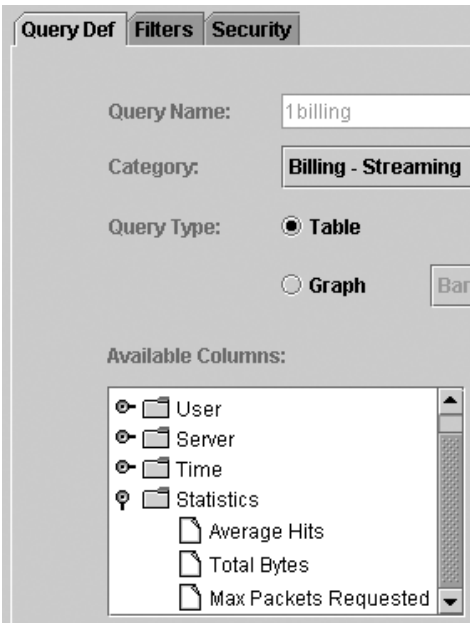
Max

Average

Reset

The Query
Definition Query
Def tab

The following screen illustrates the available Billing Statistics columns on the Query Def tab when the Administration Billing tab is configured for Total Bytes, Maximum Hits, and Average Packets Served.



Configuring Billing
aggregation

To configure Billing aggregation, complete the following steps.

Note—
Whenever you modify Billing tab settings, you clear the database of all billing data for all ContentReporter servers connected to your database. Any pre-existing query definitions with billing statistics no longer generate data. If you modify the Billing tab settings, delete any pre-existing query definitions based on Billing statistics, and create new query definitions based on Billing statistics.

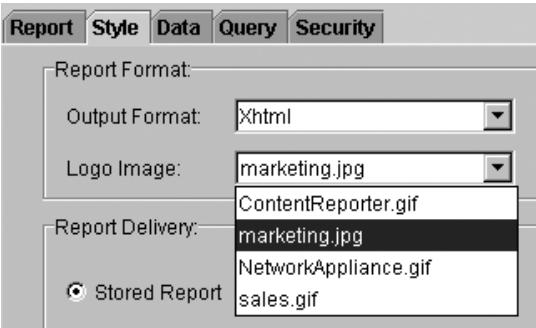
Step	Action
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.

Step	Action
2	Click the Admin button. Result: The Cache Group tab appears.
3	Click the DB Admin tab. Result: The DB Admin tab appears.
4	Ensure that the number of days to keep billing data is adequate or enter a different number, and click Apply.
5	Click the Billing tab. Result: The Billing tab appears.
6	Ensure that the “Enable billing processing” check box is checked.
7	Accept the default Billing Aggregation Interval (5 minutes), or select a different number of minutes from the drop-down list.
8	From the three Field drop-down lists, select the Billing statistics you want available for query definitions and Billing reports.
9	To the right of each Field, select the appropriate action to take upon the Field data from the Action drop-down lists.
10	Click OK or Apply to save the changes to the ContentReporter server. Result: The Billing Information Change Warning dialog box appears.
11	Click Yes. Result: You have successfully configured billing aggregation. You can now create a query definition and select these three Billing statistics, create a new (Billing) report definition and select the new query definition for the report, and then generate a Billing report with the new report definition. To learn more about creating query definitions and report definitions, see the <i>ContentReporter 3.0 Reporting Guide</i> .

Adding logo images to ContentReporter for XHTML Reports

About logo images Each XHTML report includes a logo image in its top left corner. You select a report definition’s logo image from the drop-down list on the Report Definitions Style tab. You can add multiple customized logo images to ContentReporter for different types of reports. By default, reports include a *ContentReporter.gif* logo image. To add other logo images to ContentReporter, you simply add them to the proper folder on the ContentReporter server machine.

The Report Definitions Style tab The following screen highlights the logo image drop-down list on the Report Definitions Style tab.



Adding logo images To add logo images to ContentReporter for XHTML reports, complete the following steps.

Step	Action
1	Copy the logo image file(s) into the ContentReporter server machine folder: ..Network Appliance\ContentReporter\jakarta-tomcat\webapps\ContentReporter\logo\ Result: You have successfully added the logo image(s) to ContentReporter.

About this appendix This appendix contains quick-start instructions to set up log file collection and to create and set permissions for a Local user. By following the steps in these examples, you will familiarize yourself with these major administrative tasks in ContentReporter.

Topics covered in this appendix

This appendix contains the following quick-start examples:

- ◆ [“Quick-start: Setting up log file collection”](#) on page 170
- ◆ [“Quick-start: Adding a Local user and setting the user’s permissions”](#) on page 174

Quick-start: Setting up log file collection

About this quick-start example

This quick-start example walks you through the process of defining a cache group, adding a cache to collect and process log files from a directory, creating a scheduled event to collect and process its log files, and examining the results. By following this example, you will familiarize yourself with the entire process of setting up log file collection.

Note

Before defining the cache group in this example, save or push one or more log files into a directory that is accessible to the ContentReporter service login user account.

Defining a cache group and processing its log files

To define a cache group and process its log files, complete the following steps.

Step	Action
Defining a cache group	
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	Click New Group. Result: The New Group window appears.
4	Enter a unique name for the group, check either the HTTP Analysis box, the Streaming Analysis box, or both boxes, and then click OK. Result: You return to the Cache Group tab, and this cache group appears in the cache group listing.
5	Click Apply to save the changes to the ContentReporter server. Result: You have successfully defined the cache group.
Adding a cache	

Step	Action
6	To add a cache to this cache group, select the cache group in the left-hand panel, and click New Cache. Result: The New Cache window appears.
7	Enter a name for the log file source, click the “Collect from imported directory” radio button, and click Browse to browse to the location of the saved log files. Result: The Browse for Directory path window appears.
8	Browse to the location of the saved log files, and double-click the folder (or select the folder and click OK). Result: You return to the New Cache window, and the location of the saved log files appears in the Import log files directory field.
9	If the log files contain no header, check the check box, and click the radio button for the log file’s format.
10	To delete the log files after processing, check the appropriate box.
11	Accept the default number of error lines (200), or enter another number. If you do not want the number of error lines in a log file to stop the ContentReporter server from processing, enter the number 0.
12	When you have entered all the required information, click OK. Result: You return to the Cache Groups tab and the cache appears under the cache group in the left-hand panel.
13	Click OK to save the changes to the ContentReporter server. Result: You return to the Administration page, and have successfully added a cache to collect and process log files from a directory.
Creating a scheduled event	
14	To create a Scheduled Event to collect and process the cache group’s log files, click the Scheduled Events tab. Result: The Scheduled Events page appears.

Step	Action
15	Click the New button. Result: The Details tab appears.
16	Enter a name (such as “Cache Group 1 Collection”) in the Task Name field.
17	Select “Collect and or import logs” from the Type drop-down selection list.
18	Select the cache group from the Cache Groups drop-down list.
19	Click the Schedule tab. Result: The Schedule tab appears.
20	In the Start time field, enter the time it will be two minutes from now, and click OK. Result: You return to the Scheduled Events page, and the new Scheduled Event appears on the page. It should be scheduled to run in a two minutes.
21	You can run the collection event immediately, or you can let the Scheduled Event begin in two minutes. Click Run to immediately start the collection event, or wait for the event to begin in two minutes. Result: ContentReporter begins to collect and process this cache group’s log files.
Examining the results	
22	After ContentReporter has collected and processed this cache group’s log files, a “Collect and or import logs” event appears for this cache group. The event’s name is composed of the cache group’s name and a time-stamp.
23	To view more detailed information (such as the event’s Start and Finish times) about this log file collection and processing event, check the box adjacent to this event, and click History. Result: The Scheduled Events History page appears for this event.

Step	Action
24	To view the names and locations or sources of the imported log files, check the box adjacent to this event, and click Logs. Result: The Events History Log Files page for this event appears, and lists the names and locations or sources of the imported log files.
25	After viewing the log files, click Close to return to the Scheduled Events History page for this event, and click Close again. Result: You return to the Scheduled Events page, and have successfully examined the history of the scheduled log file collection and processing event. Note_____ Now that ContentReporter has processed this cache's log files, you can create a report definition based on this cache and generate reports on this cache. To learn more about creating report definitions, see the <i>ContentReporter 3.0 Reporting Guide</i>. _____

Quick-start: Adding a Local user and setting the user's permissions

About this quick-start example

This quick-start example walks you through the process of adding a Local user and configuring the user's permissions. By following this example, you will familiarize yourself with basic authentication and permissions configuration tasks.

Adding a Local user and configuring the user's permissions

To add a Local user and configure the user's permissions, complete the following steps.

Step	Action
Adding a Local user	
1	From a page in ContentReporter, click the Administration tab. Result: The Administration page appears.
2	Click the Admin button. Result: The Cache Group tab appears.
3	Click the Authentication tab. Result: The Authentication tab appears.
4	Select Local from the Authentication Method drop-down list, and click New. Result: The New User window appears.
5	Enter a name, a password, select one of the three groups from the User Group drop down list, and, if desired, an e-mail address.
Setting permissions	
6	To set permissions for this new Local user, click Permissions. Result: The Add Permissions window appears.

Step	Action
7	To take away particular privileges, uncheck the appropriate boxes. Note_____ If you have not granted a particular permission to the user's group, checking that permission in this window will not give the user that permission. In this window you can only take away permissions from this user that you have granted to this user's group.
8	To specify the site name(s) on which the user can generate reports, click Add. Result: The Add Site Name window appears. Note_____ By default, users can generate reports on all site names. You can configure a user's permissions in the Add Site Name window so that they can only generate reports on the site names you specify.
9	Enter the site name (such as "www.netapp.com") and click OK. Result: You return to the Add Permissions window. Note_____ You can also use the * (asterisk) wildcard character in the Name field. For example, you can enter "*.edu" so that the user can only generate reports on site names with the ".edu" extension.
10	Repeat steps 8 and 9 to specify additional site names.
11	Once you have set the desired permissions, click OK. Result: You return to the New User window.
12	Click OK. Result: You return to the Authentication tab.
13	To save the changes to the ContentReporter server, click Apply or OK. Result: You have successfully added a new Local user and configured the user's permissions.

About this appendix This appendix describes how to assign a login user account to the ContentReporter service to access network resources.

Topics covered in this appendix This appendix covers the following topics:

- ◆ [“Learning about the login user account”](#) on page 178
- ◆ [“Configuring a Windows NT system”](#) on page 179
- ◆ [“Configuring a Windows 2000 system”](#) on page 181

Learning about the login user account

When you need to assign an account

You need to assign the ContentReporter service a login user account with access to network resources if you collect or import log files from, or store collected log files on, a mapped drive.

About the login user account

By default, the ContentReporter service uses the Local System Account, and automatically starts when the system starts up. This Local System Account enables ContentReporter to collect and store log files on the ContentReporter server machine. If you want ContentReporter to collect, process, and store log files on mapped or network drives, you should consider assigning a user account to the ContentReporter service, since the account must have access to mapped drives in one or more domains, and must be always logged into the ContentReporter server machine when ContentReporter is running.

Account requirements

The following table describes the ContentReporter service login user account requirements for various capabilities.

Capability	ContentReporter service login user account requirements
Collect and store log files on mapped drives	◆ Has privileges to access the mapped drives ◆ Is always logged into the ContentReporter server machine when ContentReporter is running
Collect and store log files on mapped drives in multiple domains	◆ Has privileges to access the mapped drives ◆ Exists (with same user name and password) in each domain from which the mapped drives originate ◆ Is always logged into the ContentReporter server machine when ContentReporter is running

Configuring a Windows NT system

Assigning a login user account on a Windows NT system

To assign a login user account to the ContentReporter service on a Windows NT system, complete the following steps.

Step	Action
1	From the Windows NT user interface, click Start > Settings > Control Panel, and double-click Services. Result: The Services window appears.
2	Select the ContentReporter service, and click Stop. Result: The ContentReporter service stops.
3	Click Startup. Result: The Service window appears.
4	Click the This Account radio button, and click the browse box. Result: The Add User window appears.
5	Select the user account from the drop-down list with Administration privileges on the ContentReporter server machine and access to the mapped drives, click Add, and click OK. Result: You return to the Service window, and the user account appears in the This Account field.
6	Enter the account's password in the Password field and the Confirm Password field, and click OK. Result: You return to the Services window.
7	Select the ContentReporter service, and click Start. Result: The ContentReporter service starts.

Step	Action
8	Click Close > File > Close. Result: You return to the Windows NT user interface, and have successfully assigned a login user account to the ContentReporter service. Note_____ When you start the ContentReporter service, you may need to wait a moment for the ContentReporter to start running.

Configuring a Windows 2000 system

Assigning a login user account on a Windows 2000 system

To assign a login user account to the ContentReporter service on Windows 2000 system, complete the following steps.

Step	Action
1	From the Windows 2000 user interface, click Start > Settings > Control Panel > Administrative Tools, and double-click Services. Result: The Services window appears
2	Right-click the ContentReporter service, and click Stop. Result: The service stops.
3	Right-click the ContentReporter service, and click Properties. Result: The ContentReporter Service Properties window appears.
4	Click the Log On tab. Result: The Log On tab appears.
5	Click the This account radio button, and click Browse. Result: The Select User window appears.
6	Select the user account with Administration privileges on the ContentReporter server machine and access to the mapped drives, and click OK. Result: You return to the Properties window, the user account appears in the This account field.
7	Enter the password in the Password and Confirm password field, and click OK. Result: You return to the Services window.
8	Right click the ContentReporter service, and click Start. Result: The service starts.
9	Close the window. Result: You return to the Administrative Tools window.

Step	Action
10	Click File > Close. Result: You return to the Windows 2000 user interface, and have successfully assigned a login user account to the ContentReporter service. Note_____When you start the ContentReporter service, you may need to wait a moment for the ContentReporter to start running._____

About this appendix This appendix describes various NetCache appliance configuration tasks for ContentReporter. Depending on how you use ContentReporter, you may not need to complete any of these tasks, or you may need to complete some or all of them.

Note

These instructions describe how to configure NetCache appliance 5.2 for ContentReporter. If you have a different NetCache appliance release, some of these steps may vary.

Note

To learn more about configuring your NetCache appliance, see your NetCache appliance documentation.

Topics covered in this appendix

This appendix covers the following topics:

- ◆ [“Enabling NetCache appliance Web Access logging”](#) on page 184
- ◆ [“Enabling NetCache appliance Streaming Access logging”](#) on page 185
- ◆ [“Configuring a NetCache appliance for SmartFilter reports”](#) on page 186
- ◆ [“Configuring NetCache appliance log file collection”](#) on page 188

Enabling NetCache appliance Web Access logging

About enabling Web Access logging

If you want to use HTTP analysis on NetCache log files to generate reports in ContentReporter, you must enable NetCache Web Access logging.

Enabling Web Access logging

To enable Web Access logging, complete the following steps.

Step	Action
1	To enable Web Access logging, click the Setup tab in the NetCache Manager.
2	Click HTTP > Logging.
3	Ensure that the Enable Web Access Log box is checked.
4	Ensure that the appropriate log format is selected, and click Commit Changes.

Enabling NetCache appliance Streaming Access logging

About enabling Streaming Access logging

If you want to use Streaming analysis on NetCache log files to generate reports in ContentReporter, you must enable NetCache Streaming Access logging.

Enabling Streaming Access logging

To enable Streaming Access logging, complete the following steps.

Step	Action
1	To enable Streaming Access logging, click the Setup tab in the NetCache Manager.
2	Click Streaming > Logging.
3	Ensure that the Enable Streaming Access Log box is checked.
4	Ensure that the appropriate log format is selected, and click Commit Changes.

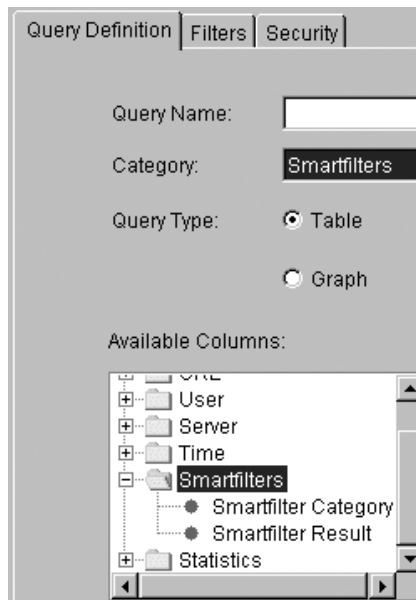
Configuring a NetCache appliance for SmartFilter reports

About the SmartFilter fields

If you want to generate SmartFilter reports in ContentReporter on NetCache appliance log files, you must configure the NetCache to generate Custom HTTP log files that include the “x-smartfilter-categories” and “x-smartfilter-result” fields.” The “x-smartfilter-categories” values are strings consisting of one or more comma-separated, two-letter codes (such as “gm” for games, or “sp,tr” for sports and travel). The “x-smartfilter-result” values are either 1 (for blocked) or 0 (for not blocked). The blocked value means the NetCache prevented the user (client IP) from opening the web page. The unblocked value means the NetCache allowed the user to open the web page.

SmartFilter data elements

The following screen highlights the two SmartFilter data elements available for query definitions on the Query Definitions Query Def tab.



Configuring a NetCache for SmartFilter reports

To configure a NetCache appliance for SmartFilter reports in ContentReporter, complete the following steps.

Step	Action
1	In the NetCache Manager window, click Setup > HTTP > Logging. Result: The HTTP - Logging page appears.
2	Scroll down to and click the Custom Log Format radio button.
3	Enter x-smartfilter-categories and x-smartfilter-result fields in the Custom box, as well as any other fields you need.
4	Click Commit Changes. Result: You have successfully configured the NetCache appliance to generate log files for SmartFilter reports.

Configuring NetCache appliance log file collection

About Configuring your NetCache for log file collection

If you intend to collect log files directly from NetCache appliances with ContentReporter, you must properly configure the caches for ContentReporter.

Configuration tasks

Depending on your needs, you will complete some or all of the following tasks:

- ◆ [“Gathering NetCache appliance information”](#) on page 189
- ◆ [“Synchronizing logging rotation and log file collection”](#) on page 191
- ◆ [“Enabling SNMP and using Auto Discovery”](#) on page 194

Gathering NetCache appliance information

The NetCache information you need

In order for ContentReporter to collect log files directly from a NetCache, you must identify the following information for the NetCache:

- ◆ User name
- ◆ Password
- ◆ IP address
- ◆ Port

Gathering the information

To gather the information you need to collect NetCache log files, complete the following steps.

Step	Action
1	To identify or create a user name and password, click the Setup tab in the NetCache appliance Manager window.
2	Click Authentication > NetCache Users.
3	Identify an existing User or (create a new User) who belongs to a group with full Admin permissions.
4	Record the user name and password.
5	To identify the IP address of the NetCache appliance, click the Setup tab in the NetCache Manager.
6	Click Network > Interfaces.
7	Identify the NetCache IP address listed in the Primary IP Address column.
8	Record the IP Address.
9	To identify the port through which to access log files, click the Setup tab in the NetCache Manager.
10	Click Administration > Administrative Access.
11	Ensure that the HTTP check box is checked, and identify a port (such as 3132) listed in the Admin Ports panel.

Step	Action
12	Record the port number.
13	Repeat steps one through twelve for each NetCache appliance from which ContentReporter will collect log files. To learn more about collecting NetCache log files, see “Adding a cache to collect from NetCache appliances” on page 78.

Synchronizing logging rotation and log file collection

Reason to synchronize log rotation and collection

If ContentReporter collects log files directly from a NetCache, you must synchronize NetCache logging rotation and ContentReporter log file collection to ensure that the NetCache does not rotate out some log files faster than the ContentReporter collects them. If a NetCache rotates out some log files before collection, data is lost. Depending on how fast your NetCache appliance log files grow in size, you might need to modify the NetCache logging rotation and maximum log file size, and increase how often the ContentReporter server collects the log files.

Note

If you do not want to synchronize NetCache logging and ContentReporter log file collection, configure your NetCache to push its log files to either a directory or an FTP server and configure ContentReporter to collect the log files from the directory or FTP server.

How NetCache logging works

When you select log rotation, the NetCache appliance saves the active log and up to 10 previous log files on disk for each type of log that is enabled. When the log reaches maximum size, or when the preset interval or time is reached, the NetCache appliance rotates out the oldest log. The previously active log then becomes the most recent old log. Logs remain on the appliance until they are rotated out. You can set the maximum log file size from 1 to 1999 megabytes.

Note

The NetCache appliance always rotates or pushes a log file when it reaches the maximum size, regardless of the settings specified in the “How to Switch Log Files” option.

Example

The following example illustrates the relationship between the NetCache appliance logging and the ContentReporter server collection of logs.

Relationship between NetCache logging and ContentReporter collection of log files
Assume you set the maximum log file size of a certain NetCache appliance to 500 megabytes, schedule its log files to rotate daily at six a.m., and schedule the ContentReporter server to collect the NetCache appliance log files every day at one a.m.

Relationship between NetCache logging and ContentReporter collection of log files	
Scenario A: Successful log file collection	If the NetCache appliance log files reach the maximum size four times in between rotation times, (and the NetCache rotates out four old log files), the ContentReporter server will successfully collect all new log files at one a.m. (At six a.m., the NetCache rotates out a fifth old log file.)
Scenario B: Unsuccessful log file collection	If the NetCache appliance log files reach the maximum size fifteen times in between rotation times, (and the NetCache rotates out fifteen old log files), the ContentReporter server will not collect up to five NetCache appliance log files that were rotated out. Any reports on this NetCache appliance generated in ContentReporter would be inaccurate. To correct this situation, you could either increase the maximum log file size to 1000 megabytes, and/or schedule the ContentReporter server to collect the log files twice a day.

Synchronizing log rotation and collection

To synchronize NetCache logging rotation and the ContentReporter server collection of log files, complete the following steps.

Note

The following instructions explain how to enable both Web Access logging and Streaming Access logging. If you collect only one type of log file, skip the instructions for enabling the other type.

Step	Action
1	In the NetCache appliance Manager window, click the Data tab
2	To examine Web Access log file rotation settings, click Log Files > Web Access. Result: The Web Access log file names, time-stamps, and sizes appear in the first panel.
3	Examine the Web Access log files to determine how quickly the log files are growing in size and rotating.
4	Record this logging information. You will use this information when you schedule log file collection.
5	To examine Streaming Access log files, click Streaming Access. Result: The Streaming Access log file names, time-stamps, and sizes appear in the first panel.

Step	Action
6	Examine the Streaming Access log files to determine how quickly the log files are growing in size and rotating.
7	Record this logging information. You use this information when you schedule log file collection.
8	To review or modify the maximum log file size and logging rotation, click the Setup tab.
9	Click System > Logging. Result: The maximum log file size and logging information displays.
10	Examine, and if necessary, modify the NetCache logging rotation as needed.
11	Record this logging information. You will use this logging information to properly schedule the log file collection in ContentReporter. To learn more about scheduling log file collection, see “Step three: Scheduling log file collection” on page 93.

Reason to enable SNMP

If you want to collect log files from several NetCache appliances, you may want to use the Auto Discovery feature of the ContentReporter server. The Auto Discovery feature enables you to quickly and easily add multiple NetCache appliances to a cache group at one time. In order to use the Auto Discovery feature, you must enable Simple Network Management Protocol (SNMP) for each NetCache appliance. You must also identify a community string name that the ContentReporter server can use to identify each NetCache appliance through Auto Discovery.

Enabling SNMP and indentifying a community string

To enable NetCache appliance SNMP for Auto Discovery and identify a community string, complete the following steps.

Step	Action
1	In the NetCache Manager window, click the Setup tab
2	Click Administration > SNMP.
3	Ensure that the Enable SNMP box is checked.
4	Identify a community string (such as “public”) listed in one of the Communities fields.
5	Record this community string name. You will enter this string when using the Auto Discovery feature in ContentReporter. To learn more about using Auto Discovery, see “ Using Auto Discovery ” on page 85.

Glossary

appliance	A device that performs a single, well-defined function and is simple to install and operate, for example, a NetCache appliance or NetApp filer.
authentication	The process of verifying the identity of a user who is logging into a computer system. The ContentReporter server authenticates a username-password combination each time a user logs in. ContentReporter gives you the ability to simultaneously use its own built-in “Local” authentication, and either a Lightweight Directory Access Protocol (LDAP) server or an NT LAN Manager (NTLM) to authenticate users. A Local user is a login account maintained in the ContentReporter application.
auto discovery	The ContentReporter feature that gives you the ability to add one or more SNMP-enabled NetCache appliances (for which you have community string names) to a cache group at one time. You can only discover NetCaches with Class C IP addresses using the auto discovery feature.
cache	A device that generates the log files that the ContentReporter server collects/imports and processes. ContentReporter can collect/import and process NetCache™ appliance log files, Web server log files, and streaming server log files.
cache group	A logically defined group of one or more caches. A cache group is a management tool that enables you to specify the time and frequency of log file collection, and the type of log file analysis for its caches.
console	A physical or virtual terminal that is used to monitor and control a NetApp appliance.
ContentReporter	A Network Appliance software solution that enables you to analyze content usage, performance, and infrastructure load across your entire content delivery network. The ContentReporter server collects and processes log files from NetCache appliances, directories, and FTP servers throughout a

network, and outputs the results of the log file processing to your enterprise database. You log into ContentReporter with a Web browser on your network, and schedule and generate customized reports on the log file data in your database.

ContentReporter log file

The log file that contains a record of the ContentReporter server activity. If you have a problem processing log files or generating reports, you may be able to discover the cause of the problem by examining this log file.

ContentReporter parser

The ContentReporter server component that processes collected log files.

ContentReporter server

The program that receives and fulfills HTTP requests from client browsers on the same or other computers. The computer on which you install ContentReporter is the ContentReporter server machine.

ContentReporter sorter

The ContentReporter server component that sorts and groups the log file data it receives from the ContentReporter parser.

ContentReporter SQL bulk uploader

The ContentReporter server component that performs bulk updates to the database.

ContentReporter user interface

A Web browser with HTTP access to the ContentReporter server. You make requests to, and receive fulfilled requests from, the ContentReporter server through a Web browser.

data element

The columns of table queries and the axes or components of graph queries. Data elements are the actual values, measurements, and statistics that make up queries. “Packets sent” and “URL” are examples of data elements. You can select which data elements to include in a particular query, and customize how each data element appears in a query.

database rollup	A scheduled database background task that converts hourly data into monthly data. The database rollup feature gives you the ability to keep a specified number of days of hourly data available for reports in your database. You can also specify the number of days of Billing data and Streaming data to keep available for reports.
Domain Name System (DNS)	An Internet service that locates and translates domain names into Internet Protocol (IP) addresses.
embedded database	A Sybase Adaptive Server Anywhere (ASA) 7.0.1 database intended for evaluation situations. When you first install ContentReporter, the ASA is your default database. You can use this database to collect and process small log files, and to generate reports on these log files.
enterprise database	The database (MS SQL 7.0, SP 2 or Oracle 8.1.7) used by the ContentReporter application. The ContentReporter server stores its settings and all aggregated log file records for each cache device in the database. All reports in ContentReporter are based on the records for each cache in the database.
filer	An appliance that attaches to a computer network and is used for data storage. NetApp filers operate using Data ONTAP software.
fully qualified domain name (FQDN)	The complete name of a specific computer on the Internet, an intranet, or a network consisting of the computer's host name and its domain name.
host name	The last domain name (with its extension) in a URL string that contains two domain names. When one web site hosts another web site, the first domain name (with its extension) is the site name. For example, in the URL string "www.netapp.com/aaa/www.webmanage.com/home.htm," "www.netapp.com" is the site name and "www.webmanage.com" is the host name.

Import log files feature	The ContentReporter feature that enables you to process log files for a cache device without creating a scheduled event. This feature gives you the ability to process log files that were not collected or processed by a scheduled event and output the result to your database for a new or existing cache.
IP address	The unique numerical Internet Protocol (IP) address of a computer that is attached to a TCP/IP network, for example, 12.34.56.78.
MIME	Multipurpose Internet Mail Extensions. A specification that defines the mechanisms for specifying and describing the format of Internet message bodies. An HTTP response containing the MIME Content-Type header allows the HTTP client to invoke the application that is appropriate for the data received.
MMS	Microsoft Media Streaming. The streaming media control protocol used in Windows Media Technologies 3 and 4 streams.
NetCache	The proprietary software that runs on NetCache appliances. Developed by Network Appliance.
NetCache appliance	An appliance designed specifically to serve Internet and intranet content quickly and reliably. Developed by Network Appliance.
NetCache Manager	The browser interface through which a NetCache appliance is managed.
NOW	NetApp On the Web. The secure customer service Web site for Network Appliance.
page permissions	Settings that specify which Local users and which groups have permission to access a page, and specify how they can use a page's features and objects. ContentReporter gives you the ability to grant Unix-style permissions (read, write, execute, and delete) for the Administration, Query Definitions, Report Definitions, Scheduled Events, and Report Results pages.

query	The tabular or graphical report results of a customized search of the database records of a report definition's cache or caches. A report query is generated by a query definition. Each report definition includes one or more query definitions.
query definition	A customizable template used to search the database records of a report definition's cache or caches that generates table and graph queries in reports. You can select the data elements to include in the query, and customize how each data element appears in a report. You can create your own customized query definitions or use the pre-defined query definitions. "Reference by Status Code" and "Top View Clips" are two of the pre-defined query definitions.
report definition	A customizable template used to generate cache device reports. You select the queries to include in a report, the format (XHTML or Text) of a report, and the delivery method (save locally, FTP, or e-mail) of a report.
RTSP	Real Time Streaming Protocol. An open standard for delivery of real-time media over the Internet.
scheduled event	A scheduled log file collection and processing event or a scheduled report generation event. You create a scheduled event to schedule the ContentReporter server to automatically collect and process log files or generate a report one time or at regular intervals.
security	Permission settings for users and groups on specific objects (query definitions, report definitions, and scheduled events) on pages. Page permissions apply to all objects on a page. Object security enables you to prevent certain users or groups who have access to the Query Definitions, Report Definitions, and Scheduled Events pages from seeing, modifying, running, selecting, or deleting particular events or definitions.
site name	The first or only domain name (with its extension) in a URL string. When one web site hosts another web site, the first domain name (with its extension) is the site name and the last domain name (with its extension) is the host name. For example, in the URL string "www.netapp.com/aaa/www.webmanage.com/home.htm," "www.netapp.com" is the site name and "www.webmanage.com" is the host name.

SSL protocol	Secure Sockets Layer (SSL) protocol. A protocol that provides an encrypted administrative exchange between a NetCache and a client browser. If you installed SecureAdmin™ software on a NetCache appliance, you can configure ContentReporter to use the SSL protocol to securely collect log files from the NetCache.
stream	A media file that is transmitted in a continuous flow over a network. Streams are of two types, live and on-demand.
streaming media	A term used to describe media files that begin playing while they are being transmitted over the network to the media player on the client computer.
streaming server	A server configured to serve streaming media to clients.

Index

A

- Administration page
 - description of 34
- authentication
 - description of 117, 125, 195
 - LDAP and NTLM failover 118
- Authentication tab
 - description of 41
- Auto Discovery
 - description of 85, 195
 - enabling SNMP on a NetCache 194

B

- billing aggregation
 - configuring 166
 - description of 163
 - query statistics
 - description of 165
 - reports
 - description of 164
 - settings
 - description of 49
- Billing tab
 - description of 48

C

- cache
 - Cache Name for SSL 79
 - collecting from a directory 76
 - collecting from a NetCache 78
 - collecting from an FTP server 91
 - configuring ContentReporter for SSL 80
 - deleting log files after parsing 75
 - description of 2, 71, 195
 - headerless log file format 75
 - import log files feature 111, 198
 - manually adding a NetCache 82
 - modifying settings 105, 107
 - NetCache Name or IP Address for SSL 79
 - quick-start instructions

- adding caches 170
 - removing a cache from a cache group 109
 - saving the certificate file for SSL 79
 - stopping parsing when error lines exceed
 - maximum 75
 - stored log files directory 74
 - using Auto Discovery to add NetCaches 85
 - using SSL to collect from NetCaches 78
- cache group
 - defining 69
 - deleting 105
 - description of 66, 195
 - HTTP analysis 68
 - modifying 103
 - quick-start instructions
 - defining a cache group 170
 - Streaming analysis 68
- Cache Group tab
 - description of 36
- certificate file
 - saving for SSL 79
- collecting log files from a directory 76
- collecting log files from a NetCache 78
 - gathering information 189
 - required information 189
 - synchronizing log rotation and collection 191
- collecting log files from an FTP server 91
- ContentReporter
 - adding logo images to ContentReporter for reports 168
 - assigning a login user account on Windows 2000 181
 - assigning a login user account on Windows NT 179
 - configuring ContentReporter logging 151
 - description of 2, 195
 - examining the ContentReporter log file 152, 158
 - header
 - description of 32
 - Home page
 - description of 33

- illustration of major components 3
- installing 6
- log file
 - description of 196
 - fields 152, 154
- logging
 - description of 149
 - levels 150
- login user account
 - description of 178
- minimum requirements 4
- parser
 - description of 196
- parser return codes 154
- repairing 10
- server 2
 - description of 196
- sorter
 - description of 196
- sorter return codes 155
- SQL bulk uploader
 - description of 196
- SQL bulk uploader return codes 156
- uninstalling 9
- user interface 2
 - description of 196

D

- data element
 - description of 196
- database
 - description of 2
 - embedded
 - description of 197
 - enterprise
 - description of 197
- database rollups
 - configuring 161
 - description of 159, 197
 - properties
 - description of 46
 - settings
 - description of 160
- DB Admin tab

- description of 46
- deleting log files after parsing
 - description of 75
- Details page
 - description of 98
- Details tab
 - description of 59

E

- embedded database
 - description of 197
 - learning about 15
 - settings 16
- enterprise database
 - description of 17, 197
- error lines
 - stopping parsing when error lines exceed maximum 75

F

- FTP server
 - collecting log files from an FTP server 91

H

- headerless log file format
 - description of 75
- History Page
 - description of 98
- host name
 - defined 121, 197
- HTTP analysis
 - description of 68

I

- import log files feature
 - description of 111, 198
- Import Log Files page
 - description of 54

J

- Java Runtime environment

installing 14

L

LDAP authentication

description of 126

settings

description of 43, 127

license information

description of 146

Licensing tab

description of 50, 147

Local user

adding 134

deleting 144

description of 134

modifying permissions 142

quick-start instructions

adding a Local user 174

Logging

the ContentReporter log file 149

logging

configuring ContentReporter logging 151

description of levels 150

parser return codes 154

sorter return codes 155

SQL bulk uploader return codes 156

logging into ContentReporter

entering the license key 12

the first time 12

Logging tab

description of 52

login user account

assigning on Windows 2000 181

assigning on Windows NT 179

description of 178

logo images

adding 168

Logs page

description of 98

M

MS SQL database

configuring 18

settings 19

multiple ContentReporter servers

configuring 29

diagram 30

N

NetCache

collecting log files from a NetCache 78

configuring for SmartFilter reports 187

enabling SNMP for Auto Discovery 194

enabling Streaming Access logging 185

enabling Web Access logging 184

information needed to collect from 189

NTLM authentication

description of 129

settings

description of 45

O

object security

description of 123

settings

table of 124

Oracle database

configuring 24

settings 25

P

page permissions

description of 119, 198

table of 120

permissions

modifying Local user permissions 142

modifying user group permissions 139

page permissions 119, 198

quick-start instructions

setting permissions 174

relationship between user and group

permissions 118

security settings

description of 199

setting user group permissions 131

site name restrictions 121

Q

query

- description of 199

query definition

- description of 199

quick-start instructions

- adding a Local user 174
- adding caches 170
- creating a scheduled event 171
- defining a cache group 170
- setting permissions 174

R

report definition

- description of 199

report query

- data elements
 - description of 196
- description of 199

rollups

- configuring 161
- description of 159, 197
- settings
 - description of 160

S

Schedule tab

- description of 61

scheduled event

- description of 199
- examining the history of 100
- quick-start instructions
 - creating a scheduled event 171

Scheduled Events page

- description of 56
- states, statuses, and conditions
 - description of 98

scheduling log file collection

- description of 94
- steps 95

security

- description of 123, 199

settings

- table of 124

Security tab

- description of 63

site name

- defined 121, 199
- restrictions 121

SmartFilter reports

- configuring a NetCache 187
- description of 186

SSL

- Cache Name for SSL 79
- configuring ContentReporter for SSL 80
- description of 78
- NetCache Name or IP Address for SSL 79
- saving the certificate file 79

SSL protocol

- description of 200

states, statuses, and conditions of scheduled events

- description of 98

stored log files directory

- description of 74

Streaming Access logging

- enabling a NetCache 185

Streaming analysis

- description of 68

U

user and group permissions

- the relationship between 118

user group

- deleting 141

user group permissions

- description of 131
- modifying permissions 139
- setting 131

User Groups tab

- description of 39

W

Web Access logging

- enabling a NetCache 184