



Informatica™

Informatica® MDM Registry Edition  
10.0.0

# Security Framework Guide

This software and documentation contain proprietary information of Informatica LLC and are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright law. Reverse engineering of the software is prohibited. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica LLC. This Software may be protected by U.S. and/or international Patents and other Patents Pending.

Use, duplication, or disclosure of the Software by the U.S. Government is subject to the restrictions set forth in the applicable software license agreement and as provided in DFARS 227.7202-1(a) and 227.7702-3(a) (1995), DFARS 252.227-7013(1)(ii) (OCT 1988), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14 (ALT III), as applicable.

The information in this product or documentation is subject to change without notice. If you find any problems in this product or documentation, please report them to us in writing.

Informatica, Informatica Platform, Informatica Data Services, PowerCenter, PowerCenterRT, PowerCenter Connect, PowerCenter Data Analyzer, PowerExchange, PowerMart, Metadata Manager, Informatica Data Quality, Informatica Data Explorer, Informatica B2B Data Transformation, Informatica B2B Data Exchange Informatica On Demand, Informatica Identity Resolution, Informatica Application Information Lifecycle Management, Informatica Complex Event Processing, Ultra Messaging and Informatica Master Data Management are trademarks or registered trademarks of Informatica LLC in the United States and in jurisdictions throughout the world. All other company and product names may be trade names or trademarks of their respective owners.

Portions of this software and/or documentation are subject to copyright held by third parties, including without limitation: Copyright DataDirect Technologies. All rights reserved. Copyright © Sun Microsystems. All rights reserved. Copyright © RSA Security Inc. All Rights Reserved. Copyright © Ordinal Technology Corp. All rights reserved. Copyright © Aandacht c.v. All rights reserved. Copyright Genivia, Inc. All rights reserved. Copyright Isomorphic Software. All rights reserved. Copyright © Meta Integration Technology, Inc. All rights reserved. Copyright © Intalio. All rights reserved. Copyright © Oracle. All rights reserved. Copyright © Adobe Systems Incorporated. All rights reserved. Copyright © DataArt, Inc. All rights reserved. Copyright © ComponentSource. All rights reserved. Copyright © Microsoft Corporation. All rights reserved. Copyright © Rogue Wave Software, Inc. All rights reserved. Copyright © Teradata Corporation. All rights reserved. Copyright © Yahoo! Inc. All rights reserved. Copyright © Glyph & Cog, LLC. All rights reserved. Copyright © Thinkmap, Inc. All rights reserved. Copyright © Clearpace Software Limited. All rights reserved. Copyright © Information Builders, Inc. All rights reserved. Copyright © OSS Nokalva, Inc. All rights reserved. Copyright Edifecs, Inc. All rights reserved. Copyright Cleo Communications, Inc. All rights reserved. Copyright © International Organization for Standardization 1986. All rights reserved. Copyright © ej-technologies GmbH. All rights reserved. Copyright © Jaspersoft Corporation. All rights reserved. Copyright © International Business Machines Corporation. All rights reserved. Copyright © yWorks GmbH. All rights reserved. Copyright © Lucent Technologies. All rights reserved. Copyright (c) University of Toronto. All rights reserved. Copyright © Daniel Veillard. All rights reserved. Copyright © Unicode, Inc. Copyright IBM Corp. All rights reserved. Copyright © MicroQuill Software Publishing, Inc. All rights reserved. Copyright © PassMark Software Pty Ltd. All rights reserved. Copyright © LogiXML, Inc. All rights reserved. Copyright © 2003-2010 Lorenzi Davide, All rights reserved. Copyright © Red Hat, Inc. All rights reserved. Copyright © The Board of Trustees of the Leland Stanford Junior University. All rights reserved. Copyright © EMC Corporation. All rights reserved. Copyright © Flexera Software. All rights reserved. Copyright © Jinfonet Software. All rights reserved. Copyright © Apple Inc. All rights reserved. Copyright © Telerik Inc. All rights reserved. Copyright © BEA Systems. All rights reserved. Copyright © PDFlib GmbH. All rights reserved. Copyright © Orientation in Objects GmbH. All rights reserved. Copyright © Tanuki Software, Ltd. All rights reserved. Copyright © Ricebridge. All rights reserved. Copyright © Sencha, Inc. All rights reserved. Copyright © Scalable Systems, Inc. All rights reserved. Copyright © jqWidgets. All rights reserved. Copyright © Tableau Software, Inc. All rights reserved. Copyright © MaxMind, Inc. All Rights Reserved. Copyright © TMate Software s.r.o. All rights reserved. Copyright © MapR Technologies Inc. All rights reserved. Copyright © Amazon Corporate LLC. All rights reserved. Copyright © Highsoft. All rights reserved. Copyright © Python Software Foundation. All rights reserved. Copyright © BeOpen.com. All rights reserved. Copyright © CNRI. All rights reserved.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>), and/or other software which is licensed under various versions of the Apache License (the "License"). You may obtain a copy of these Licenses at <http://www.apache.org/licenses/>. Unless required by applicable law or agreed to in writing, software distributed under these Licenses is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the Licenses for the specific language governing permissions and limitations under the Licenses.

This product includes software which was developed by Mozilla (<http://www.mozilla.org/>), software copyright The JBoss Group, LLC, all rights reserved; software copyright © 1999-2006 by Bruno Lowagie and Paulo Soares and other software which is licensed under various versions of the GNU Lesser General Public License Agreement, which may be found at <http://www.gnu.org/licenses/lgpl.html>. The materials are provided free of charge by Informatica, "as-is", without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

The product includes ACE(TM) and TAO(TM) software copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University, Copyright (©) 1993-2006, all rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (copyright The OpenSSL Project. All Rights Reserved) and redistribution of this software is subject to terms available at <http://www.openssl.org> and <http://www.openssl.org/source/license.html>.

This product includes Curl software which is Copyright 1996-2013, Daniel Stenberg, <daniel@haxx.se>. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at <http://curl.haxx.se/docs/copyright.html>. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

The product includes software copyright 2001-2005 (©) MetaStuff, Ltd. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at <http://www.dom4j.org/license.html>.

The product includes software copyright © 2004-2007, The Dojo Foundation. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at <http://dojotoolkit.org/license>.

This product includes ICU software which is copyright International Business Machines Corporation and others. All rights reserved. Permissions and limitations regarding this software are subject to terms available at <http://source.icu-project.org/repos/icu/icu/trunk/license.html>.

This product includes software copyright © 1996-2006 Per Bothner. All rights reserved. Your right to use such materials is set forth in the license which may be found at <http://www.gnu.org/software/kawa/Software-License.html>.

This product includes OSSP UUID software which is Copyright © 2002 Ralf S. Engelschall, Copyright © 2002 The OSSP Project Copyright © 2002 Cable & Wireless Deutschland. Permissions and limitations regarding this software are subject to terms available at <http://www.opensource.org/licenses/mit-license.php>.

This product includes software developed by Boost (<http://www.boost.org/>) or under the Boost software license. Permissions and limitations regarding this software are subject to terms available at [http://www.boost.org/LICENSE\\_1\\_0.txt](http://www.boost.org/LICENSE_1_0.txt).

This product includes software copyright © 1997-2007 University of Cambridge. Permissions and limitations regarding this software are subject to terms available at <http://www.pcre.org/license.txt>.

This product includes software copyright © 2007 The Eclipse Foundation. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at <http://www.eclipse.org/org/documents/epl-v10.php> and at <http://www.eclipse.org/org/documents/edl-v10.php>.

This product includes software licensed under the terms at <http://www.tcl.tk/software/tcltk/license.html>, <http://www.bosrup.com/web/overlib/?License>, <http://www.stlport.org/doc/license.html>, <http://asm.ow2.org/license.html>, <http://www.cryptix.org/LICENSE.TXT>, <http://hsqldb.org/web/hsqldbLicense.html>, <http://httpunit.sourceforge.net/doc/license.html>, <http://jung.sourceforge.net/license.txt>, [http://www.gzip.org/zlib/zlib\\_license.html](http://www.gzip.org/zlib/zlib_license.html), <http://www.openldap.org/software/release/license.html>, <http://www.libssh2.org>, <http://slf4j.org/license.html>, <http://www.sente.ch/software/OpenSourceLicense.html>, <http://fusesource.com/downloads/license-agreements/fuse-message-broker-v-5-3-license-agreement>; <http://antlr.org/license.html>; <http://aopalliance.sourceforge.net/>; <http://www.bouncycastle.org/license.html>; <http://www.jgraph.com/jgraphdownload.html>; <http://www.jcraft.com/jsch/LICENSE.txt>; [http://jotm.objectweb.org/bsd\\_license.html](http://jotm.objectweb.org/bsd_license.html); <http://www.w3.org/Consortium/Legal/2002/copyright-software-20021231>; <http://www.slf4j.org/license.html>; <http://nanoxml.sourceforge.net/orig/copyright.html>; <http://www.json.org/license.html>; <http://forge.ow2.org/projects/javaservice/>; <http://www.postgresql.org/about/license.html>, <http://www.sqlite.org/copyright.html>, <http://www.tcl.tk/software/tcltk/license.html>, <http://www.jaxen.org/faq.html>, <http://www.jdom.org/docs/faq.html>, <http://www.slf4j.org/license.html>; <http://www.iodbc.org/dataspace/iodbc/wiki/IODBC/License>; <http://www.keplerproject.org/md5/license.html>; <http://www.toedter.com/en/jcalendar/license.html>; <http://www.edankert.com/bounce/index.html>; <http://www.net-snmp.org/about/license.html>; <http://www.openmdx.org/#FAQ>; [http://www.php.net/license/3\\_01.txt](http://www.php.net/license/3_01.txt); <http://srp.stanford.edu/license.txt>; <http://www.schneier.com/blowfish.html>; <http://www.jmock.org/license.html>; <http://xsom.java.net>; <http://benalman.com/about/license/>; <https://github.com/CreateJS/EaselJS/blob/master/src/easeljs/display/Bitmap.js>; <http://www.h2database.com/html/license.html#summary>; <http://jsoncpp.sourceforge.net/LICENSE>; <http://jdbc.postgresql.org/license.html>; <http://protobuf.googlecode.com/svn/trunk/src/google/protobuf/descriptor.proto>; <https://github.com/rantav/hector/blob/master/LICENSE>; <http://web.mit.edu/Kerberos/krb5-current/doc/mitK5license.html>; <http://jibx.sourceforge.net/jibx-license.html>; <https://github.com/lyokato/libgohash/blob/master/LICENSE>; <https://github.com/hjiang/jsonxx/blob/master/LICENSE>; <https://code.google.com/p/lz4/>; <https://github.com/jedisct1/libsodium/blob/master/LICENSE>; <http://one-jar.sourceforge.net/index.php?page=documents&file=license>; <https://github.com/EsotericSoftware/kryo/blob/master/license.txt>; <http://www.scala-lang.org/license.html>; <https://github.com/tinkerpop/blueprints/blob/master/LICENSE.txt>; <http://gee.cs.oswego.edu/dl/classes/EDU/oswego/cs/dl/util/concurrent/intro.html>; <https://aws.amazon.com/asl/>; <https://github.com/twbs/bootstrap/blob/master/LICENSE>; <https://sourceforge.net/p/xmlunit/code/HEAD/tree/trunk/LICENSE.txt>; <https://github.com/documentcloud/underscore-contrib/blob/master/LICENSE>, and <https://github.com/apache/hbase/blob/master/LICENSE.txt>.

This product includes software licensed under the Academic Free License (<http://www.opensource.org/licenses/afl-3.0.php>), the Common Development and Distribution License (<http://www.opensource.org/licenses/cddl1.php>) the Common Public License (<http://www.opensource.org/licenses/cpl1.0.php>), the Sun Binary Code License Agreement Supplemental License Terms, the BSD License (<http://www.opensource.org/licenses/bsd-license.php>), the new BSD License (<http://opensource.org/licenses/BSD-3-Clause>), the MIT License (<http://www.opensource.org/licenses/mit-license.php>), the Artistic License (<http://www.opensource.org/licenses/artistic-license-1.0>) and the Initial Developer's Public License Version 1.0 (<http://www.firebirdsql.org/en/initial-developer-s-public-license-version-1-0/>).

This product includes software copyright © 2003-2006 Joe Walnes, 2006-2007 XStream Committers. All rights reserved. Permissions and limitations regarding this software are subject to terms available at <http://xstream.codehaus.org/license.html>. This product includes software developed by the Indiana University Extreme! Lab. For further information please visit <http://www.extreme.indiana.edu/>.

This product includes software Copyright (c) 2013 Frank Balluffi and Markus Moeller. All rights reserved. Permissions and limitations regarding this software are subject to terms of the MIT license.

See patents at <https://www.informatica.com/legal/patents.html>.

DISCLAIMER: Informatica LLC provides this documentation "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of noninfringement, merchantability, or use for a particular purpose. Informatica LLC does not warrant that this software or documentation is error free. The information provided in this software or documentation may include technical inaccuracies or typographical errors. The information in this software and documentation is subject to change at any time without notice.

#### NOTICES

This Informatica product (the "Software") includes certain drivers (the "DataDirect Drivers") from DataDirect Technologies, an operating company of Progress Software Corporation ("DataDirect") which are subject to the following terms and conditions:

1. THE DATADIRECT DRIVERS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.
2. IN NO EVENT WILL DATADIRECT OR ITS THIRD PARTY SUPPLIERS BE LIABLE TO THE END-USER CUSTOMER FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR OTHER DAMAGES ARISING OUT OF THE USE OF THE ODBC DRIVERS, WHETHER OR NOT INFORMED OF THE POSSIBILITIES OF DAMAGES IN ADVANCE. THESE LIMITATIONS APPLY TO ALL CAUSES OF ACTION, INCLUDING, WITHOUT LIMITATION, BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS.

Publication Date: 2022-04-01

# Table of Contents

<b>Preface .....</b>	<b>6</b>
Learning About Informatica MDM Registry. ....	6
What Do I Read If. ....	7
Informatica Resources. ....	7
Informatica My Support Portal. ....	8
Informatica Documentation. ....	8
Informatica Product Availability Matrixes. ....	8
Informatica Web Site. ....	8
Informatica How-To Library. ....	8
Informatica Knowledge Base. ....	8
Informatica Support YouTube Channel. ....	9
Informatica Marketplace. ....	9
Informatica Velocity. ....	9
Informatica Global Customer Support. ....	9
<b>Chapter 1: Introduction to MDM Registry Security Framework.....</b>	<b>10</b>
Overview. ....	10
Features. ....	10
Architecture. ....	11
Informatica MDM-RE Security Concepts. ....	13
<b>Chapter 2: Configuration Tasks.....</b>	<b>14</b>
Overview. ....	14
Configuring Database. ....	14
Download and Install JDBC Library. ....	17
Configuring LDAP. ....	18
<b>Chapter 3: Setting Up LDAP.....</b>	<b>19</b>
Overview. ....	19
Setting Up LDAP. ....	19
Configuring LDAP. ....	20
Configuring LDAP Proxy server. ....	21
Starting and Stopping LDAP. ....	21
Loading Schema. ....	21
Setting Up LDAP Browser. ....	21
Installing LDAP Browser. ....	22
Directory Tree Structure for LDAP. ....	23
Import Configuration into LDAP. ....	28

<b>Chapter 4: Security Implementation.....</b>	<b>29</b>
Overview. . . . .	29
Security Client Interface APIs. . . . .	29
Configuring the Security Configuration File. . . . .	34
Configuring Security Framework by Using the Security APIs. . . . .	34
Configuring the Security Configuration File by Using a Sample File. . . . .	35
Configuration Parameters. . . . .	36
Disabling Authorization. . . . .	39
Encrypting the Security Configuration File. . . . .	40
Provisioning Users. . . . .	40
<b>Index.....</b>	<b>42</b>

# Preface

The Security Framework guide provides information on the security framework implemented with MDM Registry (MDM-RE).

This guide is written for use by system administrators who configures security and developers who are responsible to perform the security implementation. This guide assumes the user to have an understanding of security standards, protocols, and MDM-RE.

## Learning About Informatica MDM Registry

This section provides details of documentation available with the Informatica MDM Registry product.

### Introduction Guide

Introduces MDM Registry product and it's related terminology. It may be read by anyone with no prior knowledge of the product who requires a general overview of MDM Registry.

### Installation Guide

This manual is intended to be the first technical material a new user reads before installing the MDM Registry software, regardless of the platform or environment.

### Design Guide

This is a guide that describes the steps needed to design, define and load an MDM Registry "System".

### Developer Guide

This manual describes how to develop a custom search client application using the MDM - Registry Edition API.

### Operations Guide

This manual describes the operation of the run-time components of MDM - Registry Edition, such as servers, search clients and other utilities.

## Populations and Controls Guide

This manual describes SSA-Name3 populations and the controls they support. The latter are added to the Controls statement used within an IDX-Definition or Search-Definition section of the SDF.

## Security Framework Guide

This manual describes how to implement security in the MDM-RE product.

## Release Notes

The Release Notes contain information about what's new in this version of MDM - Registry Edition. It is also summarizes any documentation updates as they are published.

## What Do I Read If. . .

### I am. . .

. . . a business manager

The INTRODUCTION to MDM- Registry Edition will address questions such as "Why have we got MDM - Registry Edition?", "What does MDM - Registry Edition do"?

### I am. . .

. . . installing the product?

Before attempting to install MDM-RE, you should read the INSTALLATION GUIDE to learn about the prerequisites and to help you plan the installation and implementation of the MDM-Registry Edition.

### I am. . .

...an Analyst or Application Programmer?

A high-level overview is provided specifically for Application Programmers in the INTRODUCTION to MDM Registry Edition.

When designing and developing the application programs, refer to the DEVELOPER GUIDE which describes a typical application process flow and API parameters. Working example programs that illustrate the calls to MDM-RE in various languages are available under the <MDM-RE\_client\_installation>/samples directory.

### I am. . .

...designing and administering Systems?

The process of designing, defining and creating Systems is described in the DESIGN GUIDE. Administering the servers and utilities is described in the OPERATIONS manual.

## Informatica Resources

## Informatica My Support Portal

As an Informatica customer, the first step in reaching out to Informatica is through the Informatica My Support Portal at <https://mysupport.informatica.com>. The My Support Portal is the largest online data integration collaboration platform with over 100,000 Informatica customers and partners worldwide.

As a member, you can:

- Access all of your Informatica resources in one place.
- Review your support cases.
- Search the Knowledge Base, find product documentation, access how-to documents, and watch support videos.
- Find your local Informatica User Group Network and collaborate with your peers.

## Informatica Documentation

The Informatica Documentation team makes every effort to create accurate, usable documentation. If you have questions, comments, or ideas about this documentation, contact the Informatica Documentation team through email at [infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com). We will use your feedback to improve our documentation. Let us know if we can contact you regarding your comments.

The Documentation team updates documentation as needed. To get the latest documentation for your product, navigate to Product Documentation from <https://mysupport.informatica.com>.

## Informatica Product Availability Matrixes

Product Availability Matrixes (PAMs) indicate the versions of operating systems, databases, and other types of data sources and targets that a product release supports. You can access the PAMs on the Informatica My Support Portal at <https://mysupport.informatica.com>.

## Informatica Web Site

You can access the Informatica corporate web site at <https://www.informatica.com>. The site contains information about Informatica, its background, upcoming events, and sales offices. You will also find product and partner information. The services area of the site includes important information about technical support, training and education, and implementation services.

## Informatica How-To Library

As an Informatica customer, you can access the Informatica How-To Library at <https://mysupport.informatica.com>. The How-To Library is a collection of resources to help you learn more about Informatica products and features. It includes articles and interactive demonstrations that provide solutions to common problems, compare features and behaviors, and guide you through performing specific real-world tasks.

## Informatica Knowledge Base

As an Informatica customer, you can access the Informatica Knowledge Base at <https://mysupport.informatica.com>. Use the Knowledge Base to search for documented solutions to known technical issues about Informatica products. You can also find answers to frequently asked questions, technical white papers, and technical tips. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team through email at [KB\\_Feedback@informatica.com](mailto:KB_Feedback@informatica.com).



## Informatica Support YouTube Channel

You can access the Informatica Support YouTube channel at <http://www.youtube.com/user/INFASupport>. The Informatica Support YouTube channel includes videos about solutions that guide you through performing specific tasks. If you have questions, comments, or ideas about the Informatica Support YouTube channel, contact the Support YouTube team through email at [supportvideos@informatica.com](mailto:supportvideos@informatica.com) or send a tweet to @INFASupport.

## Informatica Marketplace

The Informatica Marketplace is a forum where developers and partners can share solutions that augment, extend, or enhance data integration implementations. By leveraging any of the hundreds of solutions available on the Marketplace, you can improve your productivity and speed up time to implementation on your projects. You can access Informatica Marketplace at <http://www.informaticamarketplace.com>.

## Informatica Velocity

You can access Informatica Velocity at <https://mysupport.informatica.com>. Developed from the real-world experience of hundreds of data management projects, Informatica Velocity represents the collective knowledge of our consultants who have worked with organizations from around the world to plan, develop, deploy, and maintain successful data management solutions. If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at [ips@informatica.com](mailto:ips@informatica.com).

## Informatica Global Customer Support

You can contact a Customer Support Center by telephone or through the Online Support.

Online Support requires a user name and password. You can request a user name and password at <http://mysupport.informatica.com>.

The telephone numbers for Informatica Global Customer Support are available from the Informatica web site at <http://www.informatica.com/us/services-and-training/support-services/global-support-centers/>.

# CHAPTER 1

## Introduction to MDM Registry Security Framework

This chapter includes the following topics:

- [Overview, 10](#)
- [Architecture, 11](#)
- [Informatica MDM-RE Security Concepts, 13](#)

### Overview

MDM Registry Edition (MDM-RE) is a software to add search and matching applications to identity data stored in databases and Data Warehouses.

MDM Registry Security Framework is a Java security framework that performs authentication, authorization, cryptography, session management, and provisioning. The framework hides implementation complexities and it exposes a simple API interface that can save developer efforts in securing any application. MDM-RE security provides role-based authentication and authorization on users.

The MDM-RE Security Framework guide describes features of framework, architecture, configuration, and how to configure the framework.

### Features

The MRBS framework provides the following features:

#### **Authentication**

Authentication is the process of verifying the identity of a user to ensure that the user is valid. A user is an *individual* who wants to access the Informatica MDM-RE resources.

#### **Authorization**

Authorization is the process of determining whether a user has sufficient privileges to access the requested resource.

#### **Provisioning**

Provisioning is a process of implementing and managing the security policies for an application. Provisioning includes the following:

1. Create/Delete Users

2. Create User roles and User groups
3. System resources that needs secure access
4. Privileges and Permissions

To create the security policies to access the system resources, Provisioning creates permissions using privileges and assigning roles to permissions and roles to users.

#### **Cryptography**

Supports crypto algorithms for securing user credentials.

#### **Cache Manager**

The MRBS framework uses cache for better performance.

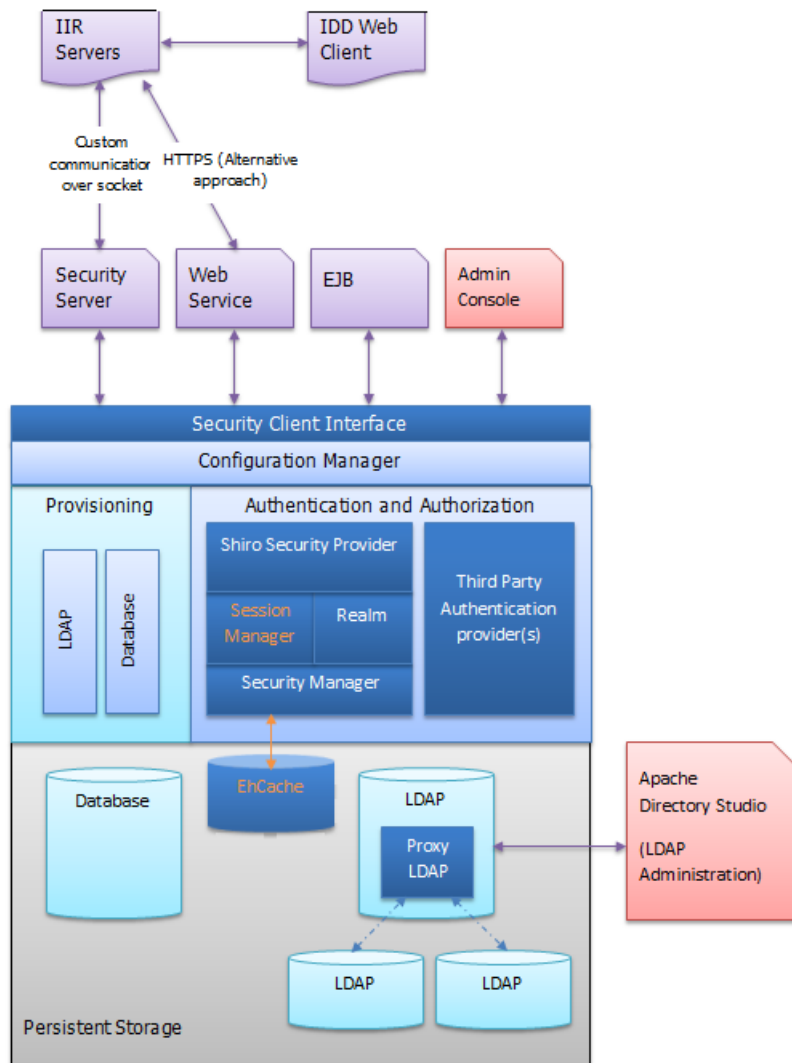
#### **Back-end support**

Database or a directory service such as LDAP (Light-Weight Directory Access Protocol) stores the application specific data such as Users, Resources, Privileges, and Permissions.

## Architecture

The security framework is a generic framework that enables users to perform authentication and authorization on top of a new security provider or an existing security provider. The framework hides implementation complexities and exposes a simple API interface that can save developer's efforts in securing any application.

The security framework consists of the Security Client Interface and Configuration Manager. The following figure shows the security framework architecture:



### Security Client Interface

The main client interface that exposes a set of APIs for client applications. The client application uses these APIs to build a security around its data model. The framework requires the user to configure the security provider using appropriate Configuration provider.

### Configuration Manager

The security framework can work with different security providers. At present, the MDM-RE Security Framework uses Apache Shiro. If required, MDM-RE can generalize to work with other third party frameworks in the future.

The framework also supports different persistent storages such as databases and LDAP directory service.

Using the Configuration Manager, you can configure the following in LDAP or Database store:

1. Security provider: Properties of the security provider
2. A persistence storage: Properties such as server address, and root user login details of the persistent storage.

The framework provides `IConfigProviderFactory` and `IConfigProvider` interfaces to enable users to configure the Security Provider that is running in the backend (may be LDAP or a database).

### **Authentication and Authorization**

The core module which performs the authentication of the user. After authenticating a user the user session stores the authentication information and generates a session token. The rest of the communication that is authorization from the client to framework uses this session token to validate the user.

For every user who has logged-in, the framework generates the authorization information by querying the persistence storage. The framework caches this authorization information into memory for boosting the performance.

### **Provisioning**

Provisioning manages the security policies for the following:

1. Creation or Deletion of users
2. User roles
3. Groups
4. System resources that needs secure access
5. Privileges and Permissions

The database or the directory services stores provisioning information.

### **Persistent Storage**

Persistent storage stores all the metadata of security framework. At present, the framework supports database and LDAP but is easily extensible for another storage if required.

### **RELATED TOPICS:**

- [“Security Client Interface APIs” on page 29](#)

## **Informatica MDM-RE Security Concepts**

Security is the ability to protect information privacy, confidentiality, and data integrity by guarding against unauthorized access. Before setting up security for Informatica MDM-RE implementation, it is important for you to understand some key concepts.

### **Authentication**

Authentication is the process of verifying the identity of a user to ensure that the user is a valid user.

A user is an individual who wants to access Informatica MDM-RE. MDM-RE authenticates based on the supplied credentials, user name / password.

### **Authorization**

Authorization is the process of determining whether a user has sufficient privileges to access a requested Informatica MDM-RE resource.

## CHAPTER 2

# Configuration Tasks

This chapter includes the following topics:

- [Overview, 14](#)
- [Configuring Database, 14](#)
- [Configuring LDAP, 18](#)

## Overview

The security framework requires certain configuration of the database and LDAP. After configuring the framework, MDM Registry Edition uses it for authentication and authorization of users.

Before you install MDM Registry Edition, perform the following configuration tasks for the security framework:

1. Configure database.
2. Configure and setup LDAP.
3. Create users.

For information about installing MDM Registry Edition, see the *MDM Registry Edition Installation Guide*.

## Configuring Database

MDM Registry Edition supports Oracle, Microsoft SQL Server, and IBM DB2 UDB databases. Configure the security framework to use the security information from the database or use the following default metadata, which is required to configure the framework appropriately.

You can find the scripts to create the required tables for different databases in the `$$SATOP/security/scripts` directory.

## Users

Column	Type	Description
REC_NO	INTEGER	The record index and is the primary key.
ID	VARCHAR(32)	User identifier. It must be unique.
FIRST_NAME	VARCHAR(64)	First name of the user.
LAST_NAME	VARCHAR(64)	Last name of the user.
EMAIL	VARCHAR(255)	Email address of the user.
PASSWORD	VARCHAR(512)	User's password.

## Roles

Column	Type	Description
REC_NO	INTEGER	The record index and is the primary key.
ID	VARCHAR(32)	Role identifier. It must be unique.
DESCRIPTION	VARCHAR(255)	Description about the role.

## Resources

Column	Type	Description
REC_NO	INTEGER	The record index and is the primary key.
ID	VARCHAR(32)	Resource identifier. It must be unique.
DESCRIPTION	VARCHAR(255)	Description about the resources.

## Privileges

Column	Type	Description
REC_NO	INTEGER	The record index and is the primary key.
ID	VARCHAR(32)	Privilege identifier. It must be unique.
DESCRIPTION	VARCHAR(255)	Description about the privilege.

## Groups

Column	Type	Description
REC_NO	INTEGER	The record index and is the primary key.
ID	VARCHAR(32)	Group identifier. It must be unique.
DESCRIPTION	VARCHAR(255)	Description about the group.

## Permissions

Column	Type	Description
REC_NO	INTEGER	The record index and is the primary key.
ID	VARCHAR(32)	Permission identifier. It must be unique.
RESOURCE_ID	INTEGER	Reference to resource record.
DESCRIPTION	VARCHAR(255)	Description about the permission.

## Privileges of permission

Column	Type	Description
PERMISSION_ID	INTEGER	Reference to permission record.
PRIVILEGE_ID	INTEGER	Reference to privilege record.

## User to role

Column	Type	Description
USER_ID	INTEGER	Reference to user record.
ROLE_ID	INTEGER	Reference to role record.

## User to group

Column	Type	Description
USER_ID	INTEGER	Reference to user record.
GROUP_ID	INTEGER	Reference to group record.



## Roles to permissions

Column	Type	Description
ROLE_ID	INTEGER	Reference to role record.
PERMISSION_ID	INTEGER	Reference to permission record.

To create schema, use the following commands:

For Oracle:

```
sqlplus <user>/<password>@service @secora.sql
```

For Microsoft SQL Server:

```
sqlcmd -U <User Id> -P <Password> -S <Server> -i secmsq.sql
```

For IBM DB2 UDB:

- Edit the `secudb.sql` file and update the line

```
CONNECT TO <service>USER <user> USING "<password>";  
db2 -tf secudb.sql
```

## Download and Install JDBC Library

The Security Framework requires JDBC libraries to connect to the database. You must download and install the appropriate JDBC libraries from your database vendor.

1. Based on the database, download the required libraries.

The following table lists the required libraries for each supported database:

Database	Library Names
DB2	db2jcc.jar
Oracle	ojdbc5.jar Orai18n.jar dms.jar
Microsoft SQL	sqljdbc4 .jar

2. Copy the library files to the following directory:

- On Windows. <MDM Registry Edition Installation Directory>\security\lib
- On UNIX. <MDM Registry Edition Installation Directory>/security/lib

3. If you use Oracle, copy the `dms.jar` file to the following directory:

- On Windows. <MDM Registry Edition Installation Directory>\tomcat\lib
- On UNIX. <MDM Registry Edition Installation Directory>/tomcat/lib

# Configuring LDAP

See the Configuring LDAP section.

## RELATED TOPICS:

- [“Configuring LDAP” on page 20](#)

# CHAPTER 3

## Setting Up LDAP

This chapter includes the following topics:

- [Overview, 19](#)
- [Setting Up LDAP, 19](#)
- [Configuring LDAP, 20](#)
- [Starting and Stopping LDAP, 21](#)
- [Setting Up LDAP Browser, 21](#)
- [Directory Tree Structure for LDAP, 23](#)
- [Import Configuration into LDAP, 28](#)

### Overview

Use LDAP (Lightweight Directory Access Protocol), Active Directory, or a database to store the application-specific data such as users, resources, privileges, and permissions. Active Directory is a directory service that Microsoft developed for Windows domain network. Active Directory uses LDAP as the core directory protocol.

### Setting Up LDAP

To set up a LDAP server on Linux machine:

1. You need to install Berkeley Database Version 11 gR2 (11.2.5.1.29) as one of the pre-requisite.

To download this software and for installation instructions, see the Oracle website.

**Note:** The latest version of Berkeley Database does not work with LDAP.

2. Before installing LDAP, set up the following environment variables:

```
$ LDFLAGS="-L/usr/local/lib -L/usr/local/BerkeleyDB.5.1/lib -R/usr/local/BerkeleyDB.5.1/lib"
$ export LDFLAGS

$ CPPFLAGS="-I/usr/local/BerkeleyDB.5.1/include/"
$ export CPPFLAGS

$ LIBS="-ldb -lgcc_s"
```

```

$ export LIBS

$ LD_LIBRARY_PATH=/usr/local/BerkeleyDB.5.1/lib
$ export LIBRARY_PATH

```

- a. Ensure that the path for Berkeley DB.5.1 lib and include folder is correct.

```

$ configure --enable-ldap
$ make depend
$ su root -c 'make install'

```

3. To install LDAP Version (2.4.23 (20100719)), download it from <ftp://ftp.openldap.org/pub/OpenLDAP/openldap-stable/openldap-stable-20100719.tgz>

## Configuring LDAP

To configure LDAP:

1. Edit the default `slapd.conf` file installed as `/usr/local/etc/openldap/slapd.conf` on your computer.

To edit this file, see the latest copy of the `slapd.conf` file from the project repository, `$$SSATOP/security/scripts/slapd.conf`

2. If the following schema files are not available, you need to add these files:

```

include      /usr/local/etc/openldap/schema/core.schema
include      /usr/local/etc/openldap/schema/cosine.schema
include      /usr/local/etc/openldap/schema/inetorperson.schema

```

3. Enter the DBD database definitions as follows:

```

database      bdb
suffix        "dc=informatica,dc=com"

## Give Admins immediate write access:
access to dn.subtree="dc=informatica,dc=com"
    by group/organizationalRole/roleOccupant=
       "cn=Administrators,ou=Groups,dc=informatica,dc=com" write
    by * none break

## This rule is needed by authz-regexp
## (Note: Since uid is used in DN, user cannot change its own uid.)
access to attrs=uid
    by anonymous read
    by users read

## Grant access to passwords for auth, but allow users to change
## their own.
access to attrs=userPassword
    by anonymous auth
    by self write

## The default rule: Allow DNs to modify their own records. Give
## read access to everyone else.
access to *
    by self write
    by users read

rootdn        "cn=Manager,dc=informatica,dc=com"
rootpw        secret
directory     /usr/local/var/informatica-data

```

```
# Indices to maintain
index objectClass eq
Save and close slapd.conf file.
```

## Configuring LDAP Proxy server

If there is any other remote LDAP sever which hosts user information, you need to define it as a proxy server.

1. To define LDAP as a proxy server, edit the `slapd.conf` file as follows:

```
database ldap
uri "ldap://10.72.40.173:389"
suffix "dc=xyz,dc=com"
#idassert-authzFrom dn.subtree="ou=users,dc=xyz,dc=com"
```

2. Create the directories for database files as:

```
/usr/local/var/openldap-data
/usr/local/var/informatica-data
```

## Starting and Stopping LDAP

You can start and stop the LDAP server using commands.

1. To start the LDAP server, use the command:

```
$ su root -c /usr/local/libexec/slapd
```

2. To stop the LDAP server, use the command:

```
$ kill `pgrep slapd`
```

## Loading Schema

1. To load schema, use the command:

```
ldapadd -x -D "cn=Manager, dc=informatica,dc=com " -W -f$SSATOP/security/scripts/
ldapstore.ldif
```

This script will create the default schema required for the security system and will create default administrator user with user id as "admin" and default password as "password".

2. From the LDAP browser utility, add new users using the following command:

```
secuser -t<DB|LDAP> -x<config file> -a(add)|-d(delete) -u<Admin User Id> -p<Admin
password> -i<User ID> -f<First Name> -l<Last Name> -w<Password>
secuser -tLDAP -x$SSATOP/security/SecConfig.xml -a -uadmin -ppassword -ijsmith -fJohn -
lSmith -wmypassword
```

## Setting Up LDAP Browser

LDAP browser is an Eclipse plug-in of Apache Directory Studio. This tool helps to read and display the tree of LDAP Server. Use this tool to create, edit, and delete entries in the tree.

## Installing LDAP Browser

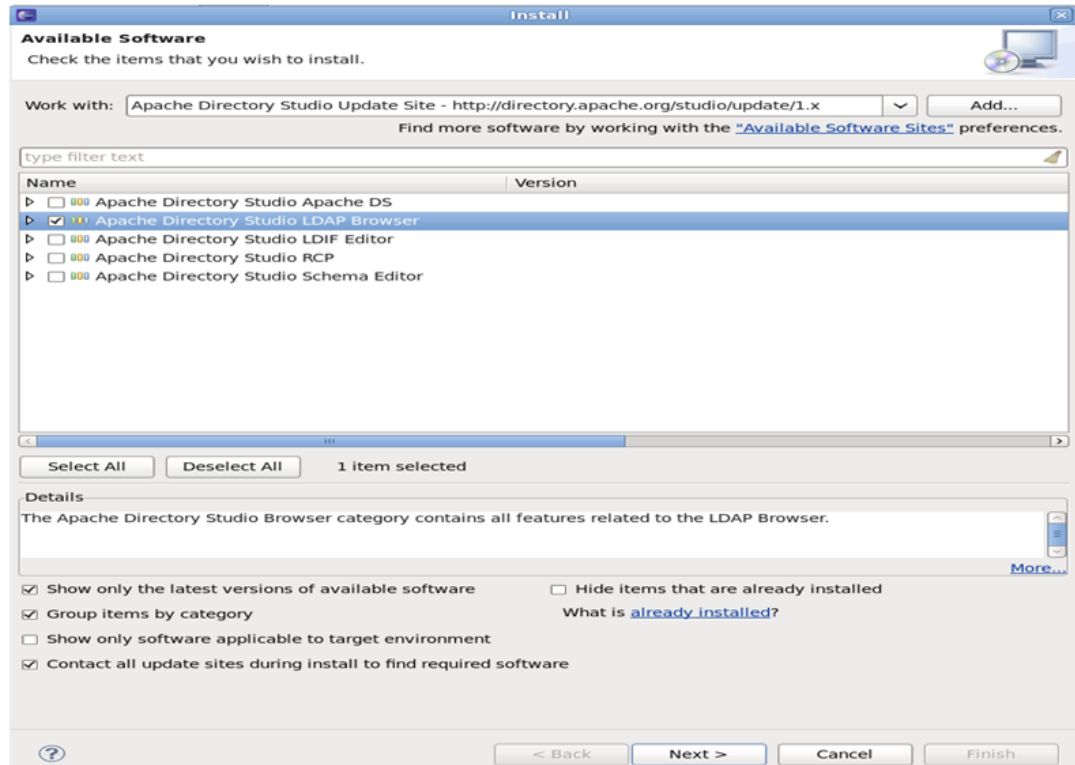
To install LDAP browser:

1. In Eclipse, go to **Help > Install new software**
2. Enter the required URL.

For more information, see the following website:

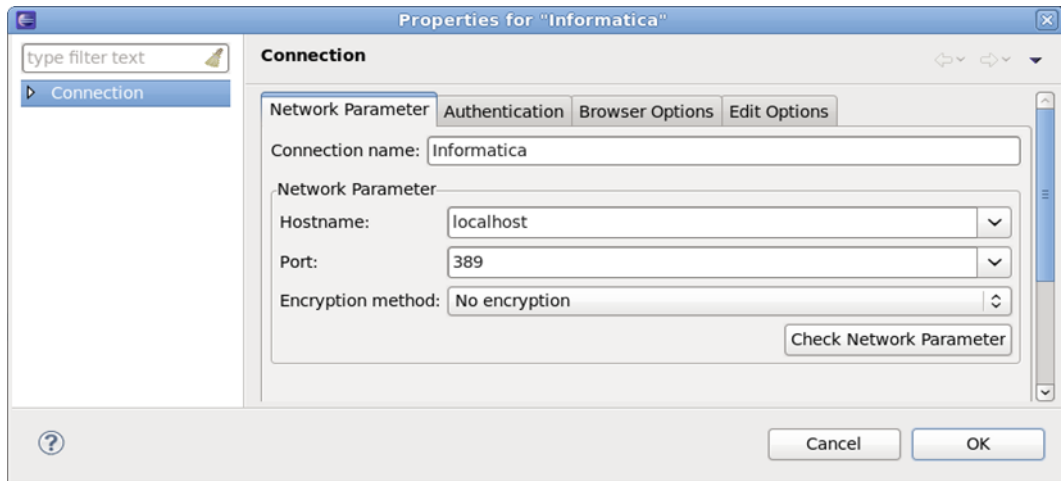
<https://directory.apache.org/studio/installation-in-eclipse.html>.

The following image shows a sample URL:

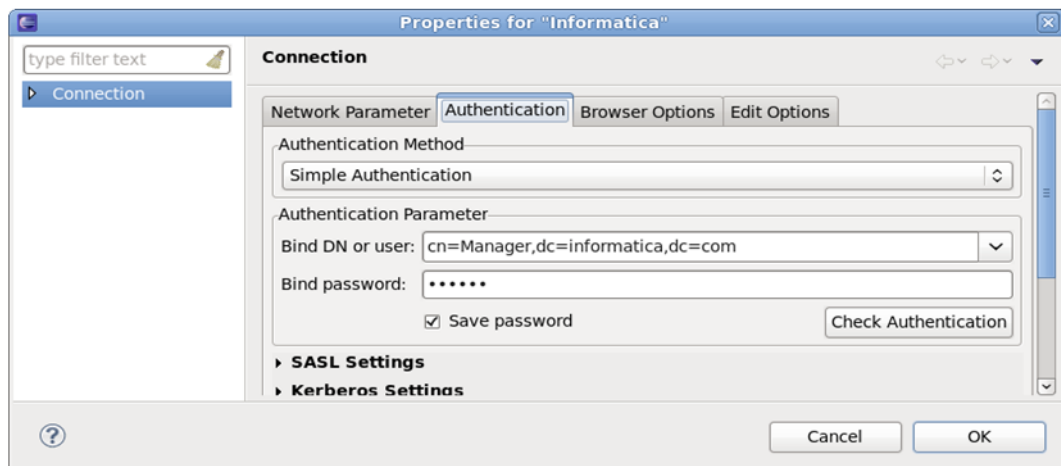


3. Select the LDAP browser and install the plug-in.
4. Open LDAP Perspective: In Eclipse go to **window > Open Perspective** and select **other**.
5. Create a connection for **informatica.com**.

6. Select the **Network Parameter** tab and enter the values for the fields as follows:

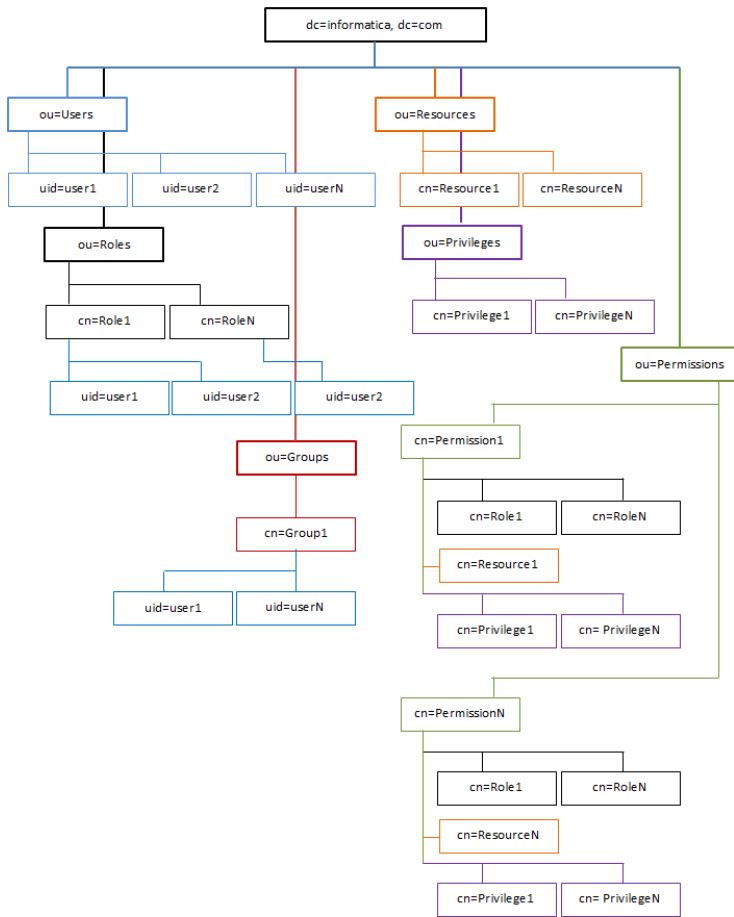


7. Select the **Authentication** tab and enter the values for the fields as follows:



## Directory Tree Structure for LDAP

Directory structure depicts the hierarchy of the organization. The following provides the directory tree structure for LDAP:



The following object classes for entities are provided:

### Root DN Record for organization

DN: dc=informatica,dc=com	
Attribute	Value
objectClass	dcObject
dc	organization (structural)
o	informatica
description	Informatica.com

### DN for Users

DN: ou=Users,dc=informatica,dc=com	
Attribute	Value
objectClass	organizationalUnit



ou	Users
description	Users of informatica.com

### DN for User

<b>DN: uid=xxxx,ou=Users,dc=informatica,dc=com</b>	
Attribute	Value
objectClass	inetOrgPerson
objectClass	organizationalPerson
objectClass	Person
cn	Common name
uid	Unique ID of user (xxxx)
userPassword	User password

### DN for Roles

<b>DN: ou=Users,dc=informatica,dc=com</b>	
Attribute	Value
objectClass	organizationalUnit
ou	Roles
description	Roles for the informatica.com

### DN for Role

<b>DN: ou=Roles,dc=informatica,dc=com</b>	
Attribute	Value
objectClass	organizationalRole
objectClass	top
cn	Name of a role
roleOccupant	uid=xxxx,ou=Users,dc=informatica,dc=com
roleOccupant	uid=yyyy,ou=Users,dc=informatica,dc=com

## DN for Resources

<b>DN: ou=Resources,dc=informatica,dc=com</b>	
<b>Attribute</b>	<b>Value</b>
objectClass	organizationalUnit
ou	Resources
description	Resources of informatica.com

## DN for Resource

<b>DN: cn=RESOURCE_NAME,ou=Resources,dc=informatica,dc=com</b>	
<b>Attribute</b>	<b>Value</b>
objectClass	organizationalRole
objectClass	top
cn	Name of a resource
Description	Description about the resource

## DN for Privileges

<b>DN: ou= Privileges,dc=informatica,dc=com</b>	
<b>Attribute</b>	<b>Value</b>
objectClass	organizationalUnit
ou	Privileges
Description	Access privileges for the system resources

## DN for Privilege

<b>DN: cn=PRIVILEGE_NAME,ou=Privileges,dc=informatica,dc=com</b>	
<b>Attribute</b>	<b>Value</b>
objectClass	organizationalRole
objectClass	top
cn	Name of a privilege
Description	Description about the privilege

## DN for Groups

DN: ou= Groups,dc=informatica,dc=com	
Attribute	Value
objectClass	organizationalUnit
ou	Groups
Description	Groups for the informatica.com

## DN for Group

DN: cn=GROUP_NAME,ou=Groups,dc=informatica,dc=com	
Attribute	Value
objectClass	organizationalRole
objectClass	top
cn	Name of a group
Description	Description about the group
roleOccupant	Users of the group

The ACL (access control list) uses the group entities to add restrictions on users. To provide admin users a write access to all, define the `slapd.conf` file as:

```
## Give Admins immediate write access:
access to dn.subtree="dc=informatica,dc=com"
by group/organizationalRole/roleOccupant=
"cn=Administrators,ou=Groups,dc=informatica,dc=com" write
by * none break
```

## DN for Permissions

DN: ou= Permissions,dc=informatica,dc=com	
Attribute	Value
objectClass	organizationalUnit
ou	Permissions
Description	Permissions for the informatica.com

## DN for Permission

<b>DN: cn=PERMISSION_NAME,ou=Permissions,dc=informatica,dc=com</b>	
<b>Attribute</b>	<b>Value</b>
objectClass	organizationalRole
objectClass	top
cn	Name of a permission
Description	Description about the permission
roleOccupant	Role entity cn=Admin,ou=Roles,dc=informatica,dc=com
roleOccupant	Resource entity cn=IDD_APPLICATION,ou=Resources,dc=informatica,dc=com
roleOccupant	Privilege entity cn=CREATE,ou=Privileges,dc=informatica,dc=com

## Import Configuration into LDAP

MDM-RE provides `ldif` files that can be imported into an existing LDAP store. The sample `ldif` scripts is found at the location: `$$$SATOP/security/scripts` directory.

To import the sample `ldif` into an LDAP store, run the following command:

```
ldapadd -x -D "cn=Manager, dc=informatica,dc=com" -W -f$$$SATOP/security/scripts/ldapstore.ldif
```

## CHAPTER 4

# Security Implementation

This chapter includes the following topics:

- [Overview, 29](#)
- [Security Client Interface APIs, 29](#)
- [Configuring the Security Configuration File, 34](#)
- [Disabling Authorization, 39](#)
- [Encrypting the Security Configuration File, 40](#)
- [Provisioning Users, 40](#)

## Overview

The security framework requires configuration parameters to enable security in MDM Registry Edition. The Security Client Interface exposes a list of security APIs for a developer to implement security.

To configure the security framework for MDM Registry Edition, specify the configuration parameters in a security configuration file, create users, and configure the MDM Registry Edition Security Server.

You can create a security configuration file by using the security APIs or the sample configuration files that MDM Registry Edition provides. A security configuration file contains information about the security provider, which can be LDAP or a database. MDM Registry Edition Security Server uses the security configuration file when the server starts.

## Security Client Interface APIs

The security framework exposes a set of APIs for a client application through the Security Client Interface, which is the main client interface to build security around the client application's data model. Use the APIs to perform the authentication, authorization, and provisioning tasks.

**Note:** MDM Registry Edition does not have a provisioning interface or an administration interface.

## Authentication and Authorization APIs

The following table describes the authentication and authorization APIs that the Security Client Interface exposes:

API	Description	Return Type
login	<code>login (String userId, String password)</code> throws <code>SecurityClientException</code> Performs a login attempt for a user.	byte[]
logout	<code>logout (byte[] sessionId)</code> throws <code>SecurityClientException</code> Logs out a user and invalidates and removes the associated session.	void
isPermitted	<code>isPermitted (byte[] sessionToken, String resourceId, String privilegeId)</code> throws <code>SecurityClientException</code> Returns true if the user is permitted to perform the action specified by the provided privilege against the provided resource.	boolean
isPermittedAll	<code>isPermittedAll (byte[] sessionToken, String resourceId, String...privilegeId)</code> throws <code>SecurityClientException</code> Returns true if the user is permitted to perform the actions specified by the provided privileges against the provided resource.	boolean
isPermittedAll	<code>isPermittedAll (byte[] sessionToken, String resourceId, Set&lt; String &gt; privilegeIds)</code> throws <code>SecurityClientException</code> Returns true if the user is permitted to perform the actions specified by the provided privileges against the provided resource.	boolean
hasRole	<code>hasRole (byte[] sessionToken, String roleId)</code> throws <code>SecurityClientException</code> Returns true if the user has the provided role.	boolean

## Provisioning APIs

The following table describes the provisioning APIs that the Security Client Interface exposes:

API	Description	Return Type
addOrUpdateResource	addOrUpdateResource (byte[] sessionToken, String resourceId, Properties resourceProperties) throws SecurityClientException <b>Add a new resource to the resource collection or update an existing resource.</b>	void
remove Resource	remove Resource (byte[] sessionToken, String resourceId) throws SecurityClientException <b>Removes resources from the resource collection.</b>	void
getAllResources	getAllResources (byte[] sessionToken) throws SecurityClientException <b>Get all the resources IDs accessible from this session.</b>	Set< String >
getResourceProperties	getResourceProperties (byte[] sessionToken, String resourceId) throws SecurityClientException <b>Return the resource properties.</b>	Properties
addOrUpdatePrivilege	addOrUpdatePrivilege (byte[] sessionToken, String privilegeId, Properties privilegeProperties) throws SecurityClientException <b>Add a new privilege or update an existing one.</b>	void
removePrivilege	removePrivilege (byte[] sessionToken, String privilegeId) throws SecurityClientException <b>Remove the privilege from the privileges collection.</b>	void
getAllPrivileges	getAllPrivileges (byte[] sessionToken) throws SecurityClientException <b>Return a collection of privileges granted to the user on the specified resource.</b>	Set< String >
getPrivilegeProperties	getPrivilegeProperties (byte[] sessionToken, String privilegeId) throws SecurityClientException <b>Return the privilege properties.</b>	Properties
addOrUpdateUser	addOrUpdateUser (byte[] sessionToken, String userId, Properties userProperties) throws SecurityClientException <b>Add a new user or update an existing one.</b>	void
removeUser	removeUser (byte[] sessionToken, String userId) throws SecurityClientException <b>Remove the user from the users collection.</b>	void

API	Description	Return Type
getAllUsers	getAllUsers (byte[] sessionToken) throws SecurityClientException <b>Get all the user IDs accessible from this session.</b>	Set< String >
getUserProperties	getUserProperties (byte[] sessionToken, String userId) throws SecurityClientException <b>Return the user properties.</b>	Properties
addOrUpdateRole	addOrUpdateRole (byte[] sessionToken, String roleId, Properties roleProperties) throws SecurityClientException <b>Add a new role or update an existing one.</b>	void
removeRole	removeRole (byte[] sessionToken, String roleId) throws SecurityClientException <b>Remove the role from the roles collection.</b>	void
getAllRoles	getAllRoles (byte[] sessionToken) throws SecurityClientException <b>Get all the role IDs accessible from this session.</b>	Set< String >
getRoleProperties	getRoleProperties (byte[] sessionToken, String roleId) throws SecurityClientException <b>Return the role properties.</b>	Properties
addOrUpdatePermission	addOrUpdatePermission (byte[] sessionToken, String permissionId, String resourceId, Set< String > privilegeId, Properties permissionProperties) throws SecurityClientException <b>Add a new permission or update an existing one.</b>	void
removePermission	removePermission (byte[] sessionToken, String permissionId) throws SecurityClientException <b>Remove the permission from the permissions collection.</b>	void
getAllPermission	getAllPermissions (byte[] sessionToken) throws SecurityClientException <b>Get all the permission IDs accessible from this session.</b>	Set< String >
getPermissionProperties	getPermissionProperties (byte[] sessionToken, String permissionId) throws SecurityClientException <b>Return the permission properties.</b>	Properties
getPermissionResourceId	getPermissionResourceId (byte[] sessionToken, String permissionId) throws SecurityClientException <b>Return the permission resource ID.</b>	String



API	Description	Return Type
getPermissionPrivilegesIds	getPermissionPrivilegesIds (byte[] sessionToken, String permissionId) throws SecurityClientException Return the permission privileges IDs.	Set< String >
getRolePermissionsIds	getRolePermissionsIds (byte[] sessionToken, String roleId) throws SecurityClientException Return the role permissions IDs.	Set< String >
getPermissionRoleIds	getPermissionRoleIds (byte[] sessionToken, String permissionId) throws SecurityClientException Return the role IDs of permission.	Set< String >
assignPermissionToRole	assignPermissionToRole (byte[] sessionToken, String permissionId, String roleId) throws SecurityClientException Assign permission to role.	void
revokePermissionFromRole	revokePermissionFromRole (byte[] sessionToken, String permissionId, String roleId) throws SecurityClientException Revoke permission from role.	void
assignRoleToUser	assignRoleToUser (byte[] sessionToken, String roleId, String userId) throws SecurityClientException Assign a role to a user.	void
revokeRoleFromUser	revokeRoleFromUser (byte[] sessionToken, String roleId, String userId) throws SecurityClientException Revoke a role from an user.	void
getAllUserRoles	getAllUserRoles (byte[] sessionToken, String userId) throws SecurityClientException Return a collection of roles IDs assign to user.	Set< String >
getAllUsersWithRole	getAllUsersWithRole (byte[] sessionToken, String roleId) throws SecurityClientException Return a collection of users IDs within role.	Set< String >
addOrUpdateUsersGroup	addOrUpdateUsersGroup (byte[] sessionToken, String usersGroupId, Properties usersGroupProperties) throws SecurityClientException Add a new users group or update an existing one.	void

API	Description	Return Type
removeUsersGroup	removeUsersGroup (byte[] sessionToken, String usersGroupId) throws SecurityClientException Remove the users group from the users group collection.	void
getAllUsersGroups	getAllUsersGroups (byte[] sessionToken) throws SecurityClientException Get all the users group IDs accessible from this session.	Set< String >
getUsersGroupProperties	getUsersGroupProperties (byte[] sessionToken, String usersGroupId) throws SecurityClientException Return the users group properties.	Properties
addUserToUserGroup	addUserToUserGroup (byte[] sessionToken, String usersGroupId, String userId) throws SecurityClientException Add a user to a users group.	void
removeUserFromUserGroup	removeUserFromUserGroup (byte[] sessionToken, String usersGroupId, String userId) throws SecurityClientException Remove a user from a users group.	void
getUsersFromUsersGroup	getUsersFromUsersGroup (byte[] sessionToken, String usersGroupId) throws SecurityClientException Get users IDs associated with the users group.	Set< String >
getUserGroupsForUser	getUserGroupsForUser (byte[] sessionToken, String userId) throws SecurityClientException Get users groups IDs for the user.	Set< String >

## Configuring the Security Configuration File

The security framework uses LDAP, Active Directory, or a database security provider. Before you use the security framework, you must specify the configuration parameters in a security configuration file. The security framework requires the security configuration file to implement security in MDM Registry Edition.

### Configuring Security Framework by Using the Security APIs

Use the `IConfigProvider` and `IConfigProviderFactory` interfaces to programmatically configure the security framework.

If you use LDAP, use the following `IConfigProvider` and `IConfigProviderFactory` interfaces:

```
IConfigProvider<?> configProvider;
IConfigProviderFactory<?> configs = null;
Class<LdapConfigProvider> ldapConfigProviderClass =
```

```

com.informatica.rbs.config.LdapConfigProvider.class;
    ConfigProviderFactory.registerProduct(SecurityUser.class.toString(), "SHIRO",
ldapConfigProviderClass);
    configs = new ConfigProviderFactory<LDAP>(<CustomImplementation>.class.toString());
    configProvider = configs.getInstance();
    configProvider.initProvider();

```

If you use a database security provider, use the following `IConfigProvider` and `IConfigProviderFactory` interfaces:

```

IConfigProvider<?> configProvider;
IConfigProviderFactory<?> configs = null;
Class<JdbcConfigProvider> jdbcConfigProviderClass =
com.informatica.rbs.config.JdbcConfigProvider.class;
    ConfigProviderFactory.registerProduct(SecurityUser.class.toString(), "SHIRO",
jdbcConfigProviderClass);
    configs = new ConfigProviderFactory<JDBC>(<CustomImplementation>.class.toString());
    configProvider = configs.getInstance();
    configProvider.initProvider();

```

Use the following APIs provided by the `IConfigProvider` interface:

- `initProvider()`
- `verifyProvider()`
- `readConfig("<File Name>")`. Reads an existing configuration XML file.
- `readConfigEncrypted("<File Name>")`. Reads an existing encrypted configuration file.
- `writeConfig("<File Name>")`. Writes a configuration file with the configured properties.

**Note:** To add or modify the security properties, you can use the other internal APIs that the security framework exposes.

Use the following APIs from the `IConfigProvider` interface to read the configuration parameters from a security configuration file or an encrypted dict file.

- `configProvider.readConfig("SecConfig.xml");` //Security configuration file
- `configProvider.readConfigEncrypted("SecConfig.dic");` //Encrypted configuration file

## Configuring the Security Configuration File by Using a Sample File

A security configuration file contains the configuration parameters that the security framework requires to implement security in MDM Registry Edition. The configuration parameters vary based on the security provider, which can be a database, LDAP, or Active Directory.

You can use the sample configuration files that you can find in the following directory to create a configuration file:

- On Windows: <MDM Registry Edition Installation Directory>\security\config
- On UNIX: <MDM Registry Edition Installation Directory>/security/config

To configure the security configuration file, perform the following tasks:

1. Perform one of the following tasks:
  - If you use the database security provider, open the `SecConfigJdbc<DBType>.xml` file, where `DBType` can be one of the following values:
    - `Msq` for Microsoft SQL Server
    - `Ora` for Oracle

- Udb for IBM DB2 UDB
  - If you use LDAP or Active Directory, open the `SecConfigLdap.xml` file.
2. Update the values of the configuration parameters, and save the file.
 

**Note:** If you use Active Directory, ensure that you change the value of the `Subtype` parameter to `PROVIDER_SUBTYPE_ADS`.
  3. Rename the file to `SecConfig.xml`.
  4. Move the `SecConfig.xml` file to the following directory:
    - On Windows: `<MDM Registry Edition Installation Directory>\security`
    - On UNIX: `<MDM Registry Edition Installation Directory>/security`

After you configure the security configuration file, configure the MDM Registry Edition Security Server. For more information about configuring the MDM Registry Edition Security Server, see the *MDM Registry Edition Installation and Upgrade Guide*.

## Configuration Parameters

Before you use the security framework, you must configure the configuration parameters for the security provider. The configuration parameters vary based on the security provider, which can be a database, LDAP, or Active Directory.

### Configuration Parameters for LDAP

The following table describes all the configuration parameters that LDAP requires:

Parameter	Description
URL	The LDAP server address for authentication and authorization.
AUTH_MECHANISM	The authentication mechanism for LDAP server.
SYSTEM_ACCOUNT	System account for the LDAP server.
SYSTEM_PASSWORD	Password for system account.
HASH_ALGORITHM_TYPE	Hash algorithm used for storing the user passwords.
USER_DN	Distinguished name for user entity.
USER_ATTRIBUTE_ID	Unique attribute ID for the user.
USER_QUERY	LDAP query for retrieving a particular users.
USER_OBJECT_CLASSES	Object classes for the User entity.
ROLE_DN	Distinguished name for role entity.
ROLE_ATTRIBUTE_ID	Unique attribute ID for the role.
RESOURCE_DN	Distinguished name for resources entity.
RESOURCE_ATTRIBUTE_ID	Unique attribute ID for the resources.

Parameter	Description
PRIVILEGE_DN	Distinguished name for Resources entity.
PRIVILEGE_ATTRIBUTE_ID	Unique attribute ID for the privileges.
PERMISSION_DN	Distinguished name for permissions entity.
PERMISSION_ATTRIBUTE_ID	Unique attribute ID for the permissions.
USERS_GROUP_DN	Distinguished name for users group entity.
USERS_GROUP_ATTRIBUTE_ID	Unique attribute ID for the permissions.
CACHE_MANAGER_CONF_FILE	Path to the cache manager file. Cache is for performance and session storage.
ACTIVE_SESSION_CACHE_NAME	Name of the cache.
ENABLE_AUTORIZATION_CACHE	Enable or disable cache for authorization information.
SESSION_TIME_OUT	Timeout value for the session, after this time user session expires.
REMEMBER_ME	Remember user credentials.

## Configuration Parameters for Active Directory

Before you configure the parameters for Active Directory, create two security groups named `IDD_ADMIN` and `IDD_APP_USER` in Active Directory. The `IDD_ADMIN` role has administrator privileges with which you can deploy an Informatica Data Director application. The `IDD_APP_USER` role has user privileges with which you can access a deployed Informatica Data Director application. You must assign the `IDD_ADMIN` and `IDD_APP_USER` roles to the appropriate users based on your requirement.

The following table describes all the configuration parameters that Active Directory requires:

Parameter	Description
URL	The Active Directory server address for authentication and authorization.
AUTH_MECHANISM	The authentication mechanism for the Active Directory server.
SYSTEM_ACCOUNT	System account for the Active Directory server.
SYSTEM_PASSWORD	Password for system account.
HASH_ALGORITHM_TYPE	Hash algorithm used for storing the user passwords.
USER_DN	Distinguished name for user entity.
USER_ATTRIBUTE_ID	Unique attribute ID for the user.
USER_QUERY	Active Directory query for retrieving a particular users.

Parameter	Description
USER_OBJECT_CLASSES	Object classes for the User entity.
ROLE_DN	Distinguished name for role entity.
ROLE_ATTRIBUTE_ID	Reserved for future use and do not remove the parameter.
RESOURCE_DN	Reserved for future use and do not remove the parameter.
RESOURCE_ATTRIBUTE_ID	Reserved for future use and do not remove the parameter.
PRIVILEGE_DN	Reserved for future use and do not remove the parameter.
PRIVILEGE_ATTRIBUTE_ID	Reserved for future use and do not remove the parameter.
PERMISSION_DN	Reserved for future use and do not remove the parameter.
PERMISSION_ATTRIBUTE_ID	Reserved for future use and do not remove the parameter.
USERS_GROUP_DN	Reserved for future use and do not remove the parameter.
USERS_GROUP_ATTRIBUTE_ID	Reserved for future use and do not remove the parameter.
CACHE_MANAGER_CONF_FILE	Path to the cache manager file. Cache is for performance and session storage.
ACTIVE_SESSION_CACHE_NAME	Name of the cache.
ENABLE_AUTHORIZATION_CACHE	Enable or disable cache for authorization information.
SESSION_TIME_OUT	Timeout value for the session, after this time user session expires.
REMEMBER_ME	Remember user credentials.
ADS_GROUPS_TO_ROLES_MAP	<p>Name of the map that defines the domain names for the <code>IDD_ADMIN</code> and <code>IDD_APP_USER</code> roles.</p> <p>You can use client tools, such as <code>ldp.exe</code> or an eclipse plug-in, to browse the Active Directory and view the domain names of the roles.</p> <p>For example:</p> <pre>&lt;ProviderMapProperties&gt;   &lt;Map name="ADS_GROUPS_TO_ROLES_MAP"&gt;     &lt;Property name="CN=IDD_ADMIN,CN=Builtin,DC=infatest,DC=local"&gt;IDD D_ADMIN&lt;/Property&gt;     &lt;Property name="CN=IDD_APP_USER,CN=Builtin,DC=infatest,DC=local " &gt;IDD_APP_USER&lt;/Property&gt;   &lt;/Map&gt; &lt;/ProviderMapProperties&gt;</pre>

## Configuration Parameters for a Database Security Provider

The following table describes all the configuration parameters that a database security provider requires:

Option	Description
DB_TYPE	Type of a database.
DB_SERVER_NAME	Address of database server.
DB_SERVER_PORT	Port address for the clients to connect the DB server.
DB_NETWORK_PROTOCOL	Network protocol for the DB connection, required for Oracle.
DB_DRIVER_TYPE	Driver type for the JDBC connection. For Oracle, the value is 'thin'.
DB_SERVICE_NAME	Service name, required when database is Oracle.
DB_USER	Database user which has admin rights of the database.
DB_PASSWORD	Password of the Database user.
DB_DATABASE_NAME	Name of the database.
HASH_ALGORITHM_TYPE	Hash algorithm used for storing the user passwords.
ENABLE_PERMISSION_LOOKUP	Enable or disable permission lookup.
AUTHENTICATION_QUERY	SQL query to perform authentication.
USER_ROLE_QUERY	SQL query to retrieve role for the particular user.
PERMISSION_QUERY	SQL query to retrieve permission details.
CACHE_MANAGER_CONF_FILE	Path to the Cache manager file. Cache is for performance and session storage.
ACTIVE_SESSION_CACHE_NAME	Name of the cache.
ENABLE_AUTHORIZATION_CACHE	Enable or disable cache for authorization information.
SESSION_TIME_OUT	Timeout value for the session, after this time user session expires.
REMEMBER_ME	Remember user credentials.

## Disabling Authorization

You can disable the authorization process based on your requirement. If you disable the authorization process, the security framework does not verify whether a user has sufficient privileges to access the requested resource. By default, the authorization process is enabled.

To disable the authorization process, configure the SSANOSECAUTHORIZATION environment variable to Yes and restart the MDM Registry Edition Server.

For example, `C:\InformaticaIR\bin>set SSANOSECAUTHORIZATION=Yes`

**Note:** If you use LDAP or a database security provider, you must disable the authorization process.

## Encrypting the Security Configuration File

Use the `secutil` command to encrypt or decrypt a security configuration file for security purposes.

The `secutil` utility uses the following syntax:

```
secutil -i<Input File> -o<Output File> [-d]
```

The `secutil` command uses the following parameters:

**-i<Input File>**

Absolute path for the security configuration file if you want to encrypt it or the encrypted dict file if you want to decrypt it. You can find the security configuration file, `SecConfig.xml`, in the following directory:

- On Windows: `<MDM Registry Edition Installation Directory>\security`
- On UNIX: `<MDM Registry Edition Installation Directory>/security`

**-o<Output File>**

Absolute path for the dict file if you want to encrypt a configuration file or the configuration file if you want to decrypt a dict file.

**-d**

Instructs the `secutil` utility to decrypt the specified dict file.

MDM Registry Edition Security Server uses the encrypted dict file when it starts. After you create the encrypted dict file, add the `SSA_SEC_DICT` environment variable to the following file:

- On Windows: `<MDM Registry Edition Installation Directory>\env\mdmres.bat`
- On UNIX: `<MDM Registry Edition Installation Directory>/env/mdmres`

For example:

- On Windows, to encrypt the security configuration file, run the following commands:

```
set SSA_SEC_CONFIG=%SSATOP%\security\SecConfig.xml
set SSA_SEC_DICT=%SSATOP%\security\SecConfig.dic
secutil -i%SSA_SEC_CONFIG% -o%SSA_SEC_DICT%
```

- On UNIX, to decrypt an encrypted dict file, run the following commands:

```
SSA_SEC_CONFIG="$SSATOP/security/SecConfig.xml"
SSA_SEC_DICT="$SSATOP/security/SecConfig.dic"
export SSA_SEC_DICT
$SSABIN/secutil -i$SSA_SEC_DICT -o$SSA_SEC_CONFIG -d
```

## Provisioning Users

Use the `secuser` utility to add or delete users. The utility requires a configuration file for the security provider.

The `secuser` utility uses the following syntax:

```
secuser -t<LDAP|DB> -x<Configuration File Name> -a|-d -u<Administrator User Name>
-p<Administrator Password> -i<User Name> -f<First Name> -l<Last Name> -w<Password>
```



The secuser command uses the following parameters:

**-t<LDAP|DB>**

Specifies whether you use LDAP or database security provider. Use `-tLDAP` for LDAP and `-tDB` for database.

**-x<Configuration File Name>**

Absolute path of the security configuration file. You can find the security configuration file, `SecConfig.xml`, in the following directory:

- On Windows: `<MDM Registry Edition Installation Directory>\security`
- On UNIX: `<MDM Registry Edition Installation Directory>/security`

**-a|-d**

Specifies whether you want to add or delete a user. Use `-a` to add a user and `-d` to delete a user.

**-u<Administrator User Name>**

Name of the administrator user.

**-p<Administrator Password>**

Password for the administrator user.

**-i<User Name>**

Name of the user that you want to add or delete.

**-f<First Name>**

First name of the user.

**-l<Last Name>**

Last name of the user.

**-w<Password>**

Password for the user that you add.

For example:

- On Windows, to add a user, run the following command:

```
secuser -tLDAP -x%SSA_SEC_CONFIG% -a -uadmin -ppassword -iuserid -ffirstname  
-llastname -wpassword
```

- On UNIX, to delete a user, run the following command:

```
secuser -tLDAP -x$SSA_SEC_CONFIG -d -uadmin -ppassword -iuserid -ffirstname  
-llastname -wpassword
```

# INDEX

## A

- access control list [23](#)
- Apache Directory Studio [21](#)
- APIs
  - Authentication and Authorization [29](#)
  - Provisioning [29](#)
- Authentication [13](#)
- Authorization [13](#)

## B

- Berkeley Database [19](#)

## C

- Configuration
  - JDBC [36](#)
  - LDAP [36](#)
- Configuration Manager [11](#)
- configuration options [36](#)
- configure
  - LDAP [20](#)
  - LDAP Proxy server [20](#)
- Cryptography [10](#)

## D

- directory tree structure [23](#)

## I

- install
  - LDAP [19](#)

- install (*continued*)
  - LDAP browser [21](#)

## L

- LDAP
  - start [21](#)
  - stop [21](#)

## M

- metadata [14](#)
- MRBS
  - Features [10](#)

## P

- Persistent Storage [11](#)
- Provisioning [11](#)

## S

- schema
  - load [21](#)
- Security Client Interface
  - APIs [29](#)
- security framework [14](#), [36](#)
- Security Server [11](#)
- slapd.conf [20](#)