

Implementing LDAP in Rhythmyx

5.7

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 Rhythmyx 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 © 1999-2005 Percussion Software.
All rights reserved

Licenses and Source Code

Rhythmyx uses Mozilla's JavaScript C API. See <http://www.mozilla.org/source.html> (<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

Other Copyrights

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

The JTDS driver is licensed and copyrighted by CDS Networks, Inc.

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 Ektron DHTML editor is licensed and copyrighted by Ektron, 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 AuthorIT Home - <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

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

Contents

Using an LDAP Directory Server with Rhythmyx 3

LDAP Directory Services Framework.....	4
Using LDAP Directory Services.....	6

Implementing LDAP Directory Services 9

Maintaining Authentications.....	11
Authentication Dialogs.....	11
Adding an Authentication.....	14
Editing an Authentication.....	15
Deleting an Authentication.....	16
Maintaining Directory Configurations.....	17
Directory Configuration Dialogs.....	17
Adding a Directory Configuration.....	21
Editing a Directory Configuration.....	22
Deleting a Directory Configuration.....	23
Maintaining Directory Sets.....	24
Directory Set Dialogs.....	24
Adding a Directory Set.....	27
Editing a Directory Set.....	28
Deleting a Directory Set.....	29
Maintaining Role Providers.....	30
Role Provider Dialogs.....	30
Adding a Role Provider.....	32
Editing a Role Provider.....	33
Deleting a Role Provider.....	33
Defining a Directory Connection Security Provider.....	35
Security Provider Dialogs.....	35
Adding a JNDI Security Provider.....	39
Editing a JNDI Security Provider.....	39
Deleting a JNDI Security Provider.....	40
Adding a Group Provider.....	40
Editing a Group Provider.....	40
Deleting a Group Provider.....	41
Troubleshooting a Directory Services Configuration.....	42

LDAP Configuration Examples 43

Example 1: Using LDAP to Authenticate Users.....	44
Creating the Authentication.....	45
Creating the Directory.....	47
Creating the Directory Set.....	50
Creating the Security Provider.....	52
Adding Users and Groups to Roles.....	55
Example 2: Using LDAP as a Role Provider.....	58
Defining Role Attributes in LDAP.....	59

Creating the Directory Server Connection.....	60
Creating the Directory Connection Security Provider	61

Using an LDAP Directory Server with Rhythmyx

The purpose of this book is to guide you in configuring your Rhythmyx server to use Lightweight Directory Access Protocol (LDAP) directory services. LDAP provides directory organization and access services to locate individuals, organizations, and other resources on private networks or on the Internet.

An LDAP directory is organized in a simple tree hierarchy, beginning with a root directory and branching out to countries, organizations, organizational units, and finally, to individuals, including people, shared files, and other resources. An LDAP directory can reside on one server or be distributed across many servers, referred to as directory servers. Rhythmyx can use LDAP directory services for many purposes, most commonly as a way to authenticate users attempting to log in to Rhythmyx and to provide Role information about Rhythmyx users.

Rhythmyx accesses LDAP directory services using the Java Naming and Directory Interface (JNDI) protocol. The JNDI protocol (part of Java 2 Platform, Enterprise Edition (J2EE)) provides access to a variety of directory services, including LDAP, Novell Directory Services (NDS), and Network Information Services (NIS). When a user provides credentials to log into Rhythmyx, Rhythmyx passes the credentials to a security provider (JNDI, in this case), which then passes them on to the LDAP directory server for authentication.

In addition to JNDI, Rhythmyx supports several other types of security providers, including OS/NT, Web server, and DBMS backend tables. For more information on these types of security providers, see the Rhythmyx online help.

This book describes the procedures to use when configuring a connection to an LDAP directory server and explains the Rhythmyx dialogs you see while performing the configuration. Procedures in this book also describe how to configure Rhythmyx to use JNDI as a security provider and how to use LDAP (optionally) as a Role Provider. Later chapters provide sample scenarios that show how you can configure Rhythmyx to use LDAP directory services. The examples build on the procedures described in the first part of the book.

LDAP Directory Services Framework

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

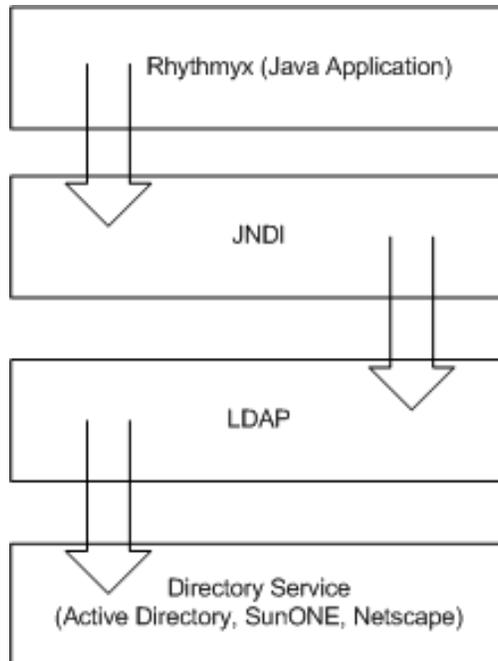


Figure 1: LDAP Directory Services Framework

LDAP directory services can be used to authenticate users as they log in to Rhythmyx 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 Rhythmyx.

As such, Rhythmyx is defined as a directory-enabled application. As currently implemented, Rhythmyx can search directory services for particular objects and retrieve any and all necessary attributes. Rhythmyx 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.

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

Using LDAP Directory Services

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

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

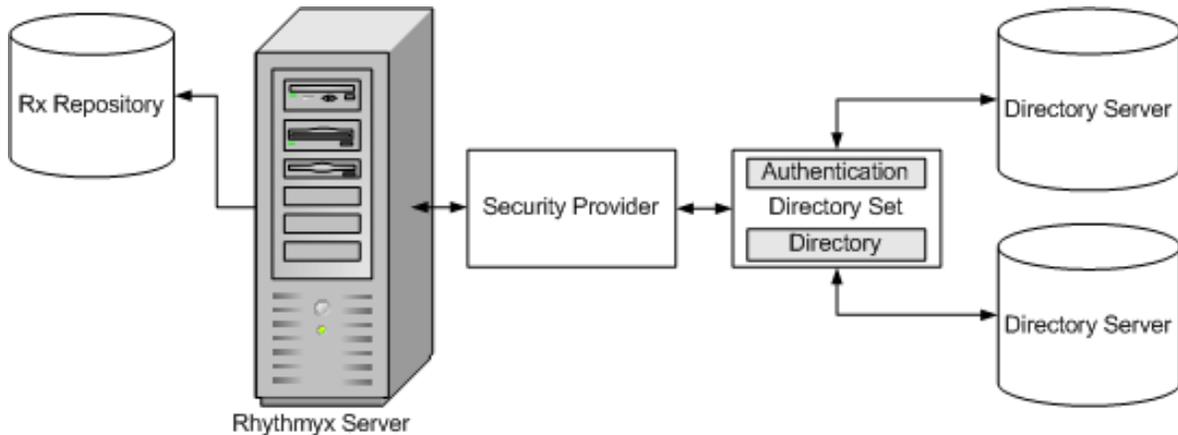


Figure 2: Sample LDAP Directory Server Configuration

Directory server connections can be used to provide user login authentication and other user details for use in Rhythmyx, 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 Rhythmyx. 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 Rhythmyx. Using this approach simplifies user maintenance in Rhythmyx.

By specifying user data in your directory server configuration, you can also use the directory server as a provider for other Rhythmyx 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.

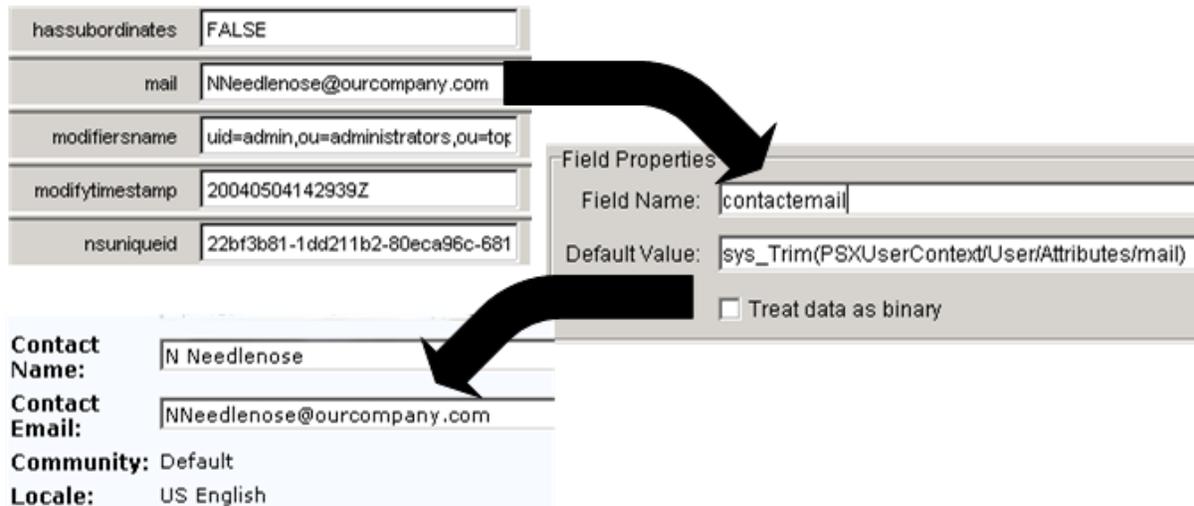


Figure 3: Using Directory Services Attributes in Rhythmyx Content Explorer

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>

Implementing LDAP Directory Services

Implementing LDAP directory services consists of two major parts:

- 1 Defining an LDAP directory services configuration
- 2 Defining the Directory Connection Security Provider (JNDI, in this case)

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
Authentication data defines the data used to log in to the directory server.
- Directory Configuration
A Directory Configuration defines the data required to connect to a specific LDAP directory.
- Directory Sets
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.

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

- Role Providers (optional)
A Role Provider defines the data that determines how Rhythmyx will use directory server information to determine the user's Roles once they have been authenticated.

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.

Defining a Directory Connection Security Provider

A Directory Connection Security Provider allows Rhythmyx to query the directory server to authenticate users and retrieve Role and other user information. Configure Rhythmyx 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 Rhythmyx Server Administrator dialogs to set up an Authentication.

- *Authentications tab* (see page [11](#))
- *Authentication Editor* (see page [12](#))

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* (see page [14](#))
- *Editing an Authentication* (see page [15](#))
- *Deleting an Authentication* (see page [16](#))

Authentications Tab

The Authentications tab lists any existing Authentications. When shipped, Rhythmyx 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.

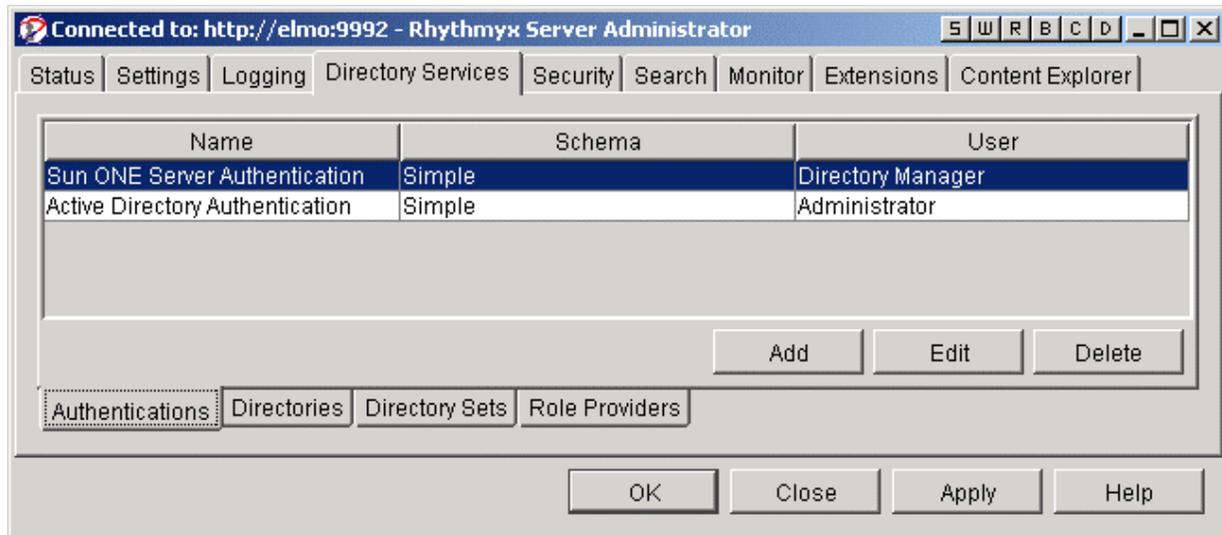


Figure 4: Authentications Tab

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 12) 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.

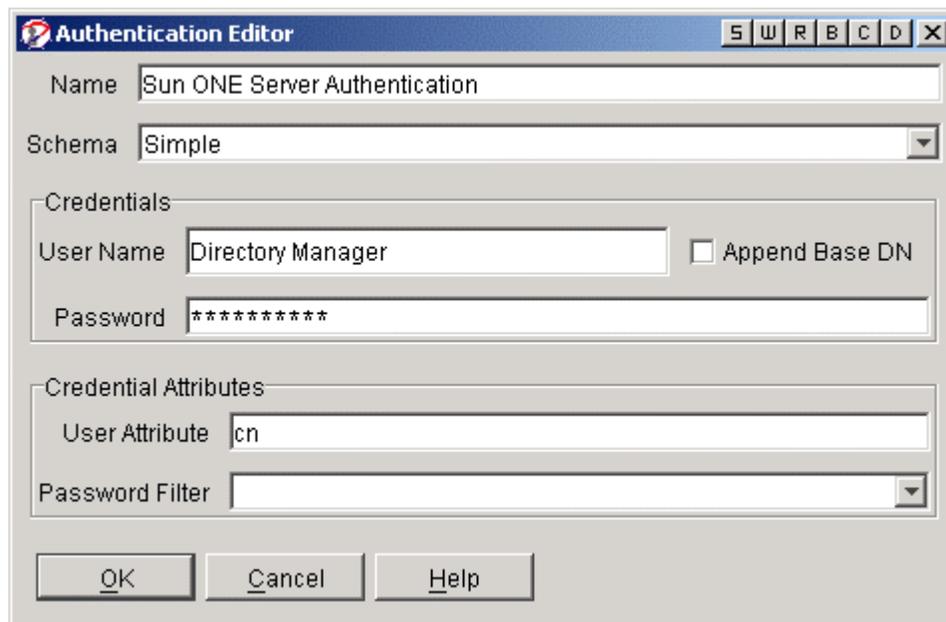


Figure 5: Example Authentication Definition

Authentication Editor Field Descriptions:

- **Name** - A description of the Authentication being registered. In this example, we used the name Sun ONE Server Authentication because this Authentication is for a Sun ONE directory server.
- **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 Rhythmyx to the directory server. Rhythmyx 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 Rhythmyx. Rhythmyx responds by encrypting the data with its password using the MD5 algorithm. The LDAP server then uses Rhythmyx'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. 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 - 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 - 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. Rhythmyx 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.

NOTE: An Authentication is valid for only one Rhythmyx server. When you have multiple Rhythmyx 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; Rhythmyx displays the Authentication Editor.

- 4 Complete the fields as described in the topic *Authentication Editor* (on page 12).

The screenshot shows the 'Authentication Editor' dialog box. It has a title bar with a red question mark icon and the text 'Authentication Editor'. The dialog contains several fields:

- Name:** A text box containing 'Sun ONE Server Authentication'.
- Schema:** A dropdown menu showing 'Simple'.
- Credentials:** A section containing:
 - User Name:** A text box containing 'Directory Manager'.
 - Append Base DN:** An unchecked checkbox.
 - Password:** A text box filled with asterisks '*****'.
- Credential Attributes:** A section containing:
 - User Attribute:** A text box containing 'cn'.
 - Password Filter:** A dropdown menu.

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

Figure 6: 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 Rhythmyx server.

Editing an Authentication

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

NOTE: If you change the name of an existing Authentication, Rhythmyx 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 12).
- 5 Click the [OK] button to close the Editor dialog.
- 6 Click the [Apply] button to commit the changes to the Rhythmyx 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 Rhythmyx server.

Maintaining Directory Configurations

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

- Name
- Catalog
- Factory
- Authentication
- Provider URL
- Returned Attributes

Directory Configuration Dialogs

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

- *Directories tab* (see page [17](#))
- *Directory Editor* (see page [18](#))
- *Provider URL Selector* (see page [20](#))

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* (see page [21](#))
- *Editing a Directory Configuration* (see page [22](#))
- *Deleting a Directory Configuration* (see page [23](#))

Directories Tab

The Directories tab lists any existing Directories. When shipped, Rhythmyx 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 7: 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* (see page 18) 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

To create a new Directory configuration:

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

The Directory Editor appears.

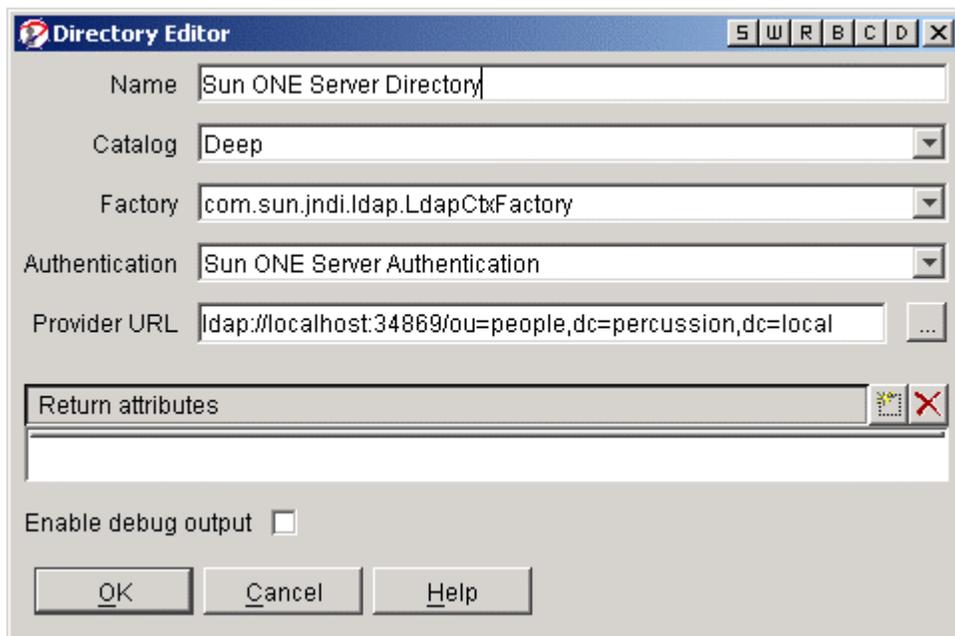


Figure 8: Directory Editor

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. Rhythmyx defines two types of directory server cataloging. Choose the one that is right for your configuration.
 - **Shallow** - Rhythmyx retrieves only those records immediately below the search base
 - **Deep** - Rhythmyx 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 20). 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.
- 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.

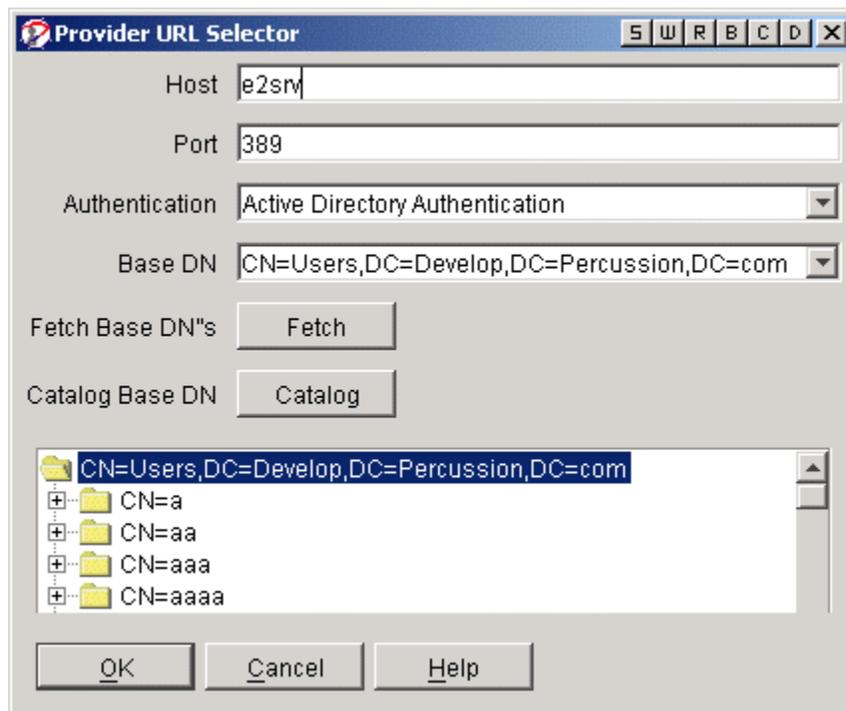


Figure 9: Provider URL Selector Dialog

Provider URL Selector Field Descriptions:

- Host - The resolvable name (or IP address) of the directory server to which Rhythmyx 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.

NOTE: 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.

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.

NOTE: A Directory configuration is valid for only one Rhythmyx server. When you have multiple Rhythmyx 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 to display the Directory Editor.

- 4 Complete the fields as described in the topics *Directory Editor* (on page 18) and *Provider URL Selector* (on page 20).

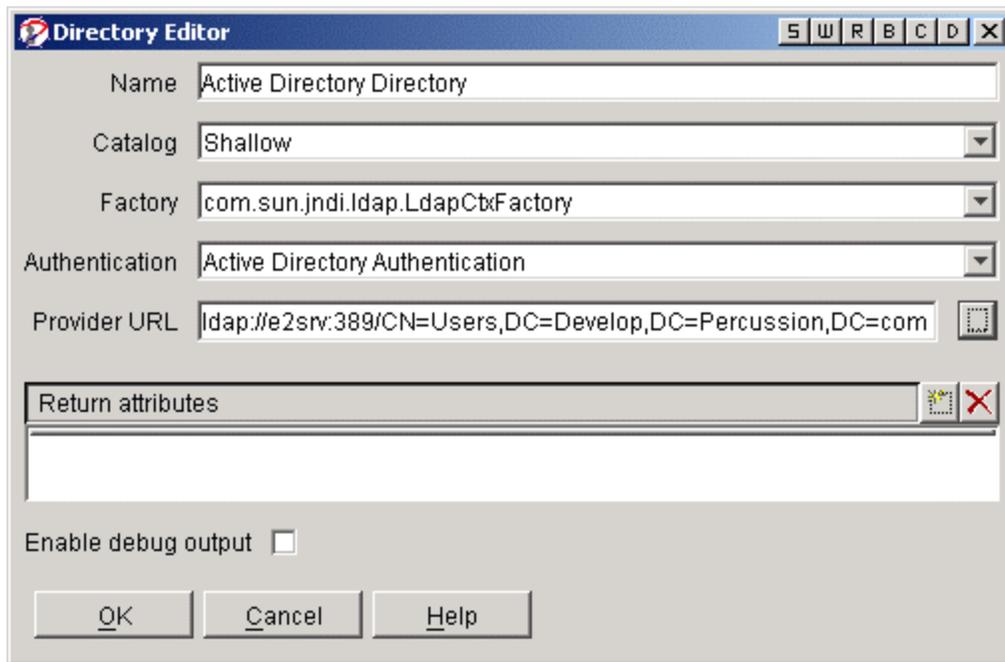


Figure 10: Example Directory Definition

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

NOTE: If you change the name of an existing Directory, Rhythmyx 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.)
- 4 Make your changes as described in the topics *Directory Editor* (on page 18) and *Provider URL Selector* (on page 20).
- 5 Click the **[OK]** button to close the Editor dialog and click the **[Apply]** button to commit the changes to the Rhythmyx server.

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 Rhythmyx server.

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* (see "[Directory Set Tab](#)" on page 24)
- *Directory Set Editor* (see page 25)

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* (see page 27)
- *Editing a Directory Set* (see page 28)
- *Deleting a Directory Set* (see page 29)

Directory Set Tab

The Directory Sets tab lists any existing Directory Sets. When shipped, Rhythmyx 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 11: 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 25) 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.

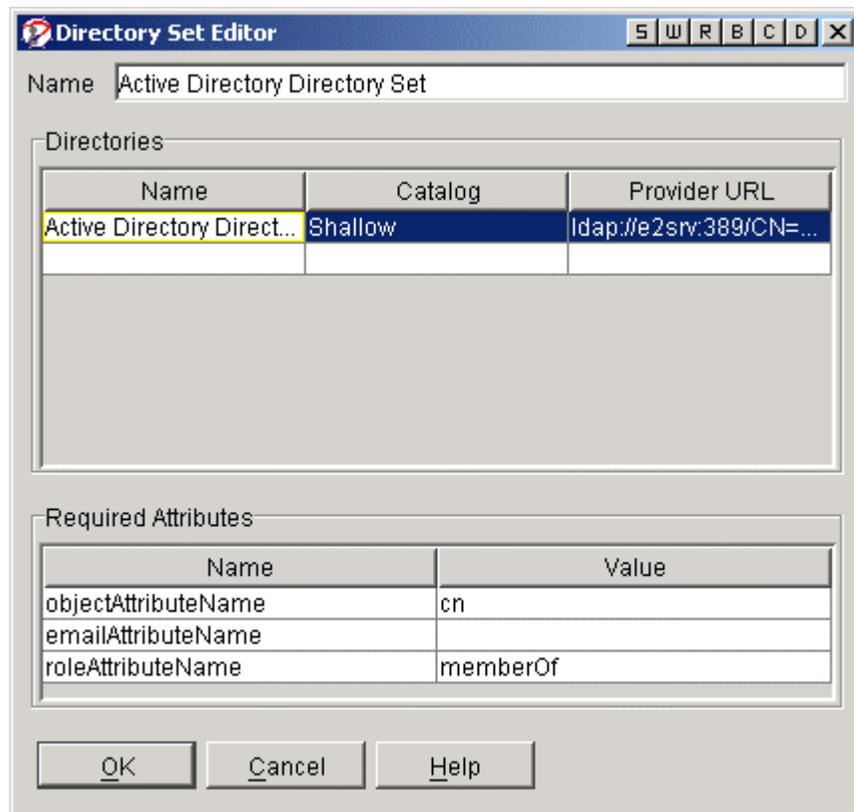


Figure 12: Directory Set Editor

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 Rhythmyx.

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

- Required Attributes - Several processes within Rhythmyx 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 Rhythmyx. 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,

Rhythmyx can send notifications to these users without having to individually define their email addresses in the Rhythmyx server.

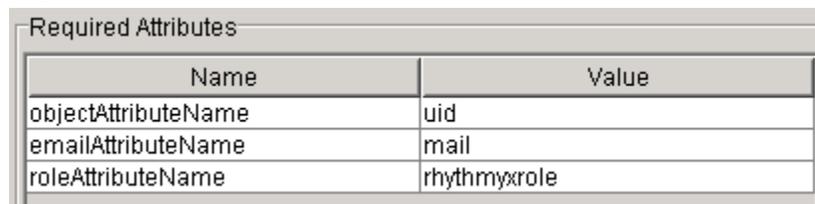
- `roleAttributeName` - Optional. The attribute used to define a user's Rhythmyx Role. In some configurations, the directory server is used to define a user's Role in Rhythmyx. If each user has both a Functional and Community Role defined in the directory server, it is not necessary to add them to a Role in Rhythmyx. 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 13: 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 Rhythmyx.



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

Figure 14: 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.

NOTE: A Directory Set is valid for only one Rhythmyx server. When you have multiple Rhythmyx 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; Rhythmyx displays the Directory Set Editor.

- 4 Complete the fields as described in the topic *Directory Set Editor* (on page 25).

Directory Set Editor

Name: Sun ONE Server Directory Set

Name	Catalog	Provider URL
Sun ONE Server Dire...	Deep	ldap://localhost:34869/ou=people,...

Name	Value
objectAttributeName	uid
emailAttributeName	mail
roleAttributeName	rhythmyxrole

Buttons: **OK**, **Cancel**, **Help**

Figure 15: 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 Rhythmyx server.

Editing a Directory Set

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

NOTE: If you change the name of an existing Directory Set, Rhythmyx 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 25)
- 5 Click the **[OK]** button to close the Editor dialog.
- 6 Click the **[Apply]** button to commit the changes to the Rhythmyx 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 Rhythmyx server.

Maintaining Role Providers

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

- Name
- Type
- Directory Set

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

NOTE: 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* (see page [30](#))
- *Role Provider Editor* (see page [31](#))

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* (see page [32](#))
- *Editing a Role Provider* (see page [33](#))
- *Deleting a Role Provider* (see page [33](#))

Role Providers Tab

The Role Providers tab lists any existing Role Providers. When shipped, Rhythmyx 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.

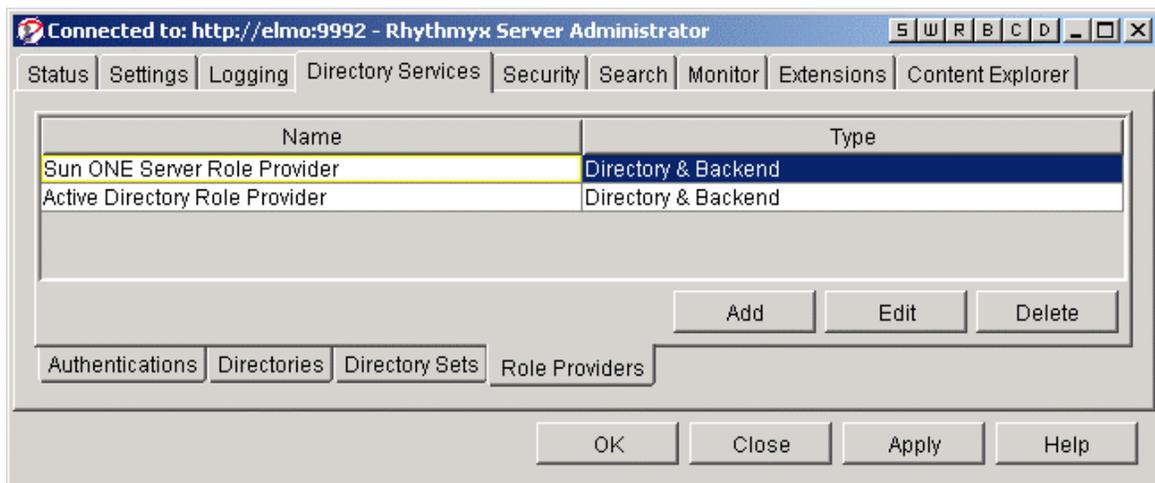


Figure 16: Role Providers Tab

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* (see page 31) 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 31) appears.



Figure 17: 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.
- Type - A description of the type of Role Provider being registered.
 - Backend - If a user has Roles defined for them in the directory server and Rhythmyx, only the Role associations in Rhythmyx are used.
 - Directory - If a user has Roles defined for them in the directory server and Rhythmyx, only the Role associations in the directory server are used.
 - Directory & Backend - If a user has Roles defined for them in the directory server and Rhythmyx, the user inherits the Roles from both providers. This is useful if the user is defined as an Author and an Editor in the directory server, but on a particular Rhythmyx server, also needs to be an Admin. The Author and Editor Roles are defined on the directory server and the user is associated with the Admin Role on the Rhythmyx server.
- 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 Rhythmyx.

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.

NOTE: A Role Provider is valid for only one Rhythmyx server. When you have multiple Rhythmyx 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.

- 4 Complete the fields as described in the topic *Role Provider Editor* (on page 31).



Figure 18: Example Role Provider Definition

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

Editing a Role Provider

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

NOTE: If you change the name of an existing Role Provider, Rhythmyx 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.)
- 4 Make your changes as described in the topic *Role Provider Editor* (on page 31)
- 5 Click the [OK] button to close the Editor dialog.
- 6 Click the [Apply] button to commit the changes to the Rhythmyx 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(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 Rhythmyx server.

Defining a Directory Connection Security Provider

Rhythmyx supports several types of security providers, including OS/NT, Web server, DBMS backend tables, and directory connection security providers, such as the Java Naming and Directory Interface (JNDI). Security providers provide access to data that can authenticate users trying to log in to Rhythmyx. JNDI allows Java-based applications, such as Rhythmyx, 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 Rhythmyx to use JNDI as a security provider. For information on using other types of security providers, see the online help.

Security Provider Dialogs

Use the following Rhythmyx Server Administrator dialogs to set up a directory connection security provider:

- *Security Providers tab* (see page 35)
- *JNDI Security Provider Details dialog* (see page 36)
- *JNDI Group Provider Details Dialog* (see page 37) (only if you are using groups)

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 security providers and group providers are in these topics:

- *Adding a JNDI Security Provider* (see page 39)
- *Editing a JNDI Security Provider* (see page 39)
- *Deleting a JNDI Security Provider* (see page 40)

Optional (only if you are using groups):

- *Adding a Group Provider* (see page 40)
- *Editing a Group Provider* (see page 40)
- *Deleting a Group Provider* (see page 41)

Security Providers Tab

The Security Providers tab lists any existing security providers. When shipped, Rhythmyx 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 \(Version 5.5 and later\)](#)" on page 36) dialog appears.

JNDI Security Provider Details Dialog

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

The JNDI Security Provider Details dialog has two tabs:

- *Provider Properties* (on page 36)
- *Group Providers* (on page 37)

Provider Properties

Use the Provider Properties tab of the *JNDI Security Provider Details dialog* (see "[JNDI Security Provider Details Dialog \(Version 5.5 and later\)](#)" on page 36) to maintain the properties of the security provider as a whole.

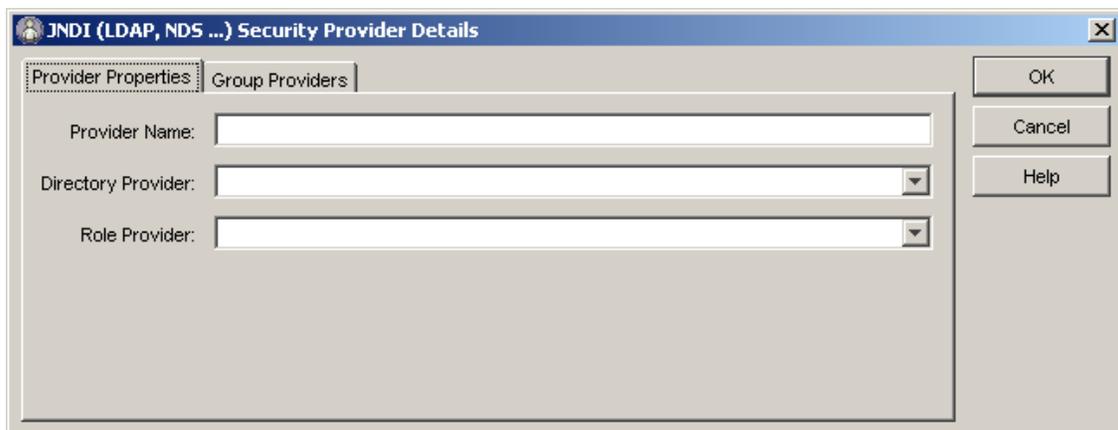


Figure 19: JNDI Security Provider Details Dialog Showing Provider Properties Tab

Provider Properties Tab 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
- Role Provider - The name of the Role Provider used to retrieve user Roles from the directory server (if you are using a Role Provider)

Group Providers

Use the Group Providers tab of the *JNDI Security Provider Details dialog* (see "[JNDI Security Provider Details Dialog \(Version 5.5 and later\)](#)" on page 36) to create, maintain, and delete group providers. Group providers define a source of the group information for the security provider to use when authenticating a user. If you are going to include a group from a directory in an ACL list or as a Role Member, you must define a group provider that security providers can use to locate the group and determine whether an authenticated user is a member of that group. Any number of security providers can refer to a group provider.

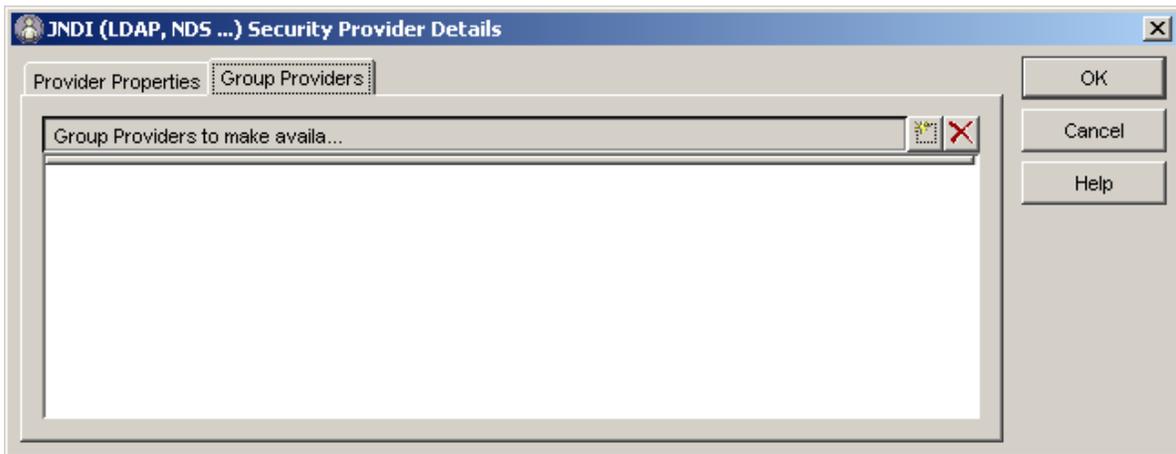


Figure 20: JNDI Security Provider Details Dialog Showing Group Providers Tab

To access the *JNDI Group Provider Details* (see "[JNDI Group Provider Details Dialog](#)" on page 37) dialog from the Group Providers tab:

- 1 Click the Insert New Entry icon  to the right of the "Group Providers to make availa..." row. A row or rows appear with a drop list arrow.
- 2 Click the arrow. If no Group Providers exist, only "Create New..." appears in the drop list. Otherwise, the existing Group Providers appear in the drop list.
- 3 Either double-click on an existing Group Provider to edit it or click Create New... to create a new Group Provider. The JNDI Group Provider Details dialog appears.

JNDI Group Provider Details Dialog

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

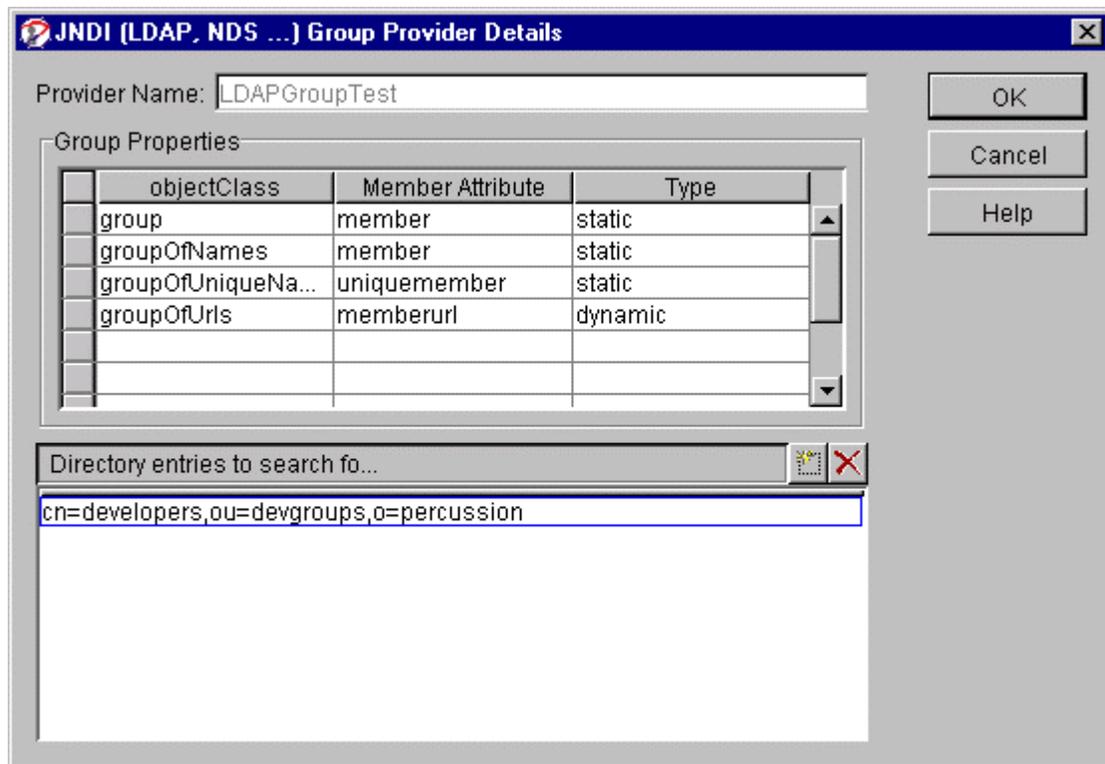


Figure 21: JNDI Group Provider Details Dialog

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. Rhythmyx 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 Rhythmyx will treat the value of the Member Attribute. Options are:
 - Static - Rhythmyx 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 - Rhythmyx 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 Rhythmyx searches for possible group entries. Each entry should be the fully qualified distinguished name (DN) from the Directory root. Rhythmyx 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.

Rhythmyx 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.

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**].
Rhythmyx displays the Select new security provider type dialog.
- 3 Choose Directory Connection Security Provider and click [**OK**].
Rhythmyx displays the *JNDI Security Provider Details dialog* (see page 36).
- 4 Complete the *Provider Properties tab* (see "[Provider Properties](#)" on page 36) (this is the default tab):
- 5 Add group providers, if necessary. To add an existing group provider or create a new one, use the *JNDI Group Provider Details dialog* (see page 37).
- 6 Click [**OK**] to save the new security provider definition.
- 7 Click [**Apply**] to commit the changes to the Rhythmyx 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.

Rhythmyx displays the *JNDI Security Provider Details dialog* (see page 36).

- 3 You can change any field on the *Provider Properties tab* (see "[Provider Properties](#)" on page 36).
- 4 Click [**OK**] to save your changes and close the dialog.
- 5 Click [**Apply**] to commit the changes to the Rhythmyx server.

Deleting a JNDI Security Provider

NOTE: Rhythmyx 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. Rhythmyx DOES NOT ask you to confirm the delete action before deleting the security provider.

Adding a Group Provider

To add a group provider:

- 1 Access the *Group Providers tab* (see "[Group Providers](#)" on page 37) of the *JNDI Security Provider Details dialog* (see "[JNDI Security Provider Details Dialog \(Version 5.5 and later\)](#)" on page 36).
- 2 Click the Insert New Entry button  to the right of the "Group Providers to Make Availa..." row.

Rhythmyx 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.

Rhythmyx displays the *JNDI Group Provider Details dialog* (on page 37).
- 3 Press the [**Enter**] or [**Return**] key and click [**OK**] to save the group provider.
- 4 Click [**Apply**] to commit the changes to the Rhythmyx server.

Editing a Group Provider

To edit a group provider:

- 1 Access the *Group Providers tab* (see "[Group Providers](#)" on page 37) of the *JNDI Security Provider Details dialog* (see "[JNDI Security Provider Details Dialog \(Version 5.5 and later\)](#)" on page 36).
- 2 Double-click the name of the group provider you want to edit.

Rhythmyx displays the *JNDI Group Provider Details dialog* (on page 37). 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 Press the [Enter] or [Return] key and click [OK] to save your changes.
- 6 Click [Apply] to commit the changes to the Rhythmyx 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 Access the *Group Providers* (on page 37) tab of the *JNDI Security Provider Details dialog* (see "[JNDI Security Provider Details Dialog \(Version 5.5 and later\)](#)" on page 36).
- 2 Select the group provider you want to remove and click the remove button .

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?

CHAPTER 3

LDAP Configuration Examples

In this chapter, we walk through examples of two ways of using LDAP directory services with Rhythmyx. 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 Rhythmyx users.

Example 1: Using LDAP to Authenticate Users

In this example, we allow users maintained in the corporate Active Directory server to access our Rhythmyx 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 Rhythmyx, only Bobby. Bobby is associated with the Rhythmyx 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.

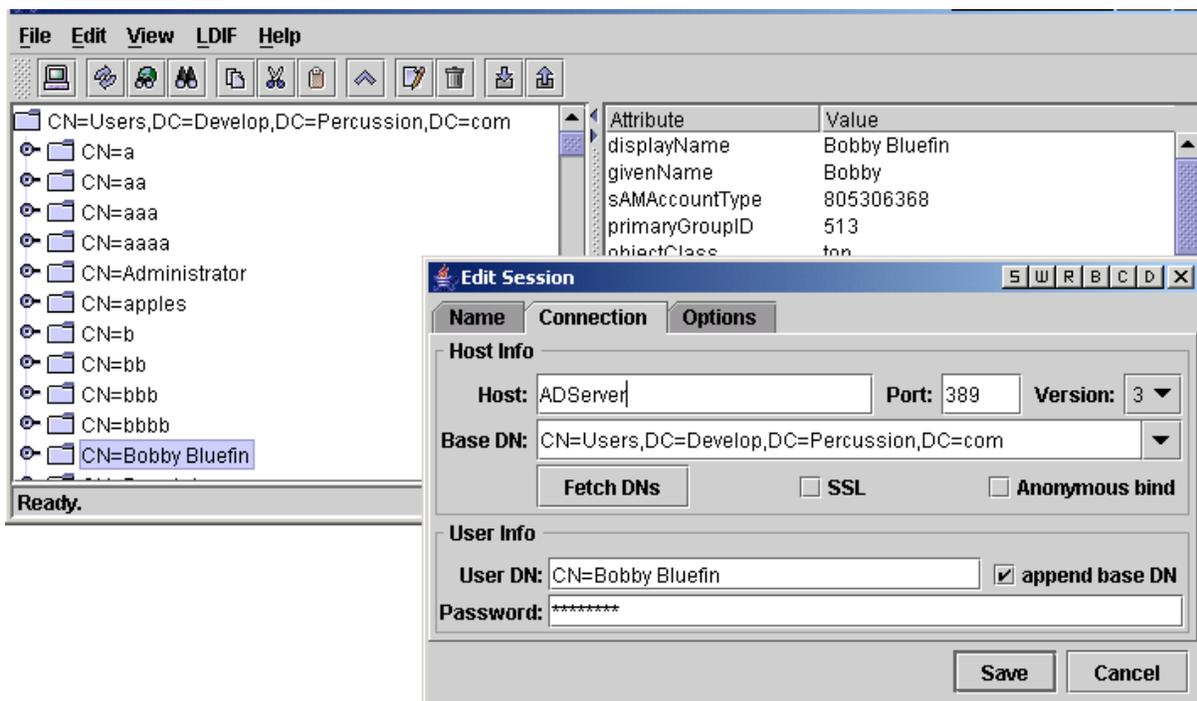


Figure 22: Using an LDAP Browser to Confirm the Configuration

Creating the Authentication

Our first step is to create an Authentication.

- 1 Start the Server Administrator client and connect to the Rhythmyx server.
- 2 Click the Directory Services tab.
- 3 Click the Authentications tab.



Figure 23: Authentications Tab

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

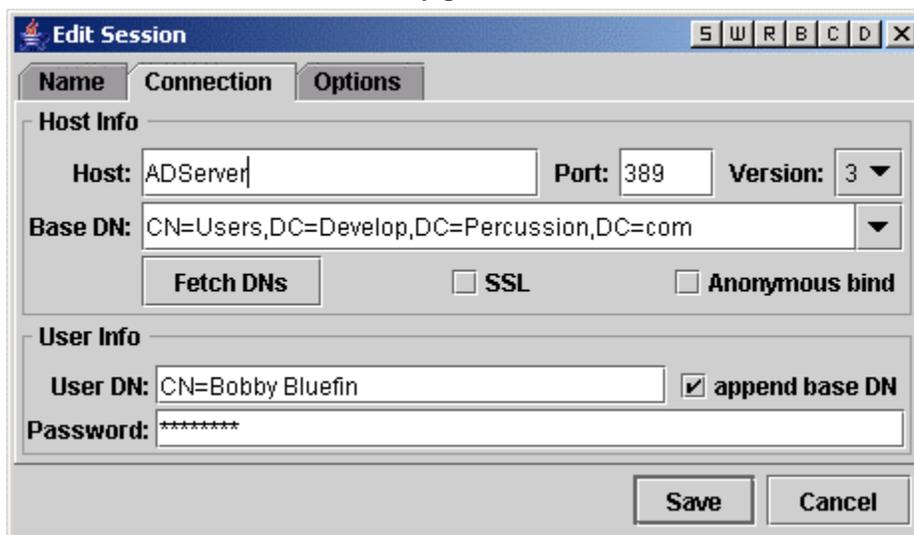


Figure 24: LDAP Browser Showing ADServer Connection

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

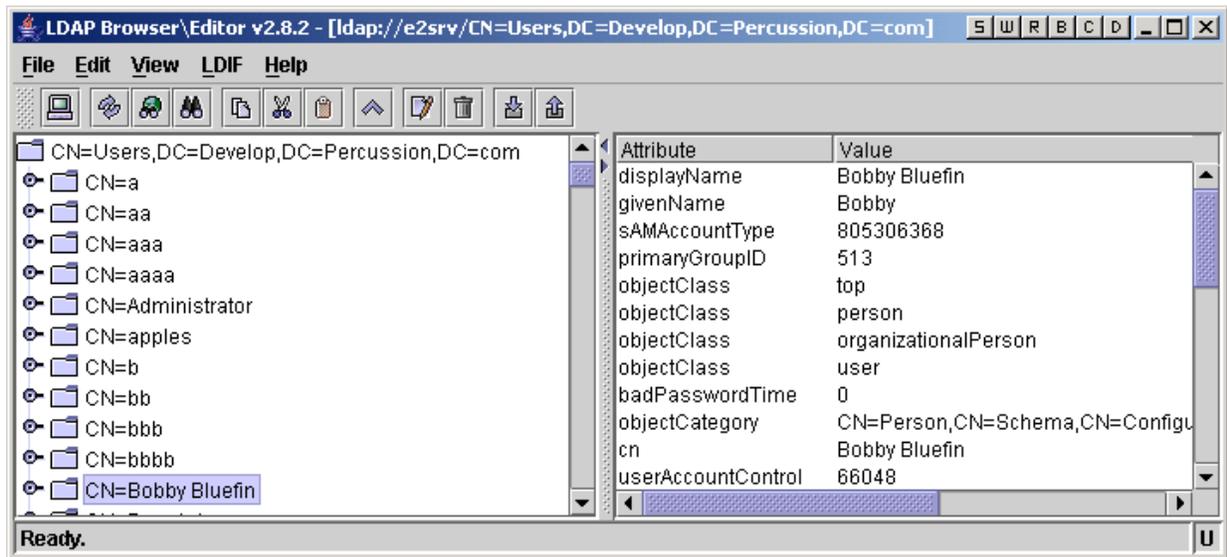


Figure 25: ADServer Directory Catalogued in LDAP Browser

NOTE: The LDAP Browser is a third-party utility, which is not a part of the Rhythmyx software and is not required.

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

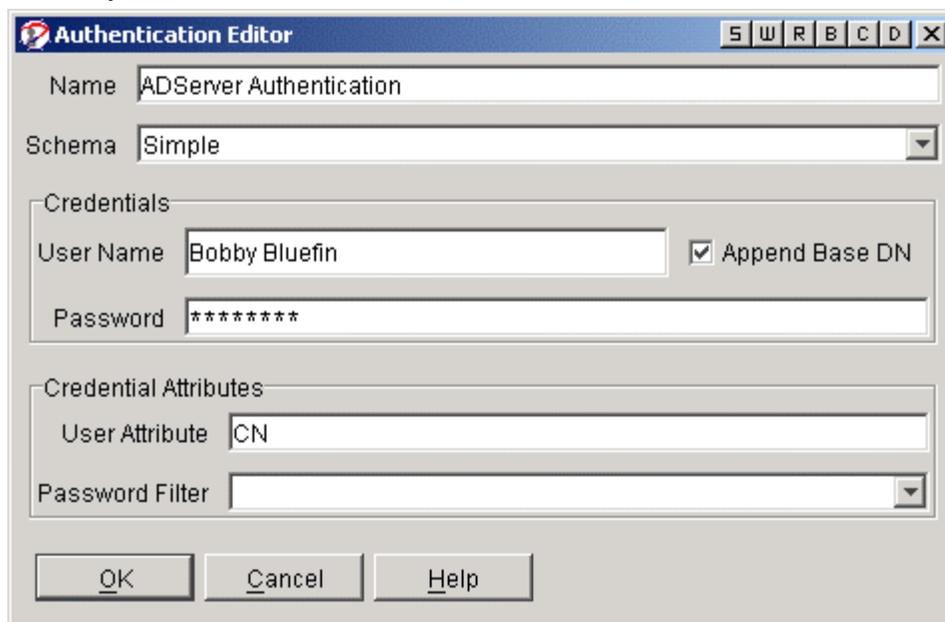


Figure 26: Creating the ADServer Authentication

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

NOTE: 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 Rhythmyx server.
- 2 Select the Directory Services tab.
- 3 Select the Directories tab.



Figure 27: 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.

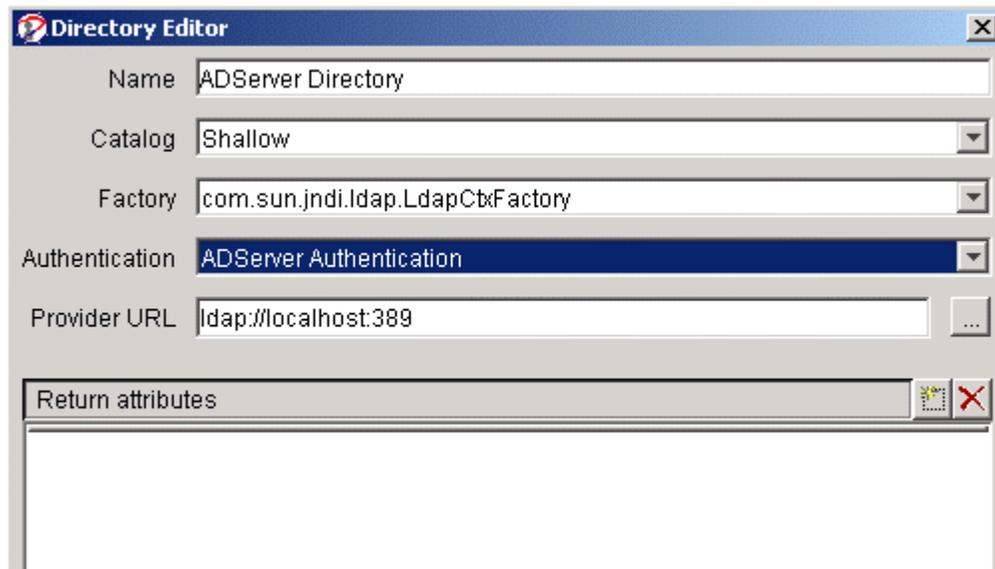


Figure 28: Directory Editor Dialog

- 6 Choose from the Authentication drop list the ADServer Authentication created in the section *Creating the Authentication* (on page 45).
- 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.

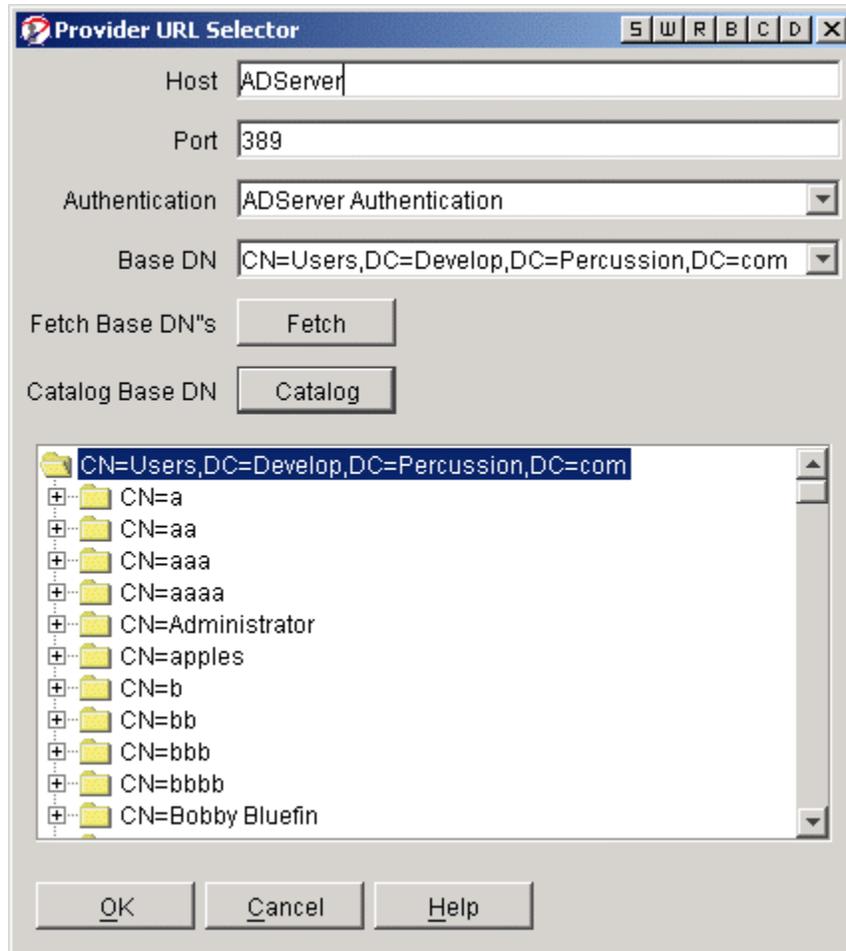


Figure 29: Provider URL Selector Dialog

NOTE: Rhythmyx 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.

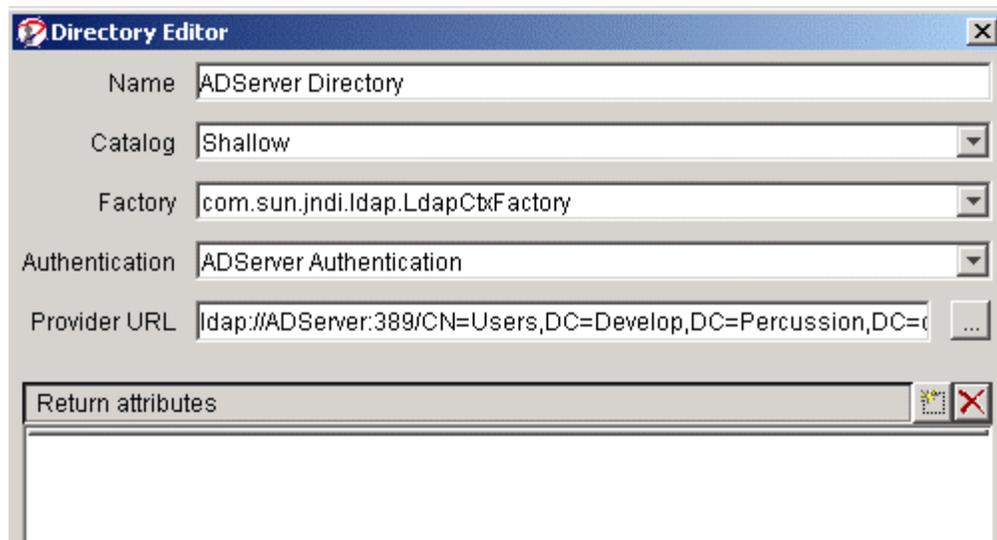


Figure 30: Directory Editor Dialog Showing Complete Provider URL

- 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 `usersName`, we would add the value, `cn=usersName`.
- 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 Rhythmyx server.
- 2 Click the Directory Services tab.

3 Click the Directory Sets tab.

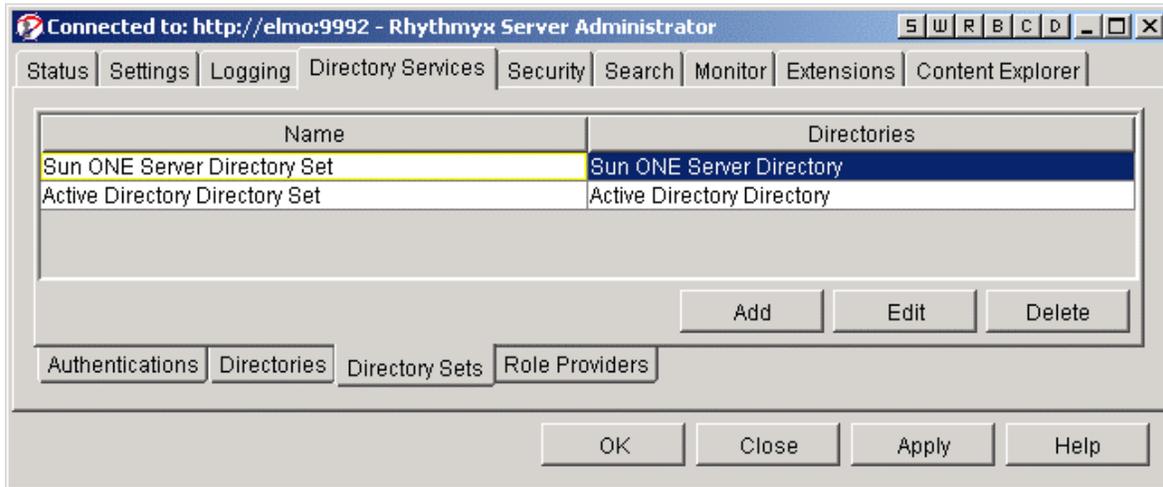


Figure 31: Directory Sets Tab

- 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 Rhythmyx. 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.

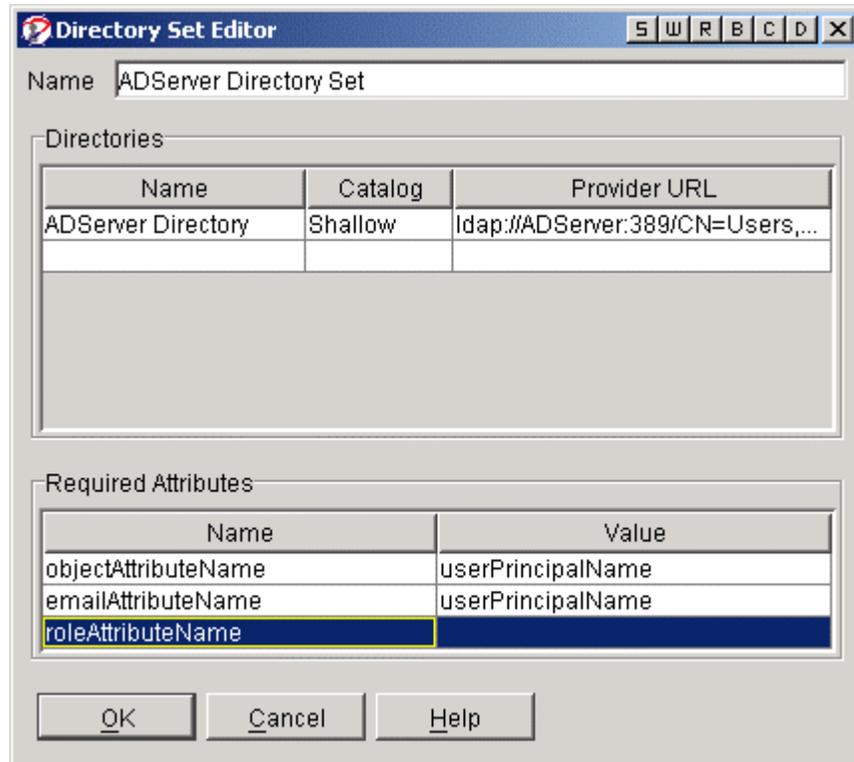


Figure 32: Directory Set Editor Dialog

- 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 Rhythmyx server.
- 2 Click the Security tab.

3 Click the Security Providers tab.

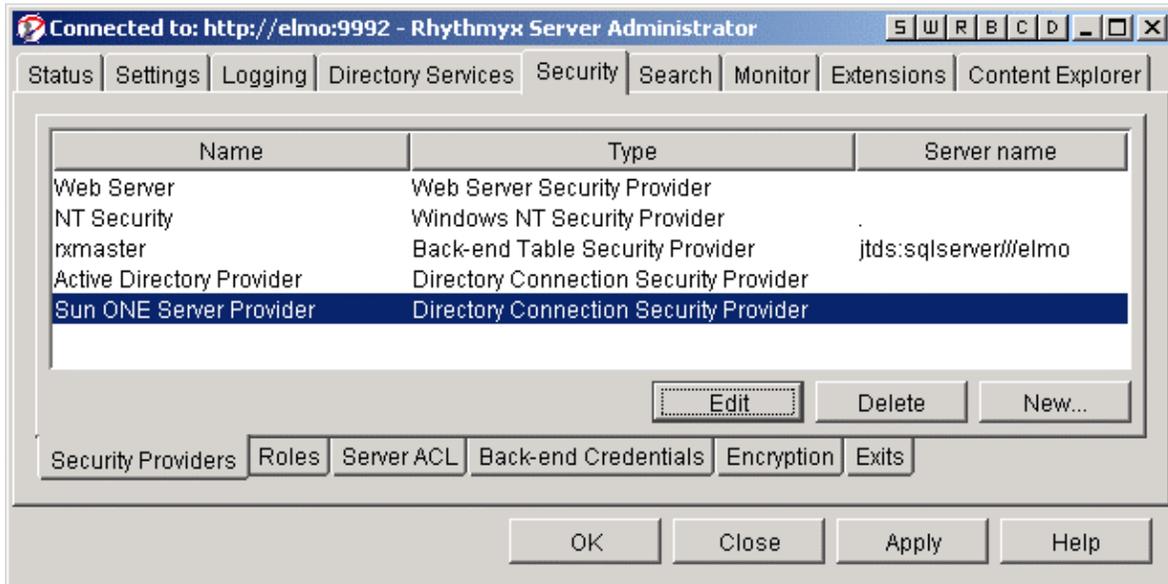


Figure 33: Security Providers Tab

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



Figure 34: Security Provider Details Dialog

- 8 Click the Group Providers tab.
- 9 Click the Insert New Entry icon (box to the right of the "Group Providers to make availa..." row under the Group Providers tab) to display the drop list.

- 10** Choose, "Create New.." from the drop list. The Group Provider Details dialog appears.



Figure 35: Group Providers Tab

- 11** 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.
- 12** 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.

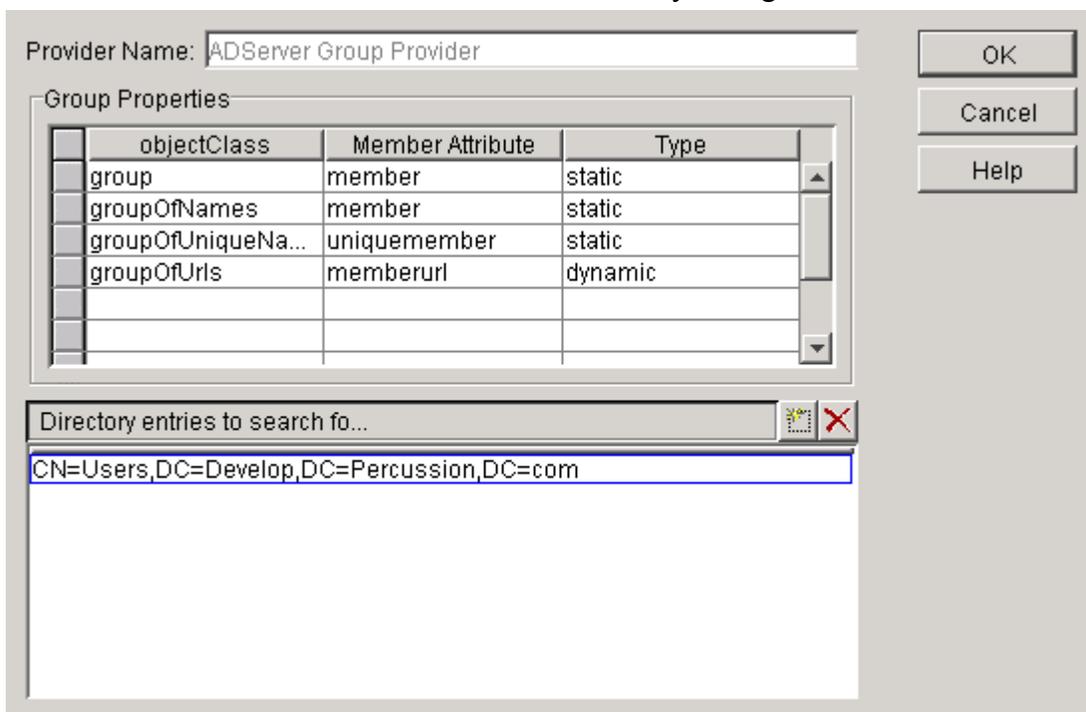


Figure 36: Group Provider Details Dialog

- 13** Click [OK] to save the Group Provider Registration.
- 14** Click [OK] to save the Provider Properties Registration.
- 15** Click [Apply] to register the new 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 Rhythmyx Roles.

- 1 Start the Server Administrator client and connect to the Rhythmyx server.
- 2 Select the Security tab.
- 3 Select the Roles tab.

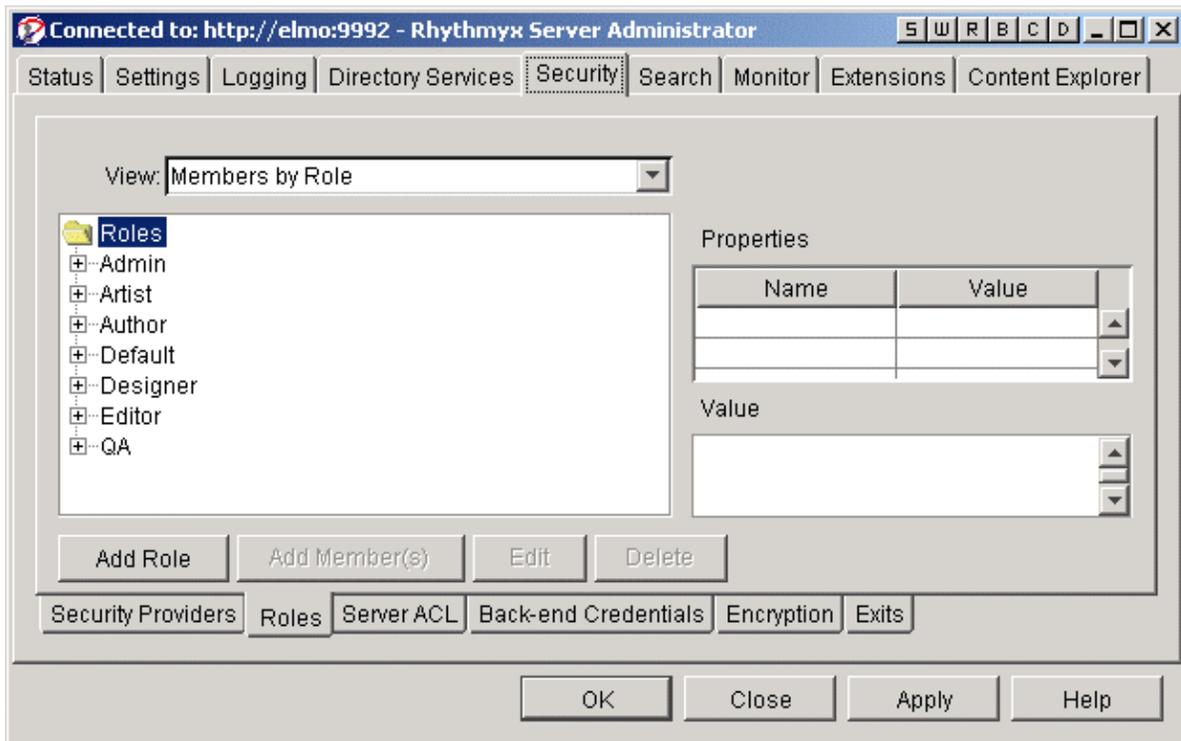


Figure 37: Roles Tab

NOTE: 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.

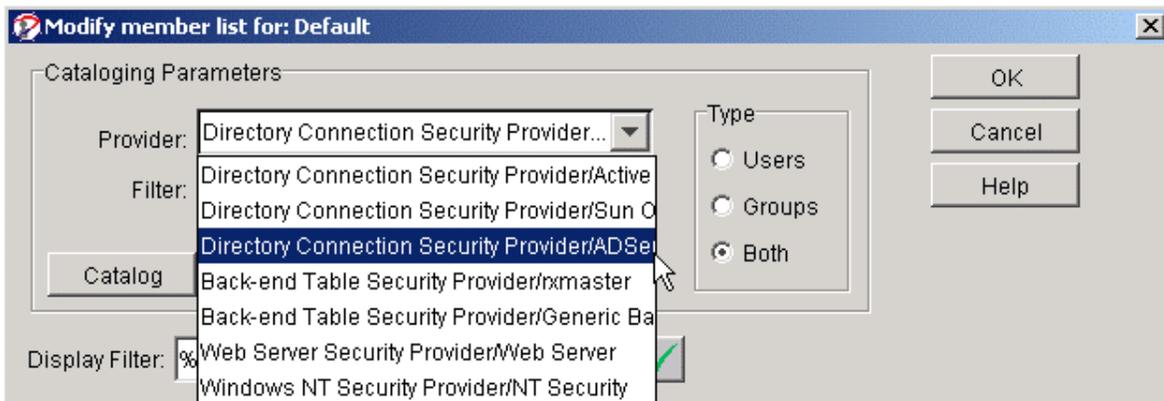


Figure 38: Choosing the AdServer Security Provider

- 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.

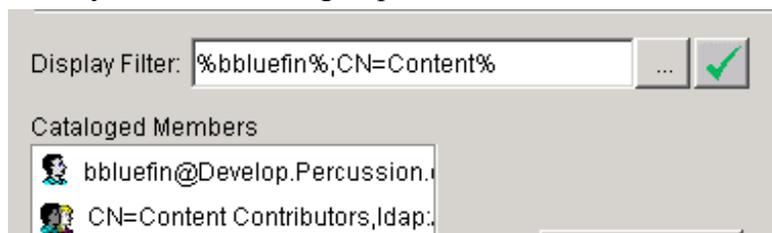


Figure 39: Result of Filtered Search on ADServer Directory Server

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

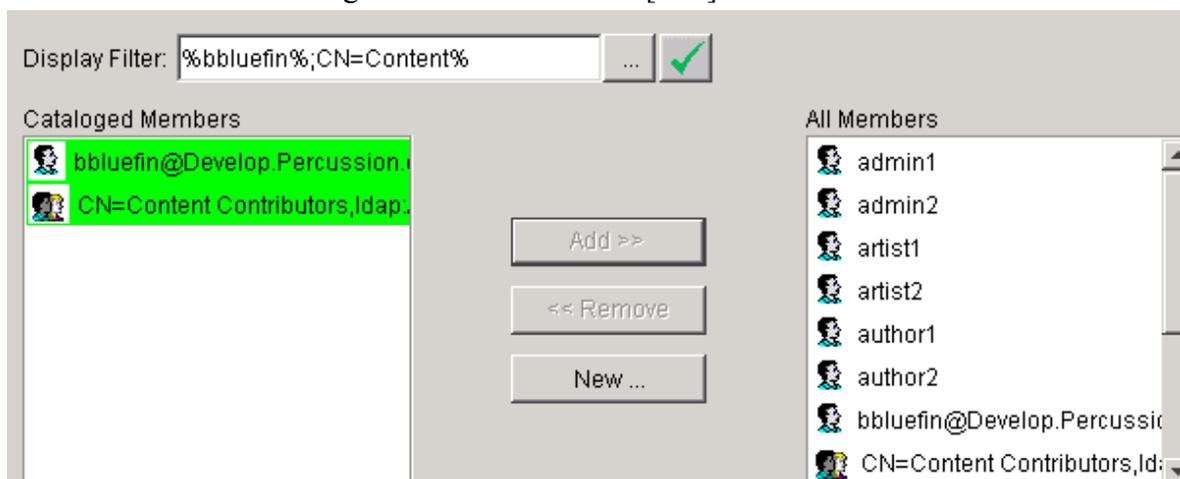


Figure 40: Cataloged Members Added to Default Role

- 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 Security 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 Security 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 (bbbluefin@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 Rhythmyx while Default describes their Community Role. Bobby has the Admin Functional Role and the Default Community Role.

NOTE: Though we will not map these directory objects directly to Rhythmyx Roles, the attribute values used to define each user's Role must exist as defined Roles in Rhythmyx. Using LDAP as a Role Provider does not generate a list of Roles to be used in Rhythmyx; instead, defining LDAP as a Role Provider implies that user objects searched during a query contain attributes that correlate to existing Rhythmyx 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* (on page 9).



Figure 41: Role Providers Tab

NOTE: 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 42: *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.

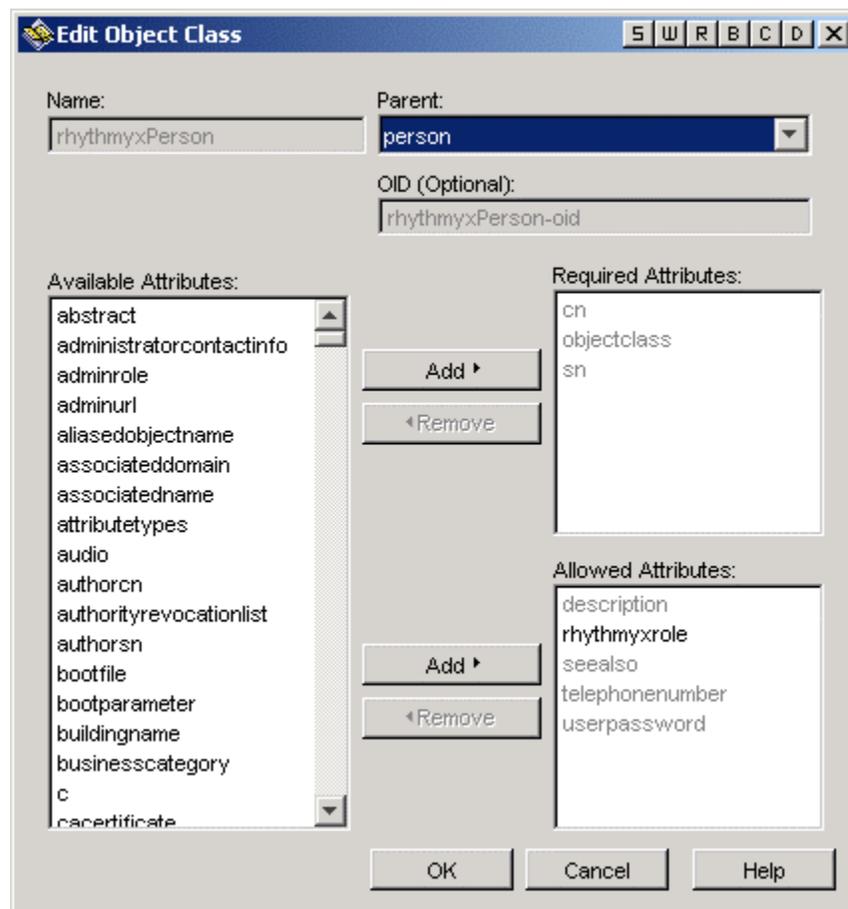


Figure 43: *rhythmyxPerson Object Class with rhythmyxrole Attribute*



Figure 44: *rhythmyxperson* Object Class Added

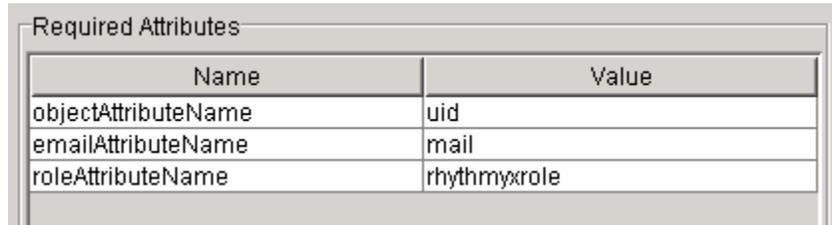
This, in turn, allowed our user object to inherit the attribute, `rhythmyxrole`. We then defined values for the `rhythmyxrole`. Each user was given a Functional and Community Role assignment.

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



Name	Value
objectAttributeName	uid
emailAttributeName	mail
roleAttributeName	rhythmyxrole

Figure 45: 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 Rhythmyx 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
 - Type - Directory
 - Directory Set - SOServer Directory Set

NOTE: By selecting Directory as the Role Provider Type, we are allowing only Roles in the Directory Set to be used for authorization.



Figure 46: Role Provider Editor

Creating the Directory Connection Security Provider

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

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

- Name - SOServer Directory Connection Security Provider
- Directory Set - SOServer Directory Set
- Role Provider - SOServer Role Provider



Figure 47: JNDI Security Provider Details Dialog

NOTE: The Group Providers tab is left blank as we will not be doing any manual mapping of groups to Rhythmyx Roles.

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