

---

CM System

# **CM System Administration Manual**

Version 7.3

## Copyright and Licensing Statement

All intellectual property rights in the SOFTWARE and associated user documentation, implementation documentation, and reference documentation are owned by Percussion Software or its suppliers and are protected by United States and Canadian copyright laws, other applicable copyright laws, and international treaty provisions. Percussion Software retains all rights, title, and interest not expressly granted. You may either (a) make one (1) copy of the SOFTWARE solely for backup or archival purposes or (b) transfer the SOFTWARE to a single hard disk provided you keep the original solely for backup or archival purposes. You must reproduce and include the copyright notice on any copy made. You may not copy the user documentation accompanying the SOFTWARE.

The information in CM System documentation is subject to change without notice and does not represent a commitment on the part of Percussion Software, Inc. This document describes proprietary trade secrets of Percussion Software, Inc. Licensees of this document must acknowledge the proprietary claims of Percussion Software, Inc., in advance of receiving this document or any software to which it refers, and must agree to hold the trade secrets in confidence for the sole use of Percussion Software, Inc.

The software contains proprietary information of Percussion Software; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between Percussion Software and the client and remains the exclusive property of Percussion Software. If you find any problems in the documentation, please report them to us in writing. Percussion Software does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Percussion Software.

Copyright © 1999-2013 Percussion Software.  
All rights reserved

## Licenses and Source Code

CM System uses Mozilla's JavaScript C API. See <http://www.mozilla.org/source.html> for the source code. In addition, see the Mozilla Public License (<http://www.mozilla.org/source.html>).

Netscape Public License

Apache Software License

IBM Public License

Lesser GNU Public License

## Other Copyrights

The CM System installation application was developed using InstallShield, which is a licensed and copyrighted by InstallShield Software Corporation.

The Sprinta JDBC driver is licensed and copyrighted by I-NET Software Corporation.

The Sentry Spellingchecker Engine Software Development Kit is licensed and copyrighted by Wintertree Software.

The Java™ 2 Runtime Environment is licensed and copyrighted by Sun Microsystems, Inc.

The Oracle JDBC driver is licensed and copyrighted by Oracle Corporation.

The Sybase JDBC driver is licensed and copyrighted by Sybase, Inc.

The AS/400 driver is licensed and copyrighted by International Business Machines Corporation.

The Ephox EditLive! for Java DHTML editor is licensed and copyrighted by Ephox, Inc.

This product includes software developed by CDS Networks, Inc.

The software contains proprietary information of Percussion Software; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between Percussion Software and the client and remains the exclusive property of Percussion Software. If you find any problems in the documentation, please report them to us in writing. Percussion Software does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Percussion Software.

AuthorIT™ is a trademark of Optical Systems Corporation Ltd.

Microsoft Word, Microsoft Office, Windows®, Window 95™, Window 98™, Windows NT® and MS-DOS™ are trademarks of the Microsoft Corporation.

This document was created using AuthorIT™, Total Document Creation (see <http://www.author-it.com>).

Schema documentation was created using XMLSpy™.

**Percussion Software**

600 Unicorn Park Drive

Woburn, MA 01801 U.S.A.

781.438.9900

Internet E-Mail: [technical\\_support@percussion.com](mailto:technical_support@percussion.com)

Website: <http://www.percussion.com>



# Contents

<b>About the CM System Administration Manual .....</b>	<b>9</b>
<b>Managing Publishing .....</b>	<b>11</b>
Reviewing Publishing Status .....	12
Publishing Editions.....	13
Cancelling an Edition.....	14
Reviewing Publishing Logs.....	15
Pruning Publishing Logs.....	18
Republishing Failed Content .....	19
Monitoring Publication of Localized Content .....	20
<b>Maintaining Schedules.....</b>	<b>21</b>
Scheduled Tasks .....	22
Scheduled Task Editor .....	23
Creating a Scheduled Task.....	24
Modifying a Scheduled Task .....	25
Copying a Scheduled Task.....	26
Timed Event Logs .....	27
Task Notifications .....	28
Task Notification Editor .....	29
Creating a Scheduled Task Notification .....	30
Modifying a Timed Event.....	31
Deleting a Scheduled Task Notification.....	31
Default Task Notification Variables .....	31
Example Task Notifications .....	34
<b>Maintaining the CM System Server.....</b>	<b>39</b>
<b>Operating the CM System Server .....</b>	<b>41</b>
Operating the CM System Server in a .....	42
Windows Environment.....	42
Starting CM System Server as a Windows Service.....	42
Starting CM System Server as an Application.....	42
Changing CM System Server Service Settings.....	43
Using a Command to Stop CM System Server.....	43
Stopping CM System Server from the Services Dialog.....	43
Operating the CM System Server in a Unix .....	44
Environment .....	44
Starting CM System Server as a Daemon in a Unix .....	44
Environment.....	44
Starting the CM System Server as a Terminal Window in a .....	44
Unix Environment .....	44
Stopping CM System Server in Unix Environment When .....	45
Running as a Daemon .....	45

Stopping CM System Server in a Unix Environment When .....	45
Running as a Terminal Window .....	45
Uninstalling the CM System Daemon Control Scripts .....	45
Troubleshooting Server Initialization .....	46
Common Server Initialization Errors .....	46
Issuing Commands to the CM System Server .....	48
Server Console Commands by Function .....	48
Server Console Commands in Alphabetical Order .....	64
Tasks Requiring Restart of the CM System.....	70
Server .....	70
<b>Maintaining Users.....</b>	<b>71</b>
Configuring Access to Content Explorer.....	72
Tabs .....	72
Security Providers and Authentication .....	74
Security Providers Tab .....	75
Defining a Directory Connection Security Provider .....	75
Web Server .....	77
Windows NT .....	80
DBMS Table Security Provider .....	80
Using Directory Services.....	87
LDAP Directory Services Framework .....	89
Implementing LDAP Directory Services .....	90
LDAP Configuration Examples .....	117
Roles.....	139
Default Roles and Members .....	140
Add/Edit Role Dialog.....	143
Modify Member List for "Role" Dialog.....	145
Role and Member Properties.....	148
Role and Member Properties Required by CM System Functions .....	148
Adding a New Role .....	149
Editing a Role .....	149
Deleting a Role.....	150
Adding Existing Members to a Role.....	150
Adding New Members to a Role.....	151
Editing a Member's Properties .....	152
Deleting a Member from a Role .....	152
<b>Search Configuration .....</b>	<b>155</b>
Deployment Options for the Full-text Search Engine and Indices .....	157
Configuring the Full-Text Search.....	159
How to Override the Default Text Extractor .....	160
How to Override the Default Text Analyzer.....	162
Disabling Full-text Search.....	164
Configuring Maximum Search Results Returned.....	165
Full-text Search in Globalized Environments.....	167
Maintaining Stop Words.....	168
Re-indexing the Full-Text Search.....	169
<b>System Management and Recovery.....</b>	<b>171</b>

Physical Architecture of CM System .....	172
All Physical Components Local .....	172
CM System Server with Local Repository, Remote Web Server Using FTP Publishing .....	173
CM System Server with Remote Repository and Remote Web Server Using FTP Publishing .....	174
Source Control and Backups .....	175
Integrating CM System with a Source Control System .....	175
Backing Up the CMS .....	175
Backing Up Your Web Site .....	176
Setting Up a CM System Failover Server.....	179
Setting Up a CM System Disaster Recovery Server.....	180
Managing Binaries.....	181
Conversion of existing binary fields .....	181
Export and Import of Binaries .....	185
Migrating table structure from previous versions of hashed binaries .....	186
New Binary tables.....	186
Removal of unreferenced binaries .....	187
Binary Metadata.....	189
<b>Index.....</b>	<b>181</b>





---

## CHAPTER 1

# About the CM System Administration Manual

The *CM System System Administration Manual* documents how to manage and maintain the CM System Content Management System. Both day-to-day and long-term administration tasks are addressed in this document.

Users of this manual should be familiar with the *CM System Concepts Guide*, but need not have read detailed implementation documentation nor attended CM System Developer's Training.

Users need not read the complete manual. In many cases, a single chapter or section may address the specific task you need to accomplish.

- If you manage Publishing, including monitoring publishing logs and troubleshooting and republishing failed Content Items, read Chapter 1, *Managing Publishing*.
- If you need to start or stop the CM System server, or issue a command to the CM System server, read Chapter 2, *Operating the CM System Server* (see page 41).
- If you need to manage users and their access to CM System, read Chapter 3, *Maintaining Users* (see page 71); specifically:
  - if you need to manage or add a new security provider, read *Maintaining Security Providers* (see "Security Providers and Authentication" on page 74);
  - if you use LDAP or Microsoft Active Directory to maintain user access to your system, read *Using Directory Services* (see page 87);
  - If you need to maintain Roles or user membership in a Role, read *Roles* (see page 139).
- If you need to manage the CM System full-text search engine, read *Search Configuration* (see page 155).
- If you need to manage the CM System Repository database, read *Repository Database Management and Maintenance*.
- If you need to manage or maintain system hardware infrastructure, read *System Management and Recovery* (see page 171); specifically:
  - If you need to plan the physical deployment of the system, read *Physical Architecture of CM System* (on page 172);
  - If you need to implement source control or manage backups of the CM System Content Management System, read *Source Control and Backups* (on page 175);
  - If you need to set up failover of the CM System Content Management System, read *Setting Up a CM System Failover Server* (on page 179).
  - If you need to set up a disaster recovery server for you system, read *Setting Up a CM System Disaster Recovery Server* (see page 180).



## CHAPTER 2

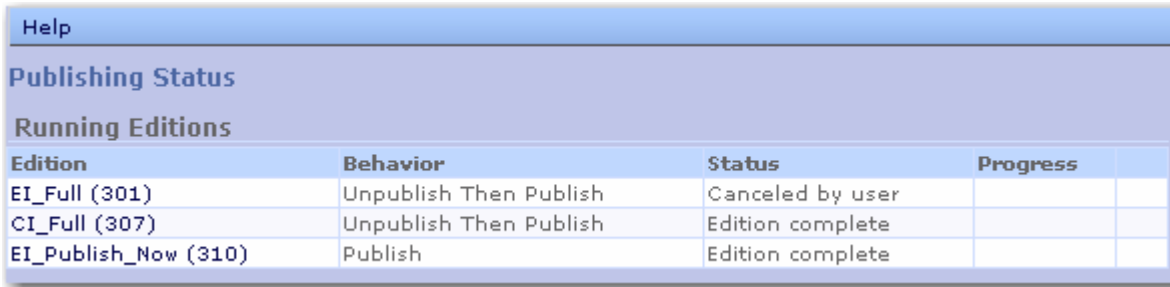
# Managing Publishing

The publishing process converts the raw Content Items entered by content contributors into output consumable by visitors to your Web site. To help manage publishing, CM System provides both logs and publication maps.

---

## Reviewing Publishing Status

For an overview of the status of all Editions currently running or recently run in the system, in the Navigation pane, click Publishing Status. The View and Edit pane displays the Publishing Status dialog



The screenshot shows a software dialog box titled "Publishing Status". At the top left is a "Help" button. Below the title bar, the text "Publishing Status" is displayed. Underneath, the section "Running Editions" is highlighted. A table follows with four columns: "Edition", "Behavior", "Status", and "Progress". The table contains three rows of data.

Edition	Behavior	Status	Progress
EI_Full (301)	Unpublish Then Publish	Canceled by user	
CI_Full (307)	Unpublish Then Publish	Edition complete	
EI_Publish_Now (310)	Publish	Edition complete	

*Figure 1: Publishing Status*

This dialog displays summaries of all Editions either currently running or that finished processing in the past hour. For details about a specific Edition, click on that Edition to see the Runtime Edition dialog.

# Publishing Editions

In a production system, Editions generally run automatically as scheduled tasks. You may sometimes need to publish an Edition manually as well.

To publish an Edition:

- 1 Open the Publishing Runtime tab of Content Explorer.
- 2 Access the Runtime Edition dialog:
  - Expand the Sites node, expand the Site with which the Edition you want to run is associated, and double-click on the Edition.

or

  - Double-click the Publishing Status link. CM System displays the Publishing Status dialog in the View and Edit pane. Double-click on the Edition you want to run.

Action							
Start Stop Help							
Sites > Enterprise_Investments > Editions > EI_Full							
Logs							
Select All   Select None							
Select	Job ID	Start Time	Elapsed (HH:mm:ss)	Status	Delivered	Removed	Failures
<input type="checkbox"/>	301	Jan 6, 2009 2:39:09 PM	00:01:07	✓	141	0	0

Figure 2: Runtime Edition page when an Edition is not running

- 3 In the Menu bar, click [**Start**].

CM System starts the Edition and adds runtime data to the Runtime Edition dialog.

**Action** Start Stop Help

Sites > Enterprise\_Investments > Editions > EI\_Full

Job ID 331

Percent Finished

Start Time Jan 7, 2009 9:15:49 AM

Elapsed 00:00:12

Current State Working

Queued 68

Prepared for Delivery 73

Delivered 0

Failed 0

**Logs**

Select All | Select None

Select	Job ID	Start Time	Elapsed (HH:mm:ss)	Status	Delivered	Removed	Failures
<input type="checkbox"/>	331	Jan 7, 2009 9:15:49 AM			0	0	0
<input type="checkbox"/>	301	Jan 6, 2009 2:39:09 PM	00:01:07		141	0	0

Figure 3: Runtime Edition page while an Edition is running

## Cancelling an Edition

When you cancel an Edition, all processing of that Edition stops and any output that has not been delivered is discarded. Delivered output is not changed, however.

To stop an Edition:

- 1 In the Navigation pane, double-click on *Publishing Status*.  
The View and Edit pane displays the Publishing Status dialog.
- 2 Select the Edition you want to cancel.
- 3 In the Menu bar, click *Stop*.

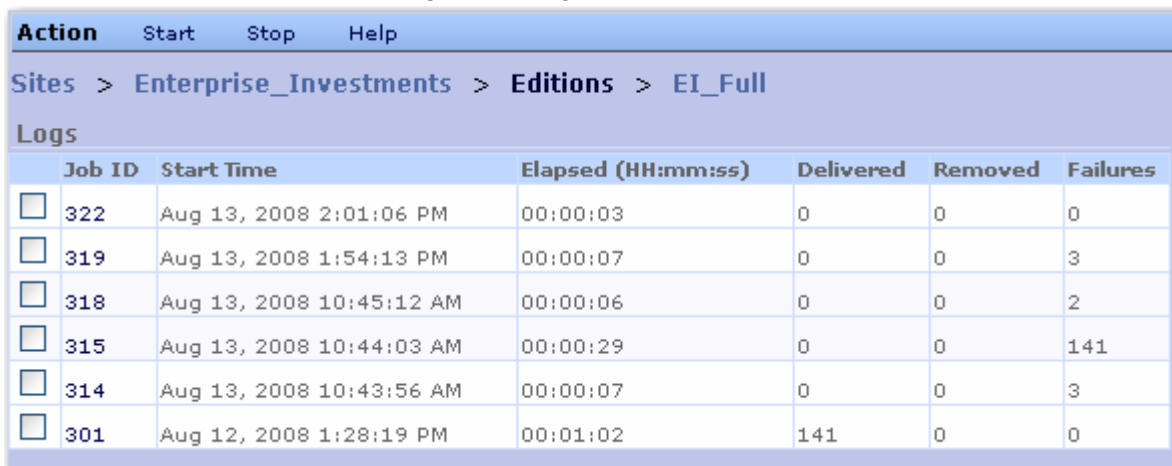
You can also cancel an Edition from the Runtime Edition dialog. If the Edition is running, the Stop menu option is enabled. Click *Stop* to cancel the Edition.

---

## Reviewing Publishing Logs

CM System maintains a log of the results of each Edition publishing job. You can access these logs in two ways:

- The Runtime Edition dialog lists all logs for the Edition.



The screenshot shows a web application interface for reviewing publishing logs. At the top, there is a navigation bar with 'Action', 'Start', 'Stop', and 'Help' buttons. Below this is a breadcrumb trail: 'Sites > Enterprise\_Investments > Editions > EI\_Full'. The main content area is titled 'Logs' and contains a table with the following columns: 'Job ID', 'Start Time', 'Elapsed (HH:mm:ss)', 'Delivered', 'Removed', and 'Failures'. The table lists six jobs with their respective start times, elapsed durations, and counts for delivered items, removed items, and failures.

Job ID	Start Time	Elapsed (HH:mm:ss)	Delivered	Removed	Failures
<input type="checkbox"/> 322	Aug 13, 2008 2:01:06 PM	00:00:03	0	0	0
<input type="checkbox"/> 319	Aug 13, 2008 1:54:13 PM	00:00:07	0	0	3
<input type="checkbox"/> 318	Aug 13, 2008 10:45:12 AM	00:00:06	0	0	2
<input type="checkbox"/> 315	Aug 13, 2008 10:44:03 AM	00:00:29	0	0	141
<input type="checkbox"/> 314	Aug 13, 2008 10:43:56 AM	00:00:07	0	0	3
<input type="checkbox"/> 301	Aug 12, 2008 1:28:19 PM	00:01:02	141	0	0

Figure 4: Runtime Edition page when not running (no status data is displayed)

- The Publishing Logs dialog lists all logs for all Editions in the Site.


Action		Help							
Publishing Logs									
Logs									
Select All   Select None									
Select	Job ID	Edition	Site	Start Time	Elapsed (HH:mm:ss)	Status	Delivered	Removed	Failures
<input type="checkbox"/>	309	EI_Full	Enterprise_Investments	Dec 2, 2008 8:11:21 AM	00:00:22	✓	141	0	0
<input type="checkbox"/>	308	EI_Incremental	Enterprise_Investments	Dec 1, 2008 6:00:00 PM	00:00:01	✓	2	0	0
<input type="checkbox"/>	307	EI_Incremental	Enterprise_Investments	Dec 1, 2008 2:00:00 PM	00:00:01	✓	2	0	0
<input type="checkbox"/>	306	EI_Incremental	Enterprise_Investments	Dec 1, 2008 1:34:49 PM	00:00:01	✓	2	0	0
<input type="checkbox"/>	305	EI_Incremental	Enterprise_Investments	Dec 1, 2008 1:30:07 PM	00:00:01	✓	2	0	0
<input type="checkbox"/>	304	EI_Incremental	Enterprise_Investments	Dec 1, 2008 1:29:39 PM	00:00:01	✓	2	0	0
<input type="checkbox"/>	303	EI_Full	Enterprise_Investments	Dec 1, 2008 1:28:45 PM	00:00:29	✓	141	0	0

Figure 5: Publishing Log

The Status column indicates the outcome of the publishing run. This column contains one of the following graphics:

Graphic	Brief description	Full Description
✓	Completed	All Content Lists were processed successfully and all Content Items were published successfully.
⚠	Completed with failures	<p>Publishing of one or more Content Items may have failed. Check the log for the run to identify the Content Items for which publishing failed to determine the causes of the failures.</p> <p>Publishing of one or more Content Lists may have failed. Check the console log (&lt;Rhythmyxroot&gt;/console.log) to determine which Content Lists failed and why.</p>
⊘	Cancelled	The Content Items were assembled and prepared for delivery but the Edition was cancelled by the user before the Content Items were delivered.



Graphic	Brief description	Full Description
	Aborted	The publishing job was aborted.

In some cases, the total number of Content Items reported in the log may not equal the total number of Content Items queued for processing. Logs results are only recorded for Content Items that have been processed by the Assembly Engine. Content Items that have been queued but not assembled will not have log results.

- The Publishing Status page lists all Editions currently running or that were run within the past hour.



Help			
Publishing Status			
Running Editions			
Edition	Behavior	Status	Progress
EI_Incremental (302)	Unpublish Then Publish	 Edition completed	

Figure 6: Publishing Status page, showing Editions currently running or run in the past hour

You can access details of each log. When you click on the log entry, CM System displays the Log View in the View and Edit pane.



Done Help						
Sites > Enterprise_Investments > Editions > EI_Full						
Job ID: 325 Start Time: Sep 3, 2008 11:12:32 AM						
Edition: EI_Full Elapsed Time: 00:00:50						
Items Tasks						
		Previous		1-25 of 141		Next 25
Content Id[Rev]	Location/Site Folder	Elapsed Time	Operation	Status	Delivery Type	Template
383[1]	/Images/Funds/EIGlobalServicesFund/item383.jpg //Sites/EnterpriseInvestments/Images/Funds/EIGlobalServicesFund	0.007s	publish	success	filesystem	B - Image
384[1]	/Images/Funds/EIGlobalServicesFund/item384.jpg //Sites/EnterpriseInvestments/Images/Funds/EIGlobalServicesFund	0.006s	publish	success	filesystem	B - Image
385[1]	/Images/Funds/EIGlobalServicesFund/item385.jpg //Sites/EnterpriseInvestments/Images/Funds/EIGlobalServicesFund	0.006s	publish	success	filesystem	B - Image
389[1]	/Images/Funds/EIGlobalHealthSciencesFund/item389.jpg //Sites/EnterpriseInvestments/Images/Funds/EIGlobalHealthSciencesFund	0.005s	publish	success	filesystem	B - Image
390[1]	/Images/Funds/EIGlobalHealthSciencesFund/item390.jpg //Sites/EnterpriseInvestments/Images/Funds/EIGlobalHealthSciencesFund	0.006s	publish	success	filesystem	B - Image

Figure 7: Publishing Job Log View

The Log View displays a list of the Content Items published with summary information about each Content Item. For details about a Content Item, double-click on the Content Item. CM System displays the Published Item Details in the View and Edit pane.



Figure 8: Published Item Detail

The Published Item Details includes publishing details for the Content Item in the Edition job. If publishing of the Content Item failed, the dialog displays an detailed error message.

## Pruning Publishing Logs

Under the default configuration, CM System automatically purges publishing logs after one month. You can manually purge or archive logs as well.

- To prune logs from the Runtime Edition page, select the logs you want to prune and
  - to delete the logs, in the Menu bar, *Action > Delete Selected Logs*;
  - to archive the logs, in the Menu bar, choose *Action > Archive Selected Logs*.
- To prune logs from the Publishing Logs page, select the logs you want to prune and
  - to delete the logs, in the Menu bar, *Action > Delete Selected Logs*;
  - to archive the logs, in the Menu bar, choose *Action > Archive Selected Logs*.

By default, archived logs are stored in the directory

<Rhythmyxroot>/AppServer/server/rx/deploy/publog.war as XML files with the name publog\_<id>.xml where <id> is the publishign job ID of the archived log; for example, publog\_109.xml.

NOTE: You can configure an alternate storage location for archived logs in the file <Rhythmyxroot>/rxconfig/server/server.properties. In Windows environments, be sure to escape the backslashes in the path. The escape character is a backslash, so the path would be C:\\Directory1\\Directory2.

---

## Republishing Failed Content

When you review the Publication log, you may find that CM System published your Edition but did not publish some Content Items. After you resolve the problems causing the publication failure of these content items, you can republish just these items to your site by publishing an incremental Edition. You do not have to republish the entire Edition.

---

## Monitoring Publication of Localized Content

Use Publishing logs to monitor the publication of localized content.

If your Publishing Model is site-centric (publishes localized content to unique sites or destinations), you will have unique Sites and Editions for each Locale. Review the log for each Edition to determine whether the content of the Edition published correctly.

If your Publishing Model is content-centric (publishes all content to a single site or destination), you use a single Edition that includes the pages for all Localized versions of your content. Check the Single Published Item details for each Content Item to see if the different versions within the Edition published correctly.

See the document *Internationalizing and Localizing CM System* for more information about localization.

If CM System publishes your Editions or Edition, but does not publish some content items, **republish the failed content** (see "Republishing Failed Content" on page 19).

## CHAPTER 3

# Maintaining Schedules

Automation of CM System processing is implemented by creating scheduled tasks in the CM System Server. CM System maintains a log of scheduled tasks as they are executed. Notification e-mails can be generated when scheduled task processing is executed.

## Scheduled Tasks

Scheduled tasks are CM System tasks that are run automatically by the server. Examples of scheduled tasks include:

- Running an Edition automatically.
- Purging logs.

Many CM System tasks can be automatically scheduled as timed events. A ScheduledTask extension must exist for the task. The standard CM System installation includes the following ScheduledTask extensions:

- `sys_purgePublishingLog`  
Purges publishing logs created more than the specified number of days in the past.
- `sys_purgeScheduledTaskLog`  
Purges Scheduled Task logs created more than the specified number of days in the past.
- `sys_runCommand`  
Runs the specified command.
- `sys_runEdition`  
Runs the specified Edition.

You can create additional custom Scheduled Tasks to meet your needs. For details, see "Scheduled Tasks" in the *CM System Technical Reference*.

The Scheduled Task List dialog lists all scheduled tasks defined in the system:

Action		Help
<b>Scheduled Tasks</b>		
	Name (id)	Cron Specification
<input type="radio"/>	<code>sys_purgePublishingLog (1)</code>	<code>0 0 0 * * ?</code>
<input type="radio"/>	<code>sys_purgeScheduledTaskLog (2)</code>	<code>0 0 1 * * ?</code>

Figure 9: Scheduled Task List

## Scheduled Task Editor

Use the Scheduled Task editor to create and maintain scheduled tasks in CM

System. To access the Scheduled Task editor:

- With the Scheduled Task List displayed, in the Menu bar, choose *Action > Create New Scheduled Task*.
- In the Scheduled Task List dialog, double-click on the timed event you want to edit.

The screenshot shows the 'Scheduled Task Editor' dialog box. At the top is a menu bar with 'Action', 'Save', 'Cancel', and 'Help'. Below the menu bar, the title bar reads 'Scheduled Tasks > sys\_purgeScheduledTaskLog'. The main area contains several fields: 'Name' (sys\_purgeScheduledTaskLog), 'Extension' (dropdown), 'Cron Specification' (0 0 1 \* \* ?), 'Server' (text box), 'Notify When' (Never dropdown), 'Notify Role' (dropdown), 'Email Addresses (',' separated)' (text area), and 'Notification Template' (dropdown).

Figure 10: Scheduled Task Editor

### Field Descriptions

**Name** Name of the schedule task configuration. Scheduled task configuration names must begin with a letter, and can contain any alphanumeric characters, underscores, hyphens, or dots (periods).

**Task** Drop List. The ScheduledTask extension to execute. Options include all ScheduledTask extensions registered in the system. For details about implementing a ScheduledTask, see "Timed Events" in the *CM System Technical Reference*. The following ScheduledTask extensions are included with CM System by default:

- `sys_PurgePublishingLog`  
This task purges the publishing log. The extension includes parameters that define how far back to preserve logs, and whether to archive logs before purging them.
- `sys_PurgeScheduledTaskLog`  
This task purges the scheduled task log. The extension includes a parameter that defines how far back to preserve logs.

- **sys\_runCommand**  
This task runs a native system command. The extension includes a parameter where you can define the command you want to run.
- **sys\_runEdition**  
This task runs an Edition. The extension includes a parameter where you can define the Edition you want to publish.

If you select a task that has parameters, an additional unnamed field is displayed where you can specify the values for the parameters. You can write a custom scheduled task extension if none of these extensions meet your needs. For details, see the *CM System Technical Reference Manual*.

**Cron specification** Set of values defining when to run the task. CM System uses the Quartz Enterprise Job Scheduler (<http://www.opensymphony.com/quartz/>). For details about writing a cron expression for Quartz, see <http://www.opensymphony.com/quartz/wikidocs/CronTriggers%20Tutorial.html>.

**Server** Name or IP address of server on which to run the task. Can be used to specify a task to run on a publishing hub. Port defaults to 9992; to specify a different port, specify the server and port as follows: server:port for example, Rhythmyx:9992. (Note: If you attempt to run a task specified for a different server, the task fails and an error will be logged. To run a task specified for another server, start a browser, connect to that server, log in to Content Explorer, go to the Admin tab, and run the task.

**Notify when** Drop list. Specifies the circumstances under which a notification should be sent out after the task is run. Options include:

- Always (Notification is always sent out after the task has run.)
- Failure (Notification is only sent out if the task fails.)
- Never (Notifications are never sent after the task has run.)

**Role to Notify** The user or Role to notify.

**CC List** List of additional recipients of any Notifications generated by this timed event.

**Notification** Drop list. The Task Notification Template to use to generate the the e-mails sent to the specified recipients.

## Creating a Scheduled Task

To create a scheduled task:

- 1 In the Rhythmyx Administration tab, click on the [ScheduledTasks](#) link.  
The View and Edit pane displays the Scheduled Tasks List.
- 2 In the Menu bar, choose *Create > Scheduled Task*.  
The View and Edit pane displays a blank scheduled task editor.
- 3 The **Name** defaults to *TimedEvent\_0*. Optionally, enter a new **Name**.
- 4 Choose the **Extension** you want to use for the scheduled task. Options include all scheduled task extensions registered in the system. The following scheduled task extensions are installed with CM System:
  - **sys\_purgePublishingLog**  
Purges publishing logs created more than the specified number of days in the past.



- `sys_purgeScheduledTaskLog`  
Purges Scheduled Task logs created more than the specified number of days in the past.
  - `sys_runCommand`  
Runs the specified command.
  - `sys_runEdition`  
Runs the specified Edition.
- 5 If the Task you chose has parameters, the editor displays fields for the parameters. Specify values for any parameters of the task.
  - 6 Enter the **Cron specification**. CM System uses the Quartz Enterprise Job Scheduler (<http://www.opensymphony.com/quartz/>). For details about writing a cron expression for Quartz, see <http://www.opensymphony.com/quartz/wikidocs/CronTriggers%20Tutorial.html>.
  - 7 All tasks run locally unless configured to run on a different server. If you want to run the task on a different server, such as a publishing hub, enter the name or IP address of that server in the **Server** field. (Note; the port defaults to 9992. If the server uses a different port, specify both the server and port as follows: `server:port`; for example, *Rhythmyx:9992*.)
  - 8 In the **Notify when** drop list, specify the circumstances under which a notification e-mail should be sent to the specified recipients. Options include *Always*, *On Failure*, and *Never*.
  - 9 If you choose *Always* or *On Failure* in the **Notify When** drop list:
    - a) You must specify a **Notify Role**. Choose the Role you want to notify from the drop list. Options include all Roles defined in the system.
    - b) You can also specify additional **Email Addresses** to receive notifications. Use commas to separate e-mail addresses.
    - c) You must also specify the **Notification Template** to use to generate notification e-mail messages. Options include all task notifications defined in the system.
  - 10 Click the [**Save**] button to save the scheduled task.

You can test your scheduled task by running it manually. To run a scheduled task manually, in the Menu bar, choose *Action > Run Now*. (Note: If you configured the task to run on a different server, you must run the task from that server. Running a task from a server other than the server for which it is configured results in an error. Start a browser and connect to the remote server, log in to Content Explorer, go to the Admin tab, and run the task)

## Modifying a Scheduled Task

To modify a scheduled task:

- 1 In the Rhythmyx Administration tab, click the [ScheduledTask](#) link  
The View and Edit tab displays the Scheduled Task List.
- 2 Double-click on the scheduled task you want to modify.

The View and Edit tab displays the scheduled task editor with the current data for the scheduled task you accessed.

- 3 You can change the value in any field. For details about writing a cron expression, see <http://www.opensymphony.com/quartz/wikidocs/CronTriggers%20Tutorial.html> (<http://www.opensymphony.com/quartz/wikidocs/CronTriggers%20Tutorial.html>).
- 4 Click the [Save] button to save your changes.

## Copying a Scheduled Task

A quick way to create a new scheduled task is to copy an existing scheduled task that closely matches the scheduled task you want to create and modify the data in the copy.

To copy a scheduled task:

- 1 In the Rhythmyx Administration tab, click the [ScheduledTask](#) link.  
The View and Edit pane displays the scheduled task list.  
In the scheduled task list, select the radio button in the row of the scheduled task you want to copy.
- 2 In the menu bar, choose *Action > Copy*.
- 3 CM System copies the scheduled task and displays the copy in the View and Edit pane. The Name of the copied scheduled task is Copy\_of\_<original scheduled task name>. All other data is copied directly from the original scheduled task.
- 4 You can change the value in any field. For details about writing a cron expression, see <http://www.opensymphony.com/quartz/wikidocs/CronTriggers%20Tutorial.html> (<http://www.opensymphony.com/quartz/wikidocs/CronTriggers%20Tutorial.html>).
- 5 Click the [Save] button to save your changes.

## Timed Event Logs

The scheduled task log lists scheduled tasks that have run, from most recent to oldest.

To access the scheduled task log, in the Rhythmyx Administration tab, click on the scheduled task Log link.



The screenshot shows a web interface for the 'Task Log'. At the top, there is a menu bar with 'Action' and 'Help' options. Below the menu bar is the title 'Task Log'. The main content is a table with the following columns: 'Task Name', 'Start Time', 'Elapsed (HH:mm:ss)', and 'Status'. Each row in the table has a small square icon to its left. The table contains seven rows of data.

Task Name	Start Time	Elapsed (HH:mm:ss)	Status
sys_purgeScheduledTaskLog	Dec 2, 2008 1:00:00 AM	00:00:00	Failed
sys_purgePublishingLog	Dec 2, 2008 12:00:00 AM	00:00:00	Failed
EI_Incremental	Dec 1, 2008 6:00:00 PM	00:00:01	Success
EI_Incremental	Dec 1, 2008 2:00:00 PM	00:00:01	Success
EI_Incremental	Dec 1, 2008 1:34:49 PM	00:00:01	Success
EI_Incremental	Dec 1, 2008 1:30:07 PM	00:00:01	Success
EI_Incremental	Dec 1, 2008 1:27:32 PM	00:00:02	Failed

Figure 11: Scheduled Task Log

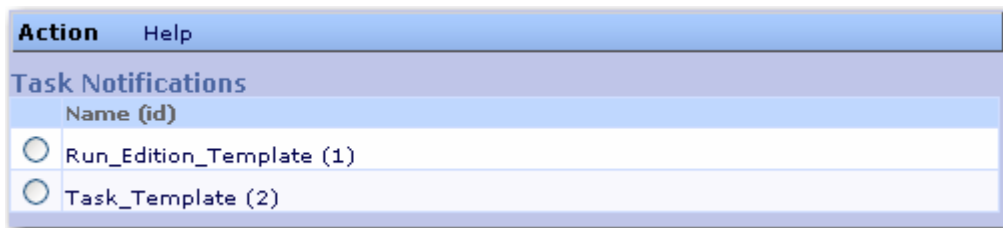
Scheduled task logs can be purged. Purging removes all scheduled task logs. To purge the scheduled task log, in the Menu bar, choose *Action > Purge Logs*.

## Task Notifications

A task notification is a template used to generate e-mails automatically sent by the scheduled task engine. The scheduled task specifies which notification to send, the events that trigger sending an e-mail, and the recipients of the message.

Scheduled tasks extensions may define binding variables that can be used to include task data in notification e-mails generated by scheduled tasks that use that extension. The variable *\$execution\_datetime* is available for all Scheduled Tasks. Other variables are defined by the Scheduled Task extension.

The Task Notification List lists all scheduled task notification defined in the system.



Action Help	
<b>Task Notifications</b>	
Name (id)	
<input type="radio"/>	Run_Edition_Template (1)
<input type="radio"/>	Task_Template (2)

*Figure 12: Task Notification List*

## Task Notification Editor

Use the Task Notification editor to define notification templates.

To access the Task Notification editor:

- On the Rhythmyx Administration tab, click on the Task Notification link, then in the Menu bar, choose *Action > Create Task Notification*.
- On the Task Notification List, double-click on the Task Notification you want to edit.

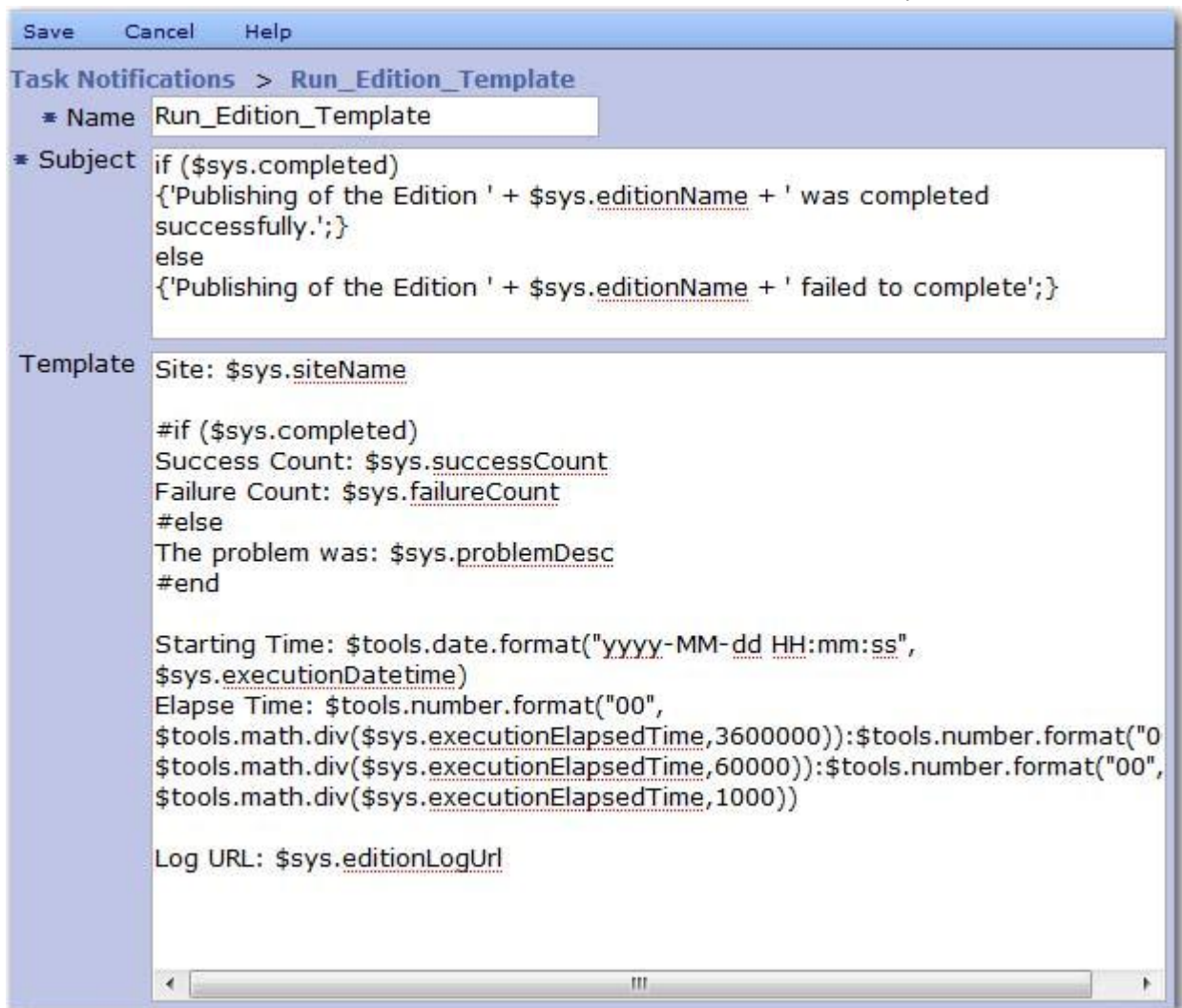


Figure 13: Task Notification Editor

### Field Descriptions

**Name** Name of the notification.

**Subject** The text of the subject line of the notification e-mail message as a JEXL expression.

**Template** Text of the notification e-mail message as a Velocity template.

Since the content of both the Subject and Template fields can use JEXL (JEXL is included in Velocity), binding variables can be included using the standard syntax *\$variablename*. The specific variables available are defined by the Scheduled Task extension. For details about the variables available for the Scheduled Task extensions that ship with CM System, see *Default Task Notification Variables* (on page 31).

- *sys\_runCommand* (see page 33)
- *sys\_runEdition* (see page 33)
- *sys\_purgePublishingLog* (see page 32)
- *sys\_purgeTaskLog* (see page 32)

The variable `$execution_datetime` is available for all scheduled tasks.

## Creating a Scheduled Task Notification

To create a scheduled task notification:

- 1 On the Rhythmyx Administration tab, click the [TaskNotifications](#) link.  
The View and Edit pane displays the Task Notifications List.
- 2 In the Menu bar, choose *Create > Task Notification*.  
The View and Edit pane displays a blank Task Notification editor.
- 3 The **Name** defaults to *Notification\_0*. Optionally, change the **Name**.
- 4 The **Subject** defaults to *'Set a new subject'*. Enter the code to generate the subject line for the notification e-mail message.
- 5 Enter the code to generate the text of the message in the **Template** field.

This value of the **Subject** and **Template** fields is a Velocity template, which means it can include HTML markup and binding variables. Use the format *\$variable\_name* to include a binding variable in the template. For all scheduled task extensions, the binding variable *\$execution\_datetime* is available. A scheduled task extension may return additional binding variables. For example, the *sys\_runEdition* Scheduled Task returns the following binding variables:

- `$edition_name`
- `$site_name`
- `$failure_count`
- `$edition_log_url`
- `$success_count`

Two example scheduled task notifications, *Run\_Edition\_Template* and *Task\_Template* are included when you install CM System. Use these as models to design the code for your own notifications.

- 6 Click the **[Save]** button to save the notification.

## Modifying a Timed Event

To modify a scheduled task notification:

- 1 In the Rhythmyx Administration tab, click the [TaskNotification](#) link.  
The View and Edit pane displays the task notification list.
- 2 Double-click on the task notification you want to modify.  
The View and Edit pane displays the notification you selected.
- 3 You can change the value in any field.
- 4 Click the [Save] button to save your changes.

## Deleting a Scheduled Task Notification

If you delete a notification, no e-mails will be generated by scheduled tasks that use that notification. No error will be returned to inform you that generation of an e-mail failed.

To delete a scheduled task notification:

- 1 In the Rhythmyx Administration tab, click the [TaskNotification](#) link.  
The View and Edit pane displays the task notification list.
- 2 Select the task notification you want to delete.
- 3 In the Menu bar, choose *Edit > Delete Selected Task Notification*.  
The notification you selected is deleted. The task notification list is refreshed to show the available notifications.

## Default Task Notification Variables

The Task Notification Variables available for each extension are defined by that extension. The following extensions are shipped with CM System:

- *sys\_runCommand* (on page 33)
- *sys\_runEdition* (on page 33)
- *sys\_purgePublishingLog* (on page 32)
- *sys\_purgeTaskLog* (on page 32)

The variable `$sys_executionDateTime` is available for all scheduled task extensions. All Velocity tool utilities available in CM System (as defined by `<Rhythmyxroot>/AppServer/server/rx/deploy/rxapp.ear/rxapp.war/WEB-INF/config/velocity/tools.xml`) are also available for use in task notifications.

## sys\_purgePublishingLog

This Scheduled Task extension purges publishing log entries created more than a specified number of days in the past. The following Task Notification variables are available from this extension:

Variable Name	Type	Description
\$numberOfDays	String	Number of days in the past to preserve logs. Logs older than the specified number of days will be purged,
\$enableArchive	Boolean	True if purged logs are archived. The default archive location is <Rhythmyxroot>/AppServer/server/rx/deploy/publogs.war. The archive file is named "publog_ID.XML" where "ID" is the ID of the archived log.
\$tools.		Velocity tools utilities available in CM System. Available utilities are defined in the file <Rhythmyxroot>/AppServer/server/rx/deploy/rxapp.ear/rxapp.war/WEB-INF/config/velocity/tools.xml
\$sys.taskName	String	The name of the task.
\$sys.completed	Booelan	True if job processing was completed; otherwise false.
\$sys.problemDesc	String	If processing was not completed, the description of the problem that caused the failure.
\$sys.executionDateTime	String	Starting date and time of processing of the extension.
\$sys.executionElapsedTime	Long	The duration of the execution in milliseconds.

## sys\_purgeTaskLog

This Scheduled Task extension purges Scheduled Task log entries created more than a specified number of days in the past. The following Task Notification variables are available from this extension:

Variable Name	Type	Description
\$numberOfDays	String	Number of days in the past to preserve logs. Logs older than the specified number of days will be purged,
\$tools.		Velocity tools utilities available in CM System. Available utilities are defined in the file <Rhythmyxroot>/AppServer/server/rx/deploy/rxapp.ear/rxapp.war/WEB-INF/config/velocity/tools.xml
\$sys.taskName	String	The name of the task.
\$sys.completed	Booelan	True if job processing was completed; otherwise false.
\$sys.problemDesc	String	If processing was not completed, the description of the problem that caused the failure.
\$sys.executionDateTime	String	Starting date and time of processing of the extension.
\$sys.executionElapsedTime	Long	The duration of the execution in milliseconds.



## sys\_runCommand

This Scheduled Task extension runs a server command. The following Task Notification variables are available from this extension:

Variable Name	Type	Description
\$command	String	The server command specified in the command parameter of the extension.
\$tools.		Velocity tools utilities available in CM System. Available utilities are defined in the file <Rhythmyxroot>/AppServer/server/rx/deploy/rxapp.ear/rxapp.war/WEB-INF/config/velocity/tools.xml
\$sys.taskName	String	The name of the task.
\$sys.completed	Booelan	True if job processing was completed; otherwise false.
\$sys.problemDesc	String	If processing was not completed, the description of the problem that cased the failure.
\$sys.executionDateTime	String	Starting date and time of processing of the extension.
\$sys.executionElapsedTime	Long	The duration of the execution in milliseconds.

## sys\_runEdition

This Scheduled Task extension publishes an Edition. The following Task Notification variables are available from this extension:

Variable Name	Type	Description
\$editionName	String	Edition name, as defined by the editionName parameter of the extension.
\$tools.		Velocity tools utilities available in CM System. Available utilities are defined in the file <Rhythmyxroot>/AppServer/server/rx/deploy/rxapp.ear/rxapp.war/WEB-INF/config/velocity/tools.xml
\$sys.taskName	String	The name of the task.
\$sys.completed	Booelan	True if job processing was completed; otherwise false.
\$sys.problemDesc	String	If processing was not completed, the description of the problem that cased the failure.
\$sys.editionName	String	Name of the published Edition.
\$sys.siteName	String	Name of the published Site.
\$sys.editionLogUrl	String	URL that can be used to view the Edition log.
\$sys.failureCount	String	Number of Content Items for which publishing failed.
\$sys.successCount	String	Number of Content Items for which publishing succeeded.
\$sys.executionDateTime	String	Starting date and time of processing of the extension.

Variable Name	Type	Description
\$sys.executionElapsedTime	Long	The duration of the execution in milliseconds.

## Example Task Notifications

Two example task notifications are installed with CM System:

- *Run\_Edition\_Template* (on page 34)
- *Task\_Template* (on page 37)

### Run\_Edition\_Template

The Run\_Edition\_Template provides a generic notification template for a notification that is very commonly desired in CM System: the results of running an Edition. This template generates an e-mail message that reports:

- the result of the run;
  - if the run completed successfully, how many individual Content Items were published successfully and how many individual Content Items failed to publish;
  - if the run failed, the cause of the failure
- the Site to which the Edition was published;
- the time publishing was initiated;
- the elapsed processing time; and
- the URL of the log of the Edition publishing run.

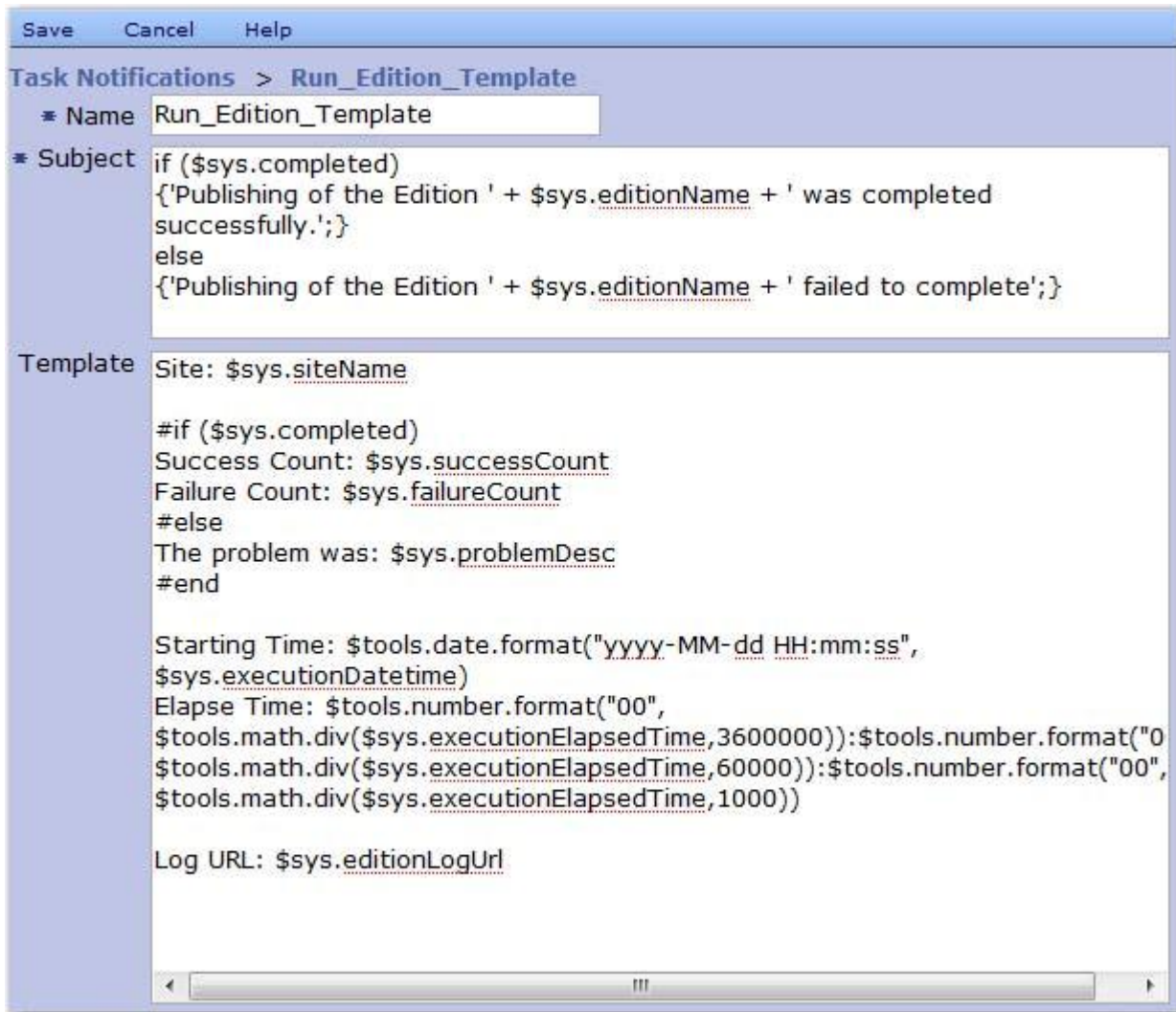


Figure 14: Task Notification Editor

The code in the **Subject** field generates text similar to one of the following

Publishing of the Edition <EditionName> was completed successfully.

This text is generated if processing of the Edition was successful. The text <EditionName> will be replaced with the name of the Edition that was processed.

Publishing of the Edition <EditionName> failed to complete.

This text is generated if processing of the Edition failed. The text <EditionName> will be replaced with the name of the Edition that was processed.

The code in the **Template** field first tells the recipient the Site to which the Edition was published.

Site: \$sys.siteName

Next, the message provides details regarding the success or failure of the publishing run. If the run was successful, the number of successful and failed Content Items is listed.

```
#if ($sys.completed)
Success Count: $sys.successCount
Failure Count: $sys.failureCount
```

If the run failed, a description of the failure is included:

```
#else
The problem was: $sys.problemDesc
```

Following that, the e-mail notes the time that the Edition was launched and the elapsed time to run it:

```
Starting Time: $tools.date.format("yyyy-MM-dd HH:mm:ss",
$sys.executionDatetime)
Elapse Time: $tools.number.format("00",
$tools.math.div($sys.executionElapsedTime,3600000)):$tools.number.format
("00",
$tools.math.div($sys.executionElapsedTime,60000)):$tools.number.format("
00", $tools.math.div($sys.executionElapsedTime,1000))
```

The value of the `$sys.execution.ElapsedTime` is the amount of time, in milliseconds, to complete processing of the Edition. Dividing by 3600000 yields the number of hours for the processing, dividing by 60000 yields the number of minutes, and dividing by 1000 yields the number of seconds. Functions from the JEXL toolkit are used to calculate these values.

Finally, the URL of the job log is included:

```
Log URL: $sys.editionLogUrl
```

## Task\_Template

The Task\_Template is a generic notification to inform the recipient about the results of a scheduled task. This template generates an e-mail that reports:

- the result of the run, and, if unsuccessful, the cause of the failure; and
- the starting time of the task and the elapsed time of the processing.

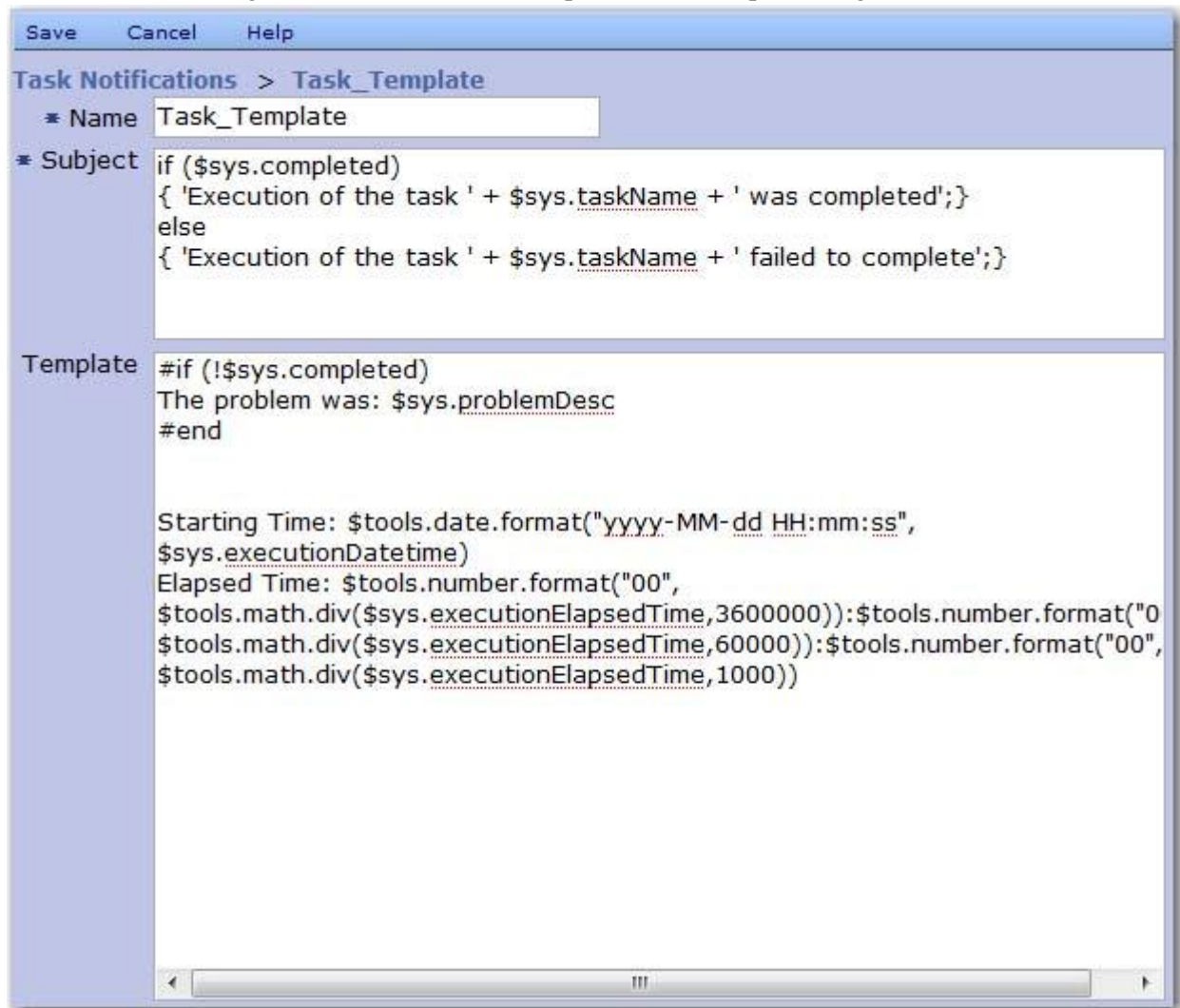


Figure 15: Task\_Template

The code in the **Subject** field generates text similar to one of the following

Execution of the task <TaskName> was completed.

This text is generated if CM System was able to execute the scheduled task. The text <TaskName> will be replaced with the name of the scheduled task that was initiated.

Execution of the task <TaskName> failed to complete.

This text is generated if CM System was not able to execute the scheduled task. The text <TaskName> will be replaced with the name of the scheduled task that was initiated.

The code in the **Template** field, if the scheduled task could not be executed, a description of the problem is included.

Following that, the e-mail notes the time that the Edition was launched and the elapsed time to run it:

```
Starting Time: $tools.date.format("yyyy-MM-dd HH:mm:ss",
$sys.executionDatetime)
Elapse Time: $tools.number.format("00",
$tools.math.div($sys.executionElapsedTime,3600000)):$tools.number.format
("00",
$tools.math.div($sys.executionElapsedTime,60000)):$tools.number.format("
00", $tools.math.div($sys.executionElapsedTime,1000))
```

The value of the `$sys.execution.ElapsedTime` is the amount of time, in milliseconds, to complete processing of the Edition. Dividing by 3600000 yields the number of hours for the processing, dividing by 60000 yields the number of minutes, and dividing by 1000 yields the number of seconds. Functions from the JEXL toolkit are used to calculate these values.

## CHAPTER 4

# Maintaining the CM System Server

Many of the remaining sections of the *Administration Manual* refer you to server maintenance tasks that are completed using the CM System Server Administrator, the CM System interface that the system administrator uses to maintain the CM System Server. To open the Server Administrator::

- In the CM System root, double-click `RhythmyxServerAdministrator.exe`.
- In Windows, access *Start > All Programs > Percussion Rhythmyx > Rhythmyx Server Administrator*.
- In Windows, open the command line interface. Change the command line directory to your Rhythmyx directory. Enter `rhythmyxserveradministrator`.
- In Windows, access *Start > Run*. Browse to the Rhythmyx root directory and double-click `RhythmyxServerAdministrator.exe`.

In each case, you are prompted to enter your password. After you click [**Login**], the Server Administrator opens:

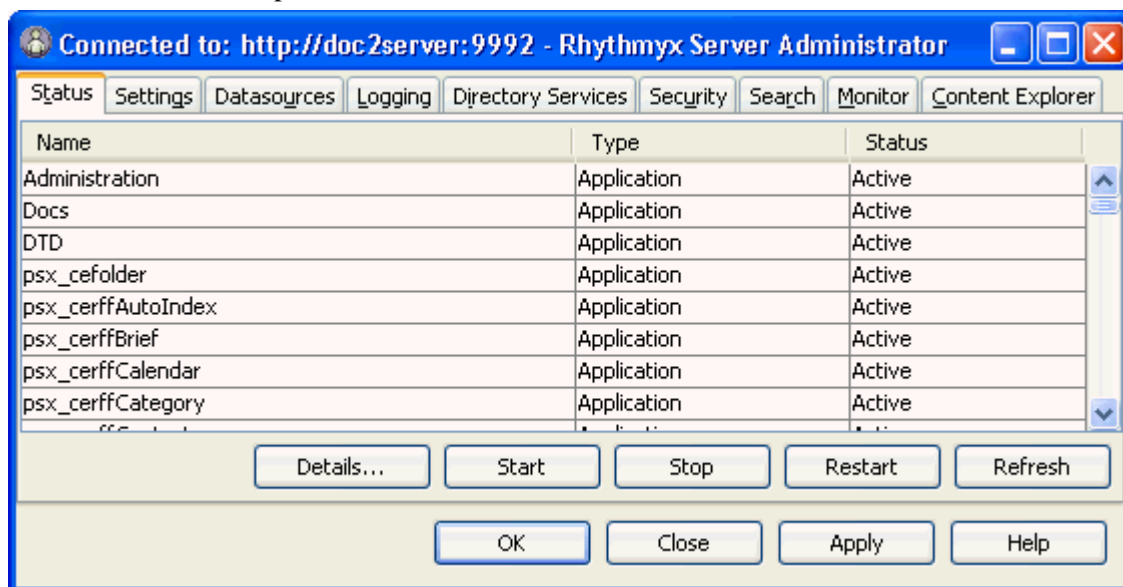


Figure 16: Status Tab

The Server Administrator separates administration tasks into nine categories displayed by its upper tabs. The tabs enable an administrator to do the following:

**Status** - Stop and start CM System applications and monitor their statistics. For more information about using the Status tab, see the Server Administrator help.

**Settings** - Optimize CM System's performance by specifying idle time limits and maximum connections. In addition, this tab lets the administrator enable or disable the server cache and set its size. For more information about using the Settings tab, see the Server Administrator help.

**Datasources** - Maintain the data CM System uses to connect to an RDBMS and to a specific database or schema in the RDBMS. The administrator can maintain database driver definitions, JNDI datasource configurations, and specify the database or schema to which CM System can connect. For more information about using the Datasources tab, see the Server Administrator help.

**Logging** - Set the types of events to log, specify how long to save log files, and query log records for information. For more information about using the Logging tab, see the Server Administrator help.

**Directory Services** - Register Directory Services, add authentication information for users connecting to a Directory Service, and provide other data necessary for connecting to and using Directory Services. For more information about using the Directory Services tab, see *Using Directory Services* (see page 87).

**Security** - Set up most of CM System's security features. For more information about using the Security tab, see *Maintaining Users* (see page 71). For complete information about this tab, see the Server Administrator help.

**Search** - Enable and disable the full-text search, change the default index directory and override the default indexing interfaces. For more information about using the Search tab, see *Search Configuration* (see page 155).

**Monitor** - Remotely enter Server commands and view the CM System Server responses on a console. For more information about using the Monitor tab, see *Issuing Commands to the CM System Server* (see page 48).

**Content Explorer** - Configure which Java Plugin Content Explorer uses and its download location, and choose when to refresh the Content Explorer screen. For more information about using the Content Explorer tab, see the Server Administrator help.



## CHAPTER 5

# Operating the CM System Server

This chapter describes:

- how to start and stop the CM System server in the following environments:
  - **Windows** (see "Operating the CM System Server in a Windows Environment" on page 42)
  - **Solaris and Linux** (see "Operating the CM System Server in a Unix Environment" on page 44)
- **troubleshooting recommendations when the CM System server fails to start** (see "Troubleshooting Server Initialization" on page 46);
- **issuing commands to the CM System server** (see page 48);
- implementation and operational **tasks that require restart of the CM System server** (see page 70).

---

# Operating the CM System Server in a Windows Environment

The CM System server can run as a Windows service or as an application. The installation sets up the CM System service to start automatically when you start Windows. Run the server as a service in production environments. Run it as an application in development and test environments.

## Starting CM System Server as a Windows Service

To start the CM System server as a Windows service

- 1 Access the Windows Services dialog. (The procedure for accessing this dialog differs depending on the version of Windows you are running. Consult the Windows Help on your installation for the procedure to access this dialog.)
- 2 Select the CM System Server service.
- 3 Right-click and from the popup menu choose *Start*.
- 4 Alternately, you can double-click on the service to display the service properties dialog for the service. Click the [**Start**] button to start the service.

## Starting CM System Server as an Application

Run CM System server as an application in development and test environments. Running CM System server as an application in production environments is not recommended.

To start CM System server as an application:

- 1 Browse to your Rhythmyx\bin folder.
- 2 Double-click the RhythmyxServer icon.

Windows will start CM System server as an application.

When starting CM System server as an application, you may get the message that authentication failed because the user does not have a required privilege. In this case, you need to modify the user's rights so they can act as part of the operating system. Consult the Help for your version of Windows for details about assigning user rights to act as part of the operating system.

## Changing CM System Server Service Settings

When the CM System installation application creates the CM System service, it defines the following settings by default:

- Start automatically when Windows starts.
- Allow service to interact with the desktop. This setting displays the service as a DOS window on the desktop.

Use the service properties dialog to change these settings. The procedure to access this dialog differs for different versions of Windows; consult the Help for your version for the correct procedure.

- To change the Startup Type, click the radio button for the start up type you prefer. Options include Automatic (starts the service automatically when you start Windows), Manual (users must manually start the service), or Disabled (disables the service so it can no longer run).
- To stop displaying the service in a DOS window, uncheck Allow Service to Interact with Desktop. (NOTE: You will have to stop and restart the server for this option to take effect.)

## Using a Command to Stop CM System Server

To stop the CM System server, *access the admin JSP page* (see page 48) and enter the command *quit*.

## Stopping CM System Server from the Services Dialog

If you do not display CM System server in a DOS window, you will have to stop the CM System server from the Services dialog. You can also use this method if the server is displayed in a DOS window.

To stop the CM System server from the services dialog:

- 1 Access the Windows Services dialog. (The procedure for accessing this dialog differs depending on the version of Windows you are running. Consult the Windows Help on your installation for the procedure to access this dialog.)
- 2 Select the Rhythmyx Server service.
- 3 Right-click and from the popup menu choose *Stop*.
- 4 Alternately, you can double-click on the service to display the service properties dialog for the service. Click the [**Stop**] button to start the service.

---

## Operating the CM System Server in a Unix Environment

Operating CM System in a Unix environment requires a user to install and run CM System. You must create a unique run user for each instance of the CM System server that you operate.

When you install CM System, the installer creates the file `rx_user.id`. This file has three entries,

```
SYSTEM_USER_ID=  
RHYTHMYX_USER_ID=admin1  
RHYTHMYX_USER_PWD=demo
```

The value of `SYSTEM_USER_ID` is set during installation. Do not change this value.

The values of `RHYTHMYX_USER_ID` and `RHYTHMYX_USER_PWD` define the user that can shut down the CM System server. CM System uses this user as part of the shut-down process. If you change the password of the `admin1` user, you will need to modify the value of the `RHYTHMYX_USER_PWD` to match the new password. If you delete the `admin1` user, you must enter a valid CM System username and password. Note that this is a user within the CM System system, not the CM System user for Unix, and this user must be in a Role that has Administrative access to the server ACL.

Other than these modifications, do not modify this file. In particular, do not change the permissions on the file.

The post-installation process determines whether CM System runs as a daemon or as a console. If you choose to install CM System as a daemon, the `InstallDaemon.sh` application creates `S15RhythmyxD` and `K15RhythmyxD` files in the `/etc/rc2.d` directory. The daemon thus starts automatically when you start your system. The daemon is controlled by a script located in `/etc/rc2.d`.

## Starting CM System Server as a Daemon in a Unix Environment

The CM System server daemon starts automatically when you start your system. If you need to restart the daemon after shutting it down, change to the `Rhythmyx bin` directory and enter the following:

```
./RhythmyxDaemon start <Rhythmyx root directory>
```

When you press <Enter>, the Rhythmyx server will start as a daemon.

## Starting the CM System Server as a Terminal Window in a Unix Environment

If you install CM System server as a console, you must start the server manually. Change to the `Rhythmyx bin` directory and enter `sh StartServer.sh`. When you press <Enter>, CM System will start as a console.

## Stopping CM System Server in Unix Environment When Running as a Daemon

To stop CM System server when running as a daemon, change to the Rhythmyx bin directory and enter the following:

```
./RhythmyxDaemon stop <Rhythmyx root directory>
```

When you press <Enter>, the Rhythmyx server will shut down.

## Stopping CM System Server in a Unix Environment When Running as a Terminal Window

To stop CM System server when running as a console, change to the Rhythmyx bin directory and enter the following:

```
./Sh StopServer.sh
```

When you press <Enter>, CM System server will shut down.

## Uninstalling the CM System Daemon Control Scripts

To uninstall all instances of the CM System daemon control scripts (for all instances of CM System), execute the following commands as the root user:

```
# rm /etc/init.d/RhythmyxD
# rm /etc/rc2.d/?15RhythmyxD
```

These commands remove the following files:

```
/etc/init.d/RhythmyxD
/etc/rc2.d/S15RhythmyxD
/etc/rc2.d/K15RhythmyxD
```

To remove a single instance from the daemon control scripts, remove the desired installation directories from the `SERVER_DIR` variable in the daemon control script `/etc/init.d/RhythmyxD`. The installation directories are colon (:) delimited. For example:

```
SERVER_DIR=/export/home/RxUser1/Rhythmyx:/export/home/RxUser2/Rhythmyx
```

---

# Troubleshooting Server Initialization

When the CM System server encounters an error during the initialization process, it shuts down immediately. The server log (<Rhythmyxroot>/AppServer/server/rx/logs/server.log) will include details about the error that caused the shutdown.

The CM System server runs as a servlet within the JBoss Web application server. In some cases, problems in server initialization and operation may be issues in JBoss rather than in CM System. For JBoss operation and maintenance, see the JBoss documentation at [www.jboss.org](http://www.jboss.org) (<http://www.jboss.org>).

## Common Server Initialization Errors

Common errors during server initialization include:

### Expired License

The server fails on startup with the following error message in the log:

```
The evaluation period for this license has expired.
```

This error indicates that your license for CM System has expired and you will need a new license. Contact Percussion Technical Support for a new license and for instructions about updating your installation.

### Database Connectivity Problems

The server fails on startup with a long stack trace in the log. The initial error may be one of the following:

```
2007-02-08 10:49:55,963 WARN
[org.jboss.resource.connectionmanager.JBossManagedConnectionPool]
Throwable while attempting to get a new connection: null
org.jboss.resource.JBossResourceException: Could not create connection;
- nested throwable: (java.sql.SQLException: Network error IOException:
Connection refused: connect)
```

This error indicates that you have a problem connecting to the database server. Either the server is down or you do not have network connectivity to the server. Confirm that the server is running and that the machine on which the CM System server resides can communicate with the machine on which the database server resides.

```
2007-02-08 11:16:43,597 WARN
[org.jboss.resource.connectionmanager.JBossManagedConnectionPool]
Throwable while attempting to get a new connection: null
org.jboss.resource.JBossResourceException: Could not create connection;
- nested throwable: (java.sql.SQLException: Unknown server host name
'RxAlt'.)
```

This error indicates that the datasource used to connect to the CM System server is misconfigured. In this specific case, the database server does not exist. This error commonly occurs when a CM System tree has been moved to a different machine

Other possible errors include incorrect login user names or passwords. The `java.sql.SQLException` should specify the error.

### **Port Conflicts**

The server starts but with a stack trace at the end of startup. The stack trace starts with the following error:

```
13:24:05,415 ERROR [Http11Protocol] Error starting endpoint
java.net.BindException: Address already in use: JVM_Bind:9662
```

This error indicates that you have a port conflict. The port CM System is trying to use is already in use. This often happens when you are restarting the CM System server when the original CM System server session did not completely terminate and is holding on to the port. Check whether the CM System process is still running. If so, terminate the process. Also, confirm that you do not have two CM System server installations on the same machine using the same port.

---

## Issuing Commands to the CM System Server

Two interfaces are available for issuing commands to the CM System server:

- administration JSP page

The administration JSP page is an HTML interface that provides the capability to issue commands to the CM System server. To access the administration JSP page, open a browser and in the Address field, enter the URL of the administration page:

`http://localhost:9992/Rhythmyx/admin/console.jsp`

where

`localhost` is the name or IP address of the machine where the CM System server resides; and

`9992` is the CM System port.

All server commands are valid using this interface.

- Rhythmyx Server Administrator

Use the Monitor tab of the Server Administrator to issue commands to the Rhythmyx server. Enter the **Command** and click the [**Execute**] button. The results are displayed in the **Command Output** field. (NOTE: The quit command is not valid using this interface.)

In both cases, the results are displayed in HTML format.

---

NOTE: In CM System Version 5.7 and earlier, commands could be issued directly to the server in the server terminal window. This functionality is not available in CM System Version 6.0 and later.

---

## Server Console Commands by Function

This section organizes server commands by function:

- *general server commands* (see "General Server Console Commands" on page 48)
- *server commands for CM System applications* (see "Server Console Commands for Applications" on page 52)
- *server commands for displaying resources* (see "Server Console Commands for Displaying Resources" on page 56)
- *server commands for flushing caches* (see "Server Console Commands for Flushing the Server and MetaData Caches" on page 58)
- *server commands for search* (see "Server Console Commands for Search" on page 63)

### General Server Console Commands

To . . .	Enter the command . . .	Notes and Examples
Empty the log queue	<code>log flush</code>	Forces the server to write all pending log messages in the log queue to the log database immediately.



To . . .	Enter the command . . .	Notes and Examples
Display server log on the console.	log dump	This command may dump a very large amount of data onto the console.
Display the server version	show version	Displays version and build of CM System. Example: <pre>show version &lt;?xml version='1.0' encoding='UTF-8'?&gt; &lt;PSXConsoleCommandResults&gt;   &lt;command&gt;show version &lt;/command&gt;   &lt;resultCode&gt;0&lt;/resultCode&gt;   &lt;resultText&gt;Release 4.5 Build 20020829 (1311)&lt;/resultText&gt; &lt;/PSXConsoleCommandResults&gt;</pre>

To . . .	Enter the command . . .	Notes and Examples
Display statistics for server handling of all requests	show status server	<p>Displays how long the server has been running, the number of events processed, failed, and pending, the number of hits and misses to the cache, and average, minimum and maximum processing time for events.</p> <p>Example:</p> <pre>show status server  &lt;?xml version='1.0' encoding='UTF-8'?&gt; &lt;PSXConsoleCommandResults&gt;   &lt;command&gt;show status server&lt;/command&gt;   &lt;resultCode&gt;0&lt;/resultCode&gt;   &lt;resultText&gt;&lt;/resultText&gt; &lt;/PSXStatistics/&gt; &lt;ElapsedTime&gt;   &lt;days&gt;0&lt;/days&gt;   &lt;hours&gt;1&lt;/hours&gt;   &lt;minutes&gt;15&lt;/minutes&gt;   &lt;seconds&gt;4&lt;/seconds&gt; &lt;milliseconds&gt;26&lt;/milliseconds&gt; &lt;/ElapsedTime&gt; &lt;Counters&gt;   .   .   . &lt;/PSXConsoleCommandResults&gt;</pre>

To . . .	Enter the command . . .	Notes and Examples
Display statistics for server handling of requests by Workbench and Server Administrator	show status objectstore	<p>Displays how long the server has been running, the number of Workbench and Server Administrator events processed, failed, and pending, the number of hits and misses by such events to the cache, and average, minimum and maximum processing time for these events.</p> <p>Example:</p> <pre>show status objectstore</pre> <pre>&lt;?xml version='1.0' encoding='UTF-8'?'&gt;</pre> <pre>&lt;PSXConsoleCommandResults&gt;</pre> <pre>  &lt;command&gt;show status</pre> <pre>objectstore&lt;/command&gt;</pre> <pre>  &lt;resultCode&gt;0&lt;/resultCode&gt;</pre> <pre>  &lt;resultText&gt;&lt;/resultText&gt;</pre> <pre>  &lt;PSXStatistics/&gt;</pre> <pre>  &lt;ElapsedTime&gt;</pre> <pre>    &lt;days&gt;0&lt;/days&gt;</pre> <pre>    &lt;hours&gt;1&lt;/hours&gt;</pre> <pre>    &lt;minutes&gt;19&lt;/minutes&gt;</pre> <pre>    &lt;seconds&gt;49&lt;/seconds&gt;</pre> <pre>  &lt;milliseconds&gt;116&lt;/milliseconds&gt;</pre> <pre>  &lt;/ElapsedTime&gt;</pre> <pre>  &lt;Counters&gt;</pre> <pre>    .</pre> <pre>    .</pre> <pre>    .</pre> <pre>&lt;/PSXConsoleCommandResults&gt;</pre>
Stop the server	stop server	

## Server Console Commands for Applications

To ...	Enter the command ...	Notes
Display a list of active server applications	show applications active	<p>Example:</p> <pre>show applications active &lt;?xml version='1.0' encoding='UTF-8'?&gt; &lt;PSXConsoleCommandResults&gt;   &lt;command&gt;show applications&lt;/command&gt;   &lt;resultCode&gt;0&lt;/resultCode&gt;   &lt;resultText&gt;&lt;/resultText&gt;   &lt;Applications&gt;     &lt;Application id="18" active="yes" enabled="yes"&gt;       &lt;name&gt;casArticle&lt;/name&gt;     &lt;/Application&gt;     &lt;Application id="531" active="yes" enabled="yes"&gt;       &lt;name&gt;casArticleWord&lt;/name&gt;       .       .       .   &lt;/Applications&gt; &lt;/PSXConsoleCommandResults&gt;</pre>

To ...	Enter the command ...	Notes
Display a list of all server applications	show applications	<p>Examples:</p> <pre>show applications &lt;?xml version='1.0' encoding='UTF-8'?&gt; &lt;PSXConsoleCommandResults&gt;   &lt;command&gt;show applications&lt;/command&gt;   &lt;resultCode&gt;0&lt;/resultCode&gt;   &lt;resultText&gt;&lt;/resultText&gt;   &lt;Applications&gt;     &lt;Application id="18" active="yes" enabled="yes"&gt; &lt;name&gt;casArticle&lt;/name&gt;     &lt;/Application&gt;     &lt;Application id="531" active="yes" enabled="yes"&gt; &lt;name&gt;casArticleWord&lt;/name&gt;     .     .     .   &lt;/Applications&gt; &lt;/PSXConsoleCommandResults&gt;</pre>

To ...	Enter the command ...	Notes
Display statistics for server handling of requests to a specific application.	<pre>show status application applicationname</pre>	<p>Displays how long the application has been running, the number of application events processed, failed, and pending, the number of hits and misses by application events to the cache, and average, minimum and maximum processing time for application events.</p> <p>Example:</p> <pre>show status application sys_cmpCommunities  &lt;?xml version='1.0' encoding='UTF-8'?&gt;  &lt;PSXConsoleCommandResults&gt;   &lt;command&gt;show status application sys_cmpCommunities&lt;/command&gt;   &lt;resultCode&gt;0&lt;/resultCode&gt;   &lt;resultText&gt;&lt;/resultText&gt;   &lt;PSXApplicationStatus&gt;  &lt;name&gt;sys_cmpCommunities&lt;/name &gt;   &lt;PSXStatistics/&gt;   &lt;ElapsedTime&gt;     &lt;days&gt;0&lt;/days&gt;     &lt;hours&gt;0&lt;/hours&gt;     &lt;minutes&gt;50&lt;/minutes&gt;     .     .     . &lt;/PSXConsoleCommandResults&gt;</pre>
Start a server application	<pre>start application applicationname</pre>	
Stop and restart a server application	<pre>restart application applicationname</pre>	
Stop a server application	<pre>stop application applicationname</pre>	

To ...	Enter the command ...	Notes
Turn on default tracing to interactively debug an application running on CM System.	<pre>trace default applicationname</pre>	<p>When tracing occurs, CM System returns the output of &lt;Rhythmyx root&gt;/&lt;application name&gt;/~, application name&gt;.trace to the console. [<a href="#">link to Tracing Results</a>]</p> <p>Example:</p> <pre>trace default sys_caContentSearch  &lt;?xml version='1.0' encoding='UTF-8'?&gt;  &lt;PSXConsoleCommandResults&gt;   &lt;command&gt;trace default sys_caContentSearch&lt;/command&gt;   &lt;resultCode&gt;0&lt;/resultCode&gt;   &lt;resultText&gt;&lt;/resultText&gt; &lt;/PSXConsoleCommandResults&gt;</pre>
Turn on specific tracing options to interactively debug an application running on CM System.	<pre>trace flag1 [flag2] [flag3] [flag4] applicationname</pre> <p><a href="#">Tracer Types and Flags</a> [<a href="#">link</a>]</p>	<p>Enter up to four trace flags in hexadecimal format.</p> <p>Example:</p> <pre>trace 0x1 0x100 0x200 0x1000 sys_caContentSearch</pre> <p>When tracing occurs, CM System returns output of &lt;Rhythmyx root&gt;/&lt;application name&gt;/~, application name&gt;.trace to the console.</p>
View tracing options	trace help	

## Server Console Commands for Displaying Resources

To ...	Enter the command ...	Notes
Display information on various system resources	dump resources	<p>Displays database pool, user thread, request queue, user session, request dispatcher, and cache statistic information.</p> <p>Example:</p> <pre>dump resources &lt;?xml version='1.0' encoding='UTF-8'?&gt; &lt;PSXConsoleCommandResults&gt;   &lt;command&gt;dump resources &lt;/command&gt;   &lt;ReaperThread isAlive="yes"/&gt;   &lt;DefaultCredentials&gt;     &lt;Credential server="INETDAE7/JENNIFER"&gt;       &lt;User name="sa" password="****"/&gt;     &lt;/Credential&gt;   &lt;/DefaultCredentials&gt;   &lt;InstalledDrivers&gt;     .     .     . &lt;/PSXConsoleCommandResults&gt;</pre>



To ...	Enter the command ...	Notes
Display summaries of datasource information	dump datasources	<p>Example:</p> <pre> dump datasource &lt;datasources&gt;   &lt;datasource name="rxdefault" isCmsRepository="yes"&gt;     &lt;jndiDatasourceName&gt;jdbc/rxdefault t       &lt;/jndiDatasourceName&gt;     &lt;jdbcUrl&gt;jdbc:jtds:sqlserver://be nder       &lt;/jdbcUrl&gt;     &lt;database&gt;rxRhino&lt;/database&gt;     &lt;schema&gt;dbo&lt;/schema&gt;   &lt;/datasource&gt; &lt;/datasources&gt; </pre>
Display information about all handlers	dump handlers	<p>Example:</p> <pre> dump handlers &lt;?xml version='1.0' encoding='UTF-8'?&gt; &lt;PSXConsoleCommandResults&gt;   &lt;command&gt;dump handlers &lt;/command&gt;   &lt;RequestHandlers size="266"&gt;     &lt;Handlers&gt;       &lt;Handler name="data- xrd_cassyndarticles" class="com.percussion.server.PSAp plicationHandler"&gt;     &lt;SupportedTypes&gt;[POST, GET]&lt;/SupportedTypes&gt;       .       .       .     &lt;/PSXConsoleCommandResults&gt; </pre>

## Server Console Commands for Flushing the Server and MetaData Caches

MetaData Cache		
To...	Enter the command...	Notes
Flush the metadata cache	<pre>flush dbmd [-d datasource] [-t table]</pre>	<p>The <code>-d</code> database and <code>-t</code> table, parameters are optional.</p> <p>Examples:</p> <p>To flush metadata for a backend table named <code>dbo.RXARTICLE</code>:</p> <pre>flush dbmd -d rxmaster -t RXARTICLE</pre>
Get Help with the flush dbmd command	<pre>flush dbmd OR flush dbmd -h</pre>	<p>Example:</p> <pre>flush dbmd -h &lt;PSXConsoleCommandResults&gt;   &lt;command&gt;flush dbmd &lt;/command&gt; &lt;resultCode&gt;0&lt;/resultCode&gt;   &lt;resultText&gt; Format of this command is: flush dbmd -d [datasource] - t [table] or flush dbmd [-h] The switches are not case sensitive, and the space . . .</pre>

Server Cache		
To...	Enter the command...	Notes
Delete all data from the server cache	flush cache	Flushes all assembler and resource pages.
Delete specific data from the server cache	<p>For assembler pages:</p> <pre>flush cache assembler [applicationname];[contentid ]; [revisionid];[variantid]</pre> <p>For resource pages:</p> <pre>flush cache resource [applicationname];[datasetna me]</pre>	<p>The parameters must be supplied in the specified orders; they may be omitted, but the semi-colon placeholder must be included.</p> <p>Example:</p> <p>To flush all pages where contentid=135 and revisionid=1:</p> <pre>flush cache ;135;1; &lt;?xml version='1.0' encoding='UTF-8'?&gt; &lt;PSXConsoleCommandResults&gt;   &lt;command&gt;flush cache ;135;1;&lt;/command&gt; &lt;resultCode&gt;1532&lt;/resultCode &gt;   &lt;resultText&gt;The cache has been flushed.&lt;/resultText&gt; &lt;/PSXConsoleCommandResults&gt;</pre>

Server Cache		
To ...	Enter the command ...	Notes
Display information from the server cache	dump cache	<p>Displays hit rate, total hits, total misses, number of items in cache, memory used, disk space used, average size of item, and disk hit rate. Amounts displayed are combined totals for cached assembler and resource pages</p> <p>Example:</p> <pre>dump cache &lt;?xml version='1.0' encoding='UTF-8'?&gt; &lt;PSXConsoleCommandResults&gt;   &lt;command&gt;dump cache &lt;/command&gt;   &lt;CacheStatistics&gt;     &lt;totalHits&gt;0&lt;/totalHits&gt;     &lt;totalRequests&gt;0&lt;/totalRequests&gt;     &lt;hitRate&gt;0%&lt;/hitRate&gt;     &lt;diskHitRate&gt;0%&lt;/diskHitRate&gt;     &lt;memoryUsage&gt;0 bytes&lt;/memoryUsage&gt;     &lt;diskUsage&gt;0 bytes&lt;/diskUsage&gt;     &lt;totalItems&gt;0&lt;/totalItems&gt;     &lt;AverageItemSize&gt;0 bytes&lt;/AverageItemSize&gt;   &lt;/CacheStatistics&gt; &lt;/PSXConsoleCommandResults&gt;</pre>
Start the server cache	start cache	Starts both assembler and resource caching.

Server Cache		
To...	Enter the command...	Notes
Stop and restart the server cache	restart cache	<p>Stops cache, restarts cache, and displays cache statistics on the server console. Applies to both assembler and resource page caching. Statistics are combined totals for assembler and resource pages.</p> <p>Example:</p> <pre>restart cache  Cache                9/6/02 11:00 AM: Restarting cache with new settings  &lt;?xml version='1.0' encoding='UTF-8'?&gt; &lt;PSXConsoleCommandResults&gt;   &lt;command&gt;restart cache &lt;/command&gt;   &lt;CacheStatistics&gt;  &lt;totalHits&gt;0&lt;/totalHits&gt;  &lt;totalRequests&gt;0&lt;/totalReque sts&gt;   &lt;hitRate&gt;0%&lt;/hitRate&gt;  &lt;diskHitRate&gt;0%&lt;/diskHitRate &gt;   &lt;memoryUsage&gt;0 bytes&lt;/memoryUsage&gt;   &lt;diskUsage&gt;0 bytes&lt;/diskUsage&gt;  &lt;totalItems&gt;0&lt;/totalItems&gt;   &lt;AverageItemSize&gt;0 bytes&lt;/AverageItemSize&gt;   &lt;/CacheStatistics&gt;  &lt;resultCode&gt;1536&lt;/resultCode &gt;   &lt;resultText&gt;The server has restarted caching.&lt;/resultText&gt; &lt;/PSXConsoleCommandResults&gt;</pre>

Server Cache		
To ...	Enter the command ...	Notes
Stop the server cache	stop cache	<p>Flushes cache, stops it, and displays cache statistics on the console. Applies to both assembler and resource caching. Statistics are combined totals for assembler and resource pages.</p> <p>Example:</p> <pre>stop cache  Cache                9/6/02 11:26 AM: Stopping cache  &lt;?xml version='1.0' encoding='UTF-8'?&gt;  &lt;PSXConsoleCommandResults&gt;   &lt;command&gt;stop cache &lt;/command&gt;   &lt;CacheStatistics&gt;  &lt;totalHits&gt;0&lt;/totalHits&gt;  &lt;totalRequests&gt;0&lt;/totalReque sts&gt;   &lt;hitRate&gt;0%&lt;/hitRate&gt;  &lt;diskHitRate&gt;0%&lt;/diskHitRate &gt;   &lt;memoryUsage&gt;0 bytes&lt;/memoryUsage&gt;   &lt;diskUsage&gt;0 bytes&lt;/diskUsage&gt;  &lt;totalItems&gt;0&lt;/totalItems&gt;   &lt;AverageItemSize&gt;0 bytes&lt;/AverageItemSize&gt;   &lt;/CacheStatistics&gt;  &lt;resultCode&gt;1534&lt;/resultCode &gt;   &lt;resultText&gt;The server has stopped caching.&lt;/resultText&gt; &lt;/PSXConsoleCommandResults&gt;</pre>

## Server Console Commands for Search

To...	Enter the command	Notes
View data about the current state of the search engine including IDs of items in the queue	show status search	<p>Console output:</p> <pre>&lt;?xml version="1.0" encoding="UTF-8"?&gt; &lt;PSXConsoleCommandResults&gt;   &lt;command&gt;status search &lt;/command&gt;   &lt;resultCode&gt;0&lt;/resultCode&gt;   &lt;resultText&gt;0: &lt;/resultText&gt;   &lt;SearchStatus runningStatus="Running"&gt;     &lt;status program="engine" state="running"/&gt;     &lt;status file-delete- count="0" program="indexer" uncommitted-libs-count="0"/&gt;   &lt;/SearchStatus&gt; &lt;/PSXConsoleCommandResults&gt;</pre>
Index a specific Content Item	search index item <i>id</i>	<i>id</i> is the Content Item ID of the item you want to index. Indexing updates the appropriate search index with the text of the Content Item.
Index all Content Items of a specific Content Type	search index type <i>id</i>	<p><i>id</i> is the Content Type ID or Content Type name of the Content Type whose Content Items you want to index. The call returns after the items have been queued for indexing. The amount of time required for the actual indexing depends on the number of Content Items queued; a large number of Content Items may take some time to queue. Search results while indexing is taking place may not be fully up to date.</p> <p>If you do not include a value for <i>id</i>, then all Content Types will be indexed. This process can take a considerable amount of time.</p>
Replace current index with an empty index for a specific Content Type	search index recreate <i>id</i>	<i>id</i> is the Content Type ID or Content Type name of the Content Type whose index you want to empty. The search engine shuts down during this operation.

To...	Enter the command	Notes
Toggle debugging	debug search on debug search off	Toggles the debug output of the search engine on or off. Equivalent to checking or unchecking the <b>Enable trace output</b> box on the Server Administrator Search tab, but the setting does not persist past server shutdown.
Remove search queue entries	search queue clear	Remove search queue entries. (This may be useful if significant search terms are not being indexed because terms before them in the queue are slowing the indexing process. )

## Server Console Commands in Alphabetical Order

Command	Function	Notes
debug search on	Toggles the debug output of the search engine on.	Equivalent to checking the <b>Enable trace output</b> box on the Server Administrator Search tab, but the setting does not persist past server shutdown.
debug search off	Toggles the debug output of the search engine off.	Equivalent to unchecking the <b>Enable trace output</b> box on the Server Administrator Search tab, but the setting does not persist past server shutdown.
dump cache	Displays combined assembler and resource page information from the server cache.	Information displayed: <ul style="list-style-type: none"> <li>▪ hit rate</li> <li>▪ total hits</li> <li>▪ total misses</li> <li>▪ number of items in cache</li> <li>▪ memory used</li> <li>▪ disk space used</li> <li>▪ average size of item</li> <li>▪ disk hit rate</li> </ul>
dump datasources	Displays a summary of datasources.	
dump handlers	Display information about all handlers.	



Command	Function	Notes
dump resources	Display information on various system resources.	Information displayed: <ul style="list-style-type: none"> <li>▪ database pool</li> <li>▪ user thread</li> <li>▪ request queue</li> <li>▪ user session</li> <li>▪ request dispatcher</li> <li>▪ cache statistic information</li> </ul>
flush cache	Delete all data from the server cache.	Deletes all assembler and resource pages.
<pre>flush cache assembler [applicationname];[contentid]; [revisionid];[variantid]  flush cache resource [applicationname];[datasetname]</pre>	Delete specific data from the server cache. Deletes an assembler page if you use flush cache assembler; deletes a resource page if you use flush cache resource.	The parameters must be supplied in the specified order; they may be omitted, but the semi-colon placeholder must be included. <p>Example:</p> To flush all pages where contentid=135 and revisionid=1: <pre>flush cache assembler ;135;1;</pre> <p>Example:</p> To flush the page where application name= sys_Compare and Dataset=145: <pre>flush cache resource sys_compare;145</pre>
flush dbmd	Get Help with the flush dbmd command.	
flush dbmd -h	Get Help with the flush dbmd command.	
flush dbmd [-d datasource] [-t table]	Flush the metadata cache	The -d database and -t table, parameters are optional. <p>Examples:</p> To flush metadata for a backend table named dbo.RXARTICLE: <pre>flush dbmd -d rxmaster -t RXARTICLE</pre>

Command	Function	Notes
<code>log dump</code>	Display server log on the console.	This command may dump a very large amount of data onto the console.
<code>log flush</code>	Forces the server to write all pending messages in the log queue to the log database immediately and returns an empty log queue.	
<code>restart application <i>applicationname</i></code>	Stop and restart a server application.	
<code>restart cache</code>	Stop and restart the server cache, and display cache statistics on the server console.	Applies to both assembler and resource caching.
<code>search index item id</code>	Indexes a specific Content Item	<i>id</i> is the Content Item ID of the item you want to index. Indexing updates the appropriate search index with the text of the Content Item.
<code>search index recreate id</code>	Replaces current index with an empty index for a specific Content Type	<i>id</i> is the Content Type ID or Content Type name of the Content Type whose index you want to empty. The search engine shuts down during this operation.
<code>search index type id</code>	Indexes all Content Items of a specific Content Type	<i>id</i> is the Content Type ID or Content Type name of the Content Type whose Content Items you want to index. The call returns after the items have been queued for indexing. The amount of time required for the actual indexing depends on the number of Content Items queued; a large number of Content Items may take some time to queue. Search results while indexing is taking place may not be fully up to date.
<code>search queue clear</code>	Remove search queue entries.	Remove search queue entries. (This may be useful if significant search terms are not being indexed because terms before them in the queue are slowing the indexing process. )

Command	Function	Notes
show applications	Display a list of all server applications.	
show applications active	Display a list of active server applications.	
show status application <i>applicationname</i>	Display statistics for server handling of requests to a specific application.	Information displayed: <ul style="list-style-type: none"> <li>▪ how long the application has been running</li> <li>▪ the number of application events:               <ul style="list-style-type: none"> <li>▪ processed</li> <li>▪ failed</li> <li>▪ pending</li> </ul> </li> <li>▪ the number of hits and misses by application events to the cache</li> <li>▪ processing time for application events               <ul style="list-style-type: none"> <li>▪ average</li> <li>▪ minimum</li> <li>▪ maximum</li> </ul> </li> </ul>
show status objectstore	Display statistics for server handling of requests by Workbench and Server Administrator.	Information displayed: <ul style="list-style-type: none"> <li>▪ how long the server has been running</li> <li>▪ the number of Workbench and Server Administrator events:               <ul style="list-style-type: none"> <li>▪ processed</li> <li>▪ failed</li> <li>▪ pending</li> </ul> </li> <li>▪ the number of hits and misses by these events to the cache</li> <li>▪ processing time for these events               <ul style="list-style-type: none"> <li>▪ average</li> <li>▪ minimum</li> <li>▪ maximum</li> </ul> </li> </ul>

Command	Function	Notes
show status search	Displays data about the current state of the search engine.	<p>Example output:</p> <pre>&lt;?xml version="1.0" encoding="UTF-8"?&gt; &lt;PSXConsoleCommandRes ults&gt;   &lt;command&gt;status search &lt;/command&gt;    &lt;resultCode&gt;0&lt;/result Code&gt;    &lt;resultText&gt;0: &lt;/resultText&gt;    &lt;SearchStatus runningStatus="Runnin g"&gt;      &lt;status program="engine" state="running"/&gt;      &lt;status file- delete-count="0" program="indexer" uncommitted-libs- count="0"/&gt;    &lt;/SearchStatus&gt;   &lt;/PSXConsoleComman dResults&gt;</pre>
show status server	Display statistics for server handling of all requests.	<p>Information displayed:</p> <ul style="list-style-type: none"> <li>▪ how long the server has been running</li> <li>▪ the number of server events: <ul style="list-style-type: none"> <li>▪ processed</li> <li>▪ failed</li> <li>▪ pending</li> </ul> </li> <li>▪ the number of hits and misses by server events to the cache</li> <li>▪ processing time for server events <ul style="list-style-type: none"> <li>▪ average</li> <li>▪ minimum</li> <li>▪ maximum</li> </ul> </li> <li>▪ IDs of items in the queue</li> </ul>

Command	Function	Notes
<code>show version</code>	Display the version of the server and CM System build.	
<code>start application <i>applicationname</i></code>	Start a server application.	
<code>start cache</code>	Start the server cache.	Starts both assembler and resource caching.
<code>stop application <i>applicationname</i></code>	Stop a server application.	
<code>stop server</code>	Stop the server.	
<code>stop cache</code>	Stop the server cache.	Flushes cache, stops it, and displays cache statistics on the console. Applies to both assembler and resource caching.
<code>trace flag1 [flag2] [flag3] [flag4] <i>applicationname</i></code>	Turn on up to four types of traces to interactively debug an application running on CM System.  Link to Tracer Types and Flags (in CM System API)	Enter up to four trace flags in hexadecimal format.  Example: <code>trace 0x1 0x100 0x200 0x1000 sys_caContentSearch</code>  When tracing occurs, CM System returns output of <code>&lt;Rhythmyx root&gt;/&lt;application name&gt;/~, application</code>
<code>trace default <i>applicationname</i></code>	Turn on default tracing to interactively debug an application running on CM System.	When tracing occurs, CM System returns the output of <code>&lt;Rhythmyx root&gt;/&lt;application name&gt;/~, application name&gt;.trace</code> to the console.
<code>trace help</code>	View tracing.	

---

## Tasks Requiring Restart of the CM System Server

Certain implementation and configuration tasks require that you restart the CM System server before changes take effect. These tasks include:

- Creating a Shared Definition
- Adding a new datasource connection configuration
- Adding a new database driver configuration
- Adding a new JNDI datasource to the CM System datasource configuration.
- Adding a new datasource file to CM System.
- Adding a new custom value to the authtypes.properties file
- Adding a new Role or Subject Cataloger
- Adding a new WebDAV configuration
- Enabling SSL
- Moving the search indexes

## CHAPTER 6

# Maintaining Users

CM System user definition and authentication data is generally maintained in an external repository.

*Security providers* (see "Security Providers and Authentication" on page 74) link to these repositories so CM System can authenticate and classify users correctly. If the security provider is an LDAP or Microsoft Active Directory server, you need to maintain a directory connection service to process this data correctly.

Each user must be included in a *Role* (see page 139) to define the Communities to which they belong and the Workflow States in which they have access to Content Items.

---

# Configuring Access to Content Explorer Tabs

Content Explorer consists of five tabs:

- **Content**  
This tab is used to access, maintain, and manage CM System Content.
- **Publishing Design**  
This tab is used to create and maintain publishing configurations, such as Sites, Content Lists, and Editions.
- **Publishing Runtime**  
This tab is used to publish content and to review publishing logs.
- **Workflow**  
This tab is used to create and maintain Workflows.
- **Admin**  
This tab is used access various administrative tools for CM System.

The Content tab is always accessible to all users. You can configure access to the Publishing Design, Publishing Runtime, Workflow, and Admin tabs individually. For example, you can give some users access to only the Publishing Runtime tab. You can allow other users access to both the Publishing Runtime and Admin tabs. Users must have access to a tab to have access to the editors on that tab.

To configure access to Content Explorer tabs:

- 1** Start and log in to the Rhythmyx Workbench. Go to the XML Server tab.
- 2** Expand the Configurations folder. Click on *Components*.  
The Rhythmyx Workbench displays the Components Editor.
- 3** Open the `cmp_banner` component.
- 4** Add a component property. The name of the component property should be one of the following (capitalization is significant):
  - `PubDesignRole`  
Use this property to configure access to the Publishing Design tab.
  - `PubRuntimeRole`  
Use this property to configure access to the Publishing Runtime tab
  - `pubrole`  
Use this property to configure access to the Publishing Design and Publishing Runtime tabs as a group.



- wfrole  
Use this property to configure visibility of the Workflow tab. (Access to this tab is controlled separately; see step 5 below.)
- sysrole  
Use this property to configure access to the Admin tab.

The value of the property is the name of the Role you want to grant access to the tab controlled by the property you specified. For example, by default, the `cmp_banner` component includes the property `sysrole` with a value of *Admin*. This configuration grants members of the Admin Role access to the Admin tab. Note that you can have multiple instances of the same property name with different values. For example, by default, the `cmp_banner` component has an addition instance of `sysrole` with a value of *Editor*. This configuration grants access to the Admin tab to members of the Editor Role in addition to members of the Admin Role.

**5** To allow access to the Workflow tab:

- a) In the Rhythmyx Workbench, expand the `.Applications` node. Expand the System Folder.
- b) Double-click on the `sys_wfEditor` application.  
The Rhythmyx Workbench displays the `sys_wfWorkflow` application editor.
- c) Right-click in the application editor and from the popup menu, choose *Security*.  
The Rhythmyx Workbench displays the Application Security Settings dialog.
- d) Click the brows button (...) next to *Entries*.  
The Rhythmyx Workbench displays the New ACL Entry dialog.
- e) Click the **Roles** radio button.
- f) In the Select Member table, select the Role to which you want to grant access to Workflow tab.
- g) Ensure that all boxes under both Runtime Access and Design Access are checked.
- h) Click the [**Close**] button.

---

## Security Providers and Authentication

Security providers link to external resources that list users that can use CM System. These external resources provide authentication support when a user attempts to log in to CM System, and in some cases also define the CM System Roles the user belongs to when logged in.

Four types of security providers are available for CM System:

- **Directory Connection**

A directory connection security provider uses a directory server, such as LDAP or Microsoft Active Directory, to list and authenticate users. This security provider can also define the CM System Roles for the users. The directory connection security provider is the recommended security provider.

- **Windows NT**

The Windows NT security provider can only be used in Windows environments. This security provider uses the operating system's security system to list and authenticate users. This security provider is the recommended alternative in Windows environments if a directory connection security provider is not an option. Percussion Software generally recommends converting your NT security to Active Directory and using a directory connection security provider instead.

- **Backend Table**

The backend table security provider uses a database table to list and authenticate users. No graphic front end is provided for this table, however, and both the user name and the password are stored as clear text. While this security provider is useful for development environments (the default CM System users shipped by Percussion Software are stored in the USERLOGIN table in the Repository database), it is not recommended for production environments.

- **Web Server**

The web server security provider derives users from a web server's security provider, and uses that security provider to authenticate the users. The exact security mechanism is controlled by the web server itself. This security provider is recommended for use only on portals or when CM System runs as a servlet on another servlet container that provides security.

## Security Providers Tab

The Security Providers tab lists any existing security providers. When shipped, CM System includes three security providers, which are listed on this tab:

- Web server
- NT security
- rxmaster backend database table

Navigate to the Security Providers tab by logging into the Rhythmyx Server Administrator, clicking the Security tab, and then clicking the Security Providers tab at the bottom of the display.

Use this tab to access dialogs to add, edit, or delete security providers.

To open an existing Security Provider configuration:

- double-click on the name of the Security Provider configuration or
- select the desired Security Provider configuration and click the **[Edit]** button.

To create a new Security Provider configuration:

- Click the **[New]** button.
- On the "Select new security provider type dialog" that appears, choose Directory Connection Security Provider.

The *JNDI Security Provider Details* (see "JNDI Security Provider Details Dialog" on page 76) dialog appears.

## Defining a Directory Connection Security Provider

Directory connection security providers, such as the Java Naming and Directory Interface (JNDI) security provider, allow CM System to query a directory server to authenticate users and, optionally, retrieve Role and other user information.

The procedures in this section describe how to configure CM System to use JNDI as a security provider.

## JNDI Security Provider Details Dialog

Use the JNDI Security Provider Details dialog to define and manage JNDI security providers.

To access the JNDI Security Provider Details dialog:

- on the Security Providers subtab of the Security tab, click the **[New]** button; on the popup dialog, choose Directory Connection and click the **[OK]** button.
- on the Security Providers subtab of the Security tab, select the security provider you want to modify and click the **[Edit]** button. If the security provider is a Directory Connection security provider, the Server Administrator displays the JNDI Security Provider Details dialog.

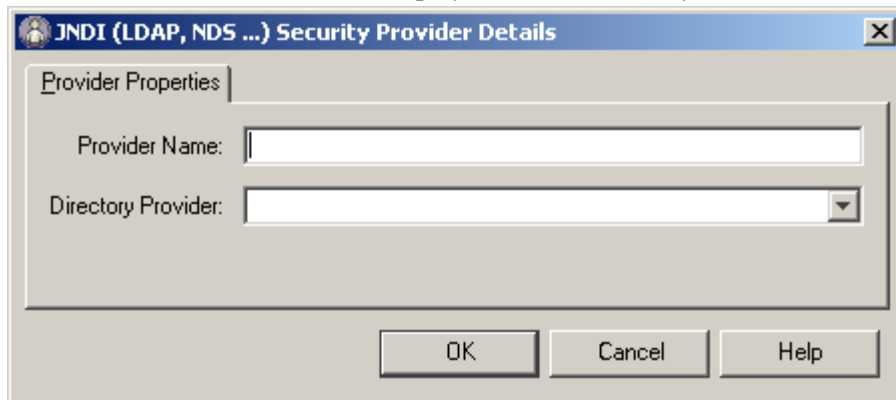


Figure 17: JNDI Security Provider Details dialog

### Field Descriptions

**Provider Name** The name of the security provider, for example, *SunONE Provider*.

**Directory Provider** The name of the Directory Set used to authenticate users

## Adding a JNDI Security Provider

To add a JNDI security provider:

- 1 On the Rhythmyx Server Administrator, choose the Security tab along the top of the dialog, then the Security Providers tab along the bottom of the dialog.
- 2 Click **[New]**.  
CM System displays the Select new security provider type dialog.
- 3 Choose Directory Connection Security Provider and click **[OK]**.  
CM System displays the *JNDI Security Provider Details dialog* (see page 76).
- 4 Enter a **Provider Name**.
- 5 Choose the *Directory Set* (see "Maintaining Directory Sets" on page 105) used to authenticate users.
- 6 Click **[OK]** to save the new security provider definition.
- 7 Click **[Apply]** to commit the changes to the CM System server.

## Editing a JNDI Security Provider

To edit a JNDI security provider:

- 1 On the Rhythmyx Server Administrator, choose the Security tab along the top of the dialog, then the Security Providers tab along the bottom of the dialog.
- 2 Select the security provider you want to edit and click **[Edit]** or double-click on the security provider name.  
CM System displays the *JNDI Security Provider Details dialog* (see page 76).
- 3 You can change the **Provider Name** or choose a different **Directory Provider**.
- 4 Click **[OK]** to save your changes and close the dialog.
- 5 Click **[Apply]** to commit the changes to the CM System server.

## Deleting a JNDI Security Provider

---

CM System does not warn you before deleting a security provider. Once you click **[Delete]** the changes are committed.

---

To delete a JNDI security provider:

- 1 On the Rhythmyx Server Administrator, choose the Security tab along the top of the dialog, then the Security Providers tab along the bottom of the dialog.
- 2 Select the security provider you want delete and click **[Delete]**.
- 3 Rhythmyx deletes the security provider. CM System DOES NOT ask you to confirm the delete action before deleting the security provider.

## Web Server

The Web Server security provider relies on an existing Web server or Web application server authentication. It is only available if you interface to CM System as a servlet under the Web server or Web application server. If the user has been authenticated by the Web server or Web application server, CM System grants access. This type of authentication is useful when accessing CM System through a Web application server, such as BEA WebLogic or IBM Websphere.

You must use the Web Server security provider if you want to implement a Single Sign-on model. In this model, a user only has to log in once to access CM System through a Web server or Web application server.

NOTE: For Single Sign-on implementation, the web server security provider requires the "Auth-Type" header to be passed into CM System. Not passing this value results in Single Sign-on returning the user to the Login page.

## Web Server Security Provider Details Dialog

Use the Web Server Security Provider Details dialog to create and manage Web server and Web application server security providers.



Figure 18: Web Server Security Provider Details Dialog

### Field Descriptions

**Security Provider Name** Required. Name of the Security Provider. The name can include spaces.

**Authentication user header name** Required. The HTTP header variable CM System examines to find the authenticated user. This name must match the name specified in the `authUserHeaderName` parameter in the setup of the CM System servlet on the Web server. If CM System cannot locate this value, the user will not be authenticated by this security provider.

**User role list header name** Required. The http header variable CM System examines to determine the Roles to which the authenticated user belongs. These Roles are included in the session.. The name must match the name specified in the `userRolesHeaderName` parameter in the setup of the CM System servlet on the Web server. The value is case-insensitive and the default value is `RxUserRoles`. If CM System cannot locate this value, it queries for the Roles internally on the server.

**Role list delimiter** Required. Specifies the character or characters used to separate each Role in the list of Roles. The default value is a semicolon (;). For example, `Author;Editor`.

## Adding a Web Server Security Provider

To add a Web server security provider:

- 1 On the Rhythmyx Server Administrator, choose the Security tab along the top of the dialog, then the Security Providers tab along the bottom of the dialog.
- 2 Click [New].  
CM System displays the Select new security provider type dialog.
- 3 Choose *Web Server Security Provider*.  
CM System displays the Web Server Security Provider Details dialog.
- 4 Enter a **Security Provider Name**.

- 5 To set up Single Sign-on:
  - a) In the **Authenticated user header name** field, enter the value of the `userRolesHeaderName` parameter from the CM System servlet setup.
  - b) In the **User role list header name** field, enter the value of the `roleListUrl` parameter from the CM System servlet setup.

NOTE: For Single Sign-on implementation, the web server security provider requires the "Auth-Type" header to be passed into CM System. Not passing this value results in Single Sign-on returning the user to the Login page.

- 6 The Role list delimiter field has a default value of “;” (semicolon). You can change this value.
- 7 Click **[OK]** to save the security provider.

## Modifying a Web Server Security Provider

To modify a Web server security provider:

- 1 On the Rhythmyx Server Administrator, choose the Security tab along the top of the dialog, then the Security Providers tab along the bottom of the dialog.
- 2 Select the security provider you want to edit and click **[Edit]**.  
CM System displays the Web Server Security Provider Details dialog.
- 3 You can change any field.
- 4 Click **[OK]** to save your edits.

## Deleting a Web Server Security Provider

---

CM System does not warn you before deleting a security

---

provider. To delete a Web server security provider:

- 1 On the Rhythmyx Server Administrator, choose the Security tab along the top of the dialog, then the Security Providers tab along the bottom of the dialog.
- 2 Select the security provider you want delete and click **[Delete]**.
- 3 CM System deletes the security provider. CM System DOES NOT ask you to confirm the delete action before deleting the security provider.

## Windows NT

Users: Any user with a system login name and password.

A Windows NT security provider passes credentials to any OS/NT directory. This includes directories foreign to the local machine where CM System is installed. NOTE: NT only.

Security provider name: A unique name for this security provider instance. For example: If you have two security providers for NT (one through Domain A and one through Domain B), you can name one security provider instance "NT Domain A" and the other instance "NT Domain B".

Domain/server name: The actual name of the Local NT Server or Trusted NT Domain being used for authentication.

- To use the Local NT Server: Enter . or \\ServerName where "ServerName" is the name of the Local NT Server where CM System is installed. (The local NT server account using "." as the server name is automatically set up during CM System installation.)
- To use a Trusted NT Domain: Enter DomainName where "DomainName" is the name of the Trusted NT Domain to be used for authentication.  
Note: To use a Trusted NT Domain, CM System must be installed on an NT Domain Controller having trust relationships defined for the specified Domain.

User ID: A user name with read access to the NT directory. (User ID provides a list of user and group names a designer can use when creating ACLs and Roles.)

Password: The User ID password to access the NT directory.

Confirm password: Same as above.

## DBMS Table Security Provider

A DBMS table security provider queries a backend table to authenticate user credentials during login. For example, the default CM System security provider, rxmaster, queries data stored in the USERLOGIN table.

At a minimum, the table must include columns to store the user name and password.

Note that CM System does not retrieve encrypted passwords, so the DBMS security provider is not recommended for production environments. This security provider is usually adequate for development environments, however.

Use the *DBMS Table Security Property Details dialog* (see page 81) to create and maintain DBMS Table security providers.

You can *add a new DBMS Table security provider* (see "Adding a DBMS Table Security Provider" on page 84) or modify an existing DBMS Table security provider.



## DBMS Table Security Property Details Dialog

Use the DBMS Table Security Property Details dialog to create and maintain DBMS Table security providers.

To access the DBMS Table Security Property Details dialog:

- On the Security Providers subtab of the Security tab, click the [New] button and on the popup dialog, select Back-end Table Security Provider and click [OK].
- On the Security Providers subtab of the Security tab, select a DBMS Table security provider and click the [Edit] button.

The DBMS Table Security Property Details dialog consists of four tabs:

- **Provider Properties** (see "DBMS Table Security Property Details Provider Properties Tab" on page 81)
- **Backend Connection** (see "DBMS Table Security Property Details Backend Connection Tab" on page 82)
- **Authentication** (see "DBMS Table Security Property Details Authentication Tab" on page 83)
- **Attributes** (see "DBMS Table Security Property Details Attributes Tab" on page 83)

### DBMS Table Security Property Details Provider Properties Tab

The Properties tab of the DBMS Table Security Property Details dialog includes general properties of the DBMS Table security provider.

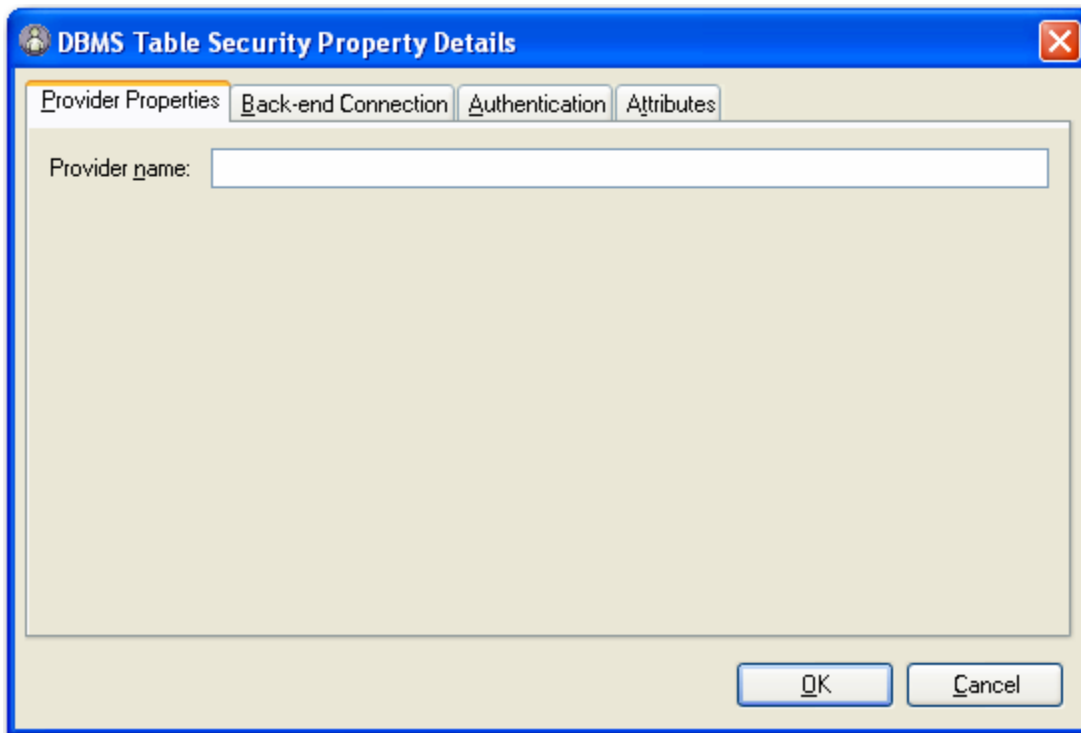


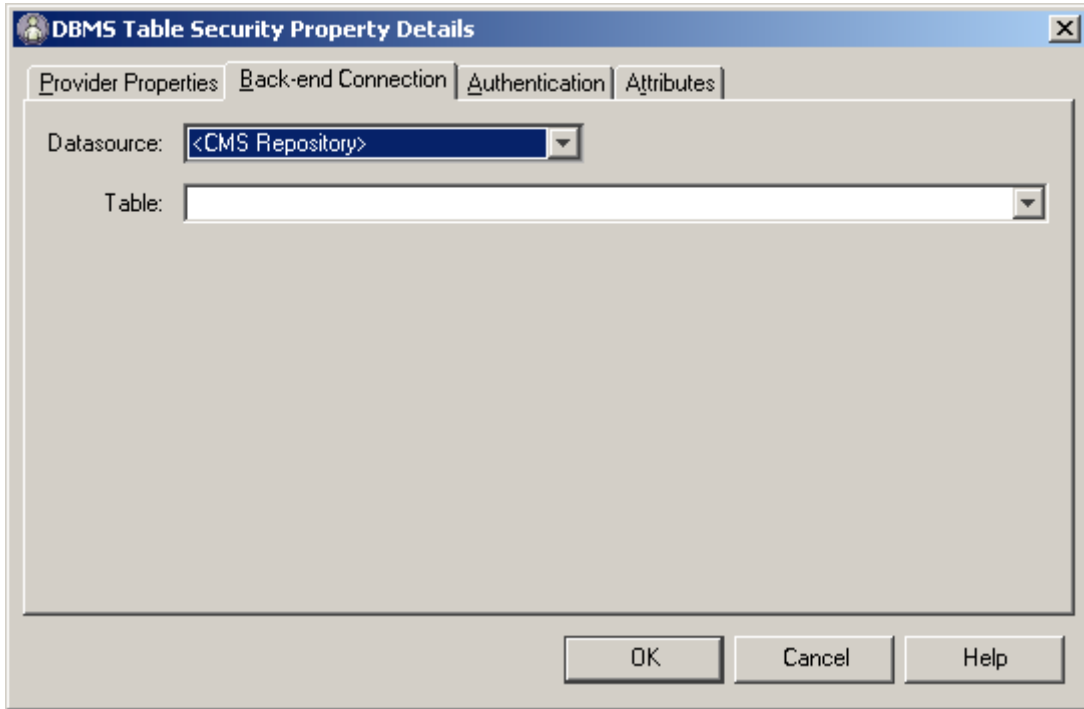
Figure 19: DBMS Table Security Property Details dialog Provider Properties tab

## Field Descriptions

**Provider name** Name of the DBMS Table security provider.

### DBMS Table Security Property Details Backend Connection Tab

Use the Back-end Connection tab of the DBMS Table Security Property Details dialog to specify the Datasource used to connect to the RDBMS server and the table that stores your authentication data.



*Figure 20: DBMS Table Security Property Provider Backend Connection Tab.*

## Field Descriptions

**Datasource** Datasource that provides the connection to the database repository where the authentication data is stored.

**Table** Table that stores the authentication data.

### DBMS Table Security Property Details Authentication Tab

Use the Authentication tab of the DBMS Table Security Provider Details dialog to specify the columns where the authentication data is stored.

You can also specify a password filter, a CM System extension that encrypts and decrypts the password so it can be stored in the database in encrypted form.

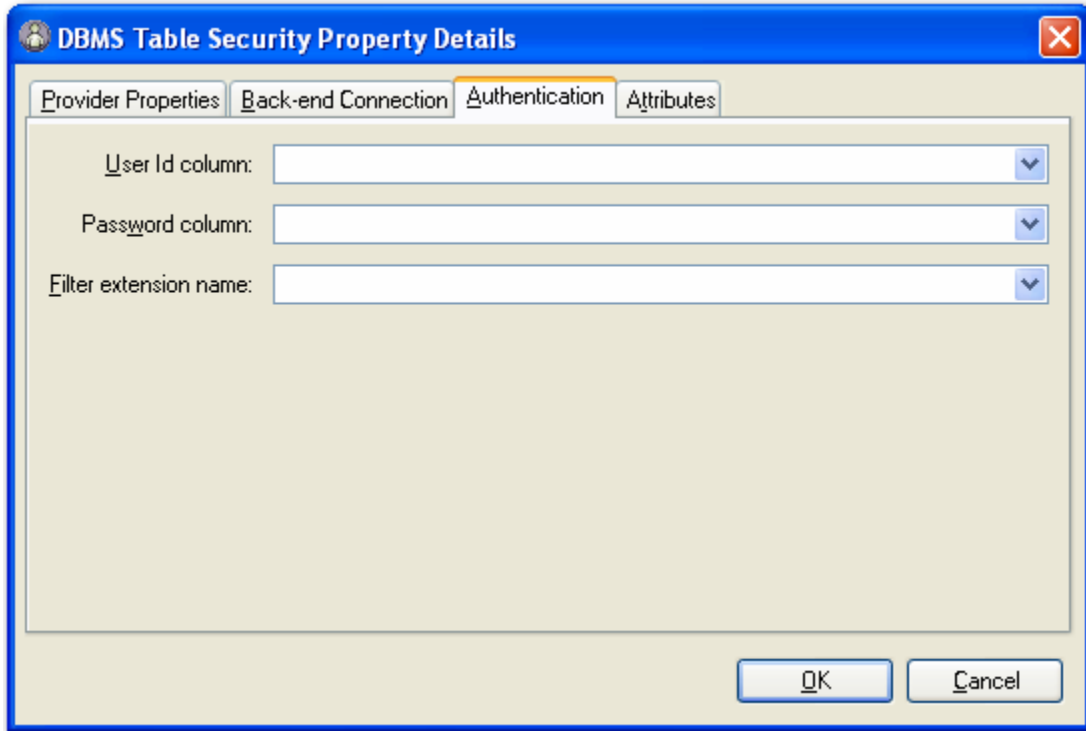


Figure 21: DBMS Table Security Property dialog Authentication tab

### Field Descriptions

**User Id column** The name of the column containing the user's login id. This column must be defined as the primary key, or it must be defined as the only key in a unique index. If this column does not guarantee uniqueness, CM System will not allow the column to be mapped as the login id.

**Password column** The name of the column containing the user's password.

**Filter extension name** Name of the CM System extension used to encrypt or decrypt the password so it can be stored encrypted in the database. CM System is shipped with a default password filter, but you can create your own password filter extension. Options include all password filter extensions defined in the system. If no password filter extension is specified, the password is stored decrypted.

### DBMS Table Security Property Details Attributes Tab

Use the Attributes tab to specify columns whose data will be passed to the User Context as attributes. You can manually map column names to session attribute names to make the attributes easier to read.

User/Attribute/attributename=columnname

Click the [**Add All**] button to add all columns in the table as attributes.

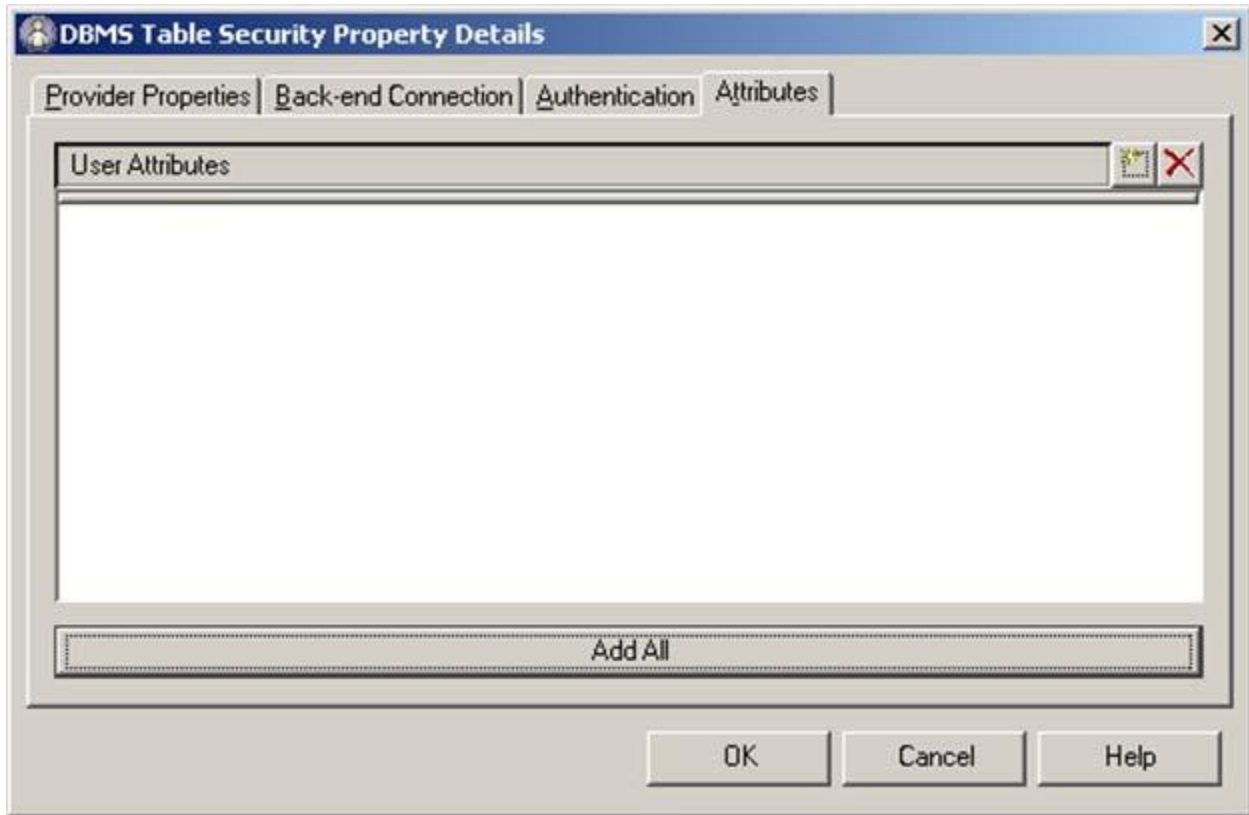


Figure 22: DBMS Table Security Property dialog Attributes tab


## Adding a DBMS Table Security Provider

To add a DBMS Table security provider:

- 1 On the Security Provider subtab of the Security tab, click the [**New**] button.
- 2 The Server Administrator displays the Select new security provider type dialog. Choose the *Back-end table security provider* and click the [**OK**] button.

The Server Administrator displays the *DBMS Table Security Property dialog* (see "DBMS Table Security Property Details Dialog" on page 81) with the *Provider Properties tab* (see "DBMS Table Security Property Details Provider Properties Tab" on page 81) selected.


- 3 Enter a **Provider Name**.
- 4 Select the *Backend Connection tab* (see "DBMS Table Security Property Details Backend Connection Tab" on page 82).
  - a) Choose the **Datasource** you want to use to connect to the database where the authentication data is stored. Options include all Datasources defined in the system.
  - b) Choose the **Table** in which your authentication data is stored.

- 5 Select the **Authentication tab** (see "DBMS Table Security Property Details Authentication Tab" on page 83).
  - a) In the **User Id column** drop list, choose column where user names are stored. Options include all columns in the specified table.
  - b) In the **Password** column drop list, choose the column where passwords are stored. Options include all columns in the table.
  - c) If you want to store and query the password in encrypted form, in the **Filter Extension Name** drop list, choose the password filter to use to encrypt and decrypt the password.
- 6 If you want to retrieve data from other columns as user attributes:
  - a) Select the **Attributes tab** (see "DBMS Table Security Property Details Attributes Tab" on page 83).
  - b) To add all columns as attributes, click the **[Add All]** button.
  - c) To add a single attribute, click the new button . The Server Administrator opens a new line on the tab.
  - d) use the following code to associate a user attribute with a column name:
 


```
User/Attribute/attributename=columnname
```
- 7 Click the **[OK]** button.

## Modifying a DBMS Table Security Provider

To modify a DBMS Table security provider:

- 1 Select the security provider you want to modify and click the **[Edit]** button.
- 2 If the security provider is a DBMS Table security provider, The Server Administrator displays the **DBMS Table Security Property Details dialog** (on page 81).
- 3 You can change any value on the **Provider Properties** (see "DBMS Table Security Property Details Provider Properties Tab" on page 81), **Backend Connections** (see "DBMS Table Security Property Details Backend Connection Tab" on page 82), and **Authentication tabs** (see "DBMS Table Security Property Details Authentication Tab" on page 83).
- 4 To add a new attribute mapping:
  - a) Select the **Attributes tab** (see "DBMS Table Security Property Details Attributes Tab" on page 83).
  - b) To add all columns as attributes, click the **[Add All]** button.
  - c) To add a single attribute, click the new button . The Server Administrator opens a new line on the tab.
  - d) use the following code to associate a user attribute with a column name:
 

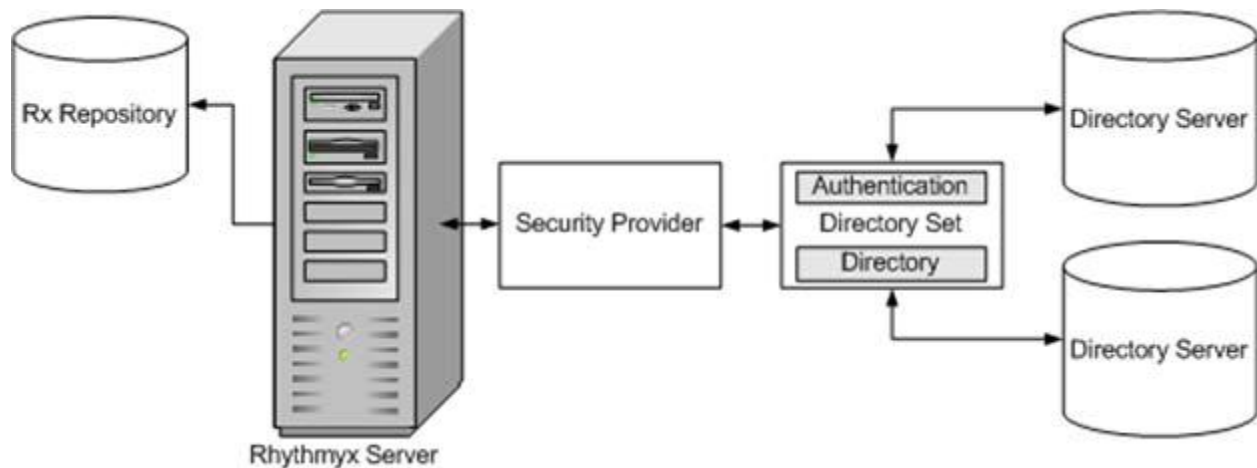
```
User/Attribute/attributename=columnname
```

- 5 Do delete an attribute mapping, select the attribute mapping you want to delete and click the delete button  .
- 6 Click the **[OK]** button

## Using Directory Services

To use a directory services provider, configure a connection between CM System and the directory server. You can connect CM System to more than one directory server, if necessary. You can configure CM System to use a directory server alone or you can specify that these services be used in conjunction with a CM System backend database that can also supply user login information.

Use the Rhythmyx Server Administrator to configure connections to directory servers.



*Figure 23: Sample LDAP Directory Server Configuration*

Directory server connections can be used to provide user login authentication and other user details for use in CM System, such as Roles. LDAP directory servers (except for the Active Directory implementation) provide the option of defining custom attribute identifiers, which provides additional flexibility for defining attributes you can use in CM System. This feature is particularly useful for associating Roles with your users. You can maintain Roles as part of the user attributes in LDAP, rather than in CM System. Using this approach simplifies user maintenance in CM System.

By specifying user data in your directory server configuration, you can also use the directory server as a provider for other CM System processing, particularly Java extensions. For example, you can use directory services to supply user phone numbers and email addresses. Directory services are reusable, allow for searches at only one directory level or in all sub-trees, and allow users to log in using any available user attribute value.

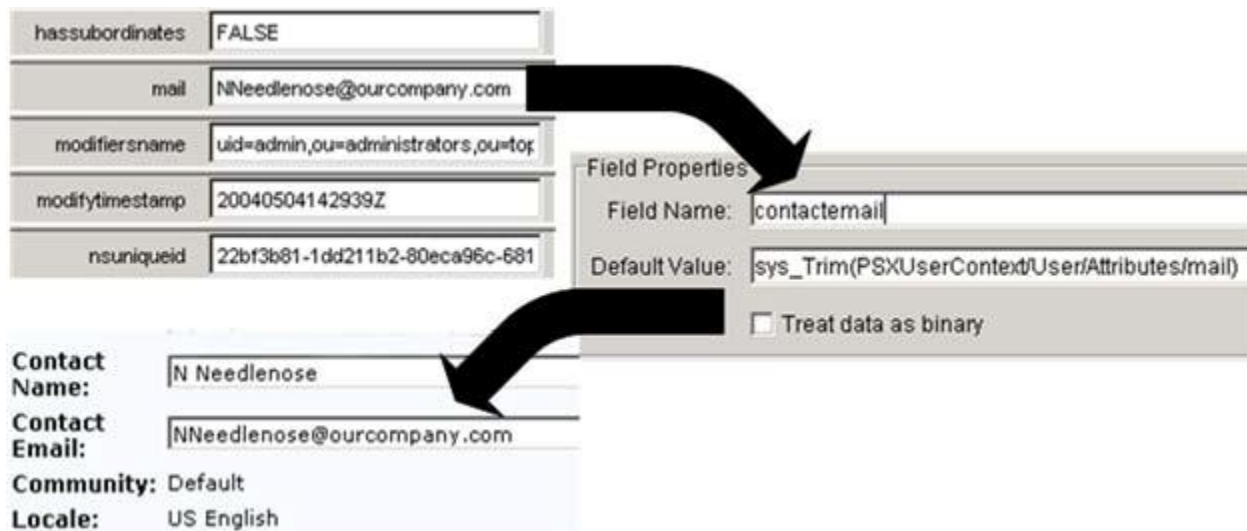


Figure 24: Using Directory Services Attributes in CM System Content Explorer

You can also aggregate multiple Directories into a common Directory Set and use this set to provide user information, which allows the use of data across Directories without redundancy. The goal of this functionality is to provide maximum reuse of Directory data while allowing access to a diverse range of directory services and configurations.

For more information on using directory servers, refer to documentation for the particular server application or third-party texts on the subject. Available resources include:

- *LDAP Directories Explained: An Introduction and Analysis* by Brian Arkills ISBN: 020178792X
- *The ABCs of LDAP: How to Install, Run, and Administer LDAP Services* by Reinhard Voglmaier ISBN: 0849313465
- *LDAP in the Solaris Operating Environment: Deploying Secure Directory Services* by Michael Haines (Author), Tom Bialaski (Author) ISBN: 0131456938
- *Active Directory*, Second Edition by Alistair G. Lowe-Norris, Robbie Allen ISBN: 0596004664
- *LDAP Directory Service - Details* <http://www.hawaii.edu/ldap/details.html>



## LDAP Directory Services Framework

CM System is a Java-based application. Using the JNDI protocol, CM System can connect to and search various implementations of LDAP directory services, including Active Directory, SunONE, Netscape, and IPlanet. CM System uses JNDI without the need for additional programming by the CM System implementer.

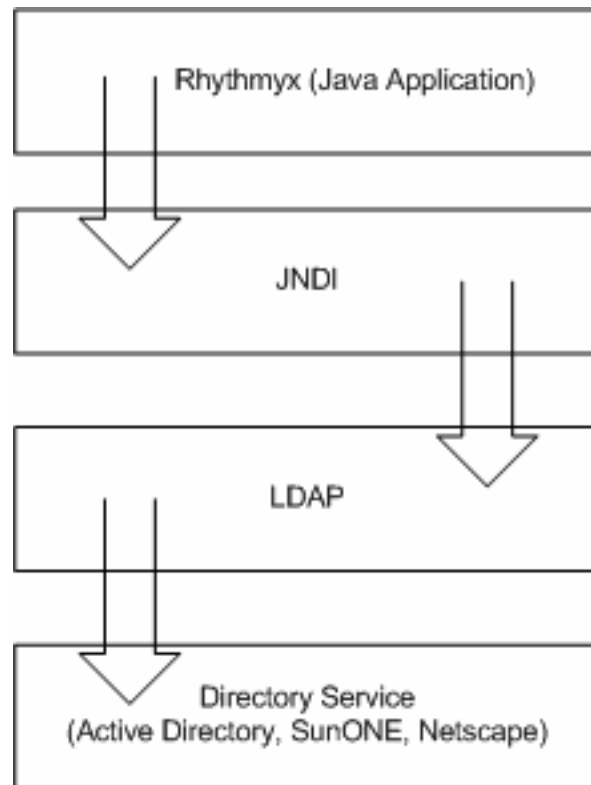


Figure 25: LDAP Directory Services Framework

LDAP directory services can be used to authenticate users as they log in to CM System in any interface – Content Explorer, Workbench, and the Server Administrator. Additionally, attributes and the values associated with each user can be used in several areas of CM System.

As such, CM System is defined as a directory-enabled application. As currently implemented, CM System can search directory services for particular objects and retrieve any and all necessary attributes. CM System is not designed to store or update objects in these repositories.

If you would like more information, consult available references on JNDI, including:

- <http://java.sun.com/products/jndi/tutorial/> - An online, downloadable tutorial providing both high- and low-level descriptions of connecting to LDAP through JNDI.
- *JNDI API Tutorial and Reference: Building Directory-Enabled Java(TM) Applications* by Rosanna Lee, Scott Seligman ISBN: 0201705028 - a Sun- recommended reference on the JNDI API.

---

These references are only necessary if you would like a more detailed understanding of JNDI.

---

## Implementing LDAP Directory Services

Implementing LDAP directory services involves two major tasks:

### 1 Defining an LDAP directory services configuration

An LDAP directory services configuration defines the data used to connect to the directory server, authenticate the user, and optionally provide additional user information. Use the Directory Services tab of the Rhythmyx Server Administrator to set up and maintain all the data for the directory services configuration.

An LDAP directory services configuration consists of the following kinds of data:

- **Authentication** (see "Maintaining Authentications" on page 91)  
Authentication data defines the data used to log in to the directory server.
- **Directory Configuration** (see "Maintaining Directory Configurations" on page 96)  
A Directory Configuration defines the data required to connect to a specific LDAP directory.
- **Directory Sets** (see "Maintaining Directory Sets" on page 105)  
A Directory Set defines a group of Directory Configurations that can be accessed together, and the data required to connect to them. A Directory Set may consist of a single Directory Configuration, of multiple Directory Configurations for directories on the same directory server, or of multiple Directory Configurations for directories on different directory servers.

You must define a Directory Set before you can define a Directory Connection Security Provider or a Role Provider.

---

- **Role Providers** (see "Maintaining Role Providers" on page 111) (optional)  
A Role Provider defines the data that determines how CM System will use directory server information to determine the user's Roles once they have been authenticated.
- **Catalogers** (see "Maintaining Catalogers" on page 115) (optional)  
A cataloger provides the ability to retrieve data from a security provider backend. Two types of catalogers are available: subject catalogers retrieve data on individual users; role catalogers determine membership in a Role.

You may find it useful to download and install an LDAP browser to facilitate your directory services configuration. The browser allows you to look up and confirm attribute, connection, and directory information. An LDAP browser makes it easier to complete the directory services configuration, but the browser is not required to complete the configuration successfully.

### 2 Defining the Directory Connection Security Provider (JNDI, in this case)

A Directory Connection Security Provider allows CM System to query the directory server to authenticate users and retrieve Role and other user information. Configure CM System to use JNDI as the Directory Connection Security Provider once you have completed the LDAP directory service configuration.

## Maintaining Authentications

Authentications include the credentials necessary to log in to a particular directory server. The data you define for an Authentication includes:

- Authentication name
- Schema
- Credentials
- Credential Attributes

### Authentication Dialogs

Use the following CM System Server Administrator dialogs to set up an Authentication.

- *Authentications tab* (on page 92)
- *Authentication Editor* (on page 93)

The topics for these two dialogs provide a description of what the dialogs contain and how to navigate to them. The procedures for adding, editing, or deleting authentications are in these topics:

- *Adding an Authentication* (on page 94)
- *Editing an Authentication* (on page 95)
- *Deleting an Authentication* (on page 95)

### Authentications Tab

The Authentications tab lists any existing Authentications. When shipped, CM System does not contain any predefined Authentications (since the services to which you will be connecting and your credentials are unknown). The display shows the Authentication's name, the schema used, and the user name being used to log in to the directory server.

Navigate to the Authentications tab by logging into the Rhythmyx Server Administrator, clicking the Directory Services tab, and then clicking the Authentications tab at the bottom of the display.

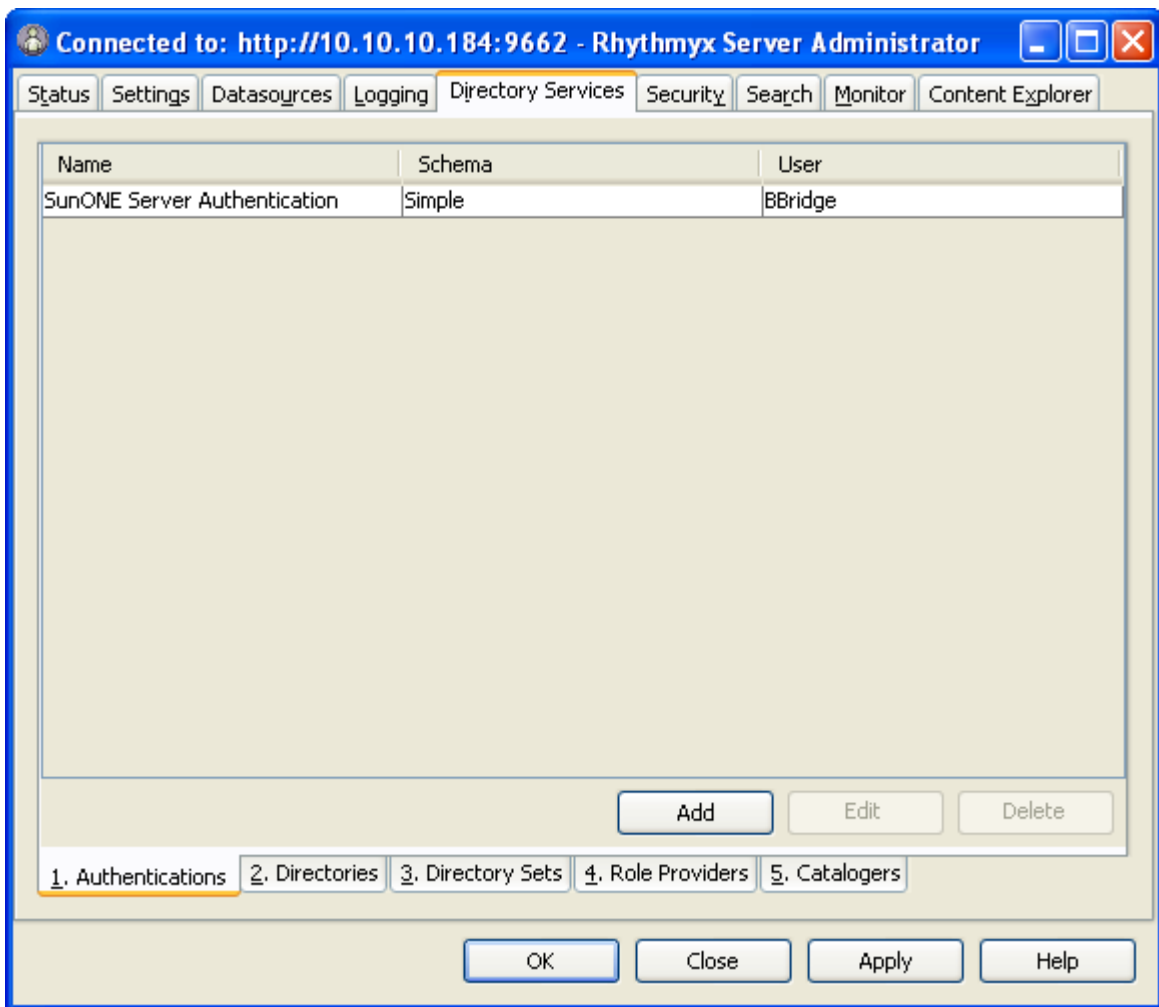


Figure 26: Authentications Tab

Use this tab to access dialogs to add, edit, or delete Authentications.

To open an existing Authentication:

- double-click on the name of the desired Authentication or
- select the desired Authentication and click the **[Edit]** button

To create a new Authentication:

- Click the **[Add]** button.

The *Authentication Editor* (on page 93) appears.

### Authentication Editor

Use the Authentication Editor to enter or modify Authentication data.

To open an existing Authentication:

- double-click on the name of the desired Authentication on the Authentications tab or
- select the desired Authentication on the Authentications tab and click the **[Edit]** button

To create a new Authentication:

- Click the **[Add]** button on the Authentications tab

The Authentication Editor appears.

*Figure 27: Example Authentication Definition*

### Authentication Editor Field Descriptions:

**Name** A description of the Authentication being registered.

**Schema** The authentication mechanism being used. Rhythmyx supports three mechanisms. Choose the one appropriate for your configuration.

- **None** - This mechanism consists of a single message from the client to the server. This mechanism does not provide a security layer. This is similar to an anonymous bind.
- **Simple** - The most commonly used Authentication mechanism. This method uses a simple clear-text user password. Clear-text passwords are simple and interoperate with almost all existing operating system authentication databases. The mechanism consists of a single message from CM System to the directory server. CM System sends a null character, followed by the user name, followed by a null character, followed by the clear-text password. Upon receipt of the message, the directory server verifies the user name and password against the service's database and verifies the credentials, permitting the user to log in.

- **CRAM-MD5** - A challenge and response authentication mechanism for LDAP v3 servers. (It was superseded by Digest-MD5.) Some existing LDAP v3 servers still support CRAM-MD5. When using CRAM-MD5, the LDAP server sends some data to CM System. CM System responds by encrypting the data with its password using the MD5 algorithm. The LDAP server then uses CM System's stored password to determine whether it used the right password. If this password is correct, the user is permitted to login.

**User Name** The user name being used to establish a connection (log in) to the directory server. Specify the fully-qualified distinguished name of the user. This user must have rights to catalog (list) all requested attribute values.

**Password** The password for the user name used to connect to the Directory Server.

**Append Base DN** (Note: This checkbox is available for backwards-compatibility with earlier versions of CM System; it should not be used in new implementations.) In some instances, the user name used for connecting to the directory server is required by the directory server to be fully qualified. When you check this box, the Base DN for the Directory (defined in the Provider URL Selector Dialog) is appended to the User Name value. (The Base DN denotes the directory location where searches on the directory server should be initiated.) Connections to Active Directory require this box to be selected.

**User Attribute** (Note: This field is available for backwards-compatibility; it should not be modified in new implementations.) The attribute associated with the User Name as viewed in the directory server. CN (common name) is the most commonly used attribute for user names.

**Password Filter** If the password is being processed by a custom encryption algorithm, the exit being used to do the encryption must be supplied here. CM System ships with one encryption filter (default encryption filter). Passwords must be decrypted by the directory server upon receipt.

### Adding an Authentication

To add a new directory services Authentication:

- 1 Log into the Rhythmyx Server Administrator and click the Directory Services tab at the top of the display.

---

An Authentication is valid for only one CM System server. When you have multiple CM System servers, you must create separate Authentications for each server.

---

- 2 Click the Authentications tab at the bottom of the display.
- 3 Click the **[Add]** button; CM System displays the Authentication Editor.

- 4 Complete the fields as described in the topic *Authentication Editor* (on page 93).

Figure 28: Example Authentication Definition

- 5 Click the **[OK]** button when you have completed the necessary fields.
- 6 Click the **[Apply]** button to commit the connection registration to the CM System server.

### Editing an Authentication

You can make changes to any value in an existing Authentication registration.

---

If you change the name of an existing Authentication, CM System prompts you to modify any Directories that reference the Authentication to reflect the new name.

---

- 1 Log into the Rhythmyx Server Administrator and click the Directory Services tab at the top of the display.
- 2 Click the Authentications tab at the bottom of the display.
- 3 Select the Authentication you want to modify and click the **[Edit]** button. (Alternatively, you can double-click the Authentication name.)
- 4 Make your changes using information in the topic *Authentication Editor* (on page 93).
- 5 Click the **[OK]** button to close the Editor dialog.
- 6 Click the **[Apply]** button to commit the changes to the CM System server.

### Deleting an Authentication

When no Directories are using an Authentication, that Authentication is obsolete. You must delete obsolete Authentications manually.

- 1 Log into the Rhythmyx Server Administrator and click the Directory Services tab at the top of the display.
- 2 Click the Authentications tab at the bottom of the display.

- 3 Select the Authentication(s) you want to delete and click the [**Delete**] button.

---

CAUTION: Once you click the [**Delete**] button, the removal is committed even if you do not click the [**Apply**] button or save the changes when closing the Server Administrator.

---

- 4 Click the [**OK**] button to close the Editor dialog.
- 5 Click the [**Apply**] button to commit the changes to the CM System server.

## Maintaining Directory Configurations

Directory configurations include the information necessary for CM System to connect to a particular directory server Directory. The data you define for the Directory configuration includes:

- Name
- Catalog
- Factory
- Authentication
- Provider URL

Optionally, you can include

- Returned Attributes
- Group Providers

### Directory Configuration Dialogs

Use the following Rhythmyx Server Administrator dialogs to set up a Directory configuration.

- *Directories tab* (on page 97)
- *Directory Editor* (on page 98)
- *Provider URL Selector* (on page 100)

The topics for these three dialogs provide a description of what the dialogs contain and how to navigate to them. The procedures for adding, editing, or deleting Directory configurations are in these topics:

- *Adding a Directory Configuration* (on page 102)
- *Editing a Directory Configuration* (on page 103)
- *Deleting a Directory Configuration* (on page 104)



### Directories Tab

The Directories tab lists any existing Directories. When shipped, CM System does not contain any predefined Directories (since the services to which you will be connecting and your credentials are unknown). The display shows the Directory's name, the catalog method used, and the URL of the directory server.

Navigate to the Directories tab by logging into the Rhythmyx Server Administrator, clicking the Directory Services tab, and then clicking the Directories tab at the bottom of the display.

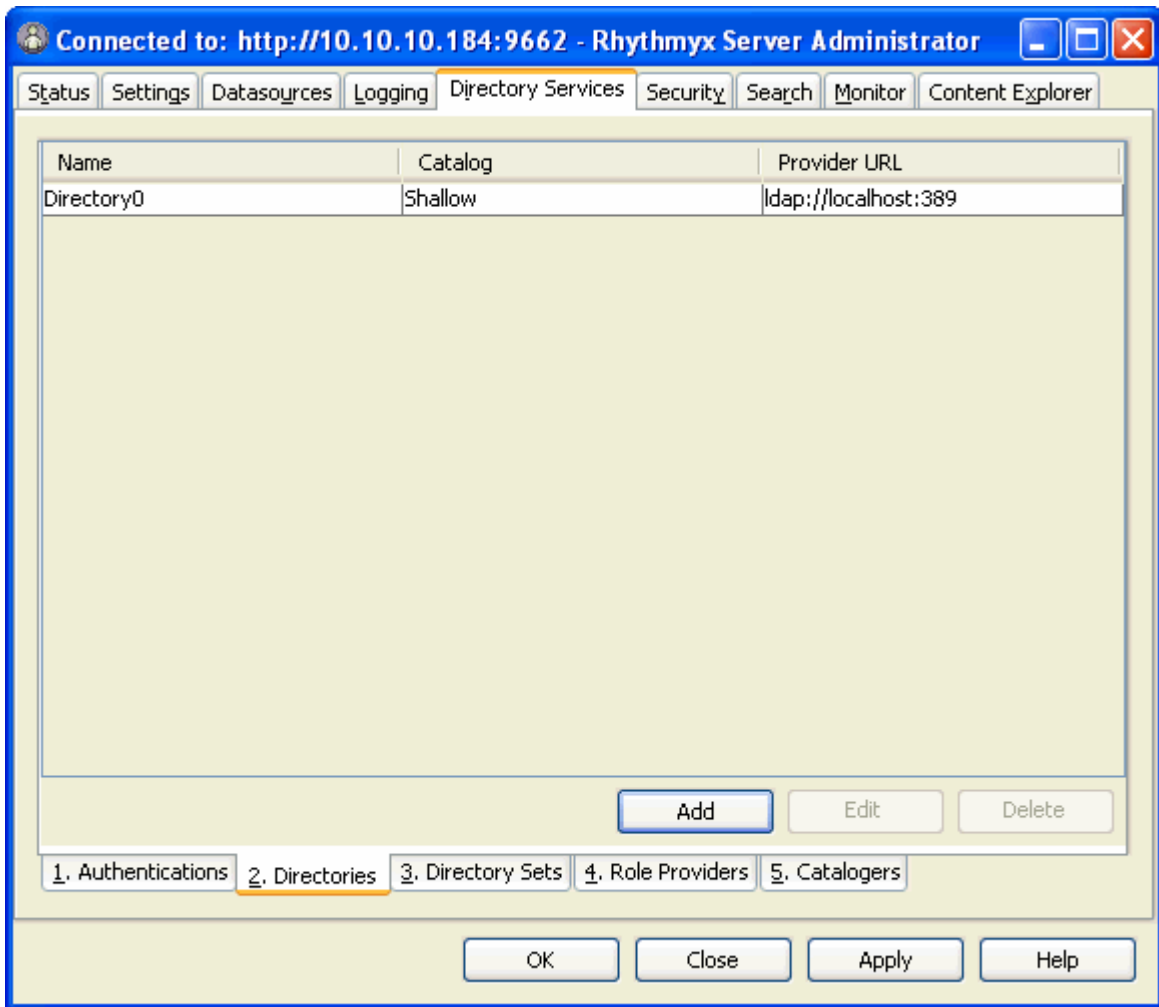


Figure 29: Directories Tab

Use this tab to access dialogs to add, edit, or delete Directory configurations.

To open an existing Directory configuration:

- double-click on the name of the desired Directory configuration or
- select the desired Directory configuration and click the [**Edit**] button

To create a new Directory configuration:

- Click the [**Add**] button.

The *Directory Editor* (on page 98) appears.

## Directory Editor

Use the Directory Editor to enter or modify Directory configuration data.

To open an existing Directory configuration:

- double-click on the name of the desired Directory configuration on the Directories tab or
- select the desired Directory on the Directories tab and click the **[Edit]** button

The screenshot shows the 'Directory Editor' dialog box. The fields are as follows:

- Name:** Sun ONE Server Directory
- Catalog:** Shallow
- Factory:** com.sun.jndi.ldap.LdapCtxFactory
- Authentication:** (empty)
- Provider URL:** ldap://localhost:389
- Return attributes:** (empty list)
- Group Providers to make availa...:** (empty list)
- Enable debug output:**

Buttons at the bottom: OK, Cancel, Help.

Figure 30: Example Directory Definition

### Directory Editor Field Descriptions:

**Name** A description of the Directory being registered. To be consistent with the naming scheme we used for the Authentication, we have named this Directory the Sun ONE Server Directory.

**Catalog** The type of cataloging being done. CM System defines two types of directory server cataloging. Choose the one that is right for your configuration.

- **Shallow:** CM System retrieves only those records immediately below the search base
- **Deep:** CM System retrieves values from the search base and all sub-trees. Depending on the size of the tree being cataloged, this setting can cause increased response times.

**Factory** The class name for the factory used to create the contexts for connections to the directory server. The most common factories are provided in a drop list.

- **LdapCtxFactory** Used for connections to LDAP servers, including Active Directory. This is the most commonly used factory.
- **NISCtxFactory** Used for connections to NIS (Network Information Services) servers.

**Authentication** Select the Authentication for this Directory from the drop list. If you need to create a new Authentication, choose "New Authentication..." from the drop list to display the Authentication Editor.

**Provider URL** The provider URL defines the URL of the directory server and the location on the directory server where searches should begin. Click the ellipsis next to the field to display the ***Provider URL Selector dialog*** (see "Provider URL Selector" on page 100). Use this dialog to help define the correct URL.

**Return Attributes** Click the Insert New Entry icon to the right of the Return Attributes row to list any specific attribute names you want a directory search to return. If this table is filled in, only the specified attributes are returned with the search results. If the table in this field is empty, all attributes are returned with the search results.

**Group Provider to make available** Group providers define a source of group information to use when authenticating a user or when retrieving user attributes from a group. Add and remove Group Providers in this field.

**Enable debug output** Check this box to request debug output to the console.

### Provider URL Selector

When defining a new Directory configuration, you must specify a Provider URL. This URL is a combination of the directory server host name, listening port, and a base DN for the directory server. The Provider URL Selector dialog helps you build the URL with a minimum of information.

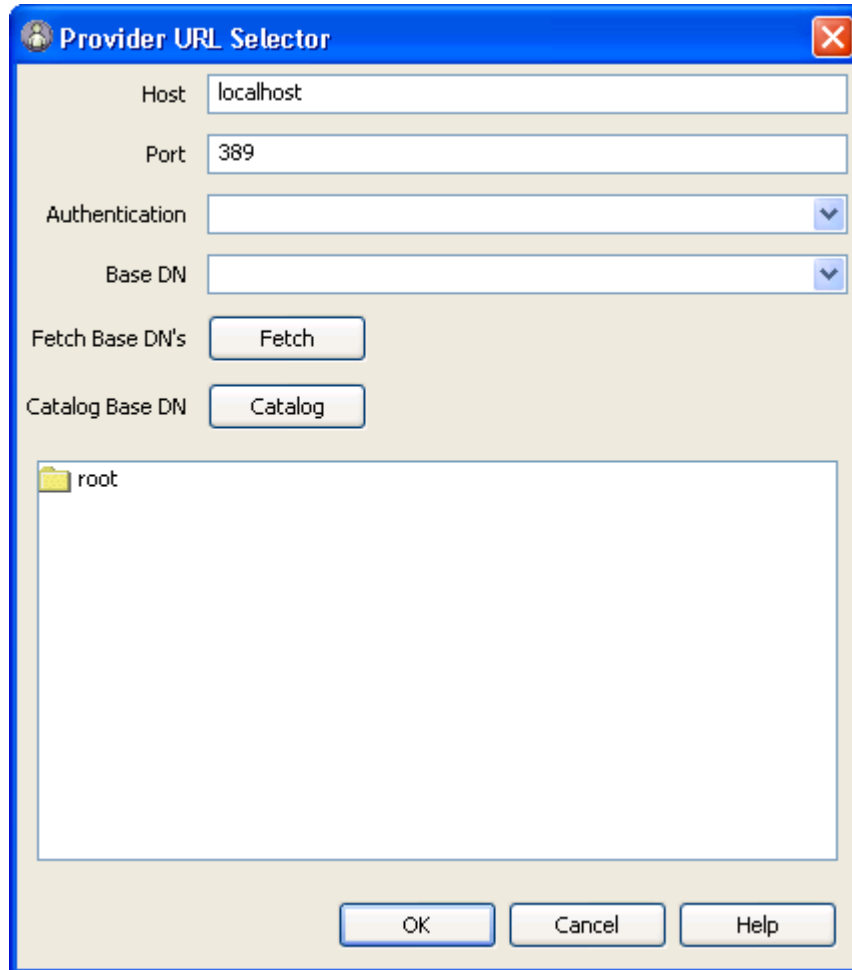


Figure 31: Provider URL Selector Dialog

#### Provider URL Selector Field Descriptions:

**Host** - The resolvable name (or IP address) of the directory server to which CM System needs to connect.

**Port** - The LDAP listening port of the named Host. The default port number for LDAP is 389.

**Authentication** - The Authentication used to connect to the named Host. If an Authentication to this Host has not yet been created, select "New Authentication..." from the drop list to define an Authentication for the Host.

**Base DN** - The place to begin searches in the directory server. If the Host, Port, and Authentication information is correct, clicking the [**Fetch**] button returns a list of available Base DNs.

**Fetch Base DNs** - Clicking the [**Fetch**] button returns a list of available Base DNs from the named Host, assuming the Host, Port, and Authentication specified in the Provider URL Selector dialog are correct.

Fetching Base DNs from an Active Directory server does not yield the proper DN for Users. Instead, on an Active Directory server, it is common to select the non-Configuration or Schema DN and prepend CN=Users.

**Catalog Base DN** - Clicking the [Catalog] button catalogs the objects in the base DN tree. Selecting an object below the Base DN narrows the list of objects searched by adding the selected objects to the Base DN. A Base DN listed without any values below it usually indicates an error in the defined Authentication or Provider information.

### JNDI Group Provider Details Dialog

Use the JNDI Group Provider Details dialog to create and maintain JNDI Group Provider records.

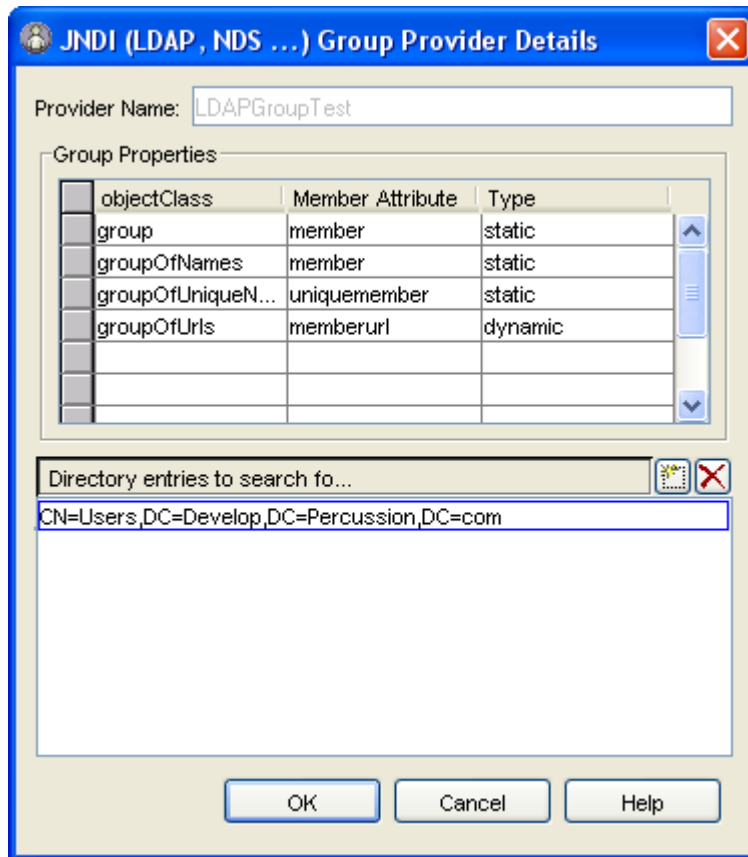



Figure 32: JNDI Group Provider Details Dialog

### JNDI Group Provider Details Dialog Field Descriptions:

- Provider Name - Name of this group provider. Editable only when creating a new group provider. When editing an existing group provider, this field is unavailable.
- Group Properties table: the Group Properties table is populated with standard values. If you do not use standard objectClasses or attributes, you can change the entries. For example, removing unused objectClasses (such as removing the groupOfUrls if you do not use dynamic groups) may improve performance slightly.
  - Group Properties: objectClass - Enter the name of a Java object class. Completing this field is required to enter a Member attribute or Type. CM System treats all LDAP entries with this object class as a group.

- Group Properties: Member Attributes - The name of the attribute used to determine the group members for entries with the specified object class.
- Group Properties: Type - The value in this field defines how CM System will treat the value of the Member Attribute. Options are:
  - Static - CM System treats the value of the attribute as if it specifies the name of another entry, either a person that is a member or another group. This is the default option.
  - Dynamic - CM System treats the value of the attribute as if it specifies an LDAP filter URL. This filter specifies the Directory entries that should be considered members of the group.
- Directory Entries to search for groups - Each entry in this list specifies a node in the Directory that CM System searches for possible group entries. Each entry should be the fully qualified distinguished name (DN) from the Directory root. CM System uses these entries to catalog groups for any directory connection security provider that lists this group provider in its definition.

To add a directory entry to search for groups:

- a) Click the Insert New Entry button  to the right of the "Directory Entries to Search For..." row.

CM System makes a new row available in the Directory entries to search for groups field.

- b) Enter the fully-qualified distinguished name (DN) of the directory entry. (NOTE: If you use a distinguished name that includes the "?" wildcard character, you must escape the character by replacing it with %3f; for example, OU=tech? should be entered as OU=tech%3f.)

### Adding a Directory Configuration

To add a new Directory configuration:


- 1 Log into the Rhythmyx Server Administrator and click the Directory Services tab at the top of the display.

---

A Directory configuration is valid for only one CM System server. When you have multiple CM System servers, you must create separate Directory configurations for each server.

---

- 2 Click the Directories tab at the bottom of the display.
- 3 Click the [**Add**] button.
- 4 The Server Administrator displays the *Directory Editor* (on page 98).
- 5 Enter a **Name** for the Directory configuration.
- 6 Choose a **Catalog** option. Options include:
  - Shallow: CM System retrieves only those records immediately below the search base
  - Deep: CM System retrieves values from the search base and all sub-trees. Depending on the size of the tree being cataloged, this setting can cause increased response times.

- 7 Choose the **Factory** used to create connections to the directory server. Default options include:
  - `LdapCtxFactory` Used for connections to LDAP servers, including Active Directory. This is the most commonly used factory.
  - `NISCtxFactory` Used for connections to NIS (Network Information Services) servers.You can also add the name of any new factory class file you might use.
- 8 Choose the **Authentication** (see "Maintaining Authentications" on page 91) you want to use to log in with this directory configuration. Options include all Authentications defined in your system.
- 9 Enter the **Provider URL**. You can use the *Provider URL Selector* (on page 100) to help you determine the correct URL.
- 10 To add a **Return Attribute**, click the New button  and enter the name of the attribute you want to return. (NOTE: If you specify any attributes in this table, only those attributes will be returned. If you do not specify any attributes, then all attributes will be returned.)
- 11 To add a **Group Provider**, see *Adding a Group Provider* (on page 104).
- 12 Click the [OK] button when you have completed the necessary fields.
- 13 Click the [Apply] button to commit the registration to the CM System server.

## Troubleshooting

If you are having trouble with your searches failing or returning incorrect data, check the following:

- Is the Authentication defined correctly?
- Is the search base too vague or too restrictive?
- Do the record and attributes actually exist?
- Is the record actually located under the search base?
- Are the directory, port, and bind id correct?
- Is there a firewall blocking access to complete the search?
- Is the directory operational at this time?
- Is there an access control list overriding the query search or response?

## Editing a Directory Configuration

You can make changes to any value in an existing Directory configuration.



---

If you change the name of an existing Directory, CM System prompts you to modify any Directory Sets that reference the Directory to reflect the new name.

---

- 1 Log into the Rhythmyx Server Administrator and click the Directory Services tab at the top of the display.
- 2 Click the Directories tab at the bottom of the display.
- 3 Select the Directory you want to modify and click the [Edit] button. (Alternatively, you can double-click the Directory name.)

The Server Administrator displays the *Directory Editor* (on page 98).

- 4 You can change the value in any field.
- 5 To add a **Return Attribute**, click the New button  and enter the name of the attribute you want to return. (NOTE: If you specify any attributes in this table, only those attributes will be returned. If you do not specify any attributes, then all attributes will be returned.)
- 6 To delete a Return Attribute, select the Return Attribute you want to delete and click the delete button .
- 7 You can *add* (see "Adding a Group Provider" on page 104), *modify* (see "Editing a Group Provider" on page 105), or *delete* (see "Deleting a Group Provider" on page 105) a Group Provider.
- 8 Click the [OK] button to close the Editor dialog.
- 9 Click the [Apply] button to commit the changes to the CM System server.

### Troubleshooting a Directory Services Configuration

If you are having trouble with your searches failing or returning incorrect data, check the following:

- Is the Authentication defined correctly?
- Is the search base too vague or too restrictive?
- Do the record and attributes actually exist?
- Is the record actually located under the search base?
- Are the directory, port, and bind id correct?
- Is there a firewall blocking access to complete the search?
- Is the directory operational at this time?
- Is there an access control list overriding the query search or response?

### Deleting a Directory Configuration

When no Directory Sets are using a Directory, that Directory is obsolete. You must delete obsolete Directories manually.

- 1 Log into the Rhythmyx Server Administrator and click the Directory Services tab at the top of the display.
- 2 Click the Directories tab at the bottom of the display.
- 3 Select the Directory(s) you want to delete and click the [Delete] button.

---

CAUTION: Once you click the [Delete] button, the removal is committed even if you do not click the [Apply] button or save the changes when closing the Server Administrator.

---


- 4 Click the [OK] button to close the Editor dialog.
- 5 Click the [Apply] button to commit the changes to the CM System server.

### Adding a Group Provider

To add a group provider:

- 1 *Add a Directory Configuration* (see "Adding a Directory Configuration" on page 102) or *Edit a Directory Configuration* (see "Editing a Directory Configuration" on page 103).



- 2 Click the Insert New Entry button  to the right of the "Group Providers to Make Availa..." row near the bottom of the dialog.

CM System displays a drop list showing all existing group providers. You can select an existing provider by double-clicking on its name. If the drop list is empty, click the arrow and click on *Create new* to create a new group provider.

CM System displays the *JNDI Group Provider Details dialog* (on page 101).

- 3 Enter information in the dialog and optionally, edit the default information.
- 4 Click [OK] to save the group provider.
- 5 Click [Apply] to commit the changes to the CM System server.

### Editing a Group Provider


To edit a group provider:

- 1 *Edit a Directory Configuration* (see "Editing a Directory Configuration" on page 103).
- 2 In the "Group Providers to Make Availa..." row near the bottom of the dialog, double click on the Group Provider that you want to edit.  
CM System displays the *JNDI Group Provider Details dialog* (on page 101). You can add new group properties or edit existing group properties.
- 3 To edit a directory entry, double-click the entry and enter your changes.
- 4 To delete a directory entry, select the entry and click the delete button.
- 5 Click [OK] to save your changes.
- 6 Click [Apply] to commit the changes to the CM System server.

### Deleting a Group Provider

Removing a group provider from a security provider only removes the association between the security provider and the group provider. The group provider is not deleted.

To remove a group provider:

- 1 *Edit a Directory Configuration* (see "Editing a Directory Configuration" on page 103).
- 2 In the "Group Providers to Make Availa..." row near the bottom of the dialog, select the group provider you want to remove and click the remove button .

## Maintaining Directory Sets

A Directory Set is an aggregation of existing Directories. The data you define for a Directory Set includes:

- Name
- Directories
- Required Attributes

## Directory Set Dialogs

Use the following Rhythmyx Server Administrator dialogs to set up a Directory Set.

- *Directory Sets tab* (on page 106)
- *Directory Set Editor* (on page 108)

The topics for these two dialogs provide a description of what the dialogs contain and how to navigate to them. The procedures for adding, editing, or deleting Directory Set configurations are in these topics:

- *Adding a Directory Set* (on page 109)
- *Editing a Directory Set* (on page 110)
- *Deleting a Directory Set* (on page 111)

## Directory Sets Tab

The Directory Sets tab lists any existing Directory Sets. When shipped, CM System does not contain any predefined Directory Sets (since the services to which you will be connecting and your credentials are unknown). The display shows the Directory Set's name and the Directory(s) aggregated in the Set.

Navigate to the Directory Sets tab by logging into the Rhythmyx Server Administrator, clicking the Directory Services tab, and then clicking the Directory Sets tab at the bottom of the display.

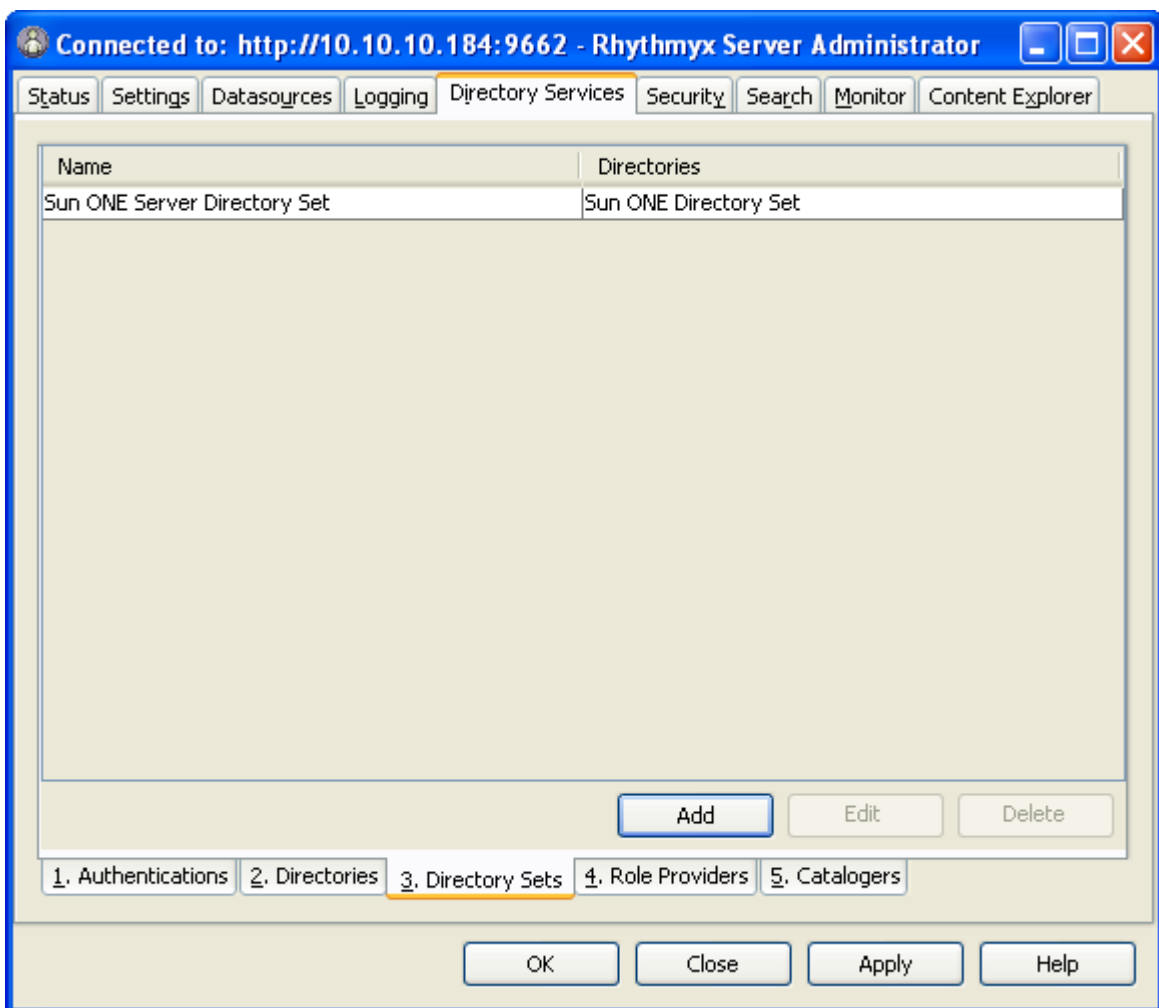


Figure 33: Directory Sets Tab

Use this tab to access dialogs to add, edit, or delete Directory Sets.

To open an existing Directory Set configuration:

- double-click on the name of the desired Directory Set configuration or
- select the desired Directory Set and click the **[Edit]** button

To create a new Directory Set configuration:

- Click the **[Add]** button

The *Directory Set Editor* (on page 108) appears.

## Directory Set Editor

Use the Directory Set Editor to enter or modify Directory Set configuration data.

To open an existing Directory Set configuration:

- double-click on the name of the desired Directory Set configuration on the Directory Set tab or
- select the desired Directory Set on the Directory Set tab and click the **[Edit]** button

To create a new Directory Set configuration:

- Click the **[Add]** button on the Directory Set tab

The Directory Set Editor appears.

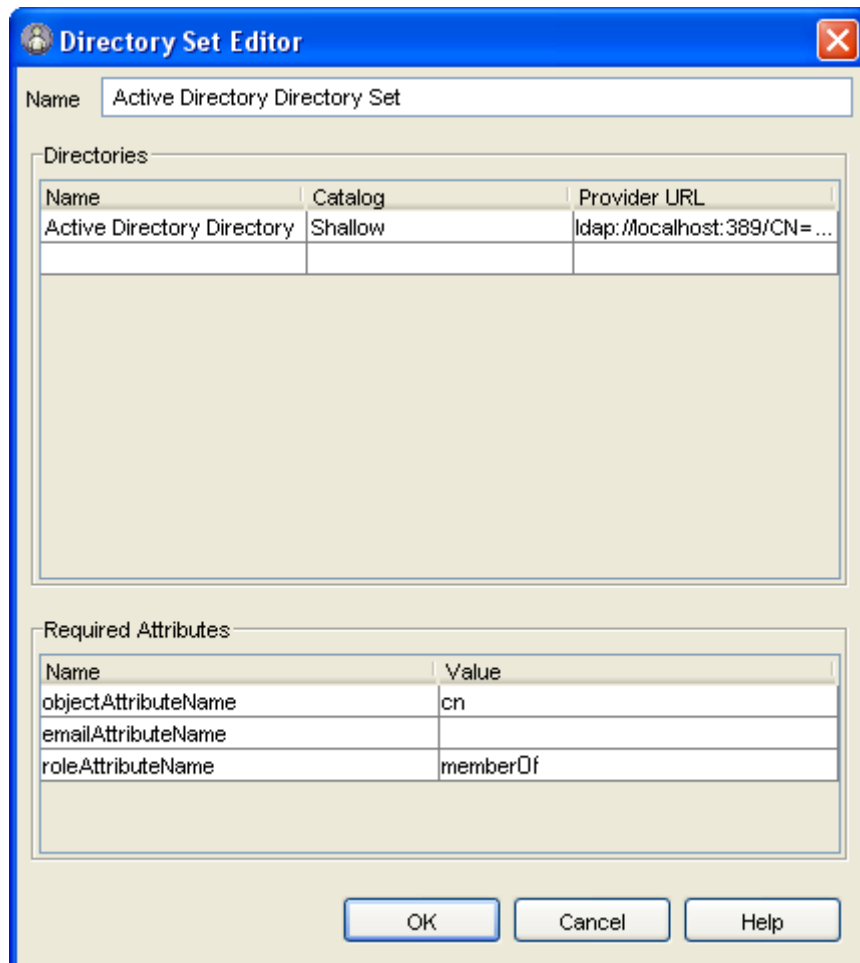


Figure 34: Directory Set Editor

### Directory Set Editor Field Descriptions:

- Name - A description of the Directory Set being registered. In this example, the screen shot shows an Active Directory Directory Set.
- Directories - A list of Directory configurations being aggregated. If a Directory configuration has not been defined for an existing Directory, (and thus does not appear in the list) double click in one of the table rows to display a drop list. Choose "New Directory..." from the drop list to open the Directory Editor and create the Directory configuration in CM System.

---

Even if only one Directory is being queried, it is necessary to define it in its own Directory Set.

---

- **Required Attributes** - Several processes within CM System require a particular attribute. These attributes must be defined for the processes to succeed.
  - **objectAttributeName** - Required. The attribute name being used during user authentication when logging into CM System. By changing the value of this attribute, it is possible to allow users to log in with any defined attribute, such as the cn or uid.
  - **emailAttributeName** - Optional. Notifications sent during Workflow Transition are sent to individual users associated with the Transition Role. By providing the emailAttributeName value used in the directory server, CM System can send notifications to these users without having to individually define their email addresses in the CM System server.
  - **roleAttributeName** - Optional. The attribute used to define a user's CM System Role. In some configurations, the directory server is used to define a user's Role in CM System. If each user has both a Functional and Community Role defined in the directory server, it is not necessary to add them to a Role in CM System. For example, the user Bobby Bluefin has the attribute rhythmyxrole defined with two values, Admin and Default, in the directory server.

rhythmyxrole	Default
	Admin

*Figure 35: Rhythmyxrole Attribute*

If the rhythmyxrole attribute is defined as the roleAttributeName in the directory set, Bobby Bluefin acquires the rights associated with those Roles when logged into CM System.

Required Attributes	
Name	Value
objectAttributeName	uid
emailAttributeName	mail
roleAttributeName	rhythmyxrole

*Figure 36: Required Attributes Area in the Directory Set Editor*

### Adding a Directory Set

To add a new Directory Set:

- 1 Log into the Rhythmyx Server Administrator and click the Directory Services tab at the top of the display.

---

A Directory Set is valid for only one CM System server. When you have multiple CM System servers, you must create separate Directory Sets for each server.

---

- 2 Click the Directory Sets tab at the bottom of the display.
- 3 Click the **[Add]** button; CM System displays the Directory Set Editor.

- 4 Complete the fields as described in the topic *Directory Set Editor* (on page 108).

**Directory Set Editor**

Name: Active Directory Directory Set

Directories

Name	Catalog	Provider URL
Active Directory Directory	Shallow	ldap://localhost:389/CN=...

Required Attributes

Name	Value
objectAttributeName	cn
emailAttributeName	
roleAttributeName	memberOf

OK Cancel Help

Figure 37: Example Directory Set Definition

- 5 Click the [OK] button when you have completed the necessary fields.
- 6 Click the [Apply] button to commit the registration to the CM System server.

### Editing a Directory Set

You can make changes to any value in an existing Directory Set.

---

If you change the name of an existing Directory Set, CM System prompts you to modify any Role Providers that reference the Directory Set to reflect the new name.

---

- 1 Log into the Rhythmyx Server Administrator and click the Directory Services tab at the top of the display.
- 2 Click the Directory Sets tab at the bottom of the display.
- 3 Select the Directory Set you want to modify and click the [Edit] button. (Alternatively, you can double-click the Directory Set name.)
- 4 Make your changes as described in the topic *Directory Set Editor* (on page 108)
- 5 Click the [OK] button to close the Editor dialog.

- 6 Click the [**Apply**] button to commit the changes to the CM System server.

### Deleting a Directory Set

When no Role Providers are using a Directory Set, the Directory Set is obsolete. You must delete obsolete Directory Sets manually.

- 1 Log into the Rhythmyx Server Administrator and click the Directory Services tab at the top of the display.
- 2 Click the Directory Sets tab at the bottom of the display.
- 3 Select the Directory Set(s) you want to delete and click the [**Delete**] button.

---

**CAUTION:** Once you click the [**Delete**] button, the removal is committed even if you do not click the [**Apply**] button or save the changes when closing the Server Administrator.

---

- 4 Click the [**OK**] button to close the Editor dialog.
- 5 Click the [**Apply**] button to commit the changes to the CM System server.

## Maintaining Role Providers

Role Providers include the information necessary to use a Directory Set to provide CM System with Role information for users. The data you define for a Role Provider includes:

- Name
- Directory Set

Creating Role Providers is optional. Use a Role Provider to maintain Roles in the directory server rather than in CM System.

---

You must create a Directory Set before you can create a Role Provider or a Security Provider.

---

### Role Provider Dialogs

Use the following Rhythmyx Server Administrator dialogs to set up a Role Provider.

- *Role Providers tab* (on page 112)
- *Role Provider Editor* (on page 113)

The topics for these two dialogs provide a description of what the dialogs contain and how to navigate to them. The procedures for adding, editing, or deleting Role Providers are in these topics:

- *Adding a Role Provider* (on page 113)
- *Editing a Role Provider* (on page 114)
- *Deleting a Role Provider* (on page 114)

### Role Providers Tab

The Role Providers tab lists any existing Role Providers. When shipped, CM System does not contain any predefined Role Providers except for the internal rxmaster Role Provider. (This Provider is not displayed in the Role Providers dialog). The display shows the Role Provider's name and type.

Navigate to the Role Providers tab by logging into the Rhythmyx Server Administrator, clicking the Directory Services tab, and then clicking the Role Providers tab at the bottom of the display.

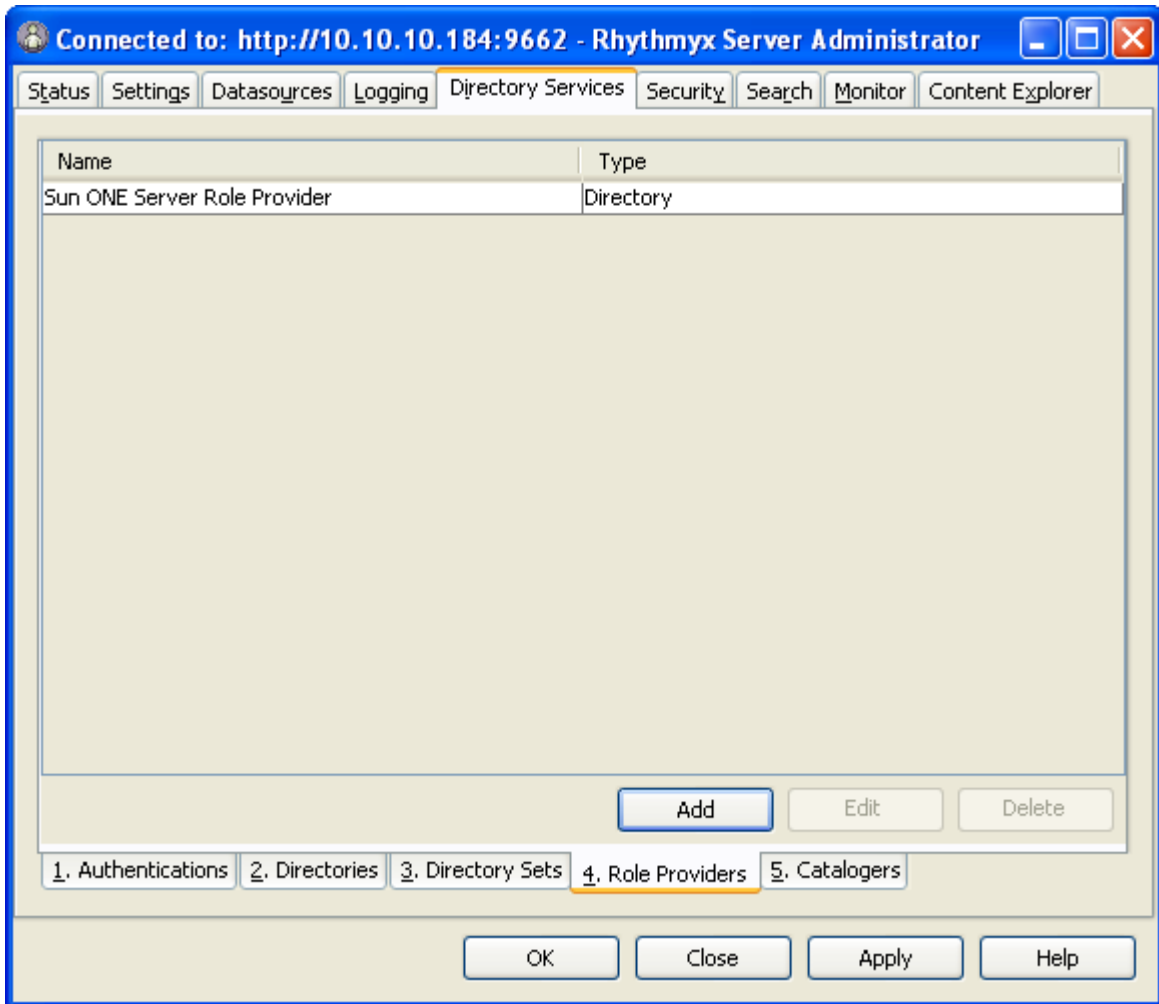


Figure 38: Role Providers Tab

Use this tab to access dialogs to add, edit, or delete Role Providers.

To open an existing Role Provider configuration:

- double-click on the name of the desired Role Provider configuration or
- select the desired Role Provider configuration and click the [**Edit**] button

To create a new Role Provider configuration:

- Click the [**Add**] button

The *Role Provider Editor* (on page 113) appears.



### Role Provider Editor

Use the Role Provider Editor to enter or modify Role Provider configuration data.

To open an existing Role Provider configuration:

- double-click on the name of the desired Role Provider configuration on the Role Providers tab or
- select the desired Role Provider on the Role Providers tab and click the [Edit] button

To create a new Role Provider configuration:

Click the [Add] button on the Role Providers tab. The *Role Provider Editor* (on page 113) appears.

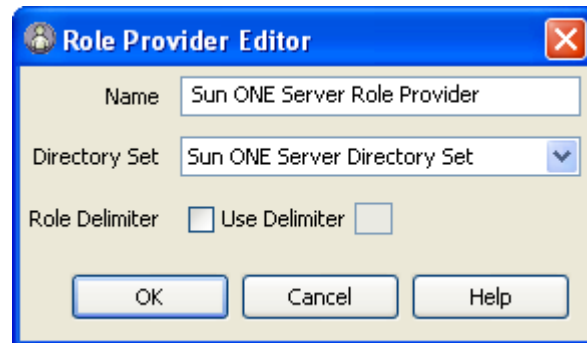


Figure 39: Example Role Provider Definition

#### Role Provider Editor Field Descriptions:

- Name - A description of the Role Provider being registered. To be consistent with the other components of the directory server configuration, we used the name Sun ONE Server Role Provider. (NOTE: The Role Provider must have the same name as the Security Provider that will use the Roles provided. If the Role Provider does not have the same name as the Security Provider, you will see the following error:

```
PSRoleCataloger 7/27/05 12:03 PM: Couldn't find a matching security
provider for role provider: RoleProvider0
```

To avoid this error, the Role Provider and the Security Provider should have the same name.)

- Directory Set - The Directory Set being used to establish the connection to the defined Role Provider. If an existing Directory Set does not appear in the drop list, select "New Directory Set..." from the drop list to bring up the Directory Set Editor and create a record for the Directory Set in CM System.
- Role Delimiter - If the LDAP attribute specified in the *Directory Set Editor* (on page 108)'s *roleAttributeName* field is a single value attribute, you must check **Role Delimiter** to instruct LDAP to use a delimiter in the attribute's value to separate multiple Role names.
- Use Delimiter - If you check **Role Delimiter**, this field becomes enabled, and you must enter the value of the delimiter to be used to separate Role names.

#### Adding a Role Provider

To add a Role Provider:

- 1 Log into the Rhythmyx Server Administrator and click the Directory Services tab at the top of the display.

---

A Role Provider is valid for only one CM System server. When you have multiple CM System servers, you must create separate Role Providers for each server.

---

- 2 Click the Role Providers tab at the bottom of the display.
- 3 Click the [**Add**] button to display the Role Provider Editor.  
The Server Administrator displays the *Role Provider Editor* (on page 113).
- 4 Enter a **Name** for the Role Provider.
- 5 Choose the **Directory Set** you want the Role Provider to use. Options include all *Directory Sets* (see "Maintaining Directory Sets" on page 105) defined in the system.
- 6 If you are using a single value LDAP attribute to specify multiple Role names, check **Role Delimiter** so that LDAP knows that multiple names are separated by a delimiter in this attribute.
- 7 If you have checked **Role Delimiter**, enter the value of the delimiter that you want to use in **Use Delimiter**.
- 8 Click the [**OK**] button when you have completed the necessary fields.
- 9 Click the [**Apply**] button to commit the registration to the CM System server.

### Editing a Role Provider

You can make changes to any value in an existing Role Provider.

---

If you change the name of an existing Role Provider, CM System prompts you to modify any Security Providers that reference the Role Provider to reflect the new name.

---

- 1 Log into the Rhythmyx Server Administrator and click the Directory Services tab at the top of the display.
- 2 Click the Role Providers tab at the bottom of the display.
- 3 Select the Role Provider you want to modify and click the [**Edit**] button. (Alternatively, you can double-click the Role Provider name.)  
The Server Administrator displays the *Role Provider Editor* (on page 113).
- 4 You can change the **Name** of the Role Provider or choose a different **Directory Set** (see "Maintaining Directory Sets" on page 105).
- 5 You can check or uncheck **Role Delimiter** and add or change the value in **Use Delimiter**.
- 6 Click the [**OK**] button to close the Editor dialog.
- 7 Click the [**Apply**] button to commit the changes to the CM System server.

### Deleting a Role Provider

When no Security Providers are using a Role Provider, the Role Provider is obsolete. You must delete obsolete Role Providers manually.

- 1 Log into the Rhythmyx Server Administrator and click the Directory Services tab at the top of the display.
- 2 Click the Role Providers tab at the bottom of the display.
- 3 Select the Role Provider you want to delete and click the [**Delete**] button.

**CAUTION:** Once you click the [**Delete**] button, the removal is committed even if you do not click the [**Apply**] button or save the changes when closing the Server Administrator.

- 4 Click the [**OK**] button to close the Editor dialog.
- 5 Click the [**Apply**] button to commit the changes to the CM System server.

## Maintaining Catalogers

Catalogers are code modules used to retrieve user and Role information from a security provider backend. Catalogers must be registered with CM System before CM System can use them.

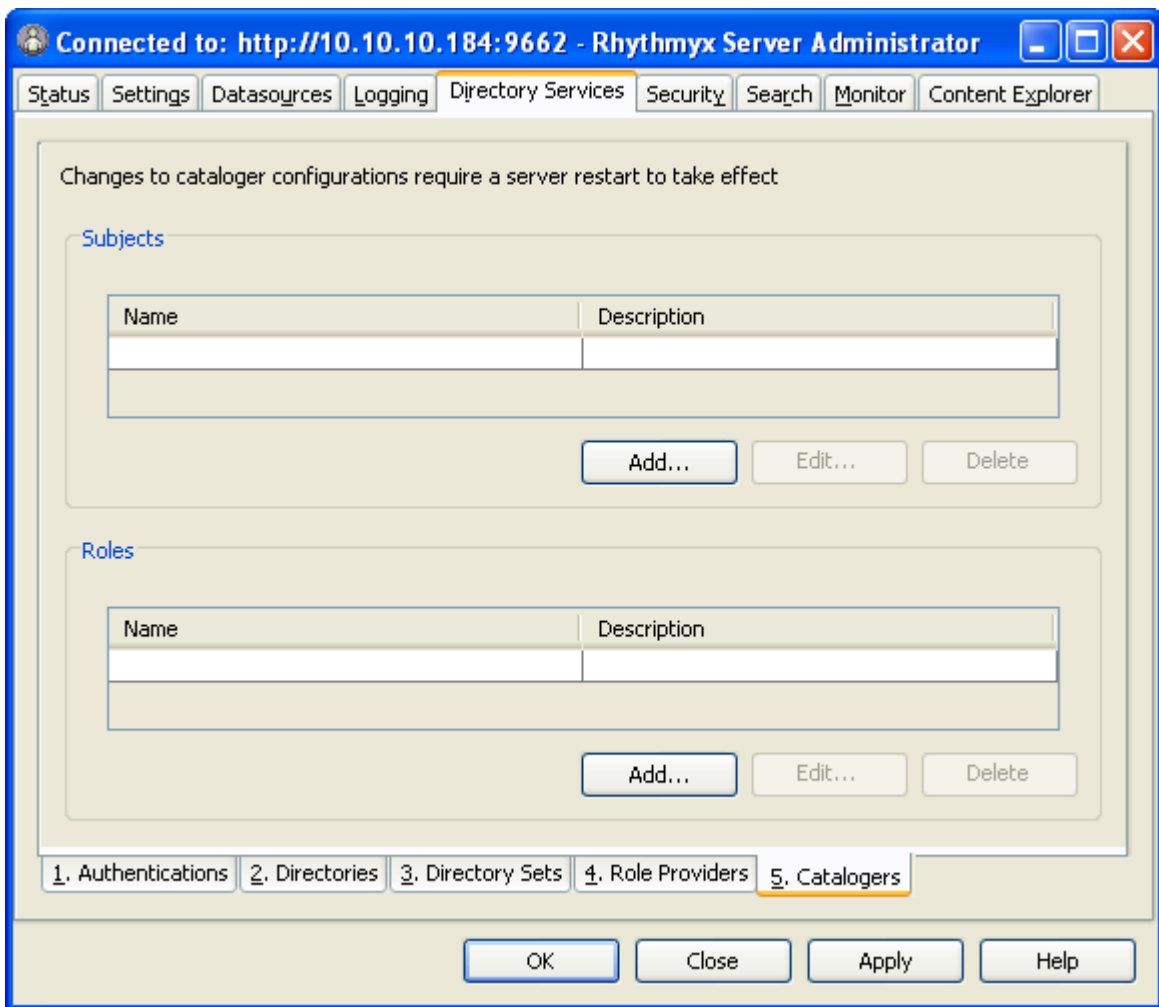


Figure 40: Catalogers Tab

You can implement two types of catalogers:

- subject catalogers retrieve data on individual users;
- role catalogers determine membership in a Role

The same dialogs and procedures are used to register both types of catalogers.

Use the *Cataloger Configuration dialog* (on page 116) to register new catalogers or to modify a cataloger registration.

You can *register a new cataloger* (see "Registering a Cataloger" on page 117), or *modify a cataloger registration* (see "Editing a Cataloger Registration" on page 117).

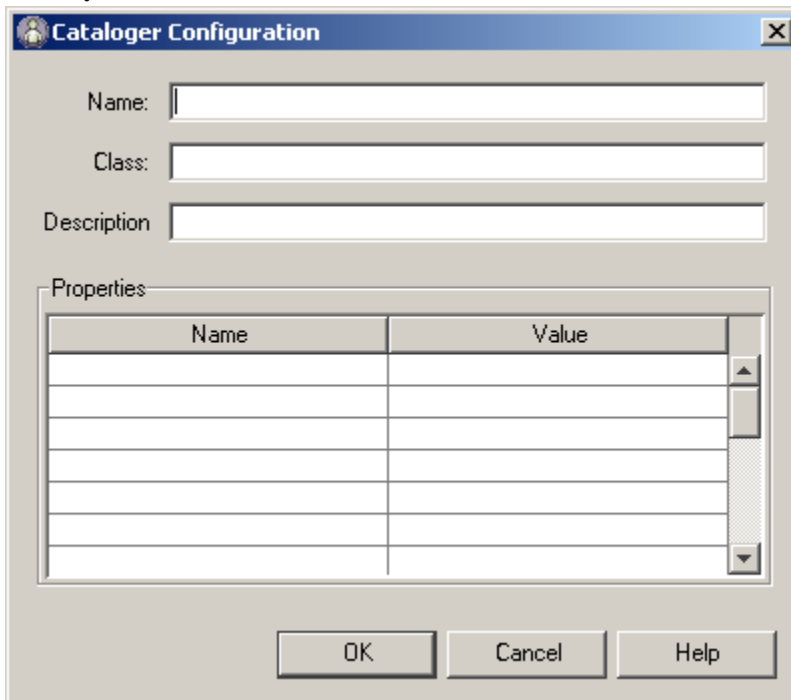
To delete a cataloger registration, select the registration you want to delete and click the **[Delete]** button.

### Cataloger Configuration Dialog

Use the Cataloger Configuration dialog to *register new catalogers* (see "Registering a Cataloger" on page 117) or to *modify the registration of an existing cataloger* (see "Editing a Cataloger Registration" on page 117).

To access the Cataloger Configuration dialog:

- on the Catalogers subtab of the Directory Services tab, click the **[Add]** button in the Subjects or Roles boxes.
- on the Catalogers subtab of the Directory Services tab, select the cataloger registration you want to modify and click the **[Edit]** button.



Name	Value

Figure 41: Cataloger Configuration dialog

### Field Descriptions

**Name** Name of the cataloger registration

**Class** Fully-qualified name of the class of the cataloger.

**Description** Free-form description of the cataloger

Properties

**Name** Name of the cataloger property.

**Value** Value of the cataloger property

### Registering a Cataloger

To register a cataloger:

- 1 On the Catalogers subtab of the Directory Services tab, in the **Subjects** or **Roles** boxes, click the **[Add]** button.  
The Server Administrator displays the *Cataloger Configuration dialog* (on page 116).
- 2 Enter a **Name** for the cataloger registration.
- 3 Enter the fully-qualified name of the cataloger **Class**.
- 4 Optionally, enter a free-form **Description** of the cataloger.
- 5 For each property of the cataloger class, enter the **Name** of the property and the **Value** of the property in the same row.
- 6 Click the **[OK]** button to save the cataloger registration.

### Editing a Cataloger Registration

To edit a cataloger registration:

- 1 On the Catalogers subtab of the Directory Services tab, select the cataloger registration you want to modify and click the **[Edit]** button.  
The Server Administrator displays the *Cataloger Configuration dialog* (on page 116).
- 2 You can modify the value in any field.
- 3 Click the **[OK]** button to save your changes.

## LDAP Configuration Examples

Now we will walk through examples of two ways of using LDAP directory services with CM System. The first example demonstrates using an Active Directory server to authenticate users. The second example demonstrates using a SunONE directory server to provide role information for CM System users.

### Example 1: Using LDAP to Authenticate Users

In this example, we allow users maintained in the corporate Active Directory server to access our CM System server. There are three users: Nancy Needlenose, Bobby Bluefin, and Tiara Tuna. Nancy and Tiara are both members of the Content Contributors group only, while Bobby is a member of the TeamCaptains group.

We do not want all members of the TeamCaptains group to have access to CM System, only Bobby. Bobby is associated with the CM System Role Admin, while the Content Contributors are members of the Author Functional Role. All are members of the Default Community Role.

We have an Active Directory server named ADServer that stores all of our user names and attributes. The Directory Service is listening on port 389. The user Bobby Bluefin is used to bind to the Active Directory Service. This user need only have the appropriate rights to catalog the directory. Bobby's user attribute is CN (CN=Bobby Bluefin) and his password is DeepSea.

We have downloaded and installed an LDAP browser to facilitate configurations. The browser allows for quick and easy confirmation of attribute, connection, and credential information. Though this is not required, it is a handy tool to have available.

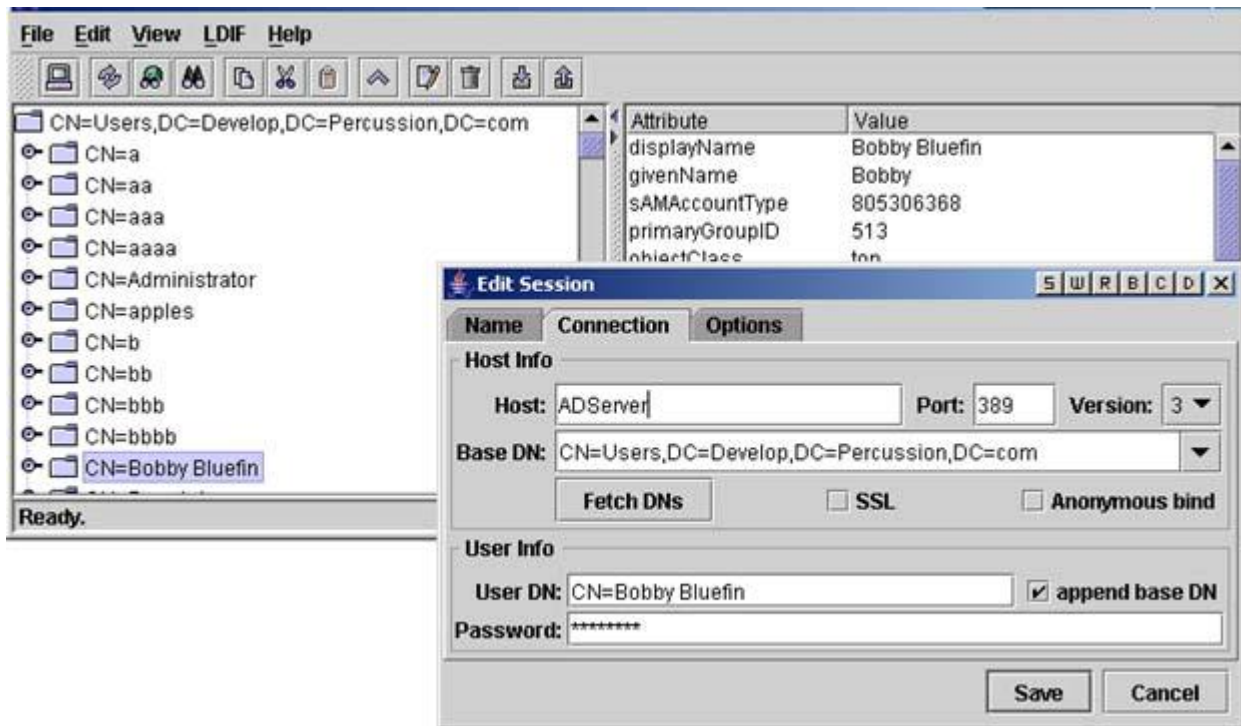


Figure 42: Using an LDAP Browser to Confirm the Configuration

## Creating the Authentication

Our first step is to create an Authentication.

- 1 Start the Server Administrator client and connect to the CM System server.
- 2 Click the Directory Services tab.

3 Click the Authentications tab.

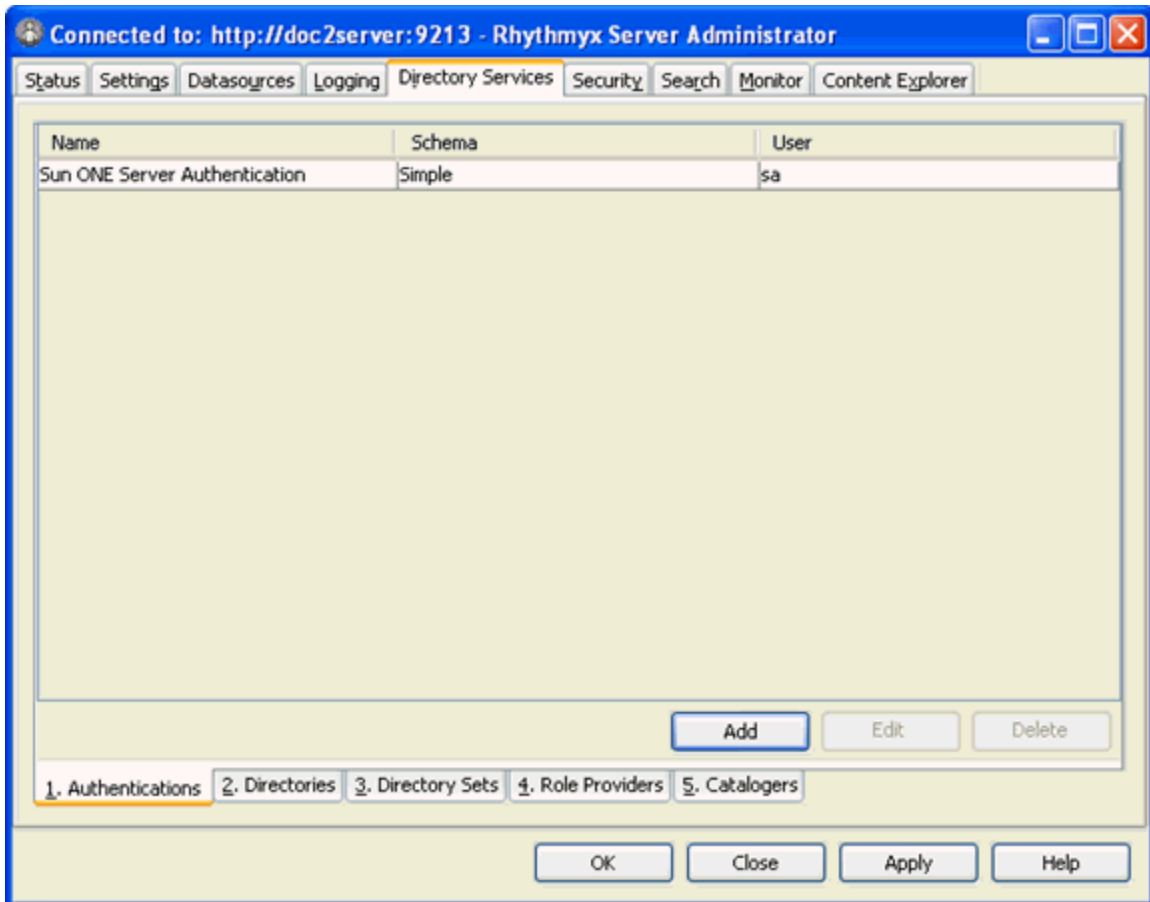


Figure 43: Authentication Tab

4 Click [Add].

- 5 If available, open an LDAP browser and create a new connection with the server information and credentials already provided.

Figure 44: LDAP Browser Showing ADServer Connection

If the credentials are correct, it should be possible to bind to and catalog the Directory.

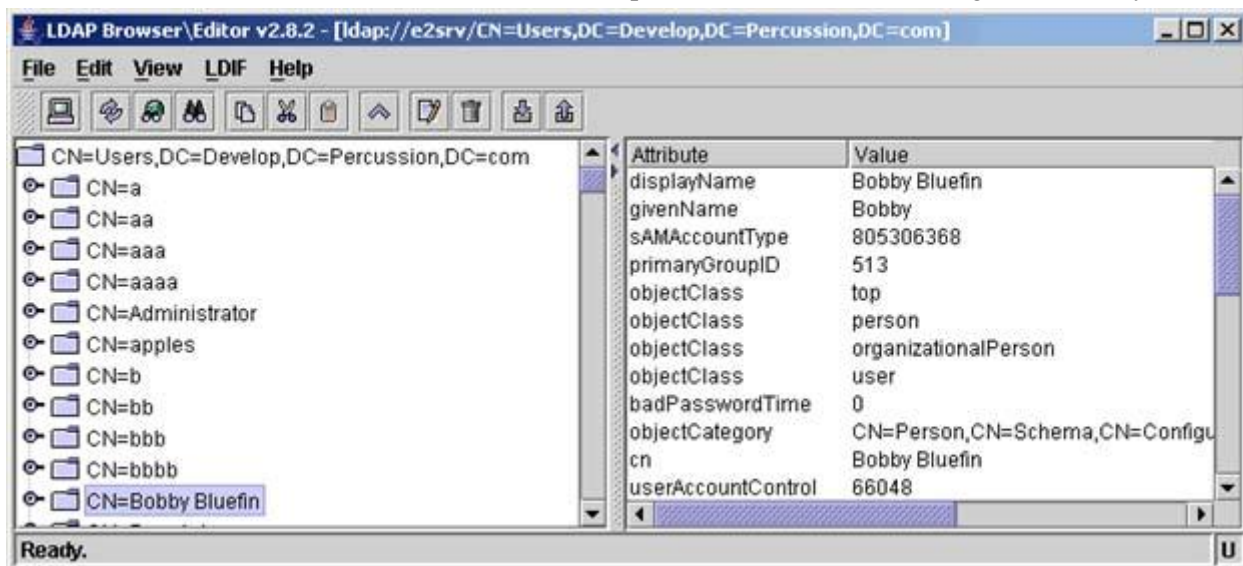
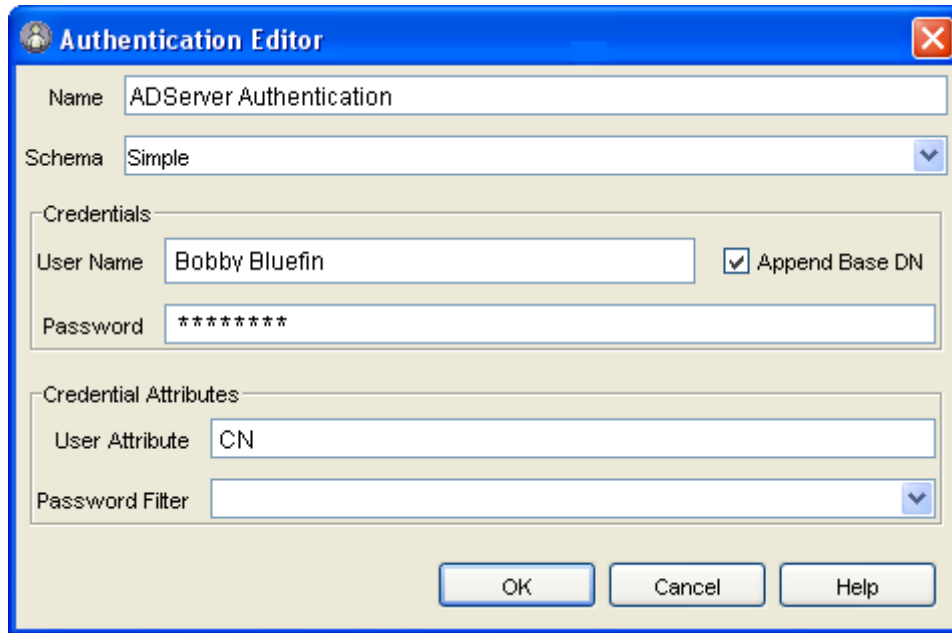


Figure 45: ADServer Directory Catalogued in LDAP Browser

The LDAP Browser is a third-party utility, which is not a part of the CM System software and is not required.



- 6 In the Rhythmyx Server Administrator's Authentication Editor, complete the fields necessary to connect to ADServer.



The screenshot shows the 'Authentication Editor' dialog box. The 'Name' field is 'ADServer Authentication'. The 'Schema' dropdown is set to 'Simple'. Under the 'Credentials' section, the 'User Name' is 'Bobby Bluefin' and the 'Password' is masked with asterisks. The 'Append Base DN' checkbox is checked. Under the 'Credential Attributes' section, the 'User Attribute' is 'CN' and the 'Password Filter' dropdown is empty. At the bottom, there are 'OK', 'Cancel', and 'Help' buttons.

Figure 46: Creating the ADServer Authentication

- 7 Click [OK] to save the new Authentication.
- 8 Click [Apply] to complete the new registration.

---

The credentials being provided in these instructions are for demonstration purposes only.

---

### Creating the Directory

Our second step is to define the Directory configuration.

- 1 Start the Server Administrator client and connect to the CM System server.
- 2 Select the Directory Services tab.

3 Select the Directories tab.

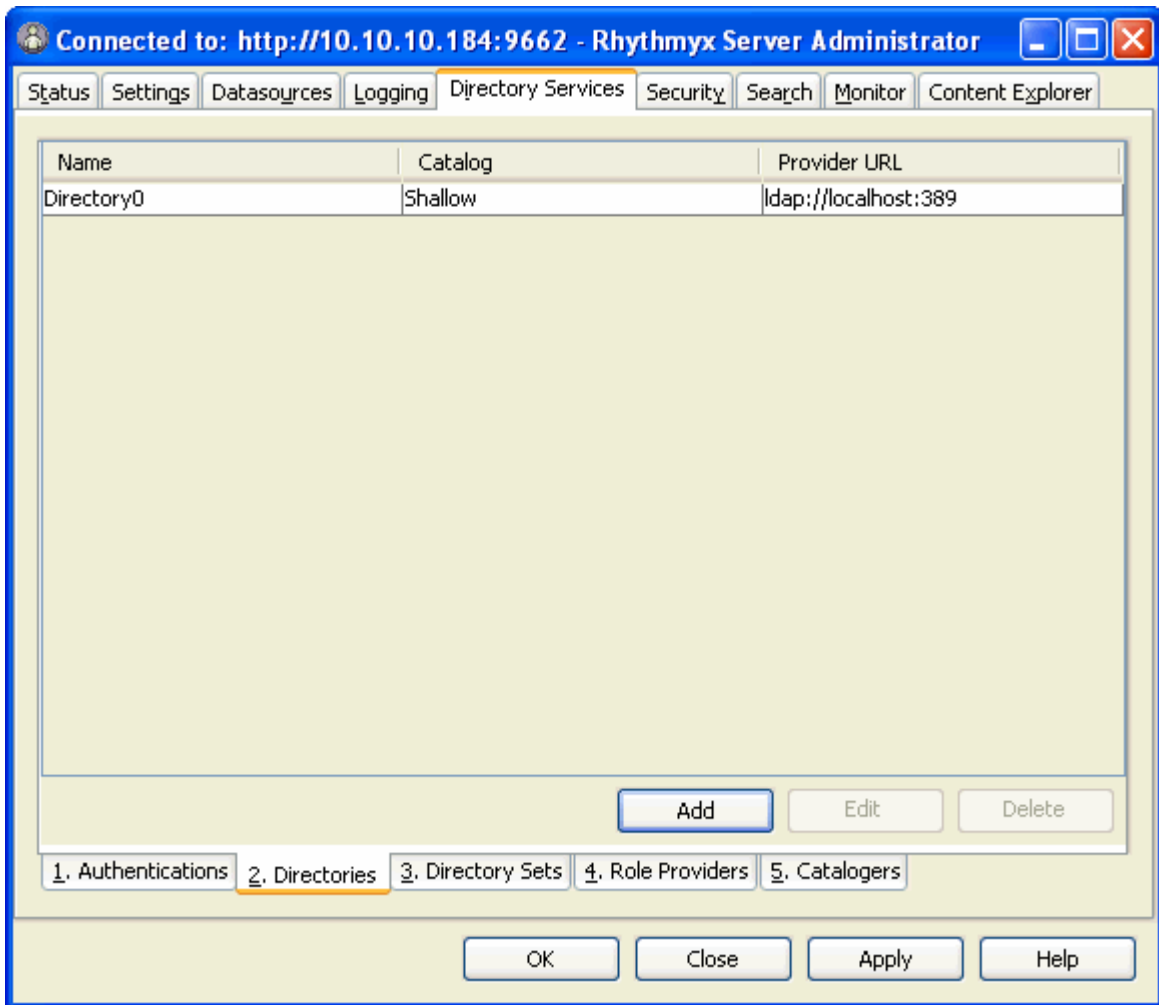


Figure 47: Directories Tab

4 Click [Add].

- 5 Using the information we confirmed in our LDAP Browser during the creation of a new Authentication, complete the Directory Editor dialog with the appropriate directory information for Name, Catalog, and Factory.

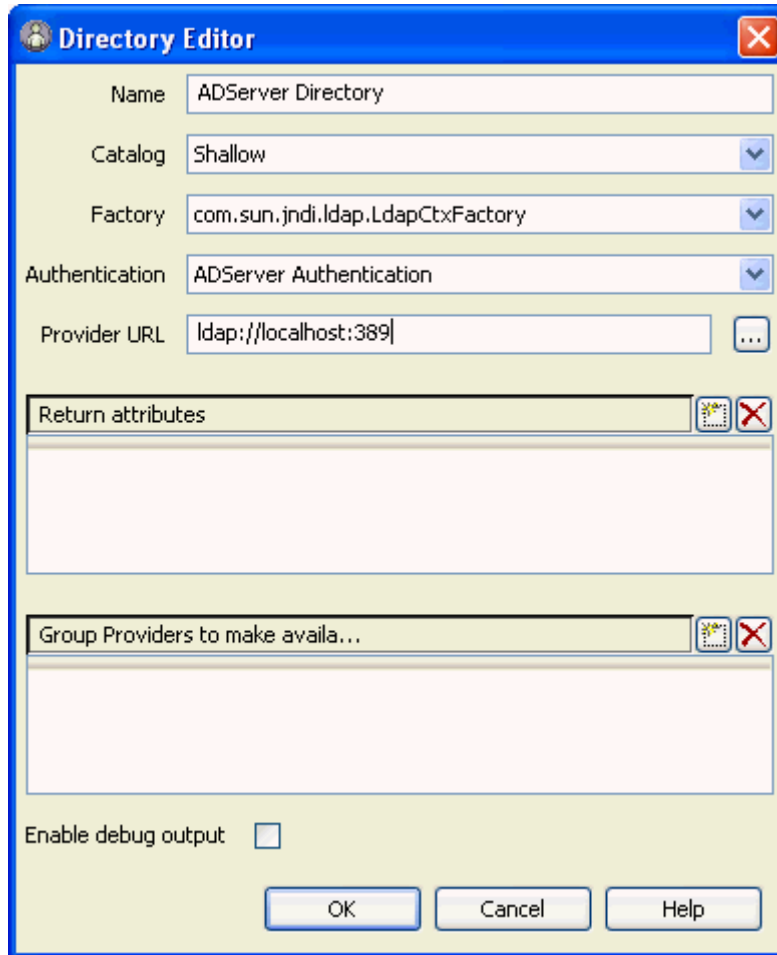


Figure 48: Adding the ADServer Directory

- 6 Choose from the Authentication drop list the ADServer Authentication created in the section **Creating the Authentication** (on page 118).
- 7 Click the ellipsis after the Provider URL field to generate the URL if you don't already know what it is. If you know the URL, enter it manually into the field.

- 8 Continue entering the data we gathered with our LDAP browser and confirm this information by pressing the catalog button to search the Base DN.

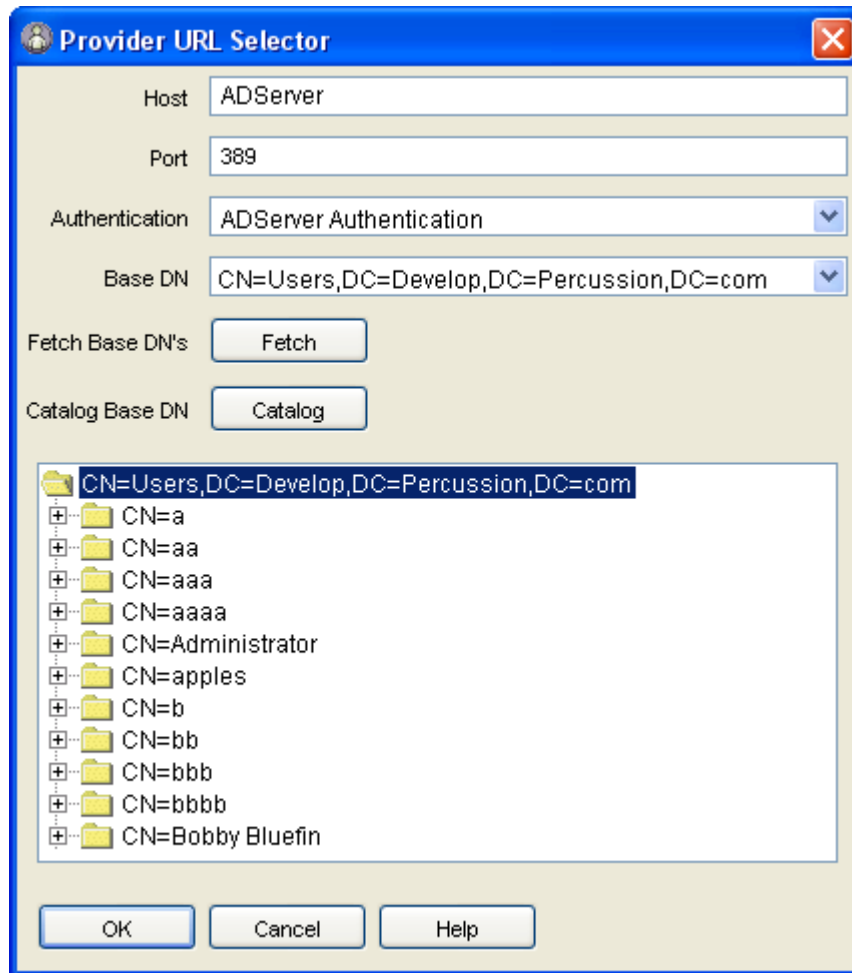


Figure 49: Provider URL Selector Dialog

---

CM System will not be able to Fetch the appropriate Active Directory Base DN. This will need to be provided manually. The example above catalogs the Active Directory "Users" in the develop.percussion.com domain.

---

- 9 If the Base DN catalogs properly, click [**OK**] to complete the creation of the Provider URL. The result is a well-formed Directory.

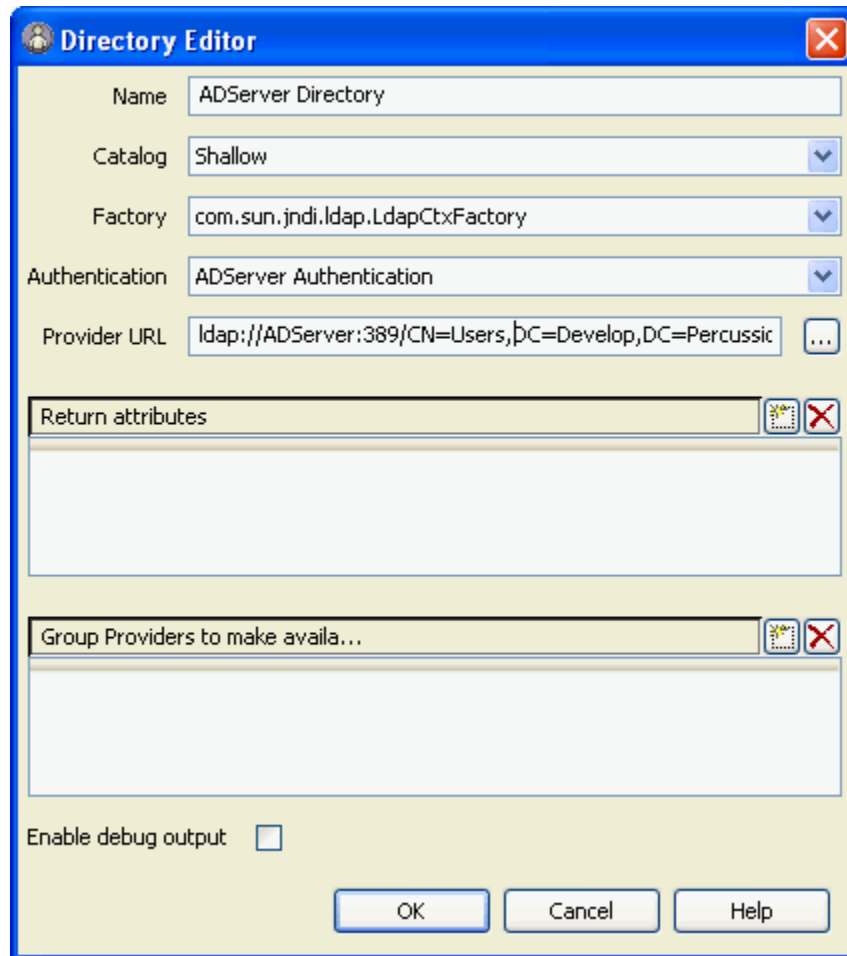



Figure 50: Directory Editor with Provider URL

- 10 If we needed to return only a limited set of attributes for our users, we would define them explicitly in the Return Attributes table by clicking the Insert New Entry button  to the right of the **Return attributes** field name. Otherwise, all attributes are returned. The format for the table entries is `directoryAttribute=mappedAttribute`. For example, if we wanted to return only each user's cn and map it to the attribute `userName`, we would add the value, `cn=userName`.
- 11 Click [**OK**] to save the Directory configuration.
- 12 Click [**Apply**] to complete the registration.

### Creating the Directory Set

The third step in creating a new LDAP connection is to define the Directory Set.

- 1 Start the Server Administrator client and connect to the CM System server.
- 2 Click the Directory Services tab.

3 Click the Directory Sets tab.

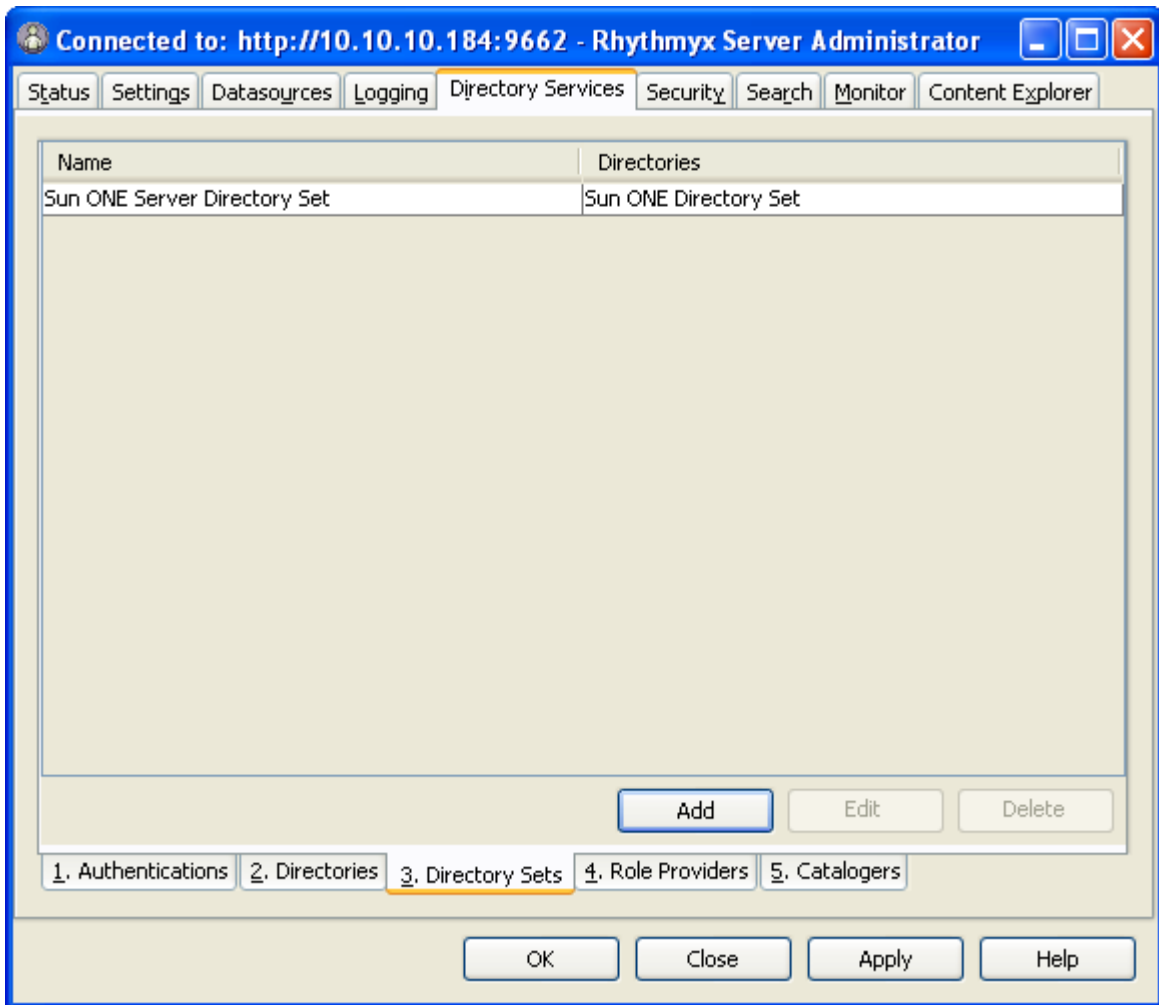


Figure 51: Directory Sets Tab

- 4 Click [Add].
- 5 Click the right-hand corner of the table below the Name column to display the existing Directories. Select our previously registered ADServer Directory entry.
- 6 We must next decide on the attribute users will use to log into CM System. Some of the available attributes in Active Directory are:

Attribute	Example Value
cn	Bobby Bluefin
userPrincipalName	BBluefin@develop.percussion.com
givenName	Bobby
sn	Bluefin

- 7 To assure a unique user id, we use userPrincipalName as the objectAttributeName. This will also be used to mine the user's email address and use it to send notifications during Workflow Transitions. We will not define a Role Attribute.

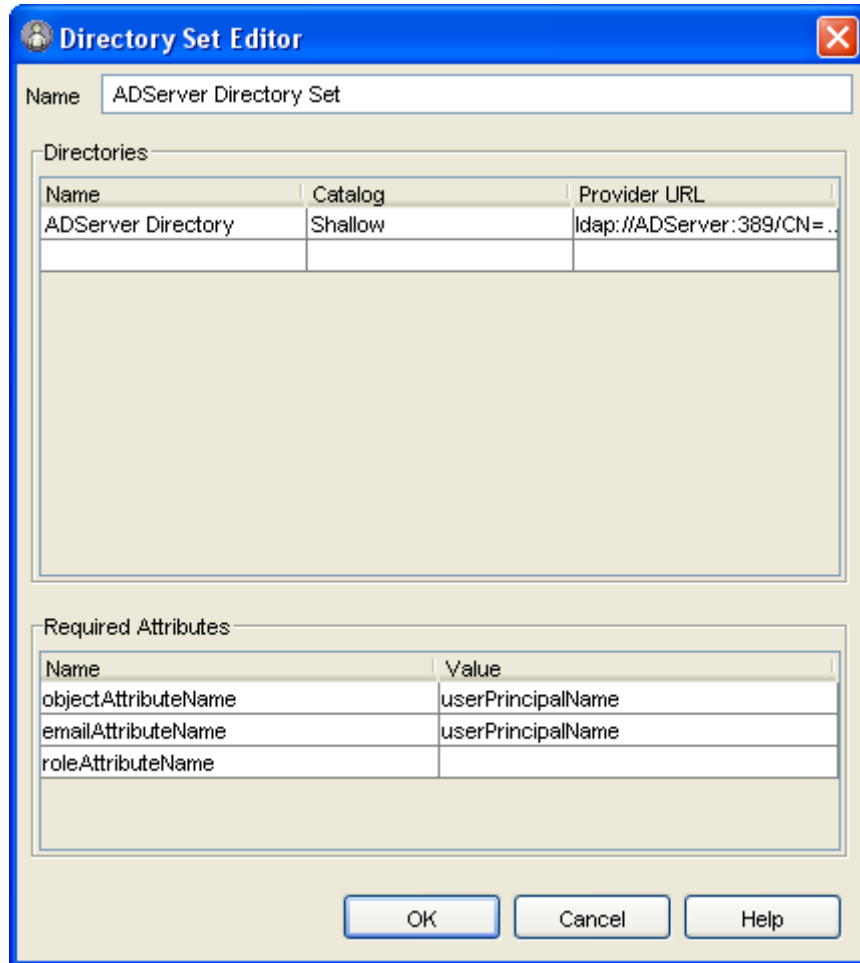


Figure 52: Directory Set Editor Dialog

- 8 When complete, click [OK] to save the new Directory Set configuration.
- 9 Click [Apply] to complete the registration.

### Creating the Security Provider

Once the Directory Set is created, it is used to define a Directory Connection Security Provider.

- 1 Start the Server Administrator client and connect to the CM System server.
- 2 Click the Security tab.

- 3 Click the Security Providers tab.

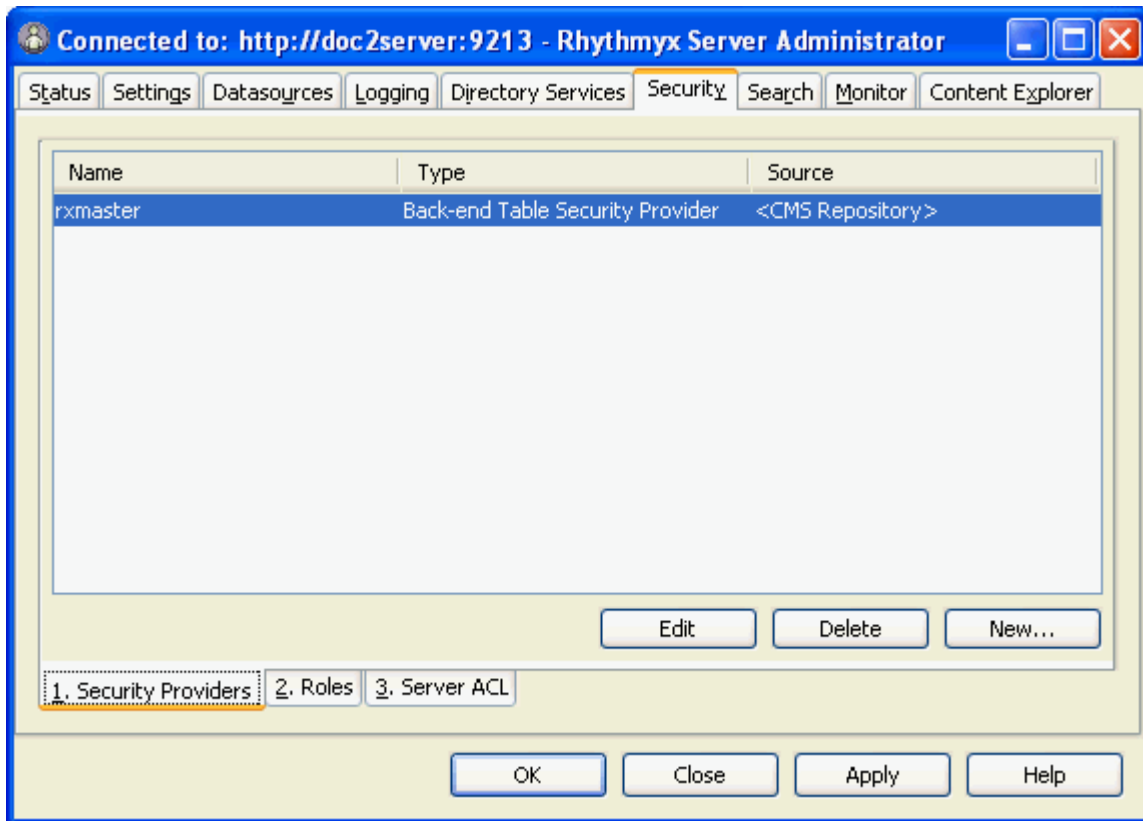


Figure 53: Security Providers Tab

- 4 Click [New].
- 5 Choose Directory Connection Security Provider from the drop list.
- 6 Click [OK].
- 7 Fill in the Provider name. Choose our previously defined ADServer Directory Set from the drop list.

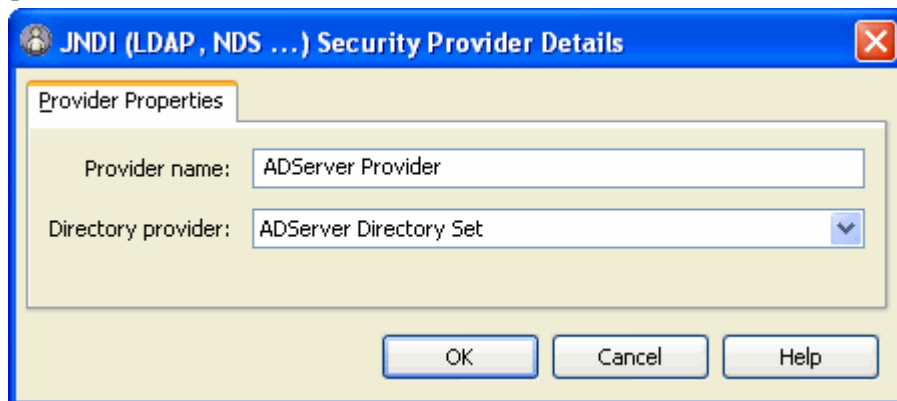


Figure 54: Security Provider Details

- 8 Click [OK] to save the Provider Properties Registration.



- 9 Click [**Apply**] to register the properties with the Provider.

### Adding a Group Provider

After we define the directory configuration, we can make a group provider available to it.

- 1 Start the Server Administrator client and connect to the CM System server.
- 2 Select the Directory Services tab.
- 3 Select the Directories tab.
- 4 Select the row for the ADServer Directory and click [**Edit**].

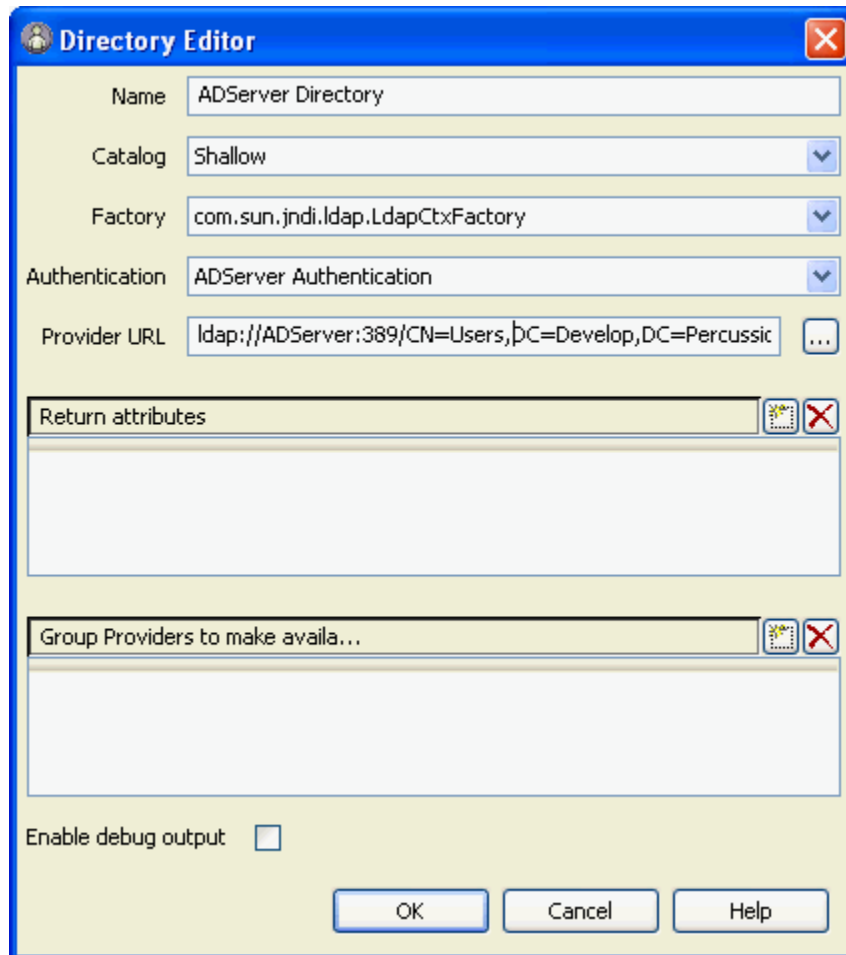




Figure 55: Directory Editor with Provider URL

- 5 Click the Insert New Entry icon  to the right of the "Group Providers to make availa..." row to display the drop list.
- 6 Choose "Create New.." from the drop list. The Group Provider Details dialog appears.
- 7 Give the new Group Provider a name. Our Active Directory example uses the default values for the objectClass, Member Attribute, and Type properties, which are in the Group Properties table. Therefore, there is no need to modify the Group Properties table.

- 8 In the "Directory Entries to Search fo..." field, click the New Entry Icon  and enter a fully qualified LDAP URL to the ADServer Active Directory Server. This URL is the same as the URL we created in the Directory configuration field Provider URL.

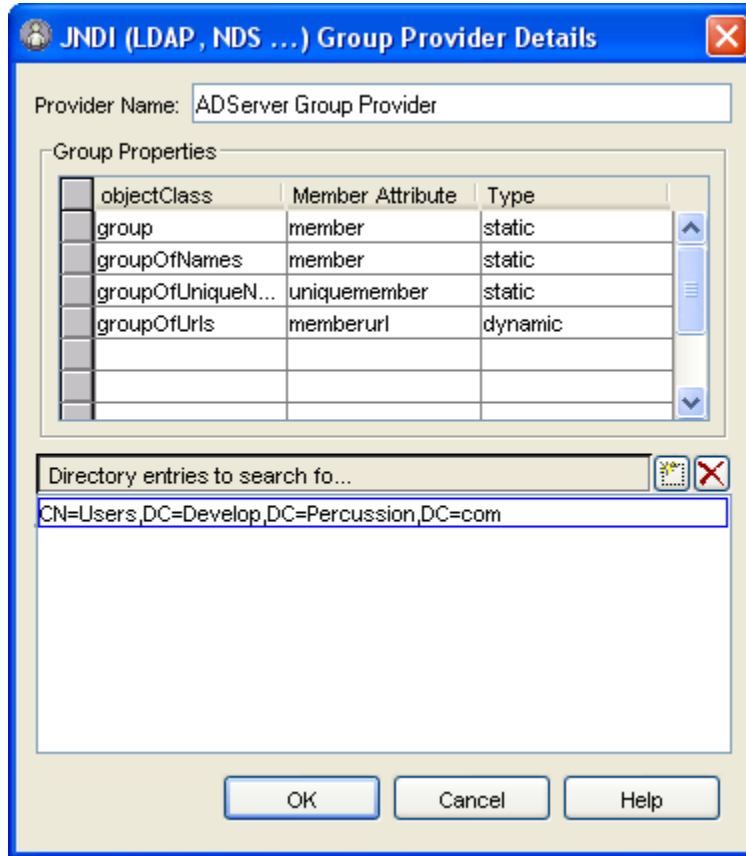


Figure 56: Group Provider Details Dialog

- 9 Click [OK] to save the Group Provider Registration.
- 10 Click [OK] to save the changes to the directory.
- 11 Click [Apply] to register the changes to the Security Provider.

### Adding Users and Groups to Roles

Once you have registered the Security Provider, you can use it to catalog users and groups. This allows you to add individual users and entire groups to both Functional and Community CM System Roles.

- 1 Start the Server Administrator client and connect to the CM System server.
- 2 Select the Security tab.

## 3 Select the Roles tab.

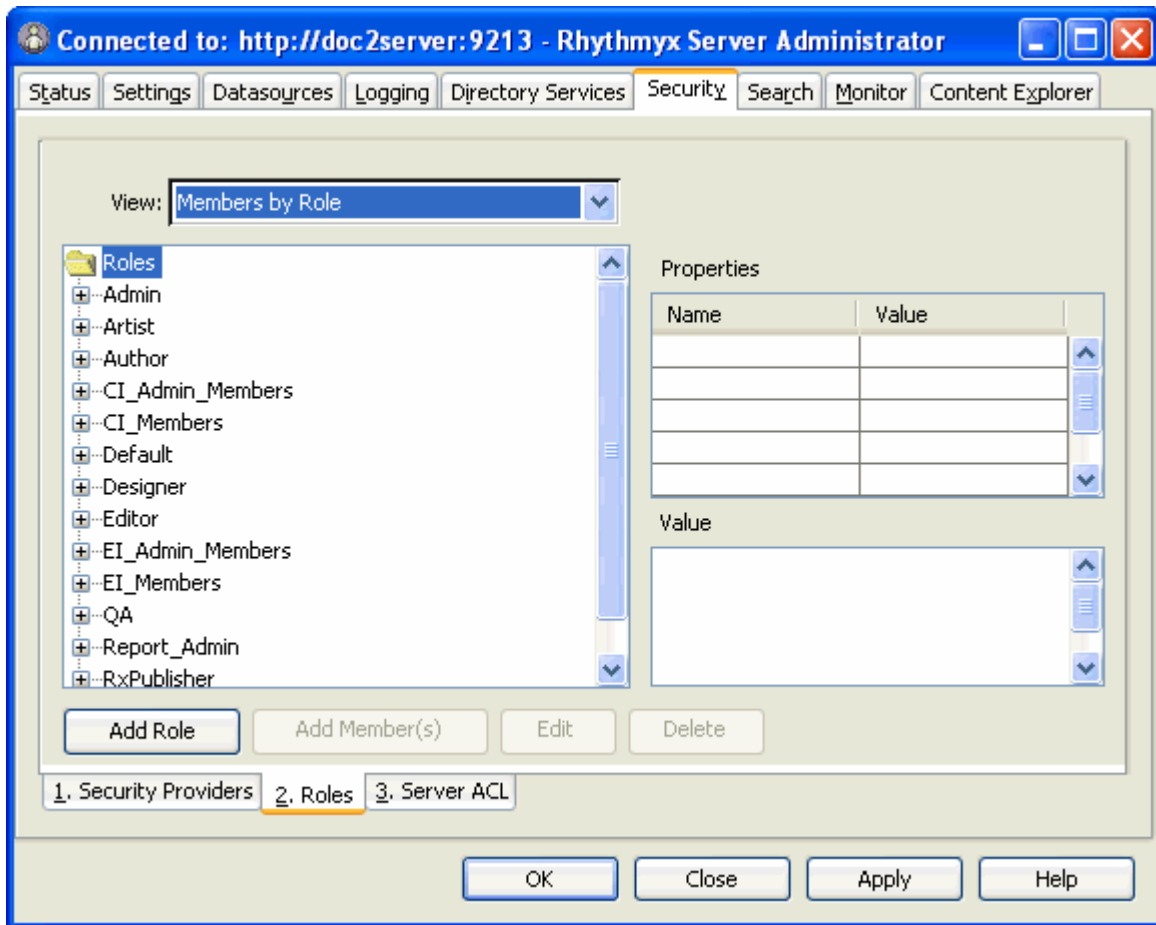


Figure 57: Adding a Role

Our original goal was to make the Content Contributors Group a member of the Author Functional Role and Default Community Role. Additionally, the user Bobby Bluefin is to be made a member of the Admin Functional Role and Default Community Role.

- 4 Select the "Default" Community Role from the list under the Roles folder.
- 5 Click the [Add Member(s)] button. The "Modify member list for: Default" dialog appears.
- 6 Click the Provider field drop list arrow and choose our newly created ADServer Security Provider.
- 7 To limit our search to only Bobby Bluefin and the Content Contributors group, specify the following in the Filter field: %bbluefin%;CN=Content%.
- 8 Click Both in the Type field to return results for both users and groups.

- 9 Click the **[Catalog]** button. The result of the search should be our two required objects, the user Bobby Bluefin and the group Content Contributors.

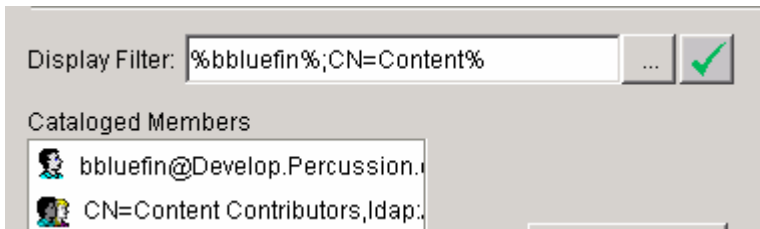


Figure 58: Result of Filtered Search on ADServer Directory Server

- 10 Select both cataloged members and click **[Add]** to add them to the Default Role.

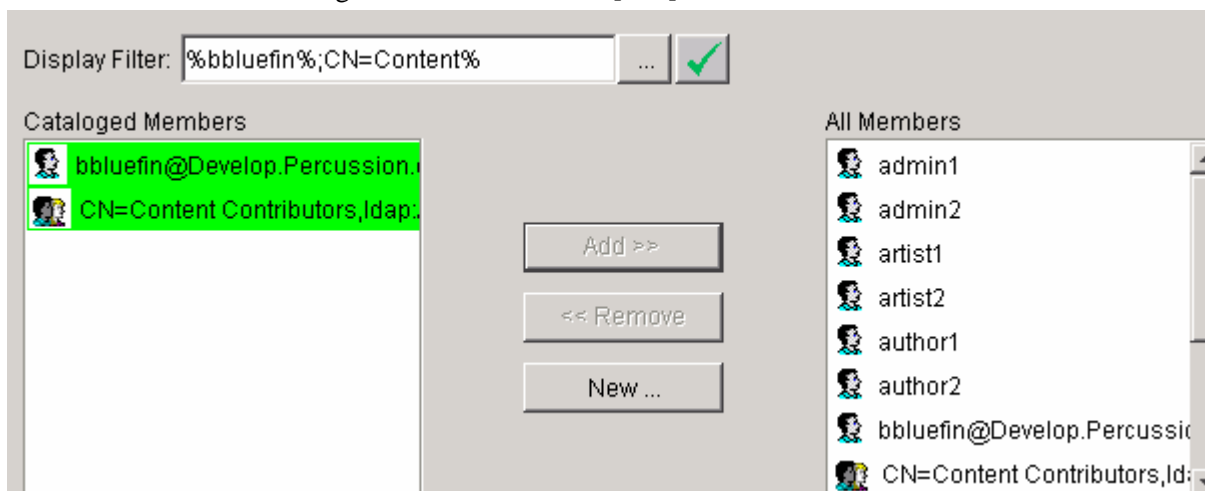


Figure 59: Cataloged Members Added to Default Role

- 11 Click **[OK]**.
- 12 Back on the Roles tab, select the Admin Functional Role from the list under the Roles folder.
- 13 Click the **[Add Member(s)]** button. The "Modify member list for: Admin" dialog appears.
- 14 Click the Provider field drop list arrow and choose our newly created ADServer Directory Set/Directory Provider.
- 15 Catalog the users.
- 16 Find and select the Bobby Bluefin user. Click the **[Add]** button to add Bobby Bluefin to the Admin Role.
- 17 Click **[OK]**.
- 18 Back on the Roles tab, select the Author Functional Role from the list under the Roles folder.
- 19 Click the **[Add Member(s)]** button. The "Modify member list for: Author" dialog appears.
- 20 Click the Provider field drop list arrow and choose our newly created ADServer Directory Set/Directory Provider.
- 21 Catalog the groups.

- 22 Find and select the Content Contributors group. Click the [**Add**] button to add Content Contributors to the Author Role.
- 23 Click [**OK**].
- 24 Click [**Apply**] to commit all registrations.

At this point, you should be able to log into the Rhythmyx Content Explorer as any of the members of the Content Contributors group (ttuna@develop.percussion.com, nneedlenose@develop.percussion.com) or as Bobby Bluefin (bbluefin@develop.percussion.com).

## Example 2: Using LDAP as a Role Provider

In this example, our SunONE Directory server contains our users Bobby Bluefin, Nancy Needlenose, and Tiara Tuna. These users have a custom attribute identifier, `rhythmyxrole`, associated with their directory objects.

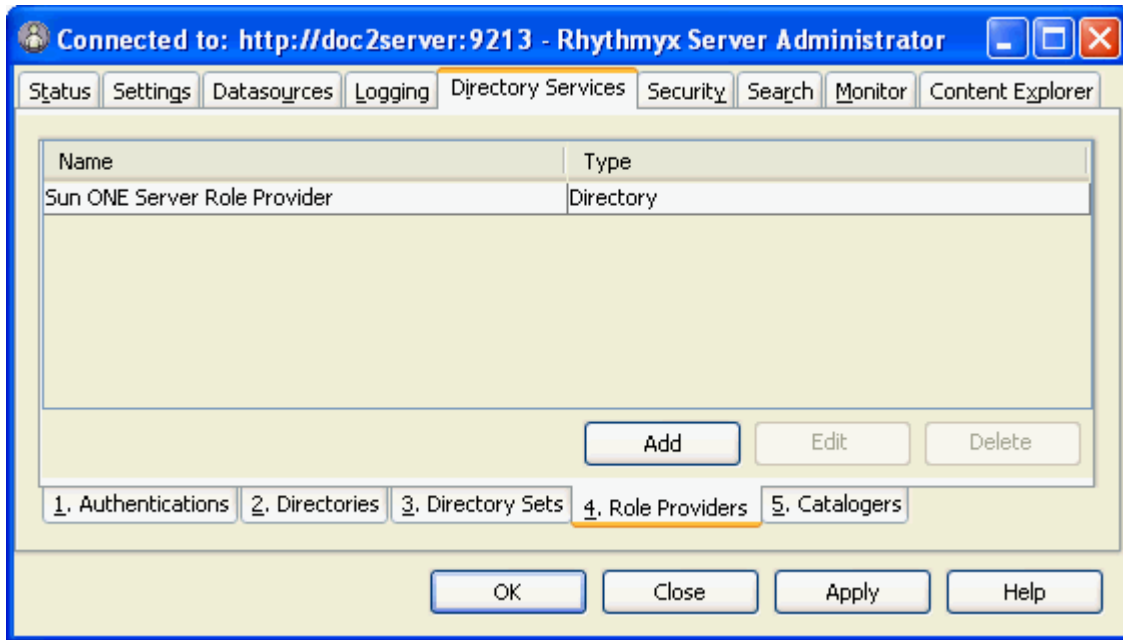
For Nancy and Tiara, the attribute values are Author and Default. Author describes their Functional Role in CM System while Default describes their Community Role. Bobby has the Admin Functional Role and the Default Community Role.

---

Though we will not map these directory objects directly to CM System Roles, the attribute values used to define each user's Role must exist as defined Roles in CM System. Using LDAP as a Role Provider does not generate a list of Roles to be used in CM System; instead, defining LDAP as a Role Provider implies that user objects searched during a query contain attributes that correlate to existing CM System Roles. The attribute identifier used in this example, `rhythmyxrole`, is not unique and the name of this identifier is not important. What is key to this functionality is that "rhythmyxrole" is mapped to the Directory Set Required Attribute, `roleAttributeName`.

---

In the procedures in this example, we assume that the processes for configuring an Authentication, Directory, Directory Set, and Security Provider are understood. For details on these directory service configuration procedures, see *Implementing LDAP Directory Services*.



*Figure 60: Directory Services/Role Providers tab*

Since Active Directory does not give us an avenue for defining custom attribute identifiers, we will use our SunONE Directory server as our Role Provider in this example.

### Defining Role Attributes in LDAP

The key to using LDAP as a Role Provider is that each user has a set of Roles (at least one Functional and one Community) associated with their user objects (or group objects). Our user objects in LDAP have the custom attribute identifier, `rhythmyxrole`, associated with them.

rhythmyxrole	Default
	Admin

Figure 61: *Rhythmyxrole Attribute*

Good practice tells us not to simply add the custom attribute to the existing object class, `person`. Instead, we created a new object class, `rhythmyxperson` with the allowed attribute, `rhythmyxrole`, and added this class to the list of attribute values for our user object.

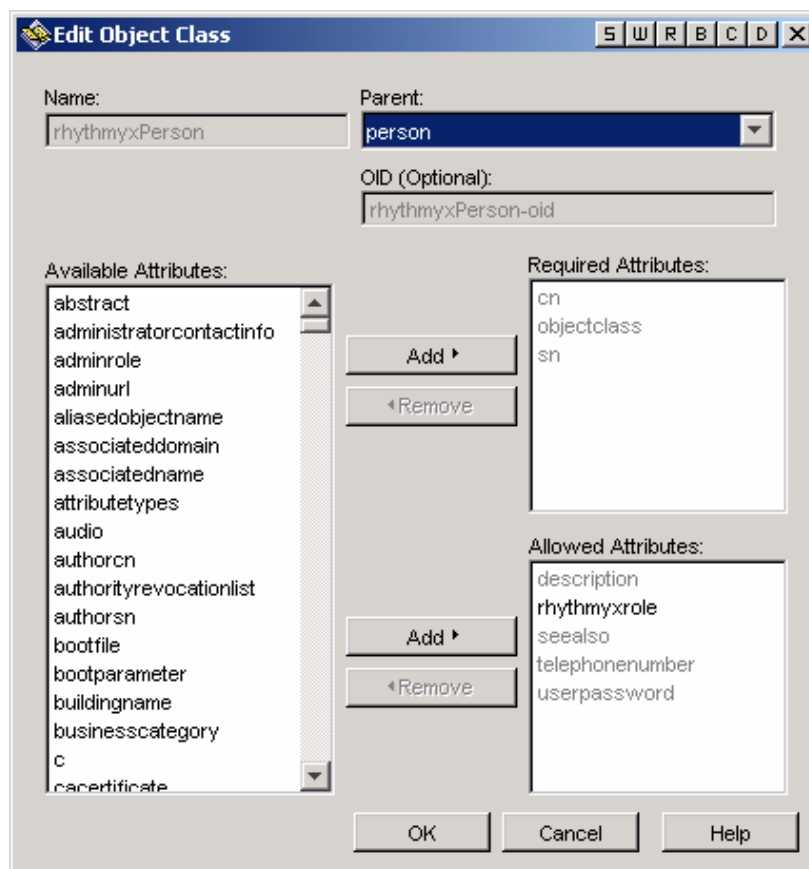


Figure 62: *rhythmyxPerson Object Class with rhythmyxrole Attribute*

Object class	top
	person
	organizationalPerson
	inetorgperson
	rhythmyxperson

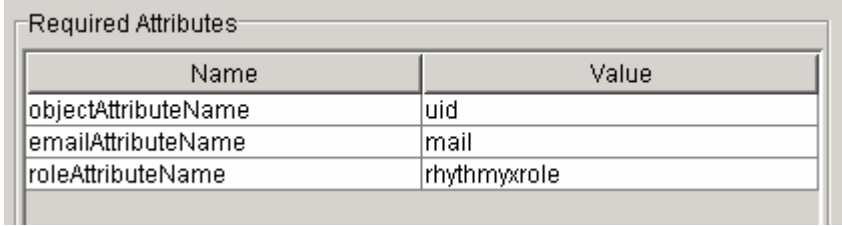
Figure 63: *rhythmyxperson Object Class Added to the User Object*

This, in turn, allowed our user object to inherit the attribute, `rhythmyxrole`. We then defined values for the `rhythmyxrole`. Each user was given a Functional and Community Role assignment.

### Creating the Directory Server Connection

We begin by creating the Authentication, Directory, and Directory Set necessary for Rhythmyx to connect to the SunONE Directory Service.

- 1 Create the Authentication, SOServer Authentication.
  - Name - SOServer Authentication
  - Schema - Simple
  - User Name - Bobby Bluefin
  - Password - DeepSea
  - Append Base DN - Leave unchecked
  - User Attribute - CN
  - Password Filter - None
- 2 Create the Directory, SOServer Directory.
  - Name - SOServer Directory
  - Catalog - Deep
  - Factory - `com.sun.jndi.ldap.LdapCtxFactory`
  - Authentication - SOServer Authentication
  - Provider URL - `ldap://SOserver:389/ou=people,dc=percussion,dc=local`
- 3 Create the Directory Set, SOServer Directory Set.
  - Name - SOServer Directory Set
  - Directories - SOServer Directory
  - Required Attributes
    - `objectAttributeName` - uid
    - `emailAttributeName` - mail
    - `roleAttributeName` - `rhythmyxrole`



Required Attributes	
Name	Value
<code>objectAttributeName</code>	uid
<code>emailAttributeName</code>	mail
<code>roleAttributeName</code>	<code>rhythmyxrole</code>

Figure 64: Required Attributes Fields in the Directory Sets Dialog



The objectAttributeName value uid allows our users to log in with their uid as it is stored in the Directory. We have mapped the value mail to the emailAttributeName to allow CM System to send messages to users at their email address as it is stored in the Directory. The key to this activity, though, is the mapping of rhythmyxrole to roleAttributeName. rhythmyxrole matches the attribute identifier associated with each user object in the Directory. Once this is defined, an authenticated user has the rights associated with their rhythmyxrole Roles.

- 4 Once the Directory Set is created, you can create the Role Provider, SOServer Role Provider.
  - Name - SOServer Role Provider
  - Directory Set - SOServer Directory Set

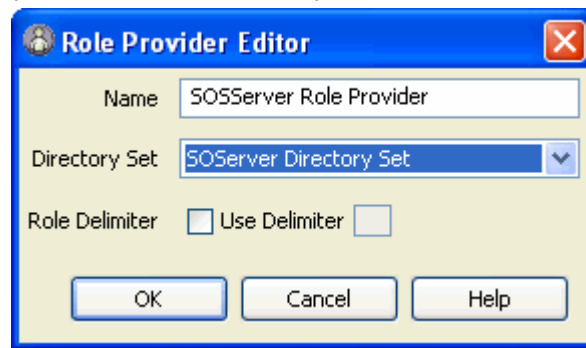


Figure 65: Role Provider Editor

### Creating the Directory Connection Security Provider

Once the Directory Set is created, you can create the Directory Connection Security Provider.

1. Create a new Directory Connection Security Provider, SOServer Directory Connection Security Provider.

- **Provider name** - SOServer Directory Connection Security Provider
- **Directory provider** - SOServer Directory Set

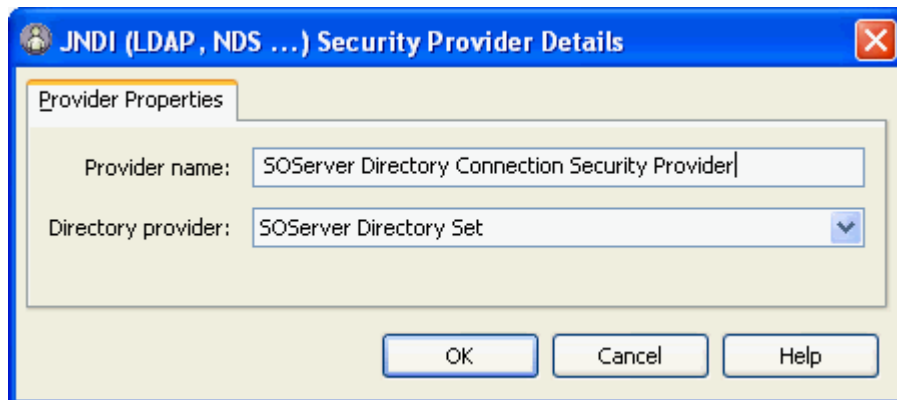


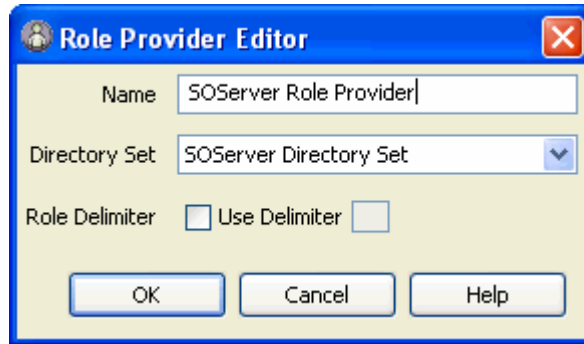
Figure 66: JNDI Security Provider Details

Once the Directory Connection Security Provider configuration is complete, create the Role Provider.

### Creating the Role Provider

Once the Directory Connection Security Provider is created, you can create the Role Provider.

- 1 Create a new Role Provider, SOServer Role Provider.
  - **Name** - SOServer Role Provider
  - **Directory Set** - SOServer Directory Set (from drop list)



*Figure 67: Role Provider Editor*

Once the Role Provider configuration is complete, users should be able to log into CM System and be assigned their corresponding Roles.

---

# Roles

A Role is a collection of users or groups of users. In CM System, Roles are used to manage access to specific applications and to manage access to content items in the Workflow.

Access to applications is granted based on the Roles to which a user belongs. Organizing users into Roles helps you manage users that have the same permissions. Instead of managing the permissions for each user, you define a Role and the permissions for it, then assign users to it. Users assigned to that Role have the permissions specified for that Role. When you assign a Role to the Access Control List of an application, the users in that Role have access to that application.

In Workflow, Roles determine which users have access to a content item and can act on it when it is in a particular State. Roles also determine which users are notified when a content item makes a Transition into or out of a State.

Each Role, and each Member in a Role, has a set of properties. Properties are defined by the administrator to provide additional options for customization. For example, a Role might have the property `sys_community`. The value of this property specifies the Community to which the members of the Role belong. CM System uses this property to implement the Communities feature, filtering the content to which the user has access, the tabs on the Content Explorer that the user can see, and the Content Types and Templates or Variants available to the user.

To maintain Roles, use the Roles tab of the Security tab in the System Administrator. Two views are available. You can view a list of Roles and the Members associated with each Role (Members by Role) or you can view a list of Members and the Roles associated with each Member (Roles by Member). Select the option you want from the **View** field.

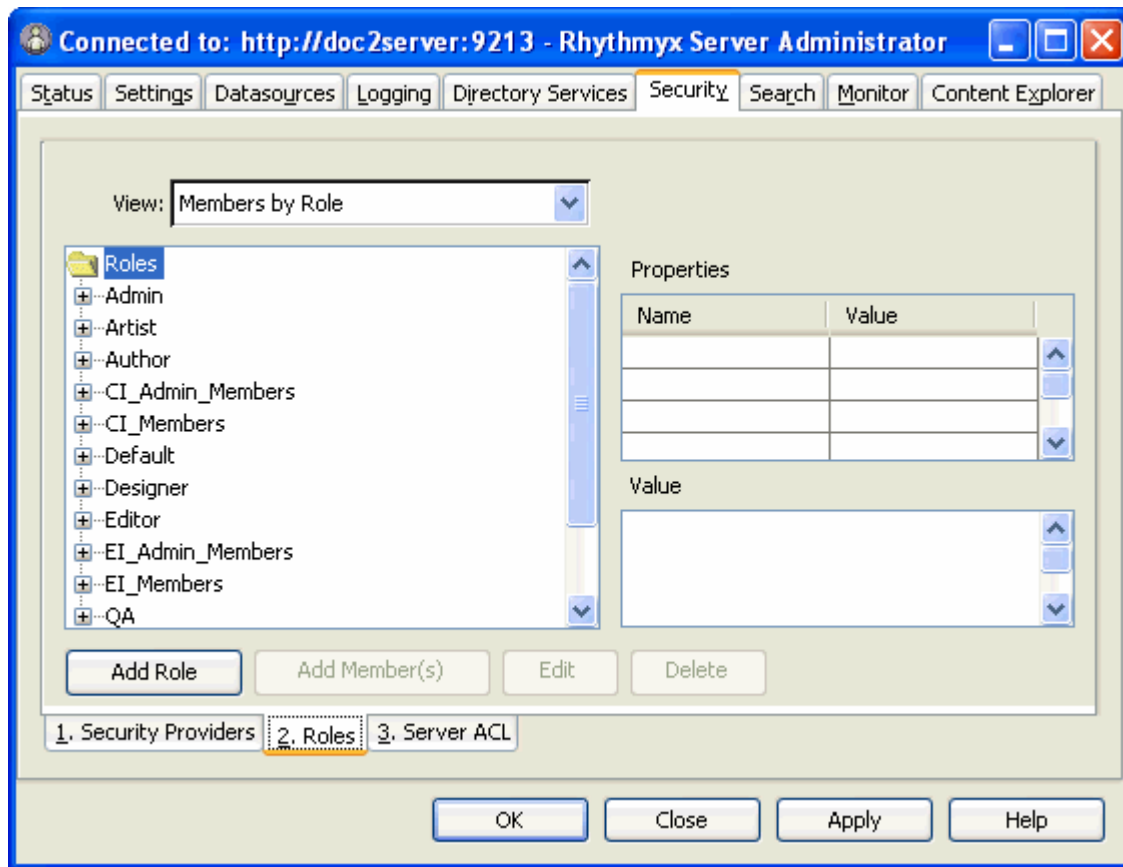


Figure 68: Roles Tab

## Default Roles and Members

CM System is shipped with the following default Roles and Members:

- Admin
  - admin1
  - admin2
  - rxserver (This is a special Member used in the Aging process. CM System uses this internal user to Transition a content item when the assigned user does not act on it within the time specified for the Transition. For more details, see "About Workflow Administrator" in the Help for the Workflow tab in Content Explorer.)
- Artist
  - artist1
  - artist2
- Author
  - author1
  - author2

- CI\_Admin\_Members
  - admin2
- CI\_Members
  - admin2
  - author2
  - editor2
  - qa2
  - rxpublisher
- Default
  - admin1
  - admin2
  - artist1
  - artist2
  - author1
  - author2
  - designer1
  - designer2
  - editor1
  - editor2
  - qa1
  - qa2
- Designer
  - designer1
  - designer2
- Editor
  - editor1
  - editor2
- EI\_Admin\_Members
  - admin1
- EI\_Members
  - admin1
  - author1
  - editor1
  - qa1

- rxpublisher
- QA
  - qa1
  - qa2
- Report\_Admin
  - admin1
  - admin2
- RxPublisher
  - rxpublisher
- Web\_Admin
  - admin1
  - admin2

---

*NOTE: If you do not have FastForward installed, the admin1, admin2, and rxserver members are listed under the Role **Admin**, and all of the members except rxserver and rxpublisher are listed under the Role **Default**. The rxpublisher member is only provided with FastForward.*

---

## Add/Edit Role Dialog

The New Role dialog and Edit Role dialog are identical, but the Name field is unavailable when the dialog is displayed as the Edit Role dialog. Users can edit the properties associated with the Role but not the name of the Role. To change the name of the Role, you must *delete the Role* (see "Deleting a Role" on page 150) and *add a new Role* with the new name.

To access the New Role dialog, click the Security tab of the Rhythmyx Server Administrator, then click Role tab. On the Role tab, click the [**Add Role**] button.

To access the Edit Role dialog, click the Security tab of the Rhythmyx Server Administrator, then click the Role tab. Select the Role whose properties you want to edit and click the [**Edit**] button.

The screenshot shows a 'New Role' dialog box with the following components:

- Title Bar:** 'New Role' with a close button (X).
- Name Field:** A text input field labeled 'Name:'.
- Properties Section:** A table with two columns: 'Name' and 'Value'. The table is currently empty.
- Edit Value Field:** A text area labeled 'Edit Value (enter multiple values one per line)' with a vertical scrollbar on the right.
- Buttons:** 'OK', 'Cancel', and 'Help' buttons at the bottom.

Figure 69: New Role Dialog

### Field Descriptions

Name - Mandatory on New Role dialog; read-only on Edit Role dialog. The name of the Role.

Properties/Name - Optional. The name of the property.

Properties/Value - Read-only. The value of the property.

Edit Value - Free-form field to enter values for the selected property. Enter each separate value on a different line.



## Modify Member List for "Role" Dialog

Use the Modify Member List for <Role> dialog to *add new members to a Role*.

To access the Modify Member List for <Role> dialog, on the Roles tab of the CM System Server Administrator, select the Role whose Member list you want to modify and click [Add Members].

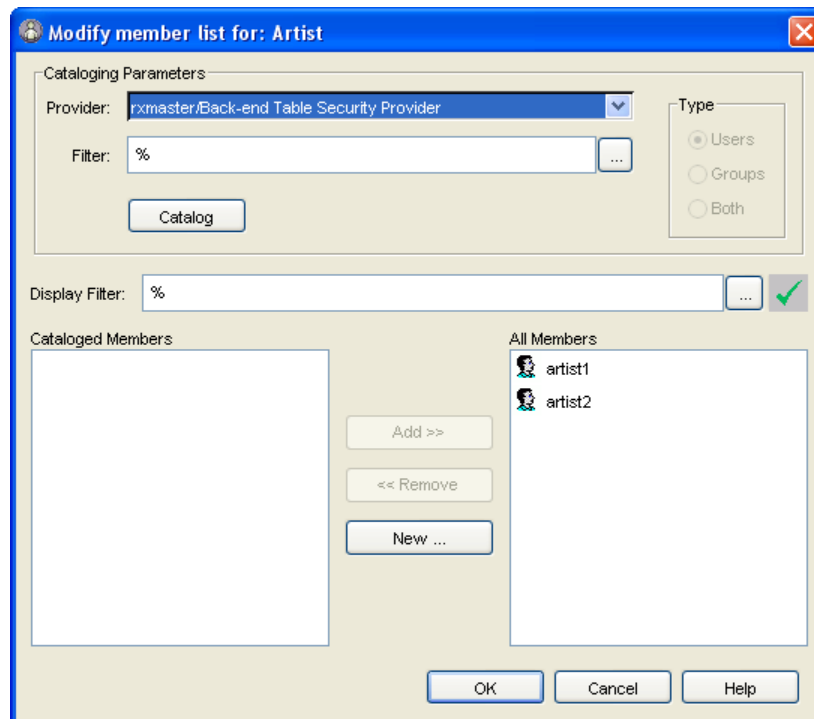

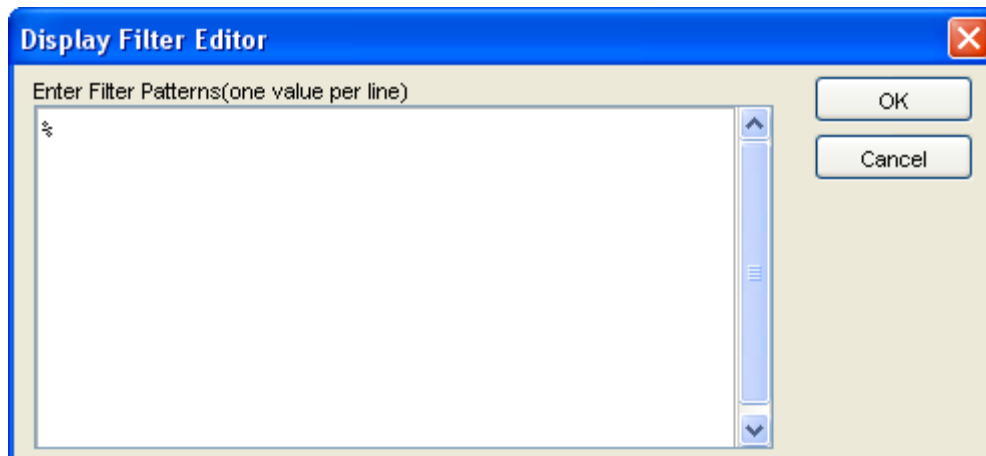


Figure 70: Modify Member List for <Role> Dialog

### Field Descriptions

**Provider** - Drop list of registered security providers.

**Filter** - Optional. Use the  button to display the Display Filter Editor dialog:



where you can enter one or more characters to use to filter the return from the security provider.

**Type** - Only editable if the Security Provider allows groups. Options are:

*Users* - The members added are users.

*Groups* - The members added are groups (collections of users managed within the security provider rather than CM System).

*Both* - The members added are users and/or groups.

**Display Filter** - Optional. This field functions in the same fashion as the Filter field, but filters only the cataloged Members displays.

**Cataloged Members** - List of Members returned from the security provider.

**All Members** - List of Members assigned to the Role.

## New Member Dialog

Use the New Member dialog to *add a new Member to a Role without cataloging the Member from a security provider*. The Edit Member Properties dialog is a variation of this dialog.

To access the New Member dialog, click [New] on the *Modify Member List for <Role> dialog*.

Name	Value
sys_email	amyadmin@percussion.com

Figure 71: New Member Dialog

### Field Descriptions

**Member Name** - Mandatory. The name of the Member you are adding to the Role.

**Provider** - Drop list. The security provider for the Member.

**Type** - Radio buttons. Indicates whether the new Member is a *Group* (collection of members managed in the security provider and outside of CM System) or an individual *User*.

**View** - Drop list. Specifies which properties you are viewing and editing. Options are Global (edit all Member properties) and Role (edit only properties associated with a specific Role).

**Role** - Drop list. Only available if the value of View is Role. The Role for which you are viewing and editing properties.

**Name** - The name of the property.

**Value** - The value of the property.

**Edit Value** - Free-form field to enter values for the selected property. Enter each separate value on a different line.

## Role and Member Properties

Role and Member properties provide a generic mechanism for storing information about users that CM System can use for processing. Properties may be associated with a Role globally (Role Properties), with individual users (Member Properties), or with individual users only within a specific Role (Role Member Properties).

In general, Role and Member properties are used either to customize interfaces or to facilitate interactions between the end-user and the CM System server. An example of a Member Property used to facilitate interaction between the server and the end-user is the Notification feature of Workflow. The user's e-mail address is defined as a Member Property, and CM System sends Notifications to this address when a content item makes a Transition into a State to which the user's Role is assigned.

## Role and Member Properties Required by CM System Functions

CM System requires that you define role properties and member properties for some of its optional features. You can define properties when you configure a *DBMS table security provider* (see "DBMS Table Security Property Details Attributes Tab" on page 83), or you can *assign LDAP attributes as properties* (see "Directory Set Editor" on page 108).

Role or Subject Property	Property Name	Function
Role	sys_defaultCommunity	Stores the name of the role's default Community. Required when you are using the default Community feature.
Role	sys_defaulthomepageurl	Stores the fully qualified or relative URL of the first CM System page that appears after login for users who log in under this role. Required when you are using the default home page feature.
Subject	sys_email	Stores the email address of the login user. Required if you are using the email notifications feature.

## Adding a New Role

To add a New Role:

- 1 In the Rhythmyx Server Administrator, click the Security tab along the top, then the Roles tab along the bottom.
- 2 Click [**Add role**].  
CM System displays the *Add Role dialog* (see "Add/Edit Role Dialog" on page 143).
- 3 Enter the Name of the new Role.
- 4 Add any Properties to the new Role. To add a property:
  - a) Click in an empty row under Name.
  - b) CM System displays a drop list of available properties.
  - c) Select the property you want to assign to the Role.
  - d) To add a value to the property, click in the same row under Value.
    - If values are pre-defined (see Maintaining Role and Member Property Names and Values), CM System will display the available properties in a drop list. Select the value you want to assign to the property.
    - If values are free-form, CM System will move your cursor to the Edit Value field, where you can enter the values. Enter each unique value on a separate line.
- 5 Click [**OK**] to save the new Role.

## Editing a Role

You can edit a Role to change the properties associated with that Role.

To edit a Role:

- 1 In the Rhythmyx Server Administrator, click the Security tab along the top, then the Roles tab along the bottom.
- 2 Select the Role whose properties you want to edit.
- 3 Click the [**Edit**] button.  
CM System displays the *Edit Role dialog* (see "Add/Edit Role Dialog" on page 143).
- 4 To add a property:
  - a) Click in an empty row under Name.
  - b) CM System displays a drop list of available properties.
  - c) Select the property you want to assign to the Role.

- d) To add a value to the property, click in the same row under Value.
  - If values are pre-defined (see Maintaining Role and Member Property Names and Values), CM System will display the available properties in a drop list. Select the value you want to assign to the property.
  - If values are free-form, CM System will move your cursor to the Edit Value field, where you can enter the values. Enter each unique value on a separate line.
- 5 To delete a property, right click on the property and select *Clear* from the popup menu.
- 6 To change the value of an existing property, click in the same row under Value.
  - If values are pre-defined, CM System will display the available properties in a drop list. Select the value you want to assign to the property.
  - If properties are free-form, CM System will display the current value of the property in the **Edit Value** field, with the cursor at the end of the last value. You can add a new value on a new line or modify or delete an existing value.
- 7 Click [**OK**] to save your changes.

## Deleting a Role

When you delete a Role, you delete all Member associations with that Role.

To delete a Role:

- 1 In the Rhythmyx Server Administrator, click the Security tab along the top, then the Roles tab along the bottom.
- 2 In the **View** field, select Members by Role.
- 3 Select the Role you want to delete. You can select multiple Roles.
- 4 Click the [**Delete**] button.
- 5 CM System displays a confirmation message. Click [**Yes**] to confirm the delete action or [**No**] to abort the delete action.

## Adding Existing Members to a Role



You can add members that already exist in a security provider to a Role. The Server Administrator includes a cataloging function that retrieves a list of users associated with a specified security provider.

To add Existing Members to a Role:

- 1 In the Rhythmyx Server Administrator, click the Security tab along the top, then the Roles tab along the bottom.
- 2 Select the Role to which you want to add Members.
- 3 Click [**Add Member(s)**].  
CM System displays the Modify Member List for <Role> dialog.
- 4 Select the security **Provider** from which you want to select Members.

- 5 Choose the Type of Member you want to add. Options are *Users* (add individual Members), *Groups* (add groups of Members managed within the security provider) or *Both* (add both individual Members and groups of Members). NOTE: Not all security providers support Groups. If the security provider you select does not support Groups, these options are not editable.
- 6 Enter an optional Filter. Use SQL syntax to define the values. Two wildcard characters are available: % matches 0 or more characters, while "\_" matches any single character. (For example, to catalog the name admin1, you would enter *admin1*. This entry would return only admin1. If you wanted to catalog all names that begin admin, you would enter *admin%*. This entry would return *admin1*, *admin2*, etc. If you wanted to return all names that begin with "ad", you would enter *ad%*. This entry would return Adams, Adkins, admin1, admin2, etc. Similarly, if you entered *ols\_n*, CM System would return Olsen, Olson, and Olsun.

Separate multiple search values with semicolons. You can also use the Catalog Filter Editor dialog to enter a filter:

- a) Click the  button.  
CM System displays the Catalog Filter Editor dialog.
- b) Enter values. Each value should be entered on a separate line.
- c) Click **[OK]** on the Catalog Filter Editor dialog.
- 7 Click the **[Catalog]** button.
- 8 CM System displays a list of Members that matches the parameters you defined. You can define a filter for this list in the Display Filter field. The same options are available for this field as for the catalog filter. Click the  button to activate the display filter.
- 9 Select the Members you want to add and click the **[Add>>]** button.
- 10 Click **[OK]** to save your edits.

## Adding New Members to a Role

To add a new Member to a Role without Cataloging:

- 1 In the Rhythmyx Server Administrator, click the Security tab along the top, then the Roles tab along the bottom.
- 2 Select the Role to which you want to add Members.
- 3 Click **[Add member(s)]**.  
CM System displays the Modify Member List for <Role> dialog.
- 4 On the Modify Member List for Role dialog, click the **[New]** button.  
CM System displays the New Member dialog.
- 5 Enter the **Member Name** of the new Member.
- 6 Choose the **Type** of new Member. Options are **Users** (individual Member) or **Group** (group of Members managed in the security provider but not managed in CM System).

- 7 Select the **Properties** you want to define. Options are *Global* (properties not associated with a specific Role) and *Role* (properties for a specific Role). If you select *Role*, you must select the Role for which you want to define properties. Options for the Role field are all Roles associated with the Member. Note that any Global property will override a property of the same name from the security provider.
- 8 To select a property, click in an empty row under **Name** and select a property from the drop list.
- 9 To add a value to a property, click in the same row under **Value**.
  - If values are pre-defined, CM System will display the available properties in a drop list. Select the value you want to assign to the property.
  - If values are free-form, CM System will move your cursor to the Edit Value field, where you can enter the values. Enter each unique value on a separate line.
- 10 Click [OK] to save the Member record.

## Editing a Member's Properties

To edit a Member's properties:

- 1 In the Rhythmyx Server Administrator, click the Security tab along the top, then the Roles tab along the bottom.
- 2 Select the Member whose record you want to edit.
- 3 Click the [Edit] button.

CM System displays the Edit Member Properties dialog (same as New Member dialog).
- 4 Select the **Properties** you want to View. Options are *Global* (view all properties) and *Role* (view properties associated with a specific Role). Note that any Global property will override a property of the same name from the security provider.
- 5 To delete a property, right click on the property and select *Clear* from the popup menu.
- 6 To change the value of an existing property, click in the same row under Value.
  - If values are pre-defined, CM System will display the available properties in a drop list. Select the value you want to assign to the property.
  - If values are free-form, CM System will display the current value of the property in the Edit Value field, with the cursor at the end of the last value. You can add a new value on a new line or modify or delete an existing value.
- 7 Click [OK].

## Deleting a Member from a Role

To delete a Member from a Role:

- 1 In the Rhythmyx Server Administrator, click the Security tab along the top, then the Roles tab along the bottom.
- 2 You have two options to delete a Member from a single Role:



- In the **View** field, select *Members by Role*, expand the Role from which you want to delete the Member, and select the Member.
  - In the **View** field, select *Role by Members*, expand the Member you want to delete from a Role, and select the Role from which you want to delete the Member.
- 3** To delete a Member from all Roles, in the **View** field, select *Roles by Member*, then select the Member you want to delete.
  - 4** Click the [**Delete**] button.
  - 5** CM System displays a confirmation message. Click [**Yes**] to confirm the delete action or [**No**] to abort the delete action.



## CHAPTER 7

# Search Configuration

The Search tab of the Rhythmyx Server Administrator includes:

- The **Full-text search sub-tab** (see page 159) allows you to enable and disable the full-text search, change the default index directory and override the default indexing interfaces.

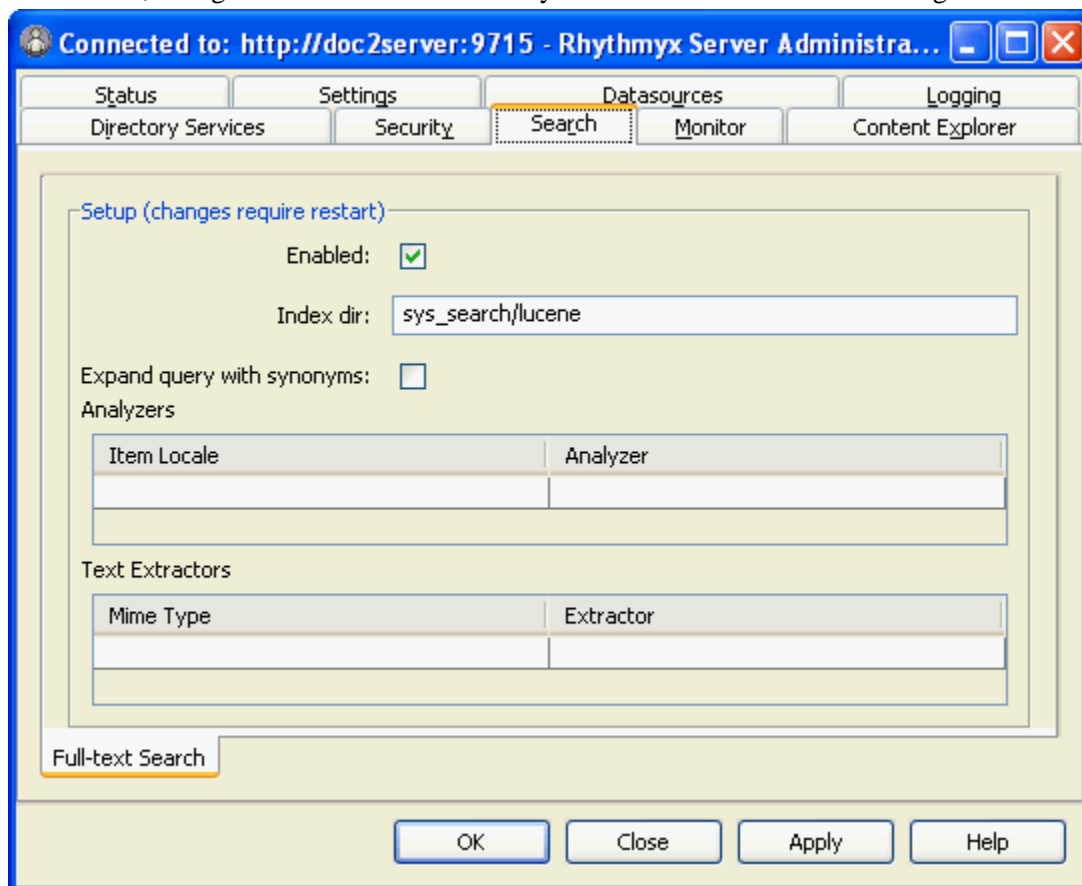


Figure 72: Search Tab

The full-text search engine is located in the CM System server, and by default, is enabled for all users. If you want your system to use the database search, disable the full-text search in this screen.

### Full Text Search Sub Tab Field Descriptions

**Enabled** - Checkbox indicating whether the full-text search engine is enabled. The default is enabled. For details see *Disabling Full-text Search* (on page 164).

**Index dir** - The location where the full-text search engine creates and reads indexes of search terms for the full-text search. The default location is <Rhythmyx root>/sys\_search/lucene. Content items are indexed to the search index when they are created or when you initiate indexing manually through a console command.

**Expand query with synonyms** - When checked, the search engine searches on words with similar meanings to the words you enter as well as matching the characters entered. Unchecked by default.

**Analyzers** - Extensions which analyze text extracted from content items and convert the text into words and phrases that are put in a search index. Text analysis might, for example, extract words and phrases, discard punctuation, and remove common words before inserting terms into an index. An analyzer works with text associated with one or more Locales.

This table does not display the out-of-the-box analyzers that the search engine uses. It is included so that you can *override the out-of-the-box analyzers* (see "How to Override the Default Text Analyzer" on page 162) or one or more Locales with your own analyzers. You can also add Locales and associate custom analyzers with them.

**Item Locale** - Content items with this Locale use the analyzer specified in this row.

**Analyzer** - Name of the analyzer that overrides the out-of-the-box analyzer for the specified Locale.

**Text Extractors** - Since the CM System search engine only indexes text strings, if content is not stored as plain text, it must be extracted from its non-text format before the search engine indexes it. A text extractor extracts text associated with a mime type.

This table does not display the out-of-the-box text extractors that the search engine uses. It is included so that you can *override the out-of-the-box text extractors* (see "How to Override the Default Text Extractor" on page 160) for one or more mime types with your own text extractors. You can also add mime types and associate custom text extractors with them.

**Mime Type** - Content items with this mime type use the text extractor specified in this row.

**Extractor** - Name of the text extractor that overrides the out-of-the-box text extractor for the specified mime type.

---

The engine for the full-text search exists within the CM System Server and cannot be moved to another location.

---

---

## Deployment Options for the Full-text Search Engine and Indices

The CM System full-text search engine is always installed on the same machine as the CM System server. However, as you add more content to your system, you may find that the full-text search indices consume an unacceptable amount of space on the CM System server's disks. In this case, you can choose to move the search indices to a different machine

Note that if you deploy the search engine indices to a separate machine, you must share or export the directory where the full-text search indices reside and map or mount this directory on the machine where the CM System server resides.

To move the full-text search indices:

- 1 Move the `/sys_search/lucene` directory to the new location.
- 2 Share/export the new directory and map/mount it on the CM System server machine.
- 3 Open the Rhythmyx Server Administrator and click the Search tab.

- 4 In **Index dir**: change the default relative path `sys_search/lucene` to the new path. You must include the full path including the drive. For example, if you moved the lucene directory to `Y:/Indexes/lucene`, the **Index dir**: field in your Search tab should appear as:

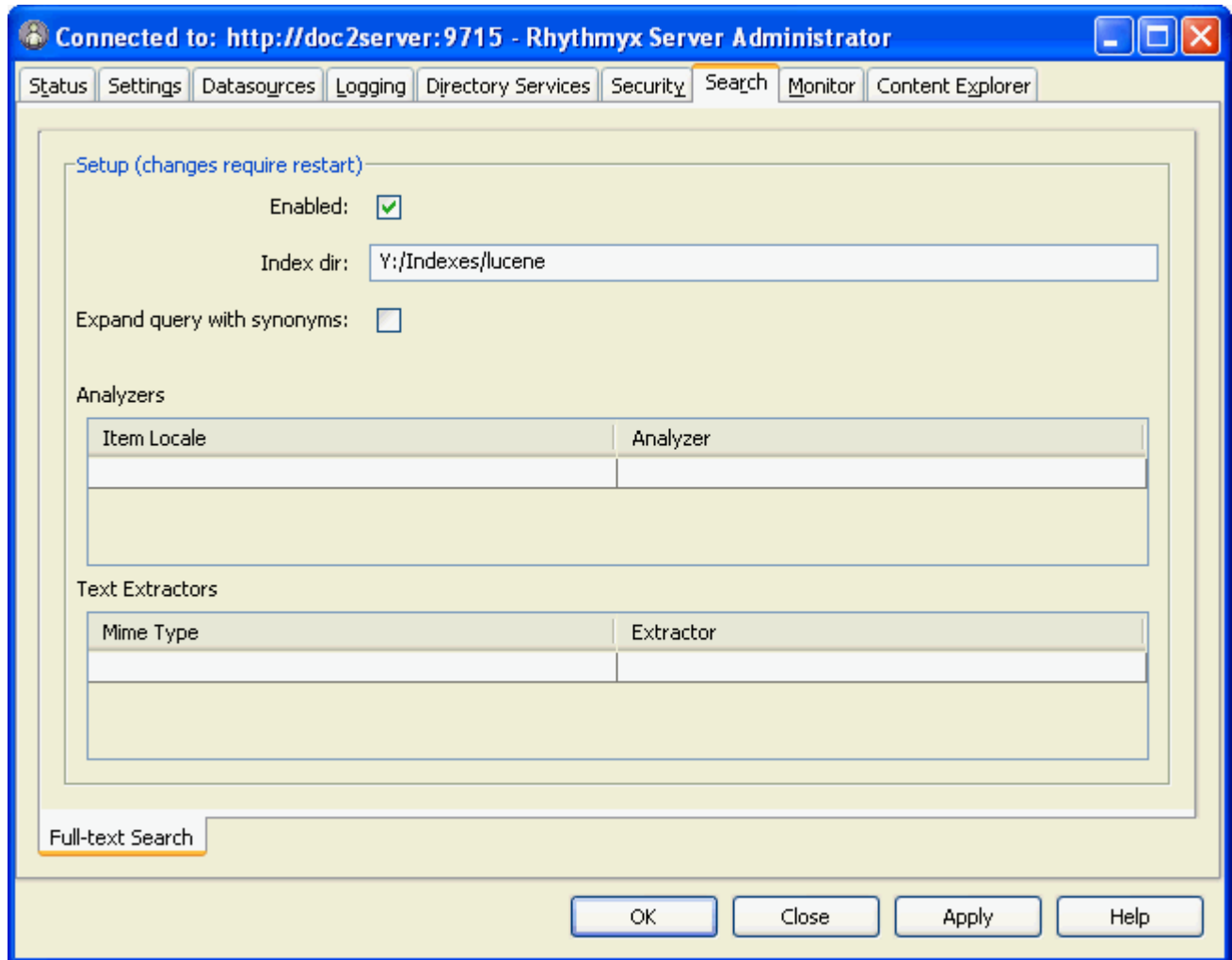


Figure 73: Changed search index directory

- 5 Click [OK] and close the Server Administrator.
- 6 Restart the CM System Server.

## Configuring the Full-Text Search

The Full-text Search sub tab allows you to enable or disable the full-text search, change the directory which stores your search index, and override the default text analyzer and text extractor extensions.

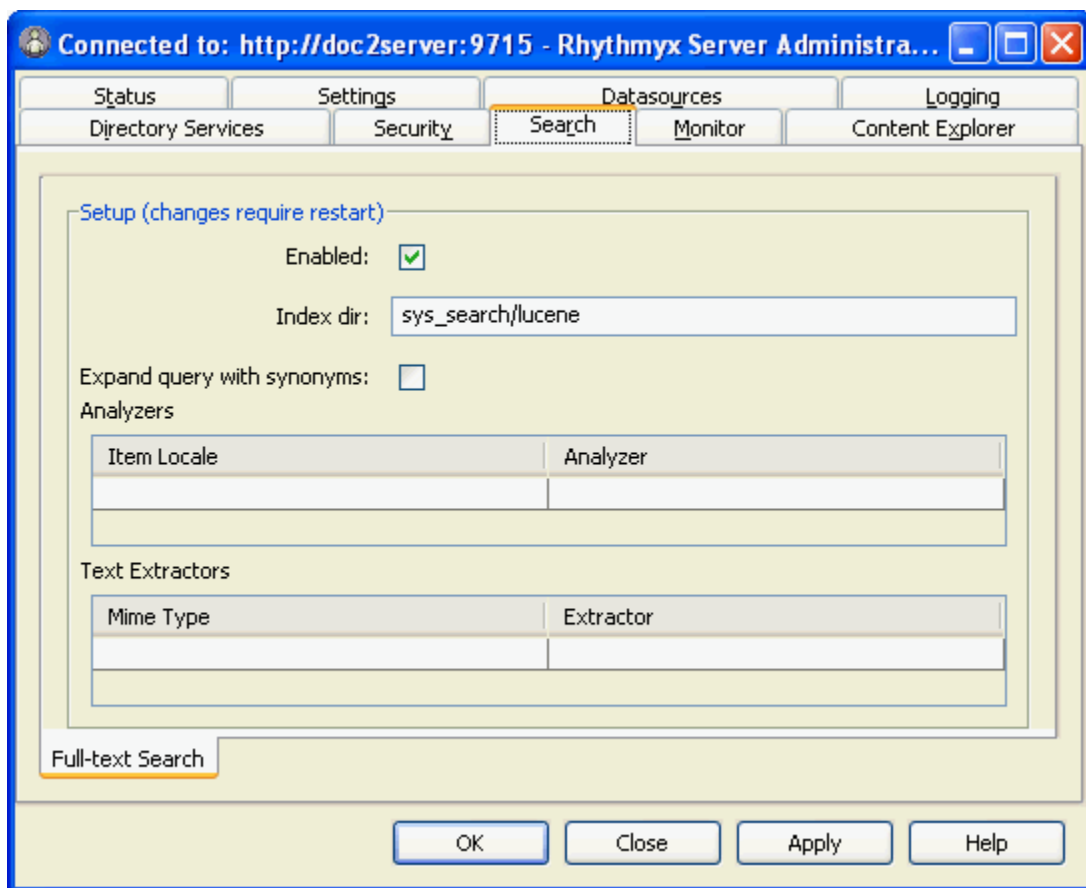


Figure 74: Search Tab

### Full Text Search Sub Tab Field Descriptions

**Enabled** - Checkbox indicating whether the full-text search engine is enabled. The default is enabled. For details see *Disabling Full-text Search* (on page 164).

**Index dir** - The location where the full-text search engine creates and reads indexes of search terms for the full-text search and for search and replace operations. The default location is <Rhythmyx root>/sys\_search/lucene. Content items are indexed to both the search index and the search and replace index when they are created or when you initiate indexing manually through a console command.

**Analyzers** - Extensions which analyze text extracted from content items and convert the text into words and phrases that are put in a search index. Text analysis might, for example, extract words and phrases, discard punctuation, and remove common words before inserting terms into an index. An analyzer works with text associated with one or more Locales.

This table does not display the out-of-the-box analyzers that the search engine uses. It is included so that you can *override the out-of-the-box analyzers* (see "How to Override the Default Text Analyzer" on page 162) or one or more Locales with your own analyzers. You can also add Locales and associate custom analyzers with them.

**Item Locale** - Content items with this Locale use the analyzer specified in this row.

**Analyzer** - Name of the analyzer that overrides the out-of-the-box analyzer for the specified Locale.

**Text Extractors** - Since the CM System search engine only indexes text strings, if content is not stored as plain text, it must be extracted from its non-text format before the search engine indexes it. A text extractor extracts text associated with a mime type.

This table does not display the out-of-the-box text extractors that the search engine uses. It is included so that you can *override the out-of-the-box text extractors* (see "How to Override the Default Text Extractor" on page 160) for one or more mime types with your own text extractors. You can also add mime types and associate custom text extractors with them.

**Mime Type** - Content items with this mime type use the text extractor specified in this row.

**Extractor** - Name of the text extractor that overrides the out-of-the-box text extractor for the specified mime type.

---

The engine for the full-text search exists within the CM System Server and cannot be moved to another location.

---

## How to Override the Default Text Extractor

In CM System, text extractors are plugins that extract text from content item fields before the text is indexed for the search engine. Each content item field is associated with a mime type, and each text extractor is associated with one or more mime types. When CM System extracts text from a field, it uses a text extractor with a mime type that matches the mime type of the field. This enables the text extractor to handle special characters and blank spaces in the text appropriately.

In some situations you may want to override CM System's default text extractors. For example:

- You may be extracting text from a file with a mime type that CM System's default text extractor supports, but you are using a version of the file that uses different characters between text strings than CM System's extractor expects. Therefore, CM System's extractor is not properly extracting text from the file.
- You may want to support text extraction for a file of a mime type that CM System's default text extractor does not support.

You can write custom text extractors and register them in the System Administrator's Full-Text Search sub-tab.

Each time that CM System extracts text from a new file, it first attempts to match the file's mime type with one of the custom extractors registered on the Full-Text Search sub-tab. If it does not find a match, it attempts to match the file's mime type with one of the default text extractors. If it still does not find a match, it attempts to find a match with one of the system's internal extractors. If a match is not found, CM System creates the item but does not index it.



To override the default text extractor:

- 1 In the Rhythmyx Workbench, open the System Design tab and add your custom extractor under the Extensions/Text Converters folder. You must select the interface: `com.percussion.search.lucene.textconverter.IPSLuceneTextConverter` for the Rhythmyx Server Administrator to include the extension in the **Extractor** drop list. For help, see the topic *Registering an Extension* in the *Rhythmyx Workbench online help*.
- 2 Open the Rhythmyx Server Administrator and click the Search tab.  
The search tab displays the Full-Text Search sub-tab.
- 3 Under the Text Extractors table, in the first available row, enter your custom text extractor.
  - a) Under **Mime Type**, choose from the drop list the mime type that your custom text extractor is associated with. (You can add additional mime types to the file `<RxRoot>/rxconfig/Server/mimemap.properties`).
  - b) Under **Extractor**, from the drop list, choose the extension name of your new text extractor.

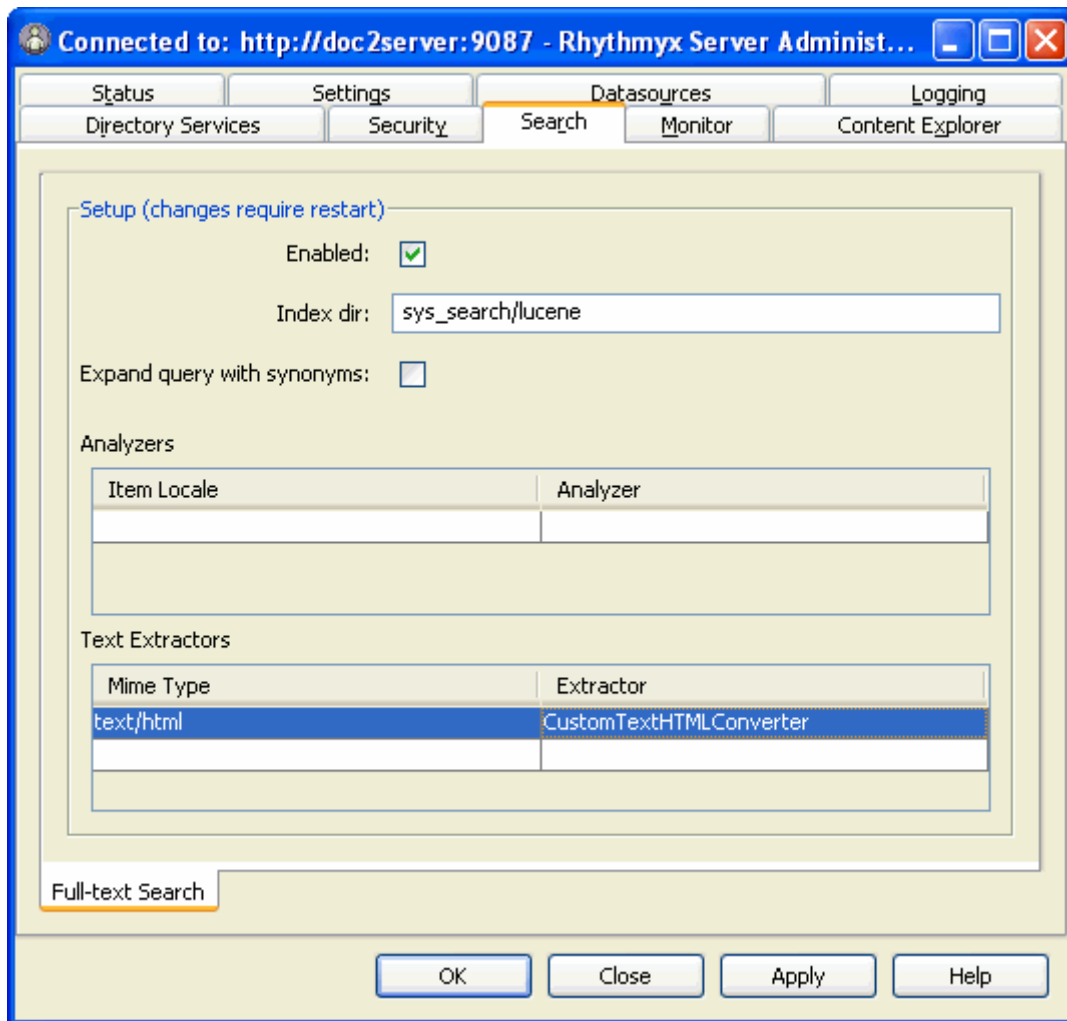


Figure 75: Search tab with custom extractor added

- 4 Click [OK] and [Close].
- 5 Restart the CM System server.

Now, CM System will first see if a file's mime type matches that of your registered extractor before attempting to match it with the out-of-the-box extractor.

For more information about the text extractors that CM System uses, see the *Technical Reference* document.

## How to Override the Default Text Analyzer

A text analyzer is a plugin that itemizes text into words and phrases for indexing after it is extracted from a file. A text analyzer must be associated with one or more languages. For more information about the text analyzers that CM System uses, see the *Technical Reference* document. In some situations you may want to override CM System's default text analyzer. For example:

- You may be analyzing text from a content item with a Locale that CM System's default text analyzer supports, but you want to leave in marks over letters that CM System's analyzer removes.
- You may want to support text analysis for content items with Locales that CM System's default text analyzer does not support.

You can write custom text analyzers and register them in the System Administrator's Full-Text Search sub-tab.

Each time that CM System analyzes text from an item, it first attempts to match the file's Locale with one of the custom analyzers registered on the Full-Text Search sub-tab. If it does not find a match, it attempts to match the item's Locale with one that the default text analyzer supports. If it still does not find a match, the system uses a standard analyzer that may or may not be effective.

To override the default text analyzer:

- 1 In the Rhythmyx Workbench, open the System Design tab and add your custom analyzer under the Extensions/Search Analyzers folder. You must select the interface:  
`com.percussion.search.lucene.analyzer.IPSLuceneAnalyzer`  
for the Rhythmyx Server Administrator to include the extension in the **Analyzer** drop list. For help, see the topic "Registering an Extension" in the *Rhythmyx Workbench online help*.
- 2 Open the Rhythmyx Server Administrator and click the Search tab.  
The search tab displays the Full-Text Search sub-tab.
- 3 Under the **Analyzers** table, in the first available row, enter your custom text analyzer.
  - a) Under **Item Locale**, from the drop list choose the Locale that your custom text analyzer is associated with. (You can add Locales to your system through the Rhythmyx Workbench. For help, see the section *Maintaining Locale Objects* in the Rhythmyx portion of the Workbench Help.)

b) Under **Analyzer**, from the drop list, choose the extension name of your new text analyzer.

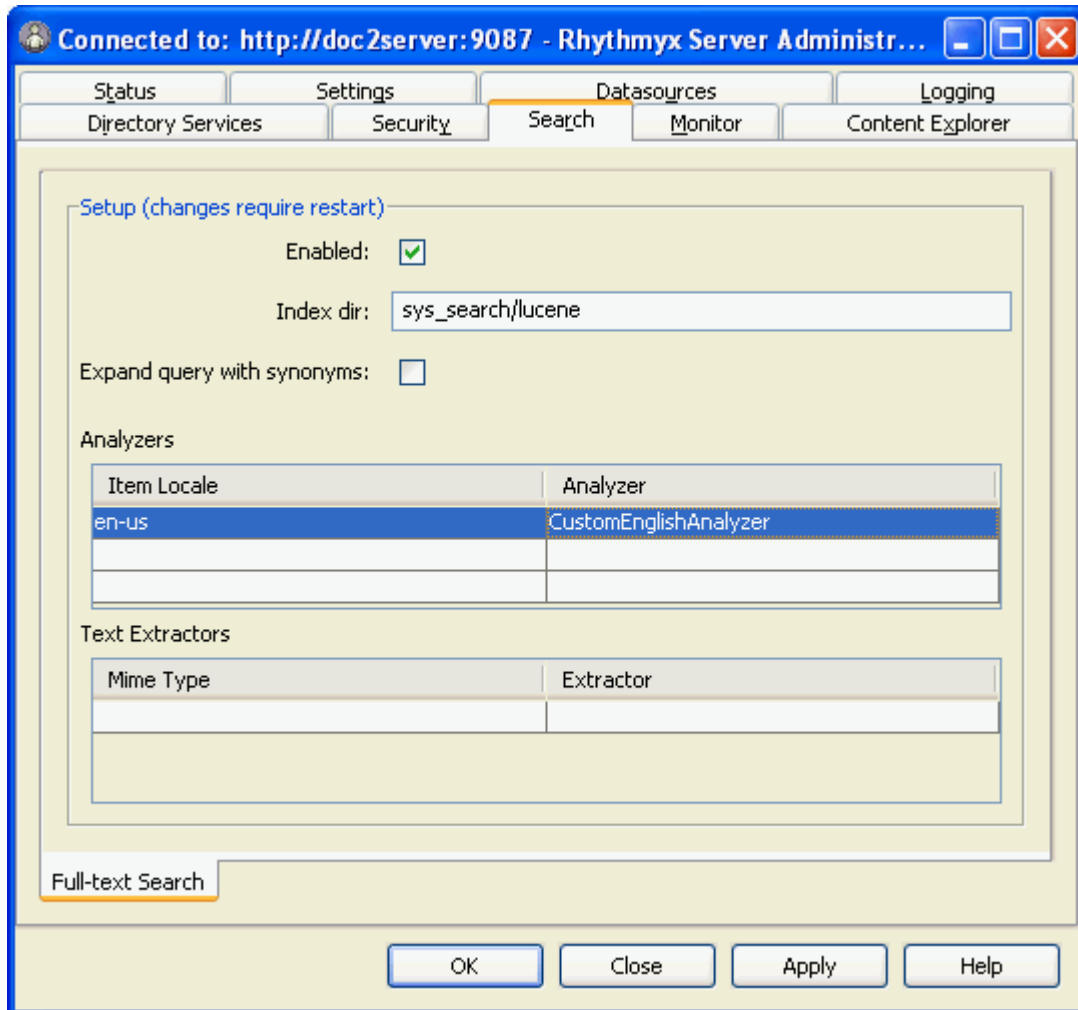


Figure 76: Search tab with custom analyzer added

- 4 Click [OK] and [Close].
- 5 Restart the Rhythmyx server.

Now, CM System will first see if a content item's Locale matches that of your registered analyzer before attempting to match it with the out-of-the-box analyzer.

---

## Disabling Full-text Search

To disable the full-text search engine, uncheck the *Enabled* checkbox on the Full-text Search tab of the Search tab in the Server Administrator.

Disabling the full-text search engine is intended as a temporary measure on development servers only. It is not intended to be used on production servers. Nor is it intended to facilitate a permanent conversion from the full-text search engine to the light-weight database search engine.

When you disable the full-text search engine, any pre-defined searches you have configured in the View/Search Editor in the Rhythmyx Workbench will be unavailable for modification. In the Content Explorer, these searches will still function, but they will use the light-weight database search engine functionality rather than the full-text search functionality, so running the search may return different results.

Any existing user-defined saved searches in Content Explorer that were created using the full-text search engine that are saved again while it is disabled will be converted to use the light-weight database search engine. They cannot be converted back to use the full-text search engine. If you convert a saved search accidentally while the full-text search engine is disabled, you will have to recreate it after enabling the full text search engine.

You determine whether or not individual fields will be included in full-text searches in the Rhythmyx Workbench's Field Properties Editor by checking or unchecking **Allow this field to be searched**. See the topic *Field Properties Editor* in the Workbench online help for more information.

---

## Configuring Maximum Search Results Returned

Some very general search queries can return large numbers of search results (on the order of thousands of Content Items). Such large numbers can cause Content Explorer to fail. To avoid this problem, configure the maximum search results for your system

The maximum search results is controlled by the `maxSearchResults` attribute of the `PSXSearchConfig` node of the server configuration XML file (`<rhythmyxroot>/rxconfig/server/config.xml`). The default value for this parameter is `-1`, which returns all results. If you change this value to a positive integer, you restrict the maximum search results to that value. For example, if you change the value of the `maxSearchResults` parameter to `200`, CM System will return no more than 200 Content Items as the results for a search. If a user configures a maximum result higher than the value of the `maxSearchResults` attribute, CM System ignores the user-defined value and uses the value defined on the server. Using the previous example, if a user attempted to configure a Maximum Result of 300, CM System would ignore that value and return only the 200 result defined in the server.

If you configure a value for the `maxSearchResults` parameter, CM System notes the allowable range for any interface in which the user can configure maximum search results. Using the example above, the search dialog in Content Explorer would resemble the following screenshot:

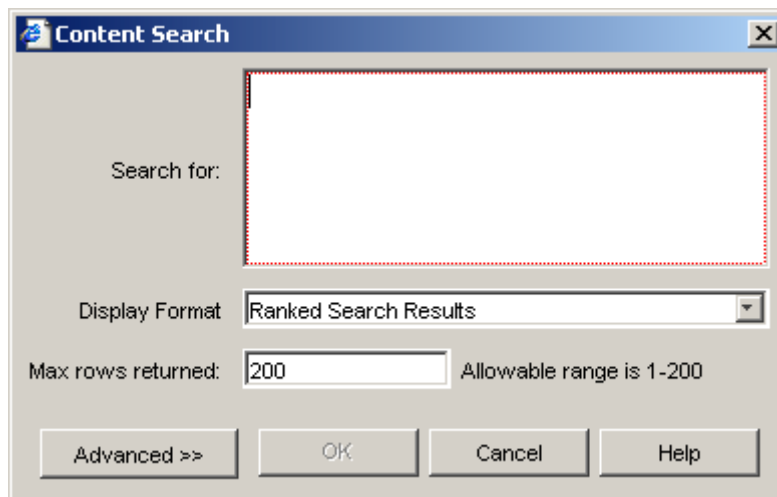


Figure 77: Content Explorer Search Dialog Showing Allowable Results Range

Note the text "Allowable range is 1-200" next to the **Max rows returned** field.

The same text is also added to the Search Query tab of the View and Search Editor in the Workbench:

General | Communities | Search Query | Properties

Search for:

Display Format: Simple

Max rows returned: 200 Allowable range is 1-200

Filter with:

Mode:  Concept  Pattern  Boolean

Expansion: Most strongly related concepts

Search Criteria

ContentId:

Title:

End User Customizable

Figure 78: Search Query Tab in View and Search Editor Illustrating the Allowable Range Text

---

## Full-text Search in Globalized Environments

The full-text search Engine shipped with CM System supports Locales that use the following languages:

- English
- French
- German
- Italian
- Portuguese
- Spanish
- Danish
- Dutch
- Finnish
- Norwegian
- Swedish
- Chinese
- Japanese
- Korean

Each Locale is associated with a specific text analyzer. Text analyzers know how to transform extracted text strings into search terms in different languages through a variety of operations such as removing common words, reducing words to root forms, and discarding punctuation.

If you are using a Locale that is not supported out of the box, you can create a custom text analyzer that supports the Locale, and register the custom text analyzer with the Locale in the Rhythmyx Server Administrator. See the topic *How to Override the Default Text Analyzer* in the Server Administrator online help.

By default, a search query is performed on the user's log-on Locale, and the text analyzer associated with the Locale also analyzes the term entered in **Search for**. In an advanced search, the user can select multiple Locales to search on. If multiple Locales are chosen, separate searches are performed for each Locale using the appropriate analyzer, and the results are combined.

---

## Maintaining Stop Words

Stop words are short words that generally serve mechanical purposes in language rather than conveying meaning (for example, *the* and *and*). Hence, stop words are generally not included in indexes or searches.

The default text analyzers for the full-text search maintain lists of stop words. However, you can override these lists by writing your own analyzers using the `IPSLuceneAnalyzer` interface (for help, see the JavaDoc), and adding your custom analyzers through the Rhythmyx Server Administrator. See the Rhythmyx Server Administrator online help for instructions on adding custom analyzers to the Search tab.



## Re-indexing the Full-Text Search

Some modifications to Content Types require you to re-index items of that Content Type for searching. If the Content Type does not include searchable fields or you have not yet created your search indexes, re-indexing is not necessary.

The following table lists modifications and whether or not they require re-indexing of the Content Type.

Modification	Re-index?	Comments
Delete a field	yes	Re-indexing is necessary to avoid matching on content in deleted fields. When the Content Type with the modifications is saved, the user is prompted to re-index.
Delete a child table	yes	Re-indexing is necessary to avoid matching on content in deleted fields. When the Content Type with the modifications is saved, the user is prompted to re-index.  If the child table does not include searchable fields or you have not yet created your search indexes, re-indexing is not necessary, and the user is not prompted to re-index.
Change value of a search property or mime type	yes	Modifications to a search property may change whether or not a field is indexed. Modifications to a mime type may change how text is extracted for indexing.
Add a field	no	In previously created content items, the field is empty. Content items created after the field is added are automatically indexed.
Add a child table	no	In previously created content items, the fields in the table are empty. Content items created after the table is added are automatically indexed.

Searches cannot be performed on a Content Type while it is being re-indexed; therefore, do not allow users to access CM System during re-indexing. To re-index a Content Type, enter the following command on your server console:

```
search index type
```

Depending on the number of existing items of the specified type, re-indexing may be a lengthy procedure.



## CHAPTER 8

# System Management and Recovery

This chapter describes the deployment and maintenance of the CM System CMS.

The first section describes the various deployment configurations of the physical components of the CM System Content Management System.

The second section describes how to set up source control and backups of the system.

The third section describes how to setup failover servers.

---

## Physical Architecture of CM System

A CM System Content Management System is comprised of three major components:

- the CM System server
- the Repository database
- the Web server.

Note that the database and Web server are third-party products not provided by Percussion Software.

These physical components can be deployed in several different configurations, with various options for communicating between the CM System server and the other components.

### All Physical Components Local

The simplest physical configuration of CM System is to install all components on the same machine:



*Figure 79: CM System Content Management System with all physical components installed locally*

## CM System Server with Local Repository, Remote Web Server Using FTP Publishing

In this configuration, the RDBMS for the CM System Repository is installed on the same machine as the CM System server. The Web server is hosted in a remote machine. CM System uses FTP to transfer the published content to the Web server.

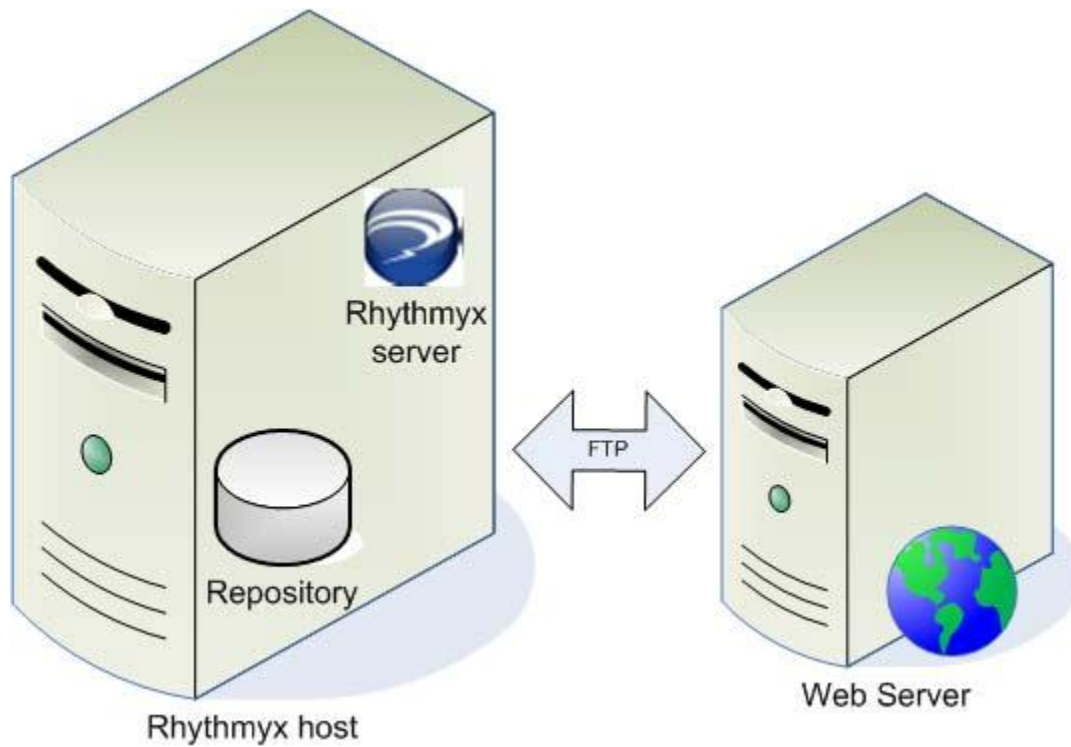


Figure 80: CM System server with local Repository and remote Web server using FTP publishing

## CM System Server with Remote Repository and Remote Web Server Using FTP Publishing

In this configuration, the CM System server, RDBMS server, and Web server are each installed on different host machines. CM System uses the propriety protocol of the RDBMS to communicate with it. Content is published to the Web server using FTP publishing.

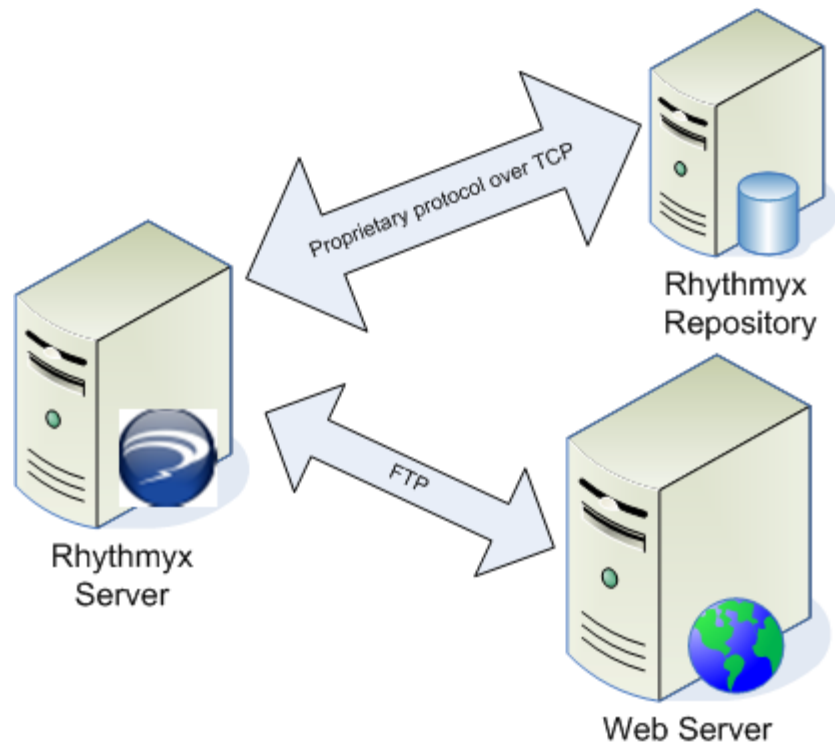


Figure 81: CM System server, RDBMS server, and Web server each on different hosts, with FTP publishing

---

## Source Control and Backups

CM System does not support version control for applications and other support files. You must use a third-party source/version control system to back up applications and other files in your CM System environment. Using a source control program is not only useful when you must perform recovery, but also helps you control production and deployment of applications.

At a minimum, you should implement a source control regime that includes CM System source files. If you use XSL Variants or other CM System applications, you should bring these under source control as well. A minimal program of source control includes:

- Source HTML for assembler applications
- Java and JavaScript extension files
- Shared Definition files
- Application directories
- Application XML files stored in ObjectStore directory
- Custom files stored in rx\_resources directory
- SQL Statements used to create tables and views

Ideally, however, you should implement a source control program that includes your entire CM System tree. Such a regimen provides an additional layer of backup and recover protection. To implement a full-tree source control program, bring your entire CM System development environment under source control.

## Integrating CM System with a Source Control System

Percussion Software, Inc., strongly recommends the use of a source control system to protect against accidental modification of your files. Percussion customers use a variety of source control systems, so you can use whatever specific system you prefer. Note, however, that some older source control systems may require workarounds. For example, CM System does not function correctly when its files are read-only, so when using Microsoft Visual SourceSafe you must copy the files to an external location where they can be writable.

This section documents the files that should be placed under source control.

Note that source control is not a substitute for backing up your systems. Development, staging, and production environments should all be backed up regularly.

## Backing Up the CMS

You should back up all CM System environments (development, staging, and production). For each environment, you should backup the complete CM System tree. In addition, backup the Repository database associated with the tree. Use the techniques recommended in your RDBMS documentation to create backups of the Repository.

## Backing Up Your Web Site

In CM System, you can roll back to previous versions of Content Items, but you cannot specify that the dependents of those Content Items return to the versions they had when the original Content Items were published. In general, using CM System as a recovery tool for your Web Server is unreliable; you should back up your Web Server each time that you publish to it. If you always publish your Web content to a staging server before publishing to your production server, your staging server may serve as your backup server. In this scenario, you can use CM System to publish to the staging server and, after testing, to publish to the production server. Alternatively, you can use CM System to publish to the staging server and then use a third-party delivery tool to synchronize the staging and production servers. If you want to publish to a production and backup server at the same time, you can use CM System to publish to the backup server and use a third party bulk copy tool (such as rsync or Open Deploy) to deploy the site to the production server.

## Java Components

All Java Extensions (and other Java Components such as Servlets) should follow your standards for Java development. These components should be separated into Packages in the normal manner.

Java component developers should supply a deployment script (Percussion Software, Inc., recommends using an ANT build file named `deploy.xml`) that installs the appropriate JARs and registers any extensions with the Extension Install Tool program. This tool is documented in the JavaDoc (installed with the Rhythmyx Workbench) at:

```
com.percussion.util.PSExtensionInstallTool
```

Percussion Software recommends developing all Java components that relate to a single project in the same source project, with a single build script and a single output JAR.

All Java Components should have readily identifiable version / build numbers and the numbering scheme should be synchronized with the source control system.

## Content Type Definitions and Templates

All Content Types and their associated Templates should be exported into an external directory and then placed in source control. Exporting these design objects produces XML files that describe the objects and can be re-imported at a later date.

Shared definitions are stored in

```
/Rhythmyx/rxconfig/Server/ContentEditors/shared
```

These files and the SQL definitions of their associated tables should be stored in source control.

Some installations will need to modify the System Definition file

(`ContentEditorSystemDef.xml`). If you modify this file, manage it under source control.

## Velocity Macros

Custom CM System macros are stored in the file

```
<Rhythmyxroot>/rx_resources/vm/rx_assembly.vm
```

If you add custom macros to this file, you should manage it under source control.



## Servlet Dispatcher Files

Installations that include custom servlets should manage

```
<Rhythmyxroot>/AppServer/server/rx/deploy/rxapp.ear/rxapp.war/WEB-INF/config/user/spring/UserDispatcher-servlet.xml
```

under source control:

Any pages added to `<Rhythmyxroot>/AppServer/server/rx/deploy/rxapp.ear/rxapp.war/user/pages/` should also be managed under source control.

## Ephox Editor Configuration

If you customize the Ephox EditLive! for Java DHTML rich text editor, you should manage the following files under source control:

```
<Rhythmyxroot>/rx_resources/ephox/rx_ephox_custom.xml
<Rhythmyxroot>/rx_resources/ephox/rx_ephox.js
<Rhythmyxroot>/rx_resources/ephox/elj_config.xml
```

## Custom Content Editor Controls

Content editor custom controls are stored in the `rx_Templates.xsl` file

```
<Rhythmyxroot>/rx_resources/stylesheets/rx_Templates.xsl
```

If you implement any custom controls, this file should be managed under source control. In addition, some controls require additional XSL and JavaScript files. These files should be managed under source control as well.

## Site Furniture

In most installations, the static site furniture is stored on the CM System server as well as the Web server, usually in the directory `<Rhythmyxroot>/web_resources`. These files should also be managed under source control.

## Legacy XML Assembly Applications

Some installations require XML applications for Assembly, lookups and other purposes. These applications should be managed under source control. For each application there is an XML file in the

`<Rhythmyxroot>/ObjectStore` directory and a directory under the CM System installation root directory. All of these files should be added to source control.

In addition, there are some stylesheets used by the XSL assembly process that should be managed under source control. These files are all stored in the directory

`<Rhythmyxroot>/rx_resources/stylesheets/asmblers/`. (These files are not used in assembly of Velocity templates.)

```
rx_Globals.xsl
rx_GlobalTemplates.xl
rx_Slots.xsl
```

## WebDAV

If your implementation includes any WebDAV configurations, you should manage `<Rhythmyxroot>/AppServer/server/rx/deploy/rxapp.ear/rxapp.war/WEB-INF/config/user/webdav/rxwebdav-servlet.xml` under source control.

## Other Design Objects

Some design objects cannot be added to source control easily. Most of these design objects are stored in a combination of tables in the Repository database and cannot be easily "exported". The best approach to managing these design objects is to document them thoroughly (including screenshots) at the time they are tested. (Relying on the Development Plan or similar document may not be adequate because the actual implementation may differ from the development plan.) Such documentation will allow you to create the design objects manually should need arise. The documentation should be managed by source control.

Design objects that should be managed this way include:

- Action Menus and Action Menu Entries
- Item Filters
- Display Formats
- Keywords
- Workflows
- Relationship Configurations

In some cases, these design objects use one or more files that can and should be added to source control. For example, an Action Menu Entry usually points to either an XML application or a user JSP page; an Item Filter will have an associated Filter Rule Java extension.

---

## Setting Up a CM System Failover Server

If you purchase a CM System Failover Server, you should configure and maintain it as an exact filesystem replica of your production CM System server. Both the production server and the failover server should use the same DBMS database repository and run on the same port.

Always deploy new and modified applications to the failover server when you deploy them to your production server. You may use any third-party filesystem replication utility to maintain synchronization between your failover and CM System servers or you can manually perform updates to the failover server each time you update the CM System Server.

Several strategies are available to seamlessly move users to a CM System Failover Server.

- **IP Address Takeover (IPAT)**  
In this scenario, the failover and main server have administrative IP addresses and share a floating IP address. During regular operation, the main server receives requests from the floating IP address; during failover, the failover server receives requests from the floating IP address.
- **MAC Address Takeover**  
Each hardware component accessed by your network has a MAC address. An IP address takeover may fail on your system if your system does not automatically refresh the cache holding the MAC addresses. In this scenario, you reassign the MAC address of hardware components.
- **Domain Name System (DNS) Reconfiguration**  
In this scenario, if a server fails, a DNS lookup returns the IP address of another machine. Applications that reconfigure the IP addresses associated with domain names when a server fails may also perform load balancing for multiple servers.

To use any of these methods, have users regularly request the CM System server by a server name or fully qualified domain name, rather than an IP address. If your main CM System Server fails, as long as you have kept the data on your failover server current, the move to the failover server will appear seamless to your users.

You may implement your own network failover strategy at the switch and router level or purchase network failover software that may offer you any number of options for failover resolution and load balancing.

---

## Setting Up a CM System Disaster Recovery Server

If you purchase a CM System Disaster Recovery Server, you should configure and maintain it as an exact filesystem replica of your production CM System server. Both the production server and the disaster recovery server should use the same DBMS database repository and run on the same port.

Always deploy new and modified applications to the disaster recovery server when you deploy them to your production server. You may use any third-party filesystem replication utility to maintain synchronization between your disaster recovery and CM System servers or you can manually perform updates to the disaster recovery server each time you update the CM System Server.

## Managing Binaries

Binaries can now be uploaded to the system through the new `sys_HashedFile` control. This control no longer stores the content of the binary in the table with the other fields for the item. Instead only a SHA1 hash is stored as the field value. The binary itself is stored in a separate binary table structure indexed from the unique hash. In this way there is only ever one version of any binary in the database at a time. This does the following

- Improves performance of operations on binary items including new revision creation, cloning of binary items even rendering of binary snippets.
- Reduces duplicates stored in new revisions of items and binaries uploaded to multiple items
- Allows for better database management of binaries e.g. using a separate tablespace for the single binary table.
- Metadata extraction is done the first time a binary is uploaded
- Allows for improved bulk import and export of binary items

When a new binary is added to the system we also extract metadata from the binary. This uses a generic metadata extraction engine called Tika <http://tika.apache.org/>. We store the extracted metadata into the database and this metadata can be referenced at assembly time to extract information like the size of the file, or even information like the number of pages in a document or when a photo was taken. Not all metadata is available for all document types and also not all documents of the same type will contain all metadata. You can click on the link on a content item the document has been uploaded to see all the metadata values for an item. See the Implementation Guide on how to use Jexl functions to extract the metadata values for an item.

Content-Type	The mimetype of the binary (always exists)
Content-Length	The size of the binary in bytes (always exists)
tiff:ImageLength	Height in pixels. Not just for tiff images but also jpg, gif etc.
tiff:ImageWidth	Width in pixels. Not just for tiff images but also jpg, gif etc.
xmpTPg:NPages	The number of pages in a document
Author	The document author
Copyright	Copyright

## Conversion of existing binary fields

The de-duplication scripts identify all unique binary files in the CMS and assign them unique hash values. It will populate binary in the new storage engine at the same time as populating a new field with the hash value in the content types table.

This ensures that all binary files are stored just once in the database and there are no duplicates.

### De-Duplication Process

The process consists of identifying all the existing binaries in the system and populating a new hash field with the sha1 hash of the binary, at the same time the unique binaries are imported into the new table structure and metadata for the item is extracted. This can take a long time for a large set of binary items.

Once the binaries are converted over, some template changes are required to use the new binaries based upon the hash value stored in the content type.

Once everything is configured and migrated the old field can be removed and the database space reclaimed.

## Limitations

Currently these binary fields cannot be used for thumbnail preview in content explorer. Any custom extensions including the PSOThumbnailGenerator that processes the uploaded file may need to be modified to work with these new binaries.

## Create new Hash Fields:

Note: Adding a field to an existing content type or shared group will cause the existing table to be backed up and the contents of the table copied back into the new schema. For large tables, especially those containing binaries, like these before conversion, this may take a very long time and may make workbench appear to not respond. It will also temporarily increase the database storage due to the `_BAK` table. One way to prevent this is to create the column in the database directly. When you attempt to create the field they system will tell you there is an existing column and you can link to that without the backup process.

In the Workbench, open a Content Type that uses binary fields.

Identify all custom or OOB binary local or shared fields (use the `sys_File` control). The OOB binary fields include `img1`, `img2`, `item_file_attachment`. These are all shared fields in the `rxs_ct_shared.xml` file.

For each of these fields, a new field needs to be created to store the hash value. If the original field is a shared field, the new field must be in the same shared field group. If the field is a local field on the content type the new field must also be a local field on the content type.

The new field must have the same name as the original field with the addition of a `_hash` suffix. The field must use the `sys_HashedFile` control

If the migration process is to go on while the system is in active use you may want to set the visibility of the new field to hidden during this process. Note though that any binaries that are added to the old field during the migration process may be skipped from migration. Rerunning the migration process below can be used to pick up any remaining items.

Repeat this process for all Content Types that have binary fields

## Migrate data into new Hashed Fields

In the Content Explorer, switch to the Admin tab and use the CM System Command Console to start, stop and check the status of the Duplication scripts:

```
binary migrate start
```

binary migrate stop  
binary migrate status

- i) Run migrate status command to find out the number of binary files in the CMS that need to be converted. This can be run during migration to check how many remain to be converted.
- ii) Run migrate start command to start the conversion process. At any time the process can be stopped with the stop command. To resume the process where it left off, run the start command again.
- iii) At the end of the process, run the migrate status command to confirm that all items have been converted. If the migrate status count returned is  $> 0$ , rerun the migrate start process until count returned = 0.
- iv) In the Workbench, for all Content Types with binary fields, change the visibility settings for all new hash fields to visible. Set the old binary field to invisible. You should also remove the sys\_ImageInfoExtractor extension on any image content type (this is no longer required)
- v) In the Content Explorer, Edit an item each of all binary Content Types to verify that the newly created hash fields have been populated. Populated fields should have the options “Preview File” and “View Metadata” visible.
- vi) In the Workbench, for all Content Types with binary fields, change the visibility settings for all old binary fields to invisible, and set the new binary field to visible.

## Convert Templates to use new fields

Each binary template needs to be modified to set the \$sys.binary and \$sys.mimetype based upon the new hash value

- i) Open all Binary Templates in Workbench:  
Every binary template will need the following 4 bindings:

Binding Variable	Binding Value
\$hash	\$sys.item.getProperty("NameofHashField").String
\$meta	\$rx.filestorage.getMeta(\$hash)
\$sys.mimetype	\$meta.get("Content-Type")
\$sys.binary	\$rx.filestorage.getFileFromHash(\$hash)

where NameofHashField is the name of the hash field that the binary template is being used for. E.g. “img1\_hash”

- ii) Modify binary snippet templates to use binary metadata  
Most of the information available about the binary used to be stored in the supporting binary fields on the content type e.g. \_size, \_type, \_height, \_width. These fields are no longer required on the content type,

(\_type is still required for icon selection in content explorer). These metadata values should now be extracted from the binary service. First you need to get the metadata HashMap. This can be set as a variable in the bindings. An example of each of the base encodings is shown below.

Original Meta name	Binding variable name	Binding Value
	\$hash	\$sys.item.getProperty("fieldName_hash").String
	\$meta	\$rx.filestorage.getMeta(\$hash)
fieldName_type	\$type	\$meta.get("Content-Type")
fieldName_width	\$width	\$meta.get("tiff:ImageWidth")
fieldName_height	\$height	\$meta.get("tiff:ImageLength")
fieldName_encoding	\$encoding	\$meta.get("Content-Encoding")

There are many other metadata values available depending upon the file type extracted. To see the full list for an item

It is recommended that \_filename is still stored as a field on the content item. The binary is unique in the system. Only the original filename is stored in the metadata, but the same file may be uploaded to different content items requiring different filenames on delivery.

To see all the available properties of the hash field, Edit an item and select the "View Metadata" option for the hash field.

Preview an item using each of the converted templates to make sure the templates are working correctly. You may need to view the html source to check if height and width attributes are being set.

## Removing old fields and data

The process of removing a field currently causes the table to be backed up and the data copied into the new schema. For large binary tables this can take a long time with the old binary data. The binary column can be set to null in the database before running this procedure to make it quicker.

Once the new hash fields have been populated and tested, the old binary fields can be removed.

- i) In the workbench, open a Content Type that uses binary fields.
- ii) Identify all original binary fields that have been converted. Open the shared fields file for these fields and delete the original binary fields. On deleting, choose the option to delete column from database.
- iii) Identify all custom binary fields that have been converted. Delete these from the Content Type. On deleting, choose the option to delete column from database.
- iv) Test all other image properties (type, width, height, size, encoding, extension, filename) to check if they have validation set. If they have no validation and are not used in the location scheme, they can be deleted. Note that all image properties are populated automatically and these should have read only set except for filename which can be manually edited.



v) In Properties tab of the Content Type, select the pre-processing tab. Delete the `imageInfoExtractor()` if set.

## Shrink the Database to reclaim space

For many databases, deleting columns does not release space automatically. Ask your DBA to manually reclaim space in the database after running the De-Dupe process.

## Export and Import of Binaries

All the binaries currently stored in the hashed binary system can be exported to the filesystem (this does not include old `sys_File` binaries that have not been converted yet) . This can be used for backup, or as a way to bulk import or export binaries to other systems.

The import and export is controlled from the admin console in the admin tab of content explorer. For a large amount of binaries this can take some time.

```
binary export {absolute path to folder on server}
binary import {absolute path to folder on server}
```

The following commands will show if the export or import is currently running

```
binary export status
binary import status
```

More detailed information on progress will be provided on the server log.

File and folder structure of exported content.

A folder is created for each file based upon the unique sha1 hash of the file, for example a file `CoupleinSunset_on.jpg` with a hash `01278a0169f18e328da4c1b74d92216d315e012d` will be created as

```
{export dir}/01/27/8a/0169f18e328da4c1b74d92216d315e012d/CoupleinSunset_on.jpg
```

The first three levels of directory make sure that no one directory contains too many files or folders for the file system. The sha1 algorithm should ensure that all binaries are spread evenly over these folders and any one binary will always generate the same folder path. In the same folder as the original file a file with the same name appended with `.sha1` is added containing the same hash. The file will only get exported with the original filename stored in the system for the item.

```
{export
dir}/01/27/8a/0169f18e328da4c1b74d92216d315e012d/CoupleinSunset_on.jpg.sha1
```

If the original filename is not descriptive for the binary it can be changed in the admin console. If the filename has been changed and an export is done to an existing folder, the export may contain both files. This will not cause duplicates when imported but the filename will be taken from the first found if it is not already in the system.

```
binary meta update filename {hash} {value}
```

e.g.

```
binary meta update filename 01278a0169f18e328da4c1b74d92216d315e012d
sunset_on.jpg
```

If filename contains spaces or special characters it can be enclosed in double quotes.

On import the specified directory is scanned looking for .sha1 files. If the file is found the contained hash is compared with the current hash storage to see if the file already exists. If the file exists it is skipped, if it does not the file is imported.

Using this mechanism exports can continually be made to the same directory to create a cumulative backup. On export if the .sha1 file is already found the binary is not exported from the system only new unknown items are exported. In a similar way an import of an existing import a second time will take a lot less time as only the missing binaries will be added.

If binaries are imported that are no longer referenced they can later be removed with the *removal of unreferenced binaries* procedure below. You may want to always run an export before removal of unreferenced binaries this way you will always be able to restore or reference any binary just by its hash.

## Migrating table structure from previous versions of hashed binaries

If the server has been upgraded from previous version using hashed binaries 7.0.2-7.2 and hashed binaries were being used these binaries need to be migrated into the new table structure. Import is the same but to export we need to specify we would like to export the old binaries.

```
binary export legacy {absolute path to folder on server}
```

After export is complete you can release the space by removing the old tables, PSX\_BINARYSTORE and PSX\_BINARYMETASTORE. The PSX\_BINARYMETASTORE table is not used in import or export as the metadata is recreated from the original file and filename in the new structure. If you have plenty of space to temporarily store two copies of all the binaries you may want to wait until the import has successfully completed in case you need to re-export.

## New Binary tables

Table Name	Description
PSX_BINARY	Stores the main information about the binary including the hash and main metadata including filename type and size
PSX_BINARYCOLUMNS	This stores references to columns in the

	database that are using binary hashes. This is then used to identify binary hashes that are no longer required and can be removed.
PSX_BINARYDATA	Stores the binary data
PSX_BINARYMETAENTRY	For each binary contains a list of values for each meta key
PSX_BINARYMETAKEY	Stores a list of metadata keys that have been found in all binaries passed to the service. Also whether the key is enabled or disabled.

## Removal of unreferenced binaries

Over time binary content items may be purged from the system. We may have more than one content item referencing the same binary by hash so we do not want to remove the actual binary in this case. We only want to remove the binary when we are sure it is no longer being referenced by the system.

In theory there is no issue with having extra binaries in the file storage service other than the space it takes up. If a user tries to re-upload the item it will see it is already there and it will be re-linked. We may even want to use this as a mechanism to pre-upload a large set of binaries that may subsequently have content items created for them through WebServices for example. When creating the content item WebServices would only need to send the hash value in the content item and not send the binary itself.

Periodically you may want to check for binaries that are no longer referenced and release the space from the database. There are some protections in place to make sure that the item really is not being used.

Before the purge operation you may choose to run an export as a file system backup of the data. This would enable you to lookup an item by its hash if only the reference remains and we do not have the binary anymore, and then could re-import that binary item.

Hash references are maintained to binaries stored from all versions of the content items in the system to allow promote revision to work for those items. If you want to remove more data and do not need the history you may want to run the purge revisions scheduled task first to remove the old revisions of items, and then use this process to remove the binaries that were de-referenced.

The purge process will check all known database columns containing hash values and will "touch" the binary in the system with the current date. Any binaries that have not been touched in a specified number of days will be removed permanently from the system. This does not affect any content types and only orphaned binaries without an active reference in any revisions of all content items will be removed.

This process will also not remove any binaries that were touched in the same day, this will prevent accidental removal. Each binary accessed from the system is touched only once a day

and this allows us to update this only on a daily basis and reduce updates to the database whenever a binary is accessed.

Before binaries are removed the current set of binary fields and database columns is analyzed and compared with the last time. If there is a difference, e.g. a content type is disabled or not running or a column is missing, a warning is provided and the delete is stopped until it is resolved.

The following admin console command will attempt to delete any binaries that have not been touched for at least the last day. Any known hash fields in the system are automatically touched first, so this should only remove items that are not being referenced.

```
binary purge delete 1
```

If you just want to validate the fields/columns without actually doing the delete (the delete does this automatically before it will actually delete) you can run.

```
binary purge validate
```

If you want to just see the number of binaries that will be removed

```
binary purge count 1
```

In uncommon circumstances you may have a different database table/column storing hashes that is not an actual field and is not known by Percussion. In this case you will need to manually add the column for checking or the system may purge the binaries thinking they are no longer required. These binaries referenced by hash in these columns will never be removed from the system unless the column is removed

```
binary purge column add TABLE_NAME.COLUMN_NAME
```

to manually remove a column from checking use

```
binary purge column remove TABLE_NAME.COLUMN_NAME
```

Before purging of any binaries a validation is done on the system. All the content types and shared fields are checked for '\_hash' fields. If any are found the backend database column is stored in the PSX\_BINARYCOLUMNS table. If an entry was previously added to this table and the field no longer is found a warning is displayed. This may be due to an error in the content type, or a change was made to the field. If you are sure that hashes previously stored in the column can be removed, or another column or field is holding the hashes you can remove the

column with the above command and re-run.

## Binary Metadata

The Tika metadata extraction engine is being used to extract full metadata from each item imported into the system. This is stored as a Map of key value pairs e.g. Content-Type = text/html. The Tika engine can extract metadata from many different file types

### Enabling/Disabling metadata keys.

Over time as documents are imported a number of different metadata keys will be imported into the system based upon the different document types. The full list of these are stored in the PSX\_BINARYMETAKEY table. Some of these values may be of no use to the system and you may want to skip the storage of those values when adding documents. To do this you need to disable the metadata key.

To list all metadata keys that shows which are active and which disabled.

```
binary meta key list
```

to disable a key

```
binary meta key disable "tiff:YResolution"
```

to enable a key

```
binary meta key enable "tiff:YResolution"
```

This will not remove the entries in the database that have already been created for existing binaries. Values for new binaries will not be stored. It will prevent these values from being displayed to the user in the content editor. To remove the existing values you would have to fully regenerate metadata for all binaries described below.

### Regenerating metadata.

Metadata for binaries may need to be regenerated for a number of reasons.

- Upgrade installs fixes or new version of Tika metadata processor.
- The wrong extension or mimetype was identified for a binary causing it to not extract correctly.
- You want to disable some of the meta data keys available to reduce data storage

For an individual binary you can reset the core metadata with the following commands. These core metadata values are used as a hint to the Tika processor to help it to select the correct metadata generator to further extract. The type and encoding may be auto corrected by Tika if they are found to be incorrect. The most common problem is that the file was uploaded with an extension that does not match the actual file type. The extension of the filename is used as a hint, but often the actual contents of the file itself can be used.

```
binary meta update filename {hash} {value}
binary meta update type {hash} {value}
binary meta update encoding {hash} {value}
```

encoding is only set and used for textual based content e.g. .txt, .html, .xml, .csv

An individual item can then be reparsed with

```
binary meta reparse hash {hash}
```

## **Reparsing all binaries.**

To reparse all binaries if you want to pick up improved metadata extraction from an update of Tika, or you have disabled a metadata key and want to release the space.

```
binary meta reparse all
```

Reparsing all binaries will take time for a large system, once it is started if the server is shut down, the process will continue where it left off when the server starts back up. You can check to see if the server is currently reparsing with

```
binary meta reparse status.
```

# Index

## A

About the CM System Administration Manual • 9  
 Add/Edit Role Dialog • 143, 149  
 Adding a DBMS Table Security Provider • 80, 84  
 Adding a Directory Configuration • 96, 102, 104  
 Adding a Directory Set • 106, 109  
 Adding a Group Provider • 103, 104, 129  
 Adding a JNDI Security Provider • 76  
 Adding a New Role • 143, 149  
 Adding a Role Provider • 111, 113  
 Adding a Web Server Security Provider • 78  
 Adding an Authentication • 91, 94  
 Adding Existing Members to a Role • 145, 150  
 Adding New Members to a Role • 147, 151  
 Adding Users and Groups to Roles • 130  
 Admin JSP Page • 48  
 All Physical Components Local • 172  
 Authentication Dialogs • 91  
 Authentication Editor • 91, 92, 93, 95  
 Authentications • 91, 92, 93, 95  
 Authentications Tab • 91, 92

## B

Backing Up the CMS • 175  
 Backing Up Your Web Site • 176  
 Backup • 175

## C

Cancelling an Edition • 14  
 Cataloger Configuration Dialog • 116, 117  
 Catalogers • 115  
 Changing CM System Server Service Settings • 43  
 Commands • 48, 52, 56, 58, 63, 64  
 Common Server Initialization Errors • 46  
 Configuring Access to Content Explorer Tabs • 72  
 Configuring Maximum Search Results Returned • 165  
 Configuring the Full-Text Search • 155, 159  
 Content Type Definitions and Templates • 176

Copying a Scheduled Task • 26  
 Creating a Scheduled Task • 24  
 Creating a Scheduled Task Notification • 30  
 Creating the Authentication • 118, 123  
 Creating the Directory • 121  
 Creating the Directory Connection Security Provider • 137  
 Creating the Directory Server Connection • 136  
 Creating the Directory Set • 125  
 Creating the Role Provider • 138  
 Creating the Security Provider • 127  
 Custom Content Editor Controls • 177

## D

DBMS Table Security Property Details  
 Attributes Tab • 81, 83, 85, 148  
 DBMS Table Security Property Details  
 Authentication Tab • 81, 83, 85  
 DBMS Table Security Property Details Backend  
 Connection Tab • 81, 82, 84, 85  
 DBMS Table Security Property Details Dialog • 80, 81, 84, 85  
 DBMS Table Security Property Details Provider  
 Properties Tab • 81, 84, 85  
 DBMS Table Security Provider • 80  
 Default Roles and Members • 140  
 Default Task Notification Variables • 30, 31  
 Defining a Directory Connection Security Provider • 75  
 Defining Role Attributes in LDAP • 135  
 Deleting a Directory Configuration • 96, 104  
 Deleting a Directory Set • 106, 111  
 Deleting a Group Provider • 104, 105  
 Deleting a JNDI Security Provider • 77  
 Deleting a Member from a Role • 152  
 Deleting a Role • 143, 150  
 Deleting a Role Provider • 111, 114  
 Deleting a Scheduled Task Notification • 31  
 Deleting a Web Server Security Provider • 79  
 Deleting an Authentication • 91, 95  
 Deployment Options for the Full-text Search Engine and Indices • 157  
 Directories Tab • 96, 97  
 Directory Configuration Dialogs • 96  
 Directory Configurations • 96  
 Directory Connection • 75, 76, 77, 127, 137  
 Directory Editor • 96, 97, 98, 102, 104  
 Directory Services • 87, 90, 117, 133  
 Directory Set Dialogs • 106

Directory Set Editor • 106, 107, 108, 110, 113, 148  
Directory Sets • 105, 106, 108, 109, 110, 111  
Directory Sets Tab • 106  
Disabling Full-text Search • 155, 159, 164  
Disaster Recovery • 179

## E

Editing a Cataloger Registration • 116, 117  
Editing a Directory Configuration • 96, 103, 104, 105  
Editing a Directory Set • 106, 110  
Editing a Group Provider • 104, 105  
Editing a JNDI Security Provider • 77  
Editing a Member's Properties • 152  
Editing a Role • 149  
Editing a Role Provider • 111, 114  
Editing an Authentication • 91, 95  
Ephox Editor Configuration • 177  
Example 1  
    Using LDAP to Authenticate Users • 117  
Example 2  
    Using LDAP as a Role Provider • 133  
Example Task Notifications • 34

## F

Failed Content • 19  
Failover • 179  
Full-text search • 159  
    Disabling • 164  
    Locales • 167  
    Maximum results • 165  
    Re-indexing • 169  
    Stop words • 168  
    Text analyzers • 162  
    Text extractors • 160  
Full-text Search in Globalized Environments • 167

## G

General Server Console Commands • 48

## H

How to Override the Default Text Analyzer • 156, 160, 162  
How to Override the Default Text Extractor • 156, 160

## I

Implementing LDAP Directory Services • 90

Indexes, Full-text search • 157  
Integrating CM System with a Source Control System • 175  
Issuing Commands to the CM System Server • 40, 41, 43, 48

## J

Java Components • 176  
JNDI Group Provider Details Dialog • 101, 105  
JNDI Security Provider Details Dialog • 75, 76, 77

## L

LDAP • 90, 91, 96, 105, 111, 117, 133, 135, 136, 137  
LDAP Configuration Examples • 117  
LDAP Directory Services Framework • 89  
Legacy XML Assembly Applications • 177  
Localized Content • 20

## M

Maintaining Authentications • 90, 91, 103  
Maintaining Catalogers • 90, 115  
Maintaining Directory Configurations • 90, 96  
Maintaining Directory Sets • 76, 90, 105, 114  
Maintaining Role Providers • 90, 111  
Maintaining Schedules • 21  
Maintaining Stop Words • 168  
Maintaining the CM System Server • 39  
Maintaining Users • 9, 40, 71  
Managing Publishing • 11  
Members • 145, 147, 148, 150, 151, 152  
Modify Member List for • 145, 147  
Modifying a DBMS Table Security Provider • 85  
Modifying a Scheduled Task • 25  
Modifying a Timed Event • 31  
Modifying a Web Server Security Provider • 79  
Monitoring Publication of Localized Content • 20

## N

New Member Dialog • 147

## O

Operating the CM System Server • 9, 41  
Operating the CM System Server in a Unix Environment • 41, 44  
Operating the CM System Server in a Windows Environment • 41, 42  
Other Design Objects • 178



**P**

Physical Architecture • 172, 173, 174  
 Physical Architecture of CM System • 9, 172  
 Provider URL Selector • 96, 99, 100, 103  
 Pruning Publishing Logs • 18  
 Publishing • 19, 20  
 Publishing Editions • 13

**R**

Registering a Cataloger • 116, 117  
 Re-indexing the Full-Text Search • 169  
 Republishing Failed Content • 19, 20  
 Restarting Server • 70  
 Reviewing Publishing Logs • 15  
 Reviewing Publishing Status • 12  
 CM System Server with Local Repository,  
 Remote Web Server Using FTP Publishing •  
 173  
 CM System Server with Remote Repository and  
 Remote Web Server Using FTP Publishing •  
 174  
 Role and Member Properties • 148  
 Role and Member Properties Required by  
 CM System Functions • 148  
 Role Provider Dialogs • 111  
 Role Provider Editor • 111, 112, 113, 114  
 Role Providers • 111, 138  
 Role Providers Tab • 111, 112  
 Roles • 9, 71, 139, 140, 143, 145, 147, 148, 149,  
 150, 151, 152  
 Run\_Edition\_Template • 34

**S**

Scheduled Task Editor • 23  
 Scheduled Tasks • 22  
 Search Configuration • 9, 40, 155  
 Search Engine • 155, 157, 164, 165, 167, 168  
 deployment options • 157  
 disabling • 164  
 moving indices • 157  
 Search Engine/configuring max results • 165  
 Search Engine/full-text search tab • 159  
 Search Engine/Locales • 167  
 Search Engine/text extractors • 160  
 Search Indices  
 Search Indices/moving • 157  
 Security Providers • 71, 74, 75, 77, 80  
 Security Providers and Authentication • 9, 71, 74  
 Security Providers Tab • 75

Server Console Commands by Function • 48  
 Server Console Commands for Applications •  
 48, 52  
 Server Console Commands for Displaying  
 Resources • 48, 56  
 Server Console Commands for Flushing the  
 Server and MetaData Caches • 48, 58  
 Server Console Commands for Search • 48, 63  
 Server Console Commands in Alphabetical  
 Order • 64  
 Server, restarting • 70  
 Servlet Dispatcher Files • 177  
 Setting Up a CM System Disaster Recovery  
 Server • 9, 180  
 Setting Up a CM System Failover Server • 9, 179  
 Site Furniture • 177  
 Source Control • 175  
 Source Control and Backups • 9, 175  
 Starting CM System Server as a Daemon in a  
 Unix Environment • 44  
 Starting CM System Server as a Windows Service  
 • 42  
 Starting CM System Server as an Application • 42  
 Starting Server • 42, 44  
 Starting the CM System Server as a Terminal  
 Window in a Unix Environment • 44  
 Stop Words • 168  
 Stopping CM System Server from the Services  
 Dialog • 43  
 Stopping CM System Server in a Unix  
 Environment When Running as a Terminal  
 Window • 45  
 Stopping CM System Server in Unix Environment  
 When Running as a Daemon • 45  
 Stopping Server • 43, 45  
 sys\_purgePublishingLog • 30, 31, 32  
 sys\_purgeTaskLog • 30, 31, 32  
 sys\_runCommand • 30, 31, 33  
 sys\_runEdition • 30, 31, 33  
 System Management and Recovery • 9, 171

**T**

Task Notification Editor • 29  
 Task Notifications • 28  
 Task\_Template • 34, 37  
 Tasks Requiring Restart of the CM System Server  
 • 41, 70  
 Timed Event Logs • 27  
 Troubleshooting

- Directory Services configuration • 104
  - server initialization • 46

- Troubleshooting a Directory Services

  - Configuration • 104

- Troubleshooting Server Initialization • 41, 46

## **U**

- Uninstalling the CM System Daemon Control Scripts • 45

- Using a Command to Stop CM System Server • 43

- Using Directory Services • 9, 40, 87

## **V**

- Velocity Macros • 176

## **W**

- Web Server • 77

- Web Server Security Provider Details Dialog • 78

- WebDAV • 178

- Windows NT • 80